1. Security: Security refers to the measures taken to protect against threats to an entity or system. This can include physical, digital, and organizational measures.
2. Cyber Security: Cybersecurity is the practice of protecting internet-connected systems, including hardware, software, and data, from attack, damage, or unauthorized access.
3. Cyber Attack: A cyber-attack is an attempt to damage or disrupt computer systems, networks, or devices using malicious code, software, or other means.
4. Confidentiality: Confidentiality refers to the assurance that information is not disclosed to unauthorized individuals, entities, or processes.
5. Integrity: Integrity refers to the assurance that information is trustworthy, accurate, and consistent.
6. Availability: Availability refers to the assurance that systems, services, and information are accessible and usable when needed.
7. Attacks on Confidentiality: Examples include data breaches, unauthorized access, eavesdropping, and interception of data in transit.
8. Attacks on Integrity: Examples include data manipulation, alteration, or destruction, tampering with data in transit, and impersonation attacks.
9. Attacks on Availability: Examples include denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, and other forms of system overload attacks.
10. Cracking Encrypted Data: This refers to the attempt to break encryption to access sensitive data. Prevention includes using strong encryption algorithms and regularly updating passwords.
11. Man In Middle Attack: In this type of attack, a third party intercepts communications between two parties and impersonates both to steal data or manipulate communication. Prevention includes using secure communication protocols, such as HTTPS.
12. Spyware: This is malicious software that is designed to collect information from a user's computer without their knowledge. Prevention includes using antivirus software and being cautious when downloading software.
13. Malware: Malware is any software designed to harm, damage, or disrupt systems, networks, or devices. Prevention includes using antivirus software and avoiding suspicious downloads.
14. Penetration Testing: Penetration testing is a security testing method used to evaluate the security of a system by simulating attacks. Tools include Nmap, Nessus, and Metasploit.
15. Web Penetration Testing: This is a type of penetration testing that focuses specifically on web applications. Tools include OWASP ZAP, Burp Suite, and SQLMap.
16. Zombie System: A zombie system is a device that has been compromised by malware and can be controlled remotely by an attacker. Prevention includes using antivirus software and avoiding suspicious downloads.

17. DOS Attack: A denial-of-service (DoS) attack is a type of attack that aims to overwhelm a system, network, or service to render it unusable. Prevention includes using a firewall and limiting network access.
18. DDoS Attack: A distributed denial-of-service (DDoS) attack is similar to a DoS attack but is carried out using a network of computers, making it more difficult to defend against. Prevention includes using a content delivery network and limiting network access.
19. Ransomware Attack: In a ransomware attack, malware is used to encrypt data and demand payment in exchange for the decryption key. Prevention includes using antivirus software and regularly backing up data.
20. Phishing: Phishing is a type of social engineering attack in which an attacker attempts to steal sensitive information by posing as a trustworthy entity. Prevention includes educating users about phishing and using spam filters.
21. Password Attacks: Password attacks involve attempting to guess or steal passwords to gain unauthorized access to a system or network. Prevention includes using strong passwords and implementing multi-factor authentication.
22. Drive by Download Attack: A drive-by download attack occurs when a user visits a website and malicious code is downloaded to their computer without their knowledge or consent. The code can install malware, steal personal information or exploit vulnerabilities in the computer's software.

Prevention: Keeping web browsers, operating systems and other software up to date, using an ad-blocker, and being cautious about clicking on links or downloading files from unfamiliar websites.

23. Malvertising: Malvertising refers to the distribution of malicious code through online advertising. Attackers create ads that appear legitimate but actually contain malicious code. When users click on the ads, they are directed to websites that install malware or exploit vulnerabilities in their computers.

Prevention: Using an ad-blocker, keeping web browsers, operating systems and other software up to date, and being cautious about clicking on ads or downloading files from unfamiliar websites.

24. Rogue Software Attack: Rogue software refers to software that appears to be legitimate but actually contains malware or other malicious code. Rogue software can be disguised as anti-virus software, system utilities or other applications.

Prevention: Using legitimate anti-virus software and being cautious about downloading software from unfamiliar websites.

25. Computer Virus: A computer virus is a type of malware that infects a computer and can spread to other computers through email attachments, file sharing, and other methods. Viruses can cause damage to computer files and systems.

