Vendor:EC-COUNCIL

Exam Code:EC0-349

Exam Name: Computer Hacking Forensic Investigator

Version: Demo

QUESTION 1

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort

B. Snort

C. Ettercap

D. RaidSniff

Correct Answer: C

QUESTION 2

What does ICMP Type 3/Code 13 mean?

A. Host Unreachable

B. Administratively Blocked

C. Port Unreachable

D. Protocol Unreachable

Correct Answer: B

QUESTION 3

Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?

A. The 10th Amendment

B. The 5th Amendment

C. The 1st Amendment

D. The 4th Amendment

Correct Answer: D

QUESTION 4

George is a senior security analyst working for a state agency in Florida. His state\\'s congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

A. Signature-based anomaly detection

B. Pattern matching

C. Real-time anomaly detection

D. Statistical-based anomaly detection

Correct Answer: C

QUESTION 5

What is the following command trying to accomplish?

A. Verify that UDP port 445 is open for the 192.168.0.0 network

B. Verify that TCP port 445 is open for the 192.168.0.0 network

C. Verify that NETBIOS is running for the 192.168.0.0 network

D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: A

QUESTION 6

What does mactime, an essential part of the coroner\\'s toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is too specific to the MAC OS and forms a core component of the toolkit

Correct Answer: A

QUESTION 7

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in- house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company\\'s main office in Iowa. She states that she needs the receptionist\\'s network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation

B. Scarcity

C. Friendship/Liking

D. Reciprocation

Correct Answer: D

QUESTION 8

To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 143

B. 25

C. 110

D. 125

Correct Answer: C

QUESTION 9

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud

B. Nessus cannot perform wireless testing

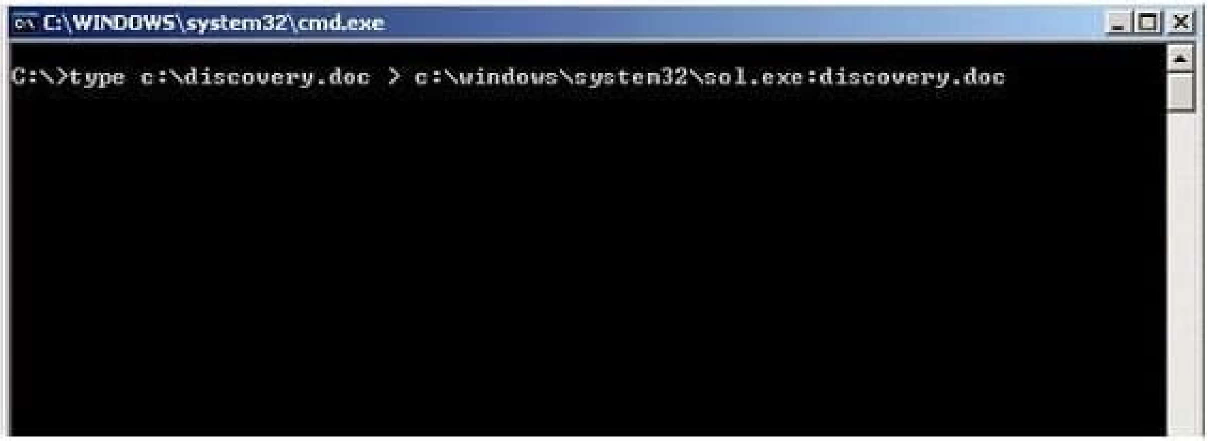
C. Nessus is not a network scanner

D. There are no ways of performing a "stealthy" wireless scan

Correct Answer: A

QUESTION 10

What feature of Windows is the following command trying to utilize?



```
C:\>type c:\discovery.doc > c:\windows\systen32\sol.exe:discovery.doc
```

A. White space

B. AFS

C. ADS

D. Slack file

Correct Answer: C

QUESTION 11

If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team

B. determine a way to obtain the suspect computer

C. assume the suspect machine is contaminated

D. do not enter alone

Correct Answer: A

QUESTION 12

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. One

B. Two

C. Three

D. Four

Correct Answer: B