BAOU
Education for All

स्वाध्यायः परम तपः

Dr. Babasaheb Ambedkar
Open University
(Established by Government of Gujarat)

Cyber Security

MSCIT - 304

Master of Science
Information Technology

2019

Cyber Security

Dr. Babasaheb Ambedkar Open University

Cyber Security

Course Writer

Dr. Ajay Patel
Dr. Amit Suthar
Mr. Nirav Parekh

Content Reviewer and Editor

Prof. (Dr.) Nilesh K. Modi

Language Editing

Prof. (Dr.) xxxxxx

June 2019
© Dr. Babasaheb Ambedkar Open University

ISBN-xxx-xx-xxx-xxxx-x

All rights reserved. No part of this work may be reproduced in any form by mimeograph or any other means, without written permission from the Dr. Babasaheb Ambedkar Open University.

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

Forward (Vice-Chancellor Message)

Dr. Babasaheb Ambedkar Open University

MCIT-304

Cyber Security

Block-1: Introduction to Cyber Security

UNIT-1
Cyber Security Essentials 02

UNIT-2
Attack Vectors, Threat, Risk and Vulnerability 16

UNIT-3
Advance Persistent Threat and Cyber Kill Chain 35

UNIT-4
Cyber Security Framework 49

Block-2: Network Defence Tools

UNIT-1
Firewall and Packet Filters 70

UNIT-2
Introduction to Windows and Linux Firewall 83

UNIT-3
Attacks on Wireless Networks 99

Block-3: Web Application Tools

UNIT-1
Scanning For Web Vulnerabilities Tools and HTTP Utilities 112

UNIT-2
Application Inspection Tools 128

UNIT-3
Password Cracking and Brute-Force Tools 143

UNIT-4
Web Attack 157

Block-4: Introduction to Cyber Crime, Law and Investigation

UNIT-1
Cyber Crimes 169

UNIT-2
Internet crime and Act 210

UNIT-3
Intellectual Property in the Cyber world 236

Block-1

Introduction to Cyber Security

Unit 1: Cyber Security Essentials

1

Unit Structure

1.1. Learning Objectives

1.2. What is Cyber Security?

1.3. Indian Cyberspace

1.4. Security Concepts

1.5. Basic Cryptography

1.6. Public Key Infrastructure

1.7. Let Us Sum Up

1.8. Check Your Progress:Possible Answers

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Define cyber security concepts
- Basic cryptography and its working
- Symmetric and asymmetric encryption
- Hash function and digital certificate
- Concept of public key

1.2WHAT IS CYBER SECURITY?

Cyber Security is a very complex term which passes through multi-dimensional request and response. In the current age, it is a challenging task for a small enterprise to big enterprise to secure themselves from external and internal cyber-attacks.

Cyber Security is a subset of information security which deals with securing the information, data and from both internal and external cyber threats. It is a proactive practice to safeguard the confidential information of the organization from unauthorized access by enforcing the layered security policies and protocol.

The task is more complex due to the variety of nature of cyber-attacks and the inability of quality response in the absence of adequate security measures.

The word 'Cyber' is not singular, it has its many forms to understand the concept using different terminologies such as:

- Cyber Space: It’s a virtual world of the digital data formed by bits.
- Cyber Economy: Complex structure of interconnected networked systems and its environment.

Cyber Space is a manmade ecosystem. It comprises of all interconnected networks, database, a source of information.

Cyber Space is not only including the software, hardware, data and information system, but the people surrounding it and social interaction within this network and infrastructure.

According to NIST (National Institute of Standards and Technology), Cyber Security is "The ability to protect or defend the use of cyberspace from cyber attacks."

1.3 INDIAN CYBERSPACE

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three Networks were set up: INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure; NICNET (the NIC Network), is a nationwide very small aperture terminal (VSAT) NW for public sector organizations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), to serve the academic and research communities.

India is an emerging country with a large scale change in digitization and scaling in all directions in every business sector. So at a national level, it is important to have the cybersecurity policy for the smooth functioning of its critical infrastructure such as Power Grids, Water Distribution, Rail Transportation, Metro Networks, Aviation Networks, Telecommunication Systems, Financial Sector, Public and Private Organizations, Healthcare and Education Sector.

Today's Cyber Space majority users are the citizens of the country using the interconnected networks of devices which is increasing every day. It is difficult to draw the boundary in the cyberspace among the different groups of people and data accessed by them.

So Indian Government has taken many initiatives in sectoral reforms and national level programs to create a safe cyber ecosystem which enables a user in access digital data and creates adequate trust and confidence in using them effectively and securely. Which includes Awareness programs, strengthen monitoring policy, Research, and Development in Cyber Security, Creating Open Standards, Strengthen Regulatory Framework, Protection of Critical Infrastructure.

There are various ongoing activities and programs of Government to address the current cybersecurity challenges and creating safe cyberspace and cyber economy

in the country. Below are some of the key initiatives launched by **GOI (Government of India)** such as:

NATIONAL CYBER SECURITY POLICY: This is created with an objective to build secure and resilient cyberspace for the citizens, businesses, and Government. It was released in 2013.

NATIONAL CYBER SECURITY COORDINATION CENTER(NCCC): The NCCC help to perform the real-time threat assessment and create early warning signs of potential cyber threats to the country.

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTER: This was created under section 70A of the Information Technology(IT) Act. It is established as a nodal agency in respect of the critical information infrastructure protection. Its aim is to protect the critical information infrastructure against the external and internal cyber threats along with the other threats.

CYBER SWACHHTA KENDRA: It was launched in 2017 to provide a platform for users to analyze and clean their systems from Viruses, Bots, Malware, Trojans, etc. It can be accessed using the following URL: *https://www.cyberswachhtakendra.gov.in*

INDIAN COMPUTER EMERGENCY RESPONSE TEAM(CERT-IN): It is National Incident Response Centre, operated under Department of Electronics and Information technology, Ministry of Communication and Information Technology, Government of India. Its primary role is to raise the security awareness among the citizens of Indian and provide the 24 x 7 technical assistance to the different organization in handling the critical security incidents.

NATIONAL TECHNICAL RESEARCH ORGANIZATION(NTRO): NTRO has the responsibility to look after the nations critical infrastructure security such as power grids, nuclear installation security, air traffic and control, monitoring satellite communications, UAV surveillance, Oil and Gas facilities.

It has three different wings. Information domination group looks after hacking and cyber applications. Net Security Team looks after emerging cyber-attacks and its analysis and mitigations. Research Group is looking towards the monitoring and surveillance of the internet.

NATIONAL INTELLIGENCE GRID (NATGRID): It is an integrated grid of connecting different state-run databases between intelligence agencies and organization providing information to enhance India's counter-terrorism measures. NATGRID would collect and collate information from different databases such as tax and bank account details, credit card information, visa and immigration records, itineraries of rail and air travel.

Combined data will be made available to 11 central agencies which are Research and Analysis Wing, Intelligence Beauro, Central Bureau of Investigation, Financial Intelligence Unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Board, Central Board of Excise and Customs and Directorate General of Excise and Customs.

Now below we will look at some fundamental concepts of principles of cybersecurity. Essentially in the following chapters, we will also learn more in detail regarding the Cyber Attacks, Vulnerability and Threats.

1.4SECURITY CONCEPTS

Information content & information determinacy determine the type of software applications. Content refers to input & output data, determinacy refers to the predictability of order & timing of information

There are three different tools which are useful for system designers to make a robust and secure product i.e. Confidentiality, Integrity, and Availability.

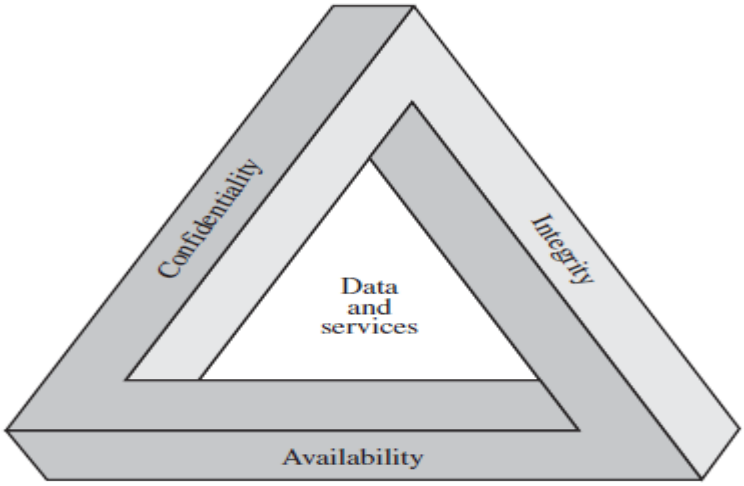


Figure 1 CIA Triad

In the above image, there are three key concepts shown and all three are related to each other, which is known as the CIA triad, it is considered to be the main pillars of the security, which anyone who protects an information system must understand: Confidentiality, Integrity, and Availability. Each component is critical to overall security, with the failure of any one component resulting in potential system compromise.

Confidentiality: It means to protect personal privacy information from unauthorized access to devices, processes or individuals. If we understand it in the parts, it can be described as Information must have protection enable from the different types of users to access it. There must be a limitation to access the information, who are authorized can only access the information. And last the authentication system which authenticates the user before accessing information.

Integrity: It normally refers to the data integrity, or to make ensure that data stored is accurate and no unauthorized modifications are done. The loss of integrity is considered as the unauthorized modification or destruction of the information. Disrupting a message in transit can have serious consequences.

For E.g.: if it is possible to modify the fund transfer message during online banking, an attacker can take this advantage to fulfill his or her benefit by stealing the credentials. So to ensure the integrity of this type of message is important for any security systems.

Availability: Ensuring the timely and reliable access of information to the authorized users for the systems to provide a value. The loss of the availability of the information is the loss or disruption of access to the information.

Although the use of CIA TRIAD to define security objective is well established, there are additional concepts which are important to learn and understand which makes the complete picture, they are Authentication, Authorization, and Nonrepudiation. Understanding each of the six concepts will help to implement robust security mechanisms.

Authentication: The primary goal is to focus the information on being genuine and source of the message for any security systems. This means that users are who they say and every piece of information came from the trusted source.

Nowadays we have seen Authentication system requires more than one factor of authentication, it is called Multifactor Authentication.

Such as password required combining with Fingerprint or retina scan or voice verification and PIN (Personal Identification Number), as it is useful in validating the user (owner of the fingerprint) and PIN number (something that user knows).

Authorization: It focuses on whether the user is verifiably granted permission to do so. When the system authenticates the user it also verifies and checks access privileges granted to the user. Which in simple terms means what a user can or cannot do while using the system.

Nonrepudiation: It is assuring that the sender of the data is provided with the proof of delivery and recipient is provided with the sender's identity, so neither can deny in later part of having processed the data. In the normal physical world, it can be understood as the notary done on the stamp paper for any kind of deals. Where neither of the parties can deny the deal in the later stages.

To meet such requirements, systems have to normally rely on the asymmetric cryptography or public key cryptography. While symmetric key systems use a single key to encrypt and decrypt the data. Asymmetric cryptography uses one key(private) for signing the data and another key(public) for verifying the data.

Check Your Progress 1

1. List all components of CIA TRIAD

   _____

2. What do we call if we combine Retina Scan with PIN

   _____

3. Which property ensures user is able to access data anywhere and anytime_____

1.5BASIC CRYPTOGRAPHY

This section will provide the information on basic cryptography to explain basics of ciphers and cryptanalysis. Our objective is to discuss the basic operation on

symmetric and asymmetric encryption algorithms. Also we will discuss the concept of the digital signatures.

The word cryptography is derived from the Greek and its literal translation is “hidden writing”. In the old times, it mostly used to send the secret messages in a way that the intended recipient can only be able to read.

Cryptography is a very critical and important part of the security applications, products, and applications in terms of using different cryptographic algorithms. Understanding how cryptography works it is important to understand to make sure that the data which is transferred between sender and receiver is safe. In early around 1900 bc Egyptians began to use pictographic to convey the secret message. This was known to be as ciphers.

Cryptography can be strong or weak. Its strength is measured in time and resources it would require to recover the plaintext.

1.5.1 HOW DOES CRYPTOGRAPHY WORK?

A cryptographic algorithm is a mathematical function which is used in encryption and decryption process. While cryptography is a science of securing data, cryptanalysis is the science of analyzing and breaking secure communication without knowledge of the key.

Combining both *Cryptography* + *Cryptanalysis* = *Cryptology*

The most common to known is the classical cipher is the substitution cipher which works by substituting each letter in the alphabet with one another when writing the secret message. The key here is the number of characters which is used for substitution. Below is one such example:

abcdefghijklmnopqrstuvwxyz

nopqrstuvwxyzabcdefghijklm

where a=n, b=o, c=p, d=q and so on

Using this cipher, the message, “hello world” would be written as “uryybjbeyq”. It is a simple substitution cipher known as Caeser Cipher.

1.5.2 SYMMETRIC ENCRYPTION

Symmetric Encryption is also known as conventional encryption which has been introduced in the late 1970s. This technique is used to provide confidentiality for the data transmission or to store data using the symmetric encryption method. There are two well-known symmetric encryption algorithms used they are: Data Encryption Standard(DES) and Advanced Encryption Standard (AES), both algorithms are block cipher encryption algorithms.

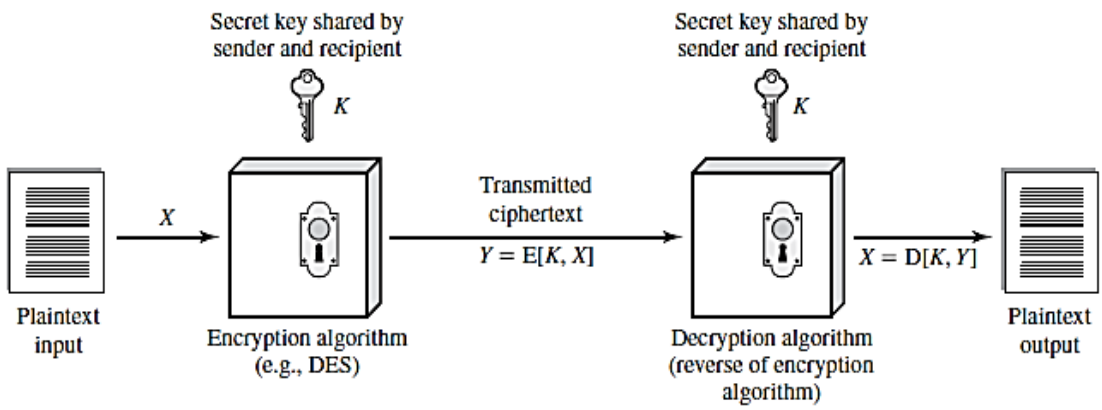


Figure 2 Symmetric Encryption Model

Let us understand each component which is shown in the above symmetric encryption model.

Plaintext: Original message or data provided as input into the algorithm.

Encryption Algorithm: Encryption algorithm used which performs operations on the plaintext.

Secret Key: Secret Key is also an input provided to the encryption algorithm. The exact number of substitution or transformations performed by an algorithm depending on the key.

Ciphertext: Encrypted message which is produced as output which depends on the plaintext and key used. For the same message, if there are different keys used, ciphertext will be different for both keys used.

Decryption Algorithm: It is the same encryption algorithm which runs in the reverse manner which takes the ciphertext and secret key as the input and generates the original plaintext.

There are two requirements for the symmetric encryption algorithms to work, the first one is strong encryption algorithms know to both the party sender and receiver and the second one is the secret key should be known only to sender and receiver only.

Ceaser cipher is a very form of symmetric key encryption. Symmetric cryptography doesn't address the following issue: Attacker can eavesdrop the shared key between sender and receiver and can steal the key and decrypt the data. This is where the concept of the Public Key Encryption OR Asymmetric key cryptography comes in picture.

1.5.3 ASYMMETRIC ENCRYPTION

Aasymmetric encryption is also known as Public Key key cryptography. It uses two mathematically related but unique keys: a public key and a private key. Each key has its own unique function. The public key is used to encrypt the data and the private key is used to decrypt the data. It is computationally infeasible to obtain the private key from the public key. Its primarily used for the authentication, non-repudiation and key exchange.

Anyone with the public key can encrypt the data but cannot decrypt the same. Only the appropriate receiver with the private key can decrypt the data. Even if the attacker knows that the sender is transmitting data to the receiver, also data passes through multiple channels, there is nothing he or she can do. As the data can only be decrypted by the private key.

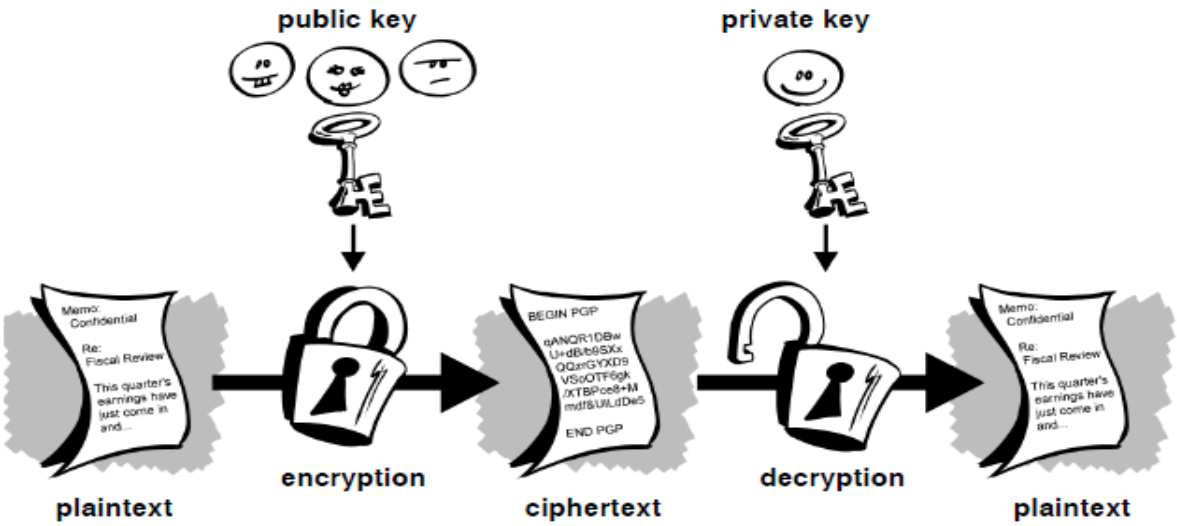


Figure 3 Asymmetric Encryption Model Source: PGP Corporation, Introduction to Cryptography

All communication which takes part between sender and receiver includes the public key. The private key is never shared, they are simply stored on the software or on the machine used. Some of the examples of the public key cryptosystem are Elgamal(named after its inventor Taher Elgamal), RSA (Ron Rivest, Adi Shamir, Leonard Adleman) which is most widely used even in current times. Diffie-Hellman.

1.5.4 HASH FUNCTIONS

Cryptographic Hash Functions are a mathematical algorithm that take the input of the arbitrary size of data and generates the fixed length hash value or message digest or simply digest and they are also designed to be the one-way functions. This means they are not reversible in nature.

There are few properties of the HASH Function which are mentioned below due to which they are still widely used in a different information security application.

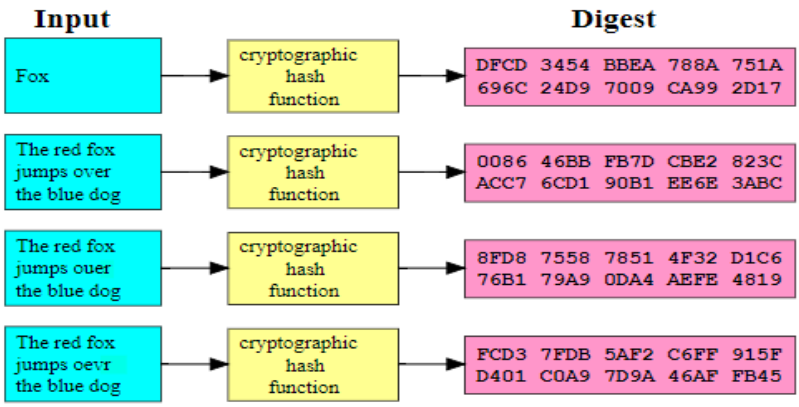


Figure 3 Hash Function Source: Wikipedia

- It is deterministic which means it will always give the same hash value for the same input message.
- Computing hash value of the message is faster.
- It is infeasible to generate the same message from the hash value.
- Even a very small change in the message will change the hash value completely.
- It is infeasible to find two different messages with the same hash value.

Due to such properties they are widely used for digital signatures, Message Authentication Code, Indexing data in the hash table, fingerprinting, finding duplicate data, Checksums to identify any modification in data.

Hash Algorithms which are commonly used today:

- **Message Digest(MD) Algorithm:** A byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message. There are various versions of these algorithms present such as MD2(RFC 1319), MD4(RFC 1320), MD5(RFC 1321).

  MD5 is the third message digest algorithm after MD3 and MD4, which process data in 512-bit blocks which is broke down into 16 words composed of 32 bit each. The output from MD5 is 128-bit message digest value.

- **Secure Hash Algorithm:** It is a cryptographic hash function published by the National Institute of Standards and Technology(NIST) as a U.S. Federal Information Processing Standard which takes an input and produces a 160-bit hash value known as a message digest – typically rendered as a hexadecimal number which is 40 digits long. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. There are a series of algorithms exist such as SHA-1, SHA-2, SHA-3.

Apart from this, there areotherwell-known HASH Functions exist which are used such as RIPEMD, WhirlPool.

Check Your Progress 2

---

1. List out atleast 3 differnet HASH Algorithms

   _____

2. What do call the output generated for the HASH algorithms

   _____

3. Describe atleast two uses of the HASH Algorithms

   _____

1.5.5 DIGITAL CERTIFICATE

There are several issues which exist with the public key cryptosystems; one of them is the man-in-the-middle attack in which is one of the potential threat. In this attack someone tries to fake the key with user ID and name, and tried to pretend the same person, which is not and resulting in this, the data is encrypted with the attackers key.

It is vital to know that the public key to which you are encrypting the data is the actual key of the intended recipient and not a forged one.

To overcome this, Digital Certificates has been introduced, which will ensure that whether a public key truly belongs to the actual owner or not. It acts much like a physical certificate.

Digital certificates consist of three things:

- A Publick Key.
- Certificate Information(Identity information about the user).
- One or more digital signature.

1.5.6PUBLIC KEY INFRASTRUCTURE

A Public Key Infrastructure(PKI) is a combination of policies, role, and procedures, which are needed to create, manage, distribute, use, store, and revoke digital certificates and manage, public-key encryption. It includes components such as Certificate Authority(CA) and the Registration Authority(RA).

Certificate Authority creates a certificate and digitally signs them using its own private key. As it is the central component of the PKI system. Using the public key of the CA one can verify the authenticity of the digital certificate and can check the integrity of the content of the certificate.

Registration Authority refers to the people which can include group, company, process, and tools which will help users to enroll them with the PKI system. It also checks the public key belongs to its owner or not. On the other hand, CA is the software which issues the actual certificates.

1.7LET US SUM UP

This chapter has provided details regarding basic cybersecurity details and current cybersecurity posture of the Nation. Moving forward we have also seen the basic security fundamentals and building blocks of the cybersecurity which are confidentiality, integrity, and availability and why are they important. Also how that

can be achieved using the different encryption models and its understanding using pictorial representation.

1.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check your progress 1

1. Components of CIA TRIAD Confidentiality, Integrity and Availability
2. Two Factor Authentication
3. Availability

Check your progress 2

1. HASH Algorithmsare MD5, SHA-1, RIPEMD
2. Message Digest OR Hash Value
3. Uses of the HASH Algorithms Data Integrity, Indexing Data in Hash Table

Unit 2: Attack Vectors, Threat, Risk And Vulnerability

2

Unit Structure

2.1. Learning Objectives

2.2. Introduction

2.3. Key Terminologies

2.4. Attack

2.5. Risk Assessment

2.6. Let Us Sum Up

2.7. Check your Progress: Possible Answers

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand various terminology related to security
- Understand of relationship between different terminologies
- Understand how risk management is done to handle the potential risk associated with the threats

2.1 INTRODUCTION

This chapter we will introduce some of the key terms which will be usedthroughout the book and also will be used in different topics for the rest of the chapters. Also, we will see what kind of relationship is there between different terminologies. Different attack vectors, threats, associated risks, vulnerability, and consequences.

Also, we will see how risk management is done to handle the potential risk associated with the threats.

2.3KEY TERMINOLOGIES

Attack OR Attack Vector

An attack vector is defined as the technique by which unauthorized access is gained inside the computer or network for a criminal purpose by exploiting the vulnerabilities in the system.

Risk

It can be defined as the probability of the loss from any particular threat from the threat landscape, which can exploit the system and gain the benefits from it such as loss of private and confidential information such as username and password, sensitive organization data, also the loss of the reputation which has occurred can be considered. Also, the loss occurred in terms of damage or destruction of hardware and software assets can be considered as Risk.

Threat

Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Vulnerability

Weaknesses or gaps in a systems security program, design policies and implementation that can be exploited by different threats to gain unauthorized access of a computer system or network.

Asset

People, property, and information. People may include employees and customers. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, or by minimizing the harm it can cause, or by discovering and reporting it so that corrective and proactive action can be taken.

Here in the below image, we will the relationship between all the different terminologies we have seen.

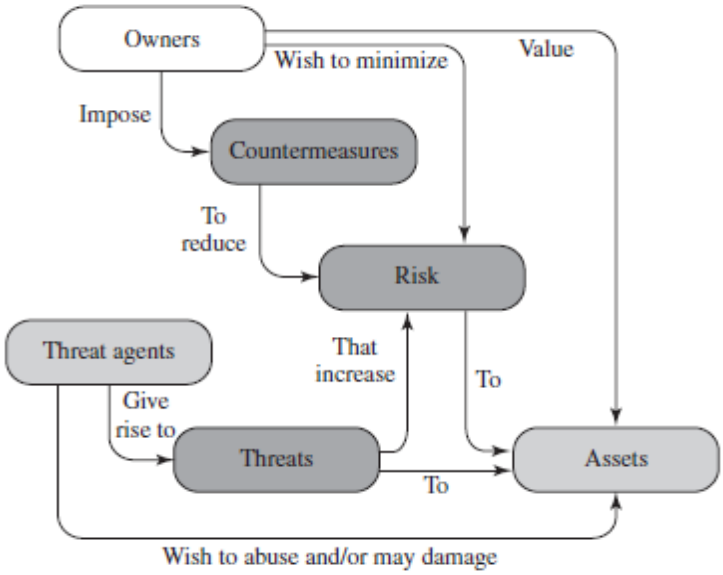


Figure 2.1 Security Concepts and Relationships

Let us start looking at each concept in details. But before that let us look key terminologies into the equation form which is given below and we will look at them in detail.

2.4ATTACK

We have already seen the definition of the attack on the previous page, we will look here the subtypes of attack and they are Active Attacks and Passive Attacks.

- **Active Attacks:** In an active attack, the attacker intercepts the connection and then modifies information.

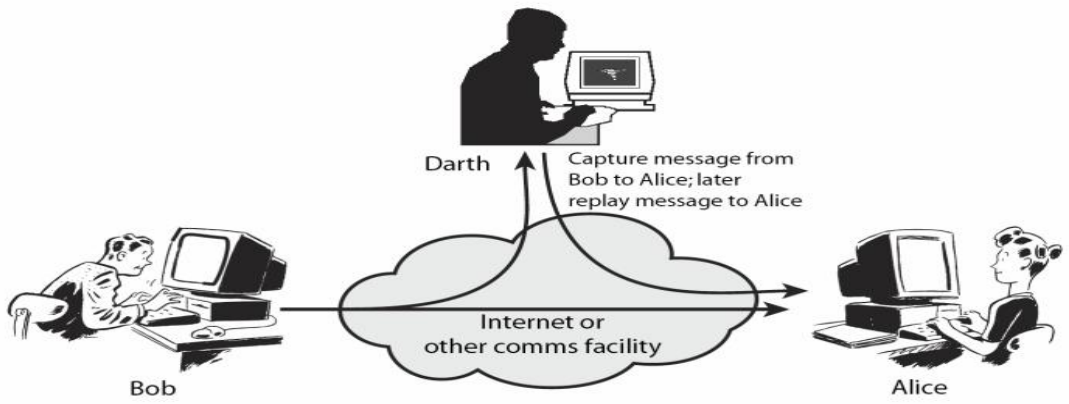


Figure 2.2 Active Attack Source:techdifferences.net

An active attack can be divided further into Masquerade, Replay attack, Modification of messages.

- **Passive Attack:** In a passive attack, the attacker intercepts the information but with the intent of reading the information and not modifying it. It can further be divided as Traffic Analysis and Release of Message content.

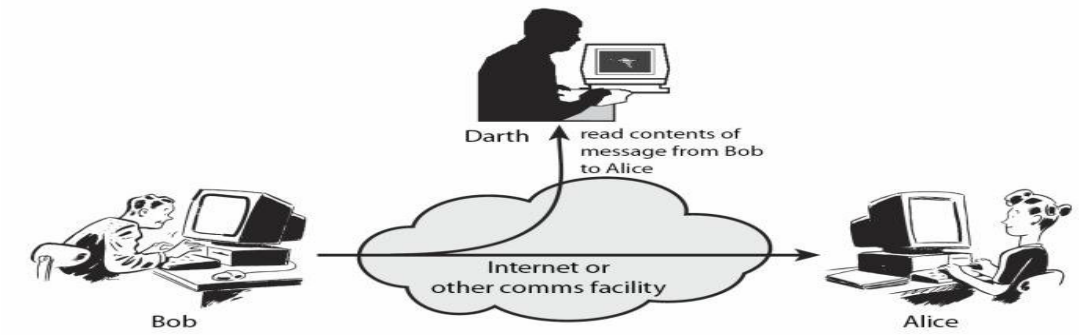


Figure 2.3 Passive Attack

We can also classify the attack based on its origin.

- **Inside Attack:** If the origin of the threat agent is from the inside the organization, which may have the authorization and access granted to the resources, but uses it with the criminal intent.
- **Outside Attack:** Origin or source of the attack is from the outside of the organization and gains the unauthorized access to the system or resources with the criminal intent.

A Cyberattack can destroy the business overnight, a proper security defense is required to stop such attacks. The main focus is to compromise the systems and gain access to sensitive data. Let us see the top cybersecurity attack and what do they do.

- **Phishing Attack:** It is a type of security attack that tricks the user to divulge the sensitive and personal/confidential information which is sometimes referred to as “Phishing Scam” also. Definitely, every user will not click the links provided in the email id for providing the details, but the attackers are smart they will perform the social engineering and will send the emails to the users with the similar content which user is already looking or interested in it.

  The most targeted business sectors are Payment Platforms, Financial and Banking organizations, Webmail services and Cloud storage/hosting providers.

  Phishing attacks engage users with a specific message and very solicit way for the response from the user which is ideally to click on the link is known as “Call To Action”. Which means the attacker wants the user action on the link provided in the email to perform the action.

  - **Spearphishing:** When a phishing attack is targeted to the specific individuals of the organization, it is known as spearphishing. Attackers use the solicit company logo, footer and all other style information which is present in the legit email to trick the user. The content of the email mainly focuses on the password reset email or, account reset activity.

For the prevention of the phishing, the user has to check clearly the from address and email content, along with the links present in the email body. Apart from this,

employees awareness using various teaching method is the most important as major data breach occurs due to human error which cannot be ignored.

- **SQL Injection Attack:** SQL which is pronounced as “squeal” stands for the structured query language. it’s a programming language used to communicate with databases. It is used to store critical data of websites/users/services in their databases which can contain personal and sensitive information such as username and password, transaction details.

  SQL Injection attack targets the database using specifically crafted SQL statements to trick the system into unexpected and undesired outputs.

  SQL Injection attack can be carried out in different ways which can be decided after the attacker identifies system behavior.

  If the web application is building a SQL query string dynamically with the account number the user will provide, it might look something like this:

  “SELECT * FROM customers WHERE account = ‘“ +
  userProvidedAccountNumber +”’;”

  While this works for users who are properly entering their account number, it leaves the door open for attackers. For example, if someone decided to provide an account number of “‘ or ‘1’ = ‘1”, that would result in a query string of:

  “SELECT * FROM customers WHERE account = ‘’ or ‘1’ = ‘1’;”

  Due to the ‘1’ = ‘1’ always evaluates to TRUE, sending this statement to the database will result in the data for all customers being returned instead of just a single customer.

  The above query might not work for all the database, but it can work where there are less or no security measures taken to filter such SQL injection queries.

Other types of SQL injection attacks include Blind SQL Injection, Out of Bound SQL Injection. SQL Injection attack can be prevented by avoiding the use of dynamic SQL, sanitize user inputs, don’t store data in plaintext, provide access control and privileges also use of web application firewall is a must.

- **Denial-of-service(DOS) and Distributed Denial of Service(DDOS):** Denial-of-Service attack focus on disrupting or preventing legitimate users from accessing

the websites or application or any other resources by sending flood of messages, packets, & connection requests, causing the target to slow down or “crash”, rendering it unavailable to its users. Attacker mostly targets high-end value organizations such as media houses, banking, and financial organization, E-Commerce to disrupt their services.

When the majority of present-day DoS attacks involve a number of systems (even into the hundreds of thousands) under the attacker’s control which are installed with the bots, all simultaneously attacking the target. This coordination of attacking systems is referred to as a “**Distributed Denial-of-Service**” **(DDoS).**

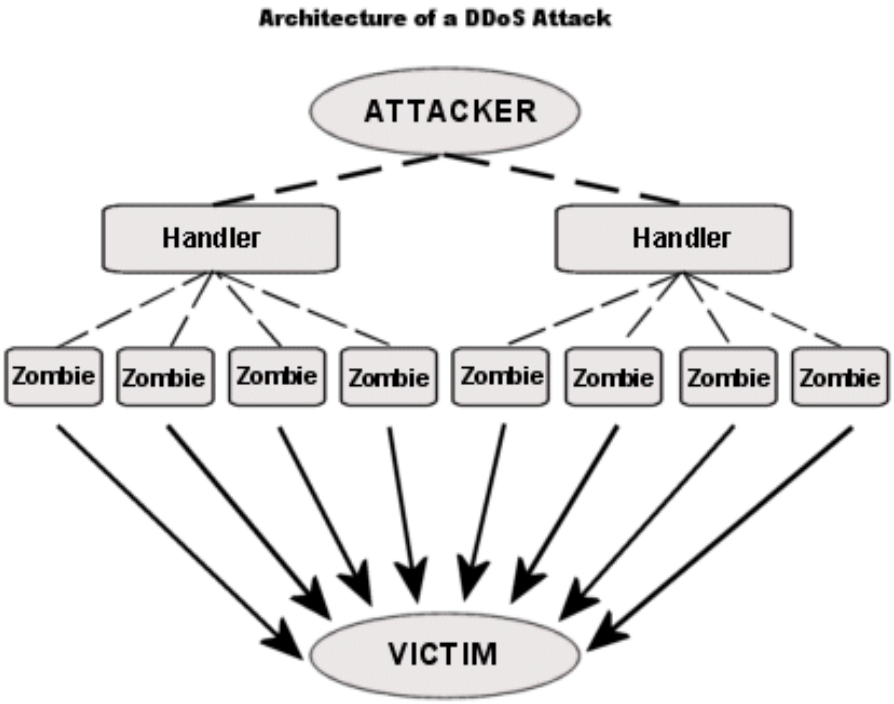


Figure 2.4 DDOS Architecture Source:Wikimedia.com

- **Man-In-The-Middle Attack and Session Hijacking:** Man-in-the-middle attacks are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen.

  When a user is using the internet and our computer performs a lot back and forth transaction, the application generates and uses a session ID which will be unique and to make the transactions private between user and application. The attacker

hijacks the session ID to eavesdrop the communication between user and application.

There are various types of Man-In-The-Middle Attack such as Rogue access points, ARP Spoofing, DNS Spoofing, Packet Injection, SSL Striping.

We can prevent such attacks by using strong WEP/WAP encryption on access points, using a virtual private network(VPN), enforce https and using a strong combination of the public key pair authentication.

- **BruteForce Attack(Password Attack):** The theory behind such an attack is that if you take an infinite number of attempts to guess a password, you are bound to be right eventually. The term brute-force means overpowering the system through repetition. A brute force attack is among the simplest and least sophisticated hacking method. Brute Force attacks often use automated systems or tools to perform the attack in which different password combinations are used to try to gain entry to a network, such as a dictionary attack list or using rainbow tables.

