| **Unit** | **Topics** |
| --- | --- |

| **I** | **Essential Knowledge about Security:** Security, Essentials, Security  **8**  Basics, Introduction to Ethical Hacking, Hacking Terminology, The Ethical Hacker.  **Reconnaissance: Information Gathering for the Ethical Hacker :** Footprinting, Passive Footprinting, Active Footprinting, Footprinting Methods and Tools, Search Engines, Website and Email Footprinting, DNS Footprinting, Network Footprinting, Other Tools.  **Scanning and Enumeration :** Fundamentals, TCP/IP Networking, Subnetting, Scanning Methodology, Identifying Targets, Port Scanning, Evasion, Vulnerability Scanning, Enumeration, Windows System,Basics, Enumeration Techniques. |
| --- | --- |
| **II** | **Sniffing and Evasion:** Essentials, Network Knowledge for Sniffing, Active and Passive, Sniffing, Sniffing Tools and Techniques, Techniques, Tools, Evasion, Devices Aligned Against You, Evasion Technique. **Attacking a System:** Getting Started, Windows Security Architecture,Linux Security Architecture, Methodology, Hacking Steps,Authentication and Passwords, Privilege Escalation and Executing Applications, Hiding Files and Covering Tracks. |
| **References:**  1. Matt Walker, “All in One, Certified Ethical Hacker”, Tata McGraw Hill, 2012. Ric 2. Messier, “CEHv10, Certified Ethical Hacker Study Guide”, Sybex – Wiley, 2019 3. I.P. Specialist, “CEH V10: EC-Council Certified Ethical Hacker Complete Training Guide”, IPSPECIALIST, 2018. | |

