DUMPSARENA

Certified Ethical Hacker Exam (CEHv13)

ECCouncil 312-50v13

Version Demo

Total Demo Questions: 20

Total Premium Questions: 572

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Pool A	140
Topic 2, Exam Pool B	182
Topic 3, Exam Pool C	250
Total	572

QUESTION NO: 1

Which of the following are well known password-cracking programs?

A. L0phtcrack

B. NetCat

C. Jack the Ripper

D. Netbus

E. John the Ripper

ANSWER: A E

Explanation:

L0phtcrack and John the Ripper are well-known password-cracking programs. L0phtcrack is used to recover passwords, primarily Microsoft Windows passwords. John the Ripper is a free and open-source password-cracking software tool, known for cracking passwords of various encrypted data formats. More information can be found on the official John the Ripper page.

QUESTION NO: 2

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

ANSWER: A C D E

Explanation:

A zone transfer is a type of DNS transaction where all or part of a DNS zone is replicated or transferred from a master to a secondary DNS server. This action is typically used to synchronize the DNS records across DNS servers. Tools commonly used to perform a zone transfer include NSLookup, Dig, and Host, which are native tools available in Unix/Linux/MacOS and even in Windows environments. These tools allow you to query DNS servers for various types of DNS records, including

performing zone transfers when not properly secured. Sam Spade is also used for network troubleshooting and can perform zone transfers. Learn more about DNS here.

QUESTION NO: 3

Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

A. Nikto

B. Nmap

C. Metasploit

D. Armitage

ANSWER: A

Explanation:

Gavin is most likely using Nikto for the website security audit. Nikto is a web server scanner that tests web servers for dangerous files/CGIs, outdated server software, and other problems. It's commonly used for checking for misconfigurations and outdated software versions on web servers. Nikto Documentation provides detailed information about its capabilities and usage.

QUESTION NO: 4

As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you choose to meet these requirements?

A. Use symmetric encryption with the AES algorithm.

The encrypted email and the encrypted symmetric key are then sent to the recipient.
• The sender also generates a digital signature for the email, using their private key and a hash function, such as SHA-256, which is a secure and widely used algorithm for generating hashes. A hash function is a mathematical function that takes any input and produces a fixed-length output, called a hash or a digest, that uniquely represents the input. A digital signature is a hash of the email that is encrypted with the sender's private key, using RS
The digital signature is then attached to the email and sent to the recipient.
• When the recipient receives the email, they first decrypt the symmetric key with their private key, using RS
They then use the symmetric key to decrypt the email content, using AES. They also verify the digital signature by decrypting it with the sender's public key, using RSA, and comparing the resulting hash with the hash of the email, using the same hash function. If the hashes match, it means that the email is authentic and has not been tampered with.
Using this technique, the email communication is secure because:
• The confidentiality of the email content is ensured by the symmetric encryption with AES, which is hard to break without knowing the symmetric key.
• The symmetric key is also protected by the asymmetric encryption with RSA, which is hard to break without knowing the recipient's private key.
• The non-repudiation of the email is ensured by the digital signature with RSA, which is hard to forge without knowing the

sender's private key.
• The digital signature also provides authentication and integrity of the email, as it proves that the email was sent by the sender and has not been altered in transit.

References:

• How to Encrypt Email (Gmail, Outlook, iOS, Yahoo, Android, AOL)

B. Use the Diffie-Hellman protocol for key exchange and encryption.

C. Apply asymmetric encryption with RSA and use the public key for encryption.

D. Apply asymmetric encryption with RSA and use the private key for signing.

ANSWER: D

Explanation:

The question is about achieving confidentiality and non-repudiation in secure email communication. Using both symmetric and asymmetric cryptography enables this goal. The confidentiality of the email content is ensured through symmetric encryption such as AES, which is efficient for encrypting bulk data. Non-repudiation is ensured by using asymmetric encryption, specifically RSA, where the sender signs the message with their private key, generating a digital signature. This signature authenticates the identity of the sender and ensures the message's integrity because it cannot be forged without access to the private key. Therefore, the correct approach is to use RSA for signing with a private key for non-repudiation. For more information on RSA and digital signatures, one can reference the NIST Special Publication 800-57 Part 1.

