UNIT I Reference Material

HACKING

UNIT I: Introduction to Hacking:

Hacking—Definition: Hacking in cyber security refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

1.Reconnaissance/Footprinting:

Reconnaissance is the first phase of ethical hacking, also known as the footprinting OR information gathering phase. This is the preliminary phase where white hat hackers gather as much information as possible and implement security measures into the targeted system or network. The information gathered by white hat hackers usually is about three groups: network, host, and people. There are mainly two types of footprinting:

- Active footprinting: Communicate with the target directly to gather information about the target.
- Passive footprinting: Seeking to get information about the target without gaining direct access to the target. Hackers exploit social media, public websites, and other public resources.

2.Scanning:

The scanning phase is the second step in an ethical hacker's methodology. It entails applying all the knowledge learned during the reconnaissance phase to the target location to search for vulnerabilities. Hackers search for data such as user accounts, credentials, IP addresses, etc. There are three types of scanning, which include:

- Port scanning: During this stage, the target is scanned for data such as open ports, live systems, and other services active on the host.
- Vulnerability scanning: This scanning technique identifies a target's vulnerabilities and weak points and attempts to exploit those bugs in various ways. It is carried out using automated tools such as Netsparker, OpenVAS, Nmap, and others.
- Network scanning: This method includes locating the organization's firewall and other routers and networks to assist them in their hacking operations.

3.**GainingAccess:**
In this phase, the hacker creates the blueprint for the target's network using the data gathered in Phases 1 and 2. Now the hacker has all of the information he requires. So he creates the network map and decides how to carry out the attack? There are various alternatives, such as:

- Phishing attacks
- Brute force attack
- Spoofing attack
- Man in the middle attack
- Dos attack
- Session hijacking
- Buffer overflow attacks

The hacker obtains access to the network, programs, and system and then extends their access permissions to manage connected systems.

4.MaintainingAccess:
When a hacker gains access, they choose to maintain it for future exploitation and attack. In addition, the hacker gains access to the organization's Rootkits and Trojans and utilizes them to execute more network attacks. An ethical hacker attempts to keep access to the target until they have completed the activities or intend to complete in that target.

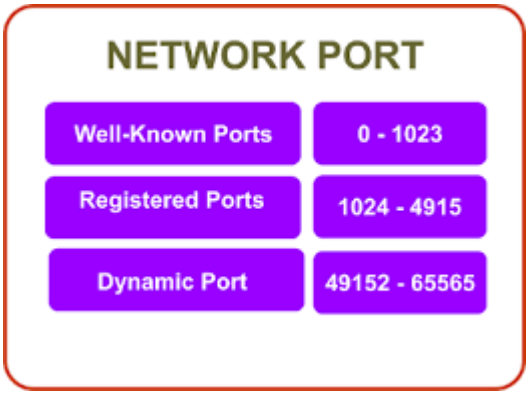
5.**ClearingTracks:**
Once a hacker has obtained access, they leave no trace to prevent detection by the security team. They execute this by deleting cache and cookies, interfering with log files, and closing all open ports. This incorporates some of the steps an ethical hacker uses to cover and eliminate their footprint.

- Deleting/corrupting all logs
- Changing the values of logs or registries
- Removing all of the folders established by the ethical hacker