Unit 1 - Chapter 1 Essential Knowledge about Security

Q. Ethernet Frame Format

Q. The five zones by ECC

Q. CIA(Confidentiality, Integrity and Availability)

Q. Security Policies and types of security policies

|  | **Unit 2:** |
| --- | --- |
|  | **CHAPTER 5 Attacking a System** |
| 1 | Write a short note on Windows Security Architecture  ANSWER:  The Windows security architecture is a collection of processes that deliver, monitor, and manage the different security components of the operating system. Architecture is based on three principles: protection, detection, and response. The three components of Windows security are:  **1. LSA (Local Security Authority)**  ➢ The LSA is responsible for validating users for both local and remote logins. The LSA also maintains the local security policy.  ➢ During the local logon to a machine, a person enters his name and password to the logon dialog. This information is passed to the LSA, which then calls the appropriate authentication package. The password is sent in a nonreversible secret key format using a one-way hash function.  **2. SAM (Security Account Manager)**  ➢ The Security Accounts Manager is a database in the Windows operating system (OS) that contains usernames and passwords. SAM is part of the registry and can be found on the hard disk.  ➢ This service is responsible for making the connection to the SAM database (Contains available user-accounts and groups). The SAM database can either be placed in the local registry or in the Active Directory (If available). When the service has made the connection, it announces to the system that the SAM-database is available, so other services can start accessing the SAM-database.  **3. SRM (Security Reference Monitor)**  ➢ Security Reference Monitor is a security architecture component that is used to control user requests to access objects in the system. The SRM enforces the access validation and audit generation. Windows NT forbids direct access to objects. Any access to an object must first be validated by the SRM. For example, if a user wants to access a specific file the SRM will be used to validate the request. The Security Reference Monitor enforces access validation and audit generation policy.  ➢ The reference monitor verifies the nature of the request against a table of allowable access types for each process on the system |
| 2 | List and explain the root-level keys in the registry.  ANSWER:  ● A key can be thought of as a location pointer (much like a folder in the regular file structure), and the value of that key defines the setting. Keys are arranged in a hierarchy, with root keys at the top, leading downward to more specific settings.  ● The root-level keys in the registry are as follows:  ➢ HKEY\_LOCAL\_MACHINE (HKLM) Contains information on hardware (processor type, bus architecture, video, disk I/O, and so on) and software (operating system, drivers, services, security, and installed applications).  ➢ HKEY\_CLASSES\_ROOT (HKCR) Contains information on file associations and Object Linking and Embedding (OLE) classes.  ➢ HKEY\_CURRENT\_USER (HKCU) Contains profile information for the user currently logged on. Information includes user-level preferences for the OS and applications.  ➢ HKEY\_USERS (HKU) Contains specific user configuration information for all currently active users on the computer.  ➢ HKEY\_CURRENT\_CONFIG (HKCC) Contains a pointer to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\ Hardware Profiles\Current, designed to make accessing and editing this profile information easier. |
| 3 | Write a short note on Linux Security Architecture.  ANSWER:  Linux Security Architecture is designed to provide a secure computing environment. Here are some key aspects:   * [**Security-Enhanced Linux (SELinux):** SELinux is a security architecture for Linux systems that allows administrators to have more control over who can access the system1](https://www.redhat.com/en/topics/linux/what-is-selinux). [It was originally developed by the United States National Security Agency (NSA) as a series of patches to the Linux kernel using Linux Security Modules (LSM)1](https://www.redhat.com/en/topics/linux/what-is-selinux). [SELinux defines access controls for the applications, processes, and files on a system1](https://www.redhat.com/en/topics/linux/what-is-selinux). * [**Open-Source Security Advantage:** Linux source code undergoes constant, thorough review by members of the vibrant, global open-source community](https://www.redhat.com/en/topics/linux/what-is-selinux)[2](https://linuxsecurity.com/features/how-secure-is-linux). [As a result of this scrutiny, Linux security vulnerabilities are generally identified and eliminated very rapidly](https://www.redhat.com/en/topics/linux/what-is-selinux)[2](https://linuxsecurity.com/features/how-secure-is-linux). * [**User Privilege Model:** Linux greatly restricts root access through a strict user privilege model](https://www.redhat.com/en/topics/linux/what-is-selinux)[2](https://linuxsecurity.com/features/how-secure-is-linux). [On Linux, the superuser owns all the privileges, and ordinary users are only granted enough permissions to accomplish common tasks](https://www.redhat.com/en/topics/linux/what-is-selinux)[2](https://linuxsecurity.com/features/how-secure-is-linux). * [**Built-In Kernel Security Defenses:** The Linux kernel boasts an array of built-in security defenses including firewalls that use packet filters in the kernel, the UEFI Secure Boot firmware verification mechanism, the Linux Kernel Lockdown configuration option and the SELinux or AppArmor Mandatory Access Control (MAC) security enhancement systems2](https://linuxsecurity.com/features/how-secure-is-linux). |
| 4 | List and explain the important folders in the Linux file structure.  ANSWER.  Here’s a list of the important folders you’ll need to know:  ● **/A** forward slash represents the root directory.  ● /bin The **/bin** directory holds numerous basic Linux commands (a lot like the C:\Windows\System32 folder in Windows).  ● /dev This **/dev** folder contains the pointer locations to the various storage and input/output systems you will need to mount if you want to use them, such as optical drives and additional hard drives or partitions. Note that everything in Linux is a file.  ● /etc The **/etc** folder contains all the administration files and passwords. Both the password and shadow files are found here.  ● /home This **/home** folder holds the user home directories.  ● **/mnt** This folder holds the access locations you’ve actually mounted.  ●  **/sbin** Another folder of great importance, the system binaries folder holds more administrative commands and is the repository for most of the routines Linux runs (known as daemons).  ● **/usr** Amazingly enough, the usr folder holds almost all of the information, commands, and files unique to the users. |
