40 Cyber Security MCQ With Answers And Explanations

The following multiple-choice questions are just a Warm-up Questions for you which are as follows:

1. Why would a hacker use a proxy server?
A. To create a stronger connection with the target.
B. To create a ghost server on the network.
C. To obtain a remote access connection.
D. To hide malicious activity on the network.

Correct Answer – D
Explanation – Proxy servers exist to act as an intermediary between the hacker and the target and services to keep the hacker anonymous to the network.

2. What type of symmetric key algorithm using a streaming cipher to encrypt information?
A. RC4
B. Blowfish
C. SHA
D. MD5

Correct Answer – A
Explanation – RC$ uses streaming ciphers.

3. Which of the following is not a factor in securing the environment against an attack on security?
A. The education of the attacker
B. The system configuration
C. The network architecture
D. The business strategy of the company
E. The level of access provided to employees

Correct Answer – D
Explanation – All of the answers are factors supporting the exploitation or prevention of an attack. The business strategy may provide the motivation for a potential attack, but by itself will not influence the outcome.

4. What type of attack uses a fraudulent server with a relay address?
A. NTLM
B. MITM
C. NetBIOS
D. SMB

Correct Answer – B
Explanation – MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.

5. What port is used to connect to the Active Directory in Windows 2000?
A. 80
B. 445

C. 139
D. 389

Correct Answer – D
Explanation – The Active Directory Administration Tool used for a Windows 2000 LDAP client uses port 389 to connect to the Active Directory service.
6. To hide information inside a picture, what technology is used?
A. Rootkits
B. Bitmapping
C. Steganography
D. Image Rendering

Correct Answer – C
Explanation – Steganography is the right answer and can be used to hide information in pictures, music, or videos.
7. Which phase of hacking performs actual attack on a network or system?
A. Reconnaissance
B. Maintaining Access
C. Scanning
D. Gaining Access

Correct Answer – D
Explanation – In the process of hacking, actual attacks are performed when gaining access, or ownership, of the network or system. Reconnaissance and Scanning are information gathering steps to identify the best possible action for staging the attack.
Maintaining access attempts to prolong the attack.
8. Attempting to gain access to a network using an employee's credentials is called the ____________ mode of ethical hacking.
A. Local networking
B. Social engineering
C. Physical entry
D. Remote networking

Correct Answer – A
Explanation – Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.
9. Which Federal Code applies the consequences of hacking activities that disrupt subway transit systems?
A. Electronic Communications Interception of Oral Communications
B. 18 U.S.C. § 1029
C. Cyber Security Enhancement Act 2002
D. 18 U.S.C. § 1030

Correct Answer – C
Explanation – The Cyber Security Enhancement Act 2002 deals with life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems.
10. Which of the following is not a typical characteristic of an ethical hacker?
A. Excellent knowledge of Windows.
B. Understands the process of exploiting network vulnerabilities.
C. Patience, persistence and perseverance.
D. Has the highest level of security for the organization.

Correct Answer – D
Explanation – Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.
11. What is the proper command to perform an Nmap XMAS scan every 15seconds?
A. nmap -sX -sneaky
B. nmap -sX -paranoid
C. nmap -sX -aggressive
D. nmap -sX -polite

Correct Answer – A
Explanation – SX is used to identify a xmas scan, while sneaky performs scans 15 seconds apart.
12. What type of rootkit will patch, hook, or replace the version of system call in order to hide information?
A. Library level rootkits
B. Kernel level rootkits
C. System level rootkits
D. Application level rootkits

Correct Answer – A
Explanation – Library leve rootkits is the correct answer. Kerel level focuses on replacing specific code while application level will concentrate on modifying the behavior of the application or replacing application binaries. The type, system level, does not exist for rootkits.
13. What is the purpose of a Denial of Service attack?
A. Exploit a weakness in the TCP/IP stack
B. To execute a Trojan on a system
C. To overload a system so it is no longer operational
D. To shutdown services by turning them off

Correct Answer – C
Explanation – DoS attacks force systems to stop responding by overloading the processing of the system.
14. What are some of the most common vulnerabilities that exist in a network or system?

A. Changing manufacturer, or recommended, settings of a newly installed application.
B. Additional unused features on commercial software packages.
C. Utilizing open source application code
D. Balancing security concerns with functionality and ease of use of a system.

Correct Answer – B
Explanation – Linux is an open source code and considered to have greater security than the commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist. Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack.
15. What is the sequence of a TCP connection?
A. SYN-ACK-FIN
B. SYN-SYN ACK-ACK
C. SYN-ACK
D. SYN-SYN-ACK

Correct Answer – B
Explanation – A three-handed connection of TCP will start with a SYN packet followed by a SYN-ACK packet. A final ACK packet will complete the connection.
16. What tool can be used to perform SNMP enumeration?
A. DNSlookup
B. Whois
C. Nslookup
D. IP Network Browser

Correct Answer – D
Explanation – SNMPUtil and IP Network Browser is SNMP enumeration tool
17. Which ports should be blocked to prevent null session enumeration?
A. Ports 120 and 445
B. Ports 135 and 136
C. Ports 110 and 137
D. Ports 135 and 139

Correct Answer – D
Explanation – Port 139 is the NetBIOS Session port typically can provide large amounts of information using APIs to connect to the system. Other ports that can be blocked in 135, 137,138, and 445.
18. The first phase of hacking an IT system is compromise of which foundation of security?
A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Correct Answer – B
Explanation – Reconnaissance is about gathering confidential information, such as usernames and passwords.
19. How is IP address spoofing detected?
A. Installing and configuring a IDS that can read the IP header
B. Comparing the TTL values of the actual and spoofed addresses
C. Implementing a firewall to the network
D. Identify all TCP sessions that are initiated but does not complete successfully