- Uninstalling all the applications

Introduction to ports and protocols

What is a port? A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

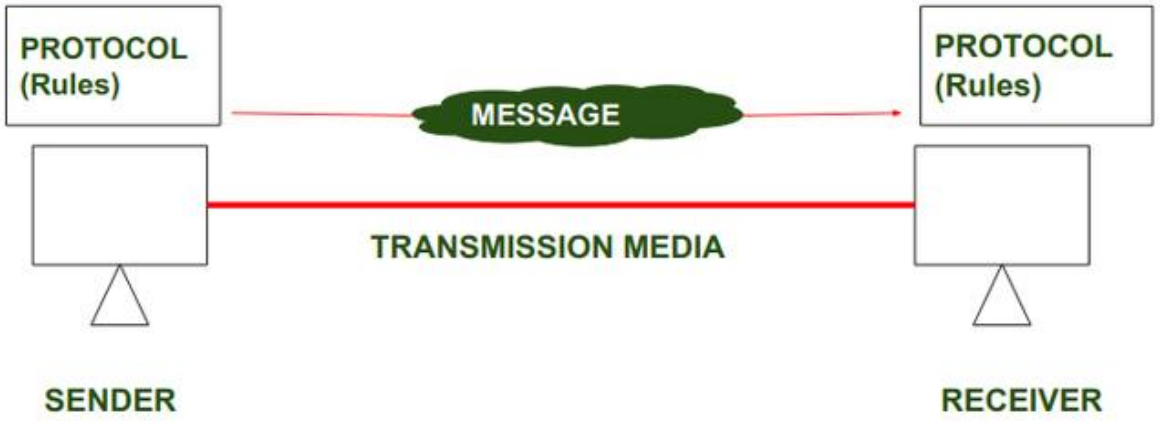


- It can either be a connecting device between two systems or part of a network address. In either way, it helps the system to pass information from one device to another and also to check the network in which the system is working. This helps the devices to maintain a protocol while the transaction of information is being carried out.
- HDMI or High Definition Media Interface helps the system to connect to any projector to display the contents it has that the user intends to show to the audience. HDMI is a port that is wedge-shaped and is present in any desktops and laptops. This is connected with the help of a cable to the projector.
- USB or Universal Serial Bus is used in the device to connect with any gadgets such as pen drives, hard disks, mobile phones, etc. This acts as a multipurpose port that it helps to connect with any gadget with the same port. USB acts as a short distance agent to cover digital communications and they are present in almost all the systems. Data transfer is faster and if the devices are chargeable, then they are charged through USB.
- Serial Port helps in transferring the information as that of a communication device in bits. This is the oldest type of port where information is transferred through external modems and is available in different versions in the market.

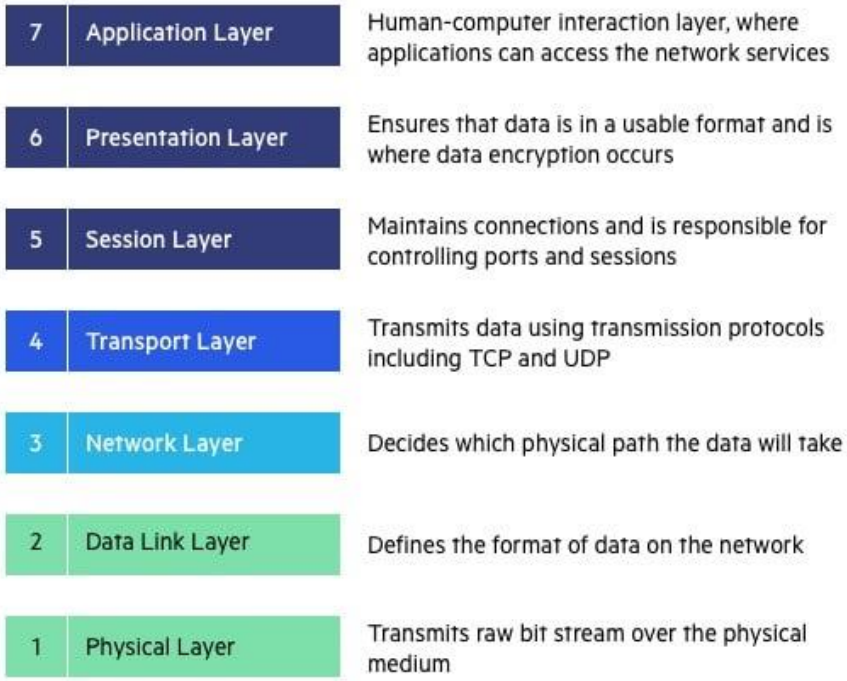
- Parallel Ports work similar to serial ports but the information transfer is done in several bits at a time. This is used even now in many external devices such as printers and scanners. Some call this as a printer port or scanner port based on their usage and there is only one model available in the market. This acts in the form of a parallel communication interface.

Protocol:

In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.



On the Internet, there are different protocols for different types of processes. Protocols are often discussed in terms of which OSI model layer The Open Systems Interconnection (OSI) model is an abstract representation of how the Internet works. It contains 7 layers, with each layer representing a different category of networking functions.



