FR. CONCEICAO RODRIGUES COLLEGE OF ENGG. **Adithya Manoj TE ECS 9462**

Fr. Agnel Ashram, Bandstand, Bandra (W) Mumbai 400 050.

SEMESTER / BRANCH: V (ECS)

Subject code: HCSC501

SUBJECT: **Cyber Security (HONORS): Ethical Hacking / First**

Assignment Date: 20-08-23 Due Date : 25-08-23

HCSC501 .1: **Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios.**

HCSC501 .2: Apply the knowledge of information gathering to perform penetration testing and social engineering attacks.

Questions :

1. What are the core components of the TCP/IP protocol stack and how do they contribute to the functioning of computer networks? (L2, CO1)
2. Explain the process of IP addressing and routing in a computer network. How does routing protocol help in efficient data transmission? (L2, CO1)
3. Outline the key steps involved in ethical hacking and describe how these steps contribute to securing computer systems. (L2, CO1)
4. Compare and contrast the OSI model and the TCP/IP model, highlighting their significance in understanding network communication. (L2, CO1)
5. Explain the process of information gathering and reconnaissance in the context of network security. How can attackers exploit this phase? (L3, CO2)
6. Differentiate between vulnerability assessment and penetration testing. Provide examples of tools used for each of these processes. (L2, CO2)
7. Describe the key characteristics of social engineering attacks and discuss how organizations can educate their employees to prevent such attacks. (L2, CO2)
8. Investigate the different types of malware threats, such as viruses, worms, and Trojans, and explain their impact on network security. (L2, CO2)

Rubrics:

Indicator	Average	Good	Excellent	Marks
Organization (2)	Readable with some mistakes and structured (1)	Readable with some mistakes and structured (1)	Very well written and structured (2)	
Level of content(4)	Minimal topics are covered with limited information (2)	Limited major topics with minor details are presented(3)	All major topics with minor details are covered (4)	
Depth and breadth of discussion(4)	Minimal points with missing information (1)	Relatively more points with information (2)	All points with in depth information(4)	
Total Marks(10)				

1. **What are the core components of the TCP/IP protocol stack and how do they contribute to the functioning of computer networks?**

Layers of TCP/IP Model
Application Layer
Transport Layer(TCP/UDP)
Network/Internet Layer(IP)
Data Link Layer (MAC)
Physical Layer

1. Physical Layer
It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

2. Data Link Layer
The packet's network protocol type, in this case, TCP/IP, is identified by the data-link layer. Error prevention and "framing" are also provided by the data-link layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

3. Internet Layer
This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

IP: IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
ICMP: ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
ARP: ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.
The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.

Example: Imagine that you are using a computer to send an email to a friend. When you click “send,” the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend’s computer can reassemble them into the original email message.

In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend’s computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

4. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

TCP: Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
UDP: The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

5. Application Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

HTTP and HTTPS: HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
SSH: SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted

connection. It sets up a secure session over a TCP/IP connection.
NTP: NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.
The host-to-host layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing communication between hosts (computers or other devices) on a network. It is also known as the transport layer.

Some common use cases for the host-to-host layer include:

Reliable Data Transfer: The host-to-host layer ensures that data is transferred reliably between hosts by using techniques like error correction and flow control. For example, if a packet of data is lost during transmission, the host-to-host layer can request that the packet be retransmitted to ensure that all data is received correctly.
Segmentation and Reassembly: The host-to-host layer is responsible for breaking up large blocks of data into smaller segments that can be transmitted over the network, and then reassembling the data at the destination. This allows data to be transmitted more efficiently and helps to avoid overloading the network.
Multiplexing and Demultiplexing: The host-to-host layer is responsible for multiplexing data from multiple sources onto a single network connection, and then demultiplexing the data at the destination. This allows multiple devices to share the same network connection and helps to improve the utilization of the network.
End-to-End Communication: The host-to-host layer provides a connection-oriented service that allows hosts to communicate with each other end-to-end, without the need for intermediate devices to be involved in the communication.
Example: Consider a network with two hosts, A and B. Host A wants to send a file to host B. The host-to-host layer in host A will break the file into smaller segments, add error correction and flow control information, and then transmit the segments over the network to host B. The host-to-host layer in host B will receive the segments, check for errors, and reassemble the file. Once the file has been transferred successfully, the host-to-host layer in host B will acknowledge receipt of the file to host A.

