210-255 Q&As

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/210-255.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which evidence is considered to be the most volatile?

A. disk

B. registers and cache

C. removable media

D. logging

Correct Answer: D

QUESTION 2

Which file system has share and file permissions?

A. NTFS

B. FAT

C. TMPFS

D. Streams

Correct Answer: A

QUESTION 3

What can be addressed when using retrospective security techniques?

A. if the affected host needs a software update

B. what system are affected

C. if the affected system needs replacement

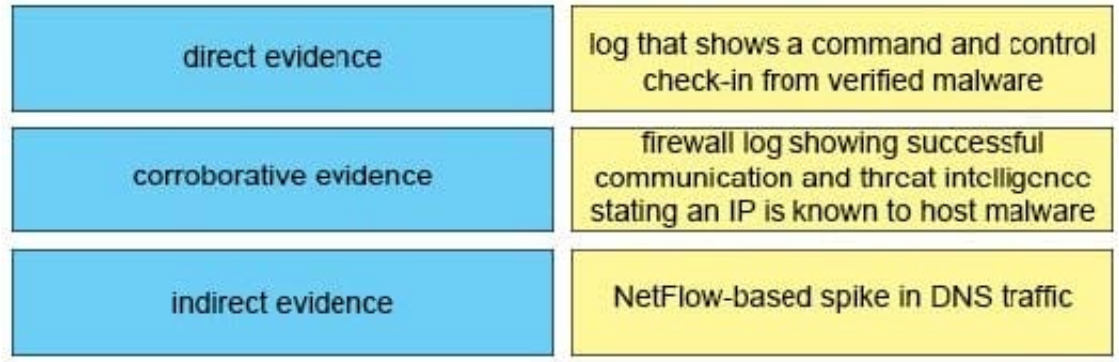
D. why the malware is still in our network

Correct Answer: D

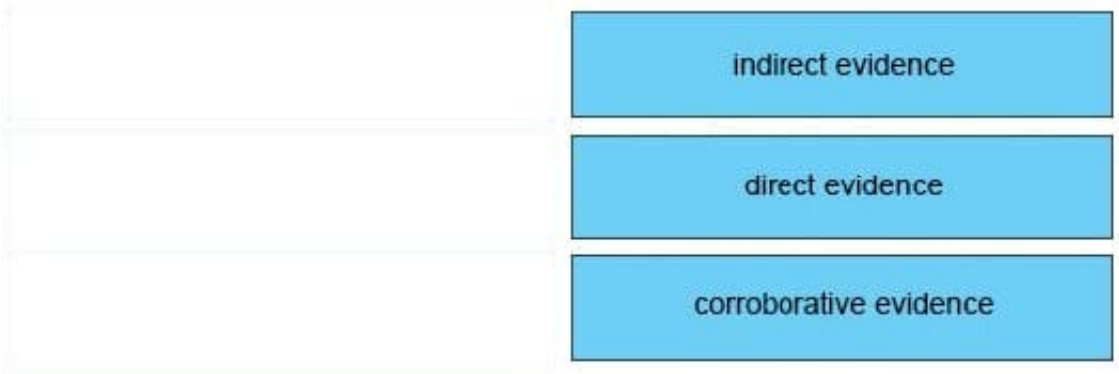
QUESTION 4

Drag and drop the type of evidence from the left onto the correct descnption(s) of that evidence on the right.

Select and Place:



Correct Answer:



QUESTION 5

When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?

A. HTTPS traffic

B. TCP traffic

C. HTTP traffic

D. UDP traffic

Correct Answer: D

QUESTION 6

Which regular expression matches "color" and "colour"?

A. col[0-9]+our

B. colo?ur

C. colou?r

D.]a-z]{7}

Correct Answer: C

QUESTION 7

Refer to the exhibit. Which item is depicted in this output?

```
Description: Nc Such Agency Collector
Destination: 10.255.255.100
Destination UDP Port 2055
Source Interface Vlan10 (10.10.10.5)
Export Version 5
Exporter Statistics
    Number of Flow Records Exported 726
    Number of Templates Exported 1
    Number of Export Packets Sent 37
    Number of Export Bytes Sent 38712
    Number of Destination Unreachable Events 0
    Number of No Buffer Events 0
    Number of Packets Dropped (No Route to Host) 0
    Number of Packets Dropped (other) 0
    Number of Packets Dropped (LC to RP Error) 0
    Number of Packets Dropped (Output Drops) 0
    Time Statistics were last cleared: Thu Mar 5 21:12:06 2018
```

A. Windows Security audit log

B. NetFlow data

C. packet capture exported text

D. VLAN 10 traffic

Correct Answer: B

QUESTION 8

Which option filters a LibPCAP capture that used a host as a gateway?

A. tcp|udp] [src|dst] port

B. [src|dst] net [{mask }|{len }]

C. ether [src|dst] host

D. gateway host

Correct Answer: D

QUESTION 9

Which of the following steps in the kill chain would come before the others?

A. C2

B. Delivery

C. Installation

D. Exploitation

Correct Answer: B

QUESTION 10

Which CVSS Attach Vector metric value means that the vulnerable component is not bound to the network stack and the path of the attacker is via read/write/execute capabilities?