  The attacker aims to forcefully gain access to a user account by attempting to guess the username/email and password. Usually, the motive behind it is to use the breached account to execute a large-scale attack, steal sensitive data, shut down the system, or a combination of the three.

  We can prevent it by using a strong password combination policy and require to change a password on regular intervals, locking out accounts on a certain number of incorrect password attempts, use captcha, two-factor authentication, monitoring server logs, limit logins from the single IP/Range.

- **Malware Attack:** Malware can be described as Malicious software that is installed in your system without your consent. It can attach itself to the legitimate process or replicate itself or can put itself to startup. The objective of the malware could be to exfiltrate information, disrupt business operations, demand payment, There are many types of malware below are some of the commonly known types:
  - **Macro Virus:** These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes

instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.

- **Trojans:** A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers
- **Logic bombs:** A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
- **Worms:** Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm can result in denial-of-service attacks against nodes on the network.
- **Dropper:** A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.
- **Ransomware:** Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion and asks for the payment in bitcoin. Which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key or using the decryptor if it is available.
- **Adware:** Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up

windows or through a bar that appears on the computer screen automatically.

- **Spyware:** Spyware is a type of program that is installed to collect information about users, their computers or their browsing history. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.
- **Zero-Day Exploit:** A zero-day exploit hits after a vulnerability has been announced, but before a patch or solution is implemented. Attacker targets the disclosed vulnerability during this window of time.

To prevent such attack we need to ensure that the anti-virus product is up-to-date with the latest signatures, continues user education, performing regular audits, regular backup of the websites, application, and databases at multiple locations.Now we will start with understanding the complete Risk Rating Methodology. It will also include different steps such as Risk Analysis, Risk Assessment, and Risk Management.

Check Your Progress 1

1. What kind of malware encrypts the file and ask for ransom to decrypt the file

   _____

2. Mention any two types of SQL injection attacks

   _____

3. Which type of malicious software captures the user data and history

   _____

2.5RISK ASSESSMENT

Identifying threats and vulnerabilities is very important to build a robust security architecture. It always starts with identifying what are the important assets which need to be secured from threats. So the first and foremost task is to define the scope

of the cybersecurity Risk Assessment. Being able to estimate the associated risk to the business is very important.

$$\text{Risk} = \frac{\text{Assets} * \text{Threats} * \text{Vulnerabilities}}{\text{Countermeasures (controls)}}$$

- Assets – what we are trying to protect
- Threats – what we are trying to protect against
- Vulnerability – what we are trying to address
- Controls – what we are doing to address them

Figure 2.5 Risk Equation

- **Assets:** We have seen the definition of the Assets in the first section under key terminologies. Now we will understand the assets in relation to threat actions and will map with the CIA triad.

  Assets can be categorized in various types such as hardware, software, Data, and communication channel(different devices including communication cables). In details if we go it can be described as follow:

  Physical assets such as Computer, Laptop, Networking Devices, Storage Devices, etc..Software such as Operating system, Application Running on the system, services running, port scanning, API services, protocols used, and policies.

  All this can be considered as an important asset and are part of the scope of the Risk Assessment. One may identify security concerns in architecture or design. By using this process it is possible to estimate the severity of all of these risks to the business and make an informed decision about what to do about those risks. Having a system in place for rating risks will save time when there is a situation arise to take the critical business decision to reduce the impact.

  - **Asset Value Assessment:** This would be the first involved in measuring the asset value which is part of the critical business process. An asset can be the people, process, hardware, software, data, any tangible or intangible(can include the reputation of the

organization, loss of customer and services) things which are part of the critical business process.

In order to achieve greater control in risk and with effective least cost, identifying and prioritizing the assets are a critical part of the process from top priority to least priority.

This can be achieved by identifying the core functions and the process of the organization. Along with this identifying the physical infrastructure, assets which can be critical hardware or software related to the business functions and safety measures which are preinstalled for the emergency situations need to be also considered.

- **Threats actions and its Consequences:** As per the RFC 2828 we will see some terminologies related to the threat, we have already seen the definition of the threat in the first section of key terminologies.

  After identifying the asset value assessment and quantifying it, next step is to conduct the Threat assessment where the potential threats are identified.

  There is another relative term “Hazard” is also used for the threats which are natural or not man-made, such as earthquake, flood or wind disaster which also needs to be considered and the man-made hazard can be either technological threats or terrorism which we can refer as “Threats” for simplicity.

  - **Threat Action:** It is an assault on system security.
  - **Threat Analysis:** An analysis of the probability of occurrences and consequences of damaging actions to a system.
  - **Threat Consequence:** A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation.

Threat Action (attack)	**Threat Consequence**
Exposure: Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive	**Unauthorized Disclosure:** A circumstance or event whereby an entity gains access to data for which the entity is not authorized.

data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.	
Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.	**Deception:** A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
Incapacitation: Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.	**Disruption:** A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Misappropriation: An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.	**Usurpation:** A circumstance or event that results in control of system services or functions by an unauthorized entity.

Table 2.1 Threat Action and Consequences Source: RFC 2828

Check Your Progress 2

1. What kind of threat action can cause the unauthorized disclosure of data _____
2. What kind of event authorized user can receive false data _____
3. What do we call if due to undesirable action data is altered _____

- **Threat Analysis:** Our next goal here is to estimate the likelihood of a successful attack by this group of threat agents for this we will use the OWASP risk rating methodology for preparing severity of the Risk Assessment Model.

  Skill level: How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9),

  Motive: How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

  Opportunity: What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

Size: How large is this group of threat agents? Developers (2), system admins (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

The use of a rating system will help in the quantification of risk. There is always difficulty in justifying the protection of assets. Management is better able to understand the implications of the threat and vulnerabilities when they are presented in the form of numbers and statistics which means quantifiable and measurable.

- **Vulnerability Analysis:**A vulnerability is a weakness that a threat can exploit to breach security and harm your organization. Vulnerabilities can be identified through vulnerability analysis, audit reports, the NIST vulnerability database, vendor data. The problem faced within many organizations is the ability to effectively filter out the false positives from assessment applications.

  The result of the various manual and automated tools must be verified in order to accurately determine the reliability of the tools in use and to avoid protecting an area that in reality does not exist. False positive results can be mitigated by ensuring that the assessment applications are up to date with the latest stable signatures and patches.

  There are two ways penetration testing and vulnerability analysis can be done, one with having the knowledge of the systems and topology, another with zero knowledge which is mostly conducted externally known as black box testing.

  Examples of vulnerabilities:

  - Lack of sufficient logging mechanism
  - Input validation vulnerability
  - Sensitive data protection vulnerability
  - Session management vulnerability
  - Cryptographic vulnerability
  - Memory leak Issue
  - Cross-site request forgery
  - Remote Code Execution
  - Business logic vulnerability

  For more similar issues refer to OWASP Top Ten Project

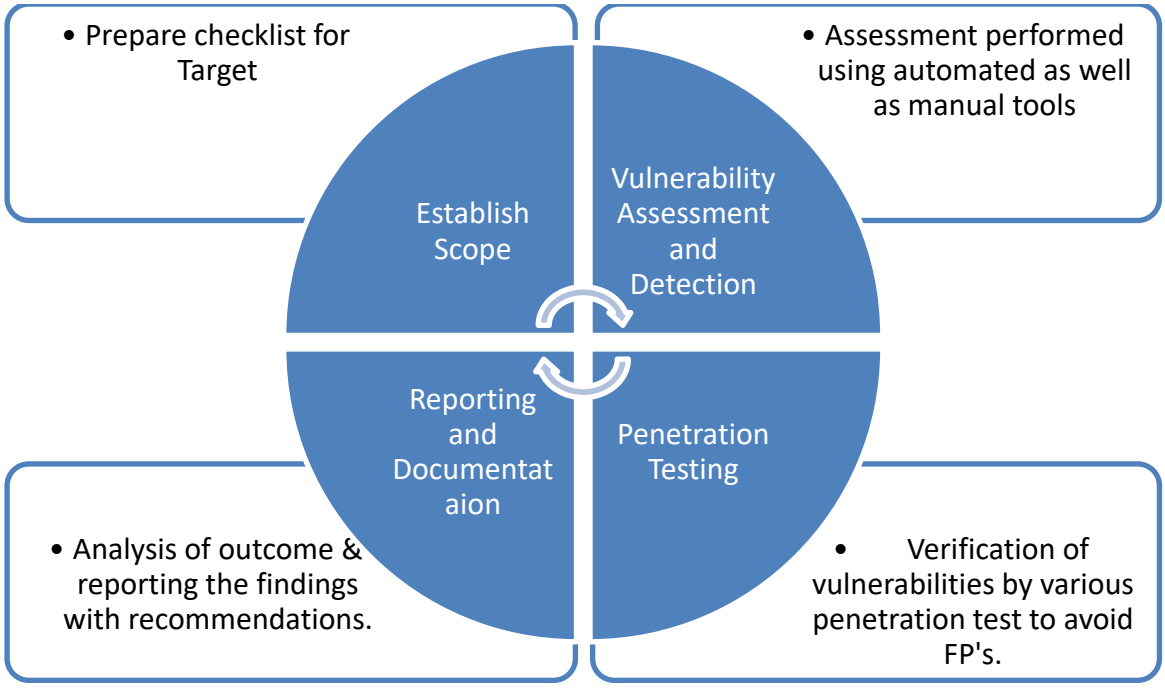


Figure 2.6 VAPT Process

- **Vulnerability Factors:** The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

  Ease of discovery: How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

  Ease of exploit: How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

  Awareness: How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

  Intrusion detection: How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

- **Estimating Impact:** When estimating the impact of the successful attack, it is important to consider the technical impact and business impact.

Ultimately the business impact would be more important. So by providing the appropriate technical risk details which will enable management to make the decision about the business risk.

- **Technical Impact Factors:** The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

  Loss of confidentiality: How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

  Loss of integrity: How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

  Loss of availability: How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)

  Loss of accountability: Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

- **Business Impact Factors:** Business impact requires a deep understanding of the different operations on which the company is working and gets maximum return on investment.

There are many factors and also may not be the same for all organization, but we will see some of the common impact factors.

- **Financial damage:** How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- **Reputation damage:** Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)

- **Non-compliance:** How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
- **Privacy violation:** How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

➢ **The severity of RISK:** We will now prepare the severity of the risk which can be obtained by combining the different impact factors.

It is divided into three parts from a 0-9 scale, low medium or high as shown below.

Impact Scale	Impact Levels
0-<3	LOW
3-<6	MEDIUM
6-9	HIGH

Table 2.2 Severity Matrix

➢ **Countermeasures(Control):** In this step, we have to identify the existing security policies and protocols which are placed. Are they are adequate with the current threat landscape? Or it needs to modify and update the security posture of the organization. What level of risk is acceptable to the organization. This will help the security team and top management to understand the risk levels and they can focus on more high-level risks.

➢ **Documentation:** This is the final step in which risk assessment report is prepared to support the management to take appropriate decision on policies, procedures, budget allocation. For each threat, the report should have corresponding vulnerabilities, assets at risk, impact, and control remediation.

2.6LET US SUM UP

In this chapter, we have seen what all different types of attacks and what it can cause. Next is we have seen threats and consequences. Which is followed by Risk Assessment procedure which includes threat assessment, vulnerability assessment

and how to prepare the severity matrix to report the threat to management. Also based on the identified risk in the report we have to recommend the security policy and procedure to rebuild the security posture of the organization from the current threats and attacks.

2.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. Ransomware
2. Blind SQL Injection & Out of bound SQL Injection
3. Spyware

Check Your Progress 2

1. Exposer
2. Deception
3. Corruption

Unit 3: Advance Persistent Threat And Cyber Kill Chain

3

Unit Structure

3.1. Learning Objectives

3.2. Understanding the Problem

3.3. Advance Persistent Threat

3.4. Cyber Kill Chain

3.5. Let US Sum Up

3.6. Check your Progress: Possible Answers

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand how the Advanced Persistent Threat(APT) can be handled in a way that traditional threats are handled.
- Understand cyber kill chain

3.2 UNDERSTANDING THE PROBLEM

In today's world organizations are facing critical issues from different types of advanced threats including to the traditional ones. However, they are still finding issues that how the Advanced Persistent Threat which is known as APT can be handled in a way those traditional threats are handled. Well, APT is much complex in nature that they cannot be handled with any single approach. It is not possible to secure any organization to handle entire security and APT in a single way.

Organizations are dealing with the APT's they are completely different in nature until the organization understands where the real issue lies and how to solve them.

To understand how to handle Advanced Persistent Threats first executives of the organization has to understand the motive behind the attack. As still management of many organizations still thinks that they have paid or invested enough to handle every kind of cyber attack. Because spending the money will not solve the issue of complete security from Advanced Threats.

In the current situations or in simple terms the traditional method which is followed is to install basic security mechanisms. Then they get compromised, they will get notifications from the law enforcement and then they start the forensic investigation.

APT's are well funded, organized group of hackers who in a systematical manner to compromise the target which is mostly government organization's, private company's. They are mainly focused on gathering critical data by exploiting the vulnerability in a stealthy manner. They are very smart in hiding their tracks. They bypass highly secure infrastructure to establish the foot-hold in the target organization and to remain there until and unless the motive is not completed.

If we look deep into the APT, attacker needs one vulnerability to compromise the security and make way to get into the organization. But for the organization, they need to find out all vulnerability and to patch them. Many organization does not still understand that what are all the point of entry points or attack vectors from where the attacker can exploit it and make their way inside. The success ratio of APT is good, as they keep on trying until they find a way to exploit the system of the target.

For APT we have to learn them first before we try to stop them. Instead of looking in the future we can start learning the APT now and we can try to build the defense based on the learning from the past attacks. Though we cannot be sure that there will be no new approach.

But there are chances that same cybercriminal groups tend to use similar tactics and techniques on similar organizations. The key objective should assume the worst attack ever and hope for the best. It will help to understand the security level of your organization and will learn something new, while indirectly help to improve the security posture of the organization. Instead of assuming the best security measures are applied and doing nothing.

The final goal should be, an organization should not lose the business due to the lack of cybersecurity measures and practice. Most of the organization so spend large amount behind the cybersecurity and defend them. But the fundamental point is to understand is to identify the priority and risk and returns from the investment. The reason behind failure to defend from APT is to identify what resources which are at high risk needs more protection. There are multiple protection mechanisms which are already in place where the APT attack has been seen such as:

- Firewall
- Application Filtering
- End-Point Detection
- Anti-Virus Solutions
- Intrusion Detection

Investing a large amount of money to defend an organization from APT doesn't guarantee the protection from the APT. But the organization should focus on high-risk vulnerabilities and resources which can cause a big impact. It is better to fix 2

high-risk vulnerabilities which can cause a big impact instead of fixing low risk 20 vulnerabilities which cause not threats.

Let us now start to learn more about the APT, what does it mean and how it works.

3.3ADVANCE PERSISTENT THREAT

The term APT sounds very simple but is often taken as for granted or been misunderstood. The term **Advance** is related to the systematically crafting an attack vector in terms of its advanced and very targeted code used which is very effective.

The way attacker crafts the attack is very advanced while the methods to deliver the same are very standard methods and most important that it will work. Most of the APT will take advantage of the available advanced technology and techniques to customize the attack.

In every APT there will be a single method which will be used to bypass the security devices, which is known as Encryption. It was created to stop attackers from accessing critical information. Most security devices are unable to read the encrypted code of payload or encrypted packets in the network. The attacker sets up the encrypted outbound tunnel to attacker system. So data is encrypted and it goes undetected on the network.

The next is **persistent**. The attacker will not stop after failing once or twice. They will keep trying until they are successful in their objective. There need to be continuous defensive measured should be established.

The persistent nature of an APT is what it causes more damage to the organization. It simply means to remain stealthy for a prolonged period of time and not get caught due to its state of the art coding techniques.

They get into the system, remain there until the data is completely exfiltrated, and they leave without getting on the surface and they do not leave any trace. So it becomes very hard for an organization during the post-investigation when any third party services such as law enforcement agency inform them regarding the APT attack on your organization. It would be very difficult for an organization, as they don’t know where to start an investigation and how to decide a timeline for that.

As mainly APT attacks are not for a few days, an attacker could have a foothold in systems from many days, weeks, months or sometimes it may be years. The persistent process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "**Threat**" process indicates human involvement in orchestrating the attack.

For an APT to work successfully, it' important to hide the identity of the attackers, as APT attribution could lead to some real-world conflicts. So the attackers will want to hide their tracks. It is not uncommon to see the use of unpatched vulnerabilities (zero-days) in this kind of operations.

Figure 3.1 Avance Persistent Threat

APT will gather as much as information as possible so it will help the attacker to customize the attack to become successful.

- **APT Intentions:** For a defender, it is very important to find out the intentions behind the APT attack. That would be useful in investigating the post-incident analysis. We will look into some of the intentions of the attacker which were concluded based on the previous APT attacks.

  Data: For any organization, it is important to understand the market strategy, other competitive organization working in the similar product market.

The intentions behind such type of attack in which an attacker tries to exfiltrate data such as proprietary designs, schematics, formulas, experiment details, source code.

Information: It is very important for any organization to keep internal information in a very closed loop. Such as its financial status, future Corporate directions, its mergers, and acquisitions. This type of information is very useful to target the organization.

- **APT Threat Vectors:**

External:

Internet:

- Email Attachments
- File Sharing
- Pirated Softwares
- Mass vulnerability Exploits

Physical:

- Infection using external devices(USB, CD, External Disk Drives)
- Malicious IT Equipment
- Rogue Wifi Access points
- Stolen Mobile devices / Laptops

Internal:

Trusted Insider:

- Rogue Employee
- Third Party Contractors & Vendors

Trusted Channel:

- Stolen Credentials
- P2P tapping
- Un-Trusted devices
- Hijacked Cell communications

There are other threat vectors which are also present which are related to Softwares used inside the organizations.

Insecure Build:

- Insecure Devices.
- Unpatched software versions.
- Misconfigured Device.

Information Leakage:

- Exposure of sensitive material on online/social media.

Application Security:

- Fuzzing / Reverse Engineering.
- Buffer Overflows.

➢ **APT- Tools:**

- Open Source exploit Softwares
- Malware: Botnets, Rootkits, Ransomware, Malicious Attachments
- Open source Available Exploit Code
- Using Zero Days.

➢ **APT- Techniques:**

- Open Source Intelligence (OSINT)
- Social Engineering / Using SET (Social Engineering Toolkit)
    - Leverage Social media information.
    - Identify contextual and behavioral information.
- Targeted Spear Phishing Attack
    - Requires in-depth knowledge of internal communication method.
    - Requires to build a strategy which lures the target and perform a predetermined action which.
- Malicious Attachments
    - File format such as PDF, Office (Word/Excel/Access) is used mostly in APTs.

- Usage of exploit kits to generate the documents which contain malicious macros and craft the malicious attachments to send it the target using a properly crafted email. Such as Fallout, Angler, RIG, Nuclear, Neutrino are well-known examples of exploit kits.
- Exploits are easy to use, can be easily obtained from the dark web.
- Provides command and control infrastructure services.

- Hardware Devices
  - Hardware exploits in the internal devices used.
  - Projectors, Printers, Shared file servers, which are now usually connected with the internet, they are left open which out any security measures. An attacker tries to use such resources gain access to the internal network.

In the below image, we can clearly see and understand how the different attack vectors take part in making a successful APT attack.

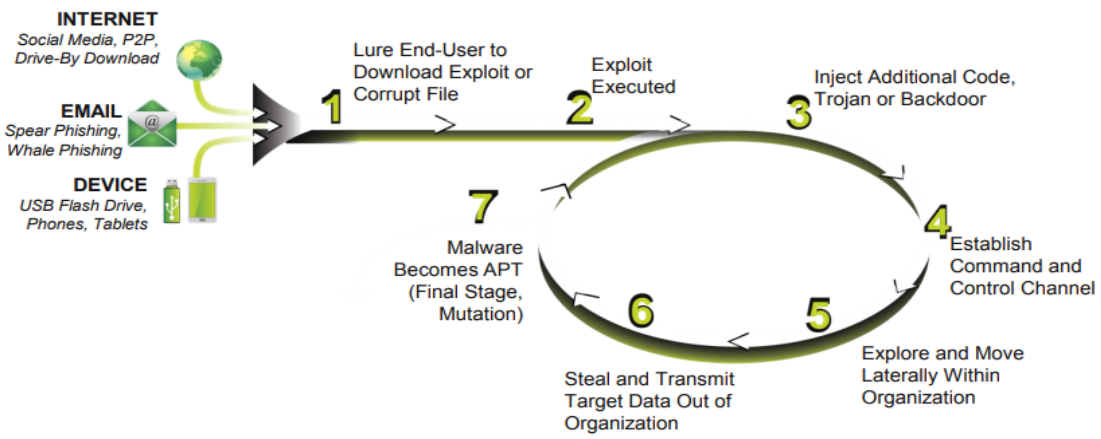


Figure 3.2 Attack Vector Cycle Source: Attack Vector chain by Brian Wrozek, Optive.com

➢ **Defending Against APT:**

We will see some of the high-level strategies that an organization must use to defend against the APT. It is always important that prevention is good but detection is a must. Mostly, the organization builds and invest in preventive measures.

But they forget that such type of APT attacks mostly comes with the legitimate traffic inside the organization and which is very difficult to identify by the installed

security measures. There are few things which an organization must do to prevent against such threats.

Raise Awareness and Control Users: Humans which are considered the end user and are targeted mostly to perform malicious actions, though they are not known what will be the consequences when clicks on such unknown links in the email. So it is better to conduct the internal phishing test and user awareness by giving basic ideas regarding phishing and how to identify them.

Reputation Scoring and Malicious Traffic Identification: Traditional security measures work on to block or access network traffic. While in APT mostly in pretends to the legitimate traffic. Once they enter into the network, they become bad or evil. So it is better to monitor the network traffic and scoring them based on their behavior in the network. That will help to identify if any malicious packets try to change its behavior from good to bad.

Monitor Outbound Traffic: Security Measures are generally built around the inbound traffic and monitor it to stop the threats from spreading. While in APTs, it is also important to monitor outbound traffic as their motive is to exfiltrate the internal data which will harm the organization. So it important to detect the anomaly in the outbound traffic also.

Understand the changing Threat Landscape: It is difficult when we don't know from what we have to defend to save ourselves. Something which is unknown or unseen. The only way to defend is to understand and learn how the offensive part works and operates. If the organization will not learn the new attack techniques and tactics they will lose the battle and not be able to tune their defensive measures.

Manage Endpoint: The ultimate goal of the attacker is to steal information which is stored on the endpoint. So even if the attacker has access inside the network, they still need to access the endpoint to get the information.

So to limit the damage, controlling the endpoint and locking down endpoint by disconnecting it from other networks and isolating it will protect the information from getting outside of the organization.

Now we will learn the complete and in-depth process and stages which the attacker performed to conduct such an APT attack. It is very important to learn each kill stage components in detail. This complete cycle is known as the Cyber Kill Chain.

It can simply be understood as a chain of multiple stages which are related to each other. The output of each stage can be considered as input for the next stage. We will see the offensive steps which are part of the cyber kill chain as well as from the defensive side, how to stop such attack.

3.4CYBER KILL CHAIN

The term kill chain was first used in the military which is related to the structuring of an attack, which includes identification of the target, getting a foothold in the organization, attack timing, and decision, destruction of the target. Though this process is not universal but is accepted by the information security community and converted into the part of the cyber kill chain to better understand it which can be useful to break the kill chain in different stages. As per the Wikipedia Traditional Military Kill Chain includes multiple stages which are listed below:

F2T2EA:

- ***Find:*** Locate the target.
- ***Fix:*** Fix their location, make it difficult for them to move.
- ***Track:*** Monitor their movement.
- ***Target:*** Select an appropriate weapon or asset to use on the target to create desired effects.
- ***Engage:*** Apply the weapon to the target.
- ***Assess:*** Evaluate the effects of the attack, including any intelligence gathered at the location.

Now we will look at the different phases of cyber kill chain part of which mention below, is majorly derived from the Lockheed Martin which was first published by them in 2011. Since then it has been adopted by many organizations. Cyber kill chain reveals different phases of a cyber attack, from the initial stage of reconnaissance to the last stage of data exfiltration.

This has been also used as a tool for the management to understand the phases of cyber attack to continuously improve their defensive measures. According to Lockheed Martin, these phases threats must pass through the model which is shown below.

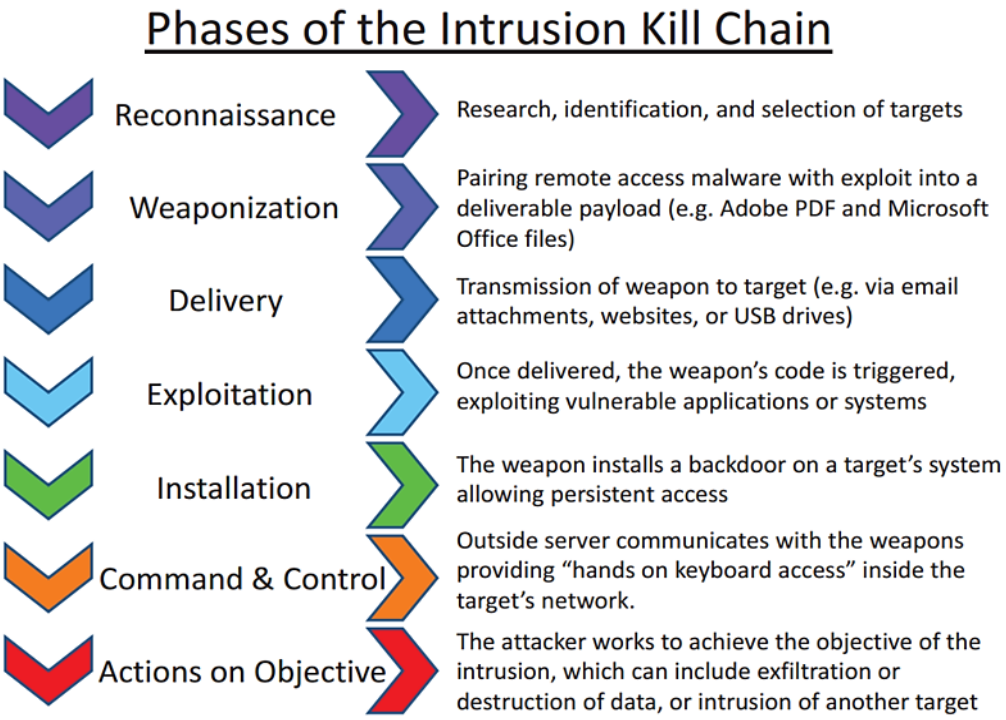


Figure 3.3 Cyber Kill Chain Source: Wikimedia.com

Check Your Progress 1

1. List out any three APT threat vectors.
2. List of any 3 exploit kit names.
3. What are software related APT threat vectors.

Let us understand all 7 technical phases in detail.

Reconnaissance: Reconnaissance means to gather information regarding the target. It can an individual or an organization. It further drills down to the identification and profiling of target. Further to extract all kinds of information from the internet such as email address, social media relationship data, blogs, sites, conferences. Information gathers from this stage will be later used in the design and delivery of payload. Reconnaissance is divided into two parts:

Active Reconnaissance: This step is to gather information regarding a target without his/her knowledge. Such as using open source intelligence tools(OSINT) for information gathering.

Passive Reconnaissance: It involved deep profiling of the target which might trigger alert to the target. Such as using network scanning tools like Nmap, Nessus,

Weaponization: In these phases, the attacker uses the details gathered from the above stage to create malicious payload such as RAT(Remote Access Trojans). Also how to deliver it to the target. The attacker leverages the usage of open source offensive framework tools such as the Metasploit, Msfvenom, Veil and to write reverse shells. Then it is injected into the legitimate software or binaries and is finally obfuscated in order to prevent from detection.

Exploit: Exploit is a part of the weapon which facilitates RAT to execute in the target machine. It uses system or software vulnerabilities to drop and execute a RAT. The major objective to use exploits is to evade the detection. Exploits can be related to MS Office (doc/ppt/excel) which can be identified from its CVE(Common Vulnerabilities and Exposure) number. Such as CVE-2017-11882, CVE-2014-9165 and so on.

There are methods which do exist in which the target system can be accessed without using exploit they are very unreliable in these times as the organization has already set up multiple security layers. Embedding RAT or an exploit code inside the legitimate file will be easier to evade the detection. In some cases, multiple exploits are used to create a payload using the exploit kits. Which provides the exploit code for different software.

Operating system level exploits use kernel level exploits or exploits the device driver itself to perform remote or local code execution. Network level exploits try to exploit network devices or protocols to perform privilege escalation.

Delivery: It is a critical part of the cyber kill chain which is responsible for an efficient and effective cyber attack. In most of the cyber attack, it is mandatory to have some user interactions such as using email attachments, drive-by downloads, USB, browser-based attack.

Check Your Progress 2

1. List out any 2 methods used for reconnaissance.
2. List of any 2 offensive framework used to prepare payload.
3. List of network scanning tools for passive reconnaissance.
4. List of any 2 Network level exploits.

For which the initial target information is necessary for deciding which method will be useful, this can be varied according to the target. There are some attacks which are performed without user interaction by exploiting network devices or services such as CVE-2014-3306, CVE-2014-9583.

Delivery is a very high-risk phase, it leaves the digital footprints behind. So most of the attacks are performed in an anonymous way using paid services. Successfully targeting the user in the first attempt cannot be guaranteed.

In such cases, the attacker will gain all information due to which the first attempt was failed and will make sure that in the second attempt it successfully exploits target machine. In some cases where one delivery method is not sufficient, multiple delivery methods are used.

Exploitation: Once the successful delivery of the weapon is done. The next step is to execute or trigger the exploit on the target side. The goal here is to silently install or execute the exploit. There are certain conditions need to be matched for this to work such as User must be using software or services for which the exploit is created.

Next operating system should not be updated with the latest patches which fail the exploit to work. And last Anti Virus software should not detect the payload.

Installation: Nowadays, traditional methods of the infection will not work in which the machine Is infected with the links created in the startup folder, or creating the registry of the file to run in a startup. As of end-user protection, mechanisms has grown.

Modern malware is multi-staged and they heavily depend on the droppers and downloaders to deliver the malware.

Command and Control: After successfully triggering the malware. The important part of the remote attack is command and controls (CnC/C&C). C&C gives the instruction to the compromised machine. There are mainly three different types of communication structures, such as centralized structure, peer-to-peer and latest social network based communication structure.

C&C communication traffic analysis is a traditional approach to detect the communication pattern in the target machines. Malware authors tend to use new techniques in which it is difficult to separate it from the legitimate traffic of the network to make it more anonymous.

Actions on Objective: In the last phase the attacker tries to achieve the final goal which is to exfiltrate the data from the compromised machine by giving instruction from the command and control server.

3.5 LET US SUM UP

In this chapter, we have seen the life cycle of the APT. We have seen the different threats and attack vectors which are part of the APT. Apart from this, we have seen tools and techniques which are used in the APT attack. Also, we have seen the different phases of the cyber kill chain along with the other technical details.

3.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. Email Attachments, File sharing, Pirated software
2. Fallout, Neutrino, Angler
3. Unpatched software, Misconfigured Devices, Fuzzing

Check Your Progress 2

1. Email address harvesting and social media related data
2. Msfvenom, Veil
3. Nmap, Nessus
4. Exploiting Network devices and Protocols

Unit 4: Cyber Security Framework

4

Unit Structure

4.1. Learning Objectives

4.2. Introduction

4.3. Cybersecurity Policy

4.4. Cybersecurity Regulations in INDIA

4.5. Cybersecurity Regulations In Other Countries

4.6. Cybersecurity Policy Framework

4.7. Let us sum up

4.8. Check your progress: Possible answers

4.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- learn different cybersecurity-related frameworks which are essential for an organization to follow to create robust security infrastructure and enforce the strong policy mechanism.
- Understand compliances and regulatory frameworkto protect assets and data.

4.2 INTRODUCTION

We have already learned the concept of the importance of cybersecurity and many other technical aspects related to it. But it is also important to establish for an organization to comply according to business functions with security standards and norms which exist.

As there is a rise in a number of cyber attacks increases day by day on the different organization it has now become essential to protect their assets and data. So there are multiple compliances and regulatory framework which organization has to follow.

4.3CYBERSECURITY POLICY

The role of policy is to construct the guidelines and principles for the management. It will help them to take future decisions and serve them as an implementation roadmap. The policy has a clear and defined measure that how the organization will protect their assets and information systems and will make ensure it complies with legal and regulatory requirements.

The goal here is to protect the organization, its vendors, customers, partners, from the resulting effect of the intentional or accidental damage. Also to protect the integrity of the data and availability of the systems for the continuity of the business.

Cybersecurity policy is not easy to understand. They become useless if the employee, customers or stakeholders are unable to understand and follow. So it is very important to have a good cybersecurity policy in place.

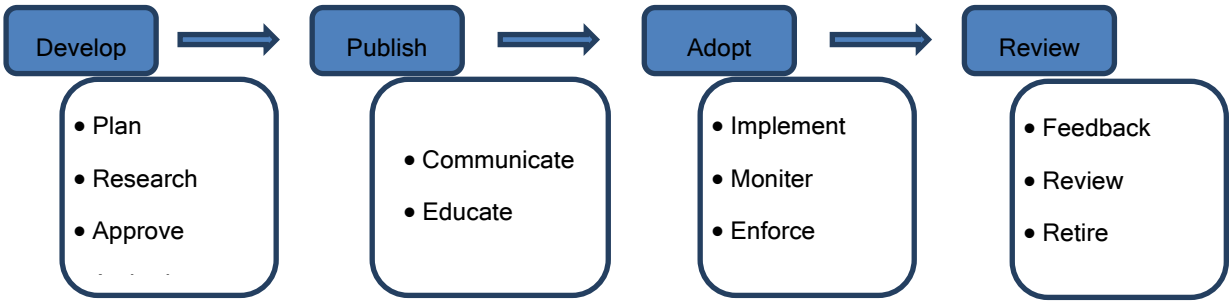


Figure 4.1 Cyber Security Policy Life Cycle

4.4 CYBER SECURITY REGULATIONS IN INDIA

Currently INDIA has the Information Act, 2000 and then it was revised in 2008 again. The Information Technology (Amendment) Bill, 2008 amended a number of sections that were related to digital data, electronic devices, and cybercrimes.

The Government approved a framework to enhance security in Indian cyberspace for cybersecurity with the National Security Council Secretariat functioning as the nodal agency.

The National Cyber Security Policy, 2013 was developed to build secure and resilient cyberspace for India's citizens and businesses.

The Ministry of Electronics and Information Technology said that the policy aims to protect information and the information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Additionally, the Indian Computer Emergency Response Team (CERT-In) is responsible for incident responses including analysis, forecasts, and alerts on cybersecurity issues and breaches.

As the INDIA is moving towards digitization government has become more strict in the banking and financial sectors. As to provide security to the transactions and payments for the customers of banks is a must.

Due to the recent cyber-attacks on banks in India has left everyone worried. Such as Pune based Cosmos Bank recently saw a massive security breach where Rs 94 crore was siphoned off. In a similar incident, about $2 million was stolen from City

Union Bank through a cyber-attack. The Union Bank of India also fell prey to a hacking attempt and lost around $171 million, though they managed to recover it.

Taking into the account for the essential need to secure from cyber-attacks, Reserve Bank of India(RBI) which is the central regulatory and monitoring authority for controlling operations of banks in India. RBI has issued multiple circulars such as RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16 and circular RBI/2018-19/63, DCBS.CO.PCB.Cir.No. 1/18.01.000/2018-19, Dated 19th October 2018 for Urban Co-operative Banks for Cybersecurity Compliance.

All Urban Co-operative Banks are required to comply with the various guidelines prescribed and submit the report of Cyber Security Compliance after framing all the required policies and implementation of Cyber Security Controls.

Let us take look into the details given by RBI from both the circulars.

Cyber-security Policy: Banks has to immediately put in place the cybersecurity policy which contains a strategy that how the bank is dealing with the cyber threats and what is the readiness of the current defensive measures. Also to provide details regarding proper incident response and recovery framework. This policy needs to be approved from the board of members who are appointed by the RBI.

Also as per the RBI Cybersecurity policy should be different from the IT security policy of the bank.

