DUMPSARENA

Understanding Cisco Cybersecurity Fundamentals

Cisco 210-250

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1138

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following are characteristics of next-generation firewalls and the Cisco Firepower Management Center (FMC) in relation to incident management? (Choose all that apply.)

A. They provide a list of separate things, such as hosts, applications, email addresses, and services, that are authorized to be installed or active on a system in accordance with a predetermined baseline.

B. These platforms support an incident lifecycle, allowing you to change an incident's status as you progress through your response to an attack.

C. You can create your own event classifications and then apply them in a way that best describes th e vulnerabilities on your network.

D. You cannot create your own event classifications and then apply them in a way that best describes the vulnerabilities on your network

ANSWER: B C

QUESTION NO: 2

What is the difference between spear phishing and whaling?

A. There is no difference. Both are targeted phishing.

B. Spear phishing focuses on voice services and whaling is primarily sent through SMS messages.

C. Both are targeted phishing, but only whaling targets individuals in executive positions.

D. Spear phishing involves email, and whaling involves DNS cache poisoning.

ANSWER: C

QUESTION NO: 3

Which port access control technology allows dynamic authorization policy to be downloaded from the authentication server?

A. VLAN map

B. Port security

C. 802.1x

D. MAC access list

ANSWER: C

QUESTION NO: 4

Which two fields are within an X.509v3 and entity certificate? (Choose two.)

A. revocation authority for use when the certificate expires

B. digital signature

C. public key associated with the certificate authority

D. public key associated with the subject

E. private key associated with the certificate authority

ANSWER: B D

QUESTION NO: 5

What is the Security Group Tag Exchange (SXP) protocol used for?

A. To transmit SGT to the egress point for enforcement

B. To send SGT information to a hardware-capable Cisco TrustSec device for tagging

C. To send SGT information from the authentication server to the authenticator

D. To send SGT information to the supplicant

ANSWER: B

QUESTION NO: 6

Which two of the following statements best describe the reasons that web proxy logs are important? (Choose two.)

A. Web proxy logs can show the activity of CnC bot traffic or evidence of dropper files.

B. Web proxy logs can only show legitimate HTTP traffic.

C. Web proxy devices such as the Cisco WSA can decrypt HTTPS traffic and enter it into the log for review later.

D. Web proxies TCP_HIT log messages can identify DoS attacks.

ANSWER: A C

QUESTION NO: 7 - (DRAG DROP)

DRAG DROP

Put the following SSH connection steps in order:

Select and Place:

The client sends the encrypted session key to the server. The server decrypts the session key using its private key. At this point, both the client and the server have the shared session key. That key is non-available to any other systems. From this point on the session between the client and server is encrypted using a symmetric encryption algorithm	1
The client and server negotiate the security transforms. The two sides agree to a mutually supported symmetric encryption algorithm. This negotiation occurs in the clear. A party that intercepts the communication will be aware of the encryption algorithm that is agreed upon	2
With privacy in place, user authentication ensues. The user's credentials and all other data are protected.	3
The client constructs a session key of the appropriate length to support the agreed-upon encryption algorithm. The client encrypts the session key. Only the server has the appropriate private key that can decrypt the session key.	4
The client connects to the server and the server presents the client with its public key	5

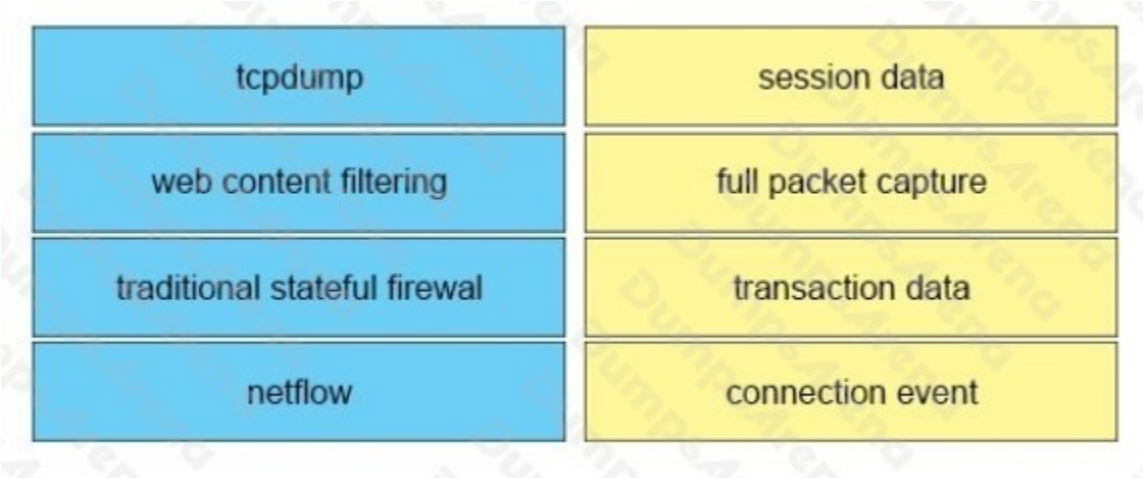
ANSWER:

QUESTION NO: 8 - (DRAG DROP)

