UNIT I

Introduction to Hacking: Hacking, Types and phases of hacking, Introduction to Ports & Protocols: Ports, Protocols, Primary Network Types, Virtualization & Introduction to Kali Linux: Virtualization, Virtualization software, supported platforms, Introduction to Penetration Testing: Penetration test, Categories and Types of Penetration tests, Structure of Penetration Test Report.

Hacking:

“Gaining Unauthorized Access Into A System” Or We Can Also Say that main aim of Hacking "is “ To compromise the Security of a system in order to gain Access into it”

“A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system.”

What is the reason for having so many security issues?

- Lack of money
- Lack of time
- Lack of expertise
- Negligence
- Convenience
- Old systems
- Too complex systems
- 3rd party components

Why Hack Happens?

ATTACKS = MOTIVE (GOAL) + METHOD + VULNERABILITY

MOTIVE: - Information theft, manipulating data, Financial loss, Revenge, Ransom, Damaging Reputation.

Ethical hacking:

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.

The primary goal of ethical hacking is to improve the security of the target system by addressing and mitigating these vulnerabilities before they can be exploited by malicious actors.

Why **Ethical hacker**?

* To prevent hackers from gaining access

* To uncover vulnerabilities

* To strengthen the organization

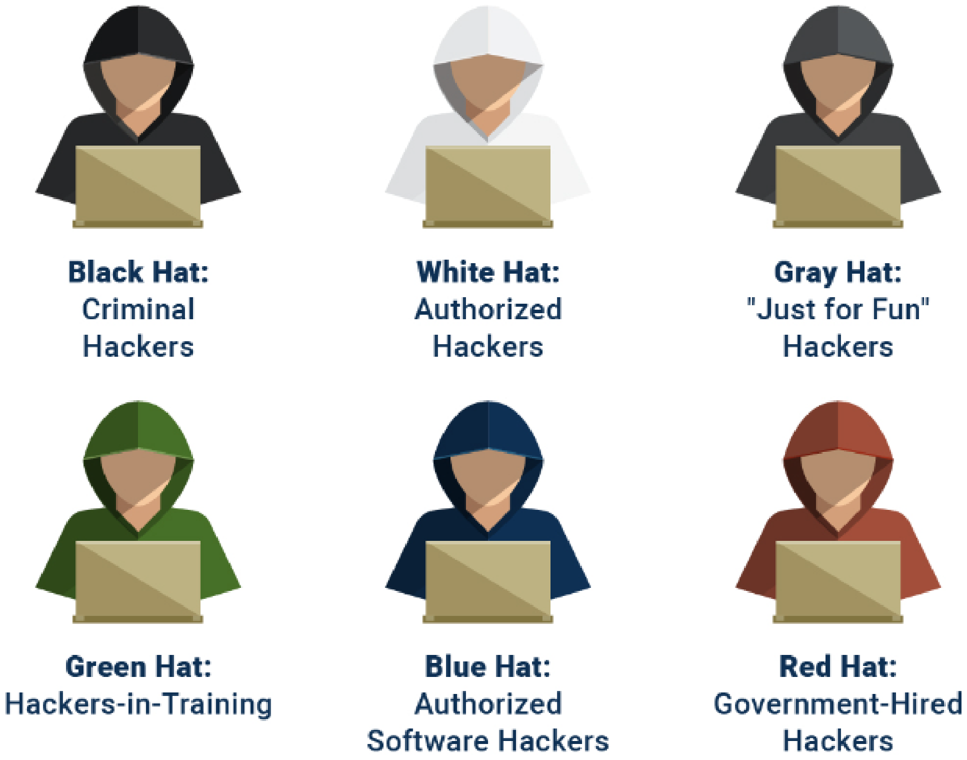
* To safeguard the data

* To avoid security Breaches

* To enhance security awareness

TYPES OF HACKERS:

Hackers can be categorized into different types based on their intentions, skills, and activities. Here are some common types of hackers:


Black Hat: Criminal Hackers
White Hat: Authorized Hackers
Gray Hat: "Just for Fun" Hackers
Green Hat: Hackers-in-Training
Blue Hat: Authorized Software Hackers
Red Hat: Government-Hired Hackers

Black Hat Hacker:

- Hacker who works offensively. They believe in breaking the security without any permission or authority. They are known as malicious hackers.
- Their activities can cause major damage to their targets and their systems.

- Black hats are usually involved with criminal activities such as stealing personal and financial information or shutting down websites and networks

White Hat Hacker:

- They work legally and are often employed by organizations to strengthen their cybersecurity defenses. They perform hacking and security checks with authority. They are known for security.
- White hat hackers think almost exactly like Black Hat hackers and will try to breach into computer systems using every possible way.
- However, they do not steal any information or cause disruption. White hat hacking techniques are extremely useful in looking for loopholes that may endanger confidential information.

Grey Hat Hacker:

- Hacker who is like a coin, two sided. They work for both offensive and defensive work. Generally benefit oriented.
- Grey hat hackers operate in a morally ambiguous space. They may uncover security flaws without permission but disclose them to the affected organization, sometimes in exchange for a fee or recognition. Their actions can be seen as both ethical and unethical, depending on the perspective.

Blue Hat:

- Tech companies hire blue hat hackers to test products and find security issues.
- These hackers typically have a background in cybersecurity and are invited by organizations to test their systems for vulnerabilities before a product launch or major update.
- They are similar to white hat hackers and are also usually external to the organization, providing an unbiased assessment of the system's security.

Red Hat:

- Red hats act aggressively to stop the black hats and employ some of their strategies. Government agencies hire red hats for their mission focus.
- They actively search for black hat hackers and shut them down. Whenever they find one, they don’t report the hacker to the authorities, but take matters into their own hands.

Green Hat:

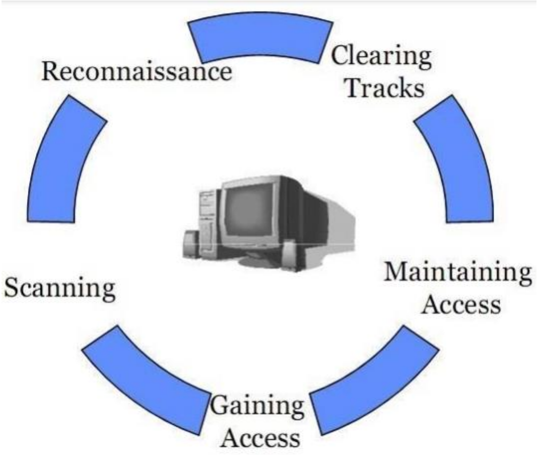
- These are the hacking beginners who want to become white, blue, or red hats (but hopefully not black hats).

- Green hat hackers are not aware of the security mechanism and the inner workings of the web, but they are keen learners and determined (and even desperate) to elevate their position in the hacker community

PHASES OF HACKING:

Hacking is an unauthorized and illegal activity that involves gaining unauthorized access to computer systems, networks, or data.

1. The Reconnaissance Phase.
2. The Scanning Phase.
3. The Gaining Access Phase.
4. The Maintaining Access Phase.
5. The Covering of Tracks Phase.



1. **Reconnaissance (Information Gathering):**

   - This is the first phase where the Hacker tries to collect information about the target. It can be done actively or passively. It brings us closer to the target by giving some sensitive information about target.
   - It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts.

Active Reconnaissance: In this process, you will directly interact with the computer system to gain information.

Passive Reconnaissance: In this process, you will not be directly connected to a computer system.

Usually, information about three groups is collected.

- Network
- Host
- People involved

2. Scanning:

- In this phase, Attacker finds much more information about Target. Attackers can perform port scanning or various assessments in order to get sensitive information about target.
- Hackers are seeking any information that can help them perpetrate attack suchas computer names, IP addresses, and user accounts

There are multiple tools like:

- network mappers
- dialers
- sweepers
- vulnerability scanners
- port scanners

that are utilized to scan data.

