GRADAMIC

B.Tech–2nd Year Session 2023–24 Odd/Even Semester

Dr. A. P. J. Abdul Kalam Technical University
Lucknow, Uttar Pradesh

CYBER SECURITY

(BCC301 / BCC401/ BCC301H / BCC401H)

app.gradamic.com

UNIT – 3rd

UNIT-III

TOOLS AND METHODS USED IN CYBER SECURITY

Q-1 What are Proxy Servers? Write advantages and disadvantages.

It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

Advantages:

- **Anonymity:** proxy servers are that they can hide your IP address from the websites you visit.
- **Security:** A proxy server advantages is that they can filter or modify your web traffic according to your preferences
- **Performance:** proxy servers is that they can improve your internet speed and performance by caching frequently accessed web pages and files

Disadvantages:

- **Lack of encryption:** they may not encrypt your data or protect you from hackers, viruses, or malware.
- **Limited usability**: they may not support all types of web protocols or applications, such as streaming, gaming etc
- **Security concerns:** free proxy servers are that they may compromise your privacy by logging or leaking your browsing history or personal information. Logging is a process of recording your online activities and storing them on a server. Some proxy servers may log or leak your browsing history or personal information for various reasons, such as marketing, analytics, or legal compliance.

Q-2 What are Anonymizer? What is the reason of using Anonymizer?

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.

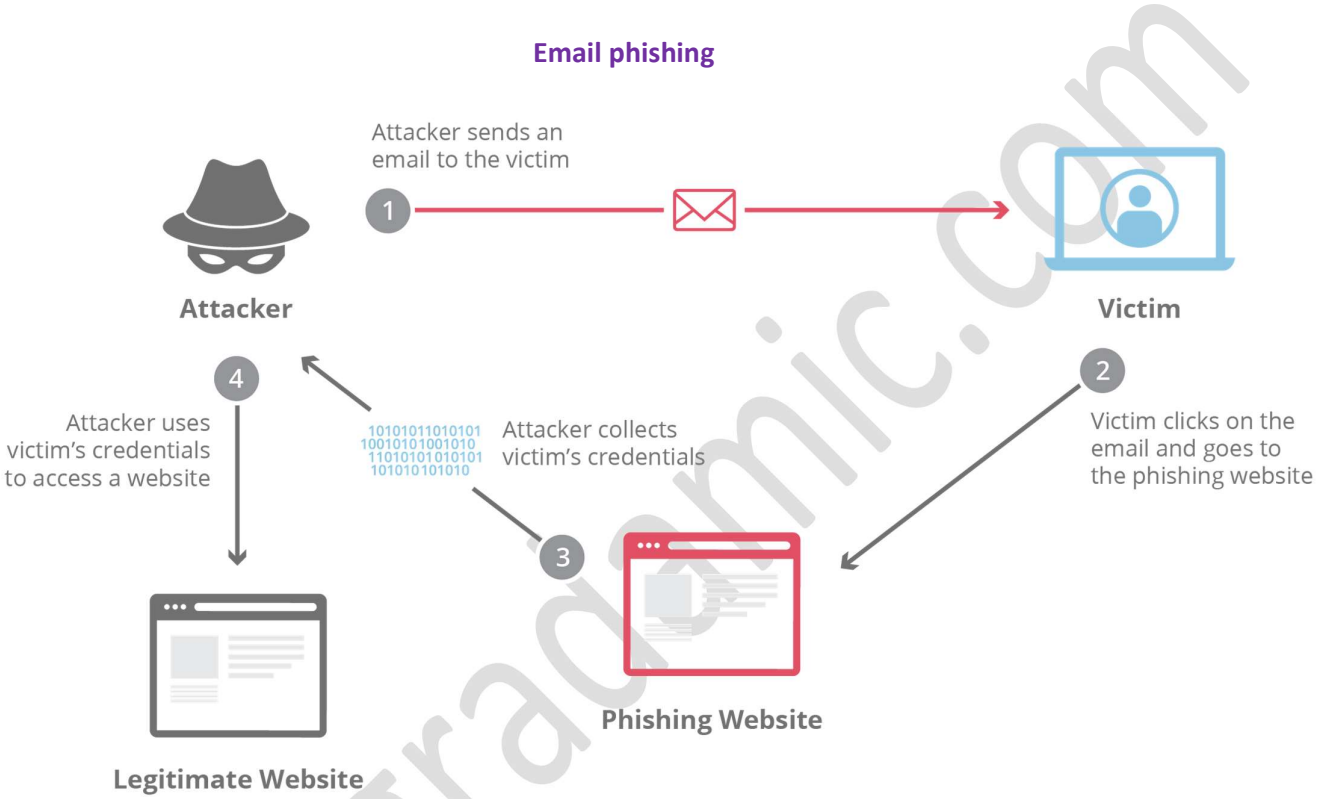
Reasons for using anonymizers.