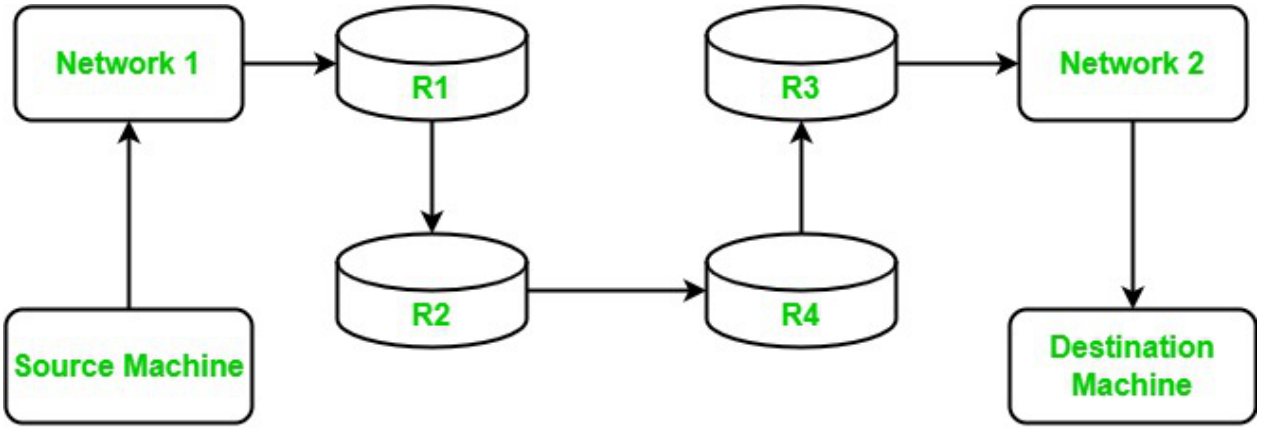
In this example, the host-to-host layer is responsible for providing a reliable connection between host A and host B, breaking the file into smaller segments, and reassembling the segments at the destination. It is also responsible for multiplexing and demultiplexing the data and providing end-to-end communication between the two hosts.

2. Explain the process of IP addressing and routing in a computer network. How does routing protocol help in efficient data transmission? (L2, CO1)

IP routing is one of the important topics in computer networks. IP routing is performed on the data which describes the path that data follows to reach from source to destination in the network. Through IP routing only the shortest path for the data is determined to reach the destination which decreases cost and data is sent in minimum time. IP routing uses different protocols and technologies for different networks. For IP routing we require some basics of IP addresses, routers, and different networks.

IP Routing:

IP routing is the process that defines the shortest path through which data travels to reach from source to destination. It determines the shortest path to send the data from one computer to another computer in the same or different network. Routing uses different protocols for the different networks to find the path that data follows. It defines the path through which data travel across multiple networks from one computer to other. Forwarding the packets from source to destination via different routers is called routing. The routing decision is taken by the routers.



IP Routing

IP (Internet Protocol) routing protocols play a crucial role in efficient data transmission across networks, especially in complex and interconnected networks. These protocols are responsible for determining the path that data should take from its source to its destination. Here are several ways in which IP routing protocols help in efficient data transmission:

Route Selection: IP routing protocols determine the best path or route for data to traverse from the source to the destination. They consider various factors such as network topology, link state, and path cost. This ensures that data takes the most efficient and reliable path, minimizing delays and packet loss.