3. Gaining Access:

- In this phase, Attacker actually performs HACK. Using the information or vulnerability found by previous phases, attacker takes advantage and perform exploit to gain access.
- The hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data.
- The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline.
- Examples include stack based buffer overflows, denial of service (DoS), and session hijacking. These topics will be discussed in later chapters. Gaining access is known in the hacker world as owning the system.

4. Maintaining Access:

- Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks. Attacker installs backdoors or Trojans in order to maintain access into the target system.

- Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

5. Covering Tracks:

- In this phase, Attacker deletes the logs and session details in order to not be get caught. Once access is gained and privileges have been escalated, the hacker seeks to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc.

- Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunneling protocols, and altering log files.

PORTS & PROTOCOLS

PORTS:

- A port is logical access channel between two devices which helps in their communication.

- Ethical hackers often interact with ports as part of their security assessments to identify vulnerabilities and potential entry points into systems.

The following are some of the most common uses of ports:

- Intercepting network traffic
- Listening for and sending traffic
- Filtering packets on the fly
- Finding vulnerabilities

A port is used to transfer the data. There are total 65535 ports.

1. Well Known Ports : 0 to 1023
2. Registered Ports : 1024 to 49151
3. Dynamic/Private Ports : 49152 to 65535

1. Well Known Ports (0 to 1023):

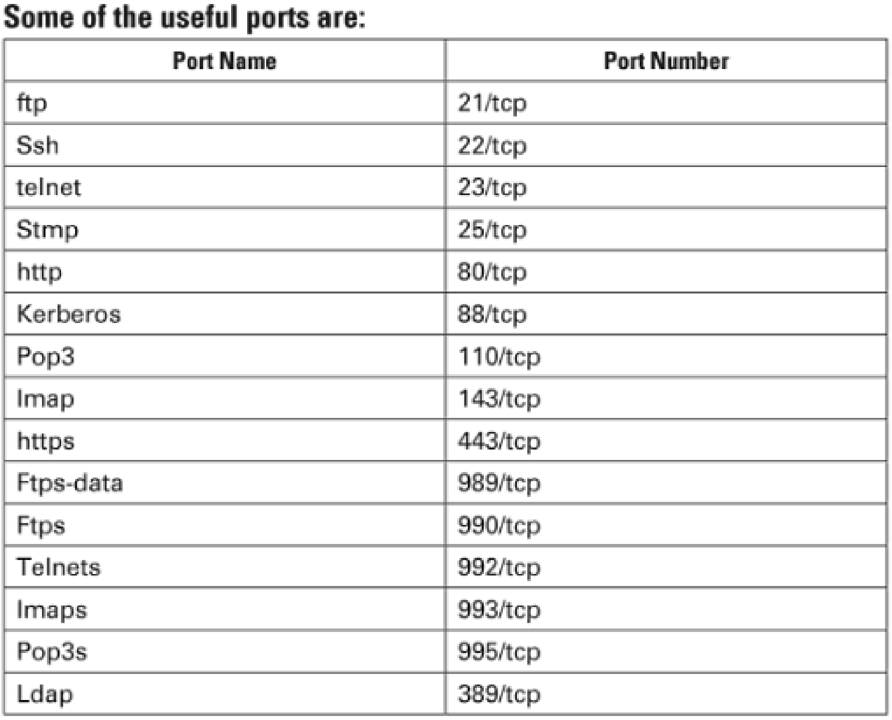
- These are also known as System Ports or Reserved Ports.
- Ports in this range are typically associated with well-known services or protocols.
- Many of these ports are standardized by organizations like the Internet Assigned Numbers Authority (IANA).
- For example, Port 80 is used for HTTP (Hypertext Transfer Protocol), Port 22 for SSH (Secure Shell), and Port 25 for SMTP (Simple Mail Transfer Protocol).

2. Registered Ports (1024 to 49151):

- These ports are also known as User Ports.
- Ports in this range are assigned by IANA to various software applications or services on a temporary or permanent basis.
- They are used for a wide range of applications beyond the well-known ones and are often allocated to specific software vendors or applications.

3. Dynamic/Private Ports (49152 to 65535):

- These are also known as Private Ports or Ephemeral Ports.
- Ports in this range are used for dynamically assigned, temporary purposes.
- They are typically chosen by client applications (source ports) when making outbound connections to servers (destination ports).
- These ports are not officially assigned by IANA and are used as needed for communication.



Some of the useful ports are:

Port Name	Port Number
ftp	21/tcp
Ssh	22/tcp
telnet	23/tcp
Stmp	25/tcp
http	80/tcp
Kerberos	88/tcp
Pop3	110/tcp
Imap	143/tcp
https	443/tcp
Ftps-data	989/tcp
Ftps	990/tcp
Telnets	992/tcp
Imaps	993/tcp
Pop3s	995/tcp
Ldap	389/tcp

PROTOCOLS

Protocol is simply a set of rules which defines a standard way for exchanging information over a network.

Ethical hacking, various protocols are relevant as they pertain to network communication, security assessments, and vulnerability testing. Ethical hackers, also known as penetration testers or white-hat hackers, often work with these protocols to assess and secure computer systems.

Most commonly used protocol are :

1. **TCP (Transmission control protocol):**

- TCP is one of the core part of IPS (internet protocol suite). When a request is sent to a server This TCP protocol takes place.
- TCP provides the facility to exchange the information or data directly between two hosts. Many major internet applications like e-mail, file transfer etc.
- TCP/IP is the foundation of the internet and is essential for ethical hackers to understand as it underlies most network communications.
- This protocol contains variety of flags like SYN, ACK, RST, FIN etc.

2. **INTERNET PROTOCOL (IP):**

This IP is used to deliver packets from source to destination. Internet Protocol is other core part of IPS. IP is the main communication protocol with is used for exchanging packets over inter-network using IPS. IP is used to deliver packets from source to destination.

3. **USER DATAGRAM PROTOCOL(UDP):**

In UDP, simple transmission model is used and there is no hand-shaking method is used which results into unreliability, duplication and missing of the information without notice.

Data on the internet is generally organized into standard TCP or UDP packets. A packet is bunch of information. Different services use different ports to exchange the information.

- No "THREE WAY HANDSHAKE" takes place
- No encyption of Data, Sends and recieves in plain Text
- Less security

<u># Other Important Protocols</u>

4. **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):**

Ethical hackers commonly analyze web applications and websites, making knowledge of HTTP and HTTPS crucial for understanding how web traffic and vulnerabilities work.

5. **INTERNET CONTROL MESSAGE PROTOCOL (ICMP):**

- To check whether a Specfic website or host is Alive ,this ICMP protocol is used
- To check, go to CMD in desktop
- And type Ping 8.8.8.8 we can see packets is recived
- If there server is down, then it will show a Error message "HOST UNREACHABLE"

6. FILE TRANSFER PROTOCOL (FTP):

- To transfer a file from one host to another , thsi FTP protocol is used
- First we should connect to a Host in which we need to transfer the files using Ftp@ip
- Then using PUT,GET command we can fetch the specific files.
- FTP runs on Port 21.

