Free Questions for CFR-210 by dumpssheet

Shared by Alexander on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

To redact or obfuscate sensitive data, a company requires its name be changed throughout a port-incident report. Using a Linux sed command, which of the following will replace the company's name with "Acme"?

Options:

A- /Orange/Acme/g

B- s/Acme/Orange/g

C- /Acme/Orange/g

D- s/Orange/Acme/g

Answer:

D

Question 2

Question Type: MultipleChoice

An incident responder suspects that a host behind a firewall is infected with malware. Which of the following should the responder use to find the IP address of the infected machine?

Options:

A- NAT table

B- ARP cache

C- DNS cache

D- CAM cable

Answer:

C

Question 3

Question Type: MultipleChoice

When investigating a wireless attack, which of the following can be obtained from the DHCP server?

Options:

A- MAC address of the attacker

B- Operating system of the attacker

C- IP traffic between the attacker and victim

D- Effectiveness of the VLAN terminator

Answer:

A

Question 4

Question Type: **MultipleChoice**

An unauthorized network scan may be detected by parsing network sniffer data for:

Options:

A- IPtraffic from a single IP address to multiple IP addresses.

B- IP traffic from a single IP address to a single IP address.

C- IP traffic from multiple IP addresses to a single IP address.

D- IP traffic from multiple IP addresses to other networks.

Answer:

A

Question 5

Question Type: MultipleChoice

Customers are reporting issues connecting to a company's Internet server. Which of the following device logs should a technician review in order to help identify the issue?

Options:

A- WIPS

B- SSH

C- WAP

D- WAF

Answer:

A

Question 6

Question Type: MultipleChoice

Which of the following is the BEST way to capture all network traffic between hosts on a segmented network?

Options:

A- HIPS

B- Firewall

C- Router

D- Protocol analyzer

Answer:

A

Question 7

Question Type: MultipleChoice

A SOC analyst has been tasked with checking all files in every employee home directory for any mention of a new product code named PitViper. Which of the following commands will return all requested data?

Options:

A- grep --i "pitviper" /home

B- grep --r "PitViper" /home

C- grep --r --v "pitviper" /home

D- grep --r --i "pitviper" /home

Answer:

A

Question 8

Question Type: MultipleChoice

An attacker has sent malicious macro-enabled Office files. Which of the following regular expressions will return a list of macro-enabled files?

Options:

A- ^.*?\.(?:xls|ppt|doc)m

B- ^.*(?:xls|ppt|doc)m.*

C- ^.*?\.(?:xls|ppt|doc)m$

D- ^.*(?:xls|ppt|doc)m

Answer:

B

Question 9

Question Type: MultipleChoice

An incident responder needs to quickly locate specific data in a large data repository. Which of the following Linux tool should be used?

Options:

A- cat

B- find

C- grep

D- man

Answer:

C

Question 10

Question Type: **MultipleChoice**

A security analyst would like to parse through several SQL logs for indicators of compromise. The analyst is aware that none of the fields should contain a string of text longer than 30 characters; however, the analyst is unaware if there are any implemented controls to prevent such an overflow. Which of the following BEST describes the regular expression the analyst should use to find any alphanumeric character string?

Options:

A- /^[a-zA-Z0-9]{5,30}$/

B- /^[a-zA-Z-9]{30}$/

C- /^[a-zA-Z]{5,30}$/

D- /^[a-Z0-9]{5,30}$/

Answer:

A