DUMPSBOSS.

Certified Ethical Hacker Exam (CEHv13)

ECCouncil 312-50v13

Version Demo

Total Demo Questions: 20

Total Premium Questions: 572

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.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

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

A. WebSite Watcher

B. web-Stat

C. Webroot

D. WAFW00F

ANSWER: B

Explanation:

Web-Stat is a service that provides detailed analytics for tracking the geographical location, operating systems, browsers, and screen sizes of the website's visitors. It also offers real-time monitoring of visitor activity on websites, making it suitable for the scenario presented. Web-Stat Official Site.

QUESTION NO: 2

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

ANSWER: B

Explanation:

The scenario described in the question is best known as 'tailgating'. Tailgating, in a cybersecurity context, refers to when an unauthorized person gains access to a restricted area by following someone who is authorized, without the person's knowledge. This is a common social engineering technique. For more details, you can refer to official security guides or trusted cybersecurity resources such as CSO Online.

QUESTION NO: 3

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: 4

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data.

However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker alters his approach and injects a ‘DROP TABLE’ statement, a move that could potentially lead to the loss of vital data stored in the application's database

B. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure

C. The hacker switches tactics and resorts to a ‘time-based blind’ SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay

D. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries

ANSWER: D

Explanation:

The strategy the hacker is most likely to employ when faced with filtering of special characters is to bypass such filters by encoding his malicious input. This may involve using techniques such as URL encoding, hexadecimal encoding, or other methods that allow the malicious input to pass through the filter undetected. When the input is decoded and executed by the database, the SQL Injection can occur successfully. This technique allows the attacker to avoid detection and exploit the vulnerability in the application. For more on SQL Injection techniques and prevention, you can refer to the official OWASP page on SQL Injection.

QUESTION NO: 5

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: 6

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company. Which information security standard is most applicable to his role?

A. FISMA

B. HITECH

C. PCI-DSS

D. Sarbanes-OxleyAct

ANSWER: C

Explanation:

PCI-DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. This is particularly relevant to Bill's role, as he is working for a credit card company that must comply with these standards to protect cardholder data. For more information, you can refer to the official PCI Security Standards Council website.

QUESTION NO: 7

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: 8

What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. That the Joe account has a SID of 500

B. These commands demonstrate that the guest account has NOT been disabled

C. These commands demonstrate that the guest account has been disabled

D. That the true administrator is Joe

E. Issued alone, these commands prove nothing

ANSWER: D

Explanation:

The commands shown use utilities that deal with Microsoft Windows Security Identifiers (SIDs). The command 'user2sid \earth guest' provides the SID for the guest account on the domain 'EARTH'. The SID 'S-1-5-21-343818398-789336058-1343024091-501' indicates that this is a standard account, while the last number '501' is the RID for the Guest user account. The command 'sid2user 5 21 343818398 789336058 1343024091 500' translates a SID to a username, showing 'Name is Joe' and 'Domain is EARTH', indicating that the account with RID 500, which is conventionally the built-in administrator account RID, matches the username 'Joe'. This demonstrates that the true administrator account corresponds to Joe. Microsoft Documentation on SIDs

QUESTION NO: 9

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented without prior manager approval.

B. Monitor all traffic using the firewall rule until a manager can approve it.

C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.

D. Immediately roll back the firewall rule until a manager can approve it

ANSWER: D

Explanation:

In network security management, having proper approvals in place is crucial as firewall rules can have a significant impact on the security posture of the organization. If a firewall rule is implemented without approval, there could be security risks associated with it. Rolling back the rule until it gets the necessary approval ensures that only vetted and authorized changes are applied to the network. This preventative step helps avoid unauthorized access or potential security breaches. More information can be found in network security best practices as advocated by the SANS Institute.

QUESTION NO: 10

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: 11

".....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of

unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there."

Fill in the blank with appropriate choice.

A. Evil Twin Attack

B. Sinkhole Attack

C. Collision Attack

D. Signal Jamming Attack

ANSWER: A

Explanation:

An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims' sensitive details. Most often, the victims of such attacks are ordinary people like you and me. The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions. An evil twin access point can also be used in a phishing scam where victims connect to the evil twin and are lured to a phishing site to enter their sensitive data. Learn more.

QUESTION NO: 12

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: 13

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: 14

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITR

D. Create a disk image of a clean Windows installation

E. org for the latest list of CVE findings

ANSWER: B

Explanation:

Using a scan tool like Nessus is one of the best approaches for discovering vulnerabilities on a Windows-based computer because it is specifically designed to highlight known vulnerabilities, misconfigurations, and deviations from policy. Nessus uses updated vulnerability information and is widely used by network and security professionals. For further information on Nessus, please visit Tenable's Official Site for Nessus.

QUESTION NO: 15

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.srcport= = 514 && ip.src= = 192.168.0.99

B. tcp.srcport= = 514 && ip.src= = 192.168.150

C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99

D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

ANSWER: D

Explanation:

To capture the traffic from the Snort machine to the Kiwi Syslog machine, you should use a Wireshark display filter that focuses on the destination IP and port. Kiwi Syslog typically listens on port 514. Therefore the correct filter would be "tcp.dstport==514 && ip.dst==192.168.0.150". This filter will display all TCP packets destined for port 514 on the machine with IP address 192.168.0.150. For more details on Wireshark display filters, refer to the Wireshark Official Documentation.

QUESTION NO: 16

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: 17

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: 18

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: 19

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110

B. 135

C. 139

D. 161

E. 445

F. 1024

ANSWER: B C E

Explanation:

Ports 135, 139, and 445 are associated with NetBIOS and other Windows networking services. Port 135 is used for RPC (Remote Procedure Call) services, port 139 is used for NetBIOS Session (message block), and port 445 is used for SMB (Server Message Block) over TCP. Blocking these ports on the firewall can help prevent unauthorized NetBIOS traffic from passing through. You can find more information on these ports at the official Microsoft documentation: Microsoft Service Overview.

QUESTION NO: 20

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration

B. Investigation

C. Reconnaissance

D. Enumeration

ANSWER: C

Explanation:

Reconnaissance is the process of gathering information about a target, often the first step in the Cyber Kill Chain. It involves researching and collecting data about the organization to exploit in future attacks. More details can be found at Cyber Kill Chain by Lockheed Martin.