QUESTION NO: 5

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. NMap

ANSWER: A B D

Explanation:

Simple Network Management Protocol (SNMP) is a protocol used for network management that operates on the application layer of the Internet Protocol Suite. SNMP is used for collecting and organizing information about managed devices on IP

networks. Tools like SNMPUtil, SNScan, and Solarwinds IP Network Browser are designed to perform SNMP requests to gather information from network devices. SolarWinds official link provides more information on SNMP monitoring tools.

QUESTION NO: 6

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications

B. Harden DNS servers

C. Use split-horizon operation for DNS servers

D. Restrict Zone transfers

E. Have subnet diversity between DNS servers

ANSWER: B C D E

Explanation:

Ensuring DNS security is crucial to maintaining the integrity and resilience of a company's network services. Recommendations to enhance DNS security include hardening DNS servers to protect against unauthorized access and attacks, using split-horizon DNS to provide different server answers to internal versus external queries, and restricting zone transfers to prevent unauthorized copying of DNS zones. Additionally, having subnet diversity between DNS servers adds redundancy and protects against subnet-specific threats. For more information, refer to the official documentation: Security Considerations for DNS.

QUESTION NO: 7

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

ANSWER: B D E

Explanation:

Enumeration is a key stage in ethical hacking and penetration testing. It involves extracting information such as usernames, group information, shared resources, and services from a target system. Tools like USER2SID and SID2USER are utilized for Windows system enumeration to resolve usernames from SID and vice versa. DumpSec is used to access and enumerate security information from Windows systems. For further insight into enumeration tools, you can visit EC-Council's official website.

QUESTION NO: 8

Bob received this text message on his mobile phone: “Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com”. Which statement below is true?

A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.

B. This is a scam because Bob does not know Scott.

C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.

D. This is probably a legitimate message as it comes from a respectable organization.

ANSWER: A

Explanation:

The message Bob received is a classic phishing attempt. Phishing is a type of scam where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker. In this case, the use of a free email service like Yahoo for official bank communications is a red flag, as legitimate financial institutions typically use their own domain rather than a public email service. This is why option A is correct. For more information, you can read official resources on phishing like the FTC’s Guide on Recognizing and Avoiding Phishing Scams.

QUESTION NO: 9

To create a botnet. the attacker can use several techniques to scan vulnerable machines. The attacker first collects Information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list Is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.

Which technique is discussed here?

A. Hit-list-scanning technique

B. Topological scanning technique

C. Subnet scanning technique

D. Permutation scanning technique

ANSWER: A

Explanation:

One of the biggest problems a worm faces in achieving a very fast rate of infection is “getting off the ground.” although a worm spreads exponentially throughout the early stages of infection, the time needed to infect say the first 10,000 hosts dominates the infection time.

There is a straightforward way for an active worm a simple this obstacle, that we term hit-list scanning. Before the worm is free, the worm author collects a listing of say ten,000 to 50,000 potentially vulnerable machines, ideally ones with sensible network connections. The worm, when released onto an initial machine on this hit-list, begins scanning down the list. once it infects a machine, it divides the hit-list in half, communicating half to the recipient worm, keeping the other half.

This fast division ensures that even if only 10-20% of the machines on the hit-list are actually vulnerable, an active worm can quickly bear the hit-list and establish itself on all vulnerable machines in only some seconds.

though the hit-list could begin at 200 kilobytes, it quickly shrinks to nothing during the partitioning. This provides a great benefit in constructing a quick worm by speeding the initial infection.

The hit-list needn't be perfect: a simple list of machines running a selected server sort could serve, though larger accuracy can improve the unfold. The hit-list itself is generated victimization one or many of the following techniques, ready well before, typically with very little concern of detection.