Redundancy and Failover: Routing protocols can establish multiple paths to a destination, creating redundancy. In case one path fails due to network issues or hardware failures, the routing protocol can quickly reroute data along an alternative

path. This redundancy improves network reliability and minimizes downtime.

Load Balancing: Many routing protocols support load balancing, distributing traffic across multiple paths or links. This optimizes network resource utilization and prevents congestion on any single route, ensuring more efficient use of available bandwidth.

Scalability: IP routing protocols are designed to scale, making them suitable for both small and large networks. They can handle the complexity of large-scale networks and efficiently route data between thousands or even millions of devices.

Dynamic Adaptation: Routing protocols are dynamic in nature, meaning they continuously adapt to network changes. When new routes become available, existing routes become congested, or network conditions change, the routing protocol can reconfigure the routing tables to ensure data is transmitted efficiently.

Topology Discovery: Routing protocols help routers and switches discover the network topology and available routes. This information allows routers to make informed decisions on how to forward data packets.

Policy Enforcement: Routing protocols can be configured to enforce network policies. For example, you can set up routing policies to prioritize specific types of traffic, ensuring that critical data gets transmitted efficiently.

QoS (Quality of Service): Some routing protocols can support Quality of Service (QoS) features, allowing

Multicast Support: Many IP routing protocols support multicast, which enables efficient one-to-many or many-to-many communication. This is particularly important for applications like video conferencing and live streaming.

Interoperability: IP routing protocols are standardized and widely adopted, ensuring that different network devices from various vendors can communicate and work together efficiently. This interoperability simplifies network management and maintenance.

Overall, IP routing protocols are the backbone of the internet and other networks. They ensure that data is transmitted efficiently, reliably, and in accordance with network policies, making them essential for modern communication and data transfer.

3. Outline the key steps involved in ethical hacking and describe how these steps contribute to securing computer systems. (L2, CO1)

1. Reconnaissance

Reconnaissance, also known as the preparatory phase, is where the hacker gathers information about a target before launching an attack and is completed in phases prior to exploiting system vulnerabilities. One of the first phases of Reconnaissance is dumpster diving. It is during this phase that the hacker finds valuable information such as old passwords, names of important employees (such as the head of the network department), and performs an active reconnaissance to know how the organization functions. As a next step, the hacker completes a process called footprinting to collect data on the security posture, reduces the focus area such as finding out specific IP addresses, identifies vulnerabilities within the target system, and finally draws a network map to know exactly how the network infrastructure works to break into it easily. Footprinting provides important information such as the domain name, TCP and UDP services, system names, and passwords. There are also other ways to do footprinting, including impersonating a website by mirroring it, using search engines to find information about the organization, and even using the information of current employees for impersonation.

2. Scanning

In this phase, the hacker identifies a quick way to gain access to the network and look for information. There are three methods of scanning: pre-attack, port scanning/sniffing, and information extraction. Each of these phases demonstrates a specific set of vulnerabilities that the hacker can utilize to exploit the system's weaknesses. The pre-attack phase is where the hacker scans the network for specific information based on the information gathered during reconnaissance. The port scanner or sniffing phase is where scanning includes the use of dialers, port scanners, vulnerability scanners, and other data-gathering equipment. The information extraction phase is where the attackers collect information about ports, live machines and OS details to launch an attack.

3. Gain Access

The hacker gains access to the system, applications, and network, and escalates their user privileges to control the systems connected to it.

4. Maintain Access

Here, the hacker secures access to the organization’s Rootkits and Trojans and uses it to launch additional attacks on the network.

5. Cover Tracks

Once the hacker gains access, they cover their tracks to escape the security personnel.

They do this by clearing the cache and cookies, tampering the log files, and closing all the open ports. This step is important because it clears the system information making hacking a great deal harder to track.

4. Compare and contrast the OSI model and the TCP/IP model, highlighting their significance in understanding network communication. (L2, CO1)

OSI Model

OSI stands for Open Systems Interconnection. It has 7 layers: Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer. Each layer performs its task independently. It was developed in 1984 by the International Organization for Standardization (ISO).

