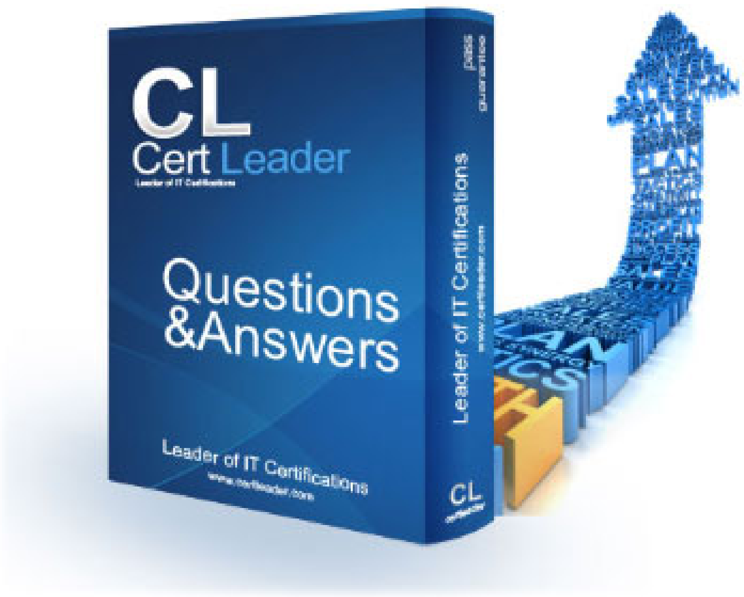
350-701 Dumps

Implementing and Operating Cisco Security Core Technologies

https://www.certleader.com/350-701-dumps.html



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

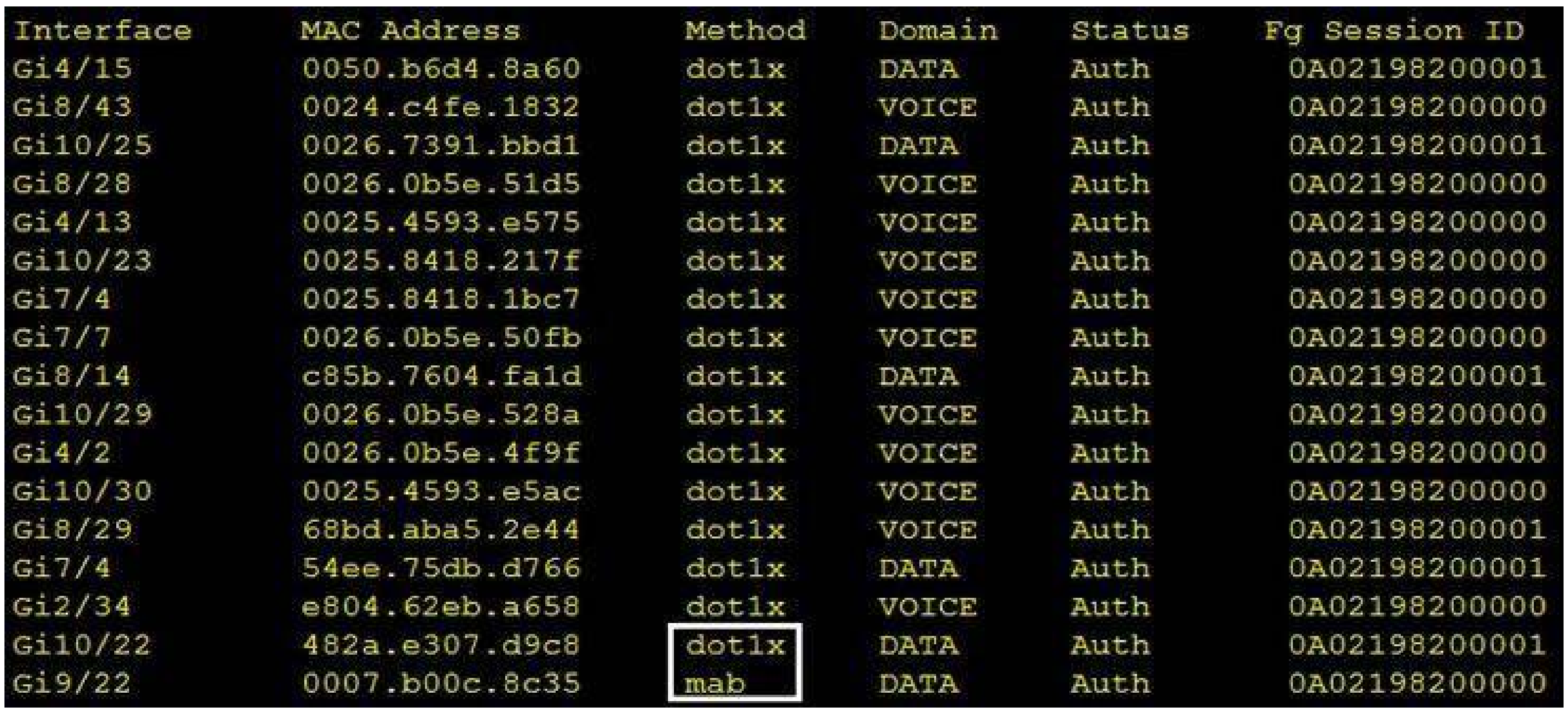
Answer: A

NEW QUESTION 2
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

A. correlation
B. intrusion
C. access control
D. network discovery

Answer: D

NEW QUESTION 3
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 4
Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

A. group policy
B. access control policy
C. device management policy
D. platform service policy

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/platform_settings_policies_for_managed_devices.pdf

NEW QUESTION 5
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 6
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 7
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 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
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus
B. Stealthwatch
C. Firepower
D. Tetration

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/index.html#~products

NEW QUESTION 10
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 10
Which two key and block sizes are valid for AES? (Choose two.)