7. ADDRESS RESOLUTION PROTOCOL (ARP)

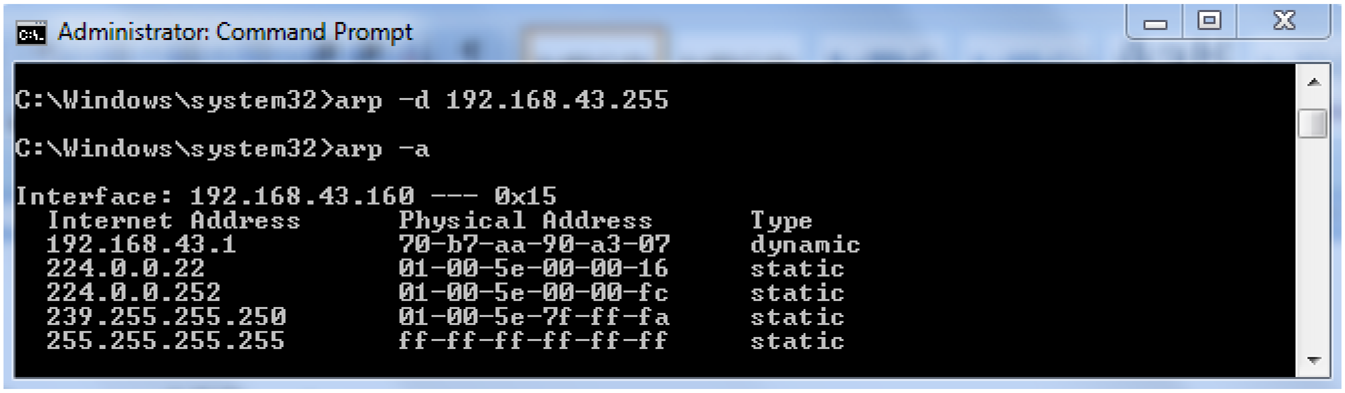
- The Address Resolution Protocol (ARP) is a fundamental networking protocol used to map an IP address to a physical (MAC) address on a local network.
- ARP plays a crucial role in local network communication by enabling devices to discover each other's hardware addresses, allowing data to be properly encapsulated and delivered at the data link layer (Layer 2) of the OSI model.

Viewing ARP Tables:

1. Open Command Prompt.

2. Type “ arp –a “.

3. ARP tables will be shown up (Shown in screenshot)



```
C:\Windows\system32>arp -d 192.168.43.255

C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

8. Dynamic Host Configuration Protocol (DHCP):

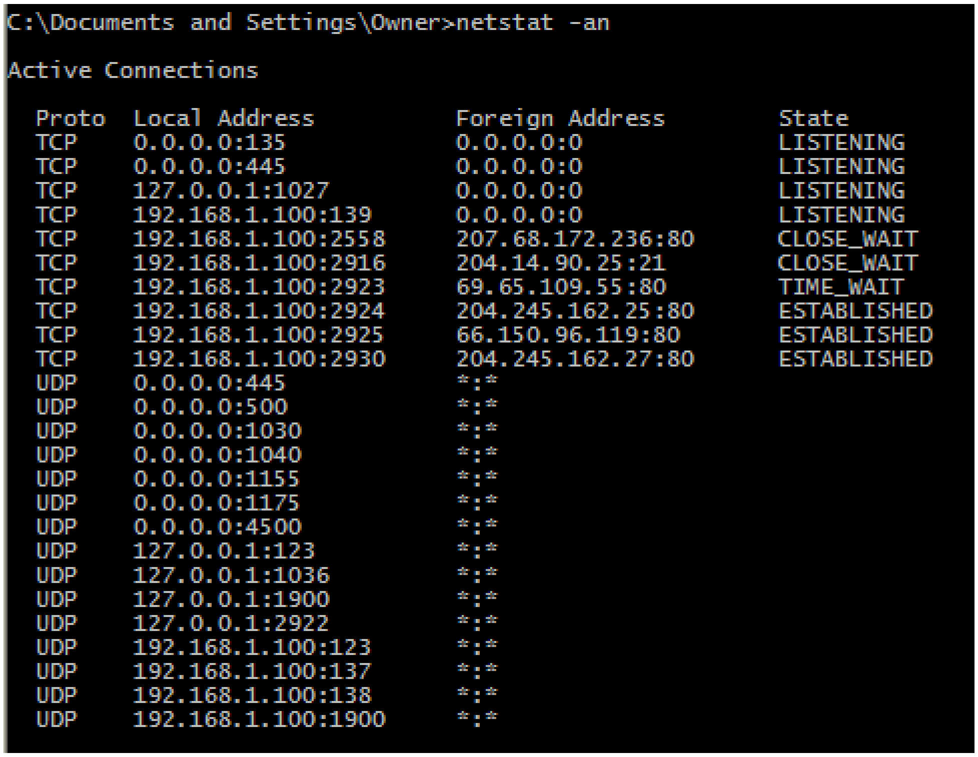
- Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a TCP/IP network.
- DHCP simplifies the process of IP address management and network configuration by dynamically allocating IP addresses as devices connect to the network.

9. Simple Mail Transfer Protocol (SMTP) :

- SMTP is the standard protocol used for exchanging the electronic mail (e-mail) across the IP networks. SMTP Uses port 25 on TCP(for outgoing mail transfer).

Viewing all TCP/UDP Connection and Listening Ports using Netstat :

1. Open Command prompt.
2. Type “netstat –an” (for the purposes mentioned above, shown in screenshot).
3. To explore more about netstat command type “netstat –h” or “netstat /?” to

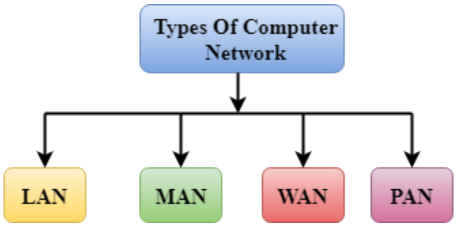


