200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.pass4itsure.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is a difference between a threat and a risk?

A. A threat can be people, property, or information, and risk is a probability by which these threats may bring harm to the business.

B. A risk is a flaw or hole in security, and a threat is what is being used against that flaw.

C. A risk is an intersection between threat and vulnerabilities, and a threat is what a security engineer is trying to protect against.

D. A threat is a sum of risks, and a risk itself represents a specific danger toward the asset.

Correct Answer: C

QUESTION 2

A network engineer noticed in the NetFlow report that internal hosts are sending many DNS requests to external DNS servers. A SOC analyst checked the endpoints and discovered that they are infected and became part of the botnet. Endpoints are sending multiple DNS requests, but with spoofed IP addresses of valid external sources. What kind of attack are infected endpoints involved in?

A. DNS tunneling

B. DNS hijacking

C. DNS amplification

D. DNS flooding

Correct Answer: C

QUESTION 3

How does an SSL certificate impact security between the client and the server?

A. by enabling an authenticated channel between the client and the server

B. by creating an integrated channel between the client and the server

C. by enabling an authorized channel between the client and the server

D. by creating an encrypted channel between the client and the server

Correct Answer: D

QUESTION 4

How does rule-based detection differ from behavioral detection?

A. Rule-based systems have predefined patterns, and behavioral systems learn the patterns that are specific to the environment.

B. Rule-based systems search for patterns linked to specific types of attacks, and behavioral systems identify attacks per signature.

C. Behavioral systems have patterns are for complex environments, and rule-based systems can be used on low-mid-sized businesses.

D. Behavioral systems find sequences that match particular attack behaviors, and rule-based systems identify potential zero-day attacks.

Correct Answer: A

QUESTION 5

What is data encapsulation?

A. Data is encrypted backwards, which makes it unusable.

B. Multiple hosts can be supported with only a few public IP addresses.

C. A protocol of the sending host adds additional data to the packet header.

D. Browsing history is erased automatically with every session.

Correct Answer: C

QUESTION 6

Which information must an organization use to understand the threats currently targeting the organization?

A. threat intelligence

B. risk scores

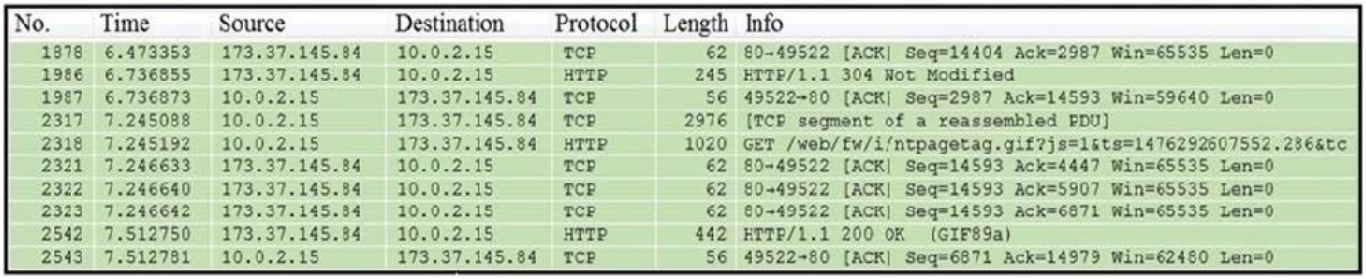
C. vendor suggestions

D. vulnerability exposure

Correct Answer: A

QUESTION 7

Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=1476292607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 2317

B. 1986

C. 2318

D. 2542

Correct Answer: D

QUESTION 8

A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

A. application identification number

B. active process identification number

C. runtime identification number

D. process identification number

Correct Answer: D

QUESTION 9

Endpoint logs indicate that a machine has obtained an unusual gateway address and unusual DNS servers via DHCP. Which type of attack is occurring?

A. evasion methods

B. phishing

C. man in the middle attack

D. command injection

Correct Answer: C

QUESTION 10

Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis

B. preparation

C. eradication

D. containment

Correct Answer: A

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity

Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).

Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

QUESTION 11

An engineer is investigating a case of the unauthorized usage of the "Tcpdump" tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?

A. tagged protocols being used on the network

B. all firewall alerts and resulting mitigations

C. tagged ports being used on the network

D. all information and data within the datagram

Correct Answer: D

QUESTION 12

Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web

application?

A. Hypertext Transfer Protocol

B. SSL Certificate

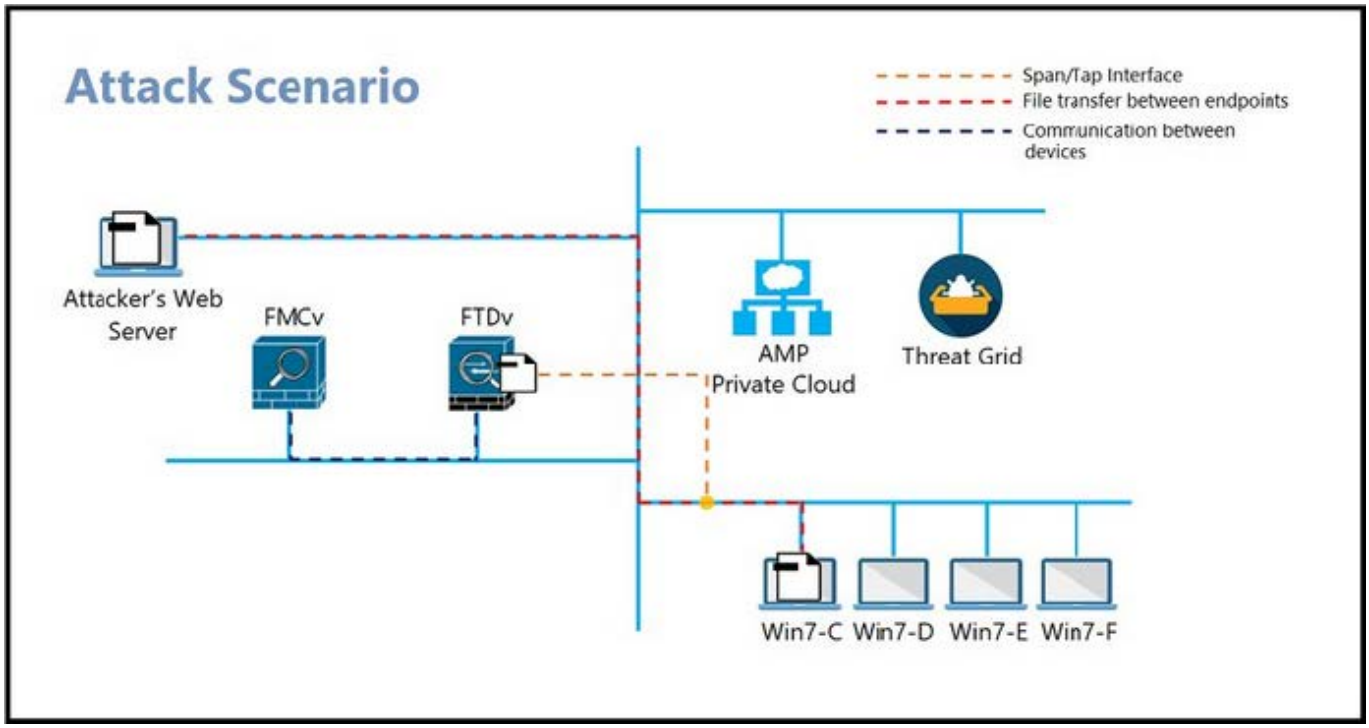
C. Tunneling

D. VPN

Correct Answer: B

QUESTION 13

Refer to the exhibit.



A workstation downloads a malicious docx file from the Internet and a copy is sent to FTDv. The FTDv sends the file hash to FMC and the tile event is recorded What would have occurred with stronger data visibility?

A. The traffic would have been monitored at any segment in the network.

B. Malicious traffic would have been blocked on multiple devices

C. An extra level of security would have been in place

D. Detailed information about the data in real time would have been provided

Correct Answer: D