- Anonymizers help minimize risk.
- They can be used to prevent identity theft, or to protect search histories from public disclosure.
- Anonymizers can help in allowing free access to all of the internet content, but cannot help against persecution for accessing the Anonymizer website itself.

Q-3 What is phishing? Explain its type and explain the working of phishing attack.

Phishing refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish. There are many type of phishing Email, spear, whaling etc.



- The general term given to any malicious email message meant to trick users into divulging private information.
- Attackers generally aim to steal account credentials, personally identifiable information (PII) and corporate trade secrets. However, attackers targeting a specific business might have other motives.

Spear phishing

These email messages are sent to specific people within an organization, usually high-privilege account holders, to trick them into divulging sensitive data, sending the attacker money or downloading malware

Whaling (CEO fraud)

- These messages are typically sent to high-profile employees of a company to trick them into believing the CEO or other executive has requested to transfer money

- CEO fraud falls under the umbrella of phishing, but instead of an attacker spoofing a popular website, they spoof the CEO of the targeted corporation.

Smishing and vishing: Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation. Angler phishing: using social media, attackers reply to posts pretending to be an official organization and trick users into divulging account credentials and personal information

Q-4 What is password cracking? Name some password cracking tools & classification of password attacks and guidelines?

Password Cracking

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources

Strong password characteristics

Be at least 12 characters long., Combine letters and a variety of characters., Avoid reusing a password., Pay attention to password strength indicators., Avoid easy-togues phrases and common passwords.

Password Cracking Tools

- **John the Ripper:** This is one of the oldest and most widely used password cracking tools. It supports various encryption algorithms and hash types and can run on multiple platforms, including Unix, Windows, macOS, and others.
- **Hash cat:** This is a highly efficient password cracking tool that supports various hash algorithms and can utilize the power of GPU acceleration to speed up the cracking process significantly.
- **Hydra:** Hydra is a popular online password cracking tool that supports various network protocols, including HTTP, FTP, SMTP, SSH, and others. It is commonly used for brute force attacks against login interfaces.
- **Medusa:** Medusa is similar to Hydra and is used for network-based password cracking. It supports various protocols and can perform brute-force attacks, dictionary attacks, and more
- **Rainbow Crack:** Rainbow Crack is a password cracking tool that uses rainbow tables to crack password hashes. Rainbow tables are precomputed tables containing the hash values of many possible passwords, which significantly speeds up the cracking process

Classification of password attack Online Password Cracking Attack:

- In online password cracking, attackers attempt to log in to a system or application using various methods to guess or steal passwords.
- Attackers may use techniques like phishing, keylogging, or social engineering to obtain passwords directly from users.
- Another method is a dictionary attack, where attackers use a list of commonly used passwords or words from the dictionary to guess passwords.

- Unlike offline attacks, online attacks require direct interaction with the target system, making them riskier for attackers as they may be detected more easily.

Example: An attacker sends phishing emails to employees of a company, tricking them into providing their passwords.

The attacker can then use these passwords to log in to the company's systems and steal sensitive information.

Offline Password Cracking:

- In offline password cracking, attackers have access to the hashed passwords but not the system or application where the passwords are used.
- Attackers use various tools and techniques to crack the hashed passwords without interacting with the target system.
- One common method is to use a precomputed table (rainbow table) that contains precomputed hash values for a large number of possible passwords.
- The attacker compares the hash values of the stolen passwords against the values in the rainbow table to find matches and recover the plaintext passwords.
- Another method is brute-force cracking, where attackers try all possible password combinations until they find the correct one.
- This method can be time-consuming and resource-intensive but is effective if the password is weak.

Example: An attacker steals a database of hashed passwords from a website and uses a rainbow table or brute-force attack to crack the passwords and gain access to user accounts.

General guidelines applicable to the password policies, which can be implemented organization-wide

- **Length & Complexity:** Require passwords to be at least 8 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters
- **Expiry & History:** Enforce password expiry every 60-90 days and prevent password reuse.
- **MFA:** Encourage or require multi-factor authentication (MFA) for sensitive systems.
- **Education:** Provide training on secure password practices and phishing awareness.
- **Storage:** Store passwords securely using strong hashing algorithms with salt.
- **Audits:** Regularly audit and review password policies for compliance and effectiveness.
- **Enforcement:** Enforce policies through technical controls and administrative measures.
- **Account Lockout:** Temporarily lock accounts after a certain number of failed login attempts.

Q-6 What is a keylogger? Also, explain the types and software that provide this facility and what is anti-keylogger.

Keylogger- It is defined like a keylogger is a type of software or hardware device that is designed to record keystrokes typed on a computer or mobile device or any electronic gadgets. Keyloggers can capture everything typed by a user, including usernames, passwords, emails, chat messages, and other sensitive information.