A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length

Answer: CD

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

NEW QUESTION 15
In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS
B. UCaaS
C. PaaS
D. SaaS

Answer: A

Explanation:
Reference: https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

NEW QUESTION 20
What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

A. STIX
B. XMPP
C. pxGrid
D. SMTP

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.pdf

NEW QUESTION 23
What are two list types within AMP for Endpoints Outbreak Control? (Choose two.)

A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL

Answer: BD

Explanation:
Reference: https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf chapter 2

NEW QUESTION 24
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 29
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 31
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 36
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 37
An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?

A. Cisco Prime Infrastructure
B. Cisco Identity Services Engine
C. Cisco Stealthwatch
D. Cisco AMP for Endpoints

Answer: B

NEW QUESTION 38
When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

A. authentication server: Cisco Identity Service Engine
B. supplicant: Cisco AnyConnect ISE Posture module
C. authenticator: Cisco Catalyst switch
D. authenticator: Cisco Identity Services Engine
E. authentication server: Cisco Prime Infrastructure

Answer: AC

Explanation:
Reference: https://www.lookingpoint.com/blog/ise-series-802.1x

NEW QUESTION 42
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 43
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 proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

A. transparent
B. redirection
C. forward
D. proxy gateway

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html

NEW QUESTION 49
Under which two circumstances is a CoA issued? (Choose two.)

A. A new authentication rule was added to the policy on the Policy Service node.
B. An endpoint is deleted on the Identity Service Engine server.
C. A new Identity Source Sequence is created and referenced in the authentication policy.
D. An endpoint is profiled for the first time.
E. A new Identity Service Engine server is added to the deployment with the Administration persona.

Answer: BD

Explanation:
Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

NEW QUESTION 54
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 56
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransomware infection? (Choose two.)

A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Answer: AC

NEW QUESTION 61
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 66
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 67
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 70
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 74
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two.)

A. put
B. options
C. get
D. push
E. connect

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

NEW QUESTION 77
In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor
B. virtual machine
C. network
D. application

Answer: D

Explanation:
Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

NEW QUESTION 82
What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch

Answer: C

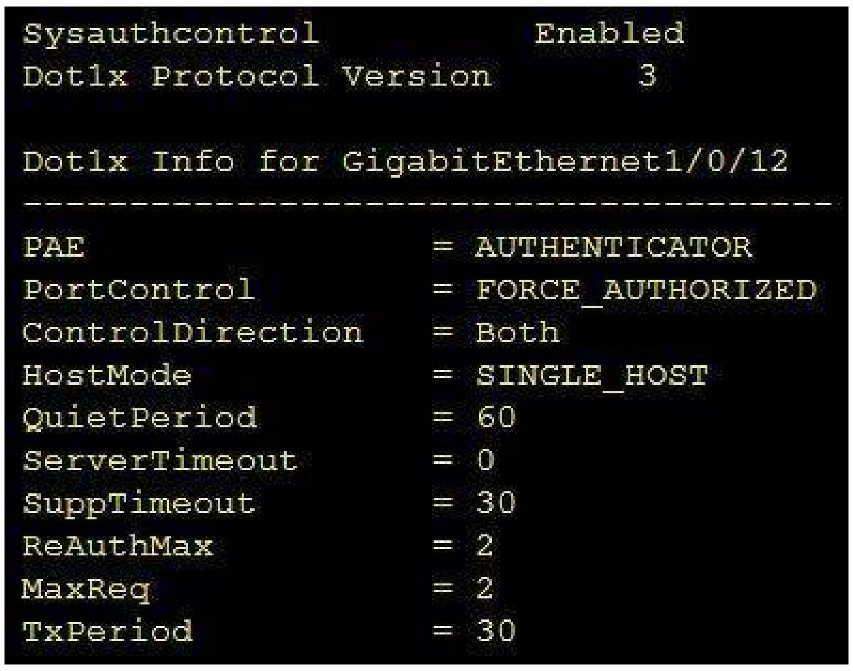
NEW QUESTION 87
Which attack is commonly associated with C and C++ programming languages?

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 91
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 92
Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

A. quality of service
B. time synchronization
C. network address translations
D. intrusion policy

Answer: B

NEW QUESTION 95
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

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

Answer: D

NEW QUESTION 97
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two.)

A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP

Answer: DE

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

NEW QUESTION 98
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists

Answer: C

NEW QUESTION 102
......