| 5 | List and explain any 6 Linux Commands.  ANSWER:   * **adduser** Adds a user to the system * **Cat** Displays the contents of a file * **Cp** Copies. * **Ifconfig** Much like ipconfig in Windows, this command displays network configuration information about your NIC. * Kill Kills a running process. (You must specify the process ID number) * **Is** Displays the contents of the folder. The I option provides the most information about the folder contents. * **Man** Displays the “manual” page for a command (much like a help file). Password Used to change your password. * **Ps** Process status command. Using the -ef option will show all the processes running on the system. * **Rm** Removes files. The command rm-r also recursively removes all directories and subdirectories on the path and provides no warning when deleting a write protected file. * **Su** Allows you to perform functions as another user. The sudo command version allows you to run programs with “super user”(root)privileges. |
| 6 | What is System Hacking? Draw a diagram representing System attack phases.  ANSWER:  System hacking is defined as the compromise between computer systems and software to access the target computer and steal or misuse their sensitive information.   * The malware and the attacker identify and exploit the vulnerability of the computer system to gain unauthorized access. * The hacking process has five phases. * These are as follows:  1. Reconnaissance 2. Scanning 3. Gaining Access 4. Maintaining access 5. Clearing tracks |
| 7 | What are Cyber Attacks? List and Explain web-based attacks.  ANSWER:  Cyber Attacks: A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic, or data and lead to cybercrimes, such as information and identity theft. We are living in a digital era. Nowadays, most people use computers and the Internet. Due to the dependency on digital things, illegal computer activity is growing and changing like any type of crime  **1. Injection attacks:** It is an attack in which some data will be injected into a web application to manipulate the application and fetch the required information. Example- SQL Injection, code Injection, log Injection, XML Injection, etc.  **2. DNS Spoofing:** DNS Spoofing is a type of computer security hacking. Whereby data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.  **3. Session Hijacking:** It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.  **4. Phishing:** Phishing is a type of attack that attempts to steal sensitive information like user login credentials and credit card numbers. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.  **5. Brute force:** It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user passwords and personal identification numbers. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.  **6. Denial of Service:** It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses a single system and a single internet connection to attack a server. It can be classified into the following Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site and is measured in bit per second. Protocol attacks- It consume actual server resources and is measured in a packet. Application layer attacks- Its goal is to crash the web server and is measured in request per second.  **7. Dictionary attacks:** This type of attack stored the list of a commonly used password and validates them to get the original password.  **8. URL Interpretation:** It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.  **9. File Inclusion attacks:** This is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the included functionality.  **10. Man in the middle attacks:** It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert, and modify the data in the intercepted connection |
| 8 | What are Cyber Attacks? List and Explain system-based attacks. |
| 9 | Explain the Importance of Ethical hacking.  ANSWER:  Ethical hacking ensures that all the systems are secure and not vulnerable to black hat hackers.   * The hackers try to hack their systems. After hacking the system, they tell all the places where they found the weakness so that the company can fix it. Many companies also perform bug bounty programs. In this program, all the hackers around the world try to hack the website or web of that company. If the hacker finds any bug, the company will pay them a reward for the bug. * Ethical hacking is used to secure important data from enemies. It works as a safeguard of your computer from blackmail by the people who want to exploit the vulnerability. Using ethical hacking, a company or organization can find out security vulnerabilities and risks. * Governments use State-sponsored hacking to prevent intelligence information about influence politics, an enemy state, etc. Ethical hacking can ensure the safety of the nation by preventing cyber-terrorism and terrorist attacks. * Hackers can think from an attacker's perspective and find the potential entry point and fix them before any attacks. * Ethical hacking helps us learn new skills used in many roles like software developer, risk management, quality assurance tester, and network defender. * In a company, the trained ethical hackers are the main strength. To ensure the functions of software aptly, ethical hackers can apply quick security tests under extreme and standard conditions. * Ethical hackers develop many tools and methods and quality assurance testers to eliminate all the system's vulnerabilities. * In an organization, ethical hacking can identify the weakness of your software security. Using the hacker's perspective, you can look at your security and fix any anomalies before making a problem in the company's success. |
| 10 | Write a short note on HACKING STEPS: Authentication and Passwords.  ANSWER:  AUTHENTICATION:  Authentication is a crucial step in the hacking process. It involves gaining access to a system or network by exploiting known vulnerabilities. Here are the key points:   1. [Gaining Access: In this phase, the hacker uses the knowledge gained from previous phases to access sensitive data](https://www.javatpoint.com/hacking-process). [Techniques like brute-forcing can be used to gain access to the system](https://www.javatpoint.com/hacking-process). 2. [Maintaining Access: Once access is gained, hackers often want to maintain that access for future use](https://www.javatpoint.com/hacking-process). [This can be done by creating a backdoor, which allows the hacker to access the system any time in the future](https://www.javatpoint.com/hacking-process). [However, backdoors can be noisy and increase the chances of a hacker being discovered](https://www.javatpoint.com/hacking-process). 3. [Clearing Tracks: An ethical hacker will never want to leave a track about the activities while hacking](https://www.javatpoint.com/hacking-process). [This is done to avoid detection and to ensure that the hacker can continue to access the system in the future](https://www.javatpoint.com/hacking-process). 4. [Two-Factor Authentication (2FA) Hacking: Even with 2FA enabled, a system can still be vulnerable to hacking](https://theconversation.com/can-i-still-be-hacked-with-2fa-enabled-144682). [One method is SIM swapping, where the hacker contacts the carrier pretending to be the victim and requests a new SIM with the victim’s number](https://theconversation.com/can-i-still-be-hacked-with-2fa-enabled-144682). [Any authentication code sent to that number then goes directly to the hacker, granting them access to the victim’s accounts](https://theconversation.com/can-i-still-be-hacked-with-2fa-enabled-144682).   