```
C:\Documents and Settings\Owner>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
  TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.100:2558     207.68.172.236:80      CLOSE_WAIT
  TCP    192.168.1.100:2916     204.14.90.25:21        CLOSE_WAIT
  TCP    192.168.1.100:2923     69.65.109.55:80        TIME_WAIT
  TCP    192.168.1.100:2924     204.245.162.25:80      ESTABLISHED
  TCP    192.168.1.100:2925     66.150.96.119:80       ESTABLISHED
  TCP    192.168.1.100:2930     204.245.162.27:80      ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1040           *:*
  UDP    0.0.0.0:1155           *:*
  UDP    0.0.0.0:1175           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1036         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:2922         *:*
  UDP    192.168.1.100:123      *:*
  UDP    192.168.1.100:137      *:*
  UDP    192.168.1.100:138      *:*
  UDP    192.168.1.100:1900     *:*
```

PRIMARY NETWORK TYPES

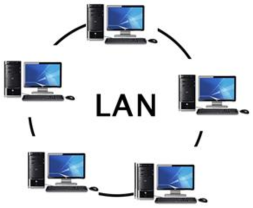
Network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size.



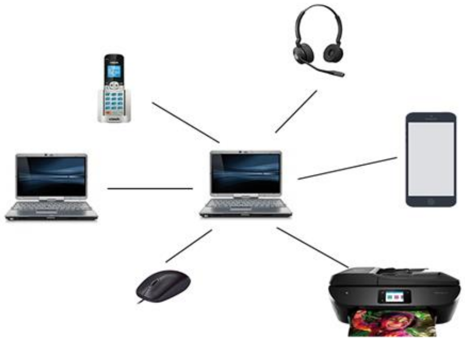
1. Local Area Network (LAN)

In LAN, a computer network cover small local area like home, office and small workgroups such as schools or university. Wi-Fi and Ethernet are commonly used for LAN.



2. PAN(Personal Area Network)

Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters. Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.



There are two types of Personal Area Network:

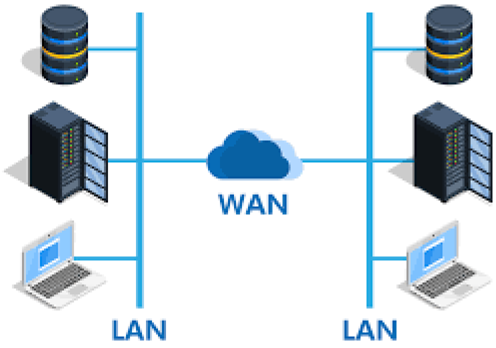
- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

3. Wide Area Network (WAN)

In WAN, a computer network cover larger area like on national or regional level. A wide area network can be used as Local area network, metropolitan area network (MAN), or for campus area network (CAN).



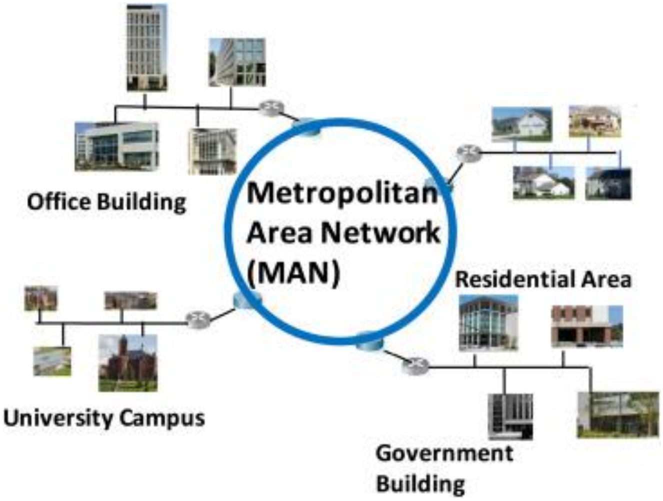
4. Wireless Local Area Network (WLAN)

In WLAN, devices are connected wirelessly by the mechanism of wireless distribution method (OFDM Radio or any other). In WLAN, generally a access point provides the connection and hence provide the user an ease of mobility. WLAN is easy to install and maintain. However it became very popular these days with laptops and Personal Devices. It had observed that at railway stations, malls, hotels, etc. are equipped with WLAN.

5. MAN(Metropolitan Area Network)

A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.

- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.



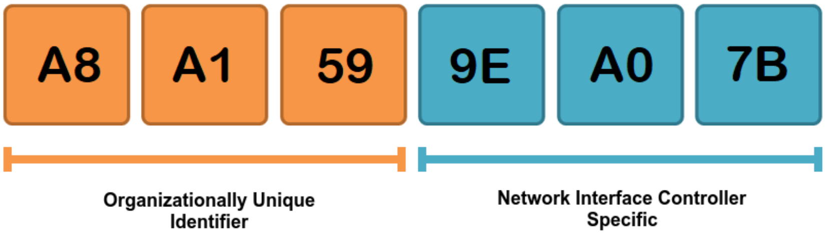
IMPORTANT TERMS ASSOCIATED WITH NETWORK

1.Product Identification number:

- PID stands for Product Identification number. PID is used to provide identification to a standalone system on a network.
- PID was developed to solve the problem of identification. In this, a unique id was hardcoded on the NIC (Network interface card).
- But due to production of NIC by more than one Manufacturer, conflicts were seen. Hence pid was not much efficiently used for identification.

2. MAC Address

- Mac Address stands for Media Access Control Address. MAC address is 48 bits hexa decimal number which is a unique number assigned to the network adaptors or NIC.
- Mac address is the combination of PID and CID (Company Identification Number). mac address is also known as physical address.


A8
A1
59
9E
A0
7B
Organizationally Unique Identifier
Network Interface Controller Specific

3. IP Address

- IP Address stands for internet protocol address. An IP (Internet Protocol) address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.

- Ip address is used for addressing the network so that it can be detected and used for transferring the information or messages. Ip address is of 32 bits. The value of ip address is in numeric format.

For ex : 127.0.0.1 (IPv4)

There are two main versions of IP addresses:

1. **IPv4 (Internet Protocol version 4):**

- IPv4 addresses are 32-bit addresses, typically represented as four decimal numbers separated by periods (e.g., 192.168.0.1).

- IPv4 has a limited address space, with approximately 4.3 billion unique addresses.

2. **IPv6 (Internet Protocol version 6):**

IPv6 addresses are 128-bit addresses, represented as eight groups of hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Ip address can be assigned by two methods:

1. **Static IP**

- Static IP is fixed IP of a system which don't change automatically.

2. **Dynamic Ip**

- Dynamic IP is IP assigned to a system which gets changed when the system or connection is restarted.

3. NetBios Name

- A NetBIOS name, also known as a NetBIOS computer name or NetBIOS host name, is a 16-character identifier used in legacy Microsoft Windows-based networks for identifying devices and resources on a local network.

- NetBIOS names were commonly used in older Windows environments, but their usage has diminished in favor of more modern networking technologies.

- For example the netbios name of XYZ represents its ip address. NetBios names are 16 characters long and may consist of alpha-numeric values.

VIRTUALIZATION & INTRODUCTION TO KALI LINUX

Virtualization:

Virtualization is a software technology by which it is possible to run multiple operating systems on the same device or server at the same time.

- It is one of the efficient way and reduce costs of multiple system setup.