Type of keylogger:

1) **Software Keyloggers:** Software keyloggers are malicious programs that are installed on a computer or device without the user's knowledge. They can be installed through various means, such as phishing emails, malicious downloads, or exploiting vulnerabilities in software.
2) **Hardware Keyloggers:** Hardware keyloggers are physical devices that are connected between the keyboard and the computer or inserted into the USB port. Hardware keyloggers record keystrokes directly from the keyboard and store the data internally. Attackers can then retrieve the recorded data by accessing the device directly.

Software which provides keylogger facility

1) **Spyrix Personal Monitor:** Spyrix is a legitimate keylogger program designed for monitoring children, employees, or other users. It can track keystrokes, screenshots, web activity, and more. It's intended for parental control or employee monitoring purposes
2) **Refog Keylogger:** Refog Keylogger is another legitimate monitoring tool that can record keystrokes, capture screenshots, and track website visits. It's often used by parents or employers to monitor computer usage.
3) **Elite Keylogger:** Elite Keylogger is a commercial keylogger program that can record keystrokes, passwords, chat conversations, and more. It's available for Windows and macOS.
4) **Actual Keylogger:** Actual Keylogger is a Windows based keylogger program that records keystrokes, clipboard contents, and screenshots. It runs in stealth mode and can be used for monitoring or malicious purposes.

ANTIKEYLOGGER

An anti-keylogger is a type of software designed to detect and prevent the activity of keyloggers on a computer or device. Its primary purpose is to protect user privacy and prevent sensitive information, such as passwords, credit card numbers, and personal messages, from being captured by malicious keylogger programs.

Advantages

- **Prevents Identity Theft:** Blocks attempts to steal sensitive information, reducing the risk of identity theft Provides Peace of Mind: Users can browse and transact online without fear of data compromise.
- **Complements Antivirus:** Adds an extra layer of protection against keyloggers, working alongside antivirus software.
- **Prevents Keylogging:** Stops malicious programs from capturing sensitive information like passwords.
- **Enhances Privacy:** Safeguards personal and financial data from unauthorized access

Q-7 What is spyware? Explain the type of spyware.

Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.

Spyware collects personal and sensitive information that it sends to advertisers, data collection firms, or malicious actors for a profit. Attackers use it to track, steal, and sell user data, such as internet usage, credit card, and bank account details, or steal user credentials to spoof their identities.

TYPES OF SPYWARE

Keyloggers

1) **Tracking cookies:** Tracking cookies are dropped onto a device by a website and then used to follow the user's online activity.
2) **Trojan Horse Virus:** This brand of spyware enters a device through Trojan malware, which is responsible for delivering the spyware program
3) **Rootkits:** These enable attackers to deeply infiltrate devices by exploiting security vulnerabilities or logging into machines as an administrator. Rootkits are often difficult and even impossible to detect.
4) **System monitors:** These also track user activity on their computer, capturing information like emails sent, social media and other sites visited, and keystrokes.

Q-8 What is virus? Write down the characteristics and its types.

A virus is a type of malicious software (malware) that is designed to infect a computer system and spread from one host to another. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened.

Characteristics

- **Infection:** Attaches to executable files or documents, activating when the file is run or opened.
- **Replication:** Spreads by attaching copies of itself to other files or programs on the same system or network.
- **Payload**: Carries out harmful actions, such as deleting files, stealing information, or facilitating other malicious activities.
- **Concealment:** Attempts to hide its presence from users and antivirus software through techniques like encryption or polymorphism.

Types of Virus

1) **Macro Virus:** This type of computer virus is normally found in Microsoft Office programs. These viruses increase the size of files when they infect them, as they attach their own code. Once a macro virus infects a file, it can easily spread to other computers when that file is shared, for example via email
2) **Boot Sector Virus:** Much like beepers boot sector viruses are terrible little things that were big in the 90s. One of the oldest types of viruses, boot sector viruses go straight for the core of your computer, affecting the startup or 'boot' process. Back in the day, these viruses were spread through floppy disks. Nowadays, they attach themselves to emails or USB sticks. If your computer catches one of these, you'll need an expert to carry out a full system reformat (Windows, Mac)

3) **Trojan Horses:** Taking their name from the huge wooden horse in which the Greeks hid to get inside the ancient city of Troy, these are among the sneakiest of computer viruses. Used by cybercriminals, Trojan horses are disguised as normal programs, tempting you to install them on your computer.
Once installed, the viruses gain access to your computer's files and capture your private data think passwords and online banking information.
This can then be used by hackers to make online purchases with your bank account or expose your private information.

