210-250 Q&As

Understanding Cisco Cybersecurity Fundamentals

Pass Cisco 210-250 Exam with 100% Guarantee

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

https://www.geekcert.com/210-250.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

which options is true when using the traffic mirror feature in a switch

A. Ethernet headers are modified

B. packets payloads are lost

C. packets are not processed

D. full capture is possible

Correct Answer: D

QUESTION 2

Which definition describes the purpose of a Security Information and Event Management?

A. a database that collects and categorizes indicators of compromise to evaluate and search for potential security threats

B. a monitoring interface that manages firewall access control lists for duplicate firewall filtering

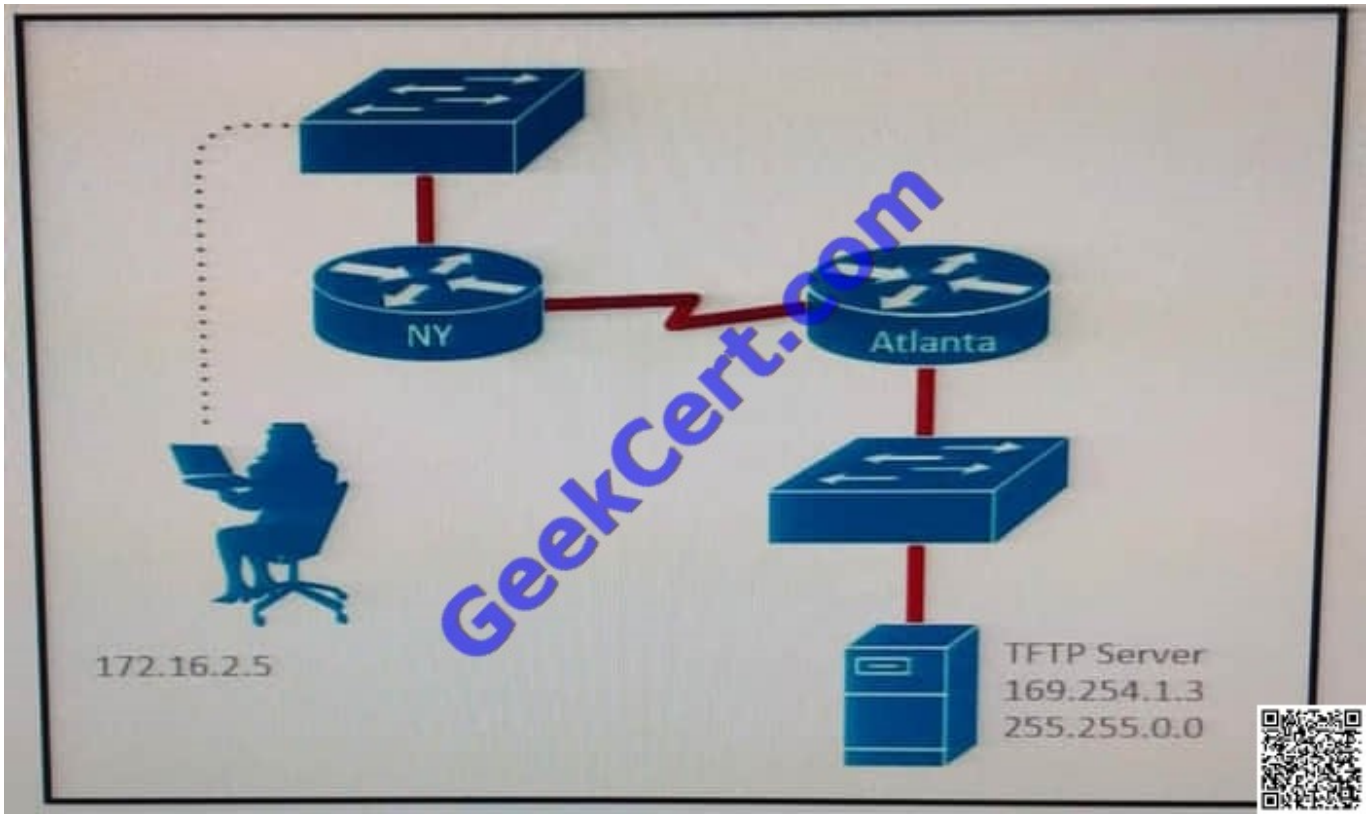
C. a relay server or device that collects then forwards event logs to another log collection device

D. a security product that collects, normalizes, and correlates event log data to provide holistic views of the security posture

Correct Answer: D

QUESTION 3

Refer to the exhibit.



A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has attempted to make a connection to the TFTP server. They are unable to back up the configuration file and Cisco IOS

of the NY router to the TFTP server.

Which cause of this problem is true?

