Free Questions for CFR-210 by braindumpscollection

Shared by Pollard on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A UNIX workstation has been compromised. The security analyst discovers high CPU usage during off-hours on the workstation. Which of the following UNIX programs can be used to detect the rogue process? (Choose two.)

Options:

A- arp

B- ps

C- who

D- dd

E- top

Answer:

C, E

Question 2

Question Type: MultipleChoice

An incident responder has captured packets associated with malware. The source port is 8765 and the destination port is 7653. Which of the following commands should be used on the source computer to help determine which program is responsible for the connection?

Options:

A- services.msc

B- psexec

C- msconfig

D- fport

Answer:

D

Question 3

Question Type: MultipleChoice

Which of the following resources BEST supports malware analysis?

Options:

A- Internet service providers

B- Government websites

C- Crowdsourced intelligence feed

D- Internal network management team

Answer:

C

Question 4

Question Type: MultipleChoice

An attacker has decided to attempt a brute force attack on a UNIX server. In order to accomplish this, which of the following steps must be performed?

Options:

A- Exfiltrate the shadow and SAM, run unshadow, and then runa password cracking utility on the output file.

B- Exfiltrate the shadow and passwd, and then run a password cracking utility on both files.

C- Exfiltrate the shadow and SAM, and then run a password cracking utility on both files.

D- Exfiltrate the shadowand passwd, run unshadow, and then run a password cracking utility on the output file.

Answer:

C

Question 5

Question Type: **MultipleChoice**

A malware analyst has been assigned the task of reverse engineering malicious code. To conduct the analysis safely, which of the following could the analyst implement?

Options:

A- Honeypot

B- VLAN

C- Lock box

D- Sandbox

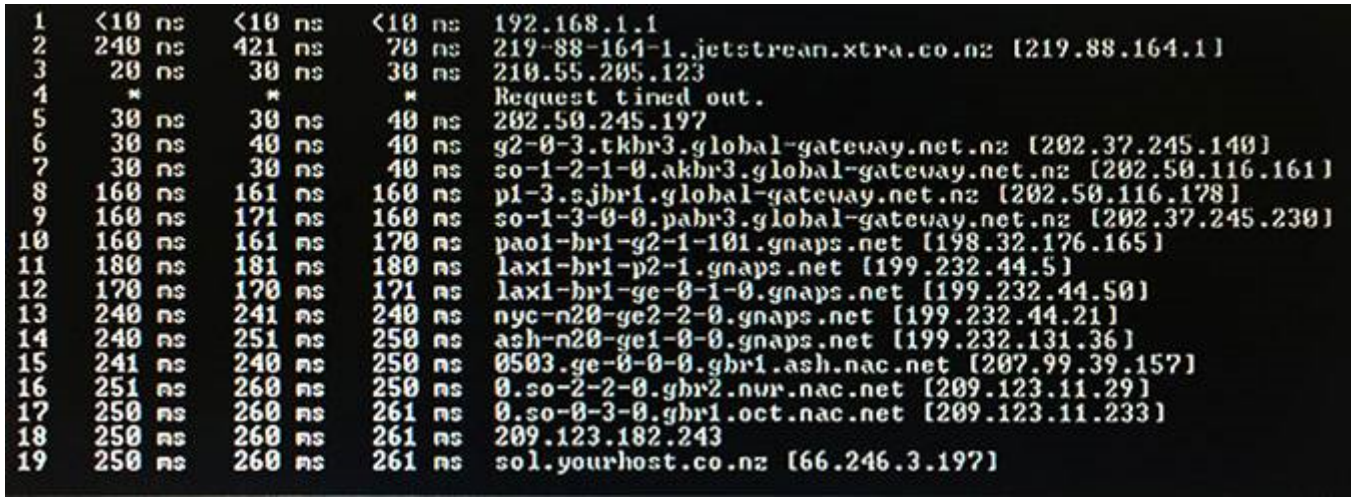
Answer:

D

Question 6

Question Type: MultipleChoice

Click the exhibit button. Which of the following Windows tools is executed?



Options:

A- nmap

B- netstat

C- tracert

D- traceroute

Answer:

D

Question 7

Question Type: **MultipleChoice**

While a network administrator is monitoring the company network, an unknown local IP address is starting to release high volumes of anonymous traffic to an unknown external IP address. Which of the following would indicate to the network administrator potential compromise?

Options:

A- Packet losses

B- Excessive bandwidth usage

C- Service disruption

D- Off-hours usage

Answer:

B

Question 8

Question Type: MultipleChoice

Malicious code that can replicate itself using various techniques is referred to as a:

Options:

A- downloader

B- rootkit

C- launcher

D- worm

Answer:

D

Question 9

Question Type: **MultipleChoice**

A company website was hacked via the SQL query below:

```
email, passwd, login_id, full_name
FROM members
WHERE email = "attacker@somewhere.com" ; DROP TABLE members;--"
```

Which of the following did the hackers perform?

Options:

A- Cleared tracks ofattacker@somewhere.comentries

B- Deleted the entirememberstable

C- Deleted the email password and login details

D- Performed an XSS attack

Answer:

D