Service or Feature	Protocol Name	Port Number
SQL Server	TCP	1433
SQL server browser	TCP	1434
Basic DTC/WMI	RPC	135
Webhook notifications/any web service	HTTP	80
Webhook notifications/any web service	HTTPS	443
Service bus Queue	AMQP	5671, 5672
BizTalk Server Availability Monitoring – Telnet	TCP	23
BizTalk Server Availability Monitoring – Ping(ICMP)	ICMP	Protocol-1

PRIMARY NETWORK TYPES:

A computer network is a system in which multiple computers are connected to share information and resources. Computer network varies with each other based on their functionality, geography, ownership, and communication media used. **network can be divided into the following types, based on the geographical area that they cover, they are:**

1. **LAN(Local Area Network)**
2. **MAN(Metropolitan Area Network)**
3. **WAN(Wide Area Network)**

- **LAN (Local Area Network)**

A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc.Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc. A LAN can use either wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed as **WLAN(Wireless Local Area Network)** .

Local Area Networks came under existence in around 1970s. IEEE developed the specifications for LAN. The speed of this network varies from 10mbps(Ethernet network) to 1gbps(FDDI or Gigabit Ethernet). Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. **For example,** a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LAN's are generally privately owned networks.

Following are the functionalities of a Local Area Network:

1. **File Serving:** In LAN, a large storage disk acts as a central storage repository.
2. **Print Serving:** Printers can be shared very easily in a LAN by various computers.
3. **Academic Support:** A LAN can be used in the classroom, labs, etc. for educational purposes.
4. **Manufacturing Support:** LAN can support the manufacturing and industrial environment.
5. **High Reliability:** Individual workstations might survive the network in case of failures.

- **MAN (Metropolitan Area Network)**

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc. **Uses of MAN are as follows:**

1. MAN can be used for connecting the various offices of the same organization, spread over the whole city.
2. It can be used for communication in various governmental departments.

- **WAN (Wide Area Network)**

A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN.

- For Example, the Internet.The protocols used in WAN are ISDN(Integrated Service Digital Network), SMDS(Switched Multi-Megabit Data Service), SONET(Synchronous Optical Network),

- HDLC (High Data Link Control), SDLC(Synchronous Data Link Control), etc.The advantage of WAN is that it spans over a very large geographical area, and connects a huge mass of people.

VIRTUALIZATION & INTRODUCTION TO KALI LINUX:

- **INTRODUCTION TO KALI LINUX :**

Kali Linux **is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts, Penetration testers, or in simple words. Kali Linux is to be used by those who are professional penetration testers, cybersecurity experts, ethical hackers, or those who know how to operate it. In simple words, if you know how to use Linux and its terminal commands, architecture, system, and file management then you are good to go with Kali Linux.**

Many people think that Kali is a tool for hacking or cracking social accounts or web servers. This is one of the biggest myths about Kali Linux. Kali Linux is just another Debian distribution with a bunch of networking and security tools. It is a weapon to train or defend yourself not to attack anyone. Kali Linux was designed mainly for professionals. It is for those who want to get their hands in Penetration Testing, Cyber Security, or Ethical Hacking.

Advantages:

- It has 600+ Penetration testing and network security tools pre-installed.
- It is completely free and open source. So you can use it for free and even contribute for its development.
- It supports many languages.
- Great for those who are intermediate in linux and have their hands on Linux commands.