Current State Assessment (As per RBI Cyber Security Framework)

1. Current State Security Assessment (CSSA)

    a. An interactive workshop to assess your current and desired state

    b. Security assessments that assess the current security landscape in your organization

    c. Recommendations for improvement

    d. The development of a security roadmap based on business and technology initiatives

2. CSSA - Value Proposition

    a. Org level view of data security control strengths and weaknesses

b. Understand business and technology risks

c. Identify critical, necessary and good-to-have controls

Drafting of Policies & Procedures & Implementation of Cyber Security Controls (As per RBI Cyber Security Framework)

Implementation

a. Security policies and procedures drafting & review
b. Risk assessment
c. Documentation structured storage and taxonomy
d. Compliance with RBI guidelines
e. Security Awareness Training

Implementation and Management of CSOC (As per RBI Cyber Security Framework): Continuous surveillance and real-time analysis were required as it helps in taking actions faster when attacked from outside. New guidelines would require banks to implement 24*7 real-time based surveillance.

Cyber Crisis Management Plan: The RBI circular calls for the establishment of a Cyber Crisis Management Plan to address the full lifecycle of detection, response, containment, and recovery. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond/recover/ contain the fallout.

Readiness Check/Audit to make sure that the RBI Cyber Security Framework has been successfully implemented.

National Cyber Security Policy, 2013: National Cyber Security Policy is a policy framework by Department of Electronics and Information technology (DeitY).

It aims at protecting public & private infrastructure from cyber attacks. It also intends to safeguard critical information such as personal information, financial & banking information, and sovereign data. Let us look into the details.

1. Set up of a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) for obtaining strategic information regarding threats to ICT infrastructure,

creating scenarios for a response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

2. Creation of a task force consisting of 5,00,000 cybersecurity professionals in the next five years through capacity building, skill development, and training.

3. Provision for fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cybersecurity.

4. Designation of CERT-In as the national nodal agency to coordinate cybersecurity-related matters and have the local (state) CERT bodies to coordinate at the respective levels.

5. All organizations to designate a CISO and allocate security budget.

6. Use of Open Standards for Cyber Security.

7. Development of a dynamic legal framework to address cybersecurity challenges (Note: The National Cyber Security Policy 2013 does not have any mention of the IT Act 2000)

8. Encouragement of wider use of Public Key Infrastructure (PKI) for government services.

9. Engagement of infosec professionals/organizations to assist e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development through PPP – a common theme across all initiatives mentioned in this policy.

10. Apart from the common theme of PPP across the cybersecurity initiatives, the policy frequently mentions of developing an infrastructure for evaluating and certifying trustworthy ICT security products.

4.5 CYBERSECURITY REGULATIONS IN OTHER COUNTRIES

Below are the major regulations entities in the European Union(EU)

European Union Agency for Network and Information Security(ENISA): An agency was initially organized by the regulation number 460/2004 of the European Parliament and of the Council of 10 March 2004 for the sole

purpose of raising information and security awareness for all the operations within the EU. ENISA currently runs under the regulation number 526/2013 which is the latest one. Their website has all the details related to the current policies, regulations and other cybersecurity related information. https://www.enisa.europa.eu.

EU General Data Protection Regulations(GDPR): It is created to maintain a single standard for the data protection among all the member states in the EU.

4.6 CYBERSECURITY POLICY FRAMEWORK

Now we will learn different cybersecurity policy framework for different business functions and understand how they are important.

Health Insurance Portability and Accountability Act(HIPAA): HIPAA was first enacted in 1996. HIPAA was established as a standard to protect the individuals' electronic personal health information(ePHI). To fulfill this U.S. Department of Health and Human Services(HHS) published the HIPAA Privacy Rule and HIPAA Security Rule.

Privacy rule deals with the standards set for the privacy of individually identifiable health information. Security Rule takes care of security standards for protecting health information that is in the electronic form. Security Rule’s goal is to secure individuals ePHI.

The components which are covers in this are allowed to adopt new technologies and to improve the quality and efficiency of patients care. It has been into light due to greater risk and data breaches in the healthcare sector.

Purpose of HIPAA:

It has two main purposes: to provide continuous health insurance coverage for workers who lose or change their job and to reduce the administrative burdens and cost of healthcare by standardizing the electronic transmission of administrative and financial transactions.

HHS expanded the act when it put the HIPAA omnibus rule in place in 2013 to implement modifications to HIPAA in accordance with guidelines set in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The omnibus rule also increased penalties for HIPAA compliance violations to a maximum of $1.5 million per incident.

The HHS Office for Civil Rights (OCR), which enforces HIPAA, issued guidance in 2016 clarifying that cloud service providers and other business associates of healthcare organizations are covered by the HIPAA privacy, security, and breach notification rules.

HIPAA violations can prove quite costly for healthcare organizations. In addition to the notification costs, healthcare organizations can encounter fines after HIPAA audits mandated by the HITECH Act which is conducted by the Office for Civil Rights. Providers could also face criminal penalties from violations of HIPAA privacy and security rules.

OCR undertook its first round of HIPAA audits of healthcare organizations in 2012 and 2013. Those pilot audits carried no fines or penalties.

A considerably wider, formal round of desk and in-person audits of about 200 healthcare-covered entities and business associates began in 2016 and continued into 2017. These audits were expected to carry fines or corrective plans.

OCR further strengthened the HIPAA security rule in 2016 by releasing a crosswalk between aspects of the National Institute of Standards and Technology's Cybersecurity Framework to identify cybersecurity gaps and align HIPAA with national cybersecurity standards.

Organizations can lower their risk of regulatory action through HIPAA compliance training programs. OCR has six educational programs on complying with privacy and security rules.

A number of consultancies and training groups offer programs, as well. Healthcare providers may also choose to create their own training programs, which often encompass each organization's current HIPAA privacy and security policies, mobile device management processes and other applicable guidelines.

What is considered protected health information under HIPAA?

- A patient's name, address, birth date, and Social Security number.
- An individual's physical or mental health condition.
- Any care provided to an individual.
- Information concerning the payment for the care provided to the individual that identifies the patient, or information for which there is a reasonable basis to believe could be used to identify the patient.

HIPAA contains five different sections or title which are listed below.

TITLE 1: HIPAA Insurance Reform

Title 1 provides health insurance coverage to individuals who lose jobs. It also provides group health plans coverage to individuals with specific disease and pre-existing conditions from setting lifetime coverage limits:

TITLE 2: HIPAA Administrative Simplification

Title 2 directs U.S. Department of Healthcare and Human Services(HHS) to establish security standards for processing the electronic healthcare transactions. It also requires for Healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations standards set by HHS.

TITLE 3: Tax Related Health Provisions

Provides guidelines for the tax-related provisions for medical care.

TITLE 4: Application and Enforcement of Group Health Plan Requirements

Provides health insurance reform. Also, it has provisions for individuals who have pre-existing medical conditions and those seeking continued coverage.

TITLE 5: Revenue Offsets:

It includes provisions for company-owned life insurance and the treatment of those who lose their U.S. citizenship for income tax purpose.

We will see more details regarding Title 2 as is more related to our context and requirements. Title 2 includes many other compliance requirements which are mentioned below:

National Provider Identifier Standard: Each healthcare entity, including individuals, employers, health plans, and healthcare providers, must have a 10 digit unique national provider number(NPI).

Transactions and Code Set Standard: Healthcare organizations must follow a standardized mechanism for electronic data interchange (EDI) in order to submit and process insurance claims.

HIPAA Privacy Rule: Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule establishes national standards to protect patient health information.

HIPAA Security Rule: The Security Standards for the Protection of Electronic Protected Health Information sets standards for patient data security.

HIPAA Enforcement Rule: This rule establishes guidelines for investigations into HIPAA compliance violations.

National Institute of Standard and Technology(NIST): President of the United States issued an Executive Order to improve the nations critical infrastructure which was directed to NIST.

NIST has worked with different stakeholders and created a framework with the collaboration between industry, government. The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. We will follow the details present in the actual source of the NIST publication under the article No: NIST.CSWP.04162018 for critical infrastructure.

Components of the Framework: Cybersecurity framework consists of three main components: The Core, Implementation Tier, and Profiles.

Framework Core provides desired activities and outcomes using a common taxonomy which is easy to understand. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

Identify: Develop the understanding to manage cybersecurity risk to systems, assets, data, and capabilities. To identify the business context, and core functional areas of the business are fundamental of this framework. Categories within this Function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Protect: Develop and implement appropriate safeguards to ensure the delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Categories within this Function include Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events. Categories within this Function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Categories within this Function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include Recovery Planning, Improvements, and Communications.

Figure 4.2 NIST Framework, Source: NIST Article: NIST.CSWP.04162018

The Framework Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

How to use Framework:

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

There are different sections present different ways in which organizations can use the Framework.

- Review Current Cybersecurity Practices
- Establish and improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders
- Buying decisions
- Identify opportunity for new or revised informative references
- Methodology to protect, privacy and civil liberties

Check Your Progress 1

---

1. Which is the most import data privacy and protection law in European Union?
2. Which function is responsible to timely identify any cyber threat according to NIST?
3. Which framework is responsible for security healthcare data of patients?

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 4.1 Function and Category Unique Identifier, Source: NIST Article NIST.CSWP.04162018

ISO/IEC 27000-series: It is also known as the 'ISMS Family of Standards' or 'ISO27K' for short comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The series provides best practice recommendations on information security management - the management of information risks through information security controls - within the context of an overall Information security management system (ISMS).

It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them (typically using information security controls) according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents. There are many documents in the ISO 27000 series and many others which are still under development.

- ISO/IEC 27000: Information security management systems. Overview and vocabulary.
- ISO/IEC 27001: Information technology Security Techniques. Information security management systems requirements. The 2013 release of the standard specifies an information security management system in the same formalized, structured and succinct manner as other ISO standards specify other kinds of management systems.
- ISO/IEC 27002: Code of practice for information security controls. Essentially a detailed catalog of information security controls that might be managed through the ISMS.
- ISO/IEC 27003: Information security management system implementation guidance
- ISO/IEC 27004: Information security management. Monitoring, measurement, analysis, and evaluation.
- ISO/IEC 27005: Information security risk management.
- ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems.
- ISO/IEC 27007: Guidelines for information security management systems auditing (focused on auditing the management system).

We will look at the ISO/IEC 27001:2013 which is: Information technology Security Techniques.

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of IT or data security specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole.

Moreover, business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management: Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts.

Design and implement a comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address risks that are deemed unacceptable and adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis. ISO/IEC 27001 is designed to cover much more than just IT.

Security Controls will be tested as part of certification to ISO/IEC 27001 which is dependent on the certification auditor. Management determines the scope of the ISMS for certification purposes and may limit it to, say, a single business unit or location.

This International Standard adopts the Plan-Do-Check-Act (PDCA) model, which is applied to construct and setup ISMS processes in an organization. It provides a robust model for implementing the principles of governing risk assessment, security design and implementation, security management, and reassessment.

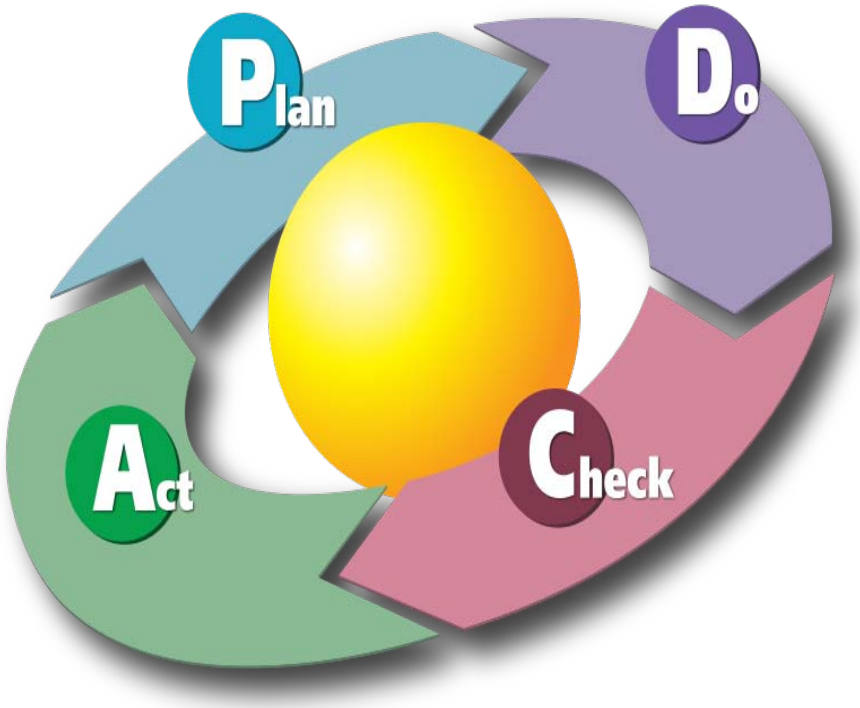


Figure 4.2 PDCS Cycle Source: Wikipedia.org

Plan (establishing the ISMS): To establish the policy, the ISMS objectives, processes, and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.

Do (implementing and workings of the ISMS): Implement ISMS policy, controls, processes and procedures.

Check (monitoring and review of the ISMS): Assess and measure the performances of the processes against the policy, objectives and practical experience and report results to management.

Act (update and improvement of the ISMS): Conduct an internal audit and undertake corrective and preventive actions, based on the audit results and take management review.

Payment Card Industry(PCI) Security Standards: The PCI security council provides a robust set of standards and supporting materials to enhance the security for payment card data security. Which includes specifications, tools, supporting resources which ensures the safe handling of cardholder information. The key to this is the PCI Data Security Standard(DSS). It provides and robust and actionable framework for payment card data security process. Which includes prevention, detection, and response to any security incident. Below is a high-level overview of the 12 PCI DSS requirements.

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and

	processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 14.2 PCI DSS Requirements and Testing Procedures

Source:www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

This above table of PCI Data Security Standard shows the requirements and Security Assessment procedures combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process.

Check Your Progress 2

1. What are the 4 phase of CCMP?

2. ISO standard which is used for Information Security and Risk Management is _____

3. Which section is respoble to secure electronic healthcare data?

PCI DSS is applicable to all who are involved in payment card processing such as merchants, service providers processors, issuers, acquirers. Also to them who are part of storing, processing or transmitting the payment card data.

Sensitive data of card holder which is defined as Account Data which further includes:

Cardholder Data includes:

- Permanent Account Number(PAN)
- Cardholder Name
- Expiry Date
- Service Code

Sensitive Authentication Data:

- Magnetic chip data or data stored on the chip.
- CVV2/CID/CAV2
- PIN

4.7LET US SUM UP

A security framework is a combination of different terminology used which provides guidance on topics related to information systems security and regarding its planning, implementation, management, auditing, review process. In this chapter, we have seen multiple frameworks which are used for different business functions and are followed to achieve the best security practices. We have National Cybersecurity Policy, 2013 from the Indian context. GDPR which is an important data privacy law in the European Union. Also, we have seen HIPAA which is used in the healthcare industry to process and store patients data and to achieve robust security control over the patient's electronic healthcare data. At last, we have seen NIST, ISO/IEC standards and PCI DSS standards.

4.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. GDPR

2. Detect Phase

3. HIPAA

Check Your Progress 2

1. 4 phase of CCMP are Detection, Response, Recovery, Containment.

2. ISO 270005

3. Title 2 Administrative Simplification

Block-2

Network DefenceTools

Unit 1: Firewall And Packet Filters

1

Unit Structure

1.1. Learning Objectives

1.2. Firewall

1.3. Packet Filtering

1.4. Intrusion Detection System(IDS)

1.5. Intrusion Prevention System(IPS)

1.6. Security Information and Event Management

1.7. Let Us Sum Up

1.8. Check Your Progress: Possible Answers

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand various types of firewalls
- Understand packet filtering
- Understand intrusion detection system

1.2 FIREWALL

Every small and big enterprise comprises the network of machines. They tend to communicate, sharing information, sharing resources, data in and out of the network. They are also connected to the internet. But once the machines are connected to the internet it opens all the ways for the outsiders or better to say hackers which has the malicious intent and start attacking the machines.

This is the point where the concept of a firewall comes into the picture. In simple terms, a firewall can be explained as a wall built to protect from the fire and slow down its spread. In networks also it has a similar concept and understanding. A firewall intended to stop unauthorized users from accessing the network. The most common place to deploy the firewall is between the trusted and untrusted network of organization which typically is the internet.

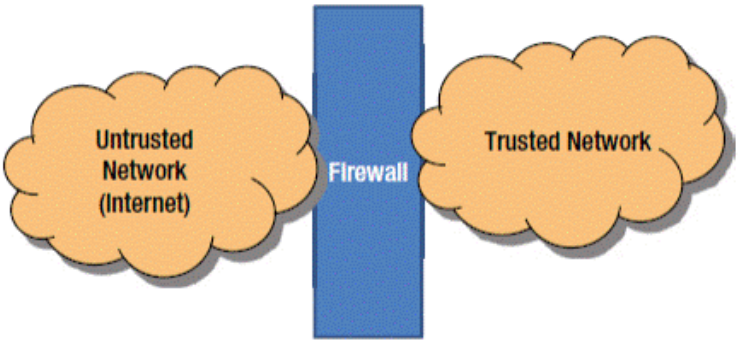


Figure 1.1 Firewall Deployment

The term firewall has different meanings which are based on the implementation and purpose. That will be the place where the security policies are implemented. The firewall's external network interface card is the gateway to the internet. The purpose is simple, to protect what is there on your side of the gateway.

According to RFC 2647l, a firewall is a device, operating system, or application program, that enforces an access control policy between networks.

A firewall acts as a gatekeeper between your local area network and the internet. All traffic from in and out of the LAN must pass through the firewall. There needs to be some type of firewall installed in your network even if you are a home user having a broadband connection or high-speed connection.

Firewall setup can be done in different ways based on implementation and usage. You can purchase a hardware firewall which is basically a router with inbuilt firewall features. Also, most of the hardware appliances come with the web-based interface which will provide an easy interface to connect with firewall and setting can be easily configured. The purpose here to configure the firewall will enforce the policy which is defined during the configuration which will allow or deny the internet traffic based on that rules and policies configured. Security policies are all about the access control and authenticated use of private or protected use of the application, file services and programs.

Another way is to install a server computer and use it as the firewall. In large networks, it is sometimes hard to figure out where to place the firewall or perimeter. Perimeter is used to describe the location of the firewall inside the large networks(WAN). Let us discuss different types of firewall techniques.

1.2.1 TYPES OF FIREWALL

Packet Filtering: Packet filter firewall examines each packet that crosses the firewall and checks the packet according to the set of rules which are defined. If all rules are satisfied with the packet that it is allowed and if not then the packet is rejected.

It is the very least expensive type of firewall. Packet filters work by inspecting the source IP address, destination IP address, a port number assigned to each service.

The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN, and ACK bits, etc.

Packet filtering rule has two parts:

- **Selection criteria** − It is used as a condition and pattern matching for decision making.

- **Action field** − This part specifies an action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules. As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permit or denies the individual packets. As it is the most common firewall technique it has its own weakness.

One of the biggest weaknesses of packet filtering is that it trusts that the packets themselves are telling the truth when they say who they're from and who they're going to. Hackers exploit this weakness by using a hacking technique called IP spoofing, in which they insert fake IP addresses in packets and they send to your network.

Another weakness of packet filtering is that it examines each without considering what packets have gone through the firewall before and what packets may follow. In other words, packet filtering is stateless. In spite of these weaknesses, packet filter firewalls have several advantages also.

Packet filters are very efficient. They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports have been determined, the packet filter quickly applies its rules and either sends the packet along or rejects it.

Packet filters are inexpensive. Most routers include built-in packet filtering.

Stateful Packet Inspection: Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established). It can tell if the MTU has changed and whether packets have fragmented. etc. Stateful firewalls are better at identifying unauthorized and forged communications.

Circuit Level Gateway: A circuit-level gateway manages connections between clients and servers based on TCP/IP addresses and port numbers. After the connection is established, the gateway doesn't interfere with packets flowing between the systems.

SOCKS (RFC 1928) refers to a circuit-level gateway. It is a networking proxy mechanism that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side without requiring direct IP reachability. The client connects to the SOCKS server at the firewall. Then the client enters a negotiation for the authentication method to be used and authenticates with the chosen method.

The client sends a connection relay request to the SOCKS server, containing the desired destination IP address and transport port. The server accepts the request after checking that the client meets the basic filtering criteria. Then, on behalf of the client, the gateway opens a connection to the requested untrusted host and then closely monitors the TCP handshaking that follows.

The SOCKS server informs the client, and in case of success, starts relaying the data between the two connections. Circuit level gateways are used when the organization trusts the internal users and does not want to inspect the contents or application data sent on the Internet.

Application Level Gateway:

Application level gateway firewall systems are more advanced in terms of its features and working in compare to packet filtering or stateful packet inspection or circuit level gateway. It treats all the packets as equal level or equal priority. Application gateway firewall system knows the details that which application has generated these packets.

In addition to that application level gateway is also worked as proxy servers. A proxy server is a server that sits between the client machine and server machine. The proxy server will intercept the packet and will identify that the packets that are intended for the server machine or not and then it process them.

For eg: web proxies are often stores the copies of the commonly used web pages in their local cache memory. When a user requests to access such pages which are present in the local cache memory that proxies itself reply to the user request, which

in turns is very effective for the faster response. If it does not have the copy of the webpage it passes the request to the server machine.

Application level gateway is aware of the details, how a server machine handles TCP/IP requests and sequence of packets. So they can easily identify if the incoming packet is legitimate or fake or is part of an attack.

Application level gateway is more costly in terms of the price and cost of configuration and maintaining them. Application level gateway can slow down the network as it checks every packet in the deep which takes more time to process the packet before allowing them in or out of the network.

Firewall with Demilitarized Zone(DMZ): The term DMZ originally arrives from the military where an area between two territories, military operations are prohibited.Similar way, many organizations are facing is how to enable or allow to access to legitimate services of their organization to public services. While considering that not to compromise any other services of the organization. To achieve this the typical approach is to use a firewall to achieve the DMZ.

It will help to maintain and improve the security of the organization, by segregating the devices and machines on the opposite sides of the firewall. DMZ will act as a small and isolated network established between that internet and private network.

Some of the important functions of the DMZ are:

- All the traffic that goes in and out is inspected.
- Resources inside the DMZ are under continuous security monitoring to save them from being compromised from external cyber attack.
- It acts as a protective boundary for the private network.

1.3 PACKET FILTERING

Packet filtering is a process of allowing or blocking packets at one of the OSI layers which are usually a network layer, which also contains an IP header. IP header is used for routing packets through the internet as it contains all the important information of all protocols, IP address such as Source IP address and port,

destination IP address and port as IP V4 is of 32 bit we have the similar IP V6 which is of 128 bit and contains similar information.

There is another protocol apart from the IP which is TCP protocol.

bit offset	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

Figure 1.2 IP Header Source: Wikipedia

Offsets Octet		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0										S Y N		Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if Data Offset > 5, padded at the end with "0" bytes if necessary) ...																															

Figure 1.3 TCP Header Source: Wikipedia

Important pieces of the TCP protocol header are the following fields:

- Source port: from which port the packet was sent.
- Destination port: to which port the packet is going.
- Flags: URG, ACK, PSH, RST, SYN, FIN

Packet filtering looks at the source IP address, destination IP address, source port number, destination port number, flags and other information to decide whether some packet should be accepted or rejected.

Usually, packet filtering is also smart enough to remember previous packets that are all analyzed together to decide if a packet is considered malicious and is rejected/dropped, or if it should be passed through.

Check Your Progress 1

---

1. Which type of firewall technique stores the local copy of the data accessed by user?

2. Which is an expensive and time consuming firewall technique ?

3. Which are 3 important piece of information which is useful in packet filtering ?

Capabilities of Packet Filter: A packet filter has to have the following capabilities:

- Examination of each packet data and headers.

  Each packet is examined when it comes to the packet filter. This is done with the help of filtering rules defined in the next point.

- Set of rules which define what to do with the packet.

  These rules define what a packet filter should look for when it receives a packet. It usually looks for the information we've already talked about, like source IP address, destination IP address, source port number, destination port number, etc.

- What actions are taken based on the result of the examination.

  There are numerous actions which can be used when a packet filter receives a packet and has filtering rules defined. Based on defined filtering rules, a packet filter can do the following:

- Accept only packets that are certainly safe based on a set of rules. Drop all other packets.

- Drop only packets that are certainly unsafe based on a set of rules. Accept all other packets.

- If a packet is received for which there is no filtering rule defined, ask a user what to do with it.
- Block a user coming from a defined source IP address because too many packets were received in too short of a time window.
- Almost any action can be applied against a packet or a set of packets. If we want to send an HTTP response, which includes “Hello, How Are You?” to every HTTP request coming from IP xxx.xxx.xxx.xxx, we could define a rule that could do that.
- Packet filter also identifies whether the packets are broken or not received properly.

Limitations:

Packet filter does not read the content of the packet or it cannot check the payload of the network packet; which implies that it cannot stop the application layer attack.

Packet Filtering Categories: Anoverview of packet filtering categories are shown in the below image.

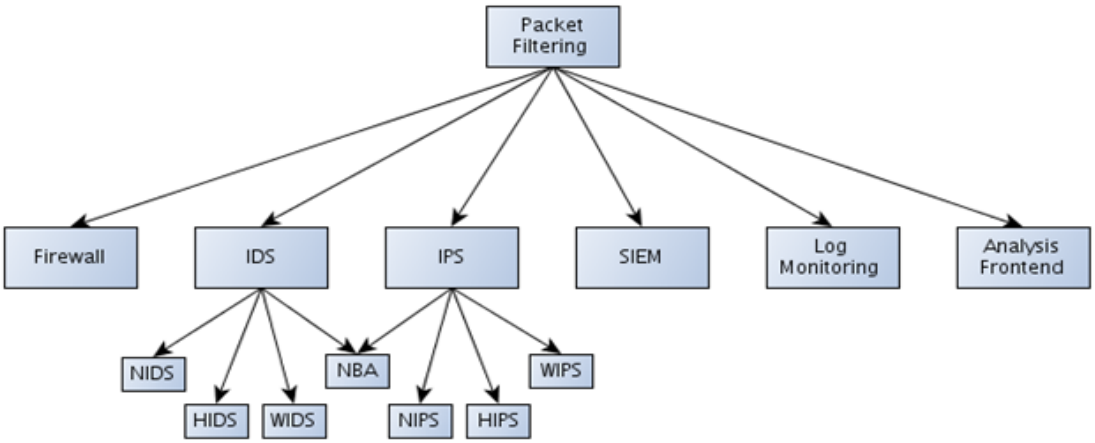


Figure 1.4 Categories of Packet Filters Source: resources.infosecinstitute.com

As we have already seen the detail introduction of Firewall we will see details regarding other components. But before that, it is better to understand that other components are not a replacement of the firewall but can be used along with the firewall for better security measures.

1.4 INTRUSION DETECTION SYSTEM(IDS)

An intrusion detection system can be software-based or hardware-based and is used to monitor network packets or system for malicious activity and perform a specific action if such activity is detected. Usually, if malicious activity is detected on the network, the source IP of the malicious traffic is blocked for a certain period of time, and all of the packets from that IP address will be rejected.

There are several types of intrusion detection systems:

- **Network intrusion detection system (NIDS)**

  NIDS detects malicious activity by monitoring and examining network traffic. This type of IDS usually runs when packets enter a specific network on a special hardware component whose only job is to monitor and accept/reject packets from the Internet and let them into the local network. Example: Snort.

- **A host-based intrusion detection system (HIDS)**

  HIDS detects malicious activity by monitoring and examining system calls, application logs, access control lists, etc. HIDS usually contains a software agent that needs to be installed on the operating system. Examples: Tripwire, OSSEC. A wireless intrusion detection system (WIDS)

  WIDS monitors the wireless network for malicious behavior, which can be the number of packets sent in a time window, too many deauthentication packets, too many broadcast requests, etc. WIDS usually run on an AP (Access Point) and doesn’t allow certain users to connect to it if malicious activity is detected.

- Network behavior analysis (NDA)

  NDA monitors network traffic passively to detect unknown and unusual patterns that might be a threat. It should be used together with the firewall as well as other types of IDS systems.

Check Your Progress 2

1. Mention the limitation of packet filtering .

2. Where the firewall is placed inside the network ?

3. Where do we generally use the ACL(Access Control List) ?

1.5 INTRUSION PREVENTION SYSTEM(IPS)

The intrusion prevention system is basically an upgrade of the intrusion detection system. Where the IDS is used to detect and log the attack, the IPS is used to detect, block and log the attack. The IPS systems are able to prevent certain attacks while they are happening. There are multiple versions of the IPS systems, but we won't describe them in detail, since they are the same as with IDS systems, with the exception that all of the types of IPS system also prevent the attack from continuing. The types of IPS systems are NIPS, HIPS, WIPS.

1.6 SECURITY INFORMATION AND EVENT MANAGEMENT

With SIEM we can monitor security alerts generated by various software or hardware solutions that are used for detecting malicious activity. SIEM consists of:

- SIM (Security Information Management): provides the analysis and reporting of the logged data.
- SEM (Security Event Management): provides monitoring and correlation of events.

A SIEM gathers information or data at a single point and provides a human-readable security report about the malicious behavior that is happening in our network. A SIEM solution must work in real time, so we can secure our network in a timely fashion.

What would happen if we received a report about a security breach that is a month old, it wouldn't help us a lot since the attacker is probably long gone with all the data that he needed.

SIEM capabilities are as following:

- Data Aggregation: provides means to join data together from many sources: network, servers, databases, applications.
- Correlation: correlates data into meaningful sets to learn something new from it.
- Alerting: analysis of correlated events and alerting the recipients of detected security issues.
- Dashboards: provides means to present data in meaningful charts.
- Compliance: automatically gather all the needed data and produce reports.
- Retention: provides long-term storage of historical data for later analysis.

SIEM also implements log monitoring and analysis frontend, but we've nevertheless pointed them out as independent points in the above picture because other tools can be available just for that. We can also write our own script that would take the logs and report some malicious activity.

Log Monitoring and Analysis Frontend: It is an important part of the overall picture since this is the tool we use to look at the malicious activity that happened on our network. There are quite a few frontends available such as OSSIM, Sguil.

1.7 LET US SUM UP

In this chapter we have seen concepts of the firewall and packet filters. Also What all different types of firewall technique is there and how it is used in the organization.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check your progress 1

1. Web Proxy

2. Application Level Gateway

3. Source & Destination IP and Flags

Check your progress 2

1. Limitation of packet filtering are it cannot read the content of the packet and make a decision, complex configuration.

2. Between trusted and untrusted network

3. ACL is generally used in routers

Unit 2: Introduction To Windows And Linux Firewall

2

Unit Structure

2.1. Learning Objectives

2.2. Introduction

2.3. Windows Firewall

2.4. Linux Firewall

2.5. Let Us Sum Up

2.6. Check your Progress: Possible Answers

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand Linux and window firewalls.

2.1 INTRODUCTION

In this chapter, we will see the details of the firewall in the different operating system such as Linux and windows and how it works. As both Windows and Linux are completely different operating systems, supports different file types, Linux is an open source and windows is a propriety one.

Both operating systems can be used as a standalone machine as well as can be used for the server machine based on the requirements. But there is something common set of requirements for any user is to secure from the external threats.

Many of the network administrators think that Linux has many advantages over windows, not just only freely available. But it is more stable than windows, less often crashing than windows. Easy configuration and less downtime required. Can be easily used for a file server, web server, email server, can be used in an intranet. Also as a router and firewall to help to connect to the network.

2.3 WINDOWS FIREWALL

Over the period of time windows operating system has grown much in providing its core functionality as an operating system. Windows Firewall was first included in Windows XP (back in 2001), and since then it has been improved in each new version of Windows. For every operating system, it is important to provide the core security infrastructure inbuilt within the operating system which handles implementing security protocols, enforcing security policies by providing dedicated firewall as software to monitor the network traffic.

One of its roles is to block unauthorized access to your computer. The second role is to permit authorized data communications to and from your computer.

Firewall Functions in Windows Operating System: Windows firewall with advanced security in windows server operating systems blocks unauthorized

network traffic flowing into or out of a local device by providing host-based, two-way network traffic filtering.

While the old Windows Firewall allowed you to configure only a single set of inbound and outbound rules (a profile), Windows Firewall with Advanced Security includes three profiles (Domain, Private and Public), so you can apply the appropriate rules to each server based on its connection to the network.

- Domain networks. Networks at a workplace that are attached to a domain.
- Private networks. Networks at home or at work where you trust the people and devices on the network. When private networks are selected, network discovery is turned on but file and printer sharing is turned off.
- Guest or public networks. Networks in public places. This location keeps the computer from being visible to other computers. When a public network is the selected network location, network discovery and file and printer sharing are turned off.

You can also configure the following options for each of the three network profiles in advance windows firewall settings:

- Firewall State. You can turn the firewall on or off independently for each profile.
- Inbound Connections. You can block connections that do not match any active firewall rules (this is the default), block all connections regardless of inbound rule specifications, or allow inbound connections that do not match an active firewall rule.
- Outbound Connections. You can allow connections that do not match any active firewall rules (this is the default) or block outbound connections that do not match an active firewall rule.
- Protected Network Connections. You can select the connections — for example, the Local Area Connection — that you want Windows Firewall to help protect.
- You can configure display notifications and unicast responses, and merge rules that are distributed through Group Policy.
- You can configure and enable logging.
- IPsec Settings. You can configure the default values for IPsec configuration.

Apart from the packet filtering, IP security windows also provide the functionality of the VPN(Virtual Private Network).

> **Virtual Private Network:** A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from getting traceback while on the public network.
>
> They originally were just a way to connect business networks together securely over the internet or allow you to access a business network from home. Most operating systems have integrated VPN support.

You can use a VPN to:

- Bypass geographic restrictions on websites or streaming audio and video.
- Protect yourself from snooping on untrustworthy Wi-Fi hotspots.
- Gain at least some anonymity online by hiding your true location.
- Protect yourself from being logged while torrenting.

By default Windows Firewall is on and can be found as Goto Control Panel then goes to Windows Firewall. Click on the Windows Firewall and you will see the current status of the firewall and types of networks. Active connections if there are any.

On the left side, there are several options to configure the default firewall setting to change it as per requirements.

On left side panel there in the above image, there is an option of Advance Setting on clicking that option will lead you to open another window of Windows Firewall with Advanced Security as shown below; Where you can set the inbound and outbound rules.

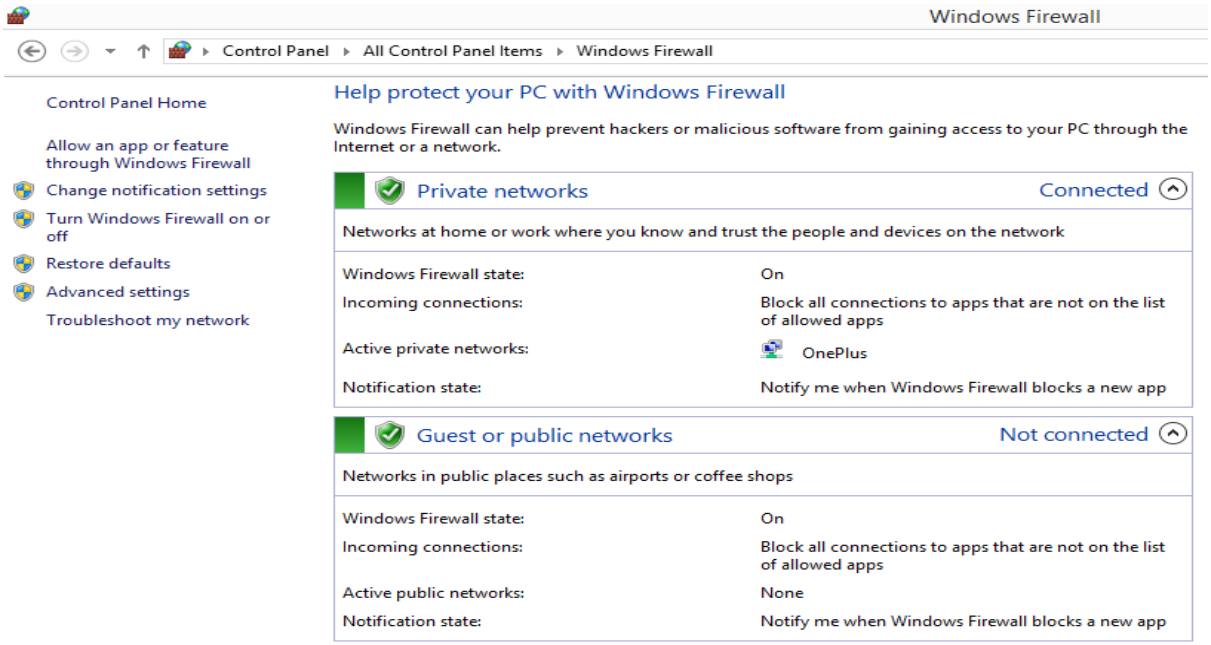


Figure 2.1 Windows Firewall

Figure 2.2 Windows Firewall with Advanced Security

2.4 LINUX FIREWALL

Before getting deep into the Linux Firewall we will go through some of the highlights of the Linux Operating System. Linux was created in 1991 by Linus Torvalds when he was an undergraduate student at the University of Helsinki in Finland. He has first

created his own operating system based on Unix. After that nearly two decades Linux has become a full-featured operating system which is fast and reliable. Linux has got a solid reputation for efficiency and security.

