Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

A. SAT
B. BAT
C. HAT
D. RAT

Answer: D

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
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 5
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis

Answer: B

Explanation:
Reference: https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories

NEW QUESTION 6
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 7
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
B. It discovers and controls cloud apps that are connected to a company's corporate environment.
C. It deletes any application that does not belong in the network.
D. It sends the application information to an administrator to act on.

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features

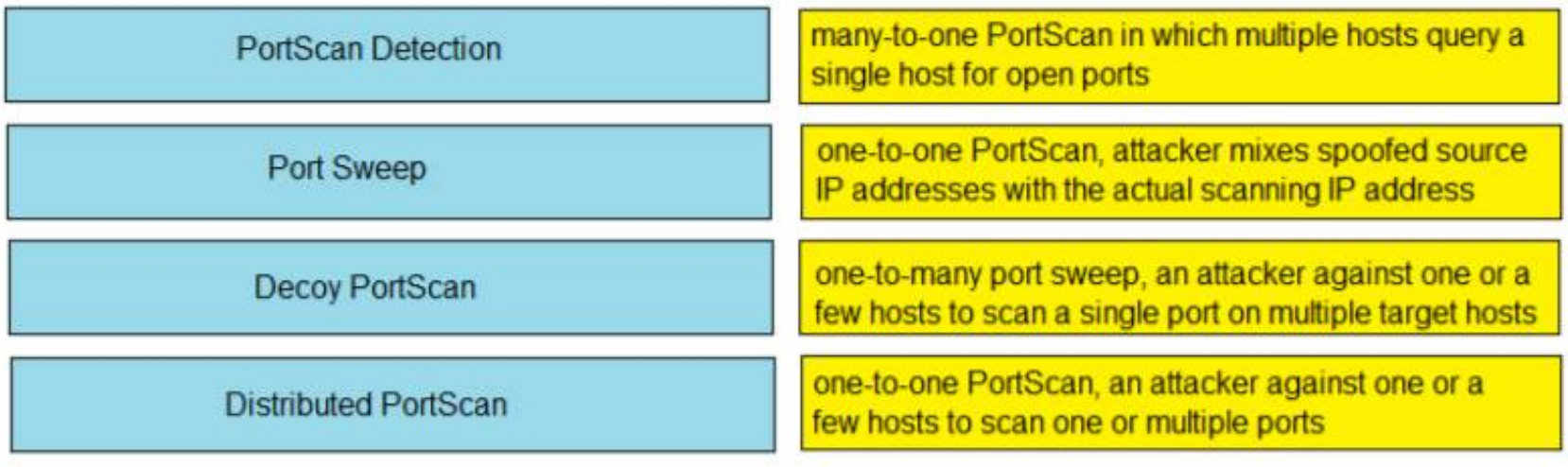
NEW QUESTION 8
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)

A. RADIUS
B. TACACS+
C. DHCP
D. sFlow
E. SMTP

Answer: AC

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

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.



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 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
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 15
Which technology is used to improve web traffic performance by proxy caching?

A. WSA
B. Firepower
C. FireSIGHT
D. ASA

Answer: A

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 21
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 26
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 31
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 32
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 34
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 37
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 39
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 43
Which two behavioral patterns characterize a ping of death attack? (Choose two.)

A. The attack is fragmented into groups of 16 octets before transmission.
B. The attack is fragmented into groups of 8 octets before transmission.
C. Short synchronized bursts of traffic are used to disrupt TCP connections.
D. Malformed packets are used to crash systems.
E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: BD

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

NEW QUESTION 47
Which feature is supported when deploying Cisco ASAv within AWS public cloud?

A. multiple context mode
B. user deployment of Layer 3 networks
C. IPv6
D. clustering

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav-aws.html

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 52
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

NEW QUESTION 57
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 61
On which part of the IT environment does DevSecOps focus?

A. application development
B. wireless network
C. data center
D. perimeter network

Answer: A

NEW QUESTION 66
What is a characteristic of traffic storm control behavior?

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
B. Traffic storm control cannot determine if the packet is unicast or broadcast.
C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html

NEW QUESTION 69
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 70
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 73
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 75
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 79
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 81
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 84
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 85
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)

A. SIP
B. inline normalization
C. SSL
D. packet decoder
E. modbus

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html

NEW QUESTION 86
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 89
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 90
.....

Relate Links

100% Pass Your 350-701 Exam with Exambible Prep Materials

https://www.exambible.com/350-701-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/