Running Kali Linux as a Virtual Machine in Windows

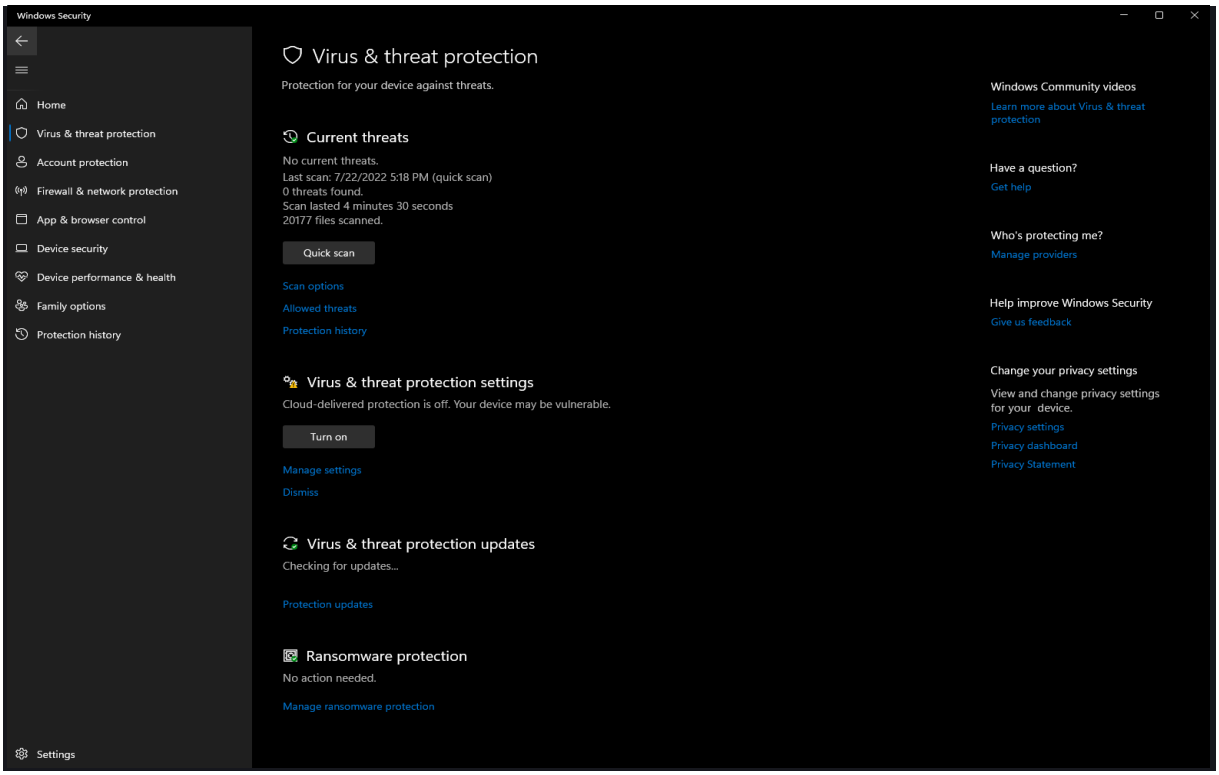
STEPS

- An antivirus signature is a sequence of bytes that are contained within a program. The files on your host system are scanned and the antivirus program compares them against there database that contains these signatures to see if there is a match. When a match is identified the file is quarantined and removed from the host system.
- Although the antivirus program is doing its job, there are some ways that we can protect our Kali Linux Virtual Machine from being quarantined by the host Antivirus Software. This process will focus on implementing these exclusions with Windows Security:

In Windows you can stop Windows Security from alerting you or blocking your virtual machine by adding it to the exclusion list. To do this you need to go to the following:

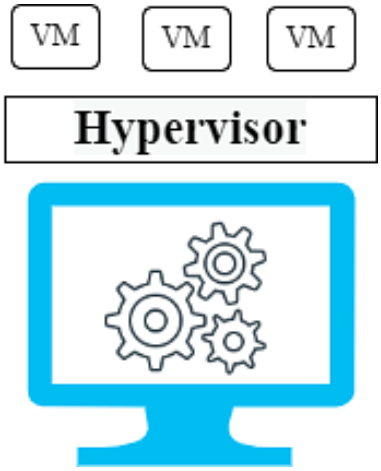
1. Select “Start” > “Settings” > “Update & Security” > “Windows Security” > “Virus & threat protection”.
2. Under “Virus & threat protection settings”, select “Manage settings”, and then under “Exclusions”, select “Add or remove exclusions”.
3. Select “Add an exclusion”. A drop down menu will appear and then you can select files, folders, file types, or process. If you select the folder exclusion will apply to all subfolders within the folder as well.

4. Select the folder you want to use that will contain the files needed to run your Kali Linux Virtual Machine. (In this situation I want to save my Kali Linux Virtual Machine in a folder that I made on my Desktop.)