DIFFERENCE BETWEEN WORMS AND VIRUS

Sr.No.	Basis of Comparison	WORMS	VIRUS
1.	Definition	A Worm is a form of malware that replicates itself and can spread to different computers via Network.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
2.	Objective	The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.	The main objective of viruses is to modify the information.
3.	Host	It doesn't need a host to replicate from one computer to another.	It requires a host is needed for spreading.
4.	Harmful	It is less harmful as compared.	It is more harmful.
5.	Detection and Protection	Worms can be detected and removed by the Antivirus and firewall.	Antivirus software is used for protection against viruses.
6.	Controlled by	Worms can be controlled by remote.	Viruses can't be controlled by remote.
7.	Execution	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.
8.	Comes from	Worms generally comes from the downloaded files or through a network connection.	Viruses generally comes from the shared or downloaded files.
9.	Symptoms	• Hampering computer performance by slowing down it • Automatic opening and running of programs • Sending of emails without your knowledge • Affected the performance of web browser	• Pop-up windows linking to malicious websites • Hampering computer performance by slowing down it • After booting, starting of unknown programs.

		• Error messages concerning to system and operating system	• Passwords get changed without your knowledge
10.	Prevention	• Keep your operating system and system in updated state • Avoid clicking on links from untrusted or unknown websites • Avoid opening emails from unknown sources • Use antivirus software and a firewall	• Installation of Antivirus software • Never open email attachments • Avoid usage of pirated software • Keep your operating system updated • Keep your browser updated as old versions are vulnerable to linking to malicious websites
11.	Types	Internet worms, Instant messaging worms, Email worms, File sharing worms, Internet relay chat (IRC) worms are different types of worms.	Boot sector virus, Direct Action virus, Polymorphic virus, Macro virus, overwrite virus, File Infector virus are different types of viruses
12.	Examples	Examples of worms include Morris worm, storm worm, etc.	Examples of viruses include Creeper, Blaster, Slammer, etc.
13.	Interface	It does not need human action to replicate.	It needs human action to replicate.
14.	Speed	Its spreading speed is faster.	Its spreading speed is slower as compared to worms.

Q-10 What is trojan horse? Also write threats by trojan.

It is a type of malware that typically gets hidden as an attachment in an email or a free to-download file, then transfers onto the user's device.

Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.

THREATS

- They erase, overwrite or corrupt data on a computer.
- They deactivate or interfere with antivirus and firewall programs.
- They allow remote access to your computer (by a remote access Trojan).
- They upload and download files without your knowledge.
- They gather E-Mail addresses and use them for Spam.
- They log keystrokes to steal information such as passwords and credit card numbers.
- They slow down, restart or shutdown the system.
- They reinstall themselves after being disabled.
- They disable the task manager.
- They disable the control panel.

Q-11 What is Backdoor? Also, write the functions.

In cyber security, a backdoor refers to a hidden or undocumented method of bypassing normal authentication or encryption mechanisms in a computer system, software application, or network device.

Backdoors are often created intentionally by developers for legitimate purposes, such as providing access for maintenance or troubleshooting. However, they can also be inserted maliciously by attackers to gain unauthorized access to systems.

Functions:

1) **Remote Control:** Allows remote manipulation of compromised systems. ¬ Persistence: Ensures ongoing access, often evading detection.
2) **Data Exfiltration:** Facilitates the theft of sensitive information.
3) **Espionage/Surveillance:** Used for monitoring, espionage, or reconnaissance.
4) **Software Development:** Legitimately employed for debugging or maintenance.
5) **Unauthorized Access:** Enables attackers to gain entry to systems without standard authentication

Q-12 How to protect from backdoors and trojans?

- **Use Antivirus Software:** Install reputable antivirus and anti-malware software on all your devices and keep it up to date.
- **Keep Software Updated:** Regularly update your operating system, applications, and security software to patch known vulnerabilities.
- **Exercise Caution with Email and Downloads:** Be cautious when opening email attachments or downloading files from the internet, especially if they are from unknown or suspicious sources.
- **Enable Firewall Protection:** Enable the built-in firewall on your operating system or use a third-party firewall to monitor and control incoming and outgoing network traffic.
- **Use Strong Authentication:** Use strong, unique passwords for all your accounts and enable multi-factor authentication whenever possible.
- **Regularly Backup Data:** Regularly backup your important files and data to an external hard drive, cloud storage service, or network-attached storage (NAS) device

Q-12 Write down the examples of backdoor trojans.

- **Netbus:** Netbus was a notorious trojan horse program that gained popularity in the late 1990s. It provided attackers with a backdoor to remotely control infected Windows systems. Attackers could perform various actions, such as viewing the victim's screen, controlling the mouse and keyboard, and transferring files.
- **Sub Seven:** Sub Seven, also known as Sub7, was another trojan horse program widely used in the late 1990s and early 2000s. It provided attackers with a comprehensive set of remote administration tools, including file management, remote shell access, keylogging, and webcam spying.
- **Back Orifice:** Back Orifice was a trojan horse program created by the hacker group Cult of the Dead Cow (cDc) in 1998. It allowed attackers to remotely control Windows systems over a

network. Back Orifice provided features such as file manipulation, registry editing, and remote shell access.

