Free Questions for CFR-210 by dumpshq

Shared by Roberts on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A system administrator needs to analyze a PCAP file on a Linux workstation where the use of GUI-based applications is restricted. Which of the following command line tools can the administrator use to analyze the PCAP?

Options:

A- nfdump

B- cryptcat

C- tshark

D- netstat

Answer:

A

Question 2

Question Type: MultipleChoice

A suspicious laptop is found in a datacenter. The laptop is on and processing data, although there is no application open on the screen. Which of the following BEST describes a Windows tool and technique that an investigator should use to analyze the laptop's RAM for working applications?

Options:

A- Net start and Network analysis

B- Regedit and Registry analysis

C- Task manager and Application analysis

D- Volatility and Memory analysis

Answer:

B

Question 3

Question Type: **MultipleChoice**

An incident responder is investigating a Linux server reported to be "behaving strangely". Which of the following commands should the incident responder use to identify any users currently logged into the system? (Choose two.)

Options:

A- lsof

B- ls

C- id

D- w

E- lastlog

Answer:

D

Question 4

Question Type: **MultipleChoice**

An organization needs to determine of any systems on its network (10.0.25.0/24) have web services running on port 80 or 443. Which of the following is the BEST command to do this?

Options:

A- netstat --p 80-443 10.0.25.0/24

B- nmap --v 80,443 10.0.25.0/24

C- netstat --v 80,443 10.0.25.0/24

D- nmap --p 80,443 10.0.25.0/24

Answer:

C

Question 5

Question Type: MultipleChoice

An attack was performed on a company's web server, disabling the company's website. The incident response team's investigation produced the following:

1. Presence of malicious code installed on employees' workstations.

2. Excessive UDP datagrams sent to a single address.

3. Web server received excessive UDP datagrams from multiple internal hosts.

4. Network experienced high traffic after 3:00 pm.

5. Employee workstations sent large traffic bursts when employees accessed the internal timecard application.

Which of the following BEST describes the attack tool used to perform the attack?

Options:

A- KeyLogger

B- Logic bomb

C- Nessus

D- Metasploit

Answer:

D

Question 6

Question Type: MultipleChoice

From a compromised system, an attacker bypasses a proxy server and sends a large amount of data to a remote location. A security analyst is tasked with finding the conduit that was used by the attacker to bypass the proxy. Which of the following Windows tools should be used to find the conduit?

Options:

A- net

B- fport

C- nbstat

D- netstat

Answer:

D

Question 7

Question Type: **MultipleChoice**

During a malware outbreak, a security analyst has been asked to capture network traffic in hourly increments for analysis by the incident response team. Which of the following tcpdump commands would generate hourly pcap files?

Options:

A- tcpdump --nn --i eth0 --w output.pcap --C 100 --W 10

B- tcpdump --nn --i eth0 --w output.pcap --W 24

C- tcpdump --nn --i eth0 --w output.pcap --G 3600 --W 14

D- tcpdump --nn --i eth0 --w output.pcap

Answer:

B

Question 8

Question Type: MultipleChoice

A file is discovered in the /etc directory of an internal server by an automated file integrity checker. A security analyst determines the file is a bash script. The contents are as follows:

#/bin/bash

```
IFS=:

[[-f/etc/passwd]] && cat/etc/passwd |

while read a b c d e f g

do

echo "$e ($a)"

done
```

Which of the following was the author of the script attempting to gather?

Options:

A- Home directory and shell

B- Username and password hash

C- User's name and username

D- UID and GID

Answer:

B