200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals
(CBROPS)

QUESTION 1

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. known-plaintext

B. replay

C. dictionary

D. man-in-the-middle

Correct Answer: D

QUESTION 2

Which type of access control depends on the job function of the user?

A. discretionary access control

B. nondiscretionary access control

C. role-based access control

D. rule-based access control

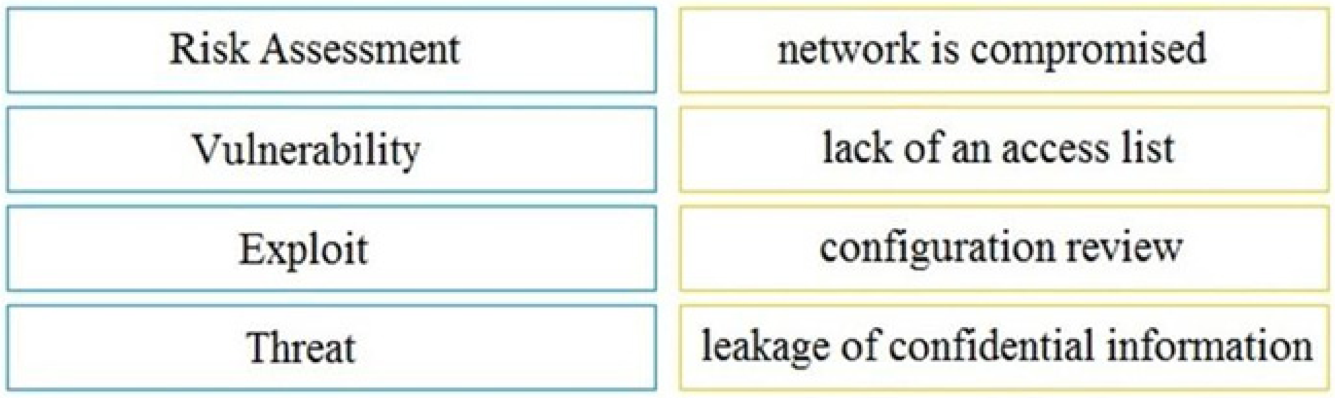
Correct Answer: C

QUESTION 3

DRAG DROP

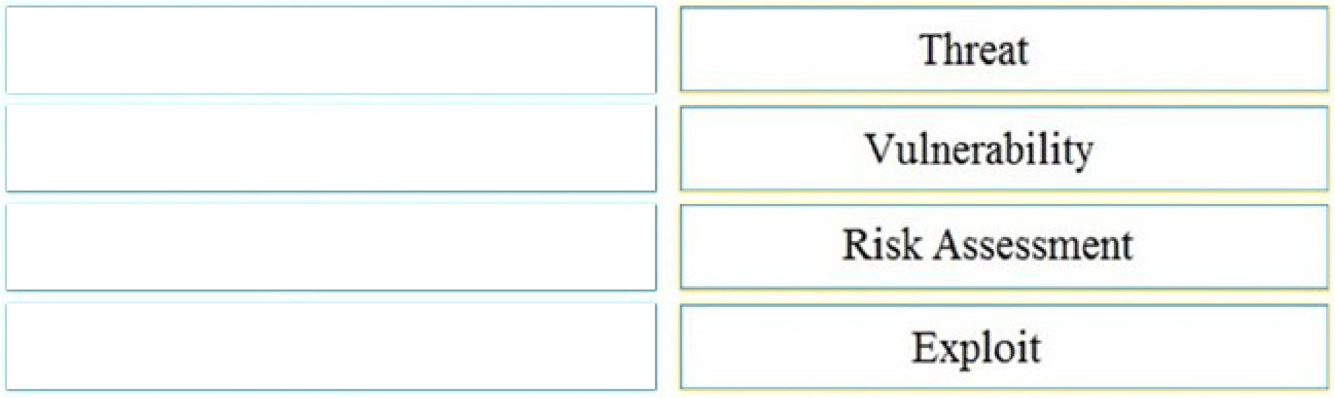
Drag and drop the security concept on the left onto the example of that concept on the right.

Select and Place:



Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

Correct Answer:



	Threat
	Vulnerability
	Risk Assessment
	Exploit

QUESTION 4

A company encountered a breach on its web servers using IIS 7 5 Dunng the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1 2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

