1. Briefly explain the basic stages of an attack used by an attacker to compromise a network.

The stages of a network attack are typically systematic, allowing attackers to gather information, infiltrate the network, and maintain control. These stages include:

Initial uncovering (Reconnaissance): The attacker gathers as much information as possible about the target using legitimate methods such as searching for the target's details on Google, social media, or news articles. They try to discover network-related information such as IP addresses or domain names.

Network probe: At this stage, the attacker uses tools like ping sweeps or port scanning to identify which systems and services are active. While still legal at this point, they are getting closer to identifying weaknesses in the network.

Crossing the line (Exploiting vulnerabilities): Here, the attacker uses specific system vulnerabilities, like weak passwords or programming flaws, to gain access to the network. Once inside, they often escalate their privileges to gain administrative access.

Capturing the network: The attacker installs backdoor programs or replaces system files with Trojan versions to ensure continuous access. They can use the compromised system to attack deeper parts of the network.

Grab the data: After compromising the network, the attacker can steal data, manipulate processes, or deface websites. Sensitive data like customer information or financial records are common targets.

Covering attacks: Finally, the attacker removes evidence of the breach, such as deleting log files or using tools to hide their activities, to avoid detection and prolong their unauthorized access.

Example: An attacker might begin by researching a company's publicly available information, probe its network for open ports, exploit a vulnerability in outdated software, gain access to sensitive data, and then delete logs to cover their tracks.

2. What are Proxy servers and Anonymizers? List the purposes of a Proxy server.

Proxy Server:

A proxy server is an intermediary that sits between the user's device and the internet. It processes requests from users and forwards them to the destination server, allowing users to access online resources while masking their identity.

Anonymizer:

An anonymizer hides a user's identity while they browse the web. It acts like a proxy but is focused on making the user's activity completely untraceable by hiding the source IP address.

Purposes of a Proxy Server:

Hide the user's IP address: Protects the user's identity by masking the original IP.
Cache frequently accessed resources: Saves web pages for faster access in the future.
Filter unwanted content: Can block certain websites or filter out harmful content like ads or malware.
Act as an IP multiplexer: Allows multiple devices to connect to the internet using a single IP address.
Log and monitor traffic: Can record and analyze user activity for security or compliance purposes.
Example: In a school setting, a proxy server can be used to prevent students from accessing inappropriate websites and to speed up access to commonly used educational resources.

3. What is Phishing? Explain the working of Phishing.

Phishing is a cyberattack where attackers send fraudulent messages, often via email, pretending to be from a legitimate organization, with the intent of stealing sensitive information such as usernames, passwords, or credit card details.

Steps in Phishing:
Planning: The attacker identifies their target and collects email addresses, often through mass mailing lists.
Setup: The attacker creates a fake but convincing webpage or email that mimics a legitimate one.
Attack: Phishing emails are sent to the target, containing malicious links that direct the victim to a fake website or prompt them to provide sensitive data.
Collection: When the victim enters their information, it is captured by the attacker.
Identity theft and fraud: The attacker uses the stolen information to commit fraud, such as making unauthorized transactions or stealing the victim's identity.
Example: A victim receives an email from a source pretending to be their bank, asking them to verify their account information by clicking on a link. The link leads to a fake bank website, and when the victim enters their login details, the attacker captures them.

4. Explain online and offline password cracking.

Password cracking is the process of recovering or guessing a password to gain unauthorized access to a system.

Online Password Cracking:
This method involves attacking a live system by repeatedly trying different passwords, often using automated scripts or tools. The attacker interacts directly with the target system during the attack.

Example: An attacker tries to guess a user's email password by entering common passwords like "password123" or "admin" directly into the login page, hoping one of them will work.

Offline Password Cracking:
Offline cracking involves the attacker obtaining a copy of the password hash or encrypted password from the system and then working on cracking it locally without needing to interact with the target system. This typically happens after a system breach, where the attacker has stolen a password file or database.

Example: A hacker steals a database containing encrypted passwords from a company's server. They then try to crack the encryption on their own machine, without interacting with the company's system.

5. Explain any two password cracking tools.
John the Ripper:
John the Ripper is a popular password-cracking tool that uses a variety of attack methods to guess passwords, such as dictionary attacks (trying common words) and brute force attacks (trying every possible combination). It is often used by system administrators to test the strength of passwords.

Example: A system administrator uses John the Ripper to check if any employees are using weak passwords like “password123” by running the tool against the company’s password hashes.