VIRTUALIZATION: Virtualization uses software to create abstraction layer computer hardware that allows the hardware elements of a single computer processors, memory, storage & more to be divided into multiple virtual computers, commonly called as virtual machines(VMs)

By using virtualization, you can interact with any hardware resource with greater flexibility. Physical servers consume electricity, take up storage space, and need maintenance VPS stands for Virtual Private Server. A **VPS** is a virtual server that runs on a remote server.It provides the same performance and features as a physical server, but is typically less expensive. This is because a VPS does not have to be purchased in bulk, and is therefore more expensive per unit.



It acts as a connection between the physical system and virtual machines to ensure the proper access of the hardware resources. It also manages so that the virtual machines don't interfere with each other's memory and computing resources. The hypervisor also manages the Virtual machines and is known as the virtual machine monitor (VMM).

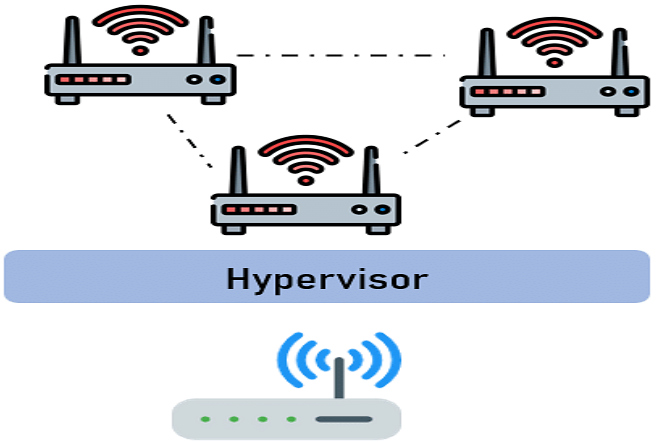
Types of Virtualization : 3 TYPES

In accordance with different IT workspace, you have multiple forms for virtualization:

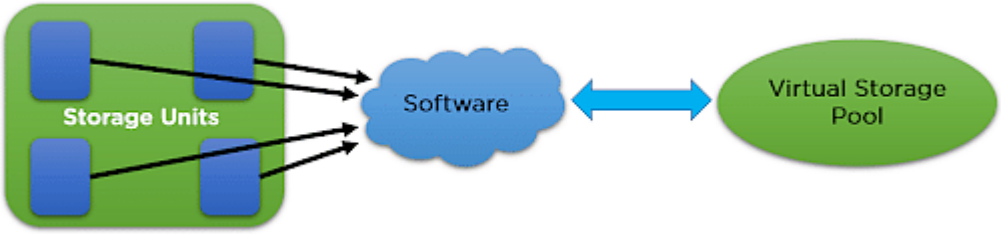
1. **Desktop Virtualization** : In this type of virtualization, you can run multiple operating systems, each in its own virtual machine on the same system.

Virtual desktop infrastructure runs numerous virtual machines on a central server and then hosts it to the host system according to the user's requirements. In this way, you can access any operating system from any device without installing the actual operating system in their local machine.

2. Network Virtualization: In this, the software creates a virtual instance of the network that can be used to manage from a single console. It forms the abstraction of the hardware components and functions (e.g., switches, routers, etc.), simplifying network management.



3.**Storage Virtualization:**This virtualization enables all the storage devices on the system to be accessed and be managed as a single storage unit pool for better maintenance.