Linux is a multiuser operating system. Which means more than one user can log on into the system and can use the system at the same time; Where mostly all versions of windows are the single-user system. Only one user at a time can log in in a windows machine and can use it.

Linux has a very different way of using the file system, unlike windows. There is no concept of “C:/” Drive in Linux. Instead, Linux combines all drives and partitions into a single directory hierarchy. In Linux, one partition is designated as “root” partition. It is similar to the C:/ drive in the windows system. There are many distributions available based on the package manager which is either Debian based or RPM-based operating system in Linux.

Though there are common components which are present in all different distributions which are Linux Kernal, administrative tools and packages. An operating system such as Ubuntu, Lubuntu, are Debian based operating system which supports .deb packages. Another one is RPM-based package manager operating system such as Fedora, CentOS. Which supports .rpm based packages. Redhat is one operating which is the most stable version of RPM-based operating system and which doesn't come freely. Let us understand the security features of the Linux operating system.

Netfilter: Netfilter is a framework provided by Linux Kernal which allows networking operations to be implemented in the form of handlers. Netfilter supports different operations and functions for packet filtering, network address translation, a port translation which allows or rejects the network packets in the network.

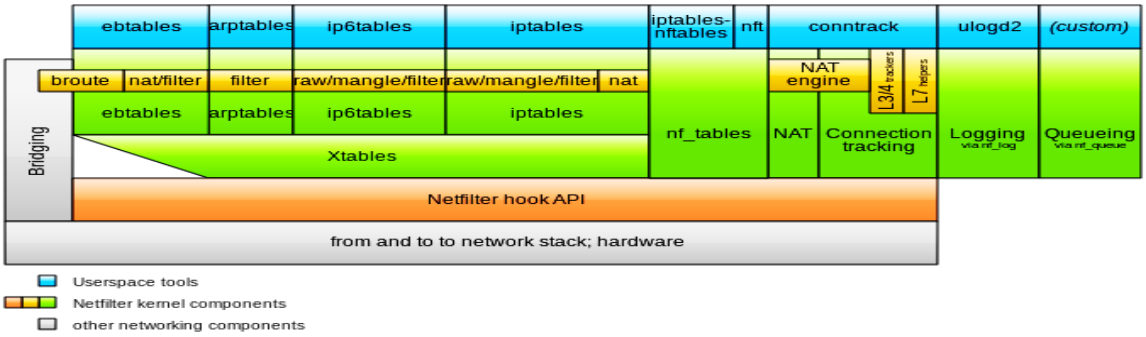


Figure 2.3 Netfilter Components Source: Wikipedia

The *Netfilter* framework included in the Linux kernel restricts incoming and outgoing network connections according to a set of rules that have been defined by the administrator. Several Linux distributions configure firewall rules by default and offer utilities for managing simple firewall configurations. You may also manage the firewall rules on any Linux system with the standard iptables and ip6tables command-line utilities. Use of iptables will only configure restrictions for IP version 4 connections and that you will need to use ip6tables to set up rules for IP version 6 as well.

Fedora, Red Hat, and SUSE automatically enable the firewall and supply their own graphical configuration utilities. You must manually configure and enable the firewall on Debian and Ubuntu systems. Current releases of Ubuntu include a command-line utility called *ufw* for firewall configuration.

Those Linux distributions that enable a firewall by default use a netfilter configuration that blocks connections from other systems. Any attempt by a remote system to access a service on a blocked port simply fails. This means that no other system may connect to an installed service unless you specifically choose to unblock the relevant port.

Let us try to understand the basic functionality such as NAT(network address translation), Port forwarding

Network Address Translation: Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

Port Forwarding: Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the

opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

IPtables: IPtables which is an inbuilt firewall in Linux system. It is a user based application for configuring the tables provided by the Linux kernel firewall. iptables is the default firewall installed with Red Hat, CentOS, Fedora distributions.

Different modules and programs are used for different protocols such as iptables for IPv4, ip6tables for IPv6 and so on. It uses the concept of IP addresses, protocols (TCP, UDP, ICMP, etc) and ports.

IPtables is a command line firewall that uses the concept of chains to handle the network traffic. It places the rules into chains, i.e., INPUT, OUTPUT, and FORWARD, which are checked against the network traffic. Decisions are made as to what to do with the packets based on these rules, i.e., whether the packet should be accepted or dropped.

These actions are referred to as targets. DROP and ACCEPT are commonly used predefined targets used for dropping and accepting the packets, respectively.

IPtable architecture comprises groups of network packets, processing rules into tables and chains for processing the rules.

Rules consist of matches to determine which packet the rule will apply to and the targets. They operate at the network layer.

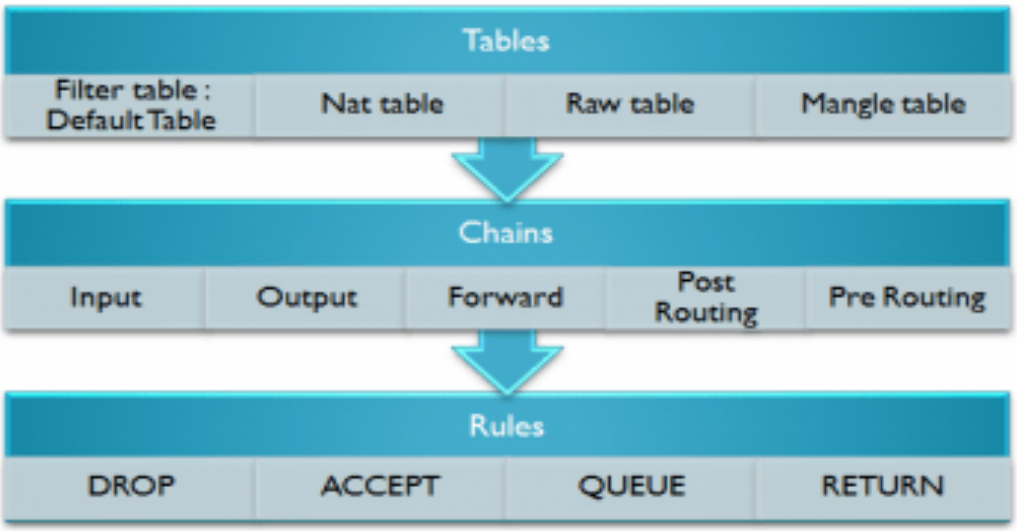


Figure 2.4 Iptables Architecture

Before you can configure rules with the iptables command, you have to understand a few concepts and Linux-specific terms:

Tables: This is a default table that Linux firewall stores and maintains sets of rules. The main table is the filter table, where you define most rules that apply to incoming and outgoing traffic. The nat table contains rules that define how Linux performs NAT. The mangle table is used for advanced packet routing.

Chains: Linux uses this term to refer to a set of rules that Linux applies when filtering network traffic. Here are the three main chains, each of which is part of the filter table:

The three predefined chains in the filter table to which rules are added for processing IP packets are:

- INPUT: These are packets destined for the host computer.
- OUTPUT: These are packets originating from the host computer that leaves from the firewall.
- FORWARD: These packets are neither destined for nor originate from the host computer, but pass through (routed by) the host computer. This chain is used if you are using your computer as a router.

Let us see with the commands used on the Linux terminal, on how to work with iptables. Linux includes many different numbers of iptables commands. We will start with the basic syntax of the command-line options.

>>iptables [-t table] CMD [chain] [filter_match] [target]

Iptables commands must specify the table where the command will be applied, the command itself, the chain to which the command will belong, an expression that defines what type of traffic the filter will apply to, and what Linux should do with the packet. For example, to add a simple rule to the input chain of the filter table that would drop all ICMP traffic, your command-line would look something like this:

>>iptables -t filter -A INPUT –p icmp DROP

Above command tells the Linux system that, when the filter table's input chain receives the packet which uses ICMP protocol, send the packet to DROP target. Which simply means that to dump all ICMP protocol-related traffic.

Before moving to see more details we will first see the most commonly used iptables commands which are described in the below table.

Table 2.1 Iptables Commands

Command	Name	Description
-A	Append	This command appends a rule to the end of a chain.
-I	Insert	This command inserts a rule to the beginning of a chain.
-D <chain><rule number>	Delete Rule	This command deletes a rule.
-L [<chain>]	List	This command lists all rules in a chain. If you don't specify a chain, the command lists the rules in all chains.
-N <chain>	New	This command creates a new user-defined chain.
-X <chain>	Delete Chain	This command deletes a user-defined chain.
-F [<chain>]	Flush	This command deletes all rules in a chain. If you don't specify a chain, the command deletes all rules in all chains.
-h	Help	This command lists all iptables commands and options.

It is important to check the order of the commands used to prepare the rules. As Linux firewall. Once it matches the packet it no further checks for next defined rules.

Because of this, iptables has the convenient -A command that appends commands to the end of the processing chain and the equally convenient -I command that adds commands to the beginning of the processing chain or a user-specified location.

Now we will check the common iptables options available to prepare the rule.

Table 2.2 Iptables Options

-p protocol	Specifies the protocol. It can be TCP, UDP, ICMP or the protocol number which is listed in /etc/protocols.
-s source_address	Specifies source address of the packet. Also, specify the subnet mask along with the source address such as –s 192.168.1.2/24
-d destination_address	Specifies the destination address of the packet.
--source-port	Specifies the source port of a TCP or UDP packet.
--destination-port	It refers to the destination port of the TCP or UDP packet.
-i interface	Specifies the network interface for the incoming packet. For eg: -i eth0.
-o interface	Specifies an output interface on which packet is to be sent. For eg: -o eth1.
-j target	Specifies that packet should be sent to the specified target. For eg: -j DROP. Which means that the packet should be sent to DROP target(to discard the packet).

To check the status of the iptables, execute the following command.

>>service iptables status

```
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

Figure 2.5 iptables status

To start and stop iptables service, use the following command on Linux terminal.

>>service iptables start / stop

To open the iptables files on the Linux system, use the following command.

>>gedit /etc/sysconfig/iptables

Here the gedit is the text editor in Linux as similar as notepad in windows for text editing operations.

Now let us create some iptables rules.

To allow SSH traffic, use the following command:

>> iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

>> iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

Above command specifies that for all input packets received on the interface eth0 for the TCP protocol with the destination port 22 (for SSH traffic) for the new connection or established one, accept the request.

Similarly, for the traffic leaving the firewall from the interface eth0 where the source port is 22 and established connection allow it to leave from the firewall.

Check Your Progress 1

---

1. Provide the iptable rule to block the ip address 9.9.8.8.

2. Provide iptable rule to accept the ping request from outside to inside and inside to outside.

3. Give short details regarding the iptables chains.

SELinux: Security-Enhanced Linux (SELinux) is a Linux kernel security module that integrated into the 2.6.x kernel using the Linux Security Modules (LSM)which provides a mechanism for supporting access control security policies, including mandatory access controls (MAC).

It is a project of the United States National Security Agency (NSA) and the SELinux community. SELinux integration into Red Hat Enterprise Linux was a joint effort

between the NSA and Red Hat. SELinux is also implemented as a standard feature in Centos/Fedora-based distributions and widely deployed.

A Linux kernel integrating SELinux enforces mandatory access control policies that confine user programs and system services, as well as access to files and network resources.

Limiting privilege to the minimum required to work eliminates the ability of these programs and daemons to cause harm if faulty or compromised (for example via buffer overflows or misconfigurations).

This confinement mechanism operates independently of the traditional Linux (discretionary) access control mechanisms.

SELinux is set in three modes:

- Enforcing – SELinux security policy is enforced. If this is set SELinux is enabled and will try to enforce the SELinux policies strictly
- Permissive – SELinux prints warnings instead of enforcing. This setting will just give a warning when any SELinux policy setting is breached
- Disabled – No SELinux policy is loaded. This will totally disable SELinux policies.

SELinux is set in two levels:

- Targeted – Targeted processes are protected.
- Mls – Multi Level Security protection.

To check whether the SELinux is enabled or not in the Linux system you can use this below commands. You can use the CentOS or Fedora (RPM) based Linux distributions for the SELinux workings.

Lets understanding the working of SELinux:

>>*getenforce*

The output will be either “enabled” or “disabled”

To check the status of the SELinux we can use:

>>*sestatus*

The output of the above command will be like:

Sample output:

SELinux status: enabled

SELinux mount : /selinux

Current mode: enforcing

Mode from config file: enforcing

Policy version: 21

Policy from config file: targeted

From the above output, we can see that SELinux is enabled and it is in enforced mode and to see detailed status you can use -b option, this will give on which services SELinux is enabled and which services are disabled.

>>sestatus -b

Sample Output:

SELinux status: enabled

SELinuxfs mount: /selinux

Current mode: permissive

Mode from config file: enforcing

Policy version: 24

Policy from config file: targeted

Policy booleans:

abrt_anon_write off

allow_console_login on

allow_corosync_rw_tmpfs off

allow_cvs_read_shadow off

allow_daemons_dump_core on

allow_daemons_use_tty on

allow_domain_fd_use on

allow_execheap off

allow_execmem on

allow_execmod on

SELinux can potentially control which activities a system allows each user, process, and daemon, with very precise specifications. It is used to confine daemons such as database engines or web servers that have clearly defined data access and activity rights.

2.5 LET US SUM UP

In this chapter, we have seen the basic fundamentals of the Windows firewall and Linux firewall. Both the operating system is different in terms of the file format, networking, security management. Windows has an inbuilt Windows Firewall which provides security management using inbound and outbound rules. Also, the user can allow which application network traffic to accept and reject. Similarly, in Linux, there are concepts of Netfilter, iptable and SELinux which are used on RPM-based distributions. In which you can there are chains which contain the set of rules/ policies defined and can be enforced on the system.

2.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. iptable rule to block the ip address 9.9.8.8:

   iptables -A INPUT -s 9.9.8.8 -j DROP

2. iptable rule to accept the ping request:

   iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

   iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

   iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

   iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

3. iptables chains:

INPUT chain – Incoming to the firewall. For packets coming to the local server.

OUTPUT chain – Outgoing from the firewall. For packets generated locally and going out of the local server.

FORWARD chain – Packet for another NIC on the local server. For packets routed through the local server.

Unit 3: Attacks On Wireless Networks

3

Unit Structure

3.1. Learning Objectives

3.2. Introduction

3.3. Basics of Wireless Network

3.4. Standards in Wireless Network

3.5. Wireless Network Attack

3.6. Let Us Sum Up

3.7. Check your Progress: Possible Answers

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- To Learn different wireless network standards.
- Current Issues with Wireless Network.
- Different attacks on wireless networks and their mitigation strategies.
- Tips to remain secure during wireless connection
- Introduction to Snort how to use it.

3.2 INTRODUCTION

In today's time, the wireless network is present everywhere from home to data centers. They make life easy from the long and bulky cables and its related issues. While ensuring the proper network connectivity with the internet to perform our everyday task. In order to learn the wireless (In short Wi-Fi which came from wires fidelity) networks. It was first invented by AT&T in the Netherlands in 1991. We will also see the basics of the wireless networks first and it's different standards, security issues, and attacks and mitigation strategies. Also, we will learn about the SNORT tools which is basically and IDS/IPS tool used for securing and monitoring the network.

3.3 BASICS OF WIRELESS NETWORK

Wireless network in simple terms means the transformation of the information or power between two nodes without any kind of physical electrical conductor. Wireless technology uses radio waves for short and long-distance communication.

There is a wide range of application of this wireless technology such as in telecommunication, satellite communications, mobiles, etc. There are multiple types of wireless network exists which I am sure you will be aware by the names as Wide Area Network(WAN), Local Area Network(LAN), Mobile Adhoc Network(MANET).

All these different types of networks are used for a different purpose but using wireless technology is at the core of all this. This network is a very popular choice for

home users and from the small and medium size organization. There are three essential components of the wireless network that are radio signals, antenna, and router. The radio waves are the key which makes the Wi-Fi networking possible. Which are then converted to signals and picked by the Wifi receivers which is transmitted by the antenna. Then users are connected through the router for the communication.

The access point or router has a unique feature called as a beacon transmission, where it keeps on sending a signal on the wireless radio spectrum. This signal contains the network identification known as the service set identifier (SSID) and some trivial error correction information.

The wireless receiver such as a laptop or any wireless device detects this signal in order to show it in the list of available wireless networks. It also detects whether or not the access point is using any security, and what level of security protocol, etc.

The access point or router contains TCP/IP stack which responds to ARP requests when a node tries to connect to it. Since wireless can allow multiple nodes at any instance, it is essential to have an authentication layer prior to starting the data transfer. It is the responsibility of the access point to ensure this security and monitor the packet transmission and data integrity.

3.4 STANDARDS IN WIRELESS NETWORKS

For the wireless networks, 802.11 is the working group from the Institute of Electrical and Electronics Engineers (IEEE) who defines the standard of operation for a specific technology. They are the group of expert members who works on it. There is multiple version of this. In each version, there is an improvement in the features of 802.11.

Standard	Frequency	Speeds	Interoperates with
802.11a	5 GHz	54 Mbps	None
802.11b	2.4 GHz	11 Mbps	None
802.11g	2.4 GHz	54 Mbps	802.11b

802.11n	2.4 / 5 GHz	100 Mbps	802.11b, 802.11g
802.11ac	5 GHz	1.3 Gpbs	802.11a, 802.11n

There are some common properties between all these standards there is also difference exist between these standards. Such as in terms of speed and speed and modulation. Whether they are backward compatible or not.

There is some difference in protocols and how the data is handled by different standards. But the attack and defense strategy will remain the same most of the time.

The 802.11 standards, will prescribe which frequencies these technologies work as well as which channel which also depends on the geographical locations. In the United States, There are 11 different channels available from 1 to 11 all are separate and they will not interfere with one another.

The wireless network can work in two different modes such as Infrastructure and Ad-Hoc.

There are some terminologies need to understand which are useful before moving forward and are related to understanding the wireless networks and communications.

SSID: Service Set Identifier is a human-readable name associated with an 802.11 wireless network. It is normally known as the network name.

BSSID: Basic Service Set Identifier uniquely identifies a specific access point and it is of the similar format as of the MAC address of the access point.

ESSID: Extended Service Set Identifier can essentially be thought of as a group of BSSID which shares the same layer of the network and same SSID.

As the wireless network doesn’t have the in-built security mechanisms. Due to which a secure layer is built on top of the wireless network protocol stack.

This is achieved by the encryption and authentication techniques such as WEP(Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access). It is very important to secure the wireless networks as it can easily be intercepted.

Let us now discuss in details regarding the attacks on the wireless networks. We will also in details regarding the steps of how to crack the wireless networks from the learning perspective which will help indirectly in how to design and implement the wireless network effectively with robust security features in an organization.

Also for the wireless network, the security comes from the selection of the security technique or the authentication method which is adopted. There are various different security technique which is available such as WEP (Wired Equivalent Privacy), WPA2(Wifi Protected Access II). WPA1 provides two different modes of operation which includes Personal or Pre-Shared Key(PSK) and Enterprise.

WEP: WEP is a very basic and original part of the 802.11 wireless standards. It provides encryption at layer 2 in an OSI layer. WEP utilizes the RC4 encryption algorithm to encrypt data and uses a shared key-system. It uses either 40 bit or 104 bit WEP key to encrypt data.

WPA2-PSK: It utilizes a shared key that is communicated to both sides access point and client before establishing a wireless connection. This key is then used for secure communication.

WPS2-Enterprise: It is also known as 802.1X which uses a RADIUS server for the authentication purpose. IT is achieved using EAP (Extensible Authentication Protocol which is defined in RFC 3748).

3.4 WIRELESS NETWORK ATTACK

Any kind of wireless network attack is vulnerable and can cause the potential business impact. We will see several classifications which are described as below:

1. **Access Control Attack:** This attack tries to penetrate the wireless network or evading the access control mechanisms.

War Driving: To discover wireless LAN network by listening to beacons using sniffing tools.

Rogue Access Point: Installing an unsecured or fake access point inside the firewall.

Ad Hoc Associations: Connecting directly to an unsecured station.

MAC Spoofing: To bypass the MAC filtering policy in access points attackers used to change the MAC address which matches to the access point MAC address whitelist. SMAC tool can help in changing the MAC address in windows.

RADIUS Cracking: RADIUS(Remote Authentication Dial In User Service) is a server which is used to authenticate client and server. This attack can be performed using a brute force attack to obtain the secret key.

2. Confidentiality Attack: In these types of attacks attackers try to intercept the private information which is sent over a wireless network.

Eavesdropping: To capture the unprotected network traffic. Attackers mostly target the public wifi where the network usually does not have strong security measures.

WEP Key Cracking: To capture the network packets to recover the WEP key using active or passive methods.

Man In The Middle Attack: Attackers will try to capture the SSL connections in wireless networks and proxy them to web page logins to conduct the phishing attack. It can successfully complete this attack by first setting up the rogue access point and try to behave like a legitimate access point.

There are several steps involved to conduct such an attack which is listed below.

1. Select and target the access point and associated clients.

2. Identify the security protocol used such as WEP/WPA2 and crack the key.

3. Configure the wireless card as a rogue access point.

4. Use Airplay-ng to send de-authentication packets to target the host to disconnect from the network.

5. The disconnected client will reconnect after scanning with the fake access point.

3. Integrity Attack: These types of attacks send the forged control and management or data frames over the wireless network to misguide them or to fulfill another attack.

Frame Injection: Specifically crafting and forging the 802.11 packets.

RADIUS Replay: To capture RADIUS accept and reject messages for later reply.

4. Authentication Attack: Attackers try to steal legitimate user identities and credentials to access private network and services.

VPN Login Craking: To get the credentials using the brute force attacks on VPN authenticated protocols.

PSK Cracking: To crack and recover the password of WPA/WPA2-PSK from captured key handshake frames using dictionary attack tools.

5. Availability Attacks: These attacks stop the delivery of wireless services to legitimate users by denying them from accessing the WLAN resources.

Beacon Flood: Generating thousands of fake beacons to make it hard for stations to find a legitimate access point.

The next point we are going to see is to see how to crack the wireless network and get the encryption key. Also, we will see the process and tools usage which are mainly present in Kali Linux operating system.

But above all, it starts from understanding the basic cryptographic algorithm before starting to break it. As it is just built by using mathematical functions.

Always under certain circumstances, weak implementation of the security mechanisms allows an attacker to reverse engineer it. It applies to the wireless network protocols too.

When a WEP encrypted packets are captured using Wireshark or any other similar tool, there is a field which is labeled as IV(Initialization Vector). Every packet has a different IV. IV is a 24-bit pseudo-random number which is there with every packet.

By passively capturing(stealth mode capture) the traffic to capture enough packets, WEP key can be cracked. As for 24-bit pseudo-random number, there are around 16 million unique IV’s, which can easily be got by capturing the busy network traffic. So there are chances that multiple packets can have the same IV’s.

Let us see the process.

1. Identify the target wireless network.

2. Passively monitor the encrypted packets between an access point and client using a sniffer tool.

3. Monitor ARP packets, as ARP packets are very small and having a unique size, also it would be easy for an attacker to reply for an ARP request and to start capturing.

4. Continue to send ARP request and get unique IV's.

5. Save around 50,000 encrypted packets to determine the WEP key.

6. Use the aircrack-ng program against the saved packets to obtain the WEP key.

(aircrack-ng tools can be found pre-installed in Kali Linux).

There are other tools which are present and used for wireless network attacks. Such as:

Airmon-ng: Bash script to enable monitor mode on a wireless interface.

Airodump-ng: Wireless packet capturing tool designed for capturing packet for aircrack-ng.

Airplay-ng: Packet Injection Tool for the wireless network to generate the traffic.

Aircrack-ng: It is a tool used for cracking key of WEP or WPA/WPA-PSK wireless network.

Various commands line utility or tools which are used for basic information gathering of wireless network which is listed below.

iwlist: Command line utility for identifying the wireless network

Kismet: Linux wireless network detection suite.

Netstumbler: Windows-based wireless network detection suite.

We have seen the basic overview of the WEP cracking, but now we will look inside each step in detail with commands. To start from identifying the NIC cards, scanning wireless networks in surroundings.

The simplest way to identify the network wireless network cards in your system is using iwconfig. It will list out all network interfaces which are present in the system.

There will be a wireless card which will be shown as *wlan0* which will support the majority of all standards from (a,b,g, and n).

Next step is to use an iwlist command which will help to gather initial information.

iwlist wlan0 scanning

This command will give information such as ESSID, channel, frequency such information will be useful in later stages.

There are several fields which will be seen in the output and use to perform the following tasks.

Encryption key: If this is set on, then the access point is using WEP encryption.

Channel: To see the current wireless channel for the specific BSSID.

Mode: If the mode is set to master, then it is an access point or else it is an Ad-Hoc Network.

Use the MAC address statically while performing such kind of testing. For cloning MAC address in Linux it is essential to bring down the interface first and to start again, this can be performed using the *ifconfig* command.

Let's begin with the process.

1. Identify the insure network using an *iwlist* command, which will consist of BSSID along with the channel.
2. Start the wireless card interface wlan0 into monitor mode using airmon-ng. For eg:

   >>airmon-ng start wlan0

   Start capturing the network traffic associated with the network using airodump-ng.

3. *>>airodump-ng –w DUMP –c <channel> --bssid <MAC Address> mon0*

   -w DUMP: It will tell airodump to name all files in output to start with DUMP*.

   -c <channel>: It tells airodump to stay connected on the channel specified, instead to jump In different channels.

   --bssid: Just capture traffic related to target bssid.

Keep the window open until we do not capture the sufficient numbers of packets. We have already seen that we need thousands of packets to gather enough number of IV to crack the WEP key.

Goto the current working directory where you will see some pcap files which can be open and view with Wireshark.

Now use aircrack-ng to see that pcap file to check how any number of packets are captured and how many numbers of unique IV are there. It will automatically tell whether we need more packets or we have enough number of the packet.

4. *>>aircrack-ng *.cap*

   If it shows “Failed”. Then try again using ARP reply attack to capture enough number of packets. As without a few thousand unique IV, we won't be able to crack the key.

5. *>>airplay-ng –arprepaly –b <MAC Address>*

   --arpreplay: Attack method.

   ARP replay attack takes time to complete the packet capturing process. Sometimes in several scenarios, if the packet capturing is not started then we have to cancel the process using CTRL-C and we have to start again.

   -b: Target MAC address.

   After some time again check with

   *>>airplay –ng *.cap*

   This will shows if the number of IV are gathered it will automatically crack the key and will show in hexadecimal form. Convert the same in ASCII format for text representation.

Now we will see about the WPA which is known as Wifi Protected Access. It has got two different versions, WPA and WPA2(802.11i).

The initial 3 steps of WEP cracking are the same for the cracking the WPA2-PSK encrypted are same but in later stages, the process becomes different which we will see below.

4. After performing the 3rd step the output will defer from what we have seen in the WEP process. Where the BSSID will show that the encryption used is WPA2 and PSK as the authentication method. Also, we can see the clients connected with the wireless network.

Now, we can wait for another client to connect with the wireless aces point or we can deauthenticate the current client and capture the WPA handshake.

Use the airplay-ng utility to deauthenticate if there is any existing client connected with the network.

5. *>>airplay-ng –deauth=5 –a <MAC Address> mon0*

-- deauth=5: To deauthenticate the client and retry it 5 times if it fails on the first time. We can set this value as per our requirement. Make a note of STMAC address in output which represents the station MAC Address which will be required in a further step.

-a: Provide target MAC Address

Now, this method will not work on a large network, this will be not in a stealthy mode which we want to be. Also broadcasting the deauthentication message will not make sure that client will reconnect to it.

Use the –c flag in the above command to make it effective.

>>airplay-ng –deauth=5 –a <MAC Address> -c <STMAC> mon0

After deauthentication of the client, it will automatically reconnect with the network and we will have the proper authentication handshake and start collecting in the pcap file. This can be seen using aircrack-ng command.

*>>aircrack-ng *.cap –w /usr/share/dict/words.*

-w: Word list can be a user-specified directory where the file is located.

Aircrack-ng checks around 1000 passwords per second. In the output, you will get the text representation of the key obtained.

Check Your Progress 1

1. List out all the commands in a sequence which is used to crack WEP encryption.

3.5 LET US SUM UP

In this chapter, we have what all kind of wireless network attacks are there. Also, we have seen how to gather initial information or how to a reconnaissance of the wireless network to crack the key. It is important to understand the commands and what it does instead of blindly entering the command in the terminal.

We have also seen the tools which can be used for a different operating system platform. Also, this does not ensure that the process mentioned will work on all environments. This can differ as per the infrastructure and network devices used. Type of the wireless network card also sometimes can create some issues related to some software or packages dependencies.

3.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

>>airmon-ng start wlan0 <channel>

>>airodump-ng -w OUT -c <channel> –bssid <MAC Address> mon0

>>aireplay-ng --arpreplay -b <MAC Address> mon0

*>>aircrack-ng *.c*

Block-3

Web Application Tools

Unit 1: Scanning For Web Vulnerabilities Tools and HTTP Utilities

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Scanning For Web Vulnerabilities Tools

1.4 HTTP Utilities

1.5 Let us sum up

1.6 Check your Progress: Possible Answers

1.7 Further Reading

1.8 Assignment

1.9 Activities

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Identify different kinds of web vulnerabilities using various tools.
- Usage of HTTP utilities.

1.2 INTRODUCTION

This block is focus to tools that aid in the analysis anddefence of the software that runs on systems and drives web applications. It explains how to use command-line and proxy tools to find vulnerabilities in web applications. Also delves into the techniques for successful, optimal password cracking.

1.3 SCANNING FOR WEB VULNERABILITIES TOOLS

Web vulnerabilities scanners are the software programs that scan web sites; generally it looks for web vulnerabilities like XSS (cross site scripting), SQL injection, file-directory listing and insecure web server configuration. This kind of software is also referred as Dynamic Application Security Testing Tools.

1.3.1 NIKTO

Nikto is a tool to find the insecure and various files, settings and programs on the web server.

When hackers or penetration testers are looking to attack a target they usually first want to compile a list of target surfaces after that they'll use a tool like Nikto to scan for vulnerabilities and discover the weakest link allowing him to spend a minimal amount of time and effort actually attacking the target.

It is examine the web server to identify potential problems, including:

- Poor server configuration settings
- Default files
- Unsafe files

Nikto is built on Perl programming Open Source platform. It includes SSL, host login authentication, proxy and many more. Nikto can be updated through command-line. Nikto is very easy to run in Windows or any Unix based operating system. In Kali

Linux it is pre-installed. You shouldn't need to install it separately. To run nikto use –h option with targeted host name or IP address in terminal to start the vulnerability scanning. The following example describes the usage of nikto tool:

```
root@kali:~# nikto -h axxxxxxxxxr.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          6x.1xx.2xx.98
+ Target Hostname:    axxxxxxxxxr.com
+ Target Port:        80
+ Start Time:         2019-04-11 10:58:06 (GMT5.5)
---------------------------------------------------------------------------
+ Server: LiteSpeed
+ Cookie PHPSESSID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME
type
+ Uncommon header 'link' found, with contents:
<https://1199.pk/index.php?rest_route=/>; rel="https://api.w.org/"
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability.
Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /old/: This might be interesting...
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory
listing.
+ OSVDB-3093: /webmail/lib/emailreader_execute_on_each_page.inc.php: This
might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ /controlpanel/: Admin login page/section found.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening
stream: can't connect (connect error): Network is unreachable
+ Scan terminated:  20 error(s) and 18 item(s) reported on remote host
+ End Time:           2019-04-11 12:01:54 (GMT5.5) (3828 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Table-1 lists the additional options to run the Nikto tool.

➢ Nikto command-line options

Following is a table

Nikto Option	Description
-config+	Use this config file

-Display+	Turn on/off display outputs
-dbcheck	Check database and other key files for syntax errors
-Format+	Save file (-o) format
-Help	Extended help information
-host+	Target host
-id+	Host authentication to use, format is id:pass or id:pass:realm
-list-plugins	List all available plugins
-output+	Write output to this file
-nossl	Disables using SSL
-no404	Disables 404 checks
-Plugins+	List of plugins to run (default: ALL)
-port+	Port to use (default 80)
-root+	Prepend root value to all requests, format is /directory
-ssl	Force ssl mode on port
-Tuning+	Scan tuning
-timeout+	Timeout for requests (default 10 seconds)
-update	Update databases and plugins from CIRT.net
-Version	Print plugin and database versions
-vhost+	Virtual host (for Host header)
	+ requires a value

Table-1 Nikto command-line options

1.3.2 W3AF

W3AF is the acronym of Web Application Attack and Audit Framework. This framework is to find the web application vulnerabilities like SQL injection, XSS and many more.

W3AF is built on Open Source community for Web Application Exploitation Framework. It also provides information about web app vulnerability and supports to pen-testing. W3AF is available for almost all operating system like Linux, MAC OS, and Windows etc. It is developed in python programming language and support for both CUI as well as GUI environment.

Before executing W3AF users should to know the basics and workflow. This will helps to user for getting better idea in the process of identifying web app vulnerabilities.

In W3AF there are main three plugin types which are as follows:

- Crawl
- Audit
- Attack

Crawl plugin

This plugin will finding only URLs in which the injection points occurs. Input for this plugin is the URL and it will provide one or more injection points.

Audit plugin

It takes the input as injection point found by crawl and identifies the web app vulnerability like SQL injection.

Attack plugin

This is to exploit the vulnerabilities found by audit. They generally return a dump of table on remote server if it is SQL injection vulnerability.

There are other plugins available in W3AF like: Infrastructure, Grep, Output, Mangle, Bruteforce, and Evasion.

How to Run W3AF

As described earlier, W3AF have CUI as well as GUI environment. For the command line execute:

```
$ ./w3f_console
w3af>>>
```

From this point you will be able to execute the various commands of W3AF.

```
w3af>>> help
|-------------------------------------------------------------- |
| start          | Start the scan.                              |
| plugins        | Enable and configure plugins.                |
| exploit        | Exploit the vulnerability.                   |
| profiles       | List and use scan profiles.                  |
| cleanup        | Cleanup before starting a new scan.          |
|-------------------------------------------------------------- |
| help           | Display help. Issuing: help [command] , prints |
|                | more specific help about "command"           |
| version        | Show w3af version information.               |
| keys           | Display key shortcuts.                       |
|-------------------------------------------------------------- |
| http-settings  | Configure the HTTP settings of the framework.  |
| misc-settings  | Configure w3af misc settings.                |
| target         | Configure the target URL. |
|-------------------------------------------------------------- |
| back           | Go to the previous menu.                     |
| exit           | Exit w3af.                                   |
|-------------------------------------------------------------- |
| kb             | Browse the vulnerabilities stored in the     |
|                | Knowledge Base                               |
|-------------------------------------------------------------- |
w3af>>>
w3af>>> help target
Configure the target URL.
w3af>>>
```

To get into configuration menu, just enter its name and press enter, you can see how prompt will change according to your context menu.

```
w3af>>> http-settings
w3af/config:http-settings>>>
```

Every configuration menus have following commands:

- Help
- View
- Set
- Back

Usage of these commands in http-settings menu as following:

```
w3af/config:http-settings>>> help
|-------------------------------------------------------------- |
| view     | List the available options and their values.      |
| set      | Set a parameter value.                            |
| save     | Save the configured settings.                     |
|-------------------------------------------------------------- |
```

```
| back     | Go to the previous menu.                                |
| exit     | Exit w3af.                                              |
|-------------------------------------------------------------------|
w3af/config:http-settings>>> view
|-------------------------------------------------------------------|
| Setting        | Value    | Description                          |
|-------------------------------------------------------------------|
| url_parameter  |     | Append the given URL parameter to
                 everyaccessed URL. |

...
|-------------------------------------------------------------------|
| basic_auth_user | | Set the basic authentication username for HTTP
requests |
| basic_auth_passwd | | Set the basic authentication password for
HTTPrequests |
| basic_auth_domain | | Set the basic authentication domain for HTTP
requests |
|-------------------------------------------------------------------|
w3af/config:http-settings>>> set timeout 5
w3af/config:http-settings>>> save
w3af/config:http-settings>>>back
w3af>>>
```

As shown in above example, the view command will display all the configurable arguments, with their possible values and description. The set command will change the value of argument. The save command will perform the commit operation over the changes in argument's value. Lastly back command will exit from current menu context.

