1. Virus

- A virus is a malicious program that attaches itself to a clean file or program.
- It spreads from one computer to another when the infected file is executed.
- Viruses can corrupt files, delete data, or slow down system performance.
- They spread through USB drives, email attachments, and infected software.
- Antivirus software helps detect, quarantine, and remove viruses.

---

2. Worm

- A worm is a self-replicating malware that spreads without human action.
- It uses networks and internet connections to spread to other systems.
- Worms consume system resources and slow down networks.
- Some worms also install backdoors for hackers to access systems.
- Firewalls and network monitoring tools help prevent worm attacks.

---

3. Trojan

- A Trojan is a malicious program disguised as a useful or legitimate software.
- It tricks users into installing it and then secretly performs harmful actions.
- Unlike viruses and worms, Trojans do not replicate themselves.
- Trojans can steal passwords, monitor keystrokes, or control devices remotely.
- They usually spread through fake downloads or email attachments.

---

4. Rootkit

- A rootkit is a stealthy malware that hides itself and other malicious programs.
- It gives attackers unauthorized administrator-level access to a computer.
- Rootkits are difficult to detect because they hide deep in the operating system.
- They are used to steal data or control systems without being noticed.
- Special rootkit scanners are used to remove them.

---

5. Spyware

• Spyware is software that secretly monitors user activities without permission.
• It collects sensitive data like passwords, browsing history, and personal info.
• Spyware often slows down system performance and internet speed.
• It usually comes bundled with free software or fake downloads.
• Anti-spyware tools help detect and remove spyware.

---

6. Ransomware

• Ransomware is malware that locks or encrypts user files.
• It demands payment (ransom) to unlock access to data.
• It usually spreads through phishing emails and infected websites.
• Ransomware attacks can cause huge financial losses.
• The best protection is backup data and strong security awareness.

---

7. Adware

• Adware is software that displays unwanted advertisements on a device.
• It tracks user activity to show targeted ads.
• While not always harmful, it can invade privacy and slow systems.
• Adware enters systems through free software or browser extensions.
• It can be removed using adware cleaners and safe browsing habits.

---

8. Crimeware

• Crimeware is malware designed specifically for online criminal activities.
• It steals financial information like bank passwords and credit card details.
• Cybercriminals use it for fraud, identity theft, and scams.
• It spreads through phishing sites and fake online banking pages.
• Encryption and secure logins help protect against crimeware.

---

9. Flaws

• Flaws are weaknesses or mistakes in software design or system setup.
• They create security gaps that hackers can exploit.
• Flaws can lead to unauthorized access or data leakage.
• They are often found during security audits or testing.
• Regular updates and patches fix system flaws.

---

10. Bugs

• Bugs are errors or defects in a software program's code.
• They cause software to behave unexpectedly or crash.
• Some bugs can create security vulnerabilities.
• Attackers may exploit bugs to perform cyberattacks.
• Debugging and software testing help remove bugs.

---

11. Social Engineering

• Social engineering is a trick used by attackers to fool people into revealing confidential information.
• It uses psychological manipulation instead of technical hacking.
• Common examples include fake calls, fake messages, and impersonation.
• It targets human weakness rather than computer systems.
• Security awareness training helps prevent social engineering.

---

12. DoS Attack (Denial of Service)

• A DoS attack attempts to overload a system or network with too much traffic.
• It makes a website or server unavailable to real users.
• Attackers flood the system using a single computer or source.
• It causes service disruption and financial loss.
• Firewalls and traffic filters help reduce DoS attacks.

---

13. DDoS Attack (Distributed Denial of Service)

- A DDoS attack is a large-scale DoS attack using multiple computers or bots.
- Attackers use a botnet (hijacked computers) to send massive fake traffic.
- The target server crashes due to heavy load.
- DDoS attacks are difficult to stop because they come from many sources.
- Strong network protection and traffic analysis tools are used for defense.

---

14. Man-in-the-Middle (MITM) Attack

- In a MITM attack, a hacker secretly intercepts communication between two users.
- The attacker can read, modify, or steal sensitive information.
- It often occurs on unsecured Wi-Fi networks.
- Online banking and login sessions are common targets.
- Using HTTPS websites and VPNs helps prevent MITM attacks.

---

15. Phishing Attack

- Phishing is a cyberattack that tricks people into sharing personal information.
- Attackers send fake emails or messages pretending to be trusted sources.
- They steal passwords, bank details, or credit card numbers.
- Phishing links often lead to fake websites.
- Awareness and email verification help avoid phishing.

---

16. Email Spoofing

- Email spoofing is sending emails with a fake sender address.
- It makes the email look like it's from a trusted person or company.
- It is used in phishing and scam attacks.
- Victims are tricked into clicking links or sharing data.
- Email security filters help detect spoofing.

---

17. IP Spoofing

- IP spoofing uses a fake IP address to hide the attacker’s identity.
- The attacker pretends to be a trusted device on the network.
- It is used in network attacks like DoS and MITM.
- It helps bypass security filters and firewalls.
- Packet filtering helps prevent IP spoofing.

