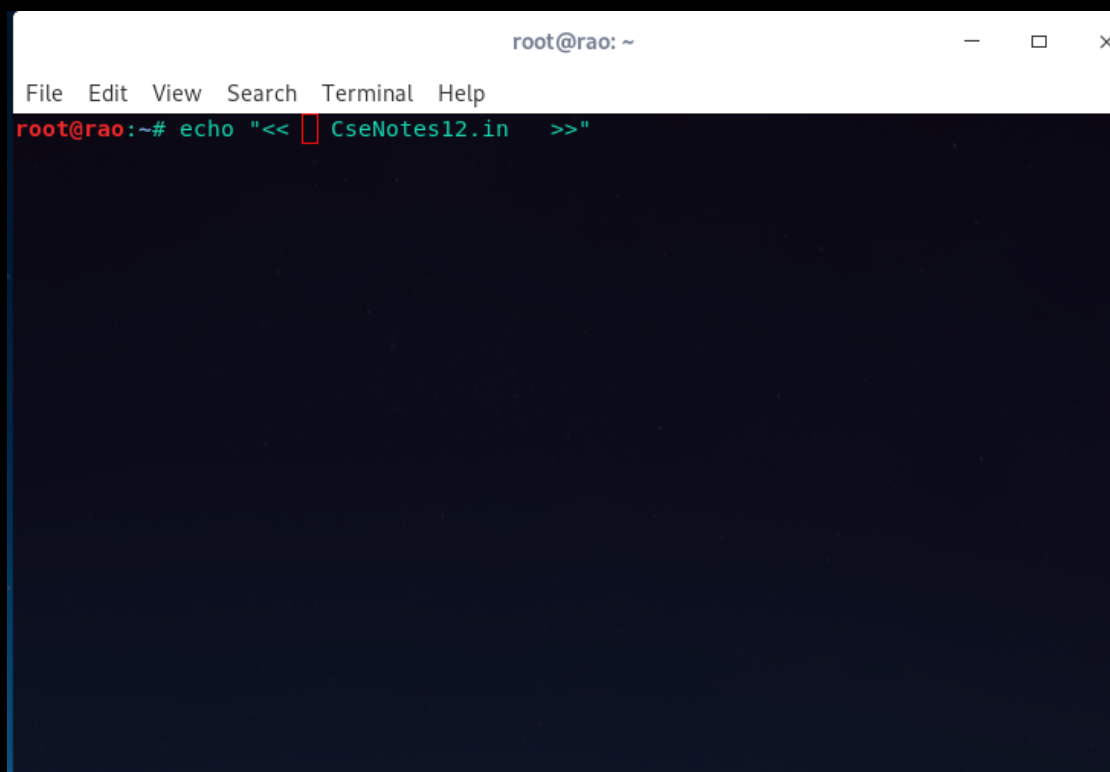


# Int 242 Mcqs Cyber Security Essentials (Mcqs) )Multiple Choice Questions Practice Questions

on September 21, 2019

## Int 242 Mcqs Cyber Security Essentials

A screenshot of a terminal window titled 'root@rao: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows a command prompt 'root@rao:~#' followed by the command 'echo "<< CseNotes12.in >>"'. The command is partially entered, with a red cursor at the end of the line.

```
root@rao: ~  
File Edit View Search Terminal Help  
root@rao:~# echo "<< CseNotes12.in >>"
```

## MCQ With Answers

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 RC4 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.

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 footprinting 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

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 &#x201C;half-open scanning,&#x201D; 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&#x2019;s IP address.

B. The Active Directory

C. The system&#x2019;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.

c) what kind of firewall is in use

d) what type of antivirus is in use

View Answer

Answer: d

Explanation: Network Mapper (Nmap) is a popular open-source tool used for discovering network as well as security auditing. It usually checks for different services used by the host, what operating

system it is running and the type of firewall it is using.

45. Which of the following deals with network intrusion detection and real-time traffic analysis?

- a) John the Ripper
- b) LophtCrack
- c) Snort
- d) Nessus

View Answer

Answer: c

Explanation: Snort is a network intrusion detecting application that deals with real-time traffic analysis. As the rules are set and kept updated, they help in matching patterns against known patterns and protect your network.