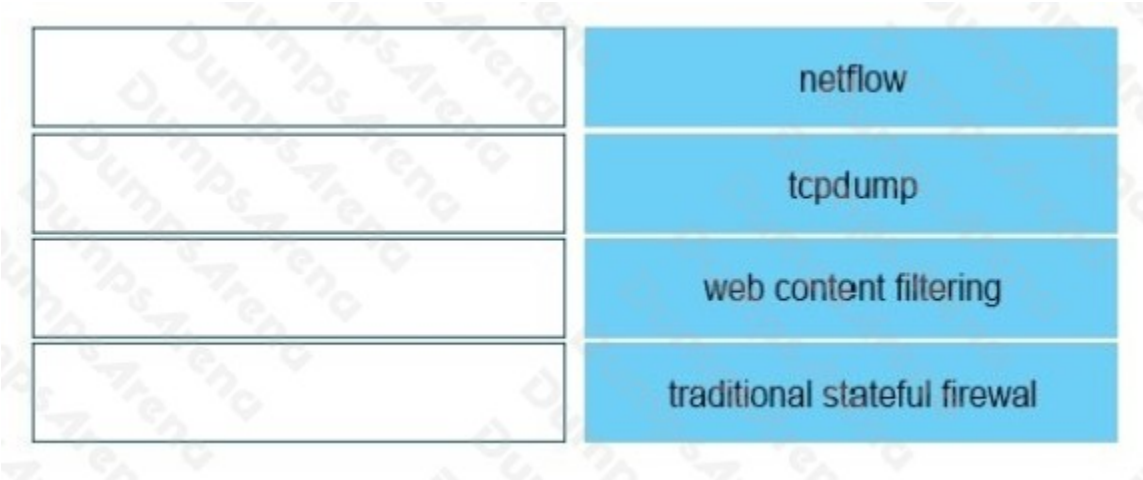
DRAG DROP

Drag the technology on the left to the data type the technology provides on the right.

Select and Place:



ANSWER:



QUESTION NO: 9

What are two data items that an analyst can learn about a data exfiltration alarm by using Cisco Stealthwatch? (Choose two.)

A. application or protocol that is used to transfer the data

B. IP address to which data was sent

C. names of files that were transferred

D. the signature that triggered the alarm

ANSWER: A B

QUESTION NO: 10

How can the established keyword in an ACL entry be used?

A. to permit only the returning TCP packets from an already existing TCP connection, and deny the initial TCP packet of a new session from an untrusted network

B. to permit both the initial TCP packet of a new session and the returning TCP packets from an existing TCP connection

C. to permit only the initial TCP packet of a new session

D. to change a router into a true stateful firewall controlling the access on a session-by-session basis

ANSWER: A

QUESTION NO: 11

What is one method of understanding how malware operates?

A. deep packet analysis

B. review logging data

C. compare attacks with known techniques

D. reverse engineer software

ANSWER: D

QUESTION NO: 12

What input validation can a program perform to prevent buffer overflow attacks?

A. Data input size matches what system has allocated.

B. User has administrative rights to install programs.

C. whether the input was downloaded from the Internet

D. Data input is not from a command line argument.

ANSWER: A

QUESTION NO: 13

Where does the RADIUS exchange happen?

A. Between the user and the network access server

B. Between the network access server and the authentication server

C. Between the user and the authentication server

D. None of the above

ANSWER: B

QUESTION NO: 14

Which three of the following statements best describe the limitations of network taps? (Choose three.)

A. Separate Rx and Tx make it difficult to determine which side of the connection sent the traffic.

B. Taps that are inserted at the physical layer can impact the performance on the inserted link.

C. Taps are unable to filter traffic.

D. Separating Rx and Tx requires multiple NICs to capture both sides of the connection.

E. Taps are expensive.

ANSWER: C D E

QUESTION NO: 15

Which term represents a weakness in a system that could lead to the system being compromised?

A. vulnerability

B. threat

C. exploit

D. risk

ANSWER: A

QUESTION NO: 16

Which of the following are reasons why an attacker might use VPN technology?

A. Attackers cannot use VPN technologies without being detected.

B. To exfiltrate data.

C. To encrypt traffic between a compromised host and a command and control system.

D. To evade detection.

ANSWER: B C D

QUESTION NO: 17

Which three are DNS vulnerabilities? (Choose three.)

A. DNS cache poisoning attacks

B. DNS resolution interception

C. DNS amplification and reflection attacks

D. TCP SYN flood

E. DNS resource utilization attacks

ANSWER: A C E

QUESTION NO: 18

Which Windows registry hive would be used to track the history of USB storage devices?

A. HKEY_LOCAL_MACHINE (HKLM)

B. HKEY_CURRENT_USER (HKCU)

C. HKEY_CLASSES_ROOT (HKCR)

D. HKEY_CURRENT_CONFIG (HKCC)

ANSWER: A

QUESTION NO: 19

Which three are valid HTTP request methods? (Choose three.)

A. GET

B. QUIT

C. PUT

D. HEAD

E. FETCH

ANSWER: A C D

QUESTION NO: 20

Which three types of traffic do a security analyst need to be aware of, because the traffic might be botnet command and control (C&C) traffic? (Choose three.)

A. P2P

B. DNS

C. SNMP

D. RCMP

E. IRC

F. RTMP

ANSWER: A B E

Explanation:

The correct answers are “P2P,” “DNS,” and “IRC.” P2P, DNS, and IRC are used to tunnel data out of a network.