Plugins can be configured using following commands:

```
w3af>>> plugins
w3af/plugins>>> help
|-------------------------------------------------------------------|
| list           |List available plugins.                           |
|-------------------------------------------------------------------|
| back           |Go to the previous menu.                          |
| exit           |Exit w3af.                                        |
|-------------------------------------------------------------------|
| output         |View, configure and enable output plugins         |
| audit          |View, configure and enable audit plugins          |
| crawl          |View, configure and enable crawl plugins          |
| bruteforce     |View, configure and enable bruteforce plugins     |
| grep           |View, configure and enable grep plugins           |
| evasion        |View, configure and enable evasion plugins        |
| infrastructure |View, configure and enable infrastructure         |
|                |plugins                                           |
| auth           |View, configure and enable auth plugins           |
| mangle         |View, configure and enable mangle plugins         |
|-------------------------------------------------------------------|
```

```
w3af/plugins>>>
```

You can list all the plugins by providing plugin name as following command:

```
w3af>>> plugins
w3af/plugins>>> list audit
|-------------------------------------------------------------------|
| Plugin name    | Status   | Conf     | Description                |
|-------------------------------------------------------------------|
| blind_sqli     |          | Yes      | Identify blind SQL         |
|                |          |          | injection vulnerabilities |
...
w3af/plugins>>>
```

To turn on the XSS and SQLI plugins, we have to apply the following command:

```
w3af/plugins>>> audit xss, sqli
w3af/plugins>>> audit
|-------------------------------------------------------------------|
| Plugin name    | Status   |Conf | Description                    |
|-------------------------------------------------------------------|
| sqli           | Enabled  |     | Find SQL injection bugs.       |
...
| xss            | Enabled  | Yes | Identify cross site scripting  |
|                |          |     | vulnerabilities.               |
...
w3af/plugins>>>
```

To start the scan, we should apply the following command:

```
w3af>>> target
w3af/config:target>>> set target http://localhost/
w3af/config:target>>> back
w3af>>> start
```

1.4HTTP UTILITIES

The following tools are used to perform connections over HTTP or HTTPS. Basically they are not supposed to find any vulnerability, but its functionality can be extends the supports towards the vulnerability scanner.

1.4.1 CURL

Transferring data from one place to another is one the main task done using computers connected to a network. There are so many GUI tools out there to send and receive data, but when you are working on a console, only equipped with command line functionality, using CURL is inevitable.

A less known fact is that CURL can work with a wide range of protocols and can solve most of your scripting tasks with ease.

CURL: CURL is an easy to use command line tool to send and receive files, and it supports almost all major protocols(DICT, FILE, FTP, FTPS, HTTP, HTTPS, LDAP, POP3, SMTP and many more) in use.

Features of CURL:

- Can be used inside your shell scripts with ease
- Supports features like pause and resume of downloads
- It has around 120 command line options for various tasks
- It runs on all major operating systems
- Supports cookies, forms and SSL
- Both CURL command line tool and libcurl library are open source, so they can be used in any of your programs
- It supports configuration files
- Multiple upload with a single command
- Progress bar, rate limiting, and download time details
- Ipv6 support

Table-2 lists the additional options of the CURL utility.

➢ CURL command-line options

Following is a table

Usage: curl [options...] <url>

CURL Option	Description
-b, --cookie <data>	Send cookies from string/file
-d, --data <data>	HTTP POST data

-G, --get	Put the post data in the URL and use GET
-I, --head	Show document info only
-H, --header <header/@file>	Pass custom header(s) to server
-0, --http1.0	Use HTTP 1.0
--http1.1	Use HTTP 1.1
--http2	Use HTTP 2
-i, --include	Include protocol response headers in the output
-4, --ipv4	Resolve names to IPv4 addresses
-6, --ipv6	Resolve names to IPv6 addresses
-l, --list-only	List only mode
-o, --output <file>	Write to file instead of stdout
-x, --proxy [protocol://]host[:port]	Use this proxy
-U, --proxy-user <user:password>	Proxy user and password
-B, --use-ascii	Use ASCII/text transfer
-u, --user <user:password>	Server user and password
-A, --user-agent <name>	Send User-Agent <name> to server
-v, --verbose	Make the operation more talkative
-V, --version	Show version number and quit

Table-2CURL command-line options

1.4.2 OpenSSL

OpenSSL is free security protocol and putting into use library given by Free Software community. OpenSSL libraries are used by a lot of businesses/projects in their systems and products. OpenSSL libraries and sets of computer instructions can be used with openssl command. It is the most common library for establishing the encrypted connection.

The S represents in HTTPS connection that uses Secure Socket Layer for transport data. Encrypted connections in web are often uses the HTTPS connection but it provides limited security. The Secure Socket Layer and Transport Layer Security protocol offer security from reading a plaintext data points between sender and receiver.

How to use OpenSSL

To check the version of OpenSSL following command will be used:

```
root@kali:~# openssl version
OpenSSL 1.1.0h 27 Mar 2018
root@kali:~#
```

To see the list of available common cipher standards

```
root@kali:~# openssl list -cipher-commands

aes-128-cbc       aes-128-ecb       aes-192-cbc       aes-192-ecb
aes-256-cbc       aes-256-ecb       base64            bf
bf-cbc            bf-cfb            bf-ecb            bf-ofb
camellia-128-cbc  camellia-128-ecb  camellia-192-cbc  camellia-192-
ecb
camellia-256-cbc  camellia-256-ecb  cast              cast-cbc
cast5-cbc         cast5-cfb         cast5-ecb         cast5-ofb
des               des-cbc           des-cfb           des-ecb
des-ede           des-ede-cbc       des-ede-cfb       des-ede-ofb
des-ede3          des-ede3-cbc      des-ede3-cfb      des-ede3-ofb
des-ofb           des3              desx              rc2
rc2-40-cbc        rc2-64-cbc        rc2-cbc           rc2-cfb
rc2-ecb           rc2-ofb           rc4               rc4-40
seed              seed-cbc          seed-cfb          seed-ecb
seed-ofb
root@kali:~#
```

We can use a listed above symmetric encryption cipher commands in OpenSSL.

Let’s see how it works in terminal.

First of all create one plaintext file using nano command and provide a name like *msg*.

```
root@kali:~# openssl enc -aes-256-cbc -base64 -in msg -out enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
root@kali:~# cat enc
U2FsdGVkX1/u76rxzLD9wtLgM2J3Ps8K7/FjMroOszzEQ/bMyQgUvu+Lxsn0F3fT
root@kali:~#
```

Above listed command is used for encryption of plaintext file named *msg* which is mentioned with *–in msg* parameter. *enc* specify the encryption using *–aes-256-cbc* cipher command with *–base64* parameter. Finally the encrypted file is transformed using *–out enc* parameter.

It will ask for the encryption password while cipher the plaintext file. It asks for retyping the password for verifying process.

Now, for decryption of file we have to use some commands like as shown below:

```
root@kali:~#openssl enc -aes-256-cbc -d -base64 -in enc -out dec
enter aes-256-cbc decryption password:
root@kali:~# cat dec
hi this is demo of OpenSSL
root@kali:~#
```

As illustrate in above *–d* parameter is used for decryption with *–base64* parameter and decrypted file will transform into plaintext file named with *dec* using *–out* parameter in the example.

1.4.3 STunnel

It is a program to provide encryption between client and remote server. It runs on cross platform operating system. You could also encrypt any type of network

communication so for instance you could encrypt unencrypted messages with Stunnel.So they're encrypted send it across the network and send it to another Stunnel program running in server mode and it will accept that secure communication and then forward it on to the service that wants it.

If you want to bypass a firewall or intrusion prevention system so you wanted to hide essentially your malware or your bad programs or your information by encrypting it. Using Stunnel you can bypass any types of detection scheme by the administration on that network would not be able to see what you are doing cause of sending encrypted traffic across the network.

There are two ways to pass encrypted message to the server over the network through Stunnel, one is to any secure service like https, pop3, imap4 and another way is to any non-secure service like http. To pass the encrypted message to any non-secure service you could use another Stunnel program situated at server side.

Any secure communications over the network rely on certificates. Firstly you required a proper PEM file which includes encryption key for communications. Stunnel has a default file named as stunnel.pem.

What is Tunneling

It means that program (daemon) runs on the client as well as server machine. For example, the Windows 2000 PC is the client and server is any *NIX machine. So, Stunnel will then execute as client on Windows and the server mod on UNIX machine.

e.g.

```
Windows:
stunnel –d 5800 –r unix_ip_address:5800 –c

UNIX:
stunnel –d 5800 –r 5801
```

As above illustrated in above example –d indicate Stunnel program execute in daemon mode on port 5800; -r indicate that remote host machine; -c indicate that client mode.

The following is the short version of configuration file avail by default. This example of file will demonstrate the use TLS client mode service like pop3, imap, smtp.

```
; Sample stunnel configuration file for Unix by Michal Trojnara
1998-2019
; Some options used here may be inadequate for your particular
configuration
; This sample file does *not* represent stunnel.conf defaults
; Please consult the manual for detailed description of available
options

; ******************************************************************
; * Global options                          ;
*******************************************************************
; It is recommended to drop root privileges if stunnel is started by
root
;setuid = nobody
;setgid = nogroup

; PID file is created inside the chroot jail (if enabled)
;pid = /usr/local/var/run/stunnel.pid
;
;
[gmail-pop3]
client = yes
accept = 127.0.0.1:110
connect = pop.gmail.com:995
verifyChain = yes
CApath = /etc/ssl/certs
checkHost = pop.gmail.com
OCSPaia = yes

[gmail-imap]
client = yes
accept = 127.0.0.1:143
connect = imap.gmail.com:993
verifyChain = yes
```

```
CApath = /etc/ssl/certs
checkHost = imap.gmail.com
OCSPaia = yes

[gmail-smtp]
client = yes
accept = 127.0.0.1:25
connect = smtp.gmail.com:465
verifyChain = yes
CApath = /etc/ssl/certs
checkHost = smtp.gmail.com
OCSPaia = yes
```

Check your Progress 1:

1. What is Nikto in Cyber Security?
2. W3AF stands for _____
3. What is the use of curl command?
4. Define OpenSSL
5. How STunnel works?

1.5LET US SUM UP

This block covers the various Web Application Tools for Pentesting as well as to find the web vulnerabilities. Using this student can learn the basic concepts of Nikto, W3AF, OpenSSL, etc.

1.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check your Progress 1:

1. The Nikto web server scanner is a security tool that will test a web site for thousands of possible security issues. Including dangerous files, mis-configured services, vulnerable scripts and other issues. It is open source and structured with plugins that extend the capabilities.

2. W3AF stands for Web Application Attack and Audit Framework.
3. The curl command transfers data to or from a network server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP or FILE). It is designed to work without user interaction, so it is ideal for use in a shell script.
4. OpenSSL is a software library for applications that secure communications over computer networks against eavesdropping or need to identify the party at the other end. It is widely used by Internet servers, including the majority of HTTPS websites.
5. STunnel works by listening on another port and then redirecting that traffic through to the unsecured port.

1.7 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer “Anti-Hacker Toolkit By Mike Shema”

1.8ASSIGNMENTS

- How to useW3AF?

1.9ACTIVITIES

- Perform Curl command on various protocol.

Unit 2: Application Inspection Tools

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Application Inspection Tools

2.4 Let us sum up

2.5 Check your Progress: Possible Answers

2.6 Further Reading

2.7 Assignment

2.8 Activities

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Identify different kinds of web vulnerabilities using various tools.
- Web app tools for inspection like ZAP, SQLMap, etc..

2.2 INTRODUCTION

This section covers tools that assist with the manual analysis of and interaction with web application. For this section we care much less about whether the application isrunning on Apache or IIS, or whether the source code is Ruby or Java. Knowing thosedetails informs and influences some of the attacks that we might try against the webapplication, but in this section we care more about how the web application handlescookie values, or how it responds to different values for a URL parameter, or whatkinds of data it accepts from a form submission.

2.3APPLICATION INSPECTION TOOLS

The previous utilities in this chapter focused on support to find vulnerabilities over the web application through the script or some legitimate code.

This section will covers the tool which identifies the SQL injection, logic flaws, XSS attack and many more. Also it focused on manual analysis of web application as well as traffic analysis over the web.

2.3.1 Zed Attack Proxy

Zed Attack Proxy (ZAP) is an open source program or tool offered by OWASP (Open Web Application Security Project) for pen testing and discovers the vulnerabilities available in your web application or website.

ZAP provides to detect following kind of threats:

- SQL Injection
- Session management

- XSS
- Broken Access Control
- Security loophole in configuration file
- Sensitive data leak
- Inadequate protection
- Unsecure APIs
- Known vulnerabilities

ZAP provides various features as shown below:

- Active Scan

  This is to discover known vulnerabilities against targeted attack.

- Alert

  An alert is the prospective vulnerabilities with specified request. It has more than one alerted on per request.

  Alert have following risk like:

  - High
  - Medium
  - Low
  - Informational
  - False Positive

  It can be raised by ZAP components.

- API

  Application Programming Interface (API) provides the functionality to configure ZAP programmatically. It supports HTML, XML and JSON formats.

- Authentication

  ZAP handles various types of authentication that is used in web application like, Manual Authentication, Form Based Authentication, HTTP Authentication and Script Based Authentication.

- HTTP Session
  Generally session is used to track the website. In ZAP, user can switch the user sessions on a website to create a new session instead of destroying the existing ones.

- Modes
  ZAP has following modes:
  - Safe: not dangerous
  - Protected: potentially dangerous actions in URL
  - Standard: you can do anything
  - Attack: new nodes are actively scanned while it discovered.

- MitM Proxy
  MitM stands for Man-In-The-Middle proxy who allows you to check all the incoming requests and outgoing responses from the web application.

- Session Management
  ZAP handles various kind of session management which will be used by website or web applications. It covers, Cookie based as well as HTTP authentication based session management.

- Tags
  It is a short information text which is associated with all requests. It can be manage by Manage Tags dialog.

The ZAP is installed by default in Kali Linux and the ZAP UI contains following elements:

(1) Menu Bar: Provide the various menus to perform the action on various tools.
(2) Standard Toolbar: This provides the button for easy access of tools.
(3) Treeview: It displays the websites tree and default context.
(4) Workarea: This displays the various tabs like Quick Start, Request and Response, also allows editing the scripts.

(5) Information view: In this section you can see tabs like History, Search, Alerts and Output.

(6) Footer: In this section you can see the status of Alert such as High, Medium, and Low etc.

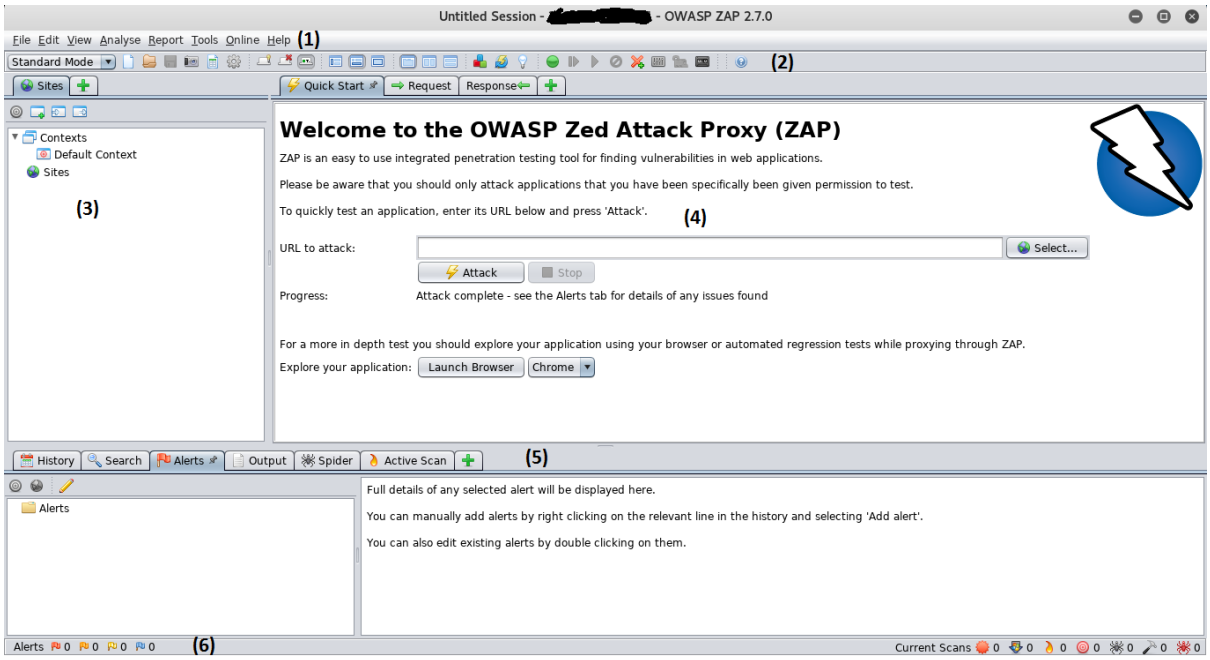


Figure 2.3.1 The ZAP UI

How to run Quick Start Scan

To run quick start scan:

(1) Start the ZAP and select Quick Start tab.

(2) In the URL to attack entry field, enter the URL or browse the URL by click on Select button.

(3) Click on Attack button.

The ZAP will process with its web crawler and scan each page of the web application or website. Then ZAP will perform the active scanner for attack on all the discovered web pages.

2.3.2 SQLMAP

It is an open source pentesting tool that automates detects and exploits the SQL injection vulnerabilities. Basically SQLMap is pre-installed in Kali Linux and operated through command line. It finds and identifies website that have vulnerable code.

Features

- It support for all known database management system like Oracle, MySQL, MSSQL, MSAccess, PostgreSQL, SQLite, Sybase.
- It support for SQL Injection techniques.
- It can directly connect with database by providing credentials.
- It supports to discover users, passwords, databases, tables, columns, roles.
- It supports to crack the password using dictionary based attack.
- It can back up the whole or partial database.
- It can upload and download the file from db server in specific database like MySQL, MSSQL, PostgreSQL.

Example

There is a website or web application which has vulnerable url like this:

```
http://www.web-site.com/example.php?id=21
```

Above listed url is prone to sql injection due to the lacking of escape the parameter id. It is simply checked by trying to open the url

```
http://www.web-site.com/example.php?id=21’
```

By adding single quotation mark in the parameter, If it throws an error or behave unexpectedly then it indicates that unexpected single quote not manage properly. So it specifies the “id” parameter is vulnerable to sql injection.

How to use SQLMap?

The sqlmap command is run using python interpreter.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21”
```

Above command will execute the sqlmap tool. Here is how the output might look

```
[*] starting at 12:10:33

[12:10:33] [INFO] resuming back-end DBMS 'mysql'
[12:10:34] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0
HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=21 AND (SELECT 1489 FROM(SELECT
COUNT(*),CONCAT(0x3a73776c3a,(SELECT (CASE WHEN (1489=1489) THEN 1
ELSE 0 END)),0x3a7a76653a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
---
[12:10:37] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
```

The output shows the operating system, database and web server with version information.

Once you identify that url is vulnerable for sql injection and its exploitable the further steps to discover the database. The –dbs option is to get the list of database list.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
dbs
```

After getting the list of database you can find the list of tables resides in particular database. The -- tables option is used to get the list of tables inside specified database using -D option.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
tables –D dbsample
```

After executing this command you will find the list of tables inside dbsample database.

Now it’s time to get columns of a table named “users” using -T option.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
columns –D dbsample –T users
```

Finally get the data from table using --dump option.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
dump –D dbsample –T users
```

2.3.3 DAMN VULNERABLE WEB APP (DVWA)

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.

Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

Before starting it must be ensure that the testing of DVWA should be done on an isolated host with either VMWare of Virtual Box, separated by a Host-only connection.

Some of the known vulnerabilities which DVWA contains as follows:

- Brute Force: HTTP Form Brute Force login page; used to test password brute force tools and show the insecurity of weak passwords.
- Command Execution: Executes commands on the underlying operatingsystem.
- Cross Site Request Forgery (CSRF): Enables an ‘attacker’ to change theapplications admin password.

- File Inclusion: Allows an ‘attacker’ to include remote/local files into the web application.
- SQL Injection: Enables an ‘attacker’ to inject SQL statements into an HTTPform input box. DVWA includes Blind and Error based SQL injection.
- Insecure File Upload: Allows an ‘attacker’ to upload malicious files on to the web server.
- Cross Site Scripting (XSS): An ‘attacker’ can inject their own scripts into theweb application/database. DVWA includes Reflected and Stored XSS.
- Easter eggs: Full path Disclosure, Authentication bypass and some others.

WARNING: THIS IS FOR EDUCATIONAL PURPOSES ONLY!

- Firstly install Xampp for windows. Then start the Xampp Control Panel from your desktop or from tray icon. Finally, start the MySQL and Apache services.
- Unpack the DVWA compressed folder into this location C:\xampp\htdocs\ dvwa.
- Now open your web-browser and type “localhost/dvwa” into the address bar. If any error occurs, this means that your PHP is not configured properly.
- Go to the web-browser and type “localhost/dvwa/setup.php” and click on “Create Database” button. Then go to “localhost/dvwa/login.php” and provide the credential ‘admin’ as username and ‘password’ as password.

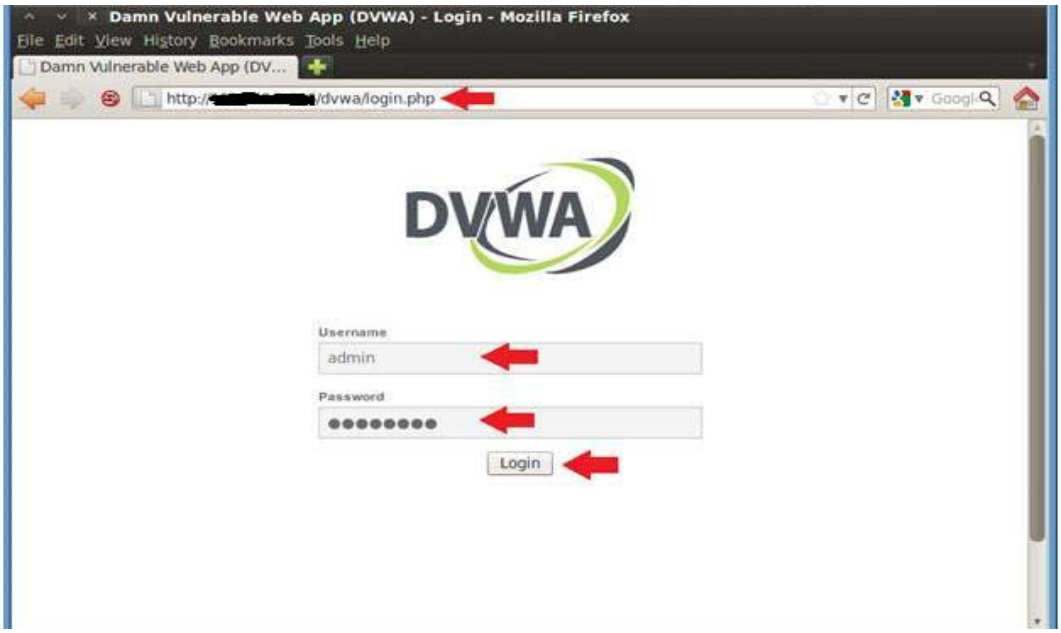


Fig. DVWA Login

- Set the DVWA Security Level Low in “Script Security” as shown in following figure.

DVWA Security

It can be divided further into two parts, one is the security level and other is PHP IDS.

The security levels are named low, medium and high. By default the security level is set to high.

- High - It is used to comparethe vulnerable source code to the secure source code.
- Medium - This security level is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure anapplication.
- Low - This security level is completely vulnerable and has no security at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learnbasic exploitation techniques.

PHP-IDS is a popular PHP Intrusion Detection System (IDS) also known as a WebApplication Firewall (WAF). PHP-IDS works by filtering any user supplied inputagainst a blacklist of potentially malicious code. PHP-IDS is used in DVWA to serveas a live example of how WAFs can help improve security in web applications.

2.3.4 WEBGOAT

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. You can install and practice with WebGoat.In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat applications.

It includes numerous exercises for topics ranging from Injection Flaws, over Cross-Site Scripting (XSS) to Denial of Service and many others.

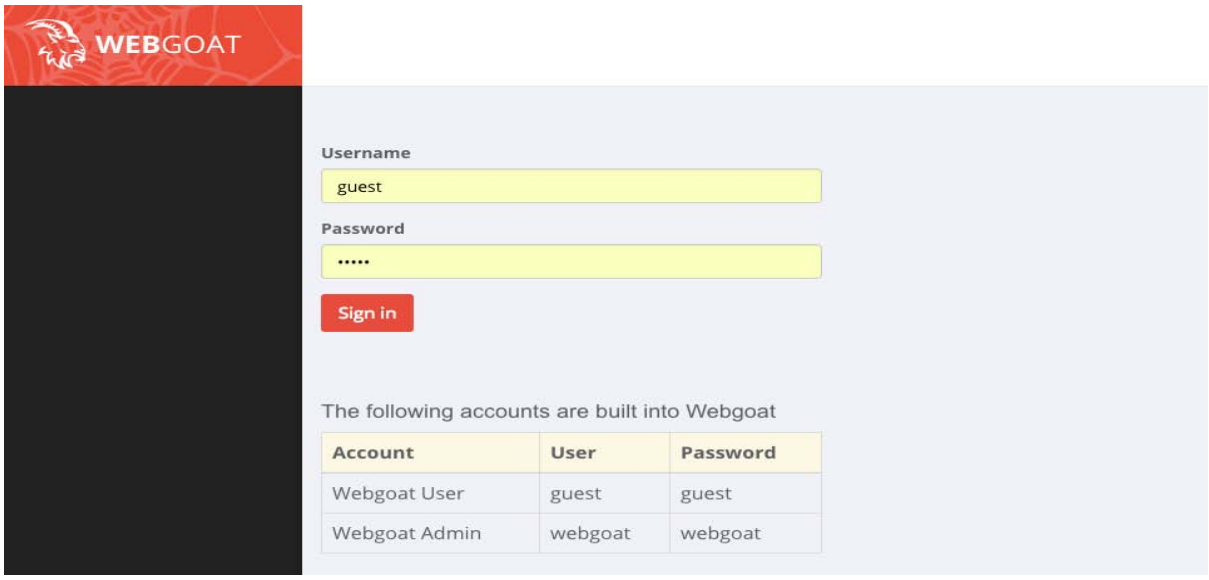
In the command-line of your liking, navigate to the location of the webgoat-container-7.1-exec.jar and start it:

java -jar webgoat-container-7.1-exec.jar

This will start a Webserver on port 8080. You can access it via http://localhost:8080/WebGoat/

Login in Webgoat

First, we log in using the guest account.

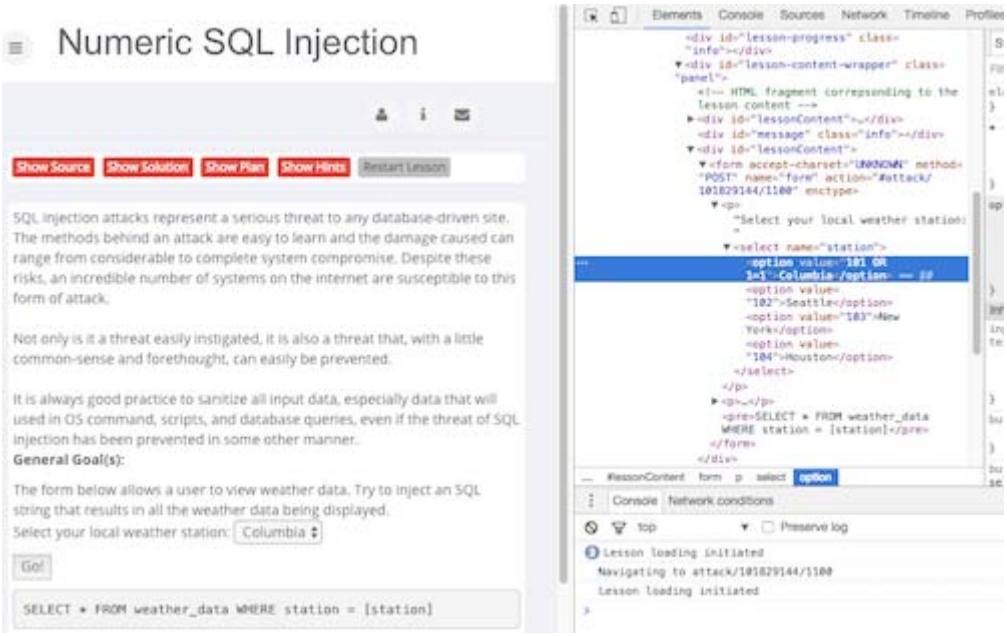


Then, we can have a look at the Tutorial with lots of helpful tips on how to get started with the WebGoat.

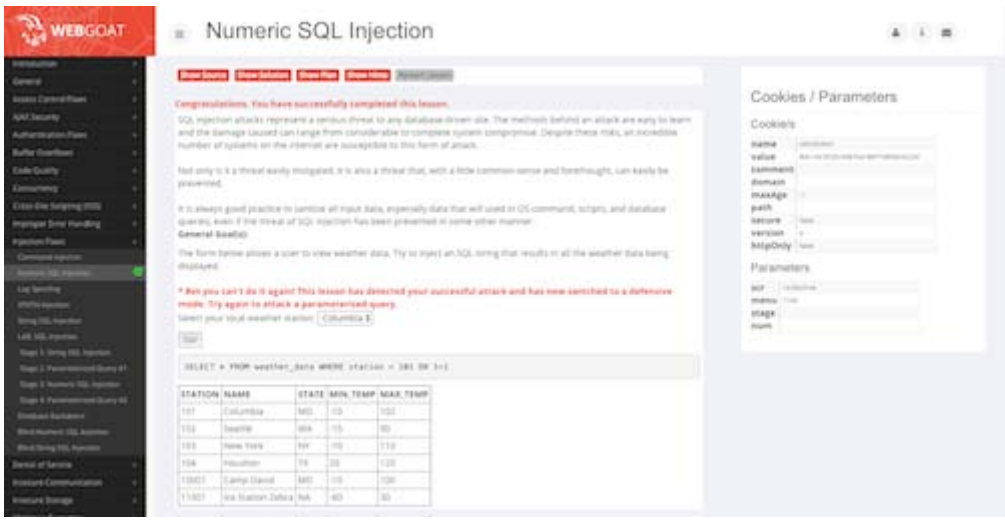
Alright, it's time for our first challenge! We will navigate to Injection Flaws and select the second entry Numeric SQL Injection from the slideout menu.

This is a nice exercise to get started. Our goal is to send a malicious query to the server, which will get it to return all the results instead of just one.

One possible solution to the Numeric SQL Injection exercise is to just open your browser dev-tools and change the value of the first option within the select field to 101 OR 1=1.



This will send the query SELECT * FROM weather_data WHERE station = 101 OR 1=1 to the server, which is always true, hence returning all the stations.



Learning the basic techniques necessary to secure web applications is absolutely essential for professional web developers. The OWASP project and especially the WebGoat are great resources for doing exactly that. Especially in the field of web security, learning how to hack can be greatly beneficial for anyone aspiring to improve their skills in web security.

Check Your Progress 1:

1. What is ZAP?
2. What is DVWA?
3. Define SQLMap
4. Describe WebGoat.

2.4LET US SUM UP

This block covers the various Web Application Tools for Pentesting as well as to find the web vulnerabilities. Using this student can learn the basic concepts of application tools such as Zed Attack Proxy, SQLMap, DVWA, WebGoat.

2.5CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. Zed Attack Proxy (ZAP) is a premier example of an interactive proxy. An interactive proxy provides the means to inspect, alter, and manipulate web traffic in order to probea web application for the presence of vulnerabilities.
2. DVWA is a DAMM VULNERABLE WEB APP coded in PHP/MYSQL. Using this app security professional, ethical hackers test their skills and run this tool in a legal environment.
3. SQLMap is an open source software that is used to detect and exploit database vulnerabilities and provides options for injecting malicious codes into them. It is a penetration testing tool that automates the process of detecting and exploiting SQL injection flaws providing its user interface in the terminal.
4. WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. This program is a demonstration of common server-side application flaws.

2.6 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer “Anti-Hacker Toolkit By Mike Shema”.

To get WebGoat: https://webgoat.github.io/WebGoat/

2.7ASSIGNMENTS

- How to get password or credential of a website using SQLMap?

2.8ACTIVITIES

- Perform DVWA Setup

Unit 3: Password Cracking and Brute-Force Tools

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Password Cracking and Brute-Force Tools

3.4 Let us sum up

3.5 Check your Progress: Possible Answers

3.6 Further Reading

3.7 Assignment

3.8 Activities

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Crack the password using tools and penetration into the system.
- Usage of brute-force tools

3.2 INTRODUCTION

This block is focus to discuss password and user account exploitation is one of largest issues in network security. In this section we will look at password cracking: the how and why of it. We will look at just how easy it is to penetrate a network, how attackers get in, the tools they use, and ways to combat it.

3.3PASSWORD CRACKING AND BRUTE-FORCE TOOLS

In general an attacker has two choices when trying to ascertain a password:

- Obtain a copy of the plaintext password or its encrypted hash and then use brute-force tools to guess what password produced the hash.
- Target a login prompt and try to guess a password.

Password cracking is an old technique that is successful mostly because humans arenot very good random-sequence generators.

A Brute-force technique is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute-force) rather than employing intellectual strategies.

3.3.1 JOHN THE RIPPER

John the Ripper is one of the speedy password cracker, presently for many known operating systems like Windows, Unix, Mac, etc. Basically its main objective is to discover weak password in operating system.

John the Ripper autodetects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match.

It also includes its own wordlists of common passwords for 20+ languages. These wordlists provide John the Ripper with thousands of possible passwords from which it can generate the corresponding hash values to make a high value guess of the target password. Since most people choose easy-to-remember passwords, It is often very effective even with its out-of-the-box wordlists of passwords.

What is John the Ripper Used for?

It is primarily a password cracker used during pentesting exercises that can help IT staff spot weak passwords and poor password policies.

Here is the list of encryption technologies found in John the Ripper:

- UNIX crypt(3)
- Traditional DES-based
- “bigcrypt”
- BSDI extended DES-based
- FreeBSD MD5-based (linux and Cisco IOS)
- OpenBSD Blowfish-based
- Kerberos/AFS
- Windows LM (DES-based)
- DES-based tripcodes
- SHA-crypt hashes (newer versions of Fedora and Ubuntu)
- SHA-crypt and SUNMD5 hashes (Solaris)

How to Download John the Ripper

It is an open-source project, so you can download and compile the source on your own, download the executable binaries, or find it as part of a penetration testing package.

The official website for John the Ripper is on https://www.openwall.com/john/. You can grab the source code and binaries there, and you can join the GitHub to contribute to the project.

John the Ripper is available on Kali Linux as part of their password cracking metapackages.

Cracking Password

John the Ripper's primary modes to crack passwords are single crack mode, wordlist mode, and incremental.

The *single crack mode* is the fastest and best mode if you have a full password file to crack.

The *wordlist mode* compares the hash to a known list of potential password matches.

The *incremental mode* is the most powerful and possibly won't complete. This is your classic brute force mode that tries every possible character combination until you have a possible result.

The easiest way to try cracking a password is to let John the Ripper go through a series of common cracking modes. This command below tells it to try "simple" mode, then the default wordlists containing likely passwords, and then "incremental" mode.

```
.\john.exe passwordfile
```

You can also download different wordlists from the Internet, and you can create your own new wordlists for John the Ripper to use with the –wordlist parameter.

```
.\john.exe passwordfile–wordlist=”wordlist.txt”
```

If you want to specify a cracking mode use the exact parameter for the mode.