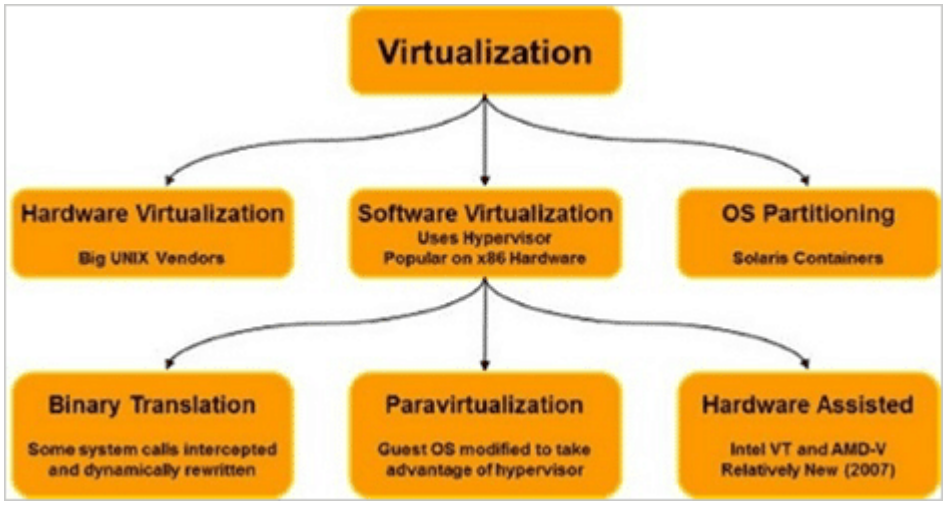
The storage virtualization collects all the storage into a single pool from which they can allocate to any of the VM on the network as required.

Virtualization Software:

The Concept of Virtualization:

Developers require multiple operating systems to build different systems in different environments. For testers, it will be an easier option as they can check different systems in different environments.

Mac users will not be able to use Windows applications without virtualization software. This, in turn, would be the case with the other operating systems as well.



Types of Software Virtualization:

- Operating System Virtualization
- Application Virtualization
- Service Virtualization

i. **Operating System Virtualization**

In operating system virtualization, the hardware is used which consists of software on which different operating systems work. Here, the operating system does not interfere with each other so that each one of them works efficiently.

ii. **Application Virtualization**

Application virtualization is a technology, encapsulates the computer program within the operating system. It can say that application virtualizations refer to running an application on a thin client.

This thin client runs an environment, which is different from what refer to as encapsulating from the operating system which is the location of it.

iii. **Service Virtualization**

In the service virtualization, the DevOps team can use the virtual servers rather than the physical one. It emulates the behaviour of essential components which will be present in the final production environment.

Supported Platform virtualization software:

- A virtualization platform is a virtual, user-friendly computer that runs on top of a more complex platform, hiding the complicated and often intimidating physical traits of the computing resources from the user. The term virtualization, which has been widely used since the 1960s, is used in this context to mean the use of software to create a system that acts as if it were a piece of hardware. Specifically emulators and hypervisors, are software packages that emulate the whole physical computer machine, often providing multiple virtual machines on one physical platform. The table below compares basic information about platform virtualization hypervisors.

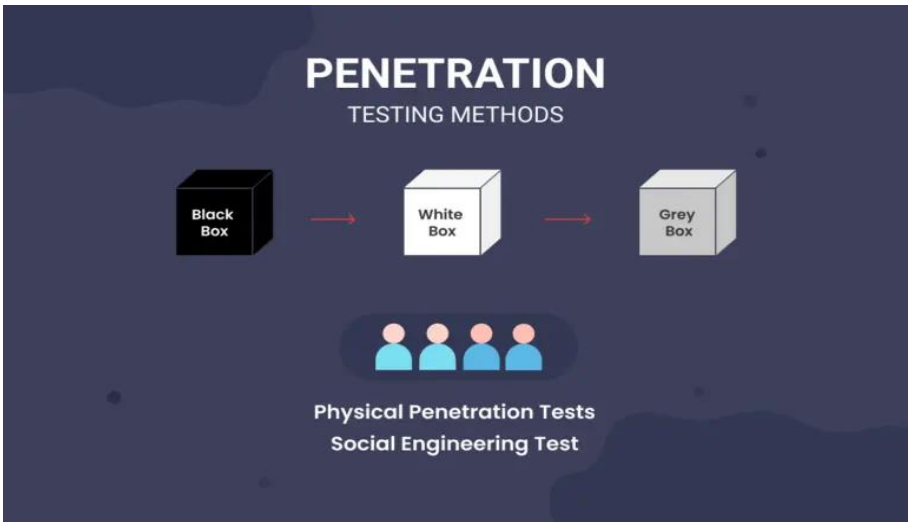
Host OS	Guest OS	Feature
1)**SolarWinds Virtualization Manager**	Windows	VM Sprawl Control, Predictive recommendations, manage across on-premise, hybrid, & cloud, etc.
2)**V2 Cloud**	Windows	Browser accessibility, Web client available on Windows & Mac, Fast performance, Technical support included.
3)VM Ware Fusion	For Mac Users	No reboot required. Can work with Cloud.

