EC-Council Certified Security Specialist (ECSS) v10

ECCouncil ECSS

Version Demo

Total Demo Questions: 15

Total Premium Questions: 337

Buy Premium PDF

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	93
Topic 2, Volume B	94
Topic 3, Volume C	150
Total	337

QUESTION NO: 1

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the preattack phase:

·Information gathering

·Determining network range

·Identifying active machines

·Finding open ports and applications

·OS fingerprinting

·Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

Each correct answer represents a complete solution. Choose all that apply.

A. Traceroute

B. NeoTrace

C. Cheops

D. Ettercap

ANSWER: A B C

QUESTION NO: 2

Andrew works as a Forensic Investigator for Passguide Inc. The company has a Windowsbased environment. The company's employees use Microsoft Outlook Express as their email client program. E-mails of some employees have been deleted due to a virus attack on the network.

Andrew is therefore assigned the task to recover the deleted mails. Which of the following tools can Andrew use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. FINALeMAIL

B. eMailTrackerPro

C. EventCombMT

D. R-mail

ANSWER: A D

QUESTION NO: 3

Fill in the blank with the appropriate name of the attack.

________ takes best advantage of an existing authenticated connection

A. session hijacking

ANSWER: A

QUESTION NO: 4

Which of the following is an example of a low-interaction production honeypot that is developed and sold by the Swiss company Netsec?

A. ManTrap

B. Specter

C. KFSensor

D. Honeyd

ANSWER: B

QUESTION NO: 5

Which of the following proxy servers is placed anonymously between the client and remote server and handles all of the traffic from the client?

A. Web proxy server

B. Caching proxy server

C. Open proxy server

D. Forced proxy server

ANSWER: D

QUESTION NO: 6

RRD Job World wants to upgrade its network. The company decides to implement a TCP/IP-based network. According to the case study, RRD Job World is concerned about security. Which of the following methods should the on-site employees use to communicate securely with the headquarters?

(Click the Exhibit button on the toolbar to see the case study.)

A. Basic (Clear Text) authentication using SSL

B. DNS security and group policies

C. L2TP over IPSec

D. Windows NT Challenge/Response (NTLM) authentication

ANSWER: A

QUESTION NO: 7

Adam works as a Security Analyst for Umbrella Inc. He is retrieving large amount of log data from syslog servers and network devices such as Router and switches. He is facing difficulty in analyzing the logs that he has retrieved. To solve this problem, Adam decides to use software called Sawmill. Which of the following statements are true about Sawmill?

Each correct answer represents a complete solution. Choose all that apply.

A. It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches & routers etc.), syslog servers etc.

B. It incorporates real-time reporting and real-time alerting.

C. It comes only as a software package for user deployment.

D. It is a software package for the statistical analysis and reporting of log files.

ANSWER: A B D

QUESTION NO: 8

Which of the following is an example of a social engineering attack?

A. Phishing

B. Man-in-the-middle attack

C. Browser Sniffing

D. E-mail bombing

ANSWER: A

QUESTION NO: 9

In which of the following complaint types does a fraudulent transaction take place?

A. Overpayment Fraud

B. FBI scams

C. Auction fraud

D. Computer damage

ANSWER: C

QUESTION NO: 10

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

A. 18 U.S.C. 2510

B. 18 U.S.C. 1362

C. 18 U.S.1030

D. 18 U.S.C. 2701

E. 18 U.S.C. 1029

ANSWER: B

QUESTION NO: 11

Which of the following statements are true about firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. Firewalking works on the UDP packets.

B. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

C. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.

D. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

ANSWER: B C D

QUESTION NO: 12

Which of the following commands is most useful for viewing large files in Linux?

A. less

B. cp

C. touch

D. cat

ANSWER: A

QUESTION NO: 13

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Web server logs

B. Event logs

C. System logs

D. Program logs

ANSWER: B C D

QUESTION NO: 14

You have been assigned the job of configuring wireless networks for a large company. The security of these networks is of great importance. One of the tools that you can use for applying security is Wireless Transport Layer Security (WTLS). What are the goals of using this tool?

Each correct answer represents a complete solution. Choose all that apply.

A. To provide authentication between the two end points

B. To provide data integrity

C. To provide privacy for the two end users

D. To provide data availability

ANSWER: A B C

QUESTION NO: 15

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Web server logs

B. Event logs

C. Program logs

D. System logs

ANSWER: B C D