```
.\john.exe --single passwordfile
.\john.exe --incremental passwordfile
```

When you want to see the list of passwords that you have cracked, use the –show parameter.

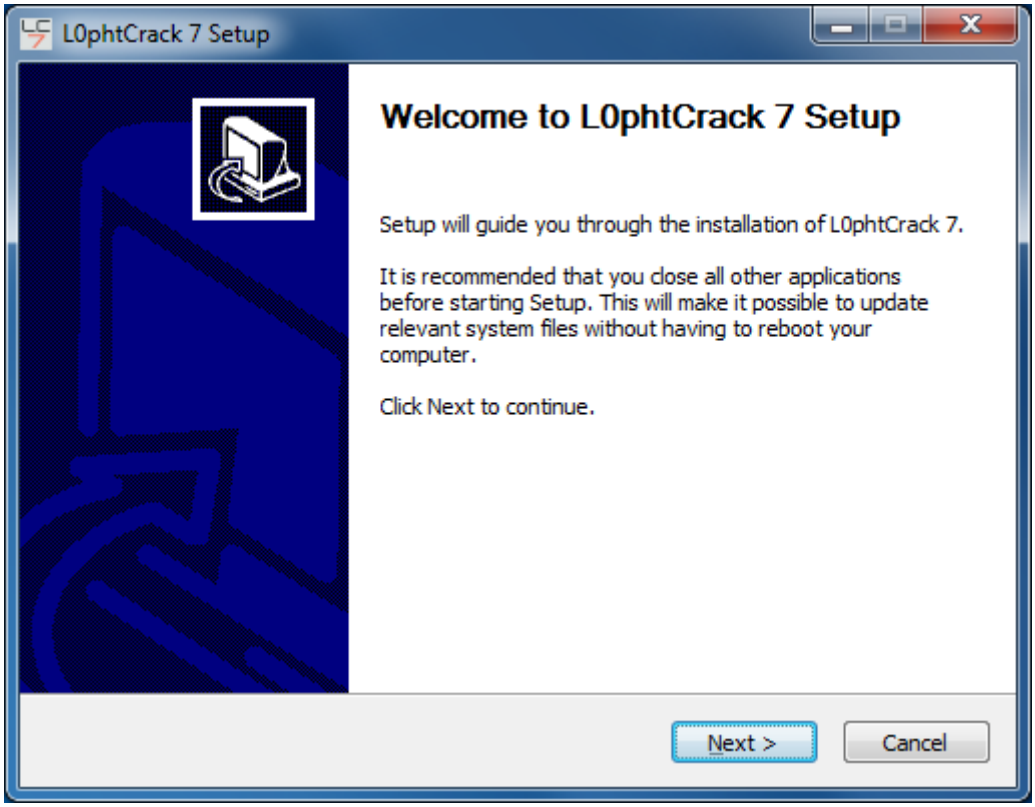
```
.\john.exe –show passwordfile
```

3.3.2 L0PHTCRACK

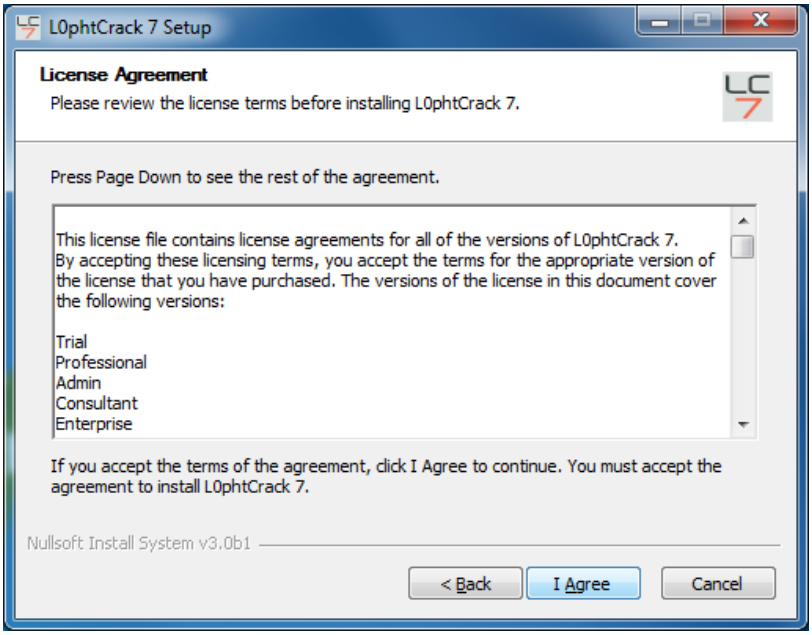
L0phtCrack is known as best windows password auditing tool. It can be used by network/system administrator for auditing weak passwords and can also help a hacker to recover password from password hashes.

To install L0phtCrack 7:

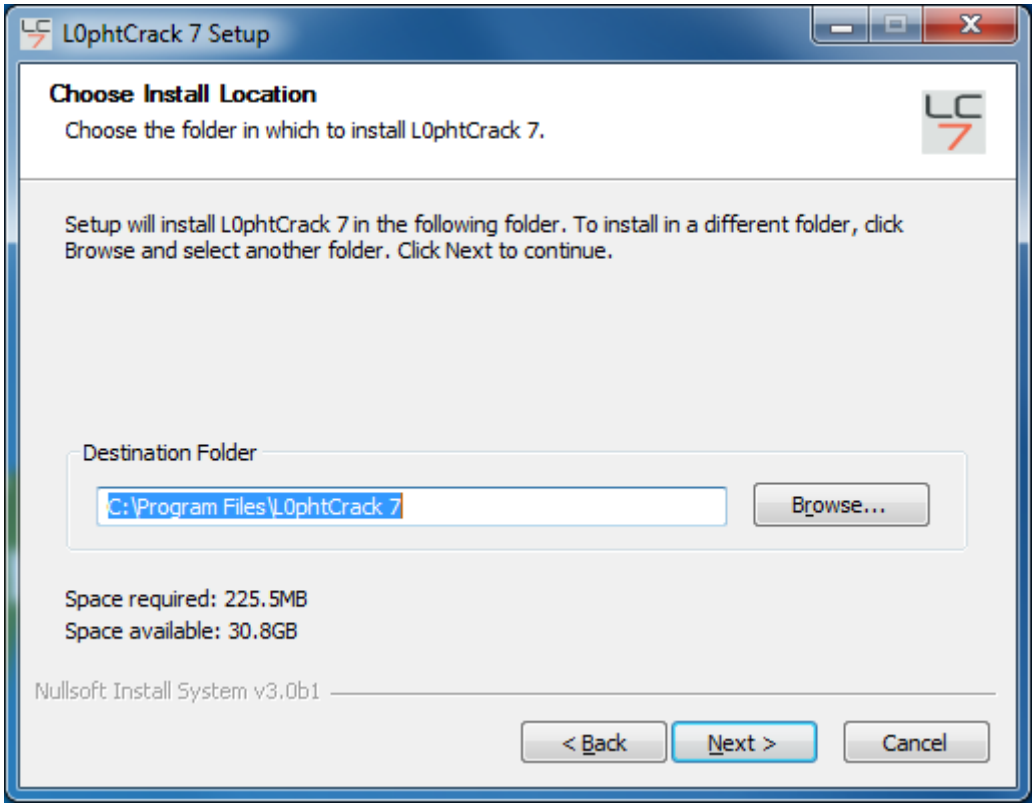
1. L0phtCrack 7 is distributed in a self-installing executable distribution file that can be downloaded for free at http://www.l0phtcrack.com/download.html.
2. Save the .exe file to your download directory.
3. In the download directory, double click the lc7setup.exe file. The installer starts a standard installation process. At the Welcome screen, click Next.



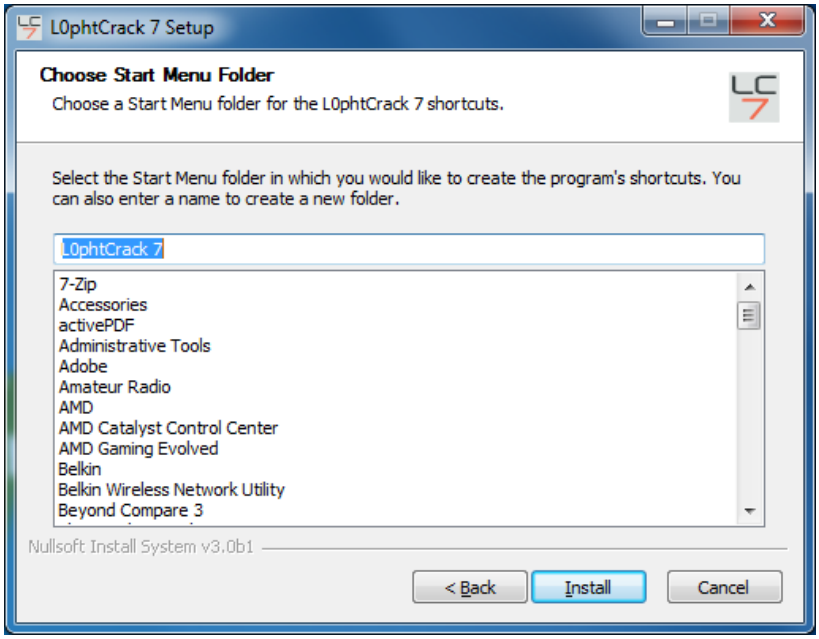
4. Read the License Agreement screen, then click I Agree to agree.



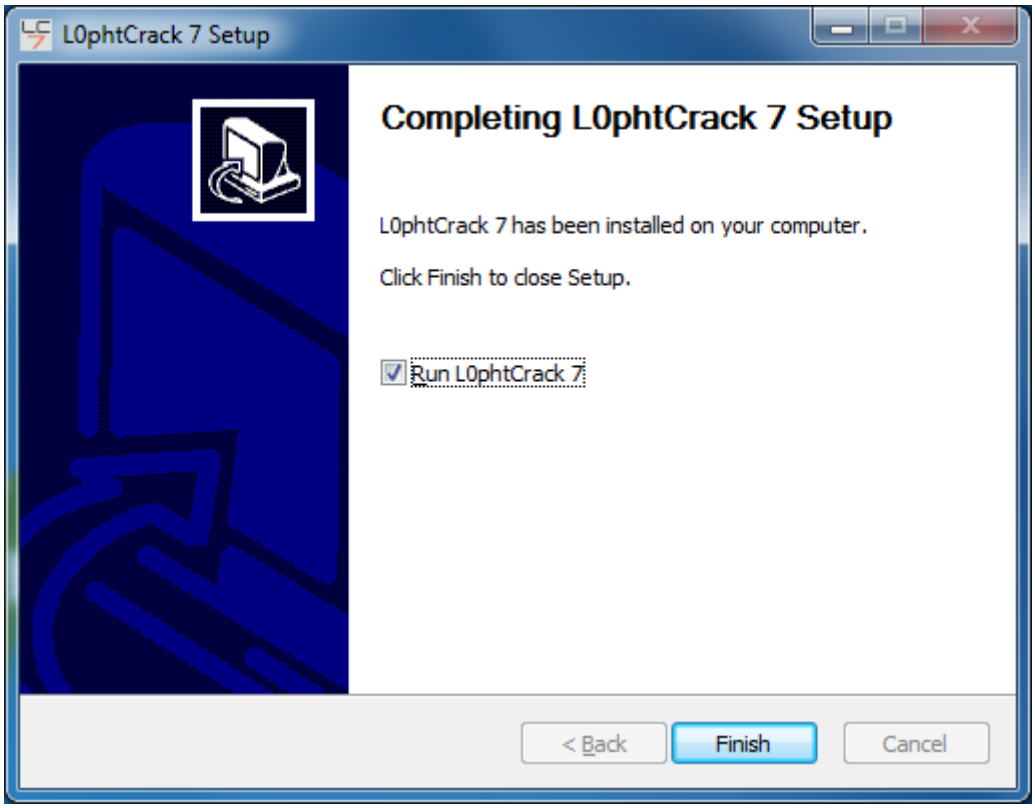
5. The installer installs L0phtCrack 7 in a default installation location: "C:\Program Files\L0phtCrack 7" or you may Browse to choose a different location. Click Next when ready.



6. A shortcut to the L0phtCrack 7 executable is installed in the Programs folder under the Start menu. The default folder name is L0phtCrack 7. You may choose a different name. Click Install when ready.



7. Click Finish when the L0phtCrack installer completes the installation. L0phtCrack will launch by default. If you don't want to run the program at this time, uncheck Run L0phtCrack 7.



8. L0phtCrack 7 is now installed on your system. You may now click the Start button, and go to the Programs folder to run L0phtCrack 7.

Importing Password Hashes

Approaches to importing password hashes differ depending on where the password resides on the computer and your ability to access them.

L0phtCrack 7 can import password hashes directly from remote machines, from the local file system, from SAM, pwdump, or shadow files, and from Active Directory. Obtaining passwords over the network requires network access and administrator privileges to the target machine.

To begin the import process select Import from the Passwords Menu Sidebar on the left hand side of the main screen. When Import is selected you will see the main window display the Import Mechanisms. When you select an Import Mechanism you will see the right side of the main window change to a dialog for the inputs required such as file and machine names.

After you input the required filenames, hostnames and options for an Import Mechanism you will see the action buttons Run Import Immediately and Add Import To Queue ungray and become active. At this point you will likely press Run Import Immediately to perform the import action. Optionally you can press Add Import to Queue to build a queue.

Import from Local Machine

To import password hashes from a local machine, you must be logged in with administrator rights or have an administrator/password pair. The local machine import works regardless of whether passwords are stored in a SAM file or in an Active Directory.

First, select Import from local Windows system. You can select to Keep Currently Imported Accounts if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. If you want to audit all system accounts, not just user accounts, you can select to Include Machine Accounts.

Next, specify the credentials that will be used to access the password hashes. You can choose Use Logged-In User Credentials. If you previously saved credentials for the local machine you can Use Saved Credentials. You can also select Use Specific

User Credentials. If specific user credentials is selected you need to specify Username, Password, and optionally a Domain. You can select Save These Credentials to save the username, password, and domain to the Windows protected store for use in future audits.

Import from Remote Machine

L0phtCrack 7 incorporates remote password hash retrieval, simplifying the process of obtaining password hashes, and reducing the need to use a third-party retrieval/dumping tool.

To import from remote machines select either Import from Linux/BSD/Solaris/AIX system over SSH if your target system is Unix-like or select Import from remote Windows system if your target system is Windows. Credentials with Root or Administrator privileges are required. If a security tool or some other element in the network environment is preventing remote hash retrieval, then you may have to use a third party tool to obtain the hashes and then follow the instructions for importing hashes from a pwdump file, SAM/System file (Windows), or shadow file (Unix).

3.3.3 PWDUMP

The original pwdump program was written by Jeremy Allison in 1997 to demonstratehow to extract password hashes from the Windows Registry. Since then,other developers have created many versions of pwdump to keep up with variousupdates to Windows. But they all rely on extracting hashes from the Registry, SAMfile, or the lsass.exe process's memory space. The lsass.exe process handles the LocalSecurity Subsystem Service; it's essentially responsible for authentication, which iswhy its memory contains the system's password hashes.

All the pwdump variants may be found at www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7. The Openwall site is also the home ofJohn the Ripper, covered previously.

How to use pwdump

The pwdump tools are simple to use. They require Administrator privileges, so you'llneed to start the cmd.exe shell with Run As Administrator. The following

exampledemonstrates pwdump6 on a 64-bit Windows system. The -x option is necessary to letpwdump6 know the target system is 64-bit. Otherwise, the process will hang withoutreturning results. The -n option instructs pwdump6 to forego the search for passwordhistories. The output may be passed to John the Ripper in order to start cracking hashes.

```
C:\pwdump6\PwDumpRelease>          PwDump.exe          -n          -x
localhostAdministrator:500:NO                PASSWORD*************:NO
PASSWORD***********:::
Abs:1007:NO PASSWORD**************:2CxxxxxxxxxxxxxxxxxC01C591BC9:::
Guest:501:NO PASSWORD***********:NO PASSWORD********************:::
Completed.
```

Note that neither the Administrator account nor the Guest account has a passwordset. This will be more common on home desktop systems because modern Windowssystems encourage users to conduct their activities under their own account privilegesand use the runas.exe or Run As Administrator commands to execute programs thatrequire privileged access.

3.3.4 THC-HYDRA

THC-Hydra (aka simply Hydra) easily surpasses the majority of brute-force toolsavailable on the Internet for two reasons: it is fast, and it targets authenticationmechanisms for several dozen protocols. Its source code and documentation are availablefrom https://www.thc.org/thc-hydra/. The Hacker's Choice web site (https://www.thc.org) contains many security tools, although some of them have not been maintainedfor several years.

THC (The Hackers Choice) created Hydra for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

Installing THC-Hydra

If you are running Kali Linux you will already have a version of Hydra installed, for all other Debian based Linux operating systems download from the repository by using.

```
sudo apt-get install hydra
```

or you can download the latest version from THC's public GitHub development repository https://github.com/vanhauser-thc/thc-hydra

Start by using git to clone the GitHub repository.

```
git clone https://github.com/vanhauser-thc/thc-hydra
```

next change into the thc-hydra directory.

```
cd thc-hydra
```

now just type.

```
./configure
```

then…

```
make
```

and then.

```
sudo make install
```

Hydra-GTK

Hydra GTK is a GUI front end for hydra, as this is a GUI for hydra you do have to have THC-hydra already installed. If you are running Kali Linux this will already be pre-installed for everyone.

Understand the Hydra Basics

When we open Hydra, we are greeted with this help screen. Note the sample syntax at the bottom of the screen. Hydra's syntax is relatively simple and similar to other password cracking tools.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
  OPT       some service modules support additional input (-U for module help)

Supported services: asterisk afp cisco cisco-enable cvs firebird ftp ftps http[s
]-{head|get} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] i
rc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql ncp nntp oracle-listener ora
cle-sid pcanywhere pcnfs pop3[s] postgres rdp rexec rlogin rsh s7-300 sip smb sm
tp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes. This tool is licensed under AGPL v3.0.
The newest version is always available at http://www.thc.org/thc-hydra
These services were not compiled in: sapr3 oracle.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY - and if needed HYDRA_PROXY_AUTH - environme
nt for a proxy setup.
E.g.:  % export HYDRA_PROXY=socks5://127.0.0.1:9150 (or socks4:// or connect://)
       % export HYDRA_PROXY_HTTP=http://proxy:8080
       % export HYDRA_PROXY_AUTH=user:pass

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/TLS:DIGEST-MD5
root@kali:~#
```

Let's take a look at it further.

```
hydra -l username -p passwordlist.txt target
```

The username can be a single user name, such as "admin" or username list, passwordlist is usually any text file that contains potential passwords, and target can be an IP address and port, or it can be a specific web form field.

Although you can use ANY password text file in Hydra, Kali has several built in. Let's change directories to /usr/share/wordlists:

```
kali > cd /usr/share/wordlists
```

Then list the contents of that directory:

```
kali >ls
```

You can see below, Kali has many word lists built in. You can use any of these or any word list you download from the web as long as it was created in Linux and is in the .txt format.

```
root@kali: /usr/share/wordlists
File  Edit  View  Search  Terminal  Help
root@kali:/# cd /usr/share/wordlists
root@kali:/usr/share/wordlists# ls
dirb        fasttrack.txt  metasploit-jtr  rockyou.txt.gz  w3af.txt   wfuzz.txt
dirbuster   fern-wifi      metasploit-pro  sqlmap.txt      webslayer
dnsmap.txt  metasploit     nmap.lst        termineter.txt  wfuzz
root@kali:/usr/share/wordlists#
```

Use Hydra to Crack Passwords

In the example below, I am using Hydra to try to crack the "admin" password using the "rockyou.txt" wordlist at 192.168.89.190 on port 80.

```
root@kali:/usr/share/wordlists# hydra -l admin -p /usr/share/wordlists/rockyou.t
xt 192.168.89.190 80
```

Check Your Progress 1:

1. Define Brute-Force attack
2. What is JtR?
3. What is the use L0PhtCrack?

3.4LET US SUM UP

This block covers the password cracking and brute-force tools like John the Ripper, L0PhtCrack, Pwdump and THC-Hydra.

3.5CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. A brute force attack is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.

2. John the Ripper (JtR) is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms.
3. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, hybrid attacks.

3.6 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer “Anti-Hacker Toolkit By Mike Shema”.
For THC Hydra: https://github.com/vanhauser-thc/thc-hydra

3.7ASSIGNMENTS

- How to use John the Ripper tool?

3.8ACTIVITIES

- Perform password recovery using brute-force tools.

Unit 4: Web Attack

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Web - Attack

4.4 Let us sum up

4.5 Check your Progress: Possible Answers

4.6 Further Reading

4.7 Assignment

4.8 Activities

4.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Study various kinds of web attack.
- Identify browser attack, phishing.
- Get the details of user from website.

4.2 INTRODUCTION

This block is focus to securing web applications has become incredibly importantas the information processed by web applications has becomecritical to corporations, customers, organizations, andcountries. Web applications manage a wide array of informationincluding financial data, medical records, social securitynumbers, intellectual property and national security data.The purpose of a web based attack is significantly differentthan other attacks; in most traditional penetration testingexercises a network or host is the target of attack. Web basedattacks focus on an application itself.

4.3WEB ATTACK

Technology growth on the Web has changed the way businesses and consumers communicate and interact with each other.The Web has become a staple for information sharing and commercial transactions. At the same time it has also becomecomplex, without boundaries and immediate in its nature.

Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

A single Web page today can be comprised of information from manysimultaneous sources from around the world. It only takes one of these sources to be compromised in order for a new Web attackto be quickly propagated and delivered

to many unsuspecting Web users. The ubiquity and complexity, compounded with holesin the infrastructure, have made the Web vulnerable to attack.

4.3.1 BROWSER ATTACKS

Of all the software in use, browsers are the most exposed. They are constantly connecting to the outside world, and frequently interacting with websites and applications that cybercriminals have infected with malware.

Browsers are powerful, data-rich tools that if compromised, can provide an attacker with a vast amount of information about you, including your personal address, phone number, credit card data, emails, IDs, passwords, browsing history, bookmarks etc.

Browsers are also perfect instruments for cybercriminals to establish a foothold on your device, your personal network, and your business systems. Browsers rely on a number of third-party plug-ins like JavaScript, Flash, and ActiveX to perform various tasks. However, these plug-ins often come with security flaws that cybercriminals exploit to get access to your systems. These vulnerabilities allow attackers to wreak havoc by, for example, installing ransomware, exfiltrating data, and stealing intellectual property.

During the past year or so, we've seen a sharp increase in web threats that are specifically designed to leverage browser-based vulnerabilities. This increase in popularity is not only because browsers are strategically desirable as hacking targets, but because browser-based web threats are difficult to detect.

Most malware detection and prevention technologies work by examining files such as downloads or attachments. However, browser-based threats don't necessarily use files, so conventional security controls have nothing to analyse. Unless organizations implement advanced tools that don't rely on analysing files, browser-based attacks will likely go undetected.

How Browser Based Cyber-threats operate

As an example of how a browser-based attack works, consider a scenario where a Windows user visits a seemingly benign but now malicious website, possibly one he

or she has visited before, or as the result of an enticing email. As soon as a connection occurs, the user's browser begins interacting with the site.

Assuming the system is using JavaScript, which according to research firms like Web Technology Surveys, 94% of all websites do and over 90% of browsers have it enabled, the browser will immediately download and start executing JavaScript files from the malicious website.

The JavaScript can harbour malicious code that's capable of capturing the victim's data, altering it, and injecting new or different data into their web applications—all in the background and invisible to the user.

For instance, one method malware authors use to accomplish this is by embedding an obfuscated Adobe Flash file within the JavaScript. Flash is frequently used due to its seemingly never-ending set of vulnerabilities. The following is representative of what typically occurs:

- The Flash code invokes PowerShell, a powerful OS tool that can perform administrative operations and exists on every Windows machine.
- Flash feeds instructions to PowerShell through its command line interface.
- PowerShell connects to a stealth command and control server owned by the attackers.
- The command and control server downloads a malicious PowerShell script to the victim's device that captures or finds sensitive data and sends it back to the attacker.
- After the attacker has met his objectives, the JavaScript, Flash, and PowerShell scripts are wiped from memory, leaving essentially no trace of the breach.

The MarioNet attack is a browser-based attack; it opens the door for assembling giant botnets from users' browsers. These botnets can be used for in-browser crypto-mining (cryptojacking), DDoS attacks, malicious files hosting/sharing, distributed password cracking, creating proxy networks, advertising click-fraud, and traffic stats boosting, researchers said.

Moreover, MarioNet can survive after users close the browser tab or move away from the website hosting the malicious code.

4.3.2 WEB ATTACKS TARGETING USERS

Cyber criminals often go after your enterprise data by preying on your end users. Here are some of the most current exploits to watch for.

Every day, criminals devise new malware and social engineering attacks that target what has become an organization's weakest link: end users and their Web-connected devices. Here are the most common attack methods and social engineering techniques, and ideas on how to stop these attacks before they infect end user devices and work their way into your corporate data.

Drive-By Downloads

Drive-by downloads are a central part of many of the most sophisticated Web attacks that criminals perpetrate against online users. They are so dangerous because they require no user action to download malicious content onto an endpoint. What's more, these attacks are often unleashed from legitimate sites.

Drive-by downloads are typically deployed by hackers who have taken advantage of Web vulnerabilities such as SQL injection that can be exploited to "allow attackers to change the content of a website," says Chris Wysopal, CTO at the app security testing company Veracode.

Once implanted on a site, drive-by downloads typically take advantage of browser vulnerabilities to automatically download anything from full-fledged viruses to less detectable downloader apps that will trick the user into eventually loading malware onto the machine via a button press or click.

Clickjacking

If the attacker requires extra interaction from the user to load malware, this will be accomplished through an attack called "clickjacking."

The purpose of this attack is to open the target website in an invisible frame and get the user to click somewhere in the frame when they don't even know they're clicking in that website," says Ari Elias-Bachrach, application security consultant and trainer for security consultancy Defensium. "In this way, you can trick the user into making a mouse click that does something [malicious] on the website.

A common example is offering a bogus pop-up window made to look like a legitimate plug-in update or antivirus alert, such as a Microsoft Security Essentials window that says you have a few viruses and should push a button to clean them. "The pop-up itself is not harmful, but if you click the button, you open the gate to infect your machine," says Rick Doten, chief information security officer for DMI, an enterprise mobility company.

Plug-In And Script-Enabled Attacks

Not only do attackers look for vulnerabilities within the browser itself, they also frequently ferret out bugs in browser plug-ins and scripting programming to help them carry out drive-by downloads and clickjacking attacks.

Since these attacks rely on known vulnerabilities, "make sure users keep browsers and browser plug-ins updated to the latest versions by enabling auto-update functions," says Wolfgang Kandek, CTO of vulnerability management firm Qualys.

In some cases, it may also make sense to turn off scripting within the browser and other susceptible programs, such as Adobe Reader. Similarly, uninstalling certain problematic plug-ins can reduce the attack surface within susceptible user bases. But you'll still need to put controls in place and train users not to undo the work.

Advanced Phishing Attacks

While phishing attacks are typically associated with email, most are perpetrated via links to malicious content on the Web, whether a simple password capture form used in traditional phish attempts or a malicious drive-by download in more advanced targeted attacks.

Phishing attacks are designed to trick users into thinking they are a link from an organization or person they know, making people feel safe enough to click or divulge information they otherwise wouldn't. Many corporate security training programs have helped users spot the most obvious first-generation phishing attempts, which were designed to steal credentials such as banking passwords. But attackers are getting more crafty.

Social (Engineering) Networks

Millions of people sharing information on social networking sites such as Facebook, Twitter, LinkedIn and Google+ creates "an ideal attack bed for someone who wants to socially engineer a target individual, group of individuals or an organization as a whole," says Joe DeSantis, manager of incident response at security consultancy SecureState.

If people don't configure their privacy settings very stringently, attackers can simply troll their pages to dig up information about the target and then hone a particularly effective spear-phishing email. Or attackers can pose as friends or family to "friend" a target -- or a friend of the target -- to gain that intelligence. They can also use a social networking connection to directly send targets malicious links on their walls or Twitter feeds.

4.3.3 OBTAINING USER OR WEBSITE DATA

The value of web data is increasing in every industry from retail competitive price monitoring to alternative data for investment research. Getting that data from a website is vital to the success of your business.

Web scrapers automatically collect information and data that’s usually only accessible by visiting a website in a browser. By doing this autonomously, web scraping scripts open up a world of possibilities in data mining, data analysis, statistical analysis, and much more.

Why Web Scraping Is Useful

We live in a day and age where information is more readily available than any other time. The infrastructure in place used to deliver these very words you are reading is a conduit to more knowledge, opinion, and news than has ever been accessible to people in the history of people.

So much so, in fact, that the smartest person’s brain, enhanced to 100% efficiency (someone should make a movie about that), would still not be able to hold 1/1000th of the data stored on the internet in the United States alone.

As our eyes and brains can't really handle all of this information, web scraping has emerged as a useful method for gathering data programmatically from the internet. Web scraping is the abstract term to define the act of extracting data from websites in order to save it locally.

Think of a type of data and you can probably collect it by scraping the web. Real estate listings, sports data, email addresses of businesses in your area, and even the lyrics from your favourite artist can all be sought out and saved by writing a small script.

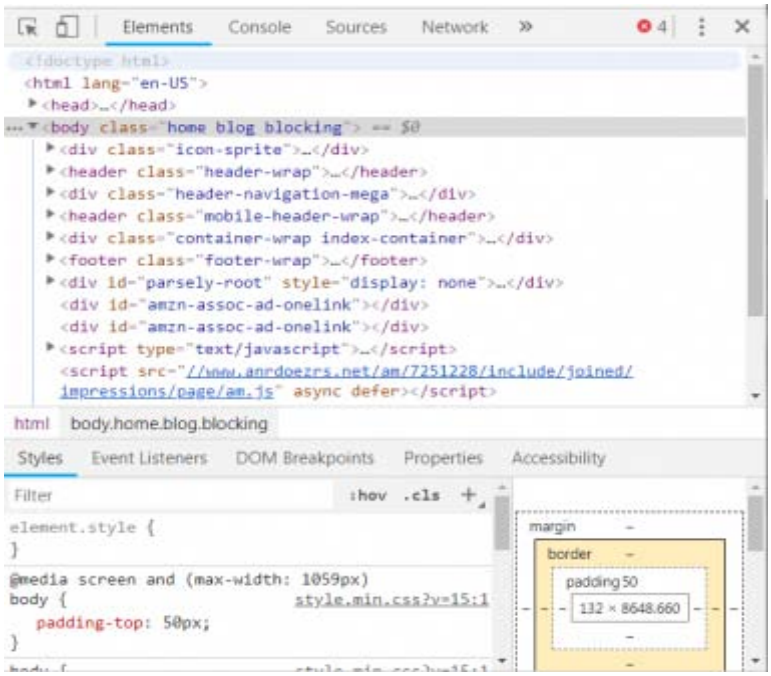
How Does a Browser Get Web Data?

First, your browser will take the URL you entered or clicked on and form a "request" to send to a server. The server will then process the request and send a response back.

The server's response contains the HTML, JavaScript, CSS, JSON, and other data needed to allow your web browser to form a web page for your viewing pleasure.

Inspecting Web Elements

Modern browsers allow us some details regarding this process. In Google Chrome on Windows you can press Ctrl + Shift + I or right click and select Inspect. The window will then present a screen that looks like the following.



Other Types of Responses

Additionally, servers can return data objects as a response to a GET request, instead of just HTML for the web page to render. A website's Application Programming Interface (or API) typically utilizes this type of exchange.

Scraping frameworks are available in Python, JavaScript, Node, and other languages. One of the easiest ways to begin scraping is by using Python and Beautiful Soup.

4.3.4 EMAIL ATTACKS

Malicious email remains one of the most significant and ongoing computer security threats that we face. Cybercriminals use a variety of email-based attacks to deliver malware, lure victims to malicious websites, and steal logon credentials, and organizations everywhere need to understand these threats and how to implement effective safeguards.

Many people rely on the Internet for many of their professional, social and personal activities. But there are also people, who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.

Email is a universal service used by over a billion people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.

Malicious email authors are clever and relentless, and they are constantly developing new or at least different ways to deceive and attack us. Although the malicious payloads found in email-based attacks frequently change, the vast majority of cybercriminals use basic strategies:

Malicious attachments: Emails often include dangerous attachments that install keyloggers, ransomware, and other malware when opened by the victim.

Links to malicious web pages: Contained in either an attachment or in the body of the email, links to dangerous web pages also account for a significant number of data breaches.

Below are some of the most common types of Attacks:

Phishing: Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person. The criminal researches the target's interests before sending the email.

Whaling: Whaling is a phishing attack that targets high profile targets within an organization such as senior executives. Additional targets include politicians or celebrities.

Pharming: Pharming is the impersonation of an authorized website in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they connected to a legitimate site.

Adware: Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyse user interests by tracking the websites visited. It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.

Spam: Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware or deceptive content. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

Check Your Progress 1:

1. What is Phishing?
2. How Email attacks happen?

4.4LET US SUM UP

This block covers the various web attacks like phishing, pharming, etc.

4.5CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
2. Malicious email remains one of the most significant and ongoing computer security threats that we face. Cybercriminals use a variety of email-based attacks by sending malicious attachment as well as links to malicious web pages.

4.6 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053.

4.7ASSIGNMENTS

- Describe various email attacks.

4.8ACTIVITIES

- Retrieve website data using web scrapper.

Block-4

Introduction to Cyber Crime, Law and Investigation

Unit 1: Cyber Crimes

1

Unit Structure

1.1. Learning Objectives

1.2. Introduction

1.3. Types of Cybercrime

1.4. Hacking

1.5. Cyberspace and Criminal Behaviour

1.6. Clarification of Terms

1.7. Traditional Problems Associated with Computer Crime

1.8. Introduction to Incident Response

1.9. Digital Forensics

1.10. Computer Language

1.11. Network Language

1.12. Realms of the Cyber world

1.13. Check your Progress: Possible Answers

1.14. Further Reading

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Types of Cybercrime,
- Hacking,
- Cyberspace and Criminal Behaviour,
- Clarification of Terms,
- Traditional Problems Associated with Computer Crime,
- Introduction to Incident Response,
- Digital Forensics,
- Computer Language,
- Network Language,
- Realms of the Cyber world

1.2 INTRODUCTION

“Cyber-Crime” Computer crime, or cybercrime, is crime that involves a computer and a network. Cyber-crime involves activities like raiding bank accounts and stealing information from companies. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet chat rooms, emails, SMS/MMS, notice boards and groups and mobile phones such crimes may threaten a nation’s security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

1.3 TYPES OF CYBERCRIME

Cybercrime includes a wide range ofactivities generally however it may beclassified into four classes as on theimage

- Crime against individual
- Crime against property
- Crimeagainstorganization
- Crime against society

Crimes against individualsemailspoofing a spoofing mail is theformation of email messages byimpersonatingcorrespondent.

Email spamming spam is amessage also called as junk mail sentwith a web link or business proposalclicking on this link or replying tocommercial offer sent to a phishingwebsite or set up a mall where in yourworkstation the sender's of thiselectronic email are always unidentified.

Crime against Propertycredit card fraud online fraud andcheating are most money spinning tradesthose are raising nowadays in the cyberspace it may have diverse forms some ofthe cases of online fraud and cheatingthat are uncovered are those referred to credit-cardoffences contractual crimes offeringemployment etc.

Intellectual property crimesintellectual property involves a list ofRights any illegal act due to which theowner is deprived entirely or part ofthe his human rights. It is a crime the verycommon form of IPRabuse may be known to be software piracy,copyright infringement, trademark andservice mark violation theft of acomputer source code.The Hyderabad Courthas in a landmark judgment has convictedthree personand sentenced them to six months custodyand fine off rupees 50,000 each forunauthorized copying and sell of piratedsoftware.

Against Organization unauthorized accessthis is generally denoted to and hackingthe intent law has however given adifferent connotation to the termhacking so we will not use the termunauthorized access interchangeably withthe term hacking to preventmisperception.As the term used in the IT Act 2000 of India is much wider thanhacking.

Denial of service attack insimple words denial of service referredthe act by which a user of any website or service denied to use the service orwebsite.In this category of cyber crime offenders in the web server of the websites and flow a large number of requests to that server this causes the use of maximum bandwidth of the website and it goes slow down not available for sometimes.