• Stealthy scans. Portscans are so common and then wide ignored that even a quick scan of the whole net would be unlikely to attract law enforcement attention or over gentle comment within the incident response community. However, for attackers wish to be particularly careful, a randomised sneaky scan taking many months would be not possible to attract much attention, as most intrusion detection systems are not currently capable of detecting such low-profile scans. Some portion of the scan would be out of date by the time it had been used, however abundant of it'd not.

• Distributed scanning. an assailant might scan the web using a few dozen to some thousand alreadycompromised "zombies," the same as what DDOS attackers assemble in a very fairly routine fashion. Such distributed scanning has already been seen within the wild–Lawrence Berkeley National Laboratory received ten throughout the past year.

• DNS searches. Assemble a list of domains (for example, by using wide offered spam mail lists, or trolling the address registries). The DNS will then be searched for the science addresses of mail-servers (via mx records) or net servers (by looking for www.domain.com).

• Spiders. For net server worms (like Code Red), use Web-crawling techniques the same as search engines so as to produce a list of most Internet-connected web sites. this would be unlikely to draw in serious attention.

• Public surveys. for many potential targets there may be surveys available listing them, like the Netcraft survey.

• Just listen. Some applications, like peer-to-peer networks, wind up advertising many of their servers. Similarly, many previous worms effectively broadcast that the infected machine is vulnerable to further attack. easy, because of its widespread scanning, during the Code Red I infection it was easy to select up the addresses of upwards of 300,000 vulnerable IIS servers–because each came knock on everyone's door!

QUESTION NO: 10

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB

B. 44EFCE164AB921CQAAD3B435B51404EE

C. 0182BD0BD4444BF836077A718CCDF409

D. CEC52EB9C8E3455DC2265B23734E0DAC

E. B757BF5C0D87772FAAD3B435B51404EE

F. E52CAC67419A9A224A3B108F3FA6CB6D

ANSWER: B E

Explanation:

LM (Lan Manager) hashes are often used for backward compatibility in older Windows systems. A password that is fewer than 8 characters long is padded with null bytes to increase the length to 8 characters before creating the hash. However, in the first part of the LM hash, the presence of a constant 'AAD3B435B51404EE' in the second half indicates it has been zero-padded due to the password not fully utilizing both blocks. Therefore, options B and E reflect passwords that are less than 8 characters long.

Microsoft Official Documentation on LM Hash

QUESTION NO: 11

What is a NULL scan?

A. A scan in which all flags are turned off

B. A scan in which certain flags are off

C. A scan in which all flags are on

D. A scan in which the packet size is set to zero

E. A scan with an illegal packet size

ANSWER: A

Explanation:

A NULL scan is a type of network scan that involves sending TCP packets with no flags set to a target host. This is done to identify open ports on the target system by analyzing the target's response or lack of response to the scan. Typically, if a port is closed, the target will respond with a TCP RST packet. If no response is received, it is likely that the port is open or filtered. NULL scans generally work on Unix-based systems and take advantage of differences in TCP/IP stack implementation. For more information, you can refer to the Nmap documentation on port scanning techniques.

QUESTION NO: 12

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MI

B. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB

B. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

WINS.MIB

MIB: Monitors and manages host resources
LNMIB2.MIB: Contains object types for workstation and server services

MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system
WINS.MIB: For the Windows Internet Name Service (WINS)

C. DHCP.MIS

D. MIB_II.MIB

ANSWER: A

Explanation:

Garry is accessing an MIB that contains object types for workstation and server services, which corresponds to the LNMIB2.MIB. This specific MIB includes descriptions and types used for managing and monitoring workstation and server service resources. Cisco Documentation on MIBs outlines how MIBs work in the scope of SNMP monitoring and management, providing insights into different MIB modules.

QUESTION NO: 13

Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service

C. A zone transfer passes all zone information that a DNS server maintains

D. A zone transfer passes all zone information that a nslookup server maintains

E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections

F. Zone transfers cannot occur on the Internet

ANSWER: A C E

Explanation:

A zone transfer is a type of DNS transaction in which a DNS server transfers a full or partial copy of its data to another DNS server. This process is typically done using TCP port 53. Ideally, zone transfers should be restricted to authorized servers to prevent unauthorized access to DNS data. Blocking inbound TCP port 53 connections can hinder unauthorized zone transfers. More details can be found in the official DNS documentation: Microsoft DNS Zone Transfer Security.