- **Dark Comet:** Dark Comet is a trojan horse program developed by Jean-Pierre Lesueur, also known as Darkcore's. It includes features for remote administration, such as file management, remote shell access, webcam spying, and keylogging. Dark Comet has been used by both cybercriminals and state-sponsored actors for espionage and surveillance purposes.
- **Poison Ivy:** Poison Ivy is a trojan horse program that provides attackers with remote access to infected Windows systems. It includes features such as file transfer, remote shell access, keylogging, and audio/video capture. Poison Ivy has been used in targeted attacks against governments, corporations, and individuals

Q-13 What is stenography AND tools?

Steganography is the technique of hiding data within an ordinary, no secret file or message to avoid detection; the hidden data is then extracted at its destination.

Steganography use can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek word Stefanos, meaning "hidden or covered," and the Greek root graph, meaning "to write.

"Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content. The secret data can be hidden inside almost any other type of digital content.

The content to be concealed through steganography -- called hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed in some method to increase the difficulty of detecting the secret content.

TOOLS

1) **Opens ego:** Opens ego is a free and open-source steganography software that supports various file formats, including images and audio files. It provides features for embedding and extracting hidden data using different steganography techniques.
2) **Steg hide:** Steg hide is another popular steganography tool that allows users to hide data inside image and audio files. It uses strong encryption algorithms to protect the hidden data and provides command-line interface for embedding and extracting hidden information
3) **Outguess:** Outguess is a steganography tool that specializes in hiding data inside image files. It offers high-level security features and supports various image formats, including JPEG, PNG, and BMP. Outguess can be used from the command line or through a graphical user interface.
4) **Quickset:** Quickset is a simple and user-friendly steganography tool that allows users to hide text messages inside image files. It provides a straightforward interface for embedding and extracting hidden data and supports popular image formats like JPEG and BMP.
5) **Steganography Studio**: Steganography Studio is a comprehensive steganography tool that supports embedding and extracting hidden data from various file types, including images, audio files, and documents. It offers advanced features for encrypting hidden data and provides a user-friendly interface for easy operation

Q-14 What is Steganalysis and its tools?

Steganalysis is the technology that tries to defeat steganography by detecting the hidden data and extracting or destroying it. Steganalysis is the procedure of detecting steganography by viewing at variances between bit patterns and unusually high file sizes. It is the art of finding and rendering meaningless covert messages

The main objective of steganalysis is to recognize suspected data streams, determine whether or not they have hidden messages encoded into them, and, if applicable, recover the hidden data

Steganalysis generally begins with several suspect data streams but uncertainty whether any of these include hidden message.

TOOLS

Steg Detect: It can detect the presence of hidden data in images and audio files. It analyses statistical properties and patterns in the carrier data to identify potential steganographic modifications

Gargoyle Investigator Forensic Pro: Gargoyle is a forensic tool that includes steganalysis capabilities for detecting hidden data in various file types, including images, audio files, and documents

Steg Expose: it is a tool that focuses on detecting steganographic content hidden in images. It analyses image files to identify potential modifications introduced by steganography techniques.

Steg Spy: Steg Spy is a steganalysis tool designed to detect hidden data in images and audio files. It employs a combination of statistical analysis, feature extraction, and machine learning techniques to identify patterns associated with steganographic content.

Q-15 What is DOS attack and classification of DOS attack and tools?

Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or Government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services.

Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.

TYPES OF DOS ATTACK

Based on Attack Vector

- **Volumetric Attacks:** These attacks flood the target network or server with a high volume of traffic, overwhelming its bandwidth and infrastructure. Examples include UDP floods, ICMP floods (Ping floods), and SYN floods.
- **Protocol Attacks**: Protocol-based attacks exploit vulnerabilities in network protocols to exhaust server resources or disrupt communication. Examples include SYN floods, DNS amplification attacks, and NTP amplification attacks.
- **Application Layer Attacks:** These attacks target specific applications or services running on the server, such as web servers, by sending malicious requests designed to consume server resources or trigger application errors. Examples include HTTP floods, Slow Loris attacks, and HTTP POST floods

Based on Target

- **Network-Level Attacks:** These attacks target the network infrastructure, such as routers, switches, or firewalls, to disrupt network connectivity or exhaust resources. Examples include ICMP floods and SYN floods
- **Server-Level Attacks:** Server-level attacks target the resources or services running on the server itself, such as web servers, DNS servers, or email servers, to make them unavailable to legitimate users. Examples include HTTP floods and DNS amplification attacks.
- **Application-Level Attacks:** These attacks target specific applications or services hosted on the server, such as web applications or databases, to disrupt their functionality or cause them to crash. Examples include SQL injection attacks and Slow Loris attacks.