Prevention: Using anti-virus software, keeping software up to date, and being cautious about opening email attachments and downloading files from unfamiliar websites.

26. Spyware: Spyware is a type of malware that secretly collects information about a user's computer activity and sends it back to the attacker. Spyware can be used to steal personal information or track online activity.

Prevention: Using anti-spyware software, being cautious about downloading software from unfamiliar websites, and avoiding clicking on suspicious links or pop-ups.

27. Worms: A worm is a type of malware that spreads through computer networks by exploiting vulnerabilities in software. Worms can cause damage to computer systems and can be difficult to detect and remove.

Prevention: Keeping software up to date, using anti-virus software, and being cautious about downloading files from unfamiliar websites.

28. Adware: Adware is software that displays unwanted advertisements on a user's computer. Adware can be installed along with other software without the user's knowledge or consent.

Prevention: Using anti-adware software, being cautious about downloading software from unfamiliar websites, and avoiding clicking on suspicious links or pop-ups.

29. Trojan Horse: A Trojan horse is a type of malware that appears to be legitimate software but actually contains malicious code. Trojans can be used to steal personal information or to give attackers remote access to a user's computer.

Prevention: Using anti-virus software, being cautious about downloading software from unfamiliar websites, and avoiding clicking on suspicious links or pop-ups.

30. Cookies Spyware: Cookies are small text files that are stored on a user's computer by websites. While cookies themselves are not malicious, some websites can use them to track a user's online activity or to collect personal information.

Prevention: Being cautious about accepting cookies from unfamiliar websites, clearing cookies regularly, and using anti-spyware software.

31. Key Logger: A keylogger is a type of software that records every keystroke made on a computer. Keyloggers can be used to steal passwords and other sensitive information.

Prevention: Using anti-virus software, being cautious about downloading software from unfamiliar websites, and avoiding clicking on suspicious links or pop-ups.

32. Brute Force Attack: A brute force attack is a method of trying every possible password combination until the correct one is found. Brute force attacks can be used to gain access to password-protected systems

34. Packet Flood: A packet flood attack is a type of DoS (Denial of Service) attack that involves sending a large number of packets to a target system, overwhelming its resources and making it unavailable to legitimate users. The attack can be launched using a single computer or multiple computers in a coordinated manner, creating a distributed denial of service (DDoS) attack.

Example: An attacker could use a tool like LOIC (Low Orbit Ion Cannon) to launch a packet flood attack against a website, causing it to become unavailable to legitimate users.

Prevention: Packet flood attacks can be prevented by implementing traffic filtering, rate limiting, and other traffic management techniques. Network administrators can also use intrusion detection and prevention systems (IDS/IPS) to detect and block suspicious traffic.

35. MITM (Man-in-the-Middle) Attack: A MITM attack involves intercepting communication between two parties and altering the messages sent between them. This can allow an attacker to steal sensitive information or manipulate communication for malicious purposes.

Example: An attacker could use a tool like Ettercap to intercept and modify messages sent between a user and a website, allowing them to steal login credentials or other sensitive information.

Prevention: MITM attacks can be prevented by using secure communication protocols like SSL/TLS, implementing strong encryption, and using digital certificates to authenticate communication partners.

36. VPN (Virtual Private Network): A VPN is a secure connection that allows users to access the internet securely and privately. It encrypts internet traffic and routes it through a secure network, providing protection against eavesdropping and other forms of cyber attacks.

Example: A user could use a VPN service like NordVPN or ExpressVPN to securely access the internet from public Wi-Fi hotspots.

Command: Some popular VPN tools include OpenVPN, WireGuard, and SoftEther.

37. Adblocker: An ad blocker is a tool that blocks online ads from appearing on a user's screen. It can improve page load times, reduce data usage, and improve privacy by blocking tracking scripts.

Example: A user could install an ad blocker extension like AdBlock Plus or uBlock Origin on their web browser to block ads on websites.

Command: Adblocker tools are usually browser extensions that can be downloaded from the browser's extension store.

38. Firewall: A firewall is a network security tool that monitors and controls incoming and outgoing traffic based on pre-defined security rules. It can prevent unauthorized access to a network and block malicious traffic.

Example: A company could use a firewall to block traffic from unauthorized sources and protect its internal network from cyber attacks.