- Virtualization is very helpful when you need to demonstrate something between two different operating systems.

For Ex, A malware target windows machine can be ran parallel to the attacker linux machine and it will be much easier to analyze the behavior.

Virtualization Software:

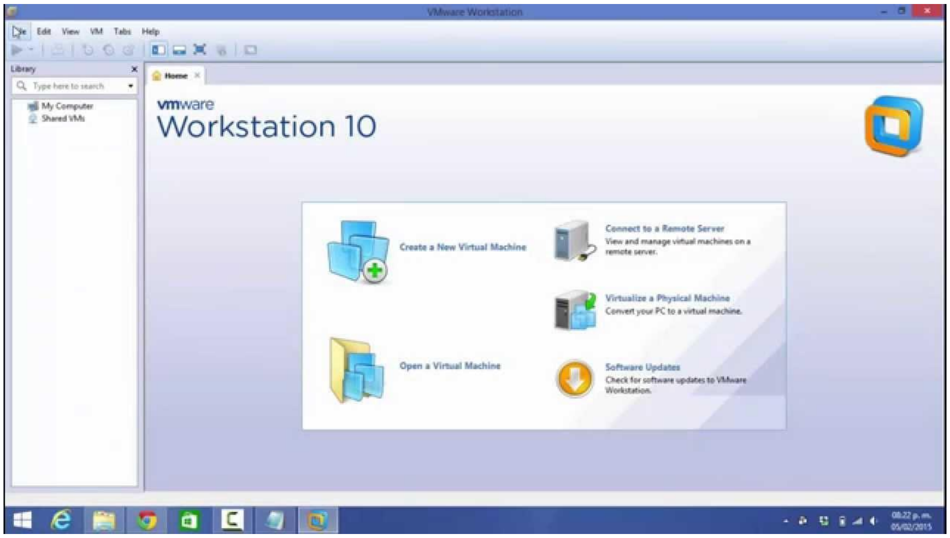
- Special software is developed for virtualization. These software are design to run multiple operating systems at the same instant on the same system.
- Virtualization software enables the creation and management of virtual machines (VMs) on a physical host machine.
- These virtualized environments can run multiple operating systems and applications independently on the same hardware, making them essential for various use cases, including development, testing, and server consolidation.

Some commonly used Virtualization Software:

1. VmWare Workstation : (Download : http://www.vmware. com/in/products/workstation)
2. Virtual Box: (Download : https://www.virtualbox.org/wiki/ Downloads)

Using VmWare Workstation:

1. Download and Install VmWare Workstation.
2. Open VmWare Workstation & Click on “ Create Virtual Machine.”
3. Choose the image file of Operating system or application.
4. Choose the name of Operating system or application and select it’s version.
5. Provide Hard-drive space for virtual machine (min. required : 20GB) and click on finish.
6. Virtual machine is ready to use. Start from the home screen of VmWare Workstation.


VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Shared VMs
Home
vmware
Workstation 10
Create a New Virtual Machine
Connect to a Remote Server
View and manage virtual machines on a remote server.
Virtualize a Physical Machine
Convert your PC to a virtual machine.
Open a Virtual Machine
Software Updates
Check for software updates to VMware Workstation.
08:22 p. m.
05/02/2015

Kali Linux:

- Kali Linux is a linux based operating system which is a powerful and most popular hacking os itself.

- Kali Linux is a specialized Linux distribution designed for cybersecurity, penetration testing, and ethical hacking. It is developed and maintained by Offensive Security, a leading cybersecurity training and services provider.

- Kali Linux provides a wide range of security tools and utilities to help cybersecurity professionals, penetration testers, and ethical hackers assess and secure computer systems, networks, and applications.

1. Contains more than 300 of pre-installed penetration testing scripts and programs.

2. NetHunter is specially designed for Android Devices. Some of the included tools are

- Wireshark
- Metasploit Framework
- Burp Suite
- Social Engineering Toolkit
- Armitage
- Nmap
- Kismet
- Aircrack
- hping3
- and many more powerful tools.

Kali linux is available for following devices :

1. BeagleBone Black
2. Hp Chromebook
3. CubieBoard 2
4. CuBox
5. Raspberry Pi
6. Utilite Pro
7. Galaxy Note 10.1
   and rest device can use via Raspberry Pi Image.

Installing Kali linux as Virtual Machine :

Installing Kali Linux as a virtual machine (VM) is a common and convenient way to set up an isolated environment.

Prerequisites:

1. Download the Kali Linux ISO image from the official Kali Linux website (https://www.kali.org/downloads/).
2. Install virtualization software on your host machine (e.g., VMware Workstation, Oracle VirtualBox, VMware Player).

Installation Steps:

1. **Create a New Virtual Machine:**
   - Open your virtualization software (e.g., VMware Workstation, VirtualBox).
   - Click on the option to create a new virtual machine or VM.

2. **Choose Guest Operating System:**

   - Select "Linux" as the guest operating system.
   - Choose the appropriate version (e.g., "Debian (64-bit)") as Kali Linux is based on Debian.

3. **Allocate Resources:**
   - Assign RAM (memory) to your VM. A minimum of 2GB is recommended, but more is better if your host system has sufficient resources.
   - Create a virtual hard disk with a recommended size of at least 20-30GB. Ensure you have enough disk space on your host machine.

4. **Select ISO Image:**
   - During the virtual machine creation process, you'll be prompted to select an installation method.
   - Choose to install from an ISO image.
   - Browse and select the Kali Linux ISO image that you downloaded earlier.

5. **Configure Networking:**

   Set up network settings for your VM. You can choose to use NAT, Bridged, or Host-Only networking, depending on your requirements.

6. **Start the VM:**
   - Click the "Start" or "Power On" button to boot the virtual machine.
   - Follow the on-screen prompts to begin the installation process.

7. **Install Kali Linux:**
   - Follow the Kali Linux installation wizard, which includes selecting your language, region, keyboard layout, and setting up a root password.
   - When prompted to partition the disk, you can choose to use the entire disk or set up custom partitions, depending on your preference.

8. **Configure the Package Manager:**

   During the installation, you'll be asked to configure the package manager. Choose a nearby mirror for package downloads.

9. **Install GRUB Boot Loader:**

   When asked to install the GRUB boot loader, select "Yes" to install it.

10. **Complete the Installation:**

    Allow the installation process to complete, which may take a few minutes.

11. **Reboot the VM:**

    Once the installation is finished, you'll be prompted to remove the installation media (the ISO image). Reboot the VM.