Based on Method of Execution

a) Direct Attacks: In direct attacks, the attacker directly sends malicious traffic to the target server or network to disrupt its availability.

b) Distributed Attacks (DDoS): Distributed Denial of Service (DDoS) attacks involve multiple compromised devices, called botnets, coordinating to launch a synchronized attack against the target. This amplifies the attack's impact and makes it more challenging to mitigate.

Protocol Attacks: Protocol-based attacks exploit vulnerabilities in network protocols to disrupt communication or exhaust server resources. Examples include

1) **DNS Amplification Attacks:** Attackers exploit vulnerable DNS servers to amplify and reflect traffic towards the target, consuming its bandwidth.
2) **NTP Amplification Attacks:** Attackers exploit vulnerable Network Time Protocol (NTP) servers to amplify and reflect traffic towards the target, causing network congestion.

Volumetric Attacks: These attacks flood the target with a high volume of traffic, overwhelming its bandwidth and infrastructure. Examples include:

1) **UDP Floods:** Attackers send a large number of User Datagram Protocol (UDP) packets to the target, consuming its network bandwidth.

ICMP Floods (Ping Floods): Attackers send a flood of Internet Control Message Protocol (ICMP) echo request packets (ping requests) to the target, consuming its network resources.

Tools to perform DOS attack

1) **LOIC (Low Orbit Ion Cannon):** LOIC is an open-source network stress testing tool that allows users to launch DoS attacks by sending a large volume of HTTP, UDP, or TCP traffic to a target server. It's relatively easy to use and is popular among less sophisticated attackers.
2) **HOIC (High Orbit Ion Cannon):** HOIC is a more advanced version of LOIC that provides additional features and customization options for launching DoS attacks. It allows users to specify attack parameters and conduct coordinated attacks with other users.
3) **Xerxes:** Xerxes is a powerful DoS tool that enables users to launch HTTP floods against target servers. It allows for simultaneous attacks from multiple sources, making it more effective at overwhelming server resources.
4) **Goldeneye:** Goldeneye is a DoS tool that focuses on launching UDP and TCP flood attacks against target servers. It allows users to specify attack parameters, such as target IP address, port number, and attack duration, to customize the attack. ¬
5) **Hoping:** Hoping is a command-line tool that provides network scanning, packet crafting, and DoS capabilities. It allows users to send custom TCP/IP packets to target hosts, making it useful for conducting SYN floods and other types of DoS attack

Q-16 What is D-DOS attack and tools used for D-DOS attack?

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate traffic from multiple sources.

Unlike a regular DoS attack, which is carried out from a single device or network, a DDoS attack involves coordinated efforts from a large number of compromised devices, called a botnet, distributed across the internet.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

The tools to perform D-DOS attack

XOR DDoS Botnet:

- XOR DDoS is a botnet-based DDoS toolkit that infects vulnerable Linux servers to create a network of compromised devices (bots).
- It uses a command-and-control (C&C) infrastructure to coordinate DDoS attacks and amplify the volume of attack traffic.

Mirai Botnet

- Mirai is a notorious IoT (Internet of Things) botnet that targets vulnerable IoT devices, such as IP cameras, routers, and DVR
- It infects devices using default or weak credentials and leverages them to launch large-scale DDoS attacks, such as DNS amplification attacks and SYN floods.

Q-17 How to protect from DOS/DDOS attacks?

1) **Network Security:** Implement network security measures to filter and block malicious traffic at the network perimeter. This includes deploying firewalls, intrusion prevention systems (IPS), and DoS mitigation appliances to detect and mitigate attack traffic in real-time.
2) **Access Control:** Enforce strict access control policies to prevent unauthorized access to network resources and services. Implement strong authentication mechanisms, such as multi-factor authentication (MFA) and access control lists (ACLs), to limit access to sensitive systems and data.
3) **Traffic Monitoring:** Continuously monitor network traffic for signs of abnormal activity, such as a sudden increase in traffic volume or a high number of connection attempts from multiple sources. Network monitoring tools and security information and event management (SIEM) systems can help detect and alert to potential DoS/DDoS attacks.
4) **Anomaly Detection:** Deploy anomaly detection systems to identify patterns of behaviour indicative of DoS/DDoS attacks. Anomaly detection algorithms can analyse network traffic and system logs to detect deviations from normal activity and trigger alerts for further investigation
5) **Rate Limiting:** Implement rate limiting measures to control the rate of incoming requests or connections to servers or network devices. Rate limiting can help mitigate the impact of DoS/DDoS attacks by limiting the amount of traffic that can reach the target, preventing resource exhaustion.
6) **Scalable Infrastructure:** Design network infrastructure and services to be scalable and resilient to withstand sudden spikes in traffic. Distributing network resources across multiple servers, data centres, or cloud providers can help distribute the load and minimize the impact of DoS/DDoS attacks.