Advantages

Both connection-oriented services and connectionless services are supported.
It is quite flexible.
All the layers work independently.
Disadvantages
Setting up a model is a challenging task.
Sometimes, it becomes difficult to fit a new protocol into this model.
It is only used as a reference model.

TCP/IP Model

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It has 4 layers named as Physical layer, Network layer, Transport layer, and Application layer. It also can be used as a communications protocol in a private computer network. It was designed by Vint Cerf and Bob Kahn in the 1970s.

Advantages

- Many Routing protocols are supported.
- It is highly scalable and uses a client-server architecture.
- It is lightweight.
- Disadvantages
- Little difficult to set up.
- Delivery of packets is not guaranteed by the transport layer.
- Vulnerable to a synchronization attack.

Similarities between OSI Model and TCP/IP Model:
OSI and TCP/IP both are logical models. One of the main similarities between the OSI and TCP/IP models is that they both describe how information is transmitted between two devices across a network. Both models define a set of layers. Each layer performs a specific set of functions to enable the transmission of data.

Another similarity between the two models is that they both use the concept of encapsulation, in which data is packaged into a series of headers and trailers that contain information about the data being transmitted and how it should be handled by the network.
For more information, you can refer to Similarities between TCP/IP model and the OSI model article.

5. Explain the process of information gathering and reconnaissance in the context of network security. How can attackers exploit this phase?

Any product, website, or network these days is not secure from cyber-attacks. To prevent vulnerabilities and attacks, organizations hire penetration testers to hack through their systems and find out these vulnerabilities to fix them. The first stage an ethical hacker or attacker has to go through during a cyber attack is called reconnaissance or Information gathering. Reconnaissance in general is a military term that means gathering information about an enemy target.

In cybersecurity, reconnaissance is a method used by cyber attackers or ethical hackers that refers to the process of gathering information about a target, such as a computer network, website, or individual, to identify vulnerabilities that can be exploited. This information-gathering process can be both automated and manual and can involve techniques such as port scanning, vulnerability scanning, social engineering, OSINT (open-source intelligence), passive reconnaissance, and active reconnaissance. The goal of reconnaissance in cybersecurity is typically to gain as much information as possible about a target to identify potential vulnerabilities that can be exploited in a future attack. Reconnaissance is the first step in the cyber kill chain, a methodology used to describe the stages of a cyber attack. It allows the attacker to gather information about the target and plan the attack accordingly.

Methods of Reconnaissance:

Several methods of information gathering are used in cybersecurity, each with its advantages and disadvantages. The two main methods of Information gathering in cyber security are :

Active Reconnaissance
This involves actively probing or interacting with the target system to gather information. Some examples of active reconnaissance include port scanning, vulnerability scanning, and social engineering. Active reconnaissance can provide a wealth of information about the target, but it also carries a higher risk of detection and can potentially disrupt the target's operations.

Passive Reconnaissance
This involves gathering information about the target without actively interacting with it. This is more like a detective gathering clues. Examples of passive reconnaissance include observing network traffic, analyzing DNS records, and using search engines to gather information about the target.

Passive reconnaissance is less likely to be detected and can provide a lot of information about the target, but it may be less detailed than active reconnaissance.

Several other information-gathering techniques come under these two methods. Some of the most common ones are listed below.

Information Gathering Techniques:

Social Engineering
Social engineering is the process of using psychological manipulation techniques to deceive people into providing sensitive information or performing certain actions. It is a form of passive reconnaissance that does not involve actively probing or interacting with a target system. Social engineering techniques can include phishing, baiting, scareware, impersonation, dumpster diving, and shoulder surfing.

Footprinting
This technique involves gathering information about the target's network infrastructure and assets, such as IP addresses, WHOIS records, DNS records, and other technical details.