INTRODUCTION TO PENETRATION TESTING:

software and systems were designed from the start with the aim of eliminating dangerous security flaws. Depending on the goals of a pen test, testers are given varying degrees of information about, or access to, the target system. In some cases, the pen testing team takes one approach at the start and sticks with it. Other times, the testing team evolves its strategy as its awareness of the system increases during the pen test. There are three levels of pen test access.

- **Opaque box.** The team doesn't know anything about the internal structure of the target system. It acts as hackers would, probing for any externally exploitable weaknesses.
- **Semi-opaque box.** The team has some knowledge of one or more sets of credentials. It also knows about the target's internal data structures, code, and algorithms. Pen testers might construct test cases based on detailed design documents, such as architectural diagrams of the target system.

- **Transparent box.** Pen testers have access to systems and system artifacts including source code, binaries, containers, and sometimes even the servers running the system. This approach provides the highest level of assurance in the smallest amount of time.



CATEGORIES AND TYPES OF PENETRATION TESTS:

Black box in ethical hacking?

In a black box penetration test, no information is provided to the tester at all. The pen tester in this instance follows the approach of an unprivileged attacker, from initial access and execution through to exploitation.

white box in hacking

White box penetration testing approach, also known as an assumed breach, clear box, or transparent box testing, is where the penetration tester has full access and complete knowledge of the target that is being tested and its features.

GREY box hacking?

In a grey box penetration test, also known as a translucent box test, only limited information is shared with the tester. Usually this takes the form of login credentials. Grey box testing is useful to help understand the level of access a privileged user could gain and the potential damage they could cause.

CATEGORIES AND TYPES OF PENETRATION TESTS:

Types of penetration test

A pen test is a form of ethical cyber security assessment aimed at finding, investigating and remediating vulnerabilities in a company's network or applications. Pen testing harnesses the same tactics, techniques and procedures (TTPs) as cyber criminals to simulate a genuine attack against an organisation, enabling them to understand whether their security controls are robust enough to withstand different kinds of threats. the types of pen test available, as engagements vary in focus, depth and duration. Common ethical hacking engagements include:

1. Internal/External Infrastructure Penetration Testing

An assessment of on-premise and cloud network infrastructure, including firewalls, system hosts and devices such as routers and switches. Can be framed as either an internal penetration test, focusing on assets inside the corporate network, or an external penetration test, targeting internet-facing infrastructure.

To scope a test, you will need to know the number of internal and external IPs to be tested, network subnet size and number of sites.

2. Wireless Penetration Testing

A test that specifically targets an organisation's WLAN (wireless local area network), as well as wireless protocols including Bluetooth, ZigBee and Z-Wave. Helps to identify rogue access points, weaknesses in encryption and WPA vulnerabilities. To scope an engagement, testers will need to know the number of wireless and guest networks, locations and unique SSIDs to be assessed.

3. Web Application Testing

An assessment of websites and custom applications delivered over the web, looking to uncover coding, design and development flaws that could be maliciously exploited. Before approaching a testing provider, it's important to ascertain the number of apps that need testing, as well as the number of static pages, dynamic pages and input fields to be assessed.

4. Mobile Application Testing

The testing of mobile applications on operating systems including Android and iOS to identify authentication, authorisation, data leakage and session handling issues. To scope a test, providers will need to know the operating system types and versions they'd like an app to be tested on, number of API calls and requirements for jailbreaking and root detection.