Q-18 What do you mean by attacking on wireless networks?

Wireless network attacks are deliberate and malicious actions aimed at exploiting vulnerabilities in wireless communication systems to gain unauthorized access, intercept sensitive data, disrupt network operations, or compromise the security of devices and users connected to the network.

These attacks target weaknesses in the protocols, configurations, or encryption mechanisms of wireless networks, taking advantage of their inherent nature of broadcasting signals over the airwaves.

Tools used for attacking on wireless networks

Air crack-ng

- Air crack-ng is a suite of wireless network security tools that includes packet sniffing, password cracking, and packet injection capabilities.

- It can be used to perform tasks such as capturing packets, generating traffic, and cracking WEP and WPA/WPA2 encryption keys.\

Wireshark

- Wireshark is a popular network protocol analyser that allows users to capture and interactively browse the traffic running on a network. It can be used to analyse wireless network packets, detect vulnerabilities, and identify suspicious activity.

Kismet

- Kismet is a wireless network detector, sniffer, and intrusion detection system that supports various wireless network interfaces. It can detect hidden wireless networks, capture packets, and identify unauthorized access points or clients.

Q-19 Explain theft of Internet Hours and Wi-Fi-based Frauds and Misuses.

Unauthorized Access

- Attackers may gain unauthorized access to WIFI networks by exploiting weak or default passwords, bypassing authentication mechanisms, or using brute-force attacks.

Stolen Credentials:

- Attackers may obtain or steal legitimate credentials, such as usernames and passwords, to access Wi-Fi networks or internet services. Stolen credentials can be used to gain unauthorized access to Wi-Fi networks, bypassing security controls, and enabling attackers to conduct fraudulent activities or perform malicious actions.

Piggybacking

- Piggybacking involves unauthorized users exploiting open or unsecured Wi-Fi networks to access the internet without permission from the network owner

Wi-Fi Phishing

- Wi-Fi phishing attacks involve creating fake Wi-Fi networks with legitimate-sounding names or enticing SSIDs to deceive users into connecting to them. Once connected, attackers can intercept and monitor network traffic, capture sensitive information, or deploy malware to compromise connected devices

DNS Hijacking

- Attackers may compromise Wi-Fi routers or access points to perform DNS hijacking attacks, redirecting users to malicious websites or phishing pages' hijacking can be used to intercept login credentials, steal personal information, or distribute malware to unsuspecting users

Q-20 How to secure wireless network and tools we can use to secure?

Change Default Settings

- Change default usernames, passwords, and SSIDs (network names) of wireless routers and access points to strong and unique values.
- Disable remote administration and unnecessary services to reduce the attack surface.
- Use Strong Encryption: Enable Wi-Fi Protected Access (WPA3) or WPA2 encryption with a strong passphrase (at least 12 characters long) to protect wireless communications.
- Avoid using outdated and insecure encryption protocols like WEP (Wired Equivalent Privacy). Implement Secure Authentication: Use WPA2-Enterprise or WPA3-Enterprise with 802.1X authentication for enterprise-grade security.
- Deploy a RADIUS server for centralized authentication and certificate-based authentication for added security.

Enable Network Segmentation

- Segment the wireless network into separate VLANs (Virtual Local Area Networks) to isolate different types of devices and restrict access to sensitive resources.
- Implement firewall rules and access control lists (ACLs) to control traffic flow between VLANs and enforce security policies.

Update Firmware Regularly

- Keep wireless routers, access points, and other network devices up to date by applying firmware updates and security patches released by manufacturers. Regularly check for firmware updates and apply them promptly to address known vulnerabilities and security issues

Enable Network Monitoring

- Use network monitoring tools like Wireshark, tcpdump, or PRTG Network Monitor to monitor wireless network traffic and detect anomalies or suspicious activities.
- Monitor for rogue access points, unauthorized devices, and unusual traffic patterns that may indicate security threats.

Deploy Intrusion Detection/Prevention Systems (IDS/IPS)

- Deploy IDS/IPS solutions capable of detecting and preventing unauthorized access attempts, intrusion attempts, and malicious activities on the wireless network.
- Configure IDS/IPS rules to alert or block suspicious traffic, such as DE authentication attacks, rogue access points, or DNS spoofing attempts.

Use Wireless Intrusion Prevention Systems (WIPS)

- Deploy WIPS solutions to detect and prevent wireless network attacks, such as rogue access points, de-authentication attacks, and Wi-Fi jamming.

- WIPS solutions provide real-time monitoring and mitigation of wireless threats to ensure the security and integrity of the wireless network.

Educate Users

- Educate users about wireless network security best practices, such as avoiding public Wi-Fi hotspots for sensitive transactions, using VPNs for secure communications, and being cautious of phishing attacks.
- Train users on how to identify and report suspicious activities or security incidents related to the wireless network.