Network Scanning
Network scanning is a technique used to identify active systems and open ports on a network. It is an active reconnaissance method that involves sending packets to a range of IP addresses or ports on a target system and analyzing the responses. Network scanning can be done using a variety of tools, such as ping sweeps and port scanners. The goal of network scanning is to create a map of the target network, including the IP addresses of active systems, open ports, and services. This information can help security professionals identify vulnerabilities and plan their attacks.

Vulnerability Scanning
This technique involves using specialized tools to scan a target's assets for known vulnerabilities.

War Dialing
War dialing is a technique used in reconnaissance in cybersecurity that involves automatically dialing a range of phone numbers to identify active modems. It is an active reconnaissance method that is used to identify potential targets for a future attack. War dialing is typically done by using specialized software tools, which can dial a large number of phone numbers in a short period. Once a modem is identified, the war dialer will attempt to connect to the modem and determine if it is accessible and what type of device it is. War dialing is a relatively simple but effective technique that can be used to identify potential vulnerabilities in a target system. It can also be used as a means of identifying phone numbers that are in use and potentially in use by employees of a target organization.

Reconnaissance with physical observation
This technique involves physically observing the target's location, activities, and assets.

Dumpster Diving

Dumpster diving is a technique used in cybersecurity that involves looking through an organization's trash to gather information. It is a form of physical reconnaissance that can be used to gain information about a target organization. Dumpster driving can be used to find information that has been discarded, such as old documents, memos, and hardware. The information found can be used to gain an understanding of the target organization's security policies and procedures, as well as gain access to sensitive information such as login credentials, network diagrams, and other confidential data.

Open-source Intelligence (OSINT)

Open-Source Intelligence (OSINT) refers to the process of collecting, analyzing, and disseminating publicly available information. The information can be found on various sources such as the internet, social media, newspapers, publications, government reports, etc.

OSINT is used to gather information about a wide range of topics, including political, economic, military, and security-related issues. The goal of OSINT is to gather the information that is not classified but could be valuable for decision-making, threat intelligence, investigations, and research purposes.

Information collected and exploited by the hackers during these phases:

MITRE(Massachusetts Institute of Technology Research and Engineering) has identified a number of reconnaissance techniques used by attackers to collect actionable information, such as:

Active IP addresses, hostnames, open ports, certificates, server banners, gateways, and routers
Credentials, emails, employee names, roles, departments/divisions, and physical location
Antivirus and EDR tools, SIEM systems (security information and event management), security vendors, software, hardware, firmware, and operating systems
Domain names, subdomains, CDN, mail servers, and other hosts
Public WHOIS data such as DNS name servers, IP blocks, and contact information
Financial data and intellectual property
Purchased data from reputable sources or black markets
While many of these data types would likely require a direct interaction such as active scanning, it’s still possible to use the results of a previous active scan in a passive analysis, for example, by using a dedicated search engine such as Shodan.

Sometimes, hackers only need Google and motivation to find vulnerabilities to exploit.

Corporate websites or apps can reveal details about the business relationships, the supply chain, and other sensitive elements. Adversaries can also leverage social media to stalk victims and collect precious information.

6. Differentiate between vulnerability assessment and penetration testing. Provide examples of tools used for each of these processes.

S.No.	Penetration Testing	Vulnerability Assessments
1.	This is meant for critical real-time systems.	This is meant for non-critical systems.
2.	This is ideal for physical environments and network architecture.	This is ideal for lab environments.
3.	It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
4.	It cleans up the system and gives a final report.	It attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
5.	It gathers targeted information and/or inspect the system.	It allocates quantifiable value and significance to the available resources.
6.	It tests sensitive data collection.	It discovers the potential threats to each resource.

7.	It determines the scope of an attack.	It makes a directory of assets and resources in a given system.
8.	The main focus is to discover unknown and exploitable weaknesses in normal business processes.	The main focus is to list known software vulnerabilities that could be exploited.
9.	It is a simulated cyberattack carried out by experienced ethical hackers in a well-defined and controlled environment.	It is an automated assessment performed with the help of automated tools.
10.	This is a goal-oriented procedure that should be carried out in a controlled manner.	This cost-effective assessment method is often considered safe to perform.

Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the preexisting flaws in their code and where they are located. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration

testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

Vulnerability assessment tools:

1. Nikto2

Nikto2 is an open-source vulnerability scanning software that focuses on web application security. Nikto2 can find around 6700 dangerous files causing issues to web servers and report outdated servers based versions. On top of that, Nikto2 can alert on server configuration issues and perform web server scans within a minimal time.

Nikto2 doesn't offer any countermeasures for vulnerabilities found nor provide risk assessment features. However, Nikto2 is a frequently updated tool that enables a broader coverage of vulnerabilities.

2. Netsparker

Netsparker is another web application vulnerability tool with an automation feature available to find vulnerabilities. This tool is also capable of finding vulnerabilities in thousands of web applications within a few hours.

Although it is a paid enterprise-level vulnerability tool, it has many advanced features. It has crawling technology that finds vulnerabilities by crawling into the application. Netsparker can describe and suggest mitigation techniques for vulnerabilities found. Also, security solutions for advanced vulnerability assessment are available.

3. OpenVAS

OpenVAS is a powerful vulnerability scanning tool that supports large-scale scans which are suitable for organizations. You can use this tool for finding vulnerabilities not only in the web application or web servers but also in databases, operating systems, networks, and virtual machines.

OpenVAS receives updates daily, which broadens the vulnerability detection coverage. It also helps in risk assessment and suggests countermeasures for the vulnerabilities detected.

4. W3AF

W3AF is a free and open-source tool known as Web Application Attack and Framework. This tool is an open-source vulnerability scanning tool for web applications. It creates a framework which helps to secure the web application by finding and exploiting the vulnerabilities. This tool is known for user-friendliness. Along with vulnerability scanning options, W3AF has exploitation facilities used for penetration testing work as well.

Moreover, W3AF covers a high-broaden collection of vulnerabilities. Domains that are attacked frequently, especially with newly identified vulnerabilities, can select this tool.

Penetration testing tools:

1. Kali Linux

Kali Linux
License: open source
Kali Linux is an operating system that facilitates penetration testing, security forensics, and related activities. It is a Linux distribution based on Debian, provided as open source and maintained by Offensive Security.

Kali Linux includes the following tools :
Armitage—graphical network attack management tool
Nmap—port scanner
Wireshark—packet analyzer
Metasploit—penetration testing framework with thousands of exploit modules
John the Ripper—password cracker
sqlmap—automated SQL injection and database import
Aircrack-ng—software suite for wireless LAN penetration testing
OWASP ZAP—web application security scanner
Burp suite—application security testing

2. Burp Suite

Burp Suite
License: free and paid options
Burp Suite is a suite of application security testing tools developed by Portswigger. The suite includes the popular web proxy Burp Proxy.

Burp Proxy allows penetration testers to conduct man-in-the-middle (MitM) attacks between a web server and a browser. They allow inspection of network traffic, which can help detect and exploit vulnerabilities and data leaks in web applications.

Key features of Burp Suite include:

- Using a dedicated client to perform manual testing for out-of-band vulnerabilities.
- Testing and confirming clickjacking attacks with specialist tooling.
- Assessment of token strength by testing quality of randomness in token data items.
- Deep manual testing, making it possible to see reflected or stored inputs to test for XSS and similar vulnerabilities.
- Records results of automated attacks and enables testers to fine-tune them in subsequent attacks.
- Enables faster brute-forcing and fuzzing with custom sequences of HTTP requests containing multiple payload sets.
- Constructs CSRF exploits, making it possible to generate exploit HTML demonstrating a CSRF attack for any suitable request

3. Wireshark
Wireshark
License: open source
Wireshark is a network monitoring solution that captures and analyzes network traffic across a variety of communication channels. Penetration testers can automatically read real-time data from different types of networks, such as Ethernet, token ring, loopback, and asynchronous transfer mode (ATM) connections.

