

100% Money Back
Guarantee

Vendor:Cisco

Exam Code:350-701

Exam Name:Implementing and Operating Cisco
Security Core Technologies (SCOR)

Version:Demo

QUESTION 1

What is provided by the Secure Hash Algorithm in a VPN?

- A. integrity
- B. key exchange
- C. encryption
- D. authentication

Correct Answer: A

Reference: <https://www.ciscopress.com/articles/article.asp?p=24833andseqNum=4>

QUESTION 2

DRAG DROP

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

Select and Place:

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Clearer pictures and no water-mask in the Premium Product	one-to-many PortScan, an attacker against one or a few hosts to scan one or multiple ports

Correct Answer:



Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting_specific_threats.html

QUESTION 3

Refer to the exhibit.

```
snmp-server group SNMP v3 auth access
15
```

What does the number 15 represent in this configuration?

- A. privilege level for an authorized user to this router
- B. access list that identifies the SNMP devices that can access the router
- C. interval in seconds between SNMPv3 authentication attempts
- D. number of possible failed attempts until the SNMPv3 user is locked out

Correct Answer: B

The syntax of this command is shown below: `snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]] [read read-view] [write write-view] [notify notify-view] [access access-list]` The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

QUESTION 4

What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

- A. Multiple NetFlow collectors are supported

- B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
- C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
- D. Flow-create events are delayed

Correct Answer: B

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.pdf>

QUESTION 5

Which security solution protects users leveraging DNS-layer security?

- A. Cisco ISE
- B. Cisco FTD
- C. Cisco Umbrella
- D. Cisco ASA

Correct Answer: C

QUESTION 6

Why is it important to implement MFA inside of an organization?

- A. To prevent man-the-middle attacks from being successful.
- B. To prevent DoS attacks from being successful.
- C. To prevent brute force attacks from being successful.
- D. To prevent phishing attacks from being successful.

Correct Answer: C

QUESTION 7

Why is it important to patch endpoints consistently?

- A. Patching reduces the attack surface of the infrastructure.
- B. Patching helps to mitigate vulnerabilities.
- C. Patching is required per the vendor contract.
- D. Patching allows for creating a honeypot.

Correct Answer: B

QUESTION 8

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

- A. NTLMSSP
- B. Kerberos
- C. CHAP
- D. TACACS+
- E. RADIUS

Correct Answer: AB

Neither RADIUS or TACACS+ authenticates the user. They facilitate communication to the authentication server. Kerberos and NTLMSSP do authenticate the user.

QUESTION 9

What is the difference between EPP and EDR?

- A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
- B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
- C. EDR focuses solely on prevention at the perimeter.
- D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

Correct Answer: B

QUESTION 10

An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is nonzero. What is the issue?

- A. The engineer is attempting to upload a hash created using MD5 instead of SHA-256
- B. The file being uploaded is incompatible with simple detections and must use advanced detections
- C. The hash being uploaded is part of a set in an incorrect format
- D. The engineer is attempting to upload a file instead of a hash

Correct Answer: A

QUESTION 11

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

- A. RADIUS-based REAP
- B. fingerprinting
- C. Dynamic ARP Inspection
- D. multifactor authentication

Correct Answer: D

QUESTION 12

DRAG DROP

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Select and Place:

Version 1	appropriate only for legacy systems
Version 5	appropriate only for the main cache
Version 8	introduced extensibility
Clearer pictures and no water-mask in the Premium Product	caches

Correct Answer:

	Version 1
	Version 5
	Version 9
Clearer pictures and no water-mask in the Premium Product	

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/BRKNMS-3132.pdf>

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average **99.9%** Success Rate

More than **800,000** Satisfied Customers Worldwide

Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.