Command: Popular firewall tools include iptables, pfSense, and Windows Firewall.

39. Antivirus: An antivirus is a security software that protects a computer from malware infections. It scans files and monitors system activity for signs of malicious activity.

Example: A user could install an antivirus software like Norton, McAfee, or Kaspersky to protect their computer from malware infections.

Command: Some popular antivirus tools include Windows Defender, Avast, and AVG.

40. SQL Injection: SQL injection is a type of cyber attack that exploits vulnerabilities in web applications to inject malicious SQL commands into a database. This can allow an attacker to steal sensitive information or modify data.

Example: An attacker could use a SQL injection attack to steal login credentials or modify user accounts on a website.

Prevention: SQL injection attacks can be prevented by using prepared statements or stored procedures, input validation, and access controls. Regular security audits and code reviews can also help identify and fix vulnerabilities.

41. DNS Poisoning: DNS poisoning, also known as DNS cache poisoning, is a type of cyber attack that involves corrupting the DNS cache of a DNS server. The attacker manipulates the DNS cache to redirect users to malicious websites, fake login pages, or phishing pages.

Example: In 2008, a group of hackers launched a DNS poisoning attack on Comcast's DNS servers. The attackers redirected Comcast's customers to a fake Comcast login page, where they were prompted to enter their login credentials.

Prevention: DNS poisoning can be prevented by implementing security measures like DNSSEC (Domain Name System Security Extensions), which provide digital signatures to DNS records to prevent unauthorized modification.

42. Cyber Crime: Cybercrime refers to criminal activities carried out using the internet, computer networks, or other digital technologies. Cybercrimes include identity theft, online scams, cyberstalking, hacking, and malware attacks.

Example: In 2017, a ransomware attack known as WannaCry spread to over 200,000 computers in 150 countries, causing massive damage to businesses and organizations worldwide.

Prevention: Cybercrime prevention involves implementing security measures like firewalls, antivirus software, and encryption to protect against attacks. Organizations can also train employees on safe online practices and regularly backup their data to minimize damage in case of an attack.

43. Structured Attacks: Structured attacks, also known as targeted attacks, involve specific individuals, organizations, or systems. The attacker spends time researching their target to gain information and develop a strategy to breach their security.

Example: In 2016, the Democratic National Committee was the target of a structured attack, where hackers gained access to sensitive data and emails. The attack was suspected to be carried out by a foreign government.

Prevention: Structured attacks can be prevented by implementing strong security measures, regularly updating software, and training employees to recognize and report suspicious activity.

44. Unstructured Attacks: Unstructured attacks, also known as opportunistic attacks, are carried out randomly, without specific targets. The attacker takes advantage of vulnerabilities in systems or software to gain unauthorized access.

Example: A common example of unstructured attacks is phishing emails, where the attacker sends fake emails to users, prompting them to click on a malicious link or download an attachment.

Prevention: Unstructured attacks can be prevented by implementing strong security measures like firewalls, antivirus software, and updating software regularly. Organizations can also train employees on safe online practices and avoid downloading or clicking on suspicious links.

45. Hack Value: Hack value refers to the reputation and recognition a hacker gains from successful cyber attacks. It is often associated with hackers who are motivated by fame, rather than financial gain or political motives.

Example: Kevin Mitnick, a notorious hacker in the 1990s, gained notoriety for his ability to breach high-profile computer systems and networks.

Prevention: Hack value can be discouraged by implementing strong security measures and increasing awareness of the legal consequences of cyber attacks.

46. Vulnerability: A vulnerability is a weakness in a system or software that can be exploited by attackers to gain unauthorized access, steal data, or carry out other malicious activities.

Example: In 2017, the Equifax data breach was caused by a vulnerability in a software application used by the company, which allowed attackers to steal sensitive data of over 143 million customers.

Prevention: Vulnerabilities can be prevented by implementing security measures like regular software updates and patches, using strong passwords, and conducting regular security assessments.

47. Exploit: An exploit is a piece of software, a technique, or a sequence of commands that takes advantage of a vulnerability in a system, application, or network to perform unauthorized actions or gain access to sensitive data. Exploits can be used by attackers to cause harm, steal data, or compromise systems.