A. The TFTP server cannot obtain an address from a DHCP Server.

B. The TFTP server has an incorrect IP address.

C. The network administrator computer has an incorrect IP address

D. The TFTP server has an incorrect subnet mask.

Correct Answer: A

QUESTION 4

Which of the following are metrics that can measure the effectiveness of a runbook?

A. Mean time to repair (MTTR)

B. Mean time between failures (MTBF)

C. Mean time to discover a security incident

D. All of the above

Correct Answer: D

QUESTION 5

Which type of exploit normally requires the culprit to have prior access to the target system?

A. local exploit

B. denial of service

C. system vulnerability

D. remote exploit

Correct Answer: A

QUESTION 6

Which three fields are within an X.509v3 end entity certificate? (Choose three).

A. Private Key associated with the certificate authority

B. Digital signature

C. Public key associated with the certificate authority

D. Public key associated with the subject

E. Basic constraints

F. Revocation authority for use when the certificate expires

Correct Answer: BDE

QUESTION 7

One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. Confidentiality, Integrity, and Availability

B. Confidentiality, Identity, and Availability

C. Confidentiality, Integrity, and Authorization

D. Confidentiality, Identity, and Authorization

Correct Answer: A

QUESTION 8

You get an alert on your desktop computer showing that an attack was successful on the host but up on investigation you see that occurred duration the attack. Which reason is true?

A. The computer has HIDS installed on it

B. The computer has NIDS installed on it

C. The computer has HIPS installed on it

D. The computer has NIPS installed on it

Correct Answer: A

QUESTION 9

After a large influx of network traffic to externally facing devices, you begin investigating what appear to be a denial of service attack. When you review packets capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

A. SYN flood.

B. Host porfiling.

C. Traffic fragmentation.

D. Port scanning.

Correct Answer: D

QUESTION 10

Which vulnerability is an example of Shellshock?

A. SQL injection

B. heap Overflow

C. cross site scripting

D. command injection

Correct Answer: D

QUESTION 11

Which cryptographic key is contained in an X.509 certificate?

A. symmetric

B. public

C. private

D. asymmetric

Correct Answer: B

QUESTION 12

What are the advantages of a full-duplex transmission mode compared to half-duplex mode? (Select all that apply.)

A. Each station can transmit and receive at the same time.

B. It avoids collisions.

C. It makes use of back off time.

D. It uses a collision avoidance algorithm to transmit.

Correct Answer: AB

QUESTION 13

Which protocol is expected to have NTP a user agent, host, and referrer headers in a packet capture?

A. NTP

B. HTTP

C. DNS

D. SSH

Correct Answer: B

QUESTION 14

Where are configuration records stored?

A. In a CMDB

B. In a MySQL DB

C. In a XLS file

D. There is no need to store them

Correct Answer: A

QUESTION 15

Which protocol is primarily supported by the third layer of the Open Systems Interconnection reference model?

A. HTTP/TLS

B. IPv4/IPv6

C. TCP/UDP

D. ATM/ MPLS

Correct Answer: B

QUESTION 16

Which two activities are examples of social engineering? (Choose two)

A. receiving call from the IT department asking you to verify your username/password to maintain the account

B. receiving an invite to your department\\'s weekly WebEx meeting B.

C. sending a verbal request to an administrator to change the password to the account of a user the

D. administrator does know

E. receiving an email from MR requesting that you visit the secure HR website and update your contract information

Correct Answer: AC

QUESTION 17

What Does the sum of the risk presented by an application represent for that application ?

A. Security violation

B. Application Attack Surface

C. HIPPA violation

D. Vulnerability

Correct Answer: B

QUESTION 18

Which of the following are public key standards?

A. IPSEC

B. PKCS #10

C. PKCS #12

D. ISO33012

E. AES

Correct Answer: BC

QUESTION 19

Which hash algorithm is the weakest?

A. SHA-512

B. RSA 4096

C. SHA-1

D. SHA-256

Correct Answer: C

QUESTION 20

What event types does FMC record?

A. standard common event logs types

B. successful login event logs

C. N/A

Correct Answer: C

QUESTION 21

For which kind of attack does an attacker use known information in encrypted files to break the encryption scheme for the rest of the file

A. known-plaintext

B. known-ciphertext

C. unknown key

D. man in the middle

Correct Answer: A

QUESTION 22

Which definition of the virtual address space for a Windows process is true?

