# DUMPSBOSS.COM

# Certified Ethical Hacker CEH v11

## ECCouncil CEH-v11

### Version Demo

### Total Demo Questions: 20

### Total Premium Questions: 528

### Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

dumpsboss.com

## QUESTION NO: 1

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

access-list 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: 2

is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

**A.** Spear phishing

**B.** Whaling

**C.** Vishing

**D.** Phishing

### ANSWER: B

## 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

## QUESTION NO: 4

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

## QUESTION NO: 5

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.

Which of the following IP addresses could be teased as a result of the new configuration?

**A.** 210.1.55.200

**B.** 10.1.4.254

**C.** 10.1.5.200

**D.** 10.1.4.156

ANSWER: C

## QUESTION NO: 6

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

**A.** Protocol analyzer

**B.** Network sniffer

**C.** Intrusion Prevention System (IPS)

**D.** Vulnerability scanner

**ANSWER: A**

## QUESTION NO: 7

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**

## QUESTION NO: 8

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**

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**

PGP, SSL, and IKE are all examples of which type of cryptography?

**A.** Digest

**B.** Secret Key

**C.** Public Key

**D.** Hash Algorithm

**ANSWER: C**

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**

## QUESTION NO: 12

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**

## QUESTION NO: 13

Which of the following is the primary objective of a rootkit?

**A.** It opens a port to provide an unauthorized service

**B.** It creates a buffer overflow

**C.** It replaces legitimate programs

**D.** It provides an undocumented opening in a program

**ANSWER: C**

## QUESTION NO: 14

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

**A.** Bluesmacking

**B.** BlueSniffing

**C.** Bluejacking

**D.** Bluesnarfing

ANSWER: C

## QUESTION NO: 15

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

## QUESTION NO: 16

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

**A.** There is no way to tell because a hash cannot be reversed

**B.** The right most portion of the hash is always the same

**C.** The hash always starts with AB923D

**D.** The left most portion of the hash is always the same

**E.** A portion of the hash will be all 0's

ANSWER: B

## QUESTION NO: 17

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**

## QUESTION NO: 18

A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

**A.** Place a front-end web server in a demilitarized zone that only handles external web traffic

**B.** Require all employees to change their anti-virus program with a new one

**C.** Move the financial data to another server on the same IP subnet

**D.** Issue new certificates to the web servers from the root certificate authority

**ANSWER: A**

## QUESTION NO: 19

what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

**A.** Decoy scanning

**B.** Packet fragmentation scanning

**C.** Spoof source address scanning

**D.** Idle scanning

> **ANSWER: D**

**Explanation:**

The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a "zombie".
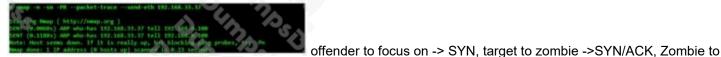
This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there's no interaction between the offender pc and also the target: the offender interacts solely with the "zombie" pc.

This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the "zombie" pc and distinction in behavior are often discovered mistreatment totally different|completely different "zombies" with proof of various privileges granted by the target to different computers.

The overall intention behind the idle scan is to "check the port standing whereas remaining utterly invisible to the targeted host."

The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.

Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence:

 offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1)

 currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender

-> RST (IPID increment by 1)

So, during this method IPID increments by a pair of finally.

When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another. Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you'll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it's best to raise permission before mistreatment someone's machines for surprising functions like idle scanning.

Simple network devices typically create nice zombies as a result of {they square measure|they're} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.

While distinguishing an acceptable zombie takes some initial work, you'll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor's man idle scanning.

## QUESTION NO: 20

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources. What is the framework used by James to conduct footprinting and reconnaissance activities?

**A.** WebSploit Framework

**B.** Browser Exploitation Framework

**C.** OSINT framework

**D.** SpeedPhish Framework

ANSWER: C