Cain and Abel:
Cain and Abel is a password recovery tool for Microsoft systems. It allows for password cracking using techniques like dictionary attacks, brute-force attacks, and cryptanalysis. It also can intercept network traffic to capture passwords.

Example: An IT specialist uses Cain and Abel to recover the administrator password for a system after an employee forgot it, instead of resetting the password.

6. List any five general guidelines applicable to the password policies, which can be implemented organization-wide.
Passwords should be at least eight characters long:
This helps ensure that the password is not too short to be easily guessed by an attacker.

Passwords should be unique for each account:
Users should not reuse the same password across multiple accounts to minimize the risk if one account is compromised.

Avoid using common words or personal information:
Passwords should not include easy-to-guess words like "password" or information like the user’s name or birthday.

Change passwords regularly:

Regularly changing passwords (e.g., every 30 to 45 days) reduces the window of time an attacker has to use a compromised password.

Lock accounts after several failed login attempts:
Implementing a lockout policy after a set number of incorrect attempts (e.g., five tries) helps prevent brute-force attacks.

Example: A company sets up a password policy requiring employees to use complex passwords of at least eight characters, which are changed every 45 days. If an employee enters the wrong password five times, their account is temporarily locked.

7. What is a keylogger? Explain the two types of keyloggers with examples.
A keylogger is a type of spyware that records every keystroke a user makes on their keyboard, usually without the user knowing, with the intent to capture sensitive information like passwords or credit card numbers.

Software Keyloggers:
These are programs installed on the computer that run in the background and log all keystrokes. They are often delivered through Trojans or viruses.

Example: A hacker sends a victim an email with an attachment that contains a software keylogger. When the victim opens the attachment, the keylogger is installed, and it records everything the victim types, including their bank login details.

Hardware Keyloggers:
These are physical devices connected between the keyboard and the computer that capture keystrokes. They require physical access to the computer to install.

Example: An attacker sneaks into an office and installs a tiny hardware keylogger between the keyboard and the computer. The keylogger records all keystrokes and stores them on the device, which the attacker can later retrieve.

8. What is a malware? Give the classification of malware.
Malware is malicious software designed to damage, disrupt, or gain unauthorized access to a system.

Classification of Malware:
Viruses:
Programs that attach themselves to legitimate software or files and replicate when the infected file is shared. Viruses can corrupt files or cause other damage.

Worms:

Self-replicating malware that spreads across networks without needing to attach to files. Worms often cause network congestion and system slowdowns.

Trojans:
Programs that appear harmless but contain malicious code. Trojans typically open backdoors for attackers to gain access to the system.

Spyware:
Software that collects information about a user's activities without their knowledge, often used to track browsing habits or steal personal information.

Ransomware:
Malware that locks a user's files or system, demanding payment to restore access.

Example: A user downloads what appears to be a free game, but it is actually a Trojan. Once installed, the Trojan allows an attacker to gain remote access to the user's system and steal personal data.

9. What is spyware? Explain the features of 007 Spy and Spector Pro spyware.

Spyware is a type of malware that is installed on a computer without the user's knowledge. Its primary function is to monitor and collect information about the user's activities, such as browsing habits, keystrokes, and sensitive data like passwords and credit card numbers. Spyware operates secretly in the background, often slowing down the system and compromising privacy.

007 Spy Features:

007 Spy is a popular spyware tool that monitors user activities like visited websites, applications used, and keystrokes entered.
It can also take screenshots at regular intervals to visually capture what is happening on the screen.
It operates invisibly, so the user remains unaware of its presence.
Spector Pro Features:

Spector Pro is another advanced spyware tool that logs every activity on a user's computer, including emails sent, chats, keystrokes, and website visits.
It provides detailed reports and can also capture screenshots of the user's activities.
Spector Pro is often used by employers to monitor employees or parents to keep track of their children's online behavior.
Example: A company installs Spector Pro on its employees' computers to monitor their internet usage, ensuring that work-related activities are prioritized over personal browsing.

10. Explain the differences between computer viruses and worms.

Computer Virus:
A virus is a type of malware that attaches itself to legitimate software or files. It requires user interaction (like opening a file or running a program) to replicate and spread. Once activated, it can corrupt, delete, or modify files.

Example: A user downloads an infected file from the internet and opens it. The virus within the file activates, spreading to other files on the user's computer.
Computer Worm:
A worm is a self-replicating malware that doesn't need user interaction to spread. It exploits vulnerabilities in network systems to propagate across computers automatically. Worms often consume bandwidth and system resources, leading to network congestion.