Example: One example of an exploit is a buffer overflow attack. In this attack, an attacker sends more data to a buffer than it can hold, causing the buffer to overflow into adjacent memory locations. The attacker can then execute arbitrary code on the system, potentially gaining complete control of the system.

Prevention: Patching systems and applications regularly and promptly, keeping up-to-date with security news and alerts, and using intrusion detection systems can help prevent exploits.

48. Payload: In the context of cybersecurity, a payload is the portion of a malware program that performs the malicious actions, such as stealing data, encrypting files, or launching further attacks. Payloads are designed to cause harm, compromise security, or create a backdoor into a system.

Example: In a ransomware attack, the payload is the part of the malware that encrypts the victim's files and demands a ransom in exchange for the decryption key.

Prevention: The best prevention against payloads is to have strong anti-malware measures in place, including updated antivirus software, firewalls, and intrusion detection systems.

49. Zero-Day Attack: A zero-day attack is a type of cyber attack that exploits a previously unknown vulnerability or software flaw in a system, application, or network. Because the vulnerability is unknown, it is not yet patched or secured, making it a valuable tool for attackers.

Example: A zero-day attack could be used to exploit a previously unknown vulnerability in a popular web browser to gain access to sensitive user data or take control of the user's computer.

Prevention: While it is not possible to completely prevent zero-day attacks, organizations can take steps to minimize their risk, such as keeping systems and applications up-to-date with the latest security patches, monitoring network traffic for suspicious activity, and using intrusion detection systems.

50. Daisy Chaining: In cybersecurity, daisy chaining is a technique used by attackers to bypass security measures by using a series of vulnerabilities, exploits, or compromised systems to gain access to a target system.

Example: An attacker might use daisy chaining to bypass a company's firewall by first compromising a vulnerable web server, then using that server to attack other systems on the network until they can gain access to the target system.

Prevention: The best prevention against daisy chaining attacks is to maintain strong cybersecurity practices, such as regularly patching systems, using strong passwords, and monitoring network traffic for suspicious activity. Additionally, organizations should implement security measures such as firewalls, intrusion detection systems, and security information and event management (SIEM) solutions to detect and respond to attacks.

51. Doxing: Doxing refers to the practice of searching, gathering and publishing private or personally identifiable information (PII) about a particular individual or organization on the internet. The information gathered can be used to intimidate, harass, embarrass, or extort the individual or organization. Examples of PII include the individual's name, address, phone number, email, social media accounts, and other sensitive information. Prevention includes limiting the amount of personal information shared publicly, using strong passwords, and being cautious about what information is shared online.

52. Bot: A bot is a software application that is designed to perform automated tasks over the internet. Bots can be used for legitimate purposes, such as web indexing by search engines, or malicious purposes, such as performing DDoS attacks or spreading malware. Some examples of malicious bots include spambots, clickbots, and credential-stuffing bots. Prevention includes using strong passwords and multi-factor authentication, monitoring network traffic for suspicious activity, and using bot detection and mitigation tools.

53. Security, Functionality, and Usability Triangle: This refers to the concept that security, functionality, and usability are interdependent and must be balanced when developing software or systems. In other words, security measures must not compromise the system's functionality or usability, and the system must remain secure while also being functional and usable. For example, adding layers of security controls may enhance the security of a system but can also make it more difficult for users to access and use the system. Finding a balance between these three elements is essential to developing a secure and effective system.

54.Hacking: Hacking refers to the act of gaining unauthorized access to computer systems, networks, or data. It can be performed for both malicious and non-malicious purposes, such as testing the security of a system or uncovering vulnerabilities. Hacking can be classified as ethical or unethical depending on the intent and motivation behind the act. Prevention includes implementing strong security measures, keeping software and systems up to date, and training users to recognize and report suspicious activity.

55.Hacker: A hacker is an individual who uses their technical knowledge and skills to gain unauthorized access to computer systems, networks, or data. The term hacker can refer to both ethical hackers who use their skills to improve security and uncover vulnerabilities, and malicious hackers who use their skills to steal data, install malware, or commit other crimes. The motivation behind hacking can vary, and not all hackers have malicious intent. Prevention includes implementing strong security measures, keeping software and systems up to date, and training users to recognize and report suspicious activity.