5. Build and Configuration Review

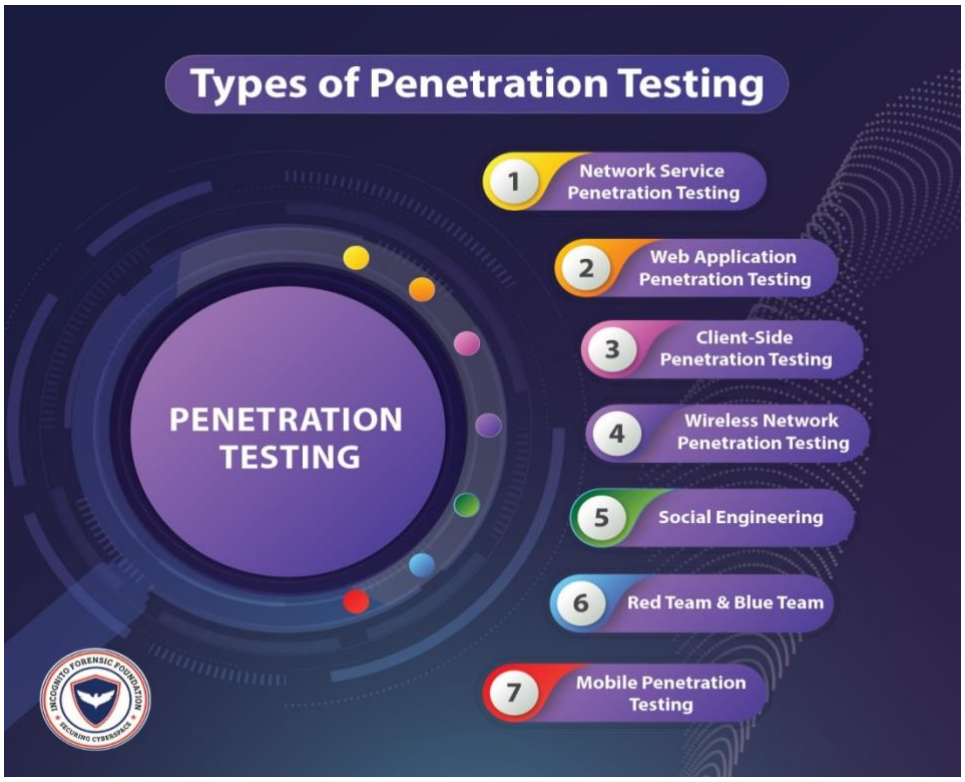
Review of network builds and configurations to identify misconfigurations across web and app servers, routers and firewalls. The number of builds, operating systems and application servers to be reviewed during testing is crucial information to help scope this type of engagement.

6. Social Engineering

An assessment of the ability of your systems and personnel to detect and respond to email phishing attacks. Gain precise insight into the potential risks through customised phishing, spear phishing and Business Email Compromise (BEC) attacks.

7. Cloud Penetration Testing

Custom cloud security assessments to help your organisation overcome shared responsibility challenges by uncovering and addressing vulnerabilities across cloud and hybrid environments that could leave critical assets exposed.



8. Agile Penetration Testing

Continuous, developer-centric security assessments designed to identify and remediate security vulnerabilities throughout the entire development cycle. This agile approach helps to ensure that every product release, whether it is a minor bug fix or a major feature, has been vetted from a security perspective.

STRUCTURE OF PENETRATION TEST REPORT:

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester's personal experience. Once the report is prepared, it is shared among the senior management staff and technical team of target organizations. If any such kind of need arises in future, this report is used as the reference.

Report Writing Stages: Due to the comprehensive writing work involved, penetration report writing is classified into the following stages −

- Report Planning
- Information Collection
- Writing the First Draft
- Review and Finalization

Report Planning

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing. This part describes why the testing is conducted, what are the benefits of pen testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are −

- **Objectives** − It describes the overall purpose and benefits of pen testing.
- **Time** − Inclusion of time is very important, as it gives the accurate status of the system. Suppose, if anything wrong happens later, this report will save the tester, as the report will illustrate the risks and vulnerabilities in the penetration testing scope during the specific period of time.
- **Target Audience** − Pen testing report also needs to include target audience, such as information security manager, information technology manager, chief information security officer, and technical team.
- **Report Classification** − Since, it is highly confidential which carry server IP addresses, application information, vulnerability, threats, it needs to be classified properly. However, this classification needs to be done on the basis of target organization which has an information classification policy.
- **Report Distribution** − Number of copies and report distribution should be mentioned in the scope of work. It also needs to mention that the hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver's name.

Information Collection

Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the methods, he also needs to mention about the systems and tools, scanning results, vulnerability assessments, details of his findings, etc.

Writing the First Draft

Once, the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

Review and Finalization

Once the report is drafted, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.