Example: A worm spreads through a company's network by exploiting a vulnerability in an outdated operating system. As it replicates itself across the network, it slows down all connected systems.
Key Differences:

Propagation Method: Viruses need user interaction to spread, while worms spread automatically.
Effects: Viruses typically modify or delete files, while worms mainly spread across networks and consume resources.
Target: Viruses often target files and programs, while worms exploit network vulnerabilities.

11. Write a note on the following types of viruses: Boot Sector viruses, Program viruses, Stealth viruses, and Polymorphic viruses.
Boot Sector Viruses:
These viruses infect the boot sector of storage devices, such as hard drives and USB sticks. The boot sector contains the information necessary to start the computer, so a boot sector virus can prevent the system from booting properly or cause it to crash.

Example: An infected USB stick is inserted into a computer. The boot sector virus transfers itself to the computer's hard drive, causing the system to fail during startup.

Program Viruses:
These viruses infect executable files (e.g., .exe, .com) and activate when the infected program is run. Once active, they replicate by infecting other program files on the system.

Example: A user installs a program downloaded from an untrusted website. The program virus infects other applications on the computer, corrupting them.

Stealth Viruses:
These viruses are designed to evade detection by hiding their presence. They can alter their own file size or modify system functions to avoid being detected by antivirus software.

Example: A stealth virus infects a system but avoids detection by antivirus programs by constantly changing its file attributes.

Polymorphic Viruses:
These viruses modify their code slightly every time they replicate, making it difficult for traditional antivirus programs to detect them. They change their virus signature with each infection.

Example: A polymorphic virus spreads through email attachments. Each time it infects a new system, it slightly alters its code to avoid detection by antivirus software.

12. What is a Trojan Horse? Give any six examples of threats posed by Trojans.
A Trojan Horse is a type of malware that appears to be a legitimate or harmless program but contains malicious code. Trojans do not replicate themselves like viruses or worms but can cause significant damage by creating backdoors or allowing unauthorized access to the system.

Examples of threats posed by Trojans:
Erasing or corrupting data: A Trojan can delete or alter important files, leading to data loss or corruption.
Spreading other malware: Some Trojans serve as "droppers" that install additional malware, such as viruses or ransomware.
Disabling security software: Trojans can deactivate antivirus programs or firewalls, leaving the system vulnerable to further attacks.
Granting remote access: Remote access Trojans (RATs) allow attackers to control the infected computer from a distance, enabling them to perform malicious activities.
Stealing personal information: Trojans can be programmed to log keystrokes, capturing sensitive information like passwords and credit card details.
Launching DDoS attacks: Some Trojans turn infected computers into "zombies" that participate in Distributed Denial of Service (DDoS) attacks.
Example: A user downloads what appears to be a free game, but it is actually a Trojan. Once installed, the Trojan opens a backdoor, allowing the attacker to steal the user’s personal data.

13. What does a Backdoor do? Explain any one well-known backdoor Trojan. How to protect from Backdoors?
A backdoor is a method that bypasses normal authentication mechanisms to gain unauthorized access to a computer system. Backdoors are often created by Trojans, allowing attackers to control the system remotely without the user's knowledge.

Example of a Backdoor Trojan: Back Orifice is a well-known backdoor Trojan that allows attackers to remotely control a Windows system. Once installed, it enables the attacker to manipulate files, execute commands, and control the system without the user's consent.

Protection from Backdoors:

Install antivirus and anti-malware software: Keep security software updated to detect and remove backdoors.
Avoid downloading untrusted software: Only download programs from reputable sources to avoid installing Trojans.
Regularly update the operating system and applications: This ensures that known vulnerabilities are patched, preventing exploitation by backdoors.
Use firewalls: Firewalls can block unauthorized access to the system, preventing backdoors from communicating with external servers.
Example: A user unknowingly installs a backdoor Trojan while downloading a free movie player. The attacker uses the backdoor to access the user's files and steal sensitive data.

14. Write a brief note on steganography.

Steganography is the practice of hiding messages or information within other non-secret text or data in such a way that only the intended recipient knows of the hidden content. Unlike cryptography, where the content of the message is hidden but the existence of the message is known, steganography conceals the very existence of the message.

Key Concept:
In digital steganography, a common technique is to hide information in digital files such as images, audio, or video files. The hidden information is typically embedded within the least significant bits (LSB) of the file, which do not visibly alter the file's appearance or quality.