12. **Log In:**

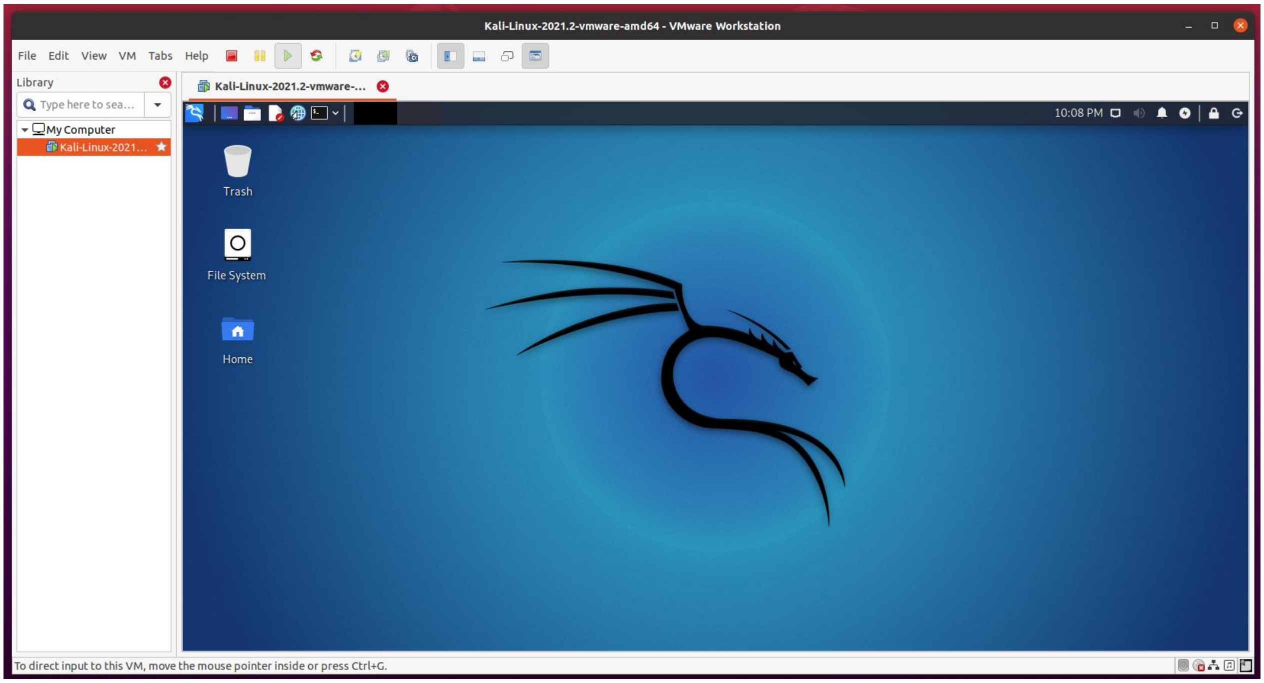
    After rebooting, you'll be presented with the Kali Linux login screen. Log in using the username "root" and the password you set during installation.

13. **Update and Upgrade:**

    Open a terminal and run the following commands to update and upgrade the system:

    - ❖ apt update
    - ❖ apt upgrade

Kali Linux virtual machine is now installed and ready for use. You can start exploring the wide range of security tools and utilities that come pre-installed, and you can also customize the environment to suit your specific needs for ethical hacking and security testing.



Kali-Linux-2021.2-vmware-amd64 - VMware Workstation

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

PENETRATION TESTING

A penetration test is a subclass of ethical hacking; it comprises a set of methods and procedures that aim at testing/protecting an organization’s security. The penetration tests prove helpful in finding vulnerabilities in an organization and check whether an attacker will be able to exploit them to gain unauthorized access to an asset.

- A penetration test, often abbreviated as "pen test," is a cybersecurity assessment and testing methodology conducted by security professionals (often referred to as penetration testers or ethical hackers) to identify and assess vulnerabilities in computer systems, networks, applications, and other digital assets.
- The primary objective of a penetration test is to simulate real-world attacks and evaluate the security posture of an organization's assets.

Vulnerability Assessments versus Penetration Test:

Both vulnerability assessments and penetration tests as part of their overall cybersecurity strategy. Vulnerability assessments help identify weaknesses, while penetration tests provide a deeper understanding of the potential impact and real-world risk associated with those vulnerabilities.

Preengagement:

Before you start doing a penetration test, there is whole lot of things you need to discuss with clients. This is the phase where both the customer and a representative from your company would sit down and discuss about the legal requirements and the “rules of engagement.”

Rules of Engagement:

Every penetration test you do would comprise of a rules of engagement, which basically defines how a penetration test would be laid out, what methodology would be used, the start and end dates, the milestones, the goals of the penetration test, the liabilities and responsibilities, etc.

■■ A proper “permission to hack” and a “nondisclosure” agreement should be signed by both the parties.

■■ The scope of the engagement and what part of the organization must be tested.

■■ The project duration including both the start and the end date.

■■ The methodology to be used for conducting a penetration test.

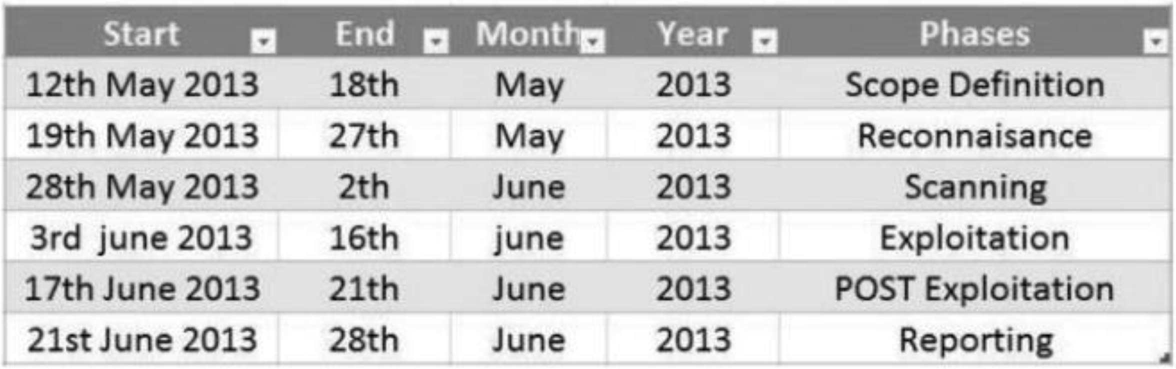
■■ The goals of a penetration test.

■■ The allowed and disallowed techniques, whether denial-of-service testing should be performed or not.

Milestones:

Before starting a penetration test, it’s good practice to set up milestones so that your project is delivered as per the dates given in the rules of engagement.

You can use either a GANTT chart or a website like Basecamp that helps you set up milestones to keep track of your progress.



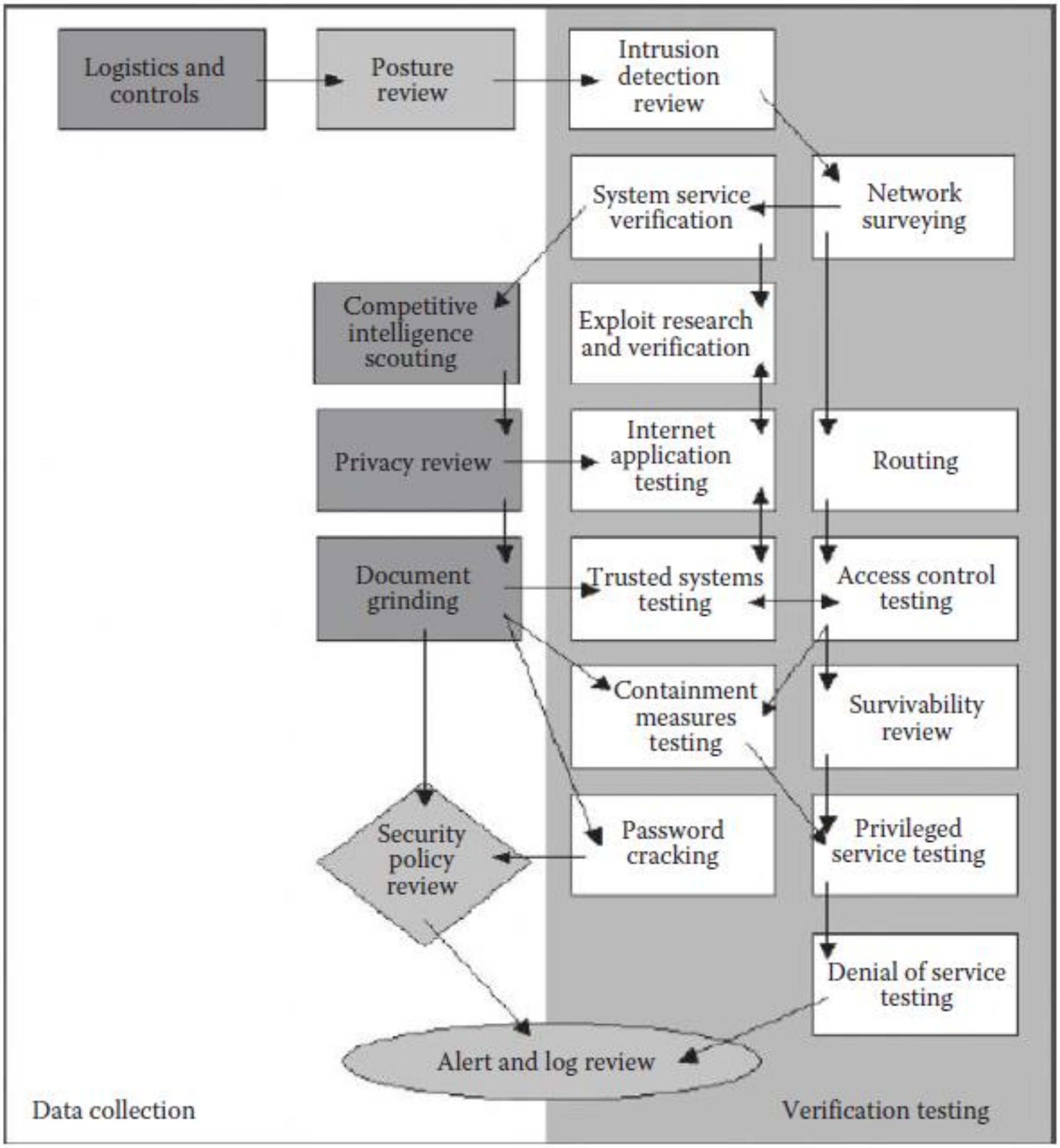
Start	End	Month	Year	Phases
12th May 2013	18th	May	2013	Scope Definition
19th May 2013	27th	May	2013	Reconnaisance
28th May 2013	2th	June	2013	Scanning
3rd june 2013	16th	june	2013	Exploitation
17th June 2013	21th	June	2013	POST Exploitation
21st June 2013	28th	June	2013	Reporting

Penetration Testing Methodologies

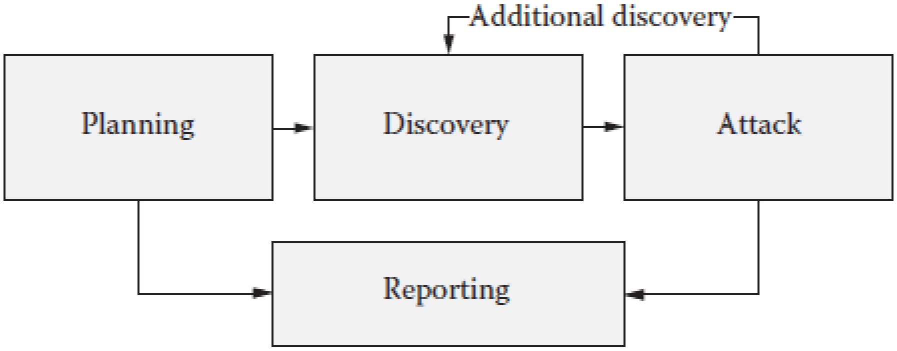
In every penetration test, methodology and the reporting are the most important steps. Let’s first talk about the methodology.

OSSTMM:

An open-source security testing methodology manual (OSSTMM) basically includes almost all the steps involved in a penetration test. The methodology employed for penetration test is concise yet it’s a cumbersome process which makes it difficult to implement it in our everyday life. Penetration tests, despite being tedious, demands a great deal of money out of company’s budgets for their completion which often are not met by a large number of organizations.



NIST: National Institute of Standards and Technology



NIST, on the other hand, is more comprehensive than OSSTMM, and it's something that you would be able to apply on a daily basis and in short engagements. The screenshot indicates the four steps of the methodology, namely, planning, discovery, attack, and reporting.

The testing starts with the planning phase, where how the engagement is going to be performed is decided upon.

This is followed by the discovery phase, which is divided into two parts—the firstpart includes information gathering, network scanning, service identification, and OS detection, and the second part involves vulnerability assessment.

The organization also has a more detailed version of the chart discussed earlier, which actually explains more about the attack phase. It consists of things such as "gaining access," "escalating privileges," "system browsing," and "install additional tools."

OWASP: Open Web Application Security Project Framework