56.Black Hat: A black hat is a term used to describe a hacker or group of hackers who use their skills for malicious purposes, such as stealing data, spreading viruses or malware, or disrupting networks. Black hat hackers often use sophisticated techniques to penetrate systems and networks, and their actions are typically illegal and unethical.

57.White Hat: A white hat hacker is a security professional who uses their skills for ethical purposes, such as testing the security of computer systems and networks, identifying vulnerabilities, and helping organizations improve their overall security posture. White hat hackers often work for companies or government agencies to ensure that their systems are secure.

58.Gray Hat: Gray hat hackers are a mix of black and white hat hackers. They use their skills for both ethical and unethical purposes. For example, a gray hat hacker might discover a vulnerability in a system and report it to the company, but also use that same vulnerability to gain access to the system for personal gain.

59.Suicide Hacker: A suicide hacker is a type of hacker who is willing to take extreme risks, including sacrificing their own life, in order to achieve their goals. Suicide hackers are typically motivated by political or ideological beliefs and are often associated with terrorist organizations.

60.Script Kiddies: Script kiddies are individuals who use pre-packaged hacking tools and scripts without actually understanding how they work. They typically lack the technical knowledge to create their own tools or write their own code and instead rely on pre-made tools to carry out attacks. Script kiddies are often associated with low-level cybercrime and are generally considered a nuisance rather than a serious threat.

61. Cyber Terrorists: Cyber terrorists are individuals, groups, or organizations that use hacking methods to create terror and chaos for political or ideological reasons. They target critical infrastructures such as government agencies, financial institutions, and transportation systems, and their attacks can have severe consequences.

62. State Sponsored Hackers: State-sponsored hackers are hackers who work for governments and use their skills to conduct cyber espionage, sabotage, and other activities to further their nation's interests. These hackers are often highly skilled and have access to significant resources and tools that allow them to carry out sophisticated attacks.

63. Hacking Phases: Hacking is a complex process that involves multiple stages, including reconnaissance, scanning, gaining access, maintaining access, and covering tracks. These phases are often referred to as the hacking lifecycle and provide a framework for attackers to follow.

64. Scanning: Scanning is the process of identifying and mapping out the target network or system to identify vulnerabilities and weaknesses. This involves using various tools and techniques to identify open ports, services, and other network resources.

65. Active and Passive Reconnaissance: Reconnaissance is the process of gathering information about the target system or network. It can be either active or passive. Active reconnaissance involves actively probing the target system or network to gather information, while passive reconnaissance involves gathering information without actively engaging with the target system or network. Examples of passive reconnaissance include browsing the target's website, reviewing public records and social media profiles, and performing WHOIS lookups. Active reconnaissance techniques include port scanning, ping sweeping, and vulnerability scanning.

66. Gaining Access: This phase involves attempting to gain access to the target system or network. This can be done by exploiting vulnerabilities, brute-forcing passwords, using social engineering tactics, or other methods.

67. Maintaining Access: Once access has been gained, the attacker seeks to maintain access for future use. This can involve creating backdoors, installing remote access trojans, or other methods.

68. Clearing Tracks: To avoid detection, attackers will often attempt to cover their tracks by deleting logs, modifying timestamps, and other methods.

69. Ethical Hacking: Ethical hacking, also known as "penetration testing," is the practice of attempting to hack into a system or network in order to identify vulnerabilities that could be exploited by malicious attackers. Ethical hackers are often hired by organizations to perform these tests in order to improve their security posture. Ethical hacking is legal and ethical, as it is conducted with the owner's permission and for the purpose of improving security.

70. Footprinting is the process of gathering information about a target system or organization. It is usually the first step in the process of hacking or penetration testing and involves gathering information from publicly available sources.

1. Search Engines: Search engines like Google, Bing, and Yahoo can be used to gather information about a target. This information can include details about the organization's website, employees, contact information, and more.

Tools: Google, Bing, Yahoo, DuckDuckGo, Shodan

2. Google Dorking: Google dorking involves using advanced search operators to narrow down search results to a specific target. This can be useful for finding sensitive information that may not be easily discoverable through regular search methods.

Tools: Google Dorking Database, GHDB, Google Hacking Database

3. Social networking sites: Social networking sites like LinkedIn, Facebook, and Twitter can be used to gather information about employees, job titles, and more.

