Cisco Network Security Final Exam

Study online at https://quizlet.com/_darscx

Which statement describes a difference between the Cisco ASA IOS CLI feature and the router IOS CLI feature?	To use a show command in a general configuration mode, ASA can use the command directly whereas a router will need to enter the do command before issuing the show command.
What provides both secure segmentation and threat defense in a Secure Data Center solution?	Adaptive Security Appliance
What are the three core components of the Cisco Secure Data Center solution? (Choose three.)	secure segmentation, visibility, threat defense
What are three characteristics of ASA transparent mode? (Choose three.)	This mode does not support VPNs, QoS, or DHCP Relay. This mode is referred to as a "bump in the wire." In this mode the ASA is invisible to an attacker.
What is needed to allow specific traffic that is sourced on the outside network of an ASA firewall to reach an internal network?	ACL
What will be the result of failed login attempts if the following command is entered into a router? login block-for 150 attempts 4 within 90	All login attempts will be blocked for 150 seconds if there are 4 failed attempts within 90 seconds.
Which two tasks are associated with router hardening? (Choose two.)	disabling unused ports and interfaces, securing administrative access
Which threat protection capability is provided by Cisco ESA?	spam protection
What are two security measures used to protect endpoints in the borderless network? (Choose two.)	denylisting, DLP
Which three types of traffic are allowed when the authentication port-control auto command has been issued and the client has not yet been authenticated? (Choose three.)	CDP, STP, EAPOL
Which statement describes a characteristic of the IKE protocol?	It uses UDP port 500 to exchange IKE information between the security gateways.
Which action do IPsec peers take during the IKE Phase 2 exchange?	negotiation of IPsec policy
What are two hashing algorithms used with IPsec AH to guarantee authenticity? (Choose two.)	SHA, MD5
Which command raises the privilege level of the ping command to 7?	privilege exec level 7 ping
What is a characteristic of a role-based CLI view of router configuration?	A single CLI view can be shared within multiple superviews.
What is a limitation to using OOB management on a large enterprise network?	All devices appear to be attached to a single management network.
Which two types of hackers are typically classified as grey hat hackers? (Choose two.)	hacktivists, vulnerability brokers
When describing malware, what is a difference between a virus and a worm?	A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently.
Which type of packet is unable to be filtered by an outbound ACL?	router-generated packet
Consider the access list command applied outbound on a router serial interface. access-list 100 deny icmp 192.168.10.0 0.0.0.255 any echo reply What is the effect of applying this access list command?	No traffic will be allowed outbound on the serial interface.
Which command is used to activate an IPv6 ACL named ENG_ACL on an interface so that the router filters traffic prior to accessing the routing table?	ipv6 traffic-filter ENG_ACL in
What technology has a function of using trusted third-party protocols to issue credentials that are accepted as an authoritative identity?	OSCP, CRL
Which protocol is an IETF standard that defines the PKI digital certificate format?	X.509