---

18. Login Spoofing

- Login spoofing uses a fake login screen to steal usernames and passwords.
- The fake screen looks like a real website or app login.
- When users enter credentials, they go to the attacker.
- It is common in banking or email scams.
- Always check URLs and use multi-factor authentication to avoid it.

---

19. Salami Attack

- A salami attack steals very small amounts of money or data over time.
- Each theft is too tiny to be noticed individually.
- Attackers usually target banks or financial systems.
- Small amounts add up to a big loss over time.
- Regular audits help detect salami attacks.

---

20. Email Bomb

- An email bomb overloads someone's inbox by sending thousands of emails.
- It slows down or crashes the email system.
- It is used for harassment or DoS attacks via email.
- It wastes storage and bandwidth.
- Email filters and blocking tools help prevent it.

---

21. Password Sniffing

- Password sniffing captures passwords during transmission over networks.
- Attackers use sniffing tools to monitor network traffic.
- It works mostly on unsecured or public Wi-Fi networks.
- Login credentials and personal data can be stolen.
- Encryption and HTTPS prevent password sniffing.

---

22. Buffer Overflow Attack

- A buffer overflow happens when extra data is written beyond the memory limit of a buffer.
- Attackers use this to crash programs or run malicious code.
- It occurs due to poor programming and lack of input validation.
- Hackers exploit this to take control of systems.
- Secure coding and memory checks prevent this attack.

---

23. Integer Overflow Attack

- Integer overflow happens when a number value exceeds its storage limit.
- It causes incorrect data processing in programs.
- Attackers use it to change program behavior or bypass security.
- It can lead to crashes or unexpected results.
- Proper input validation helps prevent this attack.

---

24. Zero Day Attack

- A zero-day attack uses a software weakness that is unknown to the developer.
- There is no security patch available at the time of attack.
- Cybercriminals exploit this vulnerability immediately.
- It is one of the most dangerous types of attacks.
- Regular software updates and threat monitoring help reduce risk.

---

25. Internal Theft

• Internal theft is done by employees or trusted insiders.
• It involves stealing company data or resources.
• Employees misuse access privileges to harm the company.
• It may result in data leaks or system sabotage.
• Monitoring and access controls help prevent insider threats.

---

26. Session Hijacking

• Session hijacking takes over a user's active session.
• Attackers steal session IDs to access accounts without passwords.
• Web sessions like banking and emails are common targets.
• It is done using network sniffer tools.
• HTTPS and secure cookies help prevent it.

---

27. Web Jacking

• Web jacking means taking control of a website illegally.
• Attackers redirect users to fake or harmful websites.
• It is used to steal data or spread malware.
• Attackers usually hack website login panels.
• Strong admin security prevents web jacking.

---

28. SQL Injection

• SQL Injection is a web attack that targets databases.
• Attackers insert malicious SQL commands into input fields.
• It allows them to view, modify, or delete database records.
• It is caused by bad input validation in web forms.
• Prepared statements and input filters prevent SQL Injection.

---

29. Cross-Site Scripting (XSS)

• XSS is a web attack where attackers inject malicious scripts into websites.
• The script runs in the victim's browser without their knowledge.
• It can steal cookies, session data, or user information.
• Comment boxes and search bars are common targets.
• Input filtering and output encoding prevent XSS.

---

30. Cross-Site Request Forgery (CSRF)

• CSRF tricks users into performing actions they didn't intend.
• Attackers send malicious links to make users unknowingly submit requests.
• It works when a user is already logged into a website.
• It can transfer money or change passwords secretly.
• Security tokens help prevent CSRF attacks.

---

31. Brute Force Attack

• A brute force attack tries many password combinations to guess the correct one.
• It is a trial-and-error method of breaking logins.
• Simple passwords are easily cracked using this method.
• Attackers use automated tools for fast guessing.
• Strong passwords and account lockout policies prevent it.

---

32. Rainbow Attack

• A rainbow attack uses pre-computed hash tables called rainbow tables.
• Hackers use it to crack hashed passwords quickly.
• It is faster than brute force attacks.
• Weak hashing algorithms are easily broken.
• Using salted hashing prevents rainbow attacks.

---

33. ARP Spoofing

- ARP spoofing sends fake ARP messages to a local network.
- It links the attacker's MAC address with the victim's IP address.
- This allows the attacker to intercept data.
- It enables MITM attacks on local networks.
- Static ARP entries help reduce ARP spoofing.

---

34. DNS Spoofing

- DNS spoofing gives users a fake website instead of the real one.
- Attackers change DNS records to redirect traffic.
- It is used to steal personal and banking data.
- Users think they are on a safe website but are not.
- Using DNS security extensions prevents this attack.

---

35. Wi-Fi Eavesdropping

- Wi-Fi eavesdropping listens to unprotected Wi-Fi communications.
- Attackers capture data like passwords and messages.
- It often happens in public Wi-Fi networks.
- It is done using packet sniffer tools.
- Using VPN and secure Wi-Fi, protects from eavesdropping.