QUESTION NO: 14

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network.

What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.

B. Use a tool like ARPwatch to monitor for strange ARP activity.

C. Use a firewall between all LAN segments.

D. If you have a small network, use static ARP entries.

E. Use only static IP addresses on all PC's.

ANSWER: A B D

Explanation:

To prevent ARP spoofing or poisoning, network administrators can implement several strategies: 1. **Port Security**: Using port security features on switches helps to control access at the network switch port level. It restricts the MAC addresses allowed to connect to the network and provides security against rogue devices by limiting MAC address spoofing. 2. **Monitor ARP Activity**: Tools like ARPwatch can watch for changes in ARP traffic on a network and alert administrators when suspicious activity is detected. 3. **Static ARP Entries**: In smaller networks, using static ARP entries ensures that the IP address to MAC address mappings do not change, providing security against unsolicited ARP replies. More information can be found on Cisco's official site regarding network security and management practices.

QUESTION NO: 15

Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.

What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

ANSWER: C

Explanation:

TCP Maimon scan

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is

FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

https://nmap.org/book/scan-methods-maimon-scan.html

How Nmap interprets responses to a Maimon scan probe

Probe Response Assigned State

No response received (even after retransmissions) open|filtered

TCP RST packet closed

ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) filtered

QUESTION NO: 16

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens. Which of the following tools is used by Gregory in the above scenario?

A. Nmap

B. Burp Suite

C. CxSAST

D. Wireshark

ANSWER: B

Explanation:

Burp Suite is a comprehensive tool designed for testing web application security. It includes an intercepting proxy that allows penetration testers to manipulate and analyze the data transmitted between the server and the endpoint application. This capability makes it a popular choice for session hijacking and inspecting the randomness of session tokens. More information about Burp Suite can be found on the [official Burp Suite website](https://portswigger.net/burp).

QUESTION NO: 17

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

ANSWER: A B D

Explanation:

Windows LAN Manager (LM) hashes have several known weaknesses that make them susceptible to attacks. Firstly, passwords are converted to uppercase letters before being hashed, which reduces the keyspace and makes it easier for attackers to crack the passwords. Secondly, the hashes can be broken into two separate 7-character chunks, making the effective length 7 characters, which is easier to brute force compared to longer passwords. Additionally, although LM hashes

themselves may not be sent in clear text, they can be easily intercepted and reversed. Therefore, it is advisable to use more secure hashing methods like NTLMv2. More information can be found on the official Microsoft documentation.

QUESTION NO: 18

Which among the following is the best example of the hacking concept called "clearing tracks"?

A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.

B. During a cyberattack, a hacker injects a rootkit into a server.

C. An attacker gains access to a server through an exploitable vulnerability.

D. During a cyberattack, a hacker corrupts the event logs on all machines.

ANSWER: D

Explanation:

Clearing tracks refers to methods employed by hackers to erase evidence of their activities on a breached system. This typically involves deleting or altering log files that record activities on a computer or network, as these logs are crucial for forensic investigations to track unauthorized access. By corrupting event logs, a hacker aims to prevent law enforcement or security professionals from tracing their activities back to them. Learn more about hacking concepts on the official EC-Council site.

QUESTION NO: 19

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's accesslist as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool.

The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file

B. Run a network sniffer and capture the returned traffic with the configuration file from the router

C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

ANSWER: B D

QUESTION NO: 20

Richard, an attacker, targets an MNC In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

A. VPN footprinting

B. Email footprinting

C. VoIP footprinting

D. Whois footprinting

ANSWER: D

Explanation:

Whois footprinting is a technique used to gather domain-specific information including the domain name, contact details of the domain owner, and key dates like creation and expiration dates. This information is typically retrieved from the public domain registration records available through a service called Whois. This detailed domain information can be used in social engineering attacks to mislead domain owners and gain further network details. ICANN - gTLD Registration Data