PASSWORD:  Hacking passwords is a common method used by hackers to gain unauthorized access to systems. Here are the key points:   1. [Dictionary Attack: This method involves using a list of dictionary words to guess the password1](https://www.javatpoint.com/password-cracking-in-ethical-hacking). [Hackers can quickly learn about a lot of passwords if they add a few punctuations like substituting $ for S and take a list of words](https://www.javatpoint.com/password-cracking-in-ethical-hacking). 2. [Brute-Force Attack: This method involves trying all possible combinations of characters until the correct password is found](https://www.javatpoint.com/password-cracking-in-ethical-hacking). [The length and complexity of the password determine the time it takes to crack it](https://www.javatpoint.com/password-cracking-in-ethical-hacking). 3. [Hybrid Attack: This is a combination of Dictionary attack and Brute force attack techniques](https://www.javatpoint.com/password-cracking-in-ethical-hacking). This attack first tries to crack the password using the dictionary attack. [If it is unsuccessful in cracking the password, it will use a brute-force attack](https://www.javatpoint.com/password-cracking-in-ethical-hacking). 4. [Credential Stuffing: In this method, hackers use stolen passwords from one online account to other accounts](https://www.datacenters.com/news/top-password-hacking-methods-plus-10-tips-for-creating-strong-passwords). 5. [Phishing Attacks: Hackers trick users into providing their passwords, often through deceptive emails or websites](https://www.makeuseof.com/tag/5-common-tactics-hack-passwords/). 6. [Keylogging: Hackers use malware to record a user’s keystrokes, capturing their passwords as they type them](https://www.datacenters.com/news/top-password-hacking-methods-plus-10-tips-for-creating-strong-passwords). |
| 11 | Write a short note on HACKING STEPS: Password Attacks.  ANSWER:  A password attack is a typical attack vector used to compromise user account authentication. As one of the most prominent application security concerns, it's responsible for most data breaches worldwide. Password breaches have far-reaching repercussions. Malevolent users only require illegal access to a single privileged account or a few users' accounts to compromise a web application. Password attacks involve abusing a compromised authorization vulnerability in the system, in combination with automatic password attack tools that accelerate password guessing and cracking. |
| 12 | Define and explain four main attack types for password cracking.  ANSWER:  ECC defines four main attack types for password cracking: non-electronic, active online, passive online, and offline.   * **Non-electronic:** - non-electronic attacks or non-technical attacks are attacks that do not require any type of technical understanding and knowledge. This is the type of attack that can be done by shoulder surfing, social engineering, and dumpster diving. For example, gathering username and password information by standing behind a target when he is logging in, interacting with sensitive information, or else. * **active online-Active** Online Attacks includes different techniques that directly interact with the target for cracking the password. Active Online attacks include: -   ➢ Dictionary Attack  ➢ Brute Force Attack  ➢ Hash Injection   * **passive online:** Passive online attacks are performed without interfering with the target. Importance of these attacks is because of extraction of the password without revealing the information as it obtains password without directly probing the target. The most common types of Passive Online Attacks are:   ➢ Wire Sniffing  ➢ Man-in-the-Middle Attack  ➢ Replay Attack   * **Offline attacks:** Offline attacks occur when the hacker steals a copy of the password file and works the cracking efforts on a separate system. These attacks may require some form of physical access to the machine where the attacker pulls the password file to removable media and then sneaks off to crack passwords at his leisure, but the point is you steal the hashes and take them somewhere else to bang on. Password cracking offline can be done in one of three main ways:   ➢ dictionary attack  ➢ hybrid attack  ➢ bruteforce attack. |
| 13 | Write a short note on: LLMNR/NBT-NS (Link-Local Multicast  Name Resolution and NetBIOS Name Service) attack.  ANSWER:  Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are two name services used by windows for resolving hostnames to IP addresses when a DNS request fails in a network. Using the LLMNR host resolution has a severe security impact, as when a non-existing host is searched using the LLMNR method. it broadcasts the request to every system that is connected to the local network. and if we have any compromised machine on the local network by default it will also receive the host query request, and the compromised machine can also send the response to the victim machine. and in turn, ask for the password hash of the victim. |
| 14 | Write a short note on HACKING STEPS: Privilege Escalation and Executing Applications |
| 15 | Write a short note on HACKING STEPS: Hiding Files and Covering Tracks.  ANSWER:  Hiding a file or folder in Windows makes it invisible when browsing through folders. You can hide files and folders in Windows by following these steps:   * Navigate to the file or folder you want to hide. * Right-click the file or folder and choose Properties. * Under the General tab, check the Hidden box and click OK. * When the confirmation message appears, select the Apply changes to this folder, subfolders, and files option to hide the folder and its content.   You can also hide files and folders in Windows using the Command Prompt. To do this, you can:   * Press Windows + R to launch the Run menu. * Enter cmd and hit Enter. * Navigate to your target folder or file using the CD and DIR commands. * To hide a file or folder, use the following command: attrib +h "replace this with target file or directory name". Covering Tracks 1. Covering tracks is the final stage of a penetration test. The goal is to erase the digital signs left by the pen tester during the earlier stages of the test. These digital signs prove the pen tester's presence in the targeted computer system. 2. Covering tracks is also important because it gives clues to forensics analysts or Intrusion Detection Systems (IDS). After gaining access, escalating privileges, and executing the application, the next step is to wipe the evidence to get back. In the phase of covering track, the attacker removes all the event logs, error messages, and other evidence to prevent its attack from being discovered easily. Most Common techniques that are often used by attackers to cover tracks on the target system are: - ● Disable Auditing ● Clearing Logs ● Manipulating Log |