Cisco Network Security Final Exam

Study online at https://quizlet.com/_darscx

A network administrator is configuring DAI on a switch. Which command should be used on the uplink interface that connects to a router?	ip arp inspection trust
What is the best way to prevent a VLAN hopping attack?	Disable trunk negotiation for trunk ports and statically set nontrunk ports as access ports.
What would be the primary reason an attacker would launch a MAC address overflow attack?	so that the attacker can see frames that are destined for other hosts
What is the main difference between the implementation of IDS and IPS devices?	An IDS would allow malicious traffic to pass before it is addressed, whereas an IPS stops it immediately.
Which attack is defined as an attempt to exploit software vulnerabilities that are unknown or undisclosed by the vendor?	zero-day
What are the three signature levels provided by Snort IPS on the 4000 Series ISR? (Choose three.)	security, connectivity, balanced
What are three attributes of IPS signatures? (Choose three.)	action, trigger, type
Which two features are included by both TACACS+ and RADIUS protocols? (Choose two.)	password encryption, utilization of transport layer protocols
What function is provided by the RADIUS protocol?	RADIUS provides separate ports for authorization and accounting.
What are three characteristics of the RADIUS protocol? (Choose three.)	uses UDP ports for authentication and accounting, supports 802.1X and SIP, is an open RFC standard AAA protocol
Which zone-based policy firewall zone is system-defined and applies to traffic destined for the router or originating from the router?	self zone
What are two benefits of using a ZPF rather than a Classic Firewall? (Choose two.)	The ZPF is not dependent on ACLs. ZPF policies are easy to read and troubleshoot.
How does a firewall handle traffic when it is originating from the private network and traveling to the DMZ network?	The traffic is usually permitted with little or no restrictions.
Which two protocols generate connection information within a state table and are supported for stateful filtering? (Choose two.)	DHCP, TCP
Which type of firewall is supported by most routers and is the easiest to implement?	stateless firewall
What network testing tool would an administrator use to assess and validate system configurations against security policies and compliance standards?	Tripwire
What type of network security test can detect and report changes made to network systems?	integrity checking
What network security testing tool has the ability to provide details on the source of suspicious network activity?	SIEM
How do modern cryptographers defend against brute-force attacks?	Use a keyspace large enough that it takes too much money and too much time to conduct a successful attack.
How does a Caesar cipher work on a message?	Letters of the message are replaced by another letter that is a set number of places away in the alphabet.
What is the main factor that ensures the security of encryption of modern algorithms?	secrecy of the keys
What is the next step in the establishment of an IPsec VPN after IKE Phase 1 is complete?	negotiation of the IPsec SA policy
After issuing a show run command, an analyst notices the following command: crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac What is the purpose of this command?	It establishes the set of encryption and hashing algorithms used to secure the data sent through an IPsec tunnel.
Which algorithm can ensure data integrity?	MD5

Cisco Network Security Final Exam

Study online at https://quizlet.com/_darscx

A company implements a security policy that ensures that a file sent from the headquarters office to the branch office can only be opened with a predetermined code. This code is changed every day. Which two algorithms can be used to achieve this task? (Choose two.)	3DES, AES
A network technician has been asked to design a virtual private network between two branch routers. Which type of cryptographic key should be used in this scenario?	symmetric key
Which two options can limit the information discovered from port scanning? (Choose two.)	intrusion prevention system, firewall
An administrator discovers that a user is accessing a newly established website that may be detrimental to company security. What action should the administrator take first in terms of the security policy?	Revise the AUP immediately and get all users to sign the updated AUP.
If AAA is already enabled, which three CLI steps are required to configure a router with a specific view? (Choose three.)	Create a view using the parser view view-name command. Assign a secret password to the view. Assign commands to the view.
ACLs are used primarily to filter traffic. What are two additional uses of ACLs? (Choose two.):	specifying internal hosts for NAT, identifying traffic for QoS
What two features are added in SNMPv3 to address the weaknesses of previous versions of SNMP? (Choose two.)	authentication, encryption
What network testing tool is used for password auditing and recovery?	L0phtcrack
Which type of firewall makes use of a server to connect to destination devices on behalf of clients?	proxy firewall
Which two statements describe the characteristics of symmetric algorithms? (Choose two.)	They are commonly used with VPN traffic. They are referred to as a pre-shared key or secret key.
A web server administrator is configuring access settings to require users to authenticate first before accessing certain web pages. Which requirement of information security is addressed through the configuration?	confidentiality
The use of 3DES within the IPsec framework is an example of which of the five IPsec building blocks?	confidentiality
What function is provided by Snort as part of the Security Onion?	to generate network intrusion alerts by the use of rules and signatures
What are two drawbacks to using HIPS? (Choose two.)	With HIPS, the network administrator must verify support for all the different operating systems used in the network. HIPS has difficulty constructing an accurate network picture or coordinating events that occur across the entire network.
In an AAA-enabled network, a user issues the configure terminal command from the privileged executive mode of operation. What AAA function is at work if this command is rejected?	authorization
A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?	authorization
What is a characteristic of a DMZ zone?	Traffic originating from the outside network going to the DMZ network is selectively permitted.
Which measure can a security analyst take to perform effective security monitoring against network traffic encrypted by SSL technology?	Deploy a Cisco SSL Appliance.
What security countermeasure is effective for preventing CAM table overflow attacks?	port security