A. actual physical location of an object in memory

B. set of virtual memory addresses that it can use

C. set of pages that are currently resident in physical memory

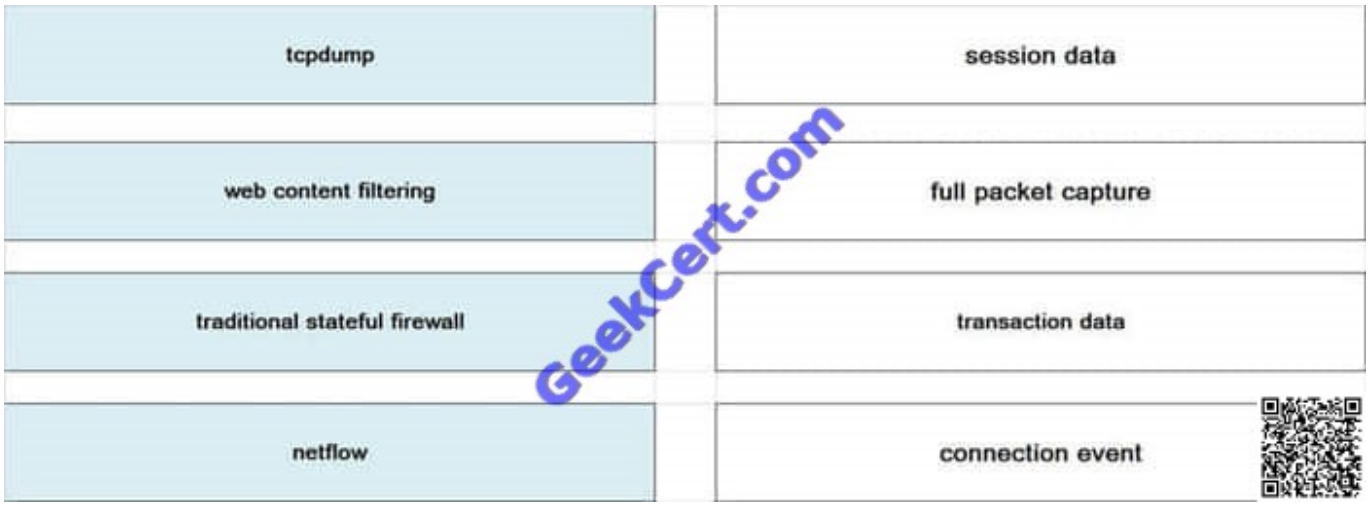
D. system-level memory protection feature that is built into the operating system

Correct Answer: B

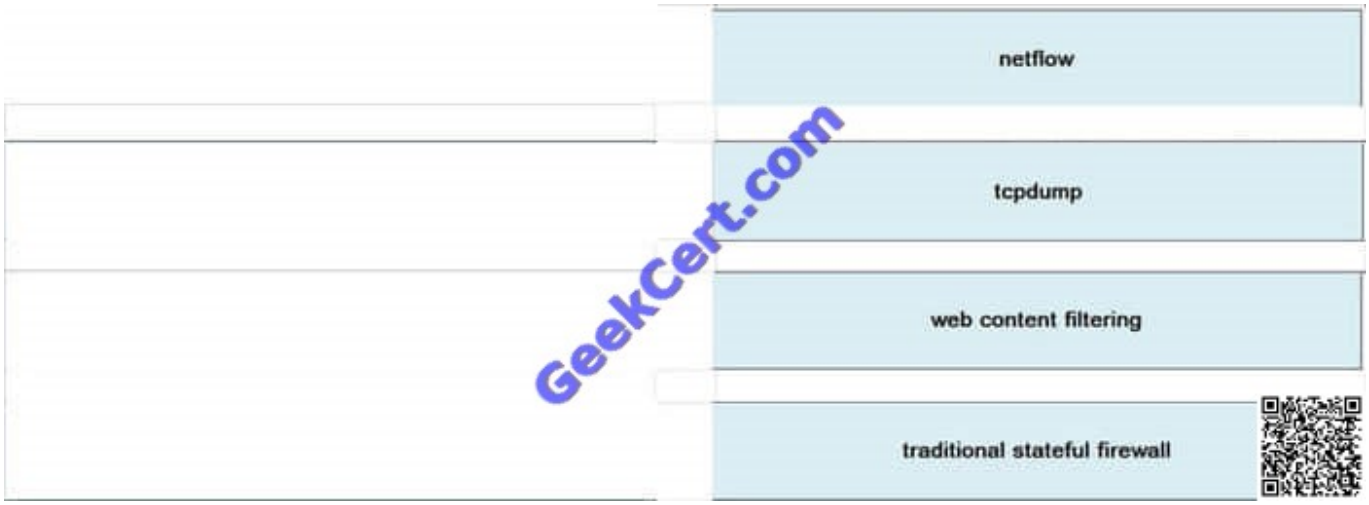
QUESTION 23

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

Select and Place:



Correct Answer:



QUESTION 24

A user reports difficulties accessing certain external web pages, when examining traffic to and from the external domain in full packet captures, you notice many SYNs that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?