**CHAPTER 4 Sniffing and Evasion**

* + - 1. Describe sniffing concepts, including active and passive sniffing.

Answer –

**Sniffing** is a network monitoring technique used to capture and analyze data packets as they travel through a network. Sniffing can be used for legitimate purposes, such as network troubleshooting and performance monitoring, or for malicious activities like capturing sensitive information such as passwords and confidential data.

**Types of Sniffing: Active and Passive**

1. **Passive Sniffing**:
   * **Definition**: Passive sniffing involves monitoring and capturing data packets without altering or interacting with the traffic on the network.
   * **Operation**: It operates by placing the network interface card (NIC) into promiscuous mode, allowing the system to capture all packets on the network segment, not just those addressed to it.
   * **Use Case**: Primarily used in networks where traffic is broadcasted, like Ethernet hubs, or on Wi-Fi networks where monitoring does not interfere with the data transmission.
   * **Detection**: Difficult to detect because it does not generate any additional network traffic or alter the flow of data.
2. **Active Sniffing**:
   * **Definition**: Active sniffing involves actively interacting with the network to capture data. This can include injecting packets, manipulating traffic, or conducting man-in-the-middle (MitM) attacks.
   * **Operation**: Techniques such as ARP (Address Resolution Protocol) spoofing, MAC (Media Access Control) flooding, and DHCP (Dynamic Host Configuration Protocol) spoofing are often used to redirect or flood network traffic, making it easier to capture.
   * **Use Case**: More commonly used in switched networks where data is sent only to the intended recipient, making passive sniffing ineffective.
   * **Detection**: Easier to detect than passive sniffing because it generates abnormal network traffic, such as unexpected ARP replies or excessive network congestion.
     + 1. Protocols Susceptible to Sniffing.

Answer –

 Unencrypted **Protocols**:

* **HTTP**: Since HTTP does not encrypt the data being transferred, it is highly vulnerable to sniffing. Any sensitive information transmitted, like login credentials or personal data, can be easily captured.
* **FTP (File Transfer Protocol)**: Like HTTP, FTP transmits data, including usernames and passwords, in plain text, making it susceptible to sniffing.
* **Telnet**: Telnet is a remote login protocol that also transmits data in plain text, allowing an attacker to capture and read login credentials and other sensitive information.
* **POP3/IMAP**: These are email protocols used to retrieve messages from a server. When used without encryption, they are vulnerable to sniffing, allowing attackers to capture email contents, including attachments.

 Vulnerable **Encrypted Protocols**:

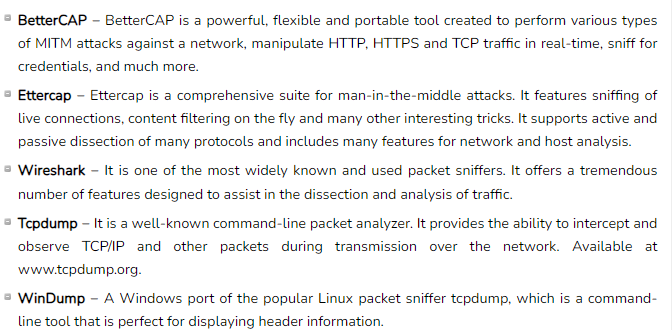
* **WEP (Wired Equivalent Privacy)**: An older encryption protocol for Wi-Fi networks, WEP is highly vulnerable to sniffing and cracking due to its weak encryption algorithm.
* **SSL/TLS (if improperly configured)**: Although SSL/TLS is designed to encrypt data, improper configuration or the use of outdated versions (like SSL 2.0/3.0) can make it vulnerable to sniffing attacks such as SSL stripping or downgrade attacks.

A close-up of a document

Description automatically generated

3. Describe sniffing tools and understand their output.

Answer –



A screenshot of a computer

Description automatically generated

4. Describe intrusion detection system (IDS) and types of Evasion Technique For IDS.

Answer –

**Intrusion Detection System (IDS)**

**IDS** stands for Intrusion Detection System. It is used to monitor traffic entering any network and helps in detecting malicious activity. It is important to note that IDS only detects malicious activities and does not prevent attacks.

This article describes various techniques to evade IDS (Intrusion Detection System) and their implementation using the NMAP tool.

