DUMPSBOSS.COM

CEH Certified Ethical Hacker (312-50v9)

ECCouncil 312-50

Version Demo

Total Demo Questions: 20

Total Premium Questions: 644

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

Topic Break Down

Topic	No. of Questions
Topic 1, Background	13
Topic 2, Analysis/Assessment	31
Topic 3, Security	61
Topic 4, Tools /Systems /Programs	74
Topic 5, Procedures/ Methodology	53
Topic 6, Regulations / Policy	10
Topic 7, Ethics	6
Topic 8, MIX QUESTIONS	396
Total	644

QUESTION NO: 1

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

A. It used TCP as the underlying protocol.

B. It uses community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. It is used by all network devices on the market.

ANSWER: B D

QUESTION NO: 2

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: 3

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. Intrusion Prevention System (IPS)

C. Network sniffer

D. Vulnerability scanner

ANSWER: A

Explanation:

A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

References: https://en.wikipedia.org/wiki/Packet_analyzer

QUESTION NO: 4

You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

A. Disable Key Services

B. Create User Account

C. Download and Install Netcat

D. Disable IPTables

ANSWER: B

QUESTION NO: 5

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Cavity virus

B. Polymorphic virus

C. Tunneling virus

D. Stealth virus

ANSWER: D

QUESTION NO: 6

Name two software tools used for OS guessing? (Choose two.)

A. Nmap

B. Snadboy

C. Queso

D. UserInfo

E. NetBus

ANSWER: A C

QUESTION NO: 7

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: 8

A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

A. Perform a dictionary attack.

B. Perform a brute force attack.

C. Perform an attack with a rainbow table.

D. Perform a hybrid attack.

ANSWER: C

QUESTION NO: 9

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

QUESTION NO: 10

A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

A. Intrusion Prevention System (IPS)

B. Vulnerability scanner

C. Protocol analyzer

D. Network sniffer

ANSWER: C

QUESTION NO: 11

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

ANSWER: B

QUESTION NO: 12

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: 13

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key

B. Receiver's private key

C. Receiver's public key

D. Sender's private key

ANSWER: D

QUESTION NO: 14

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: 15

What does a type 3 code 13 represent? (Choose two.)

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited

E. Port unreachable

F. Time exceeded

ANSWER: B D

QUESTION NO: 16

Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSEC

B. PEM

C. SET

D. PPP

ANSWER: A

QUESTION NO: 17

A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.

B. NMAP -P 192.168.0.0/16

C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0

D. NMAP -P 192.168.1/17

ANSWER: A

QUESTION NO: 18

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

A. False positive

B. False negative

C. True positve

D. True negative

ANSWER: A

QUESTION NO: 19

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

QUESTION NO: 20

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