A. insufficient network resources

B. failure of full packet capture solution

C. misconfiguration of web filter

D. TCP injection

Correct Answer: D

QUESTION 25

Netflow uses which format?

A. base 10

B. ASCII

C. Binary

D. Hexadecimal

Correct Answer: C

QUESTION 26

Which two terms are types of cross site scripting attacks? (Choose two)

A. directed

B. encoded

C. stored

D. reflected

E. cascaded

Correct Answer: CD

QUESTION 27

DNS query uses which protocol

A. TCP

B. UDP

C. HTTP

D. ICMP

Correct Answer: B

QUESTION 28

According to the common vulnerability scoring system, which term is associated with scoring multiple vulnerabilities that are exploit in the course of a single attack?

A. chained score

B. risk analysis

C. Vulnerability chaining

D. Confidentiality

Correct Answer: C

QUESTION 29

Which purpose of the certificate revocation list is true?

A. Provide a list of certificates that are trusted regardless of other validity makers.

B. Provide a list of certificates used in the chain of trust

C. Provide a list of alternate device identifiers.

D. Provide a list of certificates of certificates that are untrusted regardless of other validity makers.

Correct Answer: D

QUESTION 30

According to the attribute-based access control (ABAC) model, what is the subject location considered?

A. Part of the environmental attributes

B. Part of the object attributes

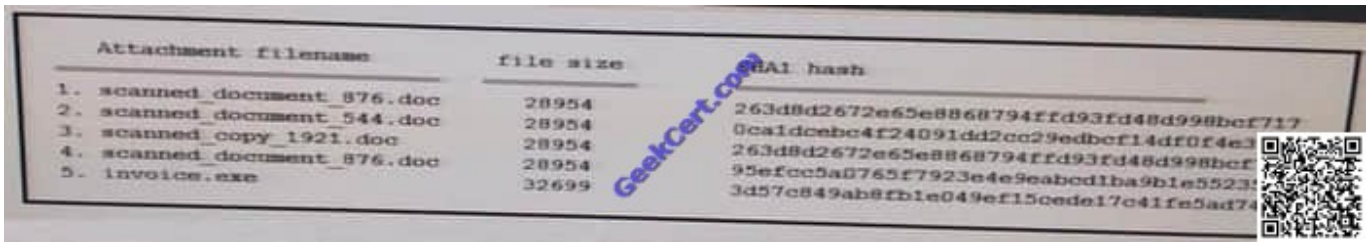
C. Part of the access control attributes

D. None of the above

Correct Answer: A

QUESTION 31

Refer to the exhibit.



During an analysis this list of email attachments is found. Which files contain the same content?

A. 1 and 4

B. 3 and 4

C. 1 and 3

D. 1 and 2

Correct Answer: C

QUESTION 32

Which Statement about personal firewalls is true?

A. They are resilient against kernel attacks

B. They can protect email messages and private documents in a similar way to a VPN

C. They can protect the network against attacks

D. They can protect a system by denying probing requests

Correct Answer: D

QUESTION 33

Where is a host-based intrusion detection system located?

A. on a particular end-point as an agent or a desktop application

B. on a dedicated proxy server monitoring egress traffic

C. on a span switch port

D. on a tap switch port

Correct Answer: A

QUESTION 34

Which three options are types of Layer 2 network attack? (Choose three.)

A. ARP attacks

B. brute force attacks

C. spoofing attacks

D. DDOS attacks

E. VLAN hopping

F. botnet attacks

Correct Answer: ACE

QUESTION 35

What does the sum of the risks presented by an application represent for that application?

A. Application attack surface

B. Security violation

C. Vulnerability

D. HIPPA violation

Correct Answer: A

QUESTION 36

An attacker installs a rogue switch that sends superior BPDUs on your network.

What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.

B. The switch could become the root bridge.

C. The switch could be allowed to join the VTP domain

D. The switch could become a transparent bridge.

Correct Answer: B

QUESTION 37

Which Linux terminal command can be used to display all the processes?

A. ps –ef

B. ps –u

C. ps –d

D. ps –m

Correct Answer: A

QUESTION 38

Which security principle states that more than one person is required to perform a critical task?

A. due diligence

B. separation of duties

C. need to know

D. least privilege

Correct Answer: B

QUESTION 39

In which context is it inappropriate to use a hash algorithm?

A. Telnet logins

B. Verifying file integrity

C. SSH logins

D. Digital signature verification

Correct Answer: A

QUESTION 40

Which hashing algorithm is the least secure?

A. MD5

B. RC4

C. SHA-3

D. SHA-2

Correct Answer: A