Correct Answer – B
Explanation – IP address spoofing is detectable by comparing TTL values of the actual and spoofed IP addresses
20. Why would a ping sweep be used?
A. To identify live systems
B. To locate live systems
C. To identify open ports
D. To locate firewalls

Correct Answer – A
Explanation – A ping sweep is intended to identify live systems. Once an active system is found on the network, other information may be distinguished, including location. Open ports and firewalls.
21. What are the port states determined by Nmap?
A. Active, inactive, standby
B. Open, half-open, closed
C. Open, filtered, unfiltered
D. Active, closed, unused

Correct Answer – C
Explanation – Nmap determines that ports are open, filtered, or unfiltered.
22. What port does Telnet use?
A. 22
B. 80
C. 20
D. 23

Correct Answer – D
Explanation – Telnet uses port 23.
23. Which of the following will allow foot printing to be conducted without detection?
A. PingSweep
B. Traceroute
C. War Dialers
D. ARIN

Correct Answer – D

Explanation – ARIN is a publicly accessible database, which has information that could be valuable. Because it is public, any attempt to obtain information in the database would go undetected.

24. Performing hacking activities with the intent on gaining visibility for an unfair situation is called ________.

A. Cracking
B. Analysis
C. Hacktivism
D. Exploitation

Correct Answer – C

Explanation – Hacktivism is the act of malicious hacking for a cause or purpose.

25. What is the most important activity in system hacking?

A. Information gathering
B. Cracking passwords
C. Escalating privileges
D. Covering tracks

Correct Answer – B

Explanation – Passwords are a key component to access a system, making cracking the password the most important part of system hacking.

26. A packet with no flags set is which type of scan?

A. TCP
B. XMAS
C. IDLE
D. NULL

Correct Answer – D

Explanation – A NULL scan has no flags set.

27. Sniffing is used to perform ______________ fingerprinting.

A. Passive stack
B. Active stack
C. Passive banner grabbing
D. Scanned

Correct Answer – A

Explanation – Passive stack fingerprinting uses sniffing technologies instead of scanning.

28. Phishing is a form of ____________________.

A. Spamming
B. Identify Theft
C. Impersonation
D. Scanning

Correct Answer – C
Explanation – Phishing is typically a potential attacker posing, or impersonating, a financial institution
29. Why would HTTP Tunneling be used?
A. To identify proxy servers
B. Web activity is not scanned
C. To bypass a firewall
D. HTTP is a easy protocol to work with

Correct Answer – C
Explanation – HTTP Tunneling is used to bypass the IDS and firewalls present on a network.
30. Which Nmap scan is does not completely open a TCP connection?
A. SYN stealth scan
B. TCP connect
C. XMAS tree scan
D. ACK scan

Correct Answer – A
Explanation – Also known as a "half-open scanning," SYN stealth scan will not complete a full TCP connection.
31. What protocol is the Active Directory database based on?
A. LDAP
B. TCP
C. SQL
D. HTTP

Correct Answer – A
Explanation – Active4 direction in Windows 200 is based on a Lightweight Directory Access Protocol (LDAP).
32. Services running on a system are determined by _____________.
A. The system's IP address.
B. The Active Directory
C. The system's network name
D. The port assigned

Correct Answer – D
Explanation – Hackers can identify services running on a system by the open ports that are found.
33. What are the types of scanning?
A. Port, network, and services
B. Network, vulnerability, and port
C. Passive, active, and interactive
D. Server, client, and network

Correct Answer – B
Explanation – The three types of accepted scans are port, network, and vulnerability.
34. Enumeration is part of what phase of ethical hacking?
A. Reconnaissance
B. Maintaining Access
C. Gaining Access
D. Scanning

Correct Answer – C
Explanation – Enumeration is a process of gaining access to the network by obtaining information on a user or system to be used during an attack.
35. Keyloggers are a form of _______________.
A. Spyware
B. Shoulder surfing
C. Trojan
D. Social engineering

Correct Answer – A
Explanation – Keyloggers are a form of hardware or software spyware installed between the keyboard and operating system.
36. What are hybrid attacks?
A. An attempt to crack passwords using words that can be found in dictionary.
B. An attempt to crack passwords by replacing characters of a dictionary word with numbers and symbols.
C. An attempt to crack passwords using a combination of characters, numbers, and symbols.
D. An attempt to crack passwords by replacing characters with numbers and symbols.

Correct Answer – B
Explanation – Hybrid attacks do crack passwords that are created with replaced characters of dictionary type words.
37. Which form of encryption does WPA use?
A. Shared key
B. LEAP
C. TKIP
D. AES

Correct Answer – C
Explanation – TKIP is used by WPA
38. What is the best statement for taking advantage of a weakness in the security of an IT system?
A. Threat
B. Attack
C. Exploit
D. Vulnerability

Correct Answer – C
Explanation – A weakness in security is exploited. An attack does the exploitation. A weakness is vulnerability. A threat is a potential vulnerability.
39. Which database is queried by Whois?
A. ICANN
B. ARIN
C. APNIC
D. DNS

Correct Answer – A
Explanation – Who utilizes the Internet Corporation for Assigned Names and Numbers.
40. Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?
A. Web-based
B. Human-based
C. User-based
D. Computer-based

Correct Answer – D
Explanation – Whether using email, a fake website, or popup to entice the used, obtaining information from an individual over the Internet is a computer-based type of social engineering