- As you might have noticed, both the methodologies focused more on performing a network penetration test rather than something specifically built for testing web applications.
- The OWASP testing methodology is what we follow for all "application penetration tests" we do here at the RHA InfoSEC.
- The OWASP testing guide basically contains almost everything that you would test a web application for.
- The methodology is comprehensive and is designed by some of the best web application security researchers.

Categories of Penetration Test:

The entire penetration test can be Black Box, White Box, or Gray Box depending upon what the organization wants to test and how it wants the security paradigm to be tested.

Black Box:

- A black box penetration test is where little or no information is provided about the specified target. In the case of a network penetration test this means that the target's DMZ, target operating system, server version, etc., will not be provided; the only thing that will be provided is the IP ranges that you would test.
- In the case of a web application penetration test, the source code of the web application will not be provided. This is a very common scenario that you will encounter when performing an external penetration test.

White Box:

- A white box penetration test is where almost all the information about the target is provided.
- In the case of a network penetration test, information on the application running, the corresponding versions, operating system, etc., are provided.
- In the case of a web application penetration test the application's source code is provided, enabling us to perform the static/dynamic "source code analysis."
- This scenario is very common in internal/onsite penetration tests, since organizations are concerned about leakage of information.

Gray Box:

- In a gray box test, some information is provided and some hidden.
- In the case of a network penetration test, the organization provides the names of the application running behind an IP; however, it doesn't disclose the exact version of the services running.
- In the case of a web application penetration test, some extra information, such as test accounts, back end server, and databases, is provided.

Types of Penetration Tests

There are several types of penetration tests; however, the following are the ones most commonly performed:

Network Penetration Test:

In a network penetration test, you would be testing a network environment for potential security vulnerabilities and threats. This test is divided into two categories: external and internal penetrationtests.

An external penetration test would involve testing the public IP addresses, whereas in an internal test, you can become part of an internal network and test that network. You may be provided VPN access to the network or would have to physically go to the work environment for the penetration test depending upon the engagement rules that were defined prior to conducting the test.

Web Application Penetration Test:

Web application penetration test is very common nowadays, since your application hosts critical data such as credit card numbers, usernames, and passwords; therefore this type of penetration test has become more common than the network penetration test.

Mobile Application Penetration Test:

The mobile application penetration test is the newest type of penetration test that has become common since almost every organization uses Android- and iOS-based mobile applications to provide services to its customers. Therefore, organizations want to make sure that their mobile applications are secure enough for users to rely on when providing personal information when using such applications.

Social Engineering Penetration Test:

A social engineering penetration test can be part of a network penetration test. In a social engineering penetration test the organization may ask you to attack its users. This is where you use speared phishing attacks and browser exploits to trick a user into doing things they did not intend to do.

Physical Penetration Test:

A physical penetration test is what you would rarely be doing in your career as a penetration tester. In a physical penetration test, you would be asked to walk into the organization’s building physically and test physical security controls such as locks and RFID mechanisms.

Report Writing:

In any penetration test, the report is the most crucial part. Writing a good report is key to successful penetration testing. The following are the key factors to a good report:

- Your report should be simple, clear, and understandable. Presentation of the report is also important. Headers, footers, appropriate fonts, well-spaced margins, etc., should be created/selected properly and with great care. For example, if you are using a red font for the heading, every heading in the document should be in that style.

- Correct spelling and grammar is important too. A misspelled word leaves a very negative impact upon the person who is reading your report. So, you should make sure that you proofread your report and perform spell-checks before submitting it to the client.

Structure of a Penetration Testing Report:

A penetration testing report is a critical deliverable that communicates the results, findings, and recommendations of a penetration test to stakeholders within an organization.