Organizations might have IDS in place to monitor network traffic before packets are routed to their internal networks. IDS employs various methods to detect suspicious activities:

1. Anomaly-based
2. Signature-based
3. Host-based
4. Network-based

**Evasion Techniques for IDS**

Attackers may use various evasion techniques to bypass an IDS, avoiding detection and gaining unauthorized access to systems or data.

**1. Packet Fragmentation:**In this technique, the IP packets are split into smaller fragments. By doing this, the TCP header is split across multiple fragments. When IDS encounter the packets, they enqueue them to check for any malicious activity. However, as the number of fragments increases, there is an increase in the CPU and network bandwidth consumption. For this reason, IDS ignores evaluating such packets. Hence, these fragments may pass undetected through the IDS.

**2. Source Routing:**Packets pass through a number of routers before reaching the target host. Routers consult the routing table to pass the packet to the next hop. IDS are also put in place to monitor the network traffic. However, the route taken by the packets can be manipulated by the attacker. The attacker can make sure that the packets take a route that does not contain the IDS.

**3. Source Port Manipulation:** Sometimes IDS might allow network packets to pass without any inspection if they arrive at a particular port like port 80 which is primarily used for HTTP. This improper configuration can be exploited by attackers by manipulating the source port of packets. Hence, packets arriving at such ports can go unnoticed by the IDS.

**4. IP Address Decoy:** The attacker sends packets to the target host by using the IP addresses of other hosts. So different packets have different IP addresses. This technique is used to scan ports at the target host. So, an attacker can identify whether a particular port at the target host is running or not.

**5. IP Address Spoofing:** IP Address Spoofing simply means using some other machine’s IP address to send packets to the target host. Again, this technique can be used to scan ports which are usually done before the actual attack. So the IDS may identify the innocent hosts as malicious ones.

**6. Customizing Packets:**IDS can be evaded by customizing the data packets. Customizing can be done by replacing data in the payload or appending data to the payload.

* Honeypot is a network-attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by hackers.
* It acts as a potential target on the internet and informs the defenders about any unauthorized attempt on the information system.
* Honeypots are mostly used by large companies and organizations involved in cybersecurity.
* It helps cybersecurity researchers to learn about the different types of attacks used by attackers.
* It is suspected that even cybercriminals use these honeypots to decoy researchers and spread wrong information.
* The cost of a honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organization’s resources still preventing attacks at the backend and access to any production system.

A honeynet is a combination of two or more honeypots on a network.

**MCQ Question & Answer**

Unit 1 - Chapter 1

**1. What is the primary goal of security in the context of information technology?**

A) To ensure data is available only to authorized users  
B) To make data publicly accessible  
C) To reduce the size of data files  
D) To hide data from all users

*Answer: A) To ensure data is available only to authorized users*

**2. Which of the following is NOT a component of the CIA triad in security?**

A) Confidentiality  
B) Integrity  
C) Availability  
D) Authentication

*Answer: D) Authentication*

**3. Which of the following best defines ethical hacking?**

A) Hacking done for personal gain  
B) Unauthorized access to systems  
C) Penetration testing with permission  
D) Spreading malware ethically

*Answer: C) Penetration testing with permission*

**4. What term is used to describe a hacker with good intentions who helps organizations improve their security?**

A) Black Hat Hacker  
B) Grey Hat Hacker  
C) White Hat Hacker  
D) Script Kiddie

*Answer: C) White Hat Hacker*

**5. In hacking terminology, what is a "zero-day" exploit?**

A) An exploit that has been patched  
B) An exploit targeting previously unknown vulnerabilities  
C) An exploit that affects only outdated systems  
D) An exploit that can be used indefinitely

*Answer: B) An exploit targeting previously unknown vulnerabilities*

**6. Which of the following is an example of social engineering?**

A) Installing antivirus software  
B) Guessing a password  
C) Phishing emails  
D) Updating a firewall

*Answer: C) Phishing emails*

**7. What is the primary role of an ethical hacker in an organization?**

A) To perform unauthorized attacks  
B) To test and improve security systems  
C) To steal sensitive data  
D) To create malware for testing purposes

*Answer: B) To test and improve security systems*

**8. Which hacking term refers to a technique used to discover live hosts, ports, or services within a network?**

A) Sniffing  
B) Spoofing  
C) Scanning  
D) Phishing

*Answer: C) Scanning*

**9. What does the term "hacker" originally refer to?**

A) A criminal breaking into systems  
B) A person who explores and learns about computer systems  
C) A person who writes viruses  
D) A professional coder

*Answer: B) A person who explores and learns about computer systems*

**10. Which of the following actions would be considered illegal hacking?**

A) Testing a company’s security with their permission  
B) Accessing a system without authorization  
C) Reporting a vulnerability to the system owner  
D) Educating users about security threats

