Free Questions for CFR-210 by actualtestdumps

Shared by Patrick on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following types of logs is shown below, and what can be discerned from its contents?

2015-07-19 12:33:31 reject UDP 146.64.21.212 192.141.173.72 1234 80

2015-07-19 12:33:31 reject UDP 166.32.22.12 192.141.173.72 1234 80

2015-07-19 12:33:31 reject UDP 123.56.71.145 192.141.173.72 1234 80

2015-07-19 12:33:31 reject UDP 146.64.21.212 192.141.173.72 1234 80

2015-07-19 12:33:32 reject UDP 166.32.22.12 192.141.173.72 1234 80

2015-07-19 12:33:32 reject UDP 123.56.71.145 192.141.173.72 1234 80

2015-07-19 12:33:32 reject UDP 146.64.21.212 192.141.173.72 1234 80

2015-07-19 12:33:33 reject UDP 166.32.22.12 192.141.173.72 1234 80

2015-07-19 12:33:33 reject UDP 123.56.71.145 192.141.173.72 1234 80

2015-07-19 12:33:33 reject UDP 146.64.21.212 192.141.173.72 1234 80

2015-07-19 12:33:34 reject UDP 166.32.22.12 192.141.173.72 1234 80

2015-07-19 12:33:34 reject UDP 123.56.71.145 192.141.173.72 1234 80

2015-07-19 12:33:34 reject UDP 146.64.21.212 192.141.173.72 1234 80

2015-07-19 12:33:35 reject UDP 166.32.22.12 192.141.173.72 1234 80

2015-07-19 12:33:35 reject UDP 123.56.71.145 192.141.173.72 1234 80

Options:

A- Firewall log showing a possible web server attack

B- Proxy log showing a possible DoS attack

C- Firewall log showing a possible DoS attack

D- Proxy log showing a possible web server attack

Answer:

C

Question 2

Question Type: **MultipleChoice**

A DMZ web server has been compromised. During the log review, the incident responder wants to parse all common internal Class A addresses from the log. Which of the following commands should the responder use to accomplish this?

Options:

A- grep --x"(10.[0-9]+.[0-9]+.[0-9]+)" etc/rc.d/apache2/access.log | output.txt

B- grep --x"(192.168.[0.9]+[0-9])" bin/apache2/access.log | output.txt

C- grep --v"(10.[0-9]+.[0-9]+.[0-9]+)" /var/log/apache2/access.log > output.txt

D- grep --v"(192.168.[0.9]+[0-9]+)" /var/log/apache2/access.log > output.txt

Answer:

C

Question 3

Question Type: **MultipleChoice**

An incident responder notices many entries in an apache access log file that contain semicolons. Which of the following attacks is MOST likely being attempted?

Options:

A- SQL injection

B- Remote file inclusion

C- Account brute force

D- Cross-site scripting

Answer:

A

Question 4

Question Type: **MultipleChoice**

An analyst would like to search for a specific text string at the beginning of a line that begins with four capital alphabetic characters. Which of the following search operators should be used?

Options:

A- /\b\w{4}\b

B- /\b[A-Z]{4}\g

C- /^\w{4}\b

D- /B[A-Z]{4}\b\g

Answer:

B

Question 5

Question Type: MultipleChoice

A network engineer has collected a packet capture using Wireshark and given it to the team for analysis. The team is looking for activity based on the internal IP address of 10.0.25.123. Which of the following filters should the team use to look at only traffic for this IP?

Options:

A- source.ip == 10.0.25.123 && destination.ip == 10.0.25.123

B- source tcp = 10.0.25.123 and destination tcp = 10.0.25.123

C- src.ip == 10.0.25.123 or dst.ip == 10.0.25.123

D- src.ip = 10.0.25.123 or dst.ip = 10.0.25.123

Answer:

D

Question 6

Question Type: MultipleChoice

Why is it important to update system clocks from a single time source?

Options:

A- For backup data timestamps

B- To ensure device data integrity

C- For log data correlation

D- To assist in network data packet capture

Answer:

B

Question 7

Question Type: MultipleChoice

An organization's firewall has recently been bombarded with an excessive amount of failed requests. A security analyst has been tasked with providing metrics on any failed attempts to ports above 1000. Which of the following regular expressions will work BEST to identify an IP address with the desired port range?

Options:

A- /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):({4,5}\d+)\b/

B- /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([4]\D+)\b/

C- /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([4]\d+)\b/

D- /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):(\d{1,5})\b/

Answer:

C

Question 8

Question Type: MultipleChoice

An incident responder is asked to work with the IT department to address patch management issues with the company servers. Which of the following is the BEST source for the incident responder to obtain the CVEs for the latest industry-recognized patches?

Options:

A- Vulnerabilities database

B- Intelligence feeds

C- Security journals

D- Security blogs

Answer:

A

Question 9

Question Type: MultipleChoice

The above Linux command is used to search for:

Options:

A- MAC addresses.

B- memory addresses.

C- IPv4 addresses.

D- IPv6 addresses.

Answer:

A

Question 10

Question Type: **MultipleChoice**

An alert on user account activity outside of normal business hours returns Windows even IDs 540 and 4624. In which of the following locations will these events be found?

Options:

A- Application event log

B- System event log

C- Setup event log

D- Security event log

Answer:

D

Question 11

Question Type: **MultipleChoice**

Which of the following commands should be used to print out ONLY the second column of items in the following file?

Source_File,txt

Alpha Whiskey

Bravo Tango

Charlie Foxtrot

Echo Oscar

Delta Roger

Options:

A- cut --d " " --f2 source_file.txt

B- cut --b7-15 source_file.txt

C- cut --d " " --f2 Source_File.txt

D- cut --c6-12 Source_File.txt

Answer:

D

Question 12

Question Type: **MultipleChoice**

During a network-based attack, which of the following data sources will provide the BEST data to quickly determine the attacker's point of origin? (Choose two.)

Options:

A- DNS logs

B- System logs

C- WIPS logs

D- Firewall logs

E- IDS/IPS logs

Answer:

A, D