Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

https://www.2passeasy.com/dumps/350-701/

NEW QUESTION 1
Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

A. security intelligence
B. impact flags
C. health monitoring
D. URL filtering

Answer: A

NEW QUESTION 2
Refer to the exhibit.

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations
B. show authentication method
C. show dot1x all
D. show authentication sessions

Answer: B

NEW QUESTION 3
An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10. What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

A. Cisco Identity Services Engine and AnyConnect Posture module
B. Cisco Stealthwatch and Cisco Identity Services Engine integration
C. Cisco ASA firewall with Dynamic Access Policies configured
D. Cisco Identity Services Engine with PxGrid services enabled

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/administration/guide/b_AnyConnect_Administrator_Guide_4-6/configure-posture.html

NEW QUESTION 4
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html

NEW QUESTION 5
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems

C. database
D. web page images

Answer: C

Explanation:
Reference: https://tools.cisco.com/security/center/resources/sql_injection

NEW QUESTION 6
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

Answer: B

NEW QUESTION 7
Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

A. SNMP
B. SMTP
C. syslog
D. model-driven telemetry

Answer: D

Explanation:
Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

NEW QUESTION 8
What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000

NEW QUESTION 9
DRAG DROP
Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.

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
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 10
Which two descriptions of AES encryption are true? (Choose two.)

A. AES is less secure than 3DES.
B. AES is more secure than 3DES.
C. AES can use a 168-bit key for encryption.
D. AES can use a 256-bit key for encryption.
E. AES encrypts and decrypts a key three times in sequence.

Answer: BD

Explanation:
Reference: https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html

NEW QUESTION 10
Which command enables 802.1X globally on a Cisco switch?

A. dot1x system-auth-control
B. dot1x pae authenticator
C. authentication port-control auto
D. aaa new-model

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/802_1x_commands.html

NEW QUESTION 15
For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)

A. computer identity
B. Windows service
C. user identity
D. Windows firewall
E. default browser

Answer: BC

NEW QUESTION 20
What is a characteristic of Dynamic ARP Inspection?

A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.
B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.
C. DAI associates a trust state with each switch.
D. DAI intercepts all ARP requests and responses on trusted ports only.

Answer: A

NEW QUESTION 25
DRAG DROP
Drag and drop the descriptions from the left onto the correct protocol versions on the right.
[MISSING]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
[MISSING]

NEW QUESTION 28
Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

NEW QUESTION 31
How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets
B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address

C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
D. by overwhelming a targeted host with ICMP echo-request packets

Answer: C

NEW QUESTION 33
What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

NEW QUESTION 36
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

A. Certificate Trust List
B. Endpoint Trust List
C. Enterprise Proxy Service
D. Secured Collaboration Proxy

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html

NEW QUESTION 39
Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Enable browser alerts for fraudulent websites.
B. Define security group memberships.
C. Revoke expired CRL of the websites.
D. Use antispyware software.
E. Implement email filtering techniques.

Answer: AE

NEW QUESTION 44
Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauth asa- host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmp- server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXXasa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa- host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: D

NEW QUESTION 48
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

A. Cisco Security Intelligence
B. Cisco Application Visibility and Control
C. Cisco Model Driven Telemetry
D. Cisco DNA Center

Answer: B

NEW QUESTION 50
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program.

Answer: DE

NEW QUESTION 51
DRAG DROP
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Configure a Machine Agent or SIM Agent.
Install monitoring extension for AWS EC2.
Update config.yaml.
Restart the Machine Agent.

NEW QUESTION 54
Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Answer: A

NEW QUESTION 59
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.
B. It alerts users when the WSA decrypts their traffic.
C. It decrypts HTTPS application traffic for authenticated users.
D. It provides enhanced HTTPS application detection for AsyncOS.

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

NEW QUESTION 63
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

A. device flow correlation
B. simple detections
C. application blocking list
D. advanced custom detections

Answer: C

NEW QUESTION 65
What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry

Answer: C

NEW QUESTION 66
Refer to the exhibit.

```
Sysauthcontrol        Enabled
Dot1x Protocol Version    3

Dot1x Info for GigabitEthernet1/0/12
------------------------------------
PAE              = AUTHENTICATOR
PortControl      = FORCE_AUTHORIZED
ControlDirection = Both
HostMode         = SINGLE_HOST
QuietPeriod      = 60
ServerTimeout    = 0
SuppTimeout      = 30
ReAuthMax        = 2
MaxReq           = 2
TxPeriod         = 30
```

Which command was used to display this output?

A. show dot1x all
B. show dot1x
C. show dot1x all summary
D. show dot1x interface gi1/0/12

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

NEW QUESTION 70
Which information is required when adding a device to Firepower Management Center?

A. username and password
B. encryption method
C. device serial number
D. registration key

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-0000069d

NEW QUESTION 72
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the
350-701 Product From:

https://www.2passeasy.com/dumps/350-701/

Money Back Guarantee

350-701 Practice Exam Features:

* 350-701 Questions and Answers Updated Frequently

* 350-701 Practice Questions Verified by Expert Senior Certified Staff

* 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year