Virus attack a computer virus is a type of malware that when executed replicates by implanting the replicas of it probably altered into other computer programs data files or the boot sector of the hard drive. When this reproduction proceeds the affected zones are then said to be infected. Viruses frequently do certain type of dangerous activity on infected hosts such as stealing hard disk space or CPU time retrieving, private information corrupting, data displaying radical often emails on the user's display spamming their links or logging their keystrokes. However not all viruses can have a damaging consignment or effort to hide themselves the describing features of viruses is that they are self-duplicating computer programs which mount themselves without the users approval.

On the other hand computer worm is a separate more than program that copies itself in order to disperse to other computers frequently. It uses a computer network to spread itself depend on security failures on the aim computer to allow it.Unlike a computer virus it does not require to join itself to a prevailing program email bombing. IN email bombing user is sending vast numbers of emails to target address and due to this that email address or mail server crashed. It feels like denial of service impression it says that spamming is a variant of male bonding salami attack.

A salami attack is when minor attacks make up a major attack which becomes untraceable because of its nature. It is also called a salami slicing though salami slicing is frequently used to transport unlawful activities it is only a plan for gaining and benefit over time by collecting it in small increments so it can be used in perfectly legal ways as well the attacker uses an online database to seize the information of customers.i.e.bank credit card details deducted very little amount from every account above a period of time the customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.

Logicbomb

a logic bomb is a piece of code intentionally inserted into a software system that will initiate mischievous features under definite conditions, for example a programmer may hide a part of code that starts initiating deleting files such as salary database. Malicious programs such as viruses and worms often contain logic bombs that execute a certain payload at a predefined time or when some other condition meets.Thistechnique can be used by a virus or wormto gain momentum and spread before beingnoticed.Some viruses attack their wholesystems on particular dates such as,April fool's Day.Trojans thattrigger on certain dates are frequentlyknown as time bomb Trojan horse

a Trojan horse or Trojan in computing is anon-self-duplicating kind of malware program comprising malicious codethatwhen implemented carries out actions determined by the nature of the Trojan Usually causing damage of stealing of data and likely system damage. Theterm is derived from the tale of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece.Becausecomputer trojans often hire a form of social engineering representingthemselves as routine valuable or interesting in order to encourage victims to install them on the computers. A Trojan generally acts as a backdoor communicating a supervisor that can have unlawful access to the affected computer. TheTrojans exit are not themselves easily noticeable but if they carry out substantial computing or communications activity may cause the computer to run noticeably slow data.

1.4 HACKING

- **Why Hackers Hack?**

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers. They just hack to see what they can hack and what they can't hack, usually by testing their own systems. Many Hackers are the guys who get kicked out of corporate and government IT and security organizations. They try to bring down the status of the organization by attacking or stealing information. The knowledge that malicious hacker's gain and the ego that comes with that knowledge are like an addiction. Some hackers want to make your life miserable, and others

simply want to be famous. Some common motives of malicious hackers are revenge, curiosity, boredom, challenge, theft for financial gain, blackmail, extortion, and corporate work pressure. Many hackers say they do not hack to harm or profit through their bad activities, which helps them justify their work. They often do not look for money full of pocket. Just proving a point is often a good enough reward for them.

- **Steps Performed By hackers**

1) Reconnaissance

   • Performing Reconnaissance

2) Scanning

   • Scanning and Enumeration

3) Gaining Access

4) Maintaining Access

   • Maintaining access and Placing Backdoors

5) Clearing Tracks

   • Covering tracks or Clearing Logs

- Phase I: Reconnaissance

  Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The Hacker seeks to find out as much information as possible about the target.

- Phase II: Scanning and Enumeration

  Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent system port scanning which is used to determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

- Phase III: Gaining Access

  This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline. Gaining access is known in the hacker world as owning the system. During a real security breach it would be this stage where the hacker can utilize simple techniques to cause irreparable damage to the target system.

- Phase IV: Maintaining Access

  Once a Hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other Hackers or security personnel by securing their exclusive access with Backdoors, Root kits, and Trojans. The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

- Phase V: Clearing Tracks

  In this phase, once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. At present, many successful security breaches are made but never detected. This includes cases where firewalls and vigilant log checking were in place.

The Indian IT Act, 2000 defines and punishes “Hacking” as follows:

Hacking with computer systems

- Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes any information residing in computer resources.

- “Whoever commits hacking shall be punished with imprisonment up to three years, with fine which may extend up to 2 lakh rupees or both”

- Hacking has been very widely defined in the law of Information Technology, which is much wider than the concept of “hacking” as understood in common.i.e. “Breaking into computer systems”.
- “Destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means”

1.5 CYBERSPACE AND CRIMINAL BEHAVIOUR

Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography. The word became popular in the 1990s when the uses of the Internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging. There are no shared definitions of cyberspace at the scientific level and every government uses a different definition. Cyberspace is the national environment in which digitized information is communicated over computer networks.” -Dictionary of Military and Associated A global domain within the information environment consisting of inter dependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems & and embedded processors and controllers.

Cyber security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. Cyber security standards are the specifications which enable organizations to practice safe security techniques to minimize the number of successful cyber-attacks. Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. Though, cyber security is important for cyberspace.

Traditional Problems Associated with Computer Crime Individuals seeking a crime has always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves no specialist users (e.g., child pornographers, narcotics traffickers, and predators). In fact, the earliest computer crimes were characterized as no technological. Theft of computer components and software piracy were particular favourites. Hacking, DDoS attacks, phishing, Botnets, and other technologically complicated computer crimes came later. Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community is experiencing unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge, allocated resources, and administrative apathy traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators and policymakers are ill-equipped to do so.Physicality and Jurisdictional Concerns The physical environment that breeds computer crime is far different from traditional venues. In fact, the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents. For example, what forensic tools are available for identifying entry points in data breaking and entering? Certainly, seasoned investigators recognize the utility of prymark analysis in home burglaries.

- **Cyberspace and Criminal Behavior**

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Associate Professor at the Sorbonne Business School), technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam. Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack – brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign.

Cyberspace has become an ideal place for criminals to remain anonymous while preying on victims. As the number of cyberspace users increase, so do the opportunities for exploitation and the need of protecting computers, networks, digital applications, programs and data (i.e., sensitive business and personal information) from unintended or unauthorized access, change or destruction. The Department of Homeland Security (DHS) affirms that there is a range of traditional crimes now being perpetrated through cyberspace.

Criminals hide in the net to perpetrate quite effortlessly crimes that, in earlier times, required physical travel and a more direct involvement. As the cyberspace is recognized as a critical domain for conducting everyday distant operations, unfortunately, it has also become a ground for cyber-terrorism and menaces of cyberwar attacks. Cyberterrorists may use various forms of computer-related abuse tactics (e.g., hacking, cracking, phishing, spamming) to accomplish their personal or politically-motivated goals.

However, countries and governments are not the only targets of cyber criminals. Businesses are not safe either; vital corporate data and industrial secrets can be

stolen from adversaries, for example, with cyber espionage; in the past, some attempts have come from countries including China and Russia. In fact, the financial sector is one of the most targeted in recent times and has been the theater of attacks that have often captured the interest of the media.

Recent news, for example, report of a large operation conducted in Europe against a multi-national organization operating in Italy, Spain, Poland, Belgium and the UK. Cyber criminals were able to infiltrate malware in the systems of some large European companies and route money to bank accounts they controlled: a $6.8 million business. EC3, the Europol's European Cybercrime Centre, discovered that the organization was operating from Cameroon, Nigeria and Spain through an impressively efficient money laundering system. Cybercrime has really no borders and boundaries.

In recent years, "information warfare," a new form of terrorism, has captured the attention of information security specialists; terrorists might tamper with computers to commit information-based threats to nations, to businesses, and to individuals.

- **Economic Impact of Cybercrime**

Cyberspace is vulnerable to a wide range of risks, affirms the DHS Cyber Security Division, saying it brings substantial human and economic consequences. All computers users are at risk of Internet crime. According to the Norton Cybercrime Report for 2011, "1m+ adults become cybercrime victims every day." As per a study jointly conducted by McAfee and the Center for Strategic and International Studies in June 2014 (Net Losses: Estimating the Global Cost of Cybercrime), computer-related crimes may cause as much as $400 billion in losses annually, while cyberattack-related losses could be as much as 575 billion. However, arriving at an estimate for the financial losses suffered because of cybercrime is difficult because many instances simply go unreported.

Cybercrime can mean incredible losses for businesses, but is a great deal for perpetrators. Trustwave's "2015 Global Security Report" estimated that the average cybercriminal has a 1,425 percent return-on-investment (ROI). These figures can definitely explain the proliferation of attacks.

- **Cybercrime Trends**

In a world where information and communications technology (ICT) that provides the means so people can work with each other electronically in a digital form over great distances, cyber threats are of great concern. Though it is difficult to keep up with the changes as ICT is constantly evolving, an understanding of the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks is paramount.

Cybercriminals often use 'bots' – a network of software robots – to infect and control networks and control them remotely for malicious purposes. From phishing and devious social engineering efforts to using spyware tactics, an invader can carry out an attack on specific targets, exploiting zero-day vulnerabilities, upload malware on certain platforms, if not collect information and gain access to systems for other purposes. In fact, botnets are often used to spread remote code execution malware. Coming familiar with botnet cyber threats (i.e., how they work and spread malicious code infecting each host and then propagate into the network) is vital to preventing the botnets from the beginning.

Examples of botnet attacks are easy to find. The GameOver Zeus botnet (a sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects) that occurred in 2014, according to the FBI, it was believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world.

As per the FBI, "Unlike earlier Zeus variants, GameOver has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin, which means that instructions to the infected computers can come from any of the infected computers, making a takedown of the botnet more difficult. But not impossible."

The growth of the use of cloud computing and the Internet of Things (IoT) is contributing greatly to the problem. According to Security Expert and bestselling author, Marc Goodman, in fact, the number of devices connected through the Internet is growing exponentially, and security is an issue: the average IoT, he estimates, has over 20 security vulnerabilities, a number that poses serious concerns.

Another alarming trend, according to Goodman, is the new cybercriminals' profile, who, in most cases, are no longer teenagers looking for glory, but consummate professionals that choose cybercrime as a profession and can sell services. The new breed of malicious hackers is made of more sophisticated criminals who can actually operate within highly organized establishments.

In addition to more specialized hackers, computer software is increasingly been used to perpetrate cybercrime. Crimeware-as-a-service is a new option for criminals without particular technical skills who can carry out their agenda by using off-the-shelves products designed for that purpose. Defending ourselves from this new, decentralized, and pervasive cybercrime is a daunting task.

There is no arguing, "Cybercrime is a global problem." With the ability to connect anything and everything to the Web, cybercriminals exploit the inherent connectivity when and where they like. When it comes to Internet crime, there are all sorts of law-breaking offenses committed that range from identity theft and fraud to unethical hacking, illegal downloading of media, online harassment (e.g., cyberstalking, cyberbullying, to include sexting, child soliciting and abuse), among others. Recurring crimes include sending malicious software to disrupt a network or gain access to a system with the motive to steal sensitive information or data, if not to cause damage to system software. Laws and regulations vary across the country. (See, for example, U.S. state-specific computer crime laws.)

Users are called upon to be the first line of defence and help reduce cyber risks and data compromised by hackers through proper use of their computer, mobile phone and other devices. A Trustwave study showed how 81% of victims they surveyed did not detect breaches in their systems but were notified by external entities. The Verizon's 2015 Data Breach Investigations Report further found that, in 66% of the cases they analysed, it actually took a few months to discover the crime. Situational awareness, then, is one of the key areas of cyber defence and is invaluable when coupled with monitoring and malware analysis from IDS alerts and log files gathered by those in the field. In 60% of the cases, it only took a few minutes for cybercriminals to cause damage to the organizations they attacked, so it is important that everyone in an organization is always looking for anything suspicious in the way

their systems behave. Even DHS has created an on going cybersecurity awareness campaign Stop.Think.Connect. launched on October 4, 2010 to help people to understand the risks that come with being online.

Despite IDS/IPS technologies being deployed, only a small percentage of IT decision makers are truly confident that these devices alone will work against a cyber-threat; therefore, they are still seeking alternative solutions, mentioned Tara Seals, US/North America News Reporter, Info security Magazine, in a recent post. Seals explains also the importance of perimeter-based cyber-security models – characterized by a multi-level approach involving firewalls, anti-virus software and powerful analytic tools searching for anomalies in network behaviour

across the enterprise – to protect against threats (or to reduce the damage they can cause), as they continue to evolve rapidly.

- **Cyberspace and Criminal behavior**

Cyberspace may be defined as the indefinite place where individuals transact and communicate. It is the place between places.4 Although originally coined in 1984 by science fiction writer William Gibson, it is hardly a new concept. In fact, traditional electronic communications have always fallen within this existential space. Telephonic conversations, occurring across time and space, were pre-dated by wire exchanges. However, the new medium known as the Internet has monumentally increased the physicality of the virtual world, outpaced only by the exponential growth in the number of users. In 2009, for example, approximately 78 percent of the United States actively used the medium as compared to 10 percent in 1995. In the UK, the growth was even more evident with users of the medium rising from 1.9 percent in 1995 to 83.2 percent in 2009.5Noothermethod of communication converges audio, video, and data entities so effectively. Unlike traditional methods, the Internet combines mail, telephone, and mass media. As stated previously, it exposes individuals to a myriad of new ideas and may serve as a social gathering place, a library, or a place to be alone. As such, the existential nature of the medium does not negate the reality of its consequences. Individual users have married, planned their lives, and stalked our children there. Unfortunately, this virtual world is often perceived as a painless alternative to worldly problems, where individuals shed

their worries and become perfect in their profiles. Privacy advocates have often overlooked the negative repercussions of this global medium, arguing zealously that the potentiality of emerging technology precludes governmental interests in monitoring citizens. The organization was co-founded by luminarieslike“TheGratefulDead’s”lyricistJohnBarlowandJohnGilmore,whoistheco-founder/inventorofCygnusSolutions,Cyberpunks,andDESCracker.BothBarlowandGilmorehavebeenmostvocalintheirdefenseofsomeofthemostnoto-riouscomputerhackersintheUnitedStatesandhavechampionedtheBillofRights.They argue that the original thrust of the frontier police, directed at ne’er-do-wells intent on compromising the privacy of American citizens, has been refocused on the very individuals that they originally protected. In fact, the two created the electronic Frontier Foundation(EFF)offeringto“fund,conduct,andsupportlegaleffortstodemonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive and unconstitutional.”7 While early actions by the U.S. Secret Service may validate some of these early concerns, the efforts of the EFF have often overlooked the negative potentiality of this global marketplace that has reunited a society that had increasingly removed itself through suburbanization.BeginningwiththeIndustrialRevolution,Americansocietyhaslongbeencharacterized by its distrust of strangers. As media attention increasingly focused on elevated levels of predatory crime perpetrated by non-acquaintances during the 1980s, this fear resulted in a myriad of proactive attempts by both government and citizens to reduce their perceived vulnerability. Among these were admonitions to children to avoid strangers and lock their doors. While such precautionary measures may have been well served in regards to physical crime, the advent of technology has lowered traditional barriers and served as an informal invitation for unknown visitors. Many—such as the victims of theft, stolen privacy, and the like—have recognized only too late the dangers of their inattentiveness, while others, yet to suffer negative consequences, remain blissfully unaware of their own vulnerability. In fact, most individuals, young and old alike, are seduced by the soft hum of a device that appears to be the gateway to worlds that were previously restricted.

Unfortunately, this fascination may be exploited by those we try most to avoid—criminals and predators. As stated previously, technological advancements have historically led to criminal innovations. Just as the Industrial Revolution enhanced threats to national security and created an environment conducive to street/predatory crime through the concentration of the urban population, the information or digital revolution has created a new forum for both terrorist activity and criminal behavior. Indeed, this latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike. Critical infrastructures, increasingly characterized by tight couplings and interdependency of IT, emergency services, public utilities, banking sectors, food supplies, and transportation systems, have resulted in an interconnectivity inconsistent with traditional security strategies. Such myopia has similarly impacted private citizens who have failed to employ rudimentary measures of cyber protection even as they add additional door locks and alarm systems to insulate themselves from physical attacks. In fact, it may be argued that the Digital or Information Revolution has created a criminogenic environment in which traditional criminals adapt and new criminals emerge.

1.6 CLARIFICATION OF TERMS

Just as debates rage over the appropriate codification of crime committed via electronic means, controversy surrounds the actual semantics associated with the phenomenon. For clarification purposes, then, it is necessary to define the historical usage of terms associated with technological or electronic crimes. Computer crime has been traditionally defined as any criminal act committed via computer. Computer-related crime has been defined as any criminal act in which a computer is involved, even peripherally. Cybercrime has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses. Finally, digital crime, a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. As data may be accessed or stored in a variety of ways and in a variety of locations, digital crime may be characterized as any of the three depending on case characteristics. While computer crime and computer-related crime will be used interchangeably throughout

the text, cybercrime will only be used to describe that criminal activity which has been facilitated via the Internet. Additionally, students should be advised that a variety of definitions exist, and that such variations have resulted in confusion among legislators and investigators alike. Some authors, for example, argue that any crime that involves digital evidence may be characterized as a computer crime. This is misleading at best and self-serving at worst. Traditional kidnapping cases in which ransom demands are communicated via telephone will always represent a crime against a person and should not be characterized as a “telecrime.” While it is desirable to establish an environment where computers are viewed as potential evidence containers in any case, to redefine traditional predatory crime as cybercrime or computer crime is absurd. Extortion is extortion and will remain such regardless of the method employed to communicate the threat. The result of such hyper-definition is to negate some emerging legislation. This is not to suggest that legislators should cease efforts to specifically criminalize computer-specific criminal activity. Indeed, further legislation should be pursued to enhance prosecutorial toolboxes, not to replace or supplant traditional mechanisms.Just as confusion exists regarding the appropriate terminology for crimes involving computers, the nomenclature of the science developed to investigate such activity lacks universality. For clarification purposes in this text, computer forensic science, computer forensics, and digital forensics may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence.

1.7 TRADITIONAL PROBLEMS ASSOCIATED WITH COMPUTER CRIME

Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late. This trend has proven to be true in contemporary society. Fortunately, much computer-related

crime involves non specialist users (e.g.,child pornographers, narcotics traffickers, and predators).In fact, the earliest computer crimes were characterized as no technological. Theft of computer components and software piracy were particular favorites. Hacking, DDoS attacks, phishing, Botnets, and other technologically complicated computer crime scame later. Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community is experiencing unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge, allocated resources, and administrative apathy traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators and policymakers are ill-equipped to do so.

1.8 INTRODUCTION TO INCIDENT RESPONSE

Incident handling is a generalized term that refers to the response by a person or organization to an attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster. This paper will provide a logical approach to handling two common forms of attack - virus outbreak and system compromise. The method that this article will propose includes the following sequence of steps that should be followed in the case of all types of attack.

1) Preparation

Comprehensively addressing the issue of security includes methods to prevent attack as well as how to respond to a successful one. In order to minimize the potential damage from an attack, some level of preparation is needed. These

practices include backup copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. Regularly-scheduled backups minimize the potential loss of data should an attack occur. Monitoring vendors' and security web sites and mailing lists is a good way to keep up to date with the state of the software and patches. It is necessary to update software in order to patch vulnerabilities that are discovered. It is also vital to update anti-virus software in order to keep system protection up-to-date. A documented security policy that outlines the responses to incidents will prove helpful in the event of an attack, as a reliable set of instructions.

2) Identification of Attack

While preparation is vital for minimizing the effects of an attack, the first post-attack step in Incident handling is the identification of an incident. Identification of an incident becomes more difficult as the complexity of the attack grows. One needs to identify several characteristics of an attack before it can be properly contained: the fact that an attack is occurring, its effects on local and remote networks and systems and from where it originates.

3) Containment of Attack

Once an attack has been identified, steps must be taken to minimize the effects of the attack. Containment allows the user or administrator to protect other systems and networks from the attack and limit damage. The response phase details the methods used to stop the attack or virus outbreak. Once the attack has been contained, the final phases are recovery and analysis.

4) Recovery and Analysis

The recovery phase allows users to assess what damage has been incurred, what information has been lost and what the post-attack status of the system is. Once the user can be assured that the attack has been contained, it is helpful to conduct an analysis of the attack. Why did it happen? Was it handled promptly and properly? Could it have been handled better? The analysis phase allows the users and administrators to determine the reason the attack succeeded and the best course of action to protect against future attacks.

- Incident Handling - Viruses
  - Preparation

    Viruses can cause irreparable harm to important files and records. The home and small office user is at even higher risk than larger organizations because the user often works with one computer or stores important information in a single location. Unlike larger organizations that have data spread across many systems in several locations, a virus outbreak in a home or small office could permanently destroy important data. This puts greater emphasis on the need for creating backups of all information. Additionally, backup disks should be kept in a separate location, away from the computer. This ensures that in case of an incident such as fire or theft of hardware that a backup copy of all information is still available.

    The second crucial step in preparing for an attack is to install anti-virus software. Anti-virus software is readily available, easy to install and operate and is affordable. New viruses are created frequently, so it is important to be diligent with anti-virus software maintenance. Almost all anti-virus vendors make updates available on their websites. Users should update their anti-virus software on a regular basis.

  - Identification of Virus Attack

    Viruses are particularly potent and frightening because of their ability to spread quickly to 'friendly' computers. Just think of the public relations nightmare your company could endure if you're the address book in your e-mail program was used to spread a virus to all your suppliers' and your customers' computers.

    Early identification of an incident is crucial to ensuring that the virus does not spread to other computers. It is crucial that users are familiar with the symptoms of a virus attack, such as mass e-mailing, file destruction or other malevolent actions the results of which can be seen immediately. Stealthy viruses require a bit more attention. The user should be aware that periodic anomalous behavior on a system is not always an indicator of a virus attack.

Other factors may cause the erratic behaviour; however, for the sake of security, the user should scan the computer comprehensively to clearly identify the cause. Configuring the anti-virus software to do real-time scanning of files and to periodically do complete system scans helps to both prevent and identify viruses.

- Containment

  Containment of the virus is pivotal in limiting the effects. Many viruses spread themselves automatically. If a non-replicating virus infects a single computer, containing the virus is fairly straightforward. The administrator, or user, should disconnect network access including shared directories and other components that may allow the virus to infect files and programs on other machines. Anti-virus software often has a "rescue" component that allows an administrator to scan and clean a system by booting from a specialized floppy disk or CDROM. If available, these tools should be utilized to disinfect the system.

  Should the anti-virus software fail to clean the system or lack the features necessary to do the cleansing, it is advisable to try other software packages that may provide more comprehensive coverage. If the system has been altered beyond repair, the last resort is to clear the system entirely and reinstall the operating system and software. If reinstalling, care should be taken to use software that is known to be uninfected and to completely reformat the hard drive to assure the eradication of the virus.

- Recovery and Analysis

  Viruses cause varying degrees of destruction- some exist merely to replicate; others attach to and destroy files and programs. Anti-virus programs can generally restore files to their original state, but there are exceptions. If there is doubt to the reliability of the data held within a file, the user should compare the damaged file to a backup copy in order to assess whether or not damage has been sustained.

  Once the system or systems have been returned to full operation, analysis should be done to determine where the defenses failed. Does fault lie in the

anti-virus software, or the frequency and reliability of updates? Or did some user behaviour - such as opening files from an unknown or untrusted source - allow the system to become infected? Once the attack was identified, were appropriate and sufficient steps taken to minimize the damage that the system sustained? Analysis of the incident allows the user to learn from the unfortunate incident and ensure that it does not happen again.

- System Compromise
  - Preparation

    System compromise is an attack in which an intruder breaks into a computer and, either sitting directly in front of it or from a remote network, is able to use that computer. The attacker typically has total access to a system and all information contained therein including files, applications and potentially any other system connected to it.

    Managing system compromise is more daunting than managing virus outbreaks. The basic steps to help prepare in case of system compromise are basically the same as are used in preparation for virus outbreaks. All vital information should be backed up on a regular basis. Software updates are also crucial. System compromise often arises due to security vulnerabilities in common software, particularly in operating system software. Users and administrators should be sure to maintain current software patches in order to protect against attacks. Patches are available through vendors' websites. Users can learn about the latest patches by monitoring vendors' web sites, mailing lists and user forums related to the software and to security.

    In order to prevent against unauthorized intrusion into a system, users should implement firewalls. Just as anti-virus software is the cornerstone of a virus prevention strategy, firewalls are extremely important in preventing unauthorized individuals from accessing network services and resources. Like anti-virus software, firewalls are relatively affordable and easy to use - they not only protect against intrusion, but some can be configured to notify the user if an intrusion is being attempted.

  - Identification

Systems compromise attacks are often indicated by missing or modified files, changes to the system configuration and services, greater memory and disk usage and unidentified network connections. Attackers will often seek to hide any indication of the intrusion by replacing files and programs with versions that protect the attacker. Programs that act normally on one occasion and strangely the next, as well as files and programs that have their time, date or size information modified may be indicative of an unauthorized intrusion. Comparison against backup copies may reveal changes to files.

Users and systems administrators can identify potential systems compromise attacks by monitoring network traffic and processes. The new wave of Intrusion Detection Systems (IDS) is extremely helpful in allowing for the monitoring of systems. By actively monitoring the network for known signs of attack and other anomalous conditions, an IDS notifies users as soon as it detects the event. IDS are useful in complex networked environments and where minimal technical staffing is available. By automatically monitoring and notifying users, an IDS can offload some responsibility from an overburdened administrator, making them invaluable resources for users and administrators in small offices and home offices.

- Containment

  Containment of an intrusion involves some effort on the part of the administrator. First, the administrator should freeze the current system as soon as an intrusion is suspected. This includes disconnecting the system from the network, stopping the operating system and disallowing anyone to use the system. As an operating system runs and people use the system files are naturally modified and updated depending on what they are doing. This normal functionality often erases important information that can be used to detect and trace an intrusion, therefore it is very important to stop the system as soon as possible after an attack is discovered. If possible, it is advisable to duplicate the hard disk of the system. This allows the administrator to begin the cleanup process on one disk and to give the other to an expert to determine the exact source and cause of the intrusion.

- Recovery and Analysis

The most devastating but least-effort method of cleaning up a compromised system is to wipe the hard disk clean and re-install the operating system and software allowing a faster return to normal operation. A more painstaking approach is to compare each individual file and program against a copy known to be original in order to determine if any modifications have been made. It is important to do a minimal level of analysis in order to determine the cause of the intrusion. Once a cause is determined, changes to the environment should be made to avoid future attacks by that method. This includes updating affected software, access control methods that allow only certain users, systems and networks to use the services, firewalls and intrusion detection systems. A combination of these changes can provide a safer and more secure working environment.

Analysis of the attack provides several benefits. The user and administrator can determine the shortcomings in existing security policies, installation methods and configurations that allow attacks to succeed. Users and administrators should periodically review existing installations, configurations and security policies. New attacks and security vulnerabilities are found often and updating the existing environment can minimize the threats of future attack.

1.9 DIGITAL FORENSICS

Digital forensics is a key component in Cyber Security. Many people hear the term forensics, or computer forensics, or digital forensics and instantly think, that’s just for law enforcement, but the truth is, digital forensics has a key place on every cyber security team. In fact, without it, chances are your organizations Security posture and maturity will fail to see its full potential.

Digital forensic practices stem from forensic science, the science of collecting and examining evidence or materials. Digital or computer forensics focuses on the digital domain including computer forensics, network forensics, and mobile forensics.

In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law. Far too many cyber-attacks are occurring across the globe where laws are

clearly broken and due to improper or non-existent forensic investigations, the cyber criminals go either unidentified, undetected, or are simply not prosecuted.

- Malware Forensics

Malware is a type of software intentionally designed with malicious functionalities. The goal of malware forensics is to find out:

- What the malware can do (and what it does in a particular situation)
- To which family it belongs to (ransomware, keyloggers, remote administration tools)
- How it can be detected and blocked, and
- How it can be cleanly removed from an infected system

To achieve these goals, there are two approaches: static analysis and dynamic analysis. Each approach has its own pitfalls and advantages. Static analysis examines the binary without running it. It is the only option when the malware cannot be run, i.e. taken from a partial memory dump, missing pieces, or having an unavailable architecture. It tells the analyst everything the program can do, but this approach is less precise because of the need to reason about the program behavior without actually executing the code. By contrast, it achieves a larger coverage: one can reason about all possible executions at the same time. Dynamic analysis runs the program and observes its behaviour. It tells the analyst exactly what the program does when it is executed in a given environment and with a particular input. It is more precise because it can observe the instructions executed and the values of registers and memory; however, it achieves a smaller coverage because it observes one execution path at the time.

A general approach to malware analysis would be:

1. Set up a controlled, isolated laboratory in which to examine the malware sample
2. Perform behavioral analysis to examine the sample’s interactions with its environment
3. Perform static code analysis to further understand the sample’s inner workings

4. Perform dynamic code analysis to understand the more difficult aspects of the code
5. If necessary, unpack the sample
6. Repeat steps 2, 3, and 4 (order may vary) until analysis objectives are met
7. Document findings and clean up the laboratory for future analysis

The following section describes each step with the common and popular tools used to achieve the goal.

Examining malicious software involves infecting a system with the malware sample and then using the appropriate behaviour analysis tools to observe its interaction with the system. This requires an isolated laboratory environment that you can infect without affecting your production environment. The most common and flexible way is to use virtualization software (e.g., VMware or VirtualBox).

To understand the threat associated with the sample, the analyst needs to examine its behaviour in the controlled environment already setup in the previous step. He uses Process Monitor to study the process, network, file, and registry interactions between the malware and the operating system.

Process Monitor is a common tool for capturing the following events:

Registry: Capture registry keys query, read, and creation operations.

File system: File creation, writing, deletion from local hard drives and network drives.

Network: Show the source and destination of TCP/UDP traffic, but it doesn't show the data.

Analysts use Wireshark to capture data. Packets can be filtered based on source destination IP/port by Process Monitor.

Process: Shows processes and threads creation and exit, etc.

Profiling: Checks the amount of CPU time used by each process or the malware being studied and the memory use.

- Is the malware a known binary?

To check if the sample is a known binary based on its hash or if it is similar to something already known based on its signature, the analyst could submit it to VirusTotal. VirusTotal is a sandbox tool for malware identification owned by Google. The tool has the biggest repository of malware and known file types around.

Malicious binaries are typically stripped of all symbols, obfuscated and packed. In addition, they implement plenty of anti-debugging and anti-analysis tricks and checks for analysis environments. Packing a program is compressing or encrypting the instructions and data in order to save disk space. It's widely used by malware writers. Many packers automatically include anti-disassembly, anti-debugging, and anti-VM techniques to further complicate the analysis.

The packer can be identified based on its signature or by using heuristics. PEiD is a popular tool that can identify most common packers, cryptors, and compilers for PE files. It packs more than 600 different signatures in PE files, which make its detection rate higher than that of other similar tools.

There are several heuristic techniques to determine whether a program is packed, including sections with high entropy, weird section names, and few entries in the import table, etc. Mandiant's Red Curtain tool computes entropy of sections. High entropy means that the program is likely packed or encrypted. The tool also scans for packing signatures and computes a threat score.

There are several approaches to unpacking a program. One first approach could be to manually reverse-engineer the packing stub and write the corresponding unpacking tool, but this is complex and time-consuming. An automatic and dynamic approach could be dumping the binary containing the unpacked program. In a few cases, the program can be unpacked automatically using a tool (e.g., the UPX tool, using –d option). PEiD comes with a set of plugins, including an UPX unpacker.

Disassemblers are among the tools that can be used to statically analyze binary programs and further understand the malware's inner workings. These tools do not require the analyzed module to operate; it can be safer to use static analysis if it is known that the module under analysis is malicious. A disassembler converts machine language into assembly language. IDAPro is popular tool for doing this job.

In order to determine the higher-level logic of a function, such as loops, switches, and conditions, the malware analyst can use a decompiler. A decompiler converts

assembly code into source code in a higher-level language such as C++ or C. Paid versions of IDAPro come with a C/C++ decompiler called Hex-Rays Decompiler. An alternative is to use a similar tool called Snowman.

The last step is to document the findings and analysis results in a report that summarizes the answers to the predefined questions. The analysis report covers, but not limited to, screenshots, notes, and observations.

- Memory Forensics

Memory forensics is the process of investigating a memory dump to locate malicious behaviors. The dump is a snapshot capture of RAM memory at a specific point of time; it can be a full physical memory dump, a crash dump, or a hibernation file.

The investigator extracts useful artifacts from memory, including running processes, URLs, passwords, encryption keys, kernel modules, shared libraries, open sockets, active connections, and open registry keys. That information can be accessed by obtaining and analyzing the target computer's physical memory dump.

A general approach to memory forensics would acquire and analyze physical memory.

Memory dump acquisition: can be performed using a program installed on the system, such as win32dd, win64dd, dumpit, or dd or by using dedicated hardware such as an internal acquisition card (PCI card), or sniffing direct memory access (DMA) transfer, or using a FireWire port. The difference is that the software may alter the system, in contrast to the use of hardware. However, using hardware may crash the system or lose information, in the case of FireWire. In addition, the hardware must be installed on the machine before an incident occurs.

Memory dump analysis: Many tools offer digital artifacts and analysis facilities. Volatility is the most popular memory forensics framework. It can extract digital artifacts from multiple types of memory (crash dump, core dump, hibernation file, etc). It provides an in-depth visibility into the runtime state of the system. Rekall is an advanced memory analysis solution. It is basically a fork of the Volatility memory analysis framework maintained by Google's incidence response team.

To start the analysis, summary information of the dump can be viewed. This information includes the operating system version and target architecture (32 or 64

bits). The most commonly used analysis approach then is to list the processes that were running in the system, the loaded kernel modules, and shared libraries to locate malicious modules. The analysis can also cover other data, such as registry keys.

In addition to the active processes, the analyst should keep track of terminated and hidden processes, since they might also load malicious modules.

The analysis may end when malicious files are dumped. Then malicious file analysis comes to play as described in the previous section.

- Email Forensics

Emails are the main channel for worms, phishing, and the transportation of spam. Email forensics involves investigating email content and sources to reveal key information, such as the recipient's identity, the trace path traversed by the message, the application used to compose the email, the timestamp when a message was generated, a unique message ID, etc.

Typically, email forensics consists of the following steps:

- Examining sender's e-mail address
- Examining message initiation protocol (HTTP, SMTP)
- Examining message ID
- Examining sender's IP address

This involves investigation of port scanning metadata and keyword searching.

There are several approaches to email forensics such as header analysis, server investigation, client-side mailer fingerprint, network devices investigation, and bait tactics.

Many tools may assist in the study of source and content of e-mail message so that an attack or the malicious intent of the intrusions may be investigated. The following is a non-exhaustive list of email forensics tools:

- MailXaminer
- Add4Mail
- eMailTrackerPro

    - AccessData's FTK
    - Paraben E-Mail Examiner
- Smartphone Forensics

Smartphone devices contain sensitive personal information such as contact lists, SMSs, calls, pictures, etc. This information can be used by attackers to impersonate the owner's identity, so it is risky if it is lost or stolen. That's why smartphones become an inevitable source for digital forensics. There are three primary approaches to smartphone forensics which focus on extraction of data that might be rightly challenged in a court of law.

General approaches to smartphone forensics

Manual Acquisition: The investigator browses the smartphone and takes pictures of each screen that contains important information. This technique does not alter the device and no tools are required to perform data acquisition. However, only data visible to the investigator can be recovered since only the user interface is used.

Physical Acquisition: The investigator clones the smartphone storage device and then normal disk forensic techniques are used (see Disk Forensics section).

Logical Acquisition: In this technique, little manual intervention or cloning is required. Here data available on the smartphone is acquired by automated tools for synchronizing the device and PC. With this technique, the investigator can't acquire deleted data and unallocated spaces.

The following is a list of the popular tools available for smartphone forensics:

    - Andriller
    - XRY
    - Oxygen Forensic
    - Ufed Touch
    - Droidspotter
    - Mobiledit Forensic
- Disk Forensics

The goal of disk forensics is to acquire a copy of data resident on hard drives and USB memory sticks, analyzing it to extract digital evidence. The acquisition can be performed at the file level or the sector level. At the file level, the investigator can't acquire deleted files and unallocated spaces. At the sector level, however, the investigator can acquire an exact copy of the device storage. If the storage is corrupt or damaged, then the investigator relies on file carving, which may recover data if the files' metadata are lost. The most popular tools are the Sleuth Kit, Digital Forensic Framework, FTK, and EnCase.