Q-21 Write down the tools to protect wireless network firewalls:

Firewalls are essential security devices that control and monitor incoming and outgoing network traffic based on predetermined security rules.

They can be deployed as hardware appliances, software solutions, or integrated into wireless routers to filter and block unauthorized access attempts and malicious traffic.

Intrusion Detection Systems (IDS)

- IDS solutions monitor network traffic for suspicious activity, anomalies, and known attack patterns.
- They detect and alert administrators about potential security breaches, unauthorized access attempts, and malicious activities occurring on the wireless network.

Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS):

- WIDS/WIPS solutions are specifically designed to monitor and protect wireless networks from security threats and vulnerabilities.
- They detect and prevent unauthorized access points, rogue devices, authentication attacks, and other wireless-specific threats.

Encryption Tools

- Encryption tools, such as VPN (Virtual Private Network) software and encryption protocols like WPA3, protect wireless communications by encrypting data in transit.
- VPNs create secure tunnels between devices and network resources, preventing eavesdropping, interception, and tampering of transmitted data.

Q-22. What is SQL injection?

A SQL injection (SQLi) attack is a type of cybersecurity attack that targets the underlying database of a web application.

It occurs when an attacker is able to manipulate the SQL query sent to the database through a vulnerable web application.

This manipulation can lead to unauthorized access, data leakage, data corruption, and other serious security issues. Here is a more detailed explanation of how SQL injection attacks work:

Identifying a Vulnerable Web Application

The attacker identifies a web application that is vulnerable to SQL injection. This vulnerability typically arises from improper input validation or insufficiently sanitized user inputs.

Crafting a Malicious SQL Query: The attacker crafts a malicious SQL query that exploits the vulnerability in the web application. This query is designed to manipulate the database in a way that benefits the attacker.

Injecting the Malicious SQL Query: The attacker injects the malicious SQL query into a vulnerable input field in the web application. Common entry points for SQL injection include login forms, search fields, and other input fields that interact with the database.

Executing the Attack: When the vulnerable web application processes the user input containing the malicious SQL query, the query is executed against the database. If successful, the attacker can gain unauthorized access to the database or manipulate its contents.

Types of SQL Injection Attacks:

Classic SQL Injection: Involves injecting malicious SQL code into a vulnerable input field. ¬Blind SQL Injection: Exploits a vulnerability where the application does not respond differently based on the result of the injected query, requiring the attacker to infer information through timing or error-based techniques.

Second-Order SQL Injection: Involves injecting malicious SQL code that does not execute immediately but is stored in the database for future execution

Consequences of SQL Injection Attacks

- **Data leakage:** Attackers can access sensitive information stored in the database, such as usernames, passwords, and personal information.
- **Data manipulation:** Attackers can modify or delete data in the database, leading to data corruption or loss.
- **Unauthorized access:** Attackers can gain unauthorized access to the web application or the underlying database server.
- **Application compromise:** SQL injection can be used to compromise the entire web application, leading to further security issues.

Q-21. What is buffer overflow?

A buffer overflow is a type of software vulnerability that occurs when a program writes more data to a buffer (a fixed-size block of memory) than it was intended to hold. This can happen when input data is not properly validated or sanitized, allowing an attacker to send data that exceeds the buffer's capacity.

Here's how a buffer overflow typically occurs

- **Buffer Allocation:** When a program is executed, it allocates memory for variables, including buffers, to store data.
- **Input Data:** The program receives input data, which is stored in a buffer. If the input data is larger than the buffer size, it can overflow into adjacent memory locations.
- **Memory Corruption:** When the buffer overflows, it can overwrite other data in memory, such as variables, function pointers, or return addresses. This can lead to the corruption of the program's state.
- **Exploitation:** An attacker can exploit a buffer overflow vulnerability to execute arbitrary code or inject malicious payloads into the program's memory. By overwriting function pointers or return addresses, the attacker can redirect the program's execution flow to malicious code that the attacker controls.
- **Consequences:** Buffer overflow vulnerabilities can be exploited to gain unauthorized access to a system, execute arbitrary code, or crash the program. They are often used as a means to inject and execute malicious code, making them a serious security risk.

Q-22 What is Identity theft?

Identity theft is a type of crime in which an attacker steals someone's personal information, such as their name, Social Security number, credit card number, or other sensitive information, with the intent to commit fraud or other crimes.

Identity theft can occur through various means, including phishing scams, data breaches, malware attacks, and physical theft of documents containing personal information. Once an attacker has stolen someone's identity, they can use it to commit a wide range of fraudulent activities, often without the victim's knowledge.

To protect against identity theft, individuals should take steps to safeguard their personal information, such as using strong, unique passwords for online accounts, being cautious of phishing attempts, monitoring financial statements for unauthorized activity, and using identity theft protection services if available. Additionally, organizations should implement strong security measures to protect customer data and comply with relevant data protection regulations.