A. Upgrade to TLS v1 3.

B. Install the latest IIS version.

C. Downgrade to TLS 1.1.

D. Deploy an intrusion detection system

Correct Answer: A

QUESTION 5

A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

A. total throughput on the interface of the router and NetFlow records

B. output of routing protocol authentication failures and ports used

C. running processes on the applications and their total network usage

D. deep packet captures of each application flow and duration

Correct Answer: A

QUESTION 6

What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive data

B. package deliberately sent to the wrong receiver to advertise a new product

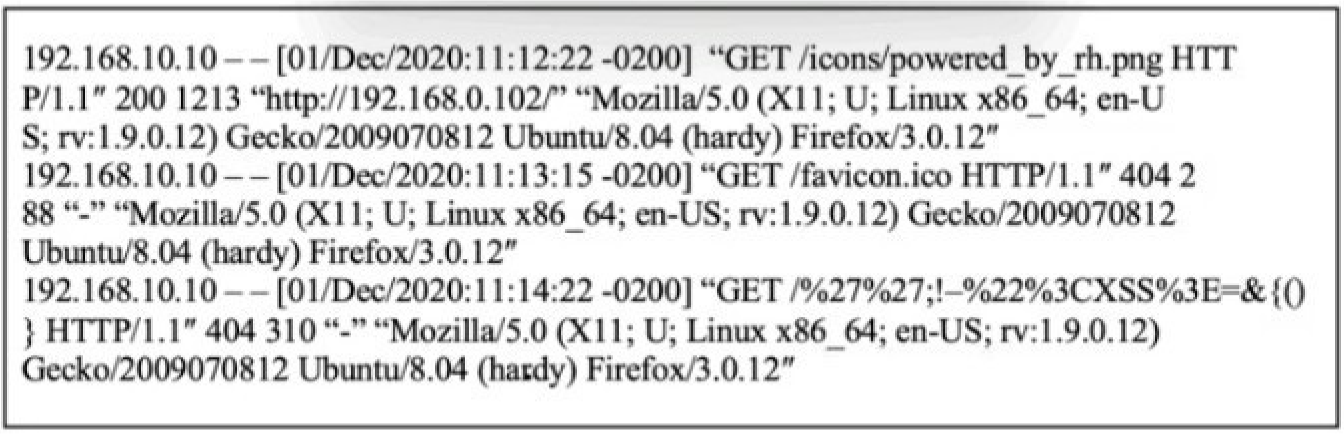
C. mistakenly received valuable order destined for another person and hidden on purpose

D. email offering last-minute deals on various vacations around the world with a due date and a counter

Correct Answer: D

QUESTION 7

Refer to the exhibit.



```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200]  "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 2
88 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812
Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!–%22%3CXSS%3E=&{()
} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

What is occurring?

A. Cross-Site Scripting attack

B. XML External Entitles attack

C. Insecure Deserialization

D. Regular GET requests

Correct Answer: A

QUESTION 8

Which type of data is used to monitor and detect anomalies within the organization\\'s network?

A. statistical

B. metadata

C. transaction

D. alert

Correct Answer: A

QUESTION 9

What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete

B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete

C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection

D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Correct Answer: D

QUESTION 10

What is email greylisting by the mail transfer agent?

A. denying any email from a sender it does not recognize

B. returning emails that are potential phishing attempts

C. allowing emails from unknown senders temporarily

D. quarantining emails sent from outside of the organization

Correct Answer: A

QUESTION 11

Which tool provides a full packet capture from network traffic?

A. Nagios

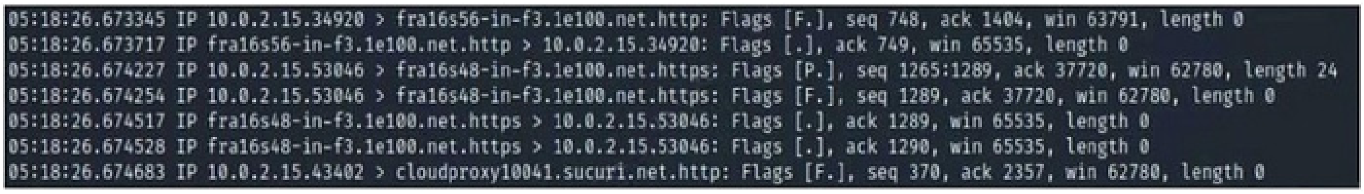
B. CAINE

C. Hydra

D. Wireshark

Correct Answer: D

QUESTION 12



```
05:18:26.673345 IP 10.0.2.15.34920 > fra16s56-in-f3.1e100.net.http: Flags [F.], seq 748, ack 1404, win 63791, length 0
05:18:26.673717 IP fra16s56-in-f3.1e100.net.http > 10.0.2.15.34920: Flags [.], ack 749, win 65535, length 0
05:18:26.674227 IP 10.0.2.15.53046 > fra16s48-in-f3.1e100.net.https: Flags [P.], seq 1265:1289, ack 37720, win 62780, length 24
05:18:26.674254 IP 10.0.2.15.53046 > fra16s48-in-f3.1e100.net.https: Flags [F.], seq 1289, ack 37720, win 62780, length 0
05:18:26.674517 IP fra16s48-in-f3.1e100.net.https > 10.0.2.15.53046: Flags [.], ack 1289, win 65535, length 0
05:18:26.674528 IP fra16s48-in-f3.1e100.net.https > 10.0.2.15.53046: Flags [.], ack 1290, win 65535, length 0
05:18:26.674683 IP 10.0.2.15.43402 > cloudproxy10041.sucuri.net.http: Flags [F.], seq 370, ack 2357, win 62780, length 0
```

What can be identified from the exhibit?

A. NetFlow data

B. spoofed TCP reset packets

C. DNS hijacking

D. tcpdump data

Correct Answer: D

QUESTION 13

What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated

B. Data is accessible and available to permitted individuals

C. Data is unaltered and its integrity is preserved

D. Data is secure and unreadable without decrypting it

Correct Answer: D

QUESTION 14

What does the Zero Trust security model signify?

A. Zero Trust security means that no one is trusted by default from inside or outside the network.

B. Zero Trust addresses access control and states that an individual should have only the minimum access privileges necessary to perform specific tasks.

C. Zero Trust states that no users should be given enough privileges to misuse the system on their own.

D. Zero Trust states that unless a subject is given explicit access to an object, it should be denied access to that object.

Correct Answer: A

QUESTION 15

What is the difference between the ACK flag and the RST flag?

A. The RST flag approves the connection, and the ACK flag terminates spontaneous connections.

B. The ACK flag confirms the received segment, and the RST flag terminates the connection.

C. The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent

D. The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake

Correct Answer: B