*Answer: B) Accessing a system without authorization*

Chapter 2

**1. What is the primary purpose of footprinting in ethical hacking?**

A) To exploit vulnerabilities in a system  
B) To gather information about a target system  
C) To delete system logs  
D) To gain unauthorized access to a network

*Answer: B) To gather information about a target system*

**2. Which of the following is an example of passive footprinting?**

A) Social engineering  
B) Port scanning  
C) WHOIS lookup  
D) Banner grabbing

*Answer: C) WHOIS lookup*

**3. Which of the following methods is commonly used in active footprinting?**

A) Searching social media profiles  
B) Checking domain registry records  
C) Conducting a DNS zone transfer  
D) Reading press releases

*Answer: C) Conducting a DNS zone transfer*

**4. What is the main difference between passive and active footprinting?**

A) Passive footprinting is legal, while active footprinting is illegal  
B) Passive footprinting gathers data without interacting with the target, while active footprinting involves direct interaction  
C) Passive footprinting requires tools, while active footprinting does not  
D) Passive footprinting is performed after gaining access to the system, while active footprinting is done before

*Answer: B) Passive footprinting gathers data without interacting with the target, while active footprinting involves direct interaction*

**5. Which tool is commonly used for DNS footprinting?**

A) Nslookup  
B) Metasploit  
C) Wireshark  
D) Nmap

*Answer: A) Nslookup*

**6. What kind of information can be gathered from a WHOIS lookup?**

A) Open ports on a server  
B) Domain ownership and contact information  
C) List of vulnerabilities  
D) IP addresses of all devices in a network

*Answer: B) Domain ownership and contact information*

**7. Which of the following tools can be used for network footprinting?**

A) Ping  
B) Maltego  
C) Traceroute  
D) All of the above

*Answer: D) All of the above*

**8. In website footprinting, what does the process of "mirroring" a website involve?**

A) Duplicating the content of a website for offline analysis  
B) Redirecting traffic to a different website  
C) Monitoring changes in a website  
D) Creating a fake website to capture user information

*Answer: A) Duplicating the content of a website for offline analysis*

**9. Which search engine technique is commonly used for finding sensitive information exposed by mistake?**

A) Google Dorking  
B) Image search  
C) Keyword stuffing  
D) PageRank analysis

*Answer: A) Google Dorking*

**Chapter 3**

**1. Which layer of the TCP/IP model is responsible for routing data between devices?**

A) Application Layer  
B) Transport Layer  
C) Network Layer  
D) Data Link Layer

*Answer: C) Network Layer*

**2. In subnetting, what does the subnet mask 255.255.255.0 indicate about the network?**

A) There are 254 usable IP addresses  
B) There are 2 usable IP addresses  
C) There are 16 usable IP addresses  
D) There are 1024 usable IP addresses

*Answer: A) There are 254 usable IP addresses*

**3. Which of the following is a popular tool for performing port scanning?**

A) Wireshark  
B) Nmap  
C) Metasploit  
D) Nessus

*Answer: B) Nmap*

**4. What is the primary purpose of vulnerability scanning in network security?**

A) To exploit vulnerabilities  
B) To identify potential security weaknesses  
C) To evade security controls  
D) To create network maps

*Answer: B) To identify potential security weaknesses*

**5. Which type of scan sends a packet to each port and waits for a response to determine if the port is open?**

A) SYN Scan  
B) ACK Scan  
C) UDP Scan  
D) FIN Scan

*Answer: A) SYN Scan*

**6. What technique is used in network scanning to avoid detection by security systems?**

A) Spoofing  
B) Evasion  
C) Enumeration  
D) Fragmentation

*Answer: B) Evasion*

**7. Which enumeration technique involves querying DNS records to gather information about a network?**

A) SNMP Enumeration  
B) SMB Enumeration  
C) Zone Transfer  
D) LDAP Enumeration

*Answer: C) Zone Transfer*

**8. In Windows, which command can be used to view the current IP configuration of a system?**

A) ipconfig  
B) netstat  
C) tracert  
D) ping

*Answer: A) ipconfig*

**9. Which scanning method involves sending ICMP echo requests to identify active hosts on a network?**

A) TCP Scan  
B) UDP Scan  
C) Ping Sweep  
D) Xmas Scan

*Answer: C) Ping Sweep*

**10. What is the primary goal of enumeration in the context of ethical hacking?**

A) To identify live hosts  
B) To gather detailed information about a target  
C) To perform denial-of-service attacks  
D) To send phishing emails

