Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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

NEW QUESTION 1
Which two capabilities does TAXII support? (Choose two.)

A. exchange
B. pull messaging
C. binding
D. correlation
E. mitigating

Answer: BC

NEW QUESTION 2
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

Answer: C

NEW QUESTION 3
Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM
B. SHA-96
C. AES-256
D. SHA-384

Answer: A

NEW QUESTION 4
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 5
What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

A. biometric factor
B. time factor
C. confidentiality factor
D. knowledge factor
E. encryption factor

Answer: AD

NEW QUESTION 6
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 7
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 8
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 9
Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

A. NGFW
B. AMP
C. WSA
D. ESA

Answer: B

NEW QUESTION 10
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 10
Which two activities can be done using Cisco DNA Center? (Choose two.)

A. DHCP
B. design
C. accounting
D. DNS
E. provision

Answer: BE

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_00.pdf

NEW QUESTION 15
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

A. RSA SecureID
B. Internal Database
C. Active Directory
D. LDAP

Answer: C

NEW QUESTION 17
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 19

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 22
Which VPN technology can support a multivendor environment and secure traffic between sites?

A. SSL VPN
B. GET VPN
C. FlexVPN
D. DMVPN

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

NEW QUESTION 24
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 28
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 33
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 37
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

A. accounting
B. assurance
C. automation
D. authentication
E. encryption

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

NEW QUESTION 41

What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable IP Layer enforcement.
B. Activate the Advanced Malware Protection license
C. Activate SSL decryption.
D. Enable Intelligent Proxy.

Answer: D

NEW QUESTION 42
Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

A. Sophos engine
B. white list
C. RAT
D. outbreak filters
E. DLP

Answer: AD

NEW QUESTION 46
How is Cisco Umbrella configured to log only security events?

A. per policy
B. in the Reporting settings
C. in the Security Settings section
D. per network in the Deployments section

Answer: A

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

NEW QUESTION 47
What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
C. EPP focuses on network security, and EDR focuses on device security.
D. EDR focuses on network security, and EPP focuses on device security.

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html

NEW QUESTION 51
Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud

Answer: A

NEW QUESTION 53
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 58
Which ASA deployment mode can provide separation of management on a shared appliance?

A. DMZ multiple zone mode
B. transparent firewall mode
C. multiple context mode
D. routed mode

Answer: C

NEW QUESTION 59
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html

NEW QUESTION 62
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 63
Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting
B. water holing
C. DDoS
D. buffer overflow

Answer: D

Explanation:
Reference: https://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION 66
An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE.
Which CoA type achieves this goal?

A. Port Bounce
B. CoA Terminate
C. CoA Reauth
D. CoA Session Query

Answer: C

NEW QUESTION 68
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 69
Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

Answer: AB

Explanation:
Reference: https://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 71
How does Cisco Stealthwatch Cloud provide security for cloud environments?

A. It delivers visibility and threat detection.
B. It prevents exfiltration of sensitive data.
C. It assigns Internet-based DNS protection for clients and servers.
D. It facilitates secure connectivity between public and private networks.

Answer: A

Explanation:
https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/FBLP/Cisco/Cisco-091919-Simple-IT-Whitepaper.pdf

NEW QUESTION 75
.....

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