IT professionals can capture packet data from live networks and analyze packets in the captured files through a graphical user interface (GUI). Wireshark allows users to modify captured files using command-line switches, apply complex filters, and create plugins to analyze new protocols. It also enables creating modelines to alter configuration files in real time.

Wireshark enables penetration testers to investigate security issues on a network, identify elements of the network that are malfunctioning and could be exploited in an attack, and detect protocol implementation or configuration errors.

Additional features include:

- Data encryption
- Compliance management capabilities
- Server monitoring and alerting
- Data import/export

4. John the Ripper
John the Ripper
License: open source
John the Ripper is a free password cracking tool that supports 15 operating systems, including 11 from the Unix family, DOS, Win32, BeOS, and OpenVMS.

The tool is customizable password cracker with many options for password testing, including:

- Auto-detection of password hash types.
- Wide support for encrypted password formats including Unix crypt hashes, Kerberos AFS tokens, and Windows LAN Manager (LM) hashes.
- Ability to crack password encryption based on DES, MD5, Blowfish, and MD4.
- Support for password hashes and passwords stored in databases and directory systems such as LDAP and MySQL.

7. Describe the key characteristics of social engineering attacks and discuss how organizations can educate their employees to prevent such attacks.

What is social engineering?
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Types of social engineering attacks:

Baiting
As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware
Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Pretexting
Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

All sorts of pertinent information and records are gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information

is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

Spear phishing
This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

How organizations can educate their employees to prevent such attacks:
Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

- Don't open emails and attachments from suspicious sources – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.

- Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multi factor authentication helps ensure your account's protection in the event of system compromise. Imperva Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.

- Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.

- Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

8. Investigate the different types of malware threats, such as viruses, worms, and Trojans, and explain their impact on network security.

Viruses-

A computer virus is a program which can harm our device and files and infect them for no further use. When a virus program is executed, it replicates itself by modifying other computer programs and instead enters its own coding. This code infects a file or program and if it spreads massively, it may ultimately result in crashing of the device. Across the world, Computer viruses are a great issue of concern as they can cause billions of dollars' worth of harm to the economy each year. Since the computer virus only hits the programming of the device, it is not visible. But there are certain indications which can help you analyze that a device is virus-hit.

Given below are such signs which may help you identify computer viruses:

- **Speed of the System** – In case a virus is completely executed into your device, the time taken to open applications may become longer and the entire system processing may start working slowly
- **Pop-up Windows** – One may start getting too many pop up windows on their screen which may be virus affected and harm the device even more
- **Self Execution of Programs** – Files or applications may start opening in the background of the system by themselves and you may not even know about them
- **Log out from Accounts** – In case of a virus attack, the probability of accounts getting hacked increase and password protected sites may also get hacked and you might get logged out from all of them
- **Crashing of the Device** – In most cases, if the virus spreads in maximum files and programs, there are chances that the entire device may crash and stop working

Worms-

A computer worm is a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems.A computer worm duplicates itself to spread to uninfected computers. It often does this by exploiting parts of an operating system that are automatic and invisible to the user.

Typically, a user only notices a worm when its uncontrolled replication consumes system resources and slows or halts other tasks. A computer worm is not to be confused with WORM, or write once, read many.

Computer worms often rely on vulnerabilities in networking protocols, such as File Transfer Protocol, to propagate.After a computer worm loads and begins running on a newly infected system, it will typically follow its prime directive: to remain active on an infected system for as long as possible and spread to as many other vulnerable systems as possible.

How do computer worms spread?

While some computer worms require user action to initially propagate, such as clicking on a link, others can easily spread without user interaction. All that's necessary is for the computer worm to become active on an infected system. Once active, the worm can spread over a network through its internet or local area network.