- Cloud Forensics

Cloud forensics involves inspecting cloud components, which include logs, virtual machine disk images, volatile memory dumps, console logs, and network captures. Cloud forensic tools collect data from the cloud, image the instances, and recover data from cloud instances. FROST is a forensics tool for OpenStack.

- Log Forensics

Logs generated by the operating systems and applications are segregated and parsed to generate useful information. Correlation mechanisms are applied to find relationships between logs and external or internal events.

1.10 COMPUTER LANGUAGE

Programming languages for Web Hacking and Pentesting

If you're interested in web hacking and pentesting, then you must learn learn below mentioned languages at-least basic and intermediate level.

1. HTML

   Always begin with basics and HTML — HyperTextMarkup Language — should be the first one you should learn as a beginner. HTML is the building blocks of the internet and an ethical hacker should know it very well to understand web action, response, structure, and logic. Also, learning HTML is not at all that tough.

2. JavaScript

   JavaScript — JavaScript is the most used as client-side programming and for web development is also the best programming language for hacking web applications.

In fact, it is the best programming language for hackers and security experts for developing cross-site scripting hacking programs.

You should learn it on high priority mode. Understanding JavaScript code logic can help you find the web-apps flaws and it is the best one to manipulate both front-end and back-end web components.

3. SQL

   SQL — Structured Query Language — is a database programming language used to query and fetch information from databases. All big and small websites and web apps are using databases to store data like login credentials and other valuable inventories — it is the most sensitive part of the Web. So a hacker must learn SQL to communicate with databases and to develop hacking programs based on SQL injection.

4. PHP

   PHP is the most popular dynamic programming language, used mainly by websites build upon popular CMS like WordPress. So knowing PHP will help you to find vulnerabilities in such network and take down a personal website or blog. Hackers use PHP mainly for developing server hacking programs as it is a server-side scripting language. So, if you are into web hacking then deeper knowledge in PHP is necessary.

5. Perl

   Perl is an important programming language for hacking to compromise old machines since many old systems still use Perl. Perl is worth learning for practical reasons — it’s very widely used for active web pages and system administration, best available language for manipulating text files on Unix systems and integration with popular web-databases. So that even if you never write Perl you should learn to read it.

   Programming Languages for writing Exploits

   Exploit writing is an advance part of hacking. It requires a higher level of programming language. Every professional hacker must know to exploit writing. It can be done in any programming language like C, C++, Ruby, Python, etc.

6. C

The mother of all programming language, C is the most important programming language used in creation for Linux and Windows. So learning C programming will help an ethical hacker to understand the way of working of these systems — like how CPU and memory interact with each other.

However, it is the best programming language for exploit writing and development. The low-level nature of C benefits security experts to develop hacking programs to access and manipulate system hardware and lower level resources.

7. C++

C++ is one of the best programming languages for hacking software comes under a proprietary license and require paid activation. Like C, C++ also gives the low-level of access to the system and helps to analyze the machine code and bypass such activation schemes. Also, many modern hacking programs are built on C++.

8. Python

Unlike any other programming language listed here, Python is the easiest one to learn. It is the most used language for exploit writing as Python is the easiest programming language to write automation scripts because of pre-built libraries with some powerful functionality.

Also “run without compilation” nature of Python makes its an essential programming language for hackers to take down web servers. It is highly recommended you to learn Python Socket Programming because it helps lot learning exploit creation.

9. Ruby

Ruby is a simple but complicated object-oriented programming language used in web development. Ruby is very useful in exploit writing. It is used for meterpreter scripting and do you know Metasploit Framework itself programmed in Ruby.

10. Java

Java is the most widely used programming language in the coding community. Java was originally released with the slogan “write once, run anywhere,” which was intended to underscore its cross-platform capabilities. Because of that Java

is the perfect programming language for hacking PC, mobile devices and web servers.

You can make tools using Java and it can also be used to create backdoor exploits as well as exploits that can kill a computer. Once you write your hacking programs with Java, you can run them on any platform that supports Java.

11. LISP

Lisp is the second-oldest high-level programming language in widespread use today. LISP is absolutely wide open, flexible and totally machine independent makes it hacker's favorite. You can define your own syntax and create any sort of programming paradigm you like and include it in your programs.

Programming languages for Reverse Engineering

Reverse engineering, also called back engineering, is the processes of extracting knowledge or design information from anything man-made and reproducing it or reproducing anything based on the extracted information. Reverse engineering is also beneficial in crime prevention, where suspected malware is reverse engineered to understand what it does, and how to detect and remove it, and to allow computers and devices to work together. Reverse engineering can also be used to "crack" software and media to remove their copy protection.

12. Assembly Language

Assembly is low level programming language but very complicated. One can instruct a machine hardware or software using Assembly language. Reverse Engineers uses Assembly language, and if you want to learn Reverse Eng, you must need to learn Assembly language.

Finally one more thing, programming languages for hacking also depends upon what program you want to hack, for example; if a web-app in coded in ASP.NET then you can't hack it using PHP knowledge, although you can understand logic but it will be harder, so always make sure what you wanna hack and in which programming the app is coded.

Also hacking is a skill and only talented well-trained could become a better security expert. So learn these programming languages to its core and hard-train your abilities to solve different coding problems.

1.11 NETWORK LANGUAGE

Network security is an integration of multiple layers of defenses in the network and at the network. Policies and controls are implemented by each network security layer. Access to networks is gained by authorized users, whereas, malicious actors are indeed blocked from executing threats and exploits.

Our world has presently been transformed by digitization, resulting in changes in almost all our daily activities. It is essential for all organizations to protect their networks if they aim at delivering the services demanded by employees and customers. This eventually protects the reputation of your organization. With hackers increasing and becoming smarter day by day, the need to utilize network security tool becomes more and more impotent.

Types of Network Security

1) Antivirus and Antimalware Software
2) Application Security
3) Behavioral Analytics
4) Data Loss Prevention (DLP)
5) Email Security
6) Firewalls
7) Intrusion Prevention System (IPS)
8) Mobile Device Security
9) Network Segmentation
10) Security Information and Event Management (SIEM)
11) Virtual Private Network (VPN)
12) Web Security
13) Wireless Security
14) Endpoint Security
15) Network Access Control (NAC)

1) Antivirus and Antimalware Software : This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses. Malware can also become very dangerous as it can infect a network and then remain calm for days or even weeks. This software handles this threat by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage.

2) Application Security: It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

3) Behavioral Analytics: In order to detect abnormal network behaviour, you will have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

4) Data Loss Prevention (DLP): Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures, that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

5) Email Security: Email gateways are considered to be the number one threat vector for a security breach. Attackers use social engineering tactics and personal information in order to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

6) Firewalls: Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed

to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

7) Intrusion Prevention System (IPS): An IPS is a network security capable of scanning network traffic in order to actively block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.
8) Mobile Device Security: Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to control which devices can access your network. It is also necessary to configure their connections in order to keep network traffic private.

9) Network Segmentation: Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The classifications are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.

10) Security Information and Event Management (SIEM): SIEM products bring together all the information needed by your security staff in order to identify and respond to threats. These products are available in different forms, including virtual and physical appliances and server software.

11) Virtual Private Network (VPN): A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPsec or Secure Sockets Layer in order to authenticate the communication between network and device.

12) Web Security: A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites, and blocking

13) Wireless Security: The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

14) Endpoint Security: Endpoint Security, also known Network Protection or Network Security, is a methodology used for protecting corporate networks when accessed through remote devices such as laptops or several other wireless devices and mobile devices. For instance, Comodo Advanced Endpoint Protection software presents seven layers of defense that include viruscope, file reputation, auto-sandbox, host intrusion prevention, web URL filtering, firewall, and antivirus software. All this is offered under a single offering in order to protect them from both unknown and known threats.

15) Network Access Control (NAC): This network security process helps you to control who can access your network. It is essential to recognize each device and user in order to keep out potential attackers. This indeed will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

- Technical Network Protection: Technical Network Protection is used to protect data within the network. Technical network protection guards both stored and in-transit data from malicious software and from unauthorized persons.
- Physical Network Protection: Physical Network Protection, or Physical Network Security, is a network security measure designed to prevent

unauthorized people from physically interfering with network components. Door locks and ID passes are essential components of physical network protection.

- Administrative Network Protection: Administrative Network Protection is a security method that control a user's network behaviour and access. It also provides a standard operating procedure for IT officers when executing changes in the IT infrastructure. Company policies and procedures are forms of Administrative network protection.

1.12 REALMS OF THE CYBER WORLD

The need for information security has ceased to be a subject of debate in technology circles. The expectations, the context and the need probably differ, however one sees a consensus on the need to secure and protect information. In the technology landscape, where jargon and acronyms occur as frequently as the tides that wash ashore, the term cyber security has grabbed a lot of attention. International Telecommunication Union (ITU) refers to cyber security as – 'Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.' Professionals, enterprises and even nations seem to focus on cyber security today. While the people at large may not ponder much, for IT professionals it may raise a few questions. Some of them are likely to be -are the terms information security and cyber security synonyms, if not what's the difference? Is cyber security is a sub set of information security or are the two entirely different? Multiple definitions that allude to the different views on cyber security are likely to be available. However it is important that we understand the core behind cyber security than get hindered by the definitions. The focus on threats, risks and controls relevant to the cyber world is the realm of cyber security. This does not mean that security in the cyber world was not addressed in the information security legacy that we inherited and that has developed over the years. The footprint of the 'cyber' aspect though, was rather limited. This limited focus was not deliberate but merely reflected the reality of the

day where connectivity to cyber space was less extensive and controlled. Hence the risks posed by the cyber world were not as extensive as they are today.

Changes in the environment triggered a focus on cyber security. The changes have been varied and extensive. The changes have not been unidimensional but have encompassed a wide landscape. The traditional view about architecture, technology, its delivery and utilization have all changed. The holy grail of technology available to a few qualified professionals is now available to the world at large. Within a short span of time, innovative and unthinkable concepts like Bring Your Own Device (BYOD) and Mobility, Cloud Computing, Social Networks, Internet of Things (IoT) have become reality of the day. This imperative has been embraced for sure–in some instances with open arms and in few other cases grudgingly. The underlying enabler for the change is connectivity that has been provided by the cyber world. The innovative and diverse leveraging of the cyber world has increased the number of cyber citizens and also the traffic flows. The perimeter has traditionally been the frontier that separated the trusted internal network from the un-trusted external network. The gatekeepers in the form of layer 3-4 firewalls provided the much needed assurance and resilience to protect from external threats. In some instances it was complemented by Intrusion Detection/Prevention Systems. The ‘internal’ elements with patched end points and antivirus software fortified the network. Alas this simplistic model, though essential

Even today no longer provides the level of assurance it provided earlier. The BYOD program saw an influx of personal devices with a variety of operating systems. The enterprise no longer owned and controlled all the end points. The devices that traditionally were outside the trusted perimeter were now connected to the internal network. These devices tip toed inside the perimeter due to their physical proximity; however some devices even when physically remote became part of the trusted network. Virtualized servers hosted by IaaS and PaaS providers and applications provided by SaaS that are physically away from the perimeter need to be part of the trusted network. The traditional firewalls that had no visibility on the application layer were not much useful in regulating traffic to the cloud since IP addresses changed at irregular intervals.

Check Your Progress :

1. Define term Cyber Crime.
2. Explain the classification of Cyber Crime.
3. Short note on Hacking.
4. Define tem Cyber Space.
5. Describe Criminal behavior.
6. List out Traditional problems with Computer crimes.
7. Explain realms of Cyber world.

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Refer the Topic no 1.2.
2. Refer the Topic no 1.3.
3. Refer the Topic no 1.4.
4. Refer the Topic no 1.5.
5. Refer the Topic no 1.5.
6. Refer the Topic no 1.7.
7. Refer the Topic no 1.12.

1.14 FURTHER READING

- Read the Cyber Crime topic related book.

Unit 2: Internet crime and Act

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 A Brief History of the Internet

2.4 Recognizing and Defining Computer Crime

2.5 Contemporary Crimes

2.6 Indian IT ACT 2000

2.7 Digital Evidences & Chain of Custody

2.8 Check your Progress: Possible Answers

2.1 LEARNING OBJECTIVES

After study this student can learn:

- Internet crime and Act: A Brief History of the Internet,
- Recognizing and Defining Computer Crime,
- Contemporary Crimes, Computers as Targets, Contaminants and Destruction of Data,
- Indian IT ACT 2000.,
- Digital Evidences, Chain of Custody
- Intellectual Property in the Cyberworld

2.2 INTRODUCTION

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software licence is controversial and still evolving in Europe and elsewhere.

2.3 A BRIEF HISTORY OF THE INTERNET

According to Ministry of Electronic and Information Technology, Government of India

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

➢ Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

- Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

- Fraud:

Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

- Copyright:

The internet has made copyright violations easier. In early days of online communication, copyright violations was too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

- Defamation:

Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

- Harassment and Stalking:

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

➢ Freedom of Speech:

Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

➢ Trade Secrets:

Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

➢ Contracts and Employment Law:

Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

➢ Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notification on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application or any other document with any office, authority, body or agency owned or controlled by the suitable Government in e-form by means of such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

2.4 RECOGNIZING AND DEFINING COMPUTER CRIME

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

- What is the importance of Cyberlaw ?

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

- Does Cyberlaw concern me ?

Yes, Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyberlegal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

- Copyright Infringement through internet

Internet has become a breeding ground for violation of copyright. This mass misuse require more stringent laws.

2.5 CONTEMPORARY CRIMES

- Cyber Stalking: Challenges in Regulating Cyber Stalking At The Cyber Space

  What Is Cyber Stalking? There is no universal accepted definition of cyber stalking. The word stalking means ‘pursue stealthily' which refers that "harass obviously".

- Policy Hampering Illegal Data Entry Via Apps/Social Media
  How do you feel if someone unknowingly spies on your credit card number online? Won’t it get on your nerves? It definitely would come out as a blast of impulsiveness. Nobody, actually, likes to keep a watch on what indeed is so sensitive.

- Data Exclusivity A Necessary Evil
  Data Exclusivity refers to a practice whereby, for a fixed period of time, drug approval authorities do not allow the test data of the innovator company to be used to register equivalent generic version of that medicine.

- Computer Law
  Data Exclusivity Law: Data exclusivity is a matter of heated controversy now-a-days all over the world and a source of tussle between developing and developed countries

- Legal Dimensions of Information Technology - issues of copyright: It is related to the cyber world and the main focus is given on the issues such as the cyber crimes, right to information and the copyright issues.

- Digital Signatures: Digital Signatures have been provided for in the Information Technology Act, 2000, to bring about a minimum level of security in the increasing amount of data transfer over the Internet

- Electronic agents: Undoubtedly, the influences of IT (‘Information Technology’) have already invaded every corner of our daily lives. Nowadays, it is unimaginable if one determines not to relevant with this new technology at all.

- Data Theft in Cyber Space: This Article highlights the suseptibilty of data to theft in the digital age. It analyses as to what are the current provisions in the existing law on such theft and whether it can be brought under the ambit of the Indian Penal Code, 1860.
- Identity Theft: All across India, the fastest growing White Collar Crime in the nation has been identified as Identity Theft and its affecting each one of us in insidious ways
- Breach of privacy and Confidentiality: The article deals with Section 72 of the Information Technology Act, 2000 which speaks about penalty for Breach of Confidentiality and privacy
- Cyber Crimes and Cyber Law: Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology
- Cyber Terrorism and Various Legal Compliances: Terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience.
- Advertising - Its Evolution, Significance & Effects.
- Plagiarism: works created by other people is rightfully their intellectual property and if we use that work we are bound to
- Cyber Crimes and General Principles: Basic overview of the concept of cyber crimes and how the concept is different from the traditional principles of criminal law.
- Cyber Squatting- Clear and Present Danger: In the new e-economy it is commercially prudent for a company to have an easily traceable address in the cyber-space
- Cyber Crime And Law: contributes an understanding of the effects of negative use of Information technology
- Cyber Hacking: 'Hackers' are very intelligent people who use their skill in a constructive and positive manner

- Electronic Contract: traditional notion of contract formation, negotiating parties must come to a "meeting of the minds"
- The Bpo Strategy: Business Process Outsourcing (BPO) is a buzzword among the corporate in the world today.
- Need For Conversion Of The Convergence Bill: The Communication Convergence Bill, is on the verge of being enacted and changing the Indian communication machinery
- Data Safety And Privacy Protection: As the situation now warranty legislation of data protection in India, visitors to any website want reassurances that privacy rights
- The Menace of Cyber Crime: In the information age the rapid development of computers, telecommunications and other technologies has led
- Cyber-Elections: Its in-serverability has grown to such heights that perhaps George Bernard Shaw would have expressed as ‘Cyber-web here
- Defamation on the web: Who do you sue?: The law of defamation addresses harm to a person's reputation or good name through slander and libel.
- Internet telephony and related Issues: The focus of the article is to examine the impact of the proposed Communications Convergence.

2.6 INDIAN IT ACT 2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the UNCITRAL Model Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000. The bill was finalised by group of officials headed by then Minister of Information Technology PramodMahajan.

The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cyber crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of the Indian Penal Code, 1860, the Indian, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

A major amendment was made in 2008. It introduced Section 66A which penalized sending of "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced provisions addressing child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in LokSabha. The next day it was passed by the RajyaSabha. It was signed into law by President PratibhaPatil, on 5 February 2009.

Offences

List of offences and the corresponding penalties:

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system	Imprisonment up to three years, or/and with fine up to ₹200,000

		or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up

			to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images	If a person publishes or	Imprisonment up to

	containing sexual acts	transmits images containing a sexual explicit act or conduct.	seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who	Imprisonment up to three years, or/and with fine up to ₹200,000

		fails to comply with any such order shall be guilty of an offence.	
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.

70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

2.7 DIGITAL EVIDENCES & CHAIN OF CUSTODY

➢ **Section 66**

- In February 2001, in one of the first cases, the Delhi police arrested two men running a web-hosting company. The company had shut down a website over

non-payment of dues. The owner of the site had claimed that he had already paid and complained to the police. The Delhi police had charged the men for hacking under Section 66 of the IT Act and breach of trust under Section 408 of the Indian Penal Code. The two men had to spend 6 days in Tihar jail waiting for bail. BhavinTurakhia, chief executive officer of directi.com, said that this interpretation of the law would be problematic for web-hosting companies.

- In February 2017, M/s Voucha Gram India Pvt. Ltd, owner of Delhi based Ecommerce Portal www.gyftr.com made a Complaint with HauzKhas Police Station against some hackers from different cities accusing them for IT Act / Theft / Cheating / Misappropriation / Criminal Conspiracy / Criminal Breach of Trust / Cyber Crime of Hacking / Snooping / Tampering with Computer source documents and the Web Site and extending the threats of dire consequences to employees, as a result four hackers were arrested by South Delhi Police for Digital Shoplifting.

➢ **Section 66A**

- In September 2012, a freelance cartoonist AseemTrivedi was arrested under the Section 66A of the IT Act, Section 2 of Prevention of Insults to National Honour Act, 1971 and for sedition under the Section 124 of the Indian Penal Code. His cartoons depicting widespread corruption in India were considered offensive.
- On 12 April 2012, a Chemistry professor from Jadavpur University, AmbikeshMahapatra, was arrested for sharing a cartoon of West Bengal Chief Minister Mamata Banerjee and then Railway Minister Mukul Roy.The email was sent from the email address of a housing society. SubrataSengupta, the secretary of the housing society, was also arrested. They were charged under Section 66A and B of the IT Act, for defamation under Sections 500, for obscene gesture to a woman under Section 509, and abetting a crime under Section 114 of the Indian Penal Code.
- On 30 October 2012, a Puducherry businessman Ravi Srinivasan was arrested under Section 66A. He had sent tweet accusing Karti Chidambaram,

son of then Finance Minister P. Chidambaram, of corruption. Karti Chidambaram had complained to the police.

- On 19 November 2012, a 21-year-old girl was arrested from Palghar for posting a message on Facebook criticising the shutdown in Mumbai for the funeral of Bal Thackeray. Another 20-year-old girl was arrested for "liking" the post. They were initially charged under Section 295A of the Indian Penal Code (hurting religious sentiments) and Section 66A of the IT Act. Later, Section 295A was replaced by Section 505(2) (promoting enmity between classes). A group of Shiv Sena workers vandalised a hospital run by the uncle of one of girls.[19] On 31 January 2013, a local court dropped all charges against the girls.
- On 18 March 2015, a teenaged boy was arrested from Bareilly, Uttar Pradesh, for making a post on Facebook insulting politician Azam Khan. The post allegedly contained hate speech against a community and was falsely attributed to Azam Khan by the boy. He was charged under Section 66A of the IT Act, and Sections 153A (promoting enmity between different religions), 504 (intentional insult with intent to provoke breach of peace) and 505 (public mischief) of Indian Penal Code. After the Section 66A was repealed on 24 March, the state government said that they would continue the prosecution under the remaining charges.

➢ **Criticisms**

- **Section 66A and restriction of free speech**

From its establishment as an amendment to the original act in 2008, Section 66A attracted controversy over its unconstitutional nature:

Section	Offence	Description	Penalty
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information	Imprisonment up to three years, with fine.

		which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	

In December 2012, P Rajeev, a RajyaSabha member from Kerala, tried to pass a resolution seeking to amend the Section 66A. He was supported by D. Bandyopadhyay, GyanPrakashPilania, BasavarajPatilSedam, Narendra Kumar Kashyap, Rama Chandra Khuntia and BaishnabCharanParida. P Rajeev pointed that cartoons and editorials allowed in traditional media, were being censored in the new media. He also said that law was barely debated before being passed in December 2008.

Rajeev Chandrasekhar suggested the 66A should only apply to person to person communication pointing to a similar section under the Indian Post Office Act, 1898. ShantaramNaik opposed any changes, saying that the misuse of law was sufficient to warrant changes. Then Minister for Communications and Information Technology KapilSibal defended the existing law, saying that similar laws existed in US and UK. He also said that a similar provision existed under Indian Post Office Act, 1898. However, P Rajeev said that the UK dealt only with communication from person to person.

- **Petitions challenging constitutionality**

In November 2012, IPS officer Amitabh Thakur and his wife social activist Nutan Thakur, filed a petition in the Lucknow bench of the Allahabad High Court claiming that the Section 66A violated the freedom of speech guaranteed in the Article 19(1)(a) of the Constitution of India. They said that the section was vague and frequently misused.

Also in November 2012, a Delhi-based law student, ShreyaSinghal, filed a Public Interest Litigation (PIL) in the Supreme Court of India. She argued that the Section 66A was vaguely phrased, as result it violated Article 14, 19

(1)(a) and Article 21 of the Constitution. The PIL was accepted on 29 November 2012.A similar petition was also filed by the founder of MouthShut.com, Faisal Farooqui, and NGO Common Cause represented by PrashantBhushan[28] In August 2014, the Supreme Court asked the central government to respond to petitions filed by Mouthshut.com and later petition filed by the Internet and Mobile Association of India (IAMAI) which claimed that the IT Act gave the government power to arbitrarily remove user-generated content.

- **Revocation by the Supreme Court**

  On 24 March 2015, the Supreme Court of India, gave the verdict that Section 66A is unconstitutional in entirety. The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech" provided under Article 19(1) of the Constitution of India. But the Court turned down a plea to strike down sections 69A and 79 of the Act, which deal with the procedure and safeguards for blocking certain websites.

- **Strict data privacy rules**

  The data privacy rules introduced in the Act in 2011 have been described as too strict by some Indian and US firms. The rules require firms to obtain written permission from customers before collecting and using their personal data. This has affected US firms which outsource to Indian companies. However, some companies have welcomed the strict rules, saying it will remove fears of outsourcing to Indian companies.

- **Section 69 and mandatory decryption**

  The Section 69 allows intercepting any information and ask for information decryption. To refuse decryption is an offence. The Indian Telegraph Act, 1885 allows the government to tap phones. But, according to a 1996 Supreme Court verdict the government can tap phones only in case of a "public emergency". But, there is no such restriction on Section 69.On 20 December 2018, the Ministry of Home Affairs cited Section 69 in the issue of an order authorising ten central agencies to intercept, monitor, and decrypt “any information generated, transmitted, received or stored in any computer.” While some claim this to be a violation of the fundamental right to

privacy, the Ministry of Home Affairs has claimed its validity on the grounds of national security.

- **The Concept of E-Evidence in India**

Due to enormous growth in e-governance throughout the Public & Private Sector and e-commerce activities Electronic Evidence have involved into a fundamental pillar of communication, processing and documentation. The government agencies are opening up to introduce various governance policies electronically and periodical filings to regulate and control the industries are done through electronic means. These various forms of Electronic Evidence/ Digital Evidence are increasingly being used in the judicial proceedings. At the stage of trial, Judges are often asked to rule on the admissibility of electronic evidence and it substantially impacts the outcome of civil law suit or conviction/acquittal of the accused. The Court continue to grapple with this new electronic frontier as the unique nature of e-evidence, as well as the ease with which it can be fabricated or falsified, creates hurdle to admissibility not faced with the other evidences. The various categories of electronic evidence such as CD, DVD, hard disk/ memory card data, website data, social network communication, e-mail, instant chat messages, SMS/MMS and computer generated documents poses unique problem and challenges for proper authentication and subject to a different set of views.

The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000 (Before amendment). Section 3 of the Act was amended and the phrase “All documents produced for the inspection of the Court” were substituted by “All documents including electronic records produced for the inspection of the Court”. Regarding the documentary evidence, in Section 59, for the words “Content of documents” the words “Content of documents or electronic records” have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence.

Under the provisions of Section 61 to 65 of the Indian Evidence Act, the word “Document or content of documents” have not been replaced by the word “Electronic documents or content of electronic documents”. Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61 to 65 to the electronic record. It is the cardinal principle of interpretation that if the legislature has

omitted to use any word, the presumption is that the omission is intentional. It is well settled that the Legislature does not use any word unnecessarily. In this regard, the Apex Court in Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa held that "...Parliament is also not expected to express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for. Parliament cannot be assumed to legislate for the sake of legislation; nor indulge in legislation merely to state what it is unnecessary to state or to do what is already validly done. Parliament may not be assumed to legislate unnecessarily."

The intention of the legislature is to introduce the specific provisions which has its origin to the technical nature of the evidence particularly as the evidence in the electronic form cannot be produced in the court of law owing to the size of computer/server, residing in the machine language and thus, requiring the interpreter to read the same. The Section 65B of the Evidence Act makes the secondary copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible. It provides: -

- Section 65B - Admissibility of Electronic Records

  Sec. 65B(1): Notwithstanding anything contained in this Act, any information contained in an electronic record -

  • which is printed on a paper, stored, recorded or

  • copied in optical or magnetic media

  • produced by a computer

  # shall be deemed to be also a document, if the conditions mentioned in this section are satisfied

  • in relation to the information and

  • computer in question and

  # shall be admissible in any proceedings, without further proof or production of the original,

  # as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

- Sec. 65B(2):

  # The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

  # Information was fed in computer in the ordinary course of the activities of the person having lawful control over the computer;

  # The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

  # Information reproduced is such as is fed into computer in the ordinary course of activity.

- Sec.65 B(3):

  The following computers shall constitute as single computer-

  # by a combination of computers operating over that period; or

  # by different computers operating in succession over that period; or

  # by different combinations of computers operating in succession over that period; or

  # in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

- Sec. 65B(4):

  Regarding the person who can issue the certificate and contents of certificate, it provides the certificate doing any of the following things:

  - identifying the electronic record containing the statement and describing the manner in which it was produced;
  - giving the particulars of device
  - dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

This contention is further strengthened by the insertion words “Notwithstanding anything contained in this Act” to Section 65A & 65B, which is a non-obstante clause, further fortifies the fact that the legislature has intended the production or exhibition of the electronic records by Section 65A & 65B only. A non-obstante clause is generally appended to a Section with a view to give the enacting part of the Section, in case of conflict, an overriding effect over the provision in the same or other act mentioned in the non-obstante clause. It is equivalent to saying that despite the provisions or act mentioned in the non-obstante clause, the provision following it will have its full operation or the provisions embraced in the non-obstante clause will not be an impediment for the operation of the enactment or the provision in which the non-obstante clause occurs.

The aforesaid principles of interpretation with respect to the non-obstante clause in form of “Notwithstanding anything contained in this Act” is further supported by the Hon’ble Apex Court in Union of India and Anr., v. G.M. Kokil and Ors. observed “It is well-known that a non obstante clause is a legislative device which is usually employed to give overriding effect to certain provisions over some contrary provisions that may be found either in the same enactment or some other enactment, that is to say, to avoid the operation and effect of all contrary provisions.” Further, the Hon’ble Apex Court in the case cited as ChandavarkarSitaRatnaRao v. Ashalata S. Guram , explained the scope of non-obstante clause as “...It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned in the non obstante clause or any contract or document mentioned the enactment following it will have its full operation..."

- What Is the Chain of Custody in Computer Forensics?

  The chain of custody in digital forensics can also be referred to as the forensic link, the paper trail, or the chronological documentation of electronic evidence. It indicates the collection, sequence of control, transfer, and analysis. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

- Why Is It Important to Maintain the Chain of Custody?

  It is important to maintain the chain of custody to preserve the integrity of the evidence and prevent it from contamination, which can alter the state of the evidence. If not preserved, the evidence presented in court might be challenged and ruled inadmissible.

- Importance to the Examiner

  Suppose that, as the examiner, you obtain metadata for a piece of evidence. However, you are unable to extract meaningful information from it. The fact that there is no meaningful information within the metadata does not mean that the evidence is insufficient. The chain of custody in this case helps show where the possible evidence might lie, where it came from, who created it, and the type of equipment that was used. That way, if you want to create an exemplar, you can get that equipment, create the exemplar, and compare it to the evidence to confirm the evidence properties.

- Importance to the Court

  It is possible to have the evidence presented in court dismissed if there is a missing link in the chain of custody. It is therefore important to ensure that a wholesome and meaningful chain of custody is presented along with the evidence at the court.

- What Is the Procedure to Establish the Chain of Custody?

  In order to ensure that the chain of custody is as authentic as possible, a series of steps must be followed. It is important to note that, the more information a forensic expert obtains concerning the evidence at hand, the

more authentic is the created chain of custody. Due to this, it is important to obtain administrator information about the evidence: for instance, the administrative log, date and file info, and who accessed the files. You should ensure the following procedure is followed according to the chain of custody for electronic evidence:

- Save the original materials: You should always work on copies of the digital evidence as opposed to the original. This ensures that you are able to compare your work products to the original that you preserved unmodified.
- Take photos of physical evidence: Photos of physical (electronic) evidence establish the chain of custody and make it more authentic.
- Take screenshots of digital evidence content: In cases where the evidence is intangible, taking screenshots is an effective way of establishing the chain of custody.
- Document date, time, and any other information of receipt. Recording the timestamps of whoever has had the evidence allows investigators to build a reliable timeline of where the evidence was prior to being obtained. In the event that there is a hole in the timeline, further investigation may be necessary.
- Inject a bit-for-bit clone of digital evidence content into our forensic computers. This ensures that we obtain a complete duplicate of the digital evidence in question.
- Perform a hash test analysis to further authenticate the working clone. Performing a hash test ensures that the data we obtain from the previous bit-by-bit copy procedure is not corrupt and reflects the true nature of the original evidence. If this is not the case, then the forensic analysis may be flawed and may result in problems, thus rendering the copy non-authentic.

The procedure of the chain of custody might be different. depending on the jurisdiction in which the evidence resides; however, the steps are largely identical to the ones outlined above.

- What Considerations Are Involved with Digital Evidence?

  A couple of considerations are involved when dealing with digital evidence. We shall take a look at the most common and discuss globally accepted best practices.

  - Never work with the original evidence to develop procedures: The biggest consideration with digital evidence is that the forensic expert has to make a complete copy of the evidence for forensic analysis. This cannot be overlooked because, when errors are made to working copies or comparisons are required, it will be necessary to compare the original and copies.
  - Use clean collecting media: It is important to ensure that the examiner's storage device is forensically clean when acquiring the evidence. This prevents the original copies from damage. Think of a situation where the examiner's data evidence collecting media is infected by malware. If the malware escapes into the machine being examined, all of the evidence can become compromised.
  - Document any extra scope: During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. It is recommended that this information be documented and brought to the attention of the case agent because the information may be needed to obtain additional search authorities. A comprehensive report must contain the following sections:
    1. Identity of the reporting agency
    2. Case identifier or submission number
    3. Case investigator
    4. Identity of the submitter
    5. Date of receipt
    6. Date of report
    7. Descriptive list of items submitted for examination, including serial number, make, and model
    8. Identity and signature of the examiner
    9. Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files

10. Results/conclusions
11. Consider safety of personnel at the scene. It is advisable to always ensure the scene is properly secured before and during the search. In some cases, the examiner may only have the opportunity to do the following while onsite:
12. Identify the number and type of computers.
13. Determine if a network is present.
14. Interview the system administrator and users.
15. Identify and document the types and volume of media, including removable media.
16. Document the location from which the media was removed.
17. Identify offsite storage areas and/or remote computing locations.
18. Identify proprietary software.
19. Determine the operating system in question.
20. The considerations above need to be taken into account when dealing with digital evidence due to the fragile nature of the task at hand.

Check Your Progress 1:

1. List the history of Internet Crime.

2. How to recognise computer crime?

3. List out Contemporary Crimes.

4.Digital Evidences & Chain of Custody

2.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. Refer the Topic no 2.2.

2. Refer the Topic no 2.4.

3. Refer the Topic no 2.5.

4. Refer the Topic no 2.7.

Unit 3: Intellectual Property in the Cyberworld

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Intellectual Property in the Cyberworld

3.4 Check your Progress: Possible Answers

3.1LEARNING OBJECTIVE

This chapter used to study about Intellectual Property in the Cyberworld.

3.2INTRODUCTION

In common use, property is simply ‘one’s own thing’ and refers to the relationship between individuals and the objects which they see as being their own to dispense with as they see fit.

- Property is often conceptualized as the rights of ‘ownership’ as defined in law.
- Private property is that which belongs to an individual; public property is that which belongs to a community collectively or a State.

The term intellectual property reflects the idea that this subject matter is the product of the mind or the intellect, and that intellectual property rights may be protected at law in the same way as any other form of property.

- Intellectual property laws are territorial such that the registration or enforcement of IP rights must be pursued separately in each jurisdiction of interest.
- There are various kinds of tools of protection that come under the umbrella term ‘intellectual property’.

3.3 INTELLECTUAL PROPERTY IN THE CYBERWORLD

Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.

To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.

Today it is critical for every business to develop an effective and collaborative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined.

Various approaches and legislations have been designed by the law-makers to up the ante in delivering a secure configuration against such cyber-threats. However it is the duty of the intellectual property right (IPR) owner to invalidate and reduce such mala fide acts of criminals by taking proactive measures.

Important among these are the following:

- Patents
- Trademarks
- Geographical Indications
- Layout Designs of Integrated Circuits
- Trade Secrets
- Copyrights
- Industrial Designs

➢ **Copyright**

- Basic Concept
  - Copyright is a right given by law to the creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordingsto do or authorize the doing of certain acts with regard to their creations.
  - It is a kind of protection against unauthorized use or misuse of a work, but for a limited duration.
  - Generally the rights include the rights of authorship, reproduction, distribution, communication to the public, broadcasting, adaptation and translation.
  - In India, copyright is governed by the Copyright Act, 1957, the Copyright Rules, 1958 and the International Copyright Order, 1999.
  - The Copyright Act provides the basic law so far as copyrights are concerned, the Copyright Rules contain the rules and regulations as well

as various procedures and the International Copyright Order extends copyright protection to works of nationals of specified foreign countries.

- Rights Included in the term ‘Copyright’
  - Copyright is a bundle of rights and this bundle can bebroadly classified into two categories, viz. economicrights and moral rights.
  - Economic rights are so called because “they imply as arule that within the limitations set by the copyright lawthe owner of the copyright may make all public use of thework conditional on payment of remuneration”.

    (a) Right of Reproduction

    (b) Right to Issue Copies of a Work

    (c) Rights of Public Performance

    (d) Right of Communication to the Public

    (e) Adaptation Right

    (f) Translation Right

Check Your Progress 1:

1. Discuss Intellectual Property in the Cyberworld.

3.3 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. Refer the Topic no 3.3

BAOU
Education for All

स्वाध्यायः परम तपः

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in | Email : office.scs@baou.edu.in