Example:
A digital image can have secret information embedded in the least significant bits of its pixel values. The change is so subtle that it doesn't noticeably affect the image's appearance, but someone who knows how to extract the information can retrieve the hidden message.

Use Case:
Steganography is often used to embed watermarks in images or videos to detect illegal copying or distribution. It's also employed by cybercriminals to hide malicious code within seemingly harmless files.

Example:
A company embeds a digital watermark within its product images using steganography. If someone attempts to steal or copy the image, the watermark can be extracted to prove ownership.

15. What is a DoS attack? What can it do? Discuss the classification of DoS attacks.

A Denial of Service (DoS) attack is a cyberattack where an attacker floods a network or system with excessive traffic or data requests, overwhelming its resources and preventing legitimate users from accessing services.

What Can a DoS Attack Do?

Flood a network with traffic: Attackers send massive amounts of data or requests, which consumes all available bandwidth, leaving no room for legitimate traffic.
Disrupt connections between systems: By overwhelming the target system with requests, attackers can disrupt the connection between the target and legitimate users.
Prevent access to services: Users attempting to access a website or service may find it inaccessible due to the system being overloaded by the attack.
Classification of DoS Attacks:

Volume-based Attacks:
These attacks involve overwhelming the network's bandwidth by sending massive amounts of data to the target. Example: UDP flood, ICMP flood (Ping of Death).

Protocol Attacks:
These attacks target weaknesses in network protocols, overloading the system's processing capabilities. Example: SYN flood, which exploits the TCP handshake process.

Application Layer Attacks:
These attacks target specific applications by sending resource-intensive requests to slow down or crash the service. Example: HTTP flood, where attackers make multiple HTTP requests to exhaust server resources.

Example:
An online retailer's website is hit by a DoS attack during a major sale event. The website becomes inaccessible to customers because the server is overwhelmed with fake traffic from the attacker.

16. What is SQL injection? Discuss the steps for SQL Injection attack.
SQL Injection (SQLi) is a type of cyberattack that exploits vulnerabilities in an application's software, allowing attackers to inject malicious SQL code into a database query. This can lead to unauthorized access, data theft, or even deletion of the entire database.

Steps for an SQL Injection Attack:
Identify vulnerable input fields:
The attacker looks for forms on websites (e.g., login pages, search bars) that accept user input but do not properly sanitize the input. They test for vulnerabilities by entering special characters like a single quote (') to check if the system returns an SQL error.

Inject SQL code:
Once the attacker finds a vulnerable input field, they inject SQL code into the field. For example, entering '; DROP TABLE users; -- into a login form could delete the entire users' table from the database if not properly protected.

Execute malicious SQL statements:

The SQL code submitted by the attacker is executed by the database, allowing the attacker to retrieve sensitive information (such as usernames and passwords) or modify the database.

Gain access or modify data:
Attackers can steal information, alter records, or even gain full administrative control of the database by exploiting SQL vulnerabilities.

Example:
An attacker enters ' OR '1'='1 into a login form. The SQL query becomes:
SELECT * FROM users WHERE username = '' OR '1'='1' AND password = ''
This query always returns true, allowing the attacker to bypass authentication and log in without a valid username and password.

17. Discuss the steps that can prevent SQL Injection attack.
Preventing SQL injection attacks involves securing the application and database by validating and sanitizing user inputs.

Input Validation:
Always validate user inputs to ensure they meet expected formats (e.g., only numbers for numeric fields). This helps prevent malicious SQL code from being injected into the query.

Use Prepared Statements (Parameterized Queries):
Rather than directly embedding user inputs in SQL queries, use prepared statements that treat inputs as data rather than part of the SQL code. This prevents the injection of malicious SQL.

Example:
Instead of:
SELECT * FROM users WHERE username = '$username'
Use:
SELECT * FROM users WHERE username = ? (and bind the parameter).

Escape Special Characters:
Sanitize inputs by escaping or removing special characters like single quotes (') that could be used in SQL injection attacks. This prevents attackers from injecting code.

Limit Database Privileges:
Limit the permissions of the database user account. For example, if the application only needs to read data, ensure the account doesn't have write or delete permissions. This limits the damage an attacker can do if an SQL injection occurs.

Use Stored Procedures:
Stored procedures encapsulate SQL code and prevent direct interaction with user inputs. However, they must also be properly parameterized to prevent injection.

Example:
A website developer implements prepared statements in the login form, ensuring that any user input is treated as data and cannot be executed as part of the SQL query, preventing an SQL injection attack.