*Answer: B) To gather detailed information about a target*

**Unit 2 - Chapter 4**

**1. What is network sniffing primarily used for?**

A) Encrypting network traffic  
B) Monitoring and capturing network data  
C) Speeding up network performance  
D) Blocking unauthorized users

*Answer: B) Monitoring and capturing network data*

**2. Which of the following best describes passive sniffing?**

A) Modifying network traffic to deceive the target  
B) Capturing data without altering the network traffic  
C) Actively intercepting and injecting packets into the network  
D) Scanning for open ports on a network

*Answer: B) Capturing data without altering the network traffic*

**3. What is an example of an active sniffing technique?**

A) Port mirroring  
B) MAC flooding  
C) Using a VPN  
D) Passive listening

*Answer: B) MAC flooding*

**4. Which tool is commonly used for network sniffing?**

A) Wireshark  
B) Microsoft Word  
C) Adobe Photoshop  
D) VMware

*Answer: A) Wireshark*

**5. What is the purpose of evasion techniques in network sniffing?**

A) To improve network speed  
B) To prevent detection by network security devices  
C) To capture all network traffic  
D) To encrypt network data

*Answer: B) To prevent detection by network security devices*

**6. Which of the following devices can detect and prevent network sniffing attempts?**

A) Hub  
B) Router  
C) Firewall  
D) Packet analyzer

*Answer: C) Firewall*

**7. What is the primary difference between active and passive sniffing?**

A) Active sniffing is undetectable, passive sniffing is detectable  
B) Active sniffing involves injecting packets, passive sniffing only listens  
C) Active sniffing is used for encryption, passive sniffing is for decryption  
D) There is no difference between active and passive sniffing

*Answer: B) Active sniffing involves injecting packets, passive sniffing only listens*

**8. Which of the following is a common technique used in evading network defenses during sniffing?**

A) Port scanning  
B) Protocol obfuscation  
C) DNS spoofing  
D) Social engineering

*Answer: B) Protocol obfuscation*

**9. What is a common defense mechanism against network sniffing?**

A) Using unencrypted protocols  
B) Implementing a flat network topology  
C) Enabling encryption protocols like HTTPS  
D) Disabling firewalls

*Answer: C) Enabling encryption protocols like HTTPS*

**10. Which of the following sniffing techniques relies on sending a flood of data to switch ports, forcing it to act like a hub?**

A) IP spoofing  
B) MAC flooding  
C) ARP poisoning  
D) DNS hijacking

*Answer: B) MAC flooding*

Chapter 5

**1. Which component is responsible for enforcing security policies in Windows Security Architecture?**

A) Registry Editor  
B) Security Account Manager (SAM)  
C) Local Security Authority (LSA)  
D) Kernel

*Answer: C) Local Security Authority (LSA)*

**2. In Linux Security Architecture, which command is used to modify file permissions?**

A) chown  
B) chmod  
C) ls  
D) ps

*Answer: B) chmod*

**3. What is the first step in the typical hacking methodology?**

A) Gaining Access  
B) Reconnaissance  
C) Covering Tracks  
D) Privilege Escalation

*Answer: B) Reconnaissance*

**4. Which of the following is a common method used to gain unauthorized access to a system?**

A) Installing updates  
B) Using a strong password  
C) Password cracking  
D) Monitoring system logs

*Answer: C) Password cracking*

**5. What is the purpose of privilege escalation in hacking?**

A) To reduce user access rights  
B) To gain higher-level access within a system  
C) To remove user access rights  
D) To disable security features

*Answer: B) To gain higher-level access within a system*

**6. Which of the following best describes a rootkit?**

A) A tool to patch software vulnerabilities  
B) A legitimate program used to manage user accounts  
C) Malicious software designed to hide the existence of certain processes or programs  
D) A method of encrypting files

*Answer: C) Malicious software designed to hide the existence of certain processes or programs*

**7. What is the primary objective of hiding files and covering tracks after a successful attack?**

A) To improve system performance  
B) To protect user data  
C) To avoid detection by system administrators  
D) To create backups of important data

*Answer: C) To avoid detection by system administrators*

**8. In Windows, what command would you use to view all running processes?**

A) ps  
B) tasklist  
C) ls  
D) netstat

*Answer: B) tasklist*

**9. In the context of authentication, what is a common weakness in password security?**

A) Using multi-factor authentication  
B) Using complex, long passwords  
C) Reusing the same password across multiple accounts  
D) Regularly updating passwords

*Answer: C) Reusing the same password across multiple accounts*

**10. What technique can be used by hackers to maintain access to a compromised Linux system?**

A) Removing user accounts  
B) Changing file ownership  
C) Installing a backdoor  
D) Disabling network services

*Answer: C) Installing a backdoor*