A. network

B. physical

C. local

D. adjacent

Correct Answer: C

Reference: https://www.first.org/cvss/specification-document

QUESTION 11

Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( http://nmap.org ) at 2018-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH  7.2p2  Ubuntu  4ubintu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp  open   smtp    Postfix  smtpd
110/tcp open   pop3    Dovecat  pop3d
143/tcp open   imap    Dovecat  imapd
Service Info:  Host:   172.18.108.139; OS: Linux; CPE: cpe:/o:linux:|linux_kernel
```

What does the output indicate about the server with IP address 172.18.104.139?

A. open port of an FTP server

B. open ports of a web server

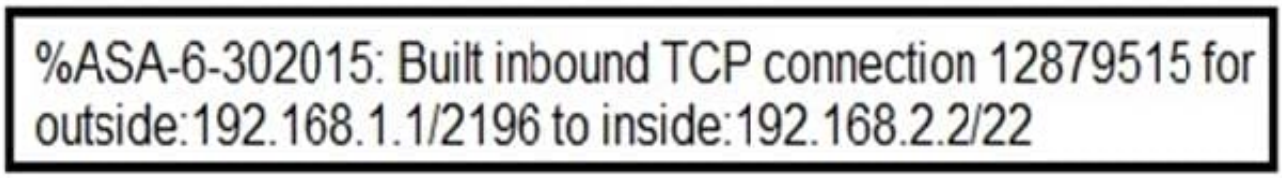
C. running processes of the server

D. open ports of an email server

Correct Answer: D

QUESTION 12

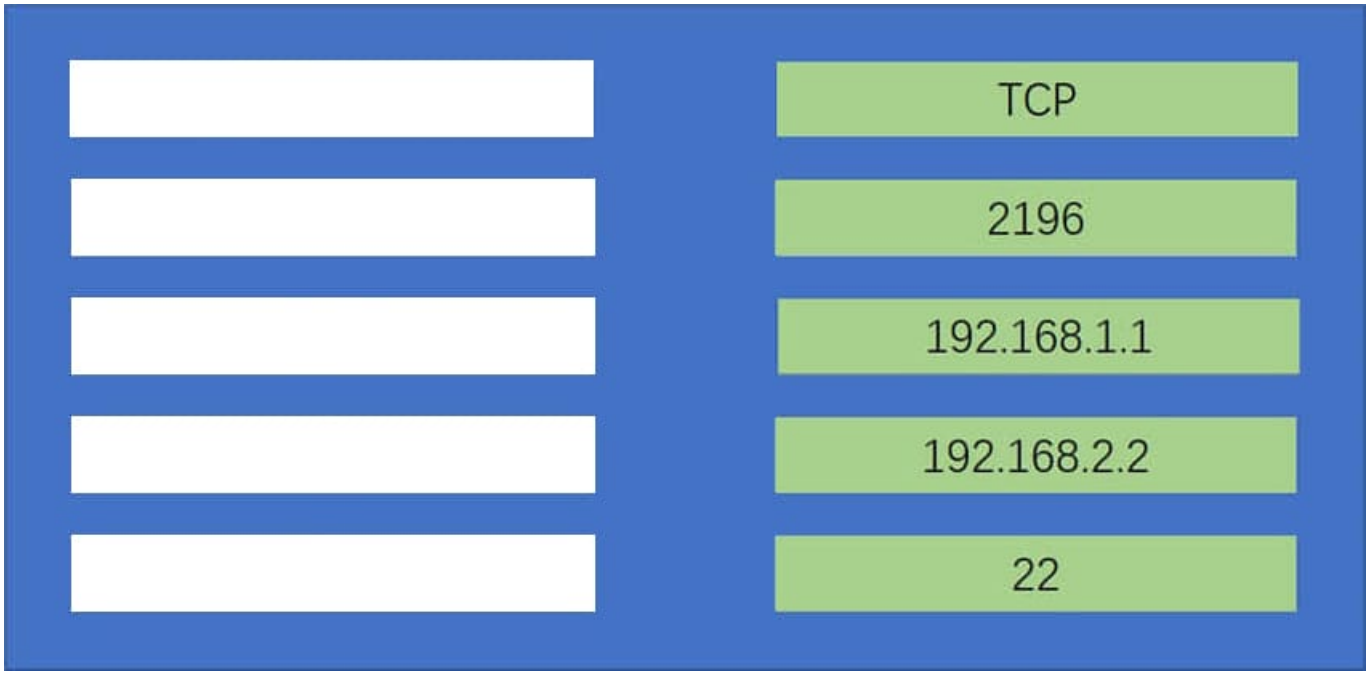
DRAG DROP



Refer to the exhibit. Drag and drop the items from the left onto the correct 5-tuple on the right.

Select and Place:

Correct Answer:



QUESTION 13

From a security perspective, why is it important to employ a clock synchronization protocol on a network?

A. so that everyone knows the local time

B. to ensure employees adhere to work schedule

C. to construct an accurate timeline of events when responding to an incident

D. to guarantee that updates are pushed out according to schedule

Correct Answer: C

QUESTION 14

You see 100 HTTP GET and POST requests for various pages on one of your webservers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. delivery

B. reconnaissance

C. action on objectives

D. installation

E. exploitation

Correct Answer: D

QUESTION 15

What is the definition of availability accord to CVSSv3 framework?

A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.

B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.

C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

Correct Answer: C