Tools: LinkedIn, Facebook, Twitter, Instagram, Snapchat

4. Website: Footprinting a website involves gathering information about the target's website, including its IP address, domain name, hosting provider, web server type, and more.

Tools: Whois, Netcraft, DNS Lookup, Nmap, Robtex

5. Email: Email footprinting involves gathering information about email accounts associated with the target, including the email address, email server, and email client used.

Tools: The Harvester, Maltego, Shodan, Metasploit

6. Whois: Whois lookup involves gathering information about the domain name, including the owner's name, contact details, and registration date.

Tools: Whois, DomainTools, ICANN WHOIS

7. Competitive Intelligence: Competitive intelligence involves gathering information about competitors in the same industry, including their products, services, pricing, and more.

Tools: LinkedIn, Glassdoor, Hoovers, Owler, Alexa, SimilarWeb

8. DNS: DNS footprinting involves gathering information about the target's DNS servers, including their IP address, domain name, and more.

Tools: NSLookup, DNSDumpster, Fierce, DNSRecon, Dig

9. Network: Network footprinting involves gathering information about the target's network, including its topology, devices, and services.

Tools: Nmap, Wireshark, Angry IP Scanner, Netcat, OpenVAS

10. Social Engineering: Social engineering involves manipulating individuals to disclose sensitive information about a target system or organization.

Tools: Phishing kits, SET, Maltego, Social-Engineer Toolkit, BeEF

71. IP Address: An IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two primary functions: host or network interface identification and location addressing.

72. Ports: A port is a communication endpoint used in computer networking. Ports allow computers to transmit and receive data across networks. There are 65,535 ports available for use in TCP/IP communication.

73. Proxy: A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. Proxies are commonly used for content filtering, security, and anonymity.

74. TCP Flags: TCP Flags are used within TCP/IP communication to control and manage the communication process. TCP Flags include ACK, SYN, RST, PSH, FIN, and URG.

75. TCP/IP Communication: TCP/IP is a suite of communication protocols used to connect devices over the internet. It consists of two main protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP).

76. Nmap: Nmap is a network exploration and security auditing tool that allows users to discover hosts and services on a computer network, as well as create a map of the network.

77. TCP Full Open Scan: TCP Full Open Scan is a type of port scanning technique used to identify open ports on a target system. It involves completing the TCP handshake and establishing a connection with the target system.

78. TCP Half Open Scan: TCP Half Open Scan is a type of port scanning technique that involves only completing the first part of the TCP handshake. This technique can be used to identify open ports without establishing a full connection.

79. UDP Scan: UDP Scan is a type of port scanning technique used to identify open UDP ports on a target system. Unlike TCP, UDP does not establish a connection before transmitting data.

80. Stealth Scan: Stealth Scan is a type of port scanning technique that attempts to avoid detection by firewalls and intrusion detection systems. It involves manipulating TCP flags to trick the target system into thinking the connection is legitimate.

81. FIN Scan: FIN scan is a type of port scanning technique in which an attacker sends packets with the FIN flag set to the target machine to identify open ports. If the target system responds with a RST packet, then the port is closed, but if it doesn't respond, the port is considered open. It is a stealth scan as it doesn't complete the three-way handshake.

82. Null Scan: A null scan is a port scanning technique in which an attacker sends TCP packets with no flags set to the target system. If the target system responds with a RST packet, then the port is closed, but if it doesn't respond, the port is considered open.

83. XMAS Scan: XMAS scan is a port scanning technique in which an attacker sends TCP packets with the FIN, PSH, and URG flags set to the target machine. If the target system responds with a RST packet, then the port is closed, but if it doesn't respond, the port is considered open.

84. Nessus: Nessus is a popular vulnerability scanner that is used to identify vulnerabilities in networks and systems. It can scan for a wide range of vulnerabilities and can be used to identify misconfigurations, outdated software, and other vulnerabilities that could be exploited by attackers.

85. Hping: Hping is a command-line tool used for network scanning, fingerprinting, and testing. It can be used for testing the security of firewalls, networks, and systems. Hping can send various types of packets, including TCP, UDP, and ICMP packets.

86. Port Scanning: Port scanning is the process of scanning a target system to identify open ports and services. Attackers use port scanning to identify potential entry points into a system or network.

87. Cyberstalking: Cyberstalking is the use of the internet or other electronic means to harass or stalk someone. It can include sending threatening messages, monitoring someone's online activity, and other forms of harassment.