Before the widespread use of networks, computer worms spread through infected storage media, such as floppy disks, which, when mounted on a system, would infect other storage devices connected to the victim system.

Today, USB drives are a common vector for computer worms, as are internet activities such as email, chat and web surfing.

Types of worms:

Email worms

Email worms work by creating and sending outbound messages to all the addresses in a user's contact list. The messages include a malicious executable file that infects the new system when the recipient opens it.

Successful email worms usually employ social engineering and phishing techniques to encourage users to open the attached file.

File-sharing worms

File-sharing worms copy themselves into shared folders and spread through peer-to-peer file-sharing networks. Worm authors often disguise these malicious programs as media files.

Stuxnet, one of the most notorious computer worms to date, consists of two components: a worm to propagate malware through USB devices infected with the host file, and malware that targets supervisory control and data acquisition systems.

File-sharing worms often target industrial environments, including power utilities, water supply services and sewage plants.

Cryptoworms

Cryptoworms work by encrypting data on the victim's system. Perpetrators can use this type of worm in ransomware attacks, where they follow up with the victim and demand payment in exchange for a key to decrypt the files.

Internet worms
Some computer worms specifically target popular websites with poor security. If they can infect the site, they can infect a computer accessing the site.
From there, internet worms spread to other devices that the infected computer connects to through the internet and private network connections.

Instant messaging worms
Like email worms, instant messaging worms are masked by attachments or links, which the worm continues to spread to the infected user's contact list. The only difference is that instead of arriving in an email, it comes as an instant message on a chat service.
If the worm hasn't had time to replicate itself onto the computer, the user can change their password on the chat service account to prevent its spread.

Trojans-

A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code or software. Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as exporting files, modifying data, deleting files or otherwise altering the contents of the device. Trojans may be packaged in downloads for games, tools, apps or even software patches. Many Trojan attacks also leverage social engineering tactics, as well as spoofing and phishing, to prompt the desired action in the user.

Trojan: Virus or Malware?
A Trojan is sometimes called a Trojan virus or Trojan horse virus, but those terms are technically incorrect. Unlike a virus or worm, Trojan malware cannot replicate itself or self-execute. It requires specific and deliberate action from the user.

Trojans are malware, and like most forms of malware, Trojans are designed to damage files, redirect internet traffic, monitor the user’s activity, steal sensitive data or set up backdoor access points to the system. Trojans may delete, block, modify, leak or copy data, which can then be sold back to the user for ransom or on the dark web.

10 Types of Trojan Malware

Exploit Trojan: As the name implies, these Trojans identify and exploit vulnerabilities within software applications in order to gain access to the system.

Downloader Trojan: This type of malware typically targets infected devices and installs a new version of a malicious program onto the device.

Ransom Trojan: Like general ransomware, this Trojan malware extorts users in order to restore an infected device and its contents.

Backdoor Trojan: The attacker uses the malware to set up access points to the network.

Distributed Denial of Service (DDoS) attack Trojan: Backdoor Trojans can be deployed to multiple devices in order to create a botnet, or zombie network, that can then be used to carry out a DDoS attack. In this type of attack, infected devices can access wireless routers, which can then be used to redirect traffic or flood a network.

Fake AV Trojan: Disguised as antivirus software, this Trojan is actually ransomware that requires users to pay fees to detect or remove threats. Like the software itself, the issues this program claims to have found are usually fake.

Rootkit Trojan: This program attempts to hide or obscure an object on the infected computer or device in order to extend the amount of time the program can run undetected on an infected system.

SMS Trojan: A mobile device attack, this Trojan malware can send and intercept text messages. It can also be used to generate revenue by sending SMS messages to premium-rate numbers.

Banking Trojan or Trojan Banker: This type of Trojan specifically targets financial accounts. It is designed to steal data related to bank accounts, credit or debit cards or other electronic payment platforms.

Trojan GameThief: This program specifically targets online gamers and attempts to access their gaming account credentials.