What are two examples of DoS attacks? (Choose two.)	ping of death buffer overflow
Which method is used to identify interesting traffic needed to create an IKE phase 1 tunnel?	a permit access list entry
When the CLI is used to configure an ISR for a site-to-site VPN connection, which two items must be specified to enable a crypto map policy? (Choose two.)	the peer a valid access list
How does a firewall handle traffic when it is originating from the public network and traveling to the DMZ network?	Traffic that is originating from the public network is inspected and selectively permitted when traveling to the DMZ network.
A client connects to a Web server. Which component of this HTTP connection is not examined by a stateful firewall?	the actual contents of the HTTP connection
Which network monitoring technology uses VLANs to monitor traffic on remote switches?	RSPAN
Which rule action will cause Snort IPS to block and log a packet?	drop
What is typically used to create a security trap in the data center facility?	IDs, biometrics, and two access doors
A company is concerned with leaked and stolen corporate data on hard copies. Which data loss mitigation technique could help with this situation?	shredding
Upon completion of a network security course, a student decides to pursue a career in cryptanalysis. What job would the student be doing as a cryptanalyst?	cracking code without access to the shared secret key
What command is used on a switch to set the port access entity type so the interface acts only as an authenticator and will not respond to any messages meant for a supplicant?	dot1x pae authenticator
What are two disadvantages of using an IDS? (Choose two.)	The IDS does not stop malicious traffic. The IDS requires other devices to respond to attacks.
What ports can receive forwarded traffic from an isolated port that is part of a PVLAN?	only promiscuous ports
A user complains about being locked out of a device after too many unsuccessful AAA login attempts. What could be used by the network administrator to provide a secure authentication access method without locking a user out of a device?	Use the login delay command for authentication attempts.
What are two drawbacks in assigning user privilege levels on a Cisco router? (Choose two.)	Assigning a command with multiple keywords allows access to all commands using those keywords. Commands from a lower level are always executable at a higher level.
What are two reasons to enable OSPF routing protocol authentication on a network? (Choose two.)	to prevent data traffic from being redirected and then discarded, to prevent redirection of data traffic to an insecure link
Which three functions are provided by the syslog logging service? (Choose three.)	gathering logging information, specifying where captured information is stored, distinguishing between information to be captured and information to be ignored
What two ICMPv6 message types must be permitted through IPv6 access control lists to allow resolution of Layer 3 addresses to Layer 2 MAC addresses? (Choose two.)	neighbor solicitations, neighbor advertisements
Which three services are provided through digital signatures? (Choose three.)	authenticity, nonrepudiation, integrity
A technician is to document the current configurations of all network devices in a college, including those in off-site buildings. Which protocol would be best to use to securely access the network devices?	SSH