88. IP Spoofing: IP Spoofing is a technique used by attackers to forge IP packets to appear as if they were sent from a trusted source. It is used to bypass authentication or access controls and to launch attacks that appear to come from a legitimate source.

89. Homograph Attack: A homograph attack is a type of phishing attack in which an attacker uses a domain name that looks similar to a legitimate website to trick users into entering sensitive information. For example, an attacker could use a domain name like "g00gle.com" instead of "google.com" to trick users.

90. Phreaking Attack: Phreaking is the process of exploiting vulnerabilities in telecommunications systems to gain unauthorized access. It can include tapping phone lines, bypassing long-distance charges, and other forms of telephone fraud.

91. ICMP Attack: ICMP (Internet Control Message Protocol) is a protocol that allows network devices to send error messages to each other. ICMP attacks involve sending a large number of ICMP packets to a target system in an attempt to overwhelm it and cause a denial of service. These attacks can also be used to map out a network's topology.

92. Connect Scan: A connect scan is a type of port scan that sends a full connection request to a target port. If the port is open, the target system will respond with a connection established message. This type of scan can be easily detected by firewalls and IDS systems.

93. Hacktivist: A hacktivist is a person who uses hacking techniques to promote a political or social cause. Hacktivists are often associated with hacktivist groups such as Anonymous or LulzSec.

94. Botnet: A botnet is a network of computers that have been infected with malware and are under the control of a hacker. Botnets can be used to launch DDoS attacks, steal sensitive information, or distribute spam.

95. Cyber Squatting: Cyber squatting involves registering a domain name that is similar to an existing brand or trademark with the intention of profiting from it. Cyber squatters may also create websites that mimic the look and feel of the original website in order to deceive users.

96. Packet Sniffing: Packet sniffing involves intercepting and analyzing network traffic in order to extract sensitive information such as passwords or credit card numbers. This can be done using specialized software or hardware tools.

97. Teardrop Attack: A teardrop attack is a type of DoS attack that involves sending malformed IP packets to a target system. These packets are designed to cause the target system to crash or become unresponsive.

98. Fingerprinting: Fingerprinting is the process of gathering information about a target system in order to identify its operating system, software, and other characteristics. This can be done using tools such as Nmap or by analyzing network traffic.

99. Dumpster Diving: Dumpster diving involves searching through a target's trash in order to find sensitive information such as passwords or confidential documents. This can be a surprisingly effective way to gather information about a target organization.

100. Enumeration: Enumeration involves gathering information about a target system or network in order to identify potential vulnerabilities. This can be done using tools such as Nmap or by analyzing network traffic.

101. Network Probe: A network probe is a type of software tool or technique that is used by hackers to gain information about a target network. Network probing is the process of actively seeking out devices and systems on a network to identify vulnerabilities that can be exploited.

102. RST Cookies: RST cookies are a type of anti-DDoS (Distributed Denial of Service) technique that is used by firewalls and other network security devices to block TCP connections that are initiated by attackers. RST cookies work by sending a reset signal to the attacker's IP address when a connection request is made. This effectively blocks the attacker from establishing a connection with the target network.

103. IDS: IDS stands for Intrusion Detection System. An IDS is a security tool or system that monitors network traffic for signs of unauthorized or malicious activity. When an IDS detects suspicious activity, it will generate an alert, which can be used by security personnel to investigate and respond to potential security threats.

104. IPS: IPS stands for Intrusion Prevention System. An IPS is a type of security tool or system that is designed to prevent security threats before they can occur. IPS devices can be used to block network traffic that is deemed to be suspicious or malicious, as well as to enforce security policies and rules on a network.

105. Smishing Attack: Smishing is a type of social engineering attack that uses text messages (SMS) to trick people into revealing sensitive information or downloading malware onto their devices. In a smishing attack, the attacker sends a text message to the victim that appears to be from a legitimate source, such as a bank or other financial institution. The message will usually

contain a link or phone number that the victim is instructed to click on or call, which will then lead to a phishing website or malware download. To protect against smishing attacks, users should always be cautious of text messages that request sensitive information or contain suspicious links. It is recommended to avoid clicking on unknown links and to verify the source of the message before responding to any requests for information.