46. Wireshark is a \_\_\_\_\_ tool.

- a) network protocol analysis
- b) network connection security
- c) connection analysis
- d) defending malicious packet-filtering

View Answer

Answer: a

Explanation: Wireshark is popular standardized network protocol analysis tools that allow in-depth check and analysis of packets from different protocols used by the system.

47. Which of the below-mentioned tool is used for Wi-Fi hacking?

- a) Wireshark
- b) Nessus
- c) Aircrack-ng
- d) Snort

View Answer

Answer: c

Explanation: Weak wireless encryption protocols get easily cracked using Aircrack WPA and Aircrack WEP attacks that comes with Aircrack-ng tool. Its packet sniffing feature keeps track of all its traffic without making any attack.

48. Aircrack-ng is used for \_\_\_\_\_

- a) Firewall bypassing
- b) Wi-Fi attacks
- c) Packet filtering

d) System password cracking

View Answer

Answer: b

Explanation: Weak wireless encryption protocols get easily cracked using Aircrack WPA and Aircrack WEP. Its packet sniffing feature keeps track of all its traffic without making any attack.

49. \_\_\_\_\_ is a popular IP address and port scanner.

- a) Cain and Abel
- b) Snort
- c) Angry IP Scanner
- d) Ettercap

View Answer

Answer: c

Explanation: Angry IP scanner is a light-weight, cross-platform IP



and port scanning tool that scans a range of IP. It uses the concept of multithreading for making fast efficient scanning.

50. \_\_\_\_\_ is a popular tool used for network analysis in multiprotocol diverse network.

- a) Snort
- b) SuperScan
- c) Burp Suit
- d) EtterPeak

View Answer

Answer: d

Explanation: EtterPeak is a network analysis tool that can be used for multiprotocol heterogeneous networking architecture. It can help in sniffing packets of network traffic.

51. \_\_\_\_\_ scans TCP ports and resolves different hostnames.

- a) SuperScan
- b) Snort
- c) Ettercap
- d) QualysGuard

View Answer

Answer: a

Explanation: SuperScan has a very nice user-friendly interface and it is used for scanning TCP ports as well as resolve hostnames. It is popularly used for scanning ports from a given range of IP.

52. \_\_\_\_\_ is a web application assessment security tool.

- a) LC4
- b) WebInspect
- c) Ettercap
- d) QualysGuard

View Answer

Answer: b

Explanation: WebInspect is a popular web application security tool used for identifying known vulnerabilities residing in web-application layer. It also helps in penetration testing of web servers.

53. Which of the following attack-based checks WebInspect cannot do?

- a) cross-site scripting
- b) directory traversal
- c) parameter injection
- d) injecting shell code

View Answer

Answer: d

Explanation: WebInspect can check whether a web server is properly configured or not by attempting for common attacks such as Cross-site scripting, directory traversal, and parameter injection. But it cannot inject malicious shell code in the server.

54. \_\_\_\_\_ is a password recovery and auditing tool.

- a) LC3

- b) LC4
- c) Network Stumbler
- d) Maltego

[View Answer](#)

Answer: b

Explanation: LC4 which was previously known as LophtCrack is a password auditing and recovery tool; used for testing strength of a password and also helps in recovering lost Microsoft Windows passwords.

55. LophtCrack is formerly known as LC3.

- a) True
- b) False

[View Answer](#)

Answer: b

Explanation: LophtCrack is now commonly known as LC4 is a password auditing and recovery tool; used for testing strength of a password and also helps in recovering lost Microsoft Windows passwords.

To leave a comment, click the button below to sign in with Google.

[SIGN IN WITH GOOGLE](#)



## Mobile Holder

Free Shipping | Flat 50% Off |  
Last Day Offer | COD Available  
[theurbangadget.com](http://theurbangadget.com)

Order Now >

## Popular Posts




### CSE 423 Virtualization and Cloud Computing

*CSE423 : VIRTUALIZATION AND CLOUD COMPUTING Syllabus : Unit I: Virtualization techniques: virtualization technology, overview of x86 virtualization, types of virtualization, virtualization products, cloud interoperability standards, concept of VLAN ,VSAN and bene ...*



### JAVA PPT

*JAVA LECTURE 310 FOR fourth SEMESTER*

 Powered by Blogger