Cover Page:

We start with the cover page; this is where you would include details such as your company logo, title, and a short description about the penetration test.

Table of Contents:

On the very next page, you should have an index so that the audience interested in reading a particular portion of the report can easily skip to that portion.

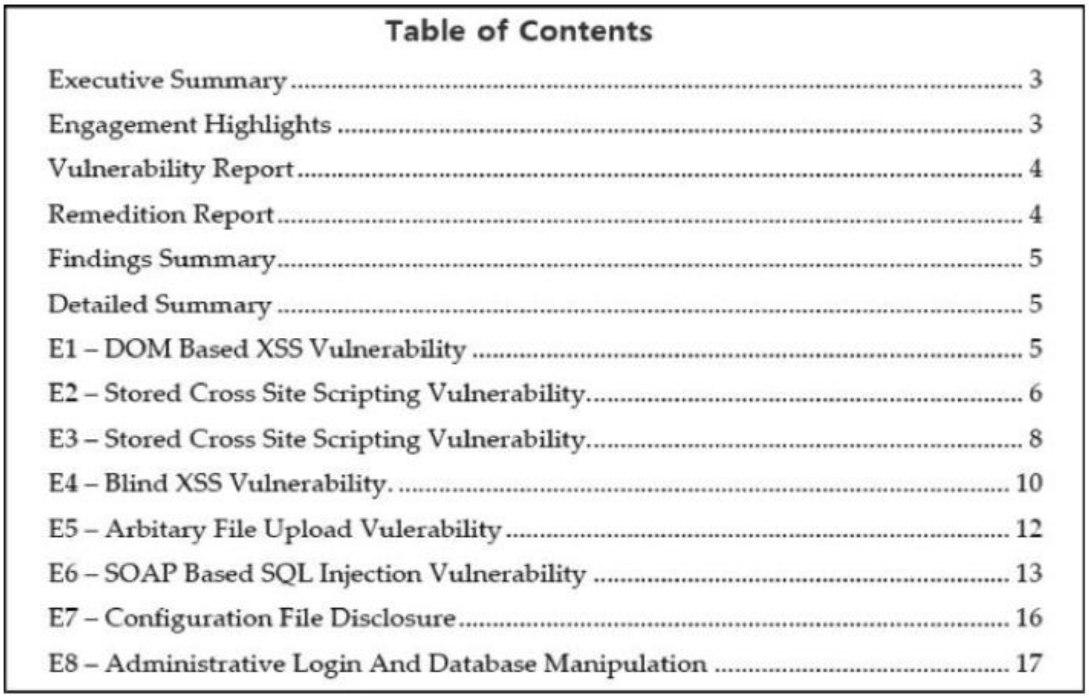


Table of Contents

Executive Summary 3
Engagement Highlights 3
Vulnerability Report 4
Remedition Report 4
Findings Summary 5
Detailed Summary 5
E1 – DOM Based XSS Vulnerability 5
E2 – Stored Cross Site Scripting Vulnerability 6
E3 – Stored Cross Site Scripting Vulnerability 8
E4 – Blind XSS Vulnerability. 10
E5 – Arbitary File Upload Vulerability 12
E6 – SOAP Based SQL Injection Vulnerability 13
E7 – Configuration File Disclosure 16
E8 – Administrative Login And Database Manipulation 17

Executive Summary

As the name suggests, an executive summary is the portion that is specifically addressed to executives such as the CEO or the CIO of the company.

Introduction: Briefly introduce the report and its purpose.

Scope: Define the scope of the penetration test, including target systems, networks, and objectives.

Key Findings: Summarize the most critical vulnerabilities and their potential impact.

Recommendations: Provide high-level recommendations for addressing the identified security issues.

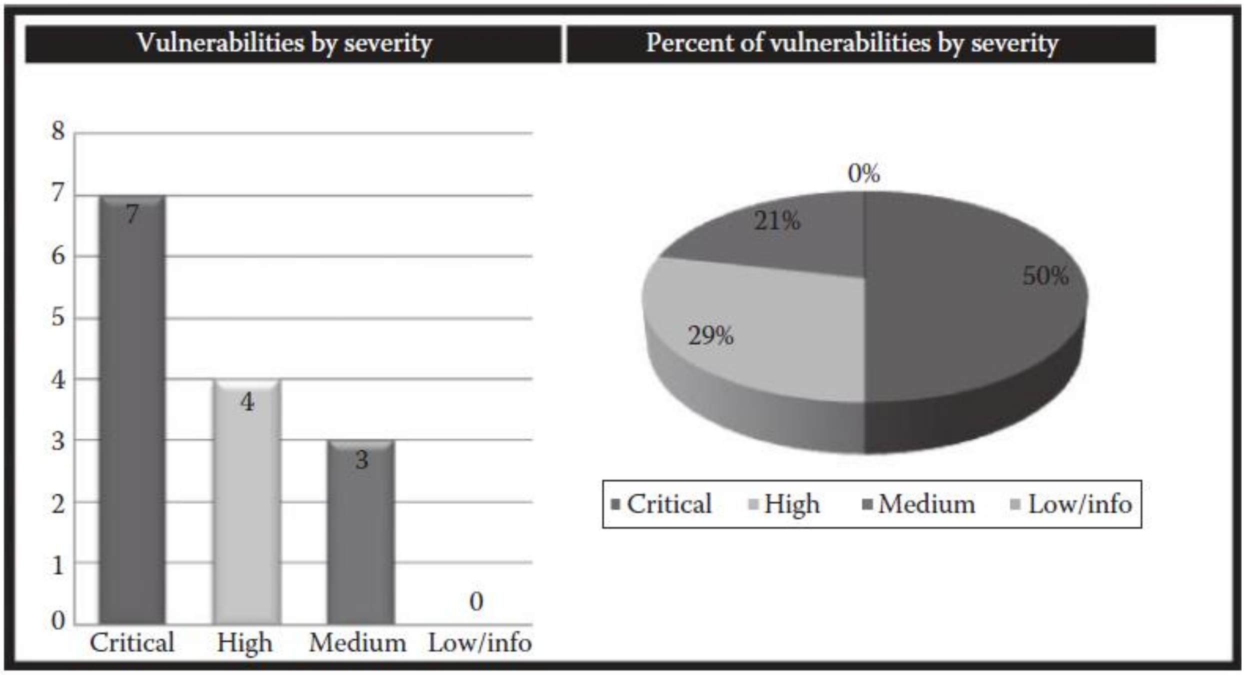
Risk Assessment: Present an overall risk assessment, highlighting potential business impacts and likelihoods.

Remediation Report

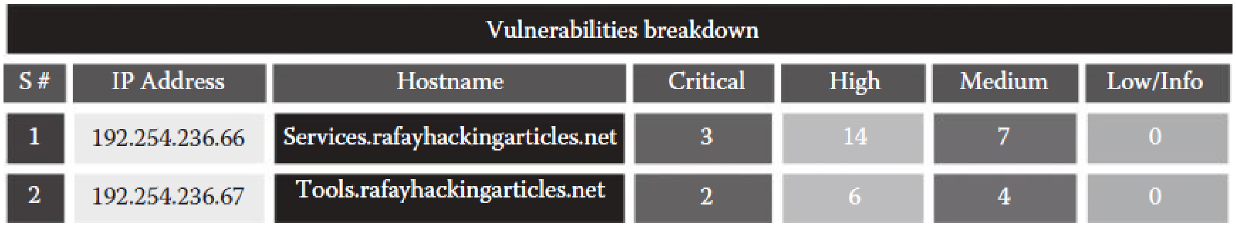
- Next up we have the remediation report, which contains the overall recommendations that once implemented would increase the security of the organization.
- This is specifically an area of interest for the management class, as they are the ones that are going to enforce the security policies of an organization.
- Things that could improve overall security such as implementing SDLC, a firewall, and an intrusion detection system should be recommended.

Vulnerability Assessment Summary

- Next, we have the vulnerability assessment summary, sometimes referred to as "findings summary". This is where we present the findings from our engagement.
- Things such as the overall strengths and weaknesses and risk assessment summary can also be included under this section.
- There are different ways for representing vulnerability assessment outputs in the form of graphical charts.
- Personally, I include two graphs; the first one classifies the vulnerability assessment on the basis of the severity and the second one on percentage.



Next, I include a "vulnerabilities breakdown" chart, where I talk about the findings for a particular host followed by the number of vulnerabilities that were found.

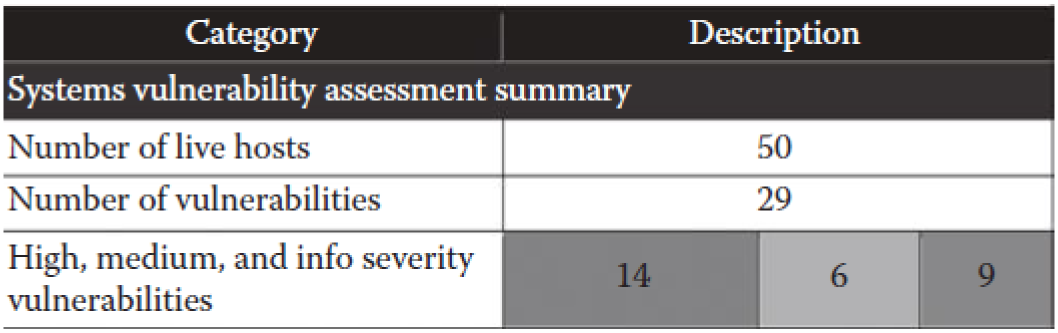


Vulnerabilities breakdown

S #	IP Address	Hostname	Critical	High	Medium	Low/Info
1	192.254.236.66	Services.rafayhackingarticles.net	3	14	7	0
2	192.254.236.67	Tools.rafayhackingarticles.net	2	6	4	0

Tabular Summary

A tabular summary is also a great way to present the findings of a vulnerability assessment to a customer. The following screenshot comes directly from the "NII Report" and summarizes the vulnerability assessment based upon the number of live hosts and also talks about the number of findings with high, moderate, or low risk.



<table>
<tr><th>Category</th><th colspan="3">Description</th></tr>
<tr><td colspan="4">Systems vulnerability assessment summary</td></tr>
<tr><td>Number of live hosts</td><td colspan="3">50</td></tr>
<tr><td>Number of vulnerabilities</td><td colspan="3">29</td></tr>
<tr><td>High, medium, and info severity vulnerabilities</td><td>14</td><td>6</td><td>9</td></tr>
</table>

Risk Assessment

- **Impact Analysis:** Evaluate the potential business impact of each vulnerability, including financial and operational impacts.
- **Likelihood Assessment:** Assess the likelihood of each vulnerability being exploited.
- **Risk Rating:** Assign a risk rating to each vulnerability based on its impact and likelihood.

Methodology:

- **Testing Approach:** Explain the methodologies and techniques used during the penetration test, including any specific tools and tactics.
- **Rules of Engagement:** Detail the rules and limitations defined for the engagement, including what was in scope and out of scope.

Detailed Findings:

- **Vulnerability List:** Provide a comprehensive list of identified vulnerabilities, categorized by severity.
- **Exploitation Details:** Describe how each vulnerability was exploited (or tested) and the potential impact if successfully exploited.
- **Screenshots and Evidence:** Include screenshots, logs, and other evidence to support findings.
- **Recommendations:** Suggest remediation actions for each identified vulnerability.

Recommendations

- **Mitigation Strategies:** Provide detailed recommendations for remediation, including technical, procedural, and policy changes.
- **Priority:** Prioritize the recommendations based on risk and criticality.
- **Timeline:** Suggest timelines for addressing each recommendation**.**

Conclusion

- **Summary:** Summarize the key findings, risk assessment, and recommendations.
- **Overall Assessment:** Provide an overall assessment of the security posture based on the test results.