Cisco Network Security Final Exam

Study online at https://quizlet.com/_darscx

An administrator is trying to develop a BYOD security policy for employees that are bringing a wide range of devices to connect to the company network. Which three objectives must the BYOD security policy address? (Choose three.)	Rights and activities permitted on the corporate network must be defined. Safeguards must be put in place for any personal device being compromised. The level of access of employees when connecting to the corporate network must be defined.
What is the function of the pass action on a Cisco IOS Zone-Based Policy Firewall?	forwarding traffic from one zone to another
What network testing tool can be used to identify network layer protocols running on a host?	nmap
In the implementation of security on multiple devices, how do ASA ACLs differ from Cisco IOS ACLs?	Cisco IOS ACLs are configured with a wildcard mask and Cisco ASA ACLs are configured with a subnet mask.
Which statement describes an important characteristic of a site-to-site VPN?	It must be statically set up.
Which two options are security best practices that help mitigate BYOD risks? (Choose two.)	Keep the device OS and software updated. Only turn on Wi-Fi when using the wireless network.
A recently created ACL is not working as expected. The admin determined that the ACL had been applied inbound on the interface and that was the incorrect direction. How should the admin fix this issue?	Delete the original ACL and create a new ACL, applying it outbound on the interface.
What characteristic of the Snort term-based subscriptions is true for both the community and the subscriber rule sets?	Both offer threat protection against security threats.
A security analyst is configuring Snort IPS. The analyst has just downloaded and installed the Snort OVA file. What is the next step?	Configure Virtual Port Group interfaces.
The security policy in a company specifies that employee workstations can initiate HTTP and HTTPS connections to outside websites and the return traffic is allowed. However, connections initiated from outside hosts are not allowed. Which parameter can be used in extended ACLs to meet this requirement?	established
A researcher is comparing the differences between a stateless firewall and a proxy firewall. Which two additional layers of the OSI model are inspected by a proxy firewall? (Choose two.)	Layer 5 and 7
Which privilege level has the most access to the Cisco IOS?	level 15
A network analyst is configuring a site-to-site IPsec VPN. The analyst has configured both the ISAKMP and IPsec policies. What is the next step?	Apply the crypto map to the appropriate outbound interfaces.
When an inbound Internet-traffic ACL is being implemented, what should be included to prevent the spoofing of internal networks?	ACEs to prevent traffic from private address spaces
Which two types of attacks are examples of reconnaissance attacks? (Choose two.)	port scan ping sweep
Which Cisco solution helps prevent ARP spoofing and ARP poisoning attacks?	Dynamic ARP Inspection
When the Cisco NAC appliance evaluates an incoming connection from a remote device against the defined network policies, what feature is being used?	posture assessment
Which two steps are required before SSH can be enabled on a Cisco router? (Choose two.)	Give the router a host name and domain name. Generate a set of secret keys to be used for encryption and decryption.
The network administrator for an e-commerce website requires a service that prevents customers from claiming that legitimate orders are fake. What service provides this type of guarantee?	nonrepudiation
What functionality is provided by Cisco SPAN in a switched network?	It mirrors traffic that passes through a switch port or VLAN to another port for traffic analysis.

Cisco Network Security Final Exam

Study online at https://quizlet.com/_darscx

Which three statements are generally considered to be best practices in the placement of ACLs? (Choose three.)	Filter unwanted traffic before it travels onto a low-bandwidth link. Place standard ACLs close to the destination IP address of the traffic. Place extended ACLs close to the source IP address of the traffic.
What function is performed by the class maps configuration object in the Cisco modular policy framework?	identifying interesting traffic
In an attempt to prevent network attacks, cyber analysts share unique identifiable attributes of known attacks with colleagues. What three types of attributes or indicators of compromise are helpful to share? (Choose three.)	IP addresses of attack servers changes made to end system software features of malware files
What two assurances does digital signing provide about code that is downloaded from the Internet? (Choose two.)	The code is authentic and is actually sourced by the publisher. The code has not been modified since it left the software publisher.
Which two statements describe the use of asymmetric algorithms? (Choose two.)	If a private key is used to encrypt the data, a public key must be used to decrypt the data. If a public key is used to encrypt the data, a private key must be used to decrypt the data.
Which statement is a feature of HMAC?	HMAC uses a secret key as input to the hash function, adding authentication to integrity assurance.
What is the purpose of the webtype ACLs in an ASA?	to filter traffic for clientless SSL VPN users
Which two statements describe the effect of the access control list wildcard mask 0.0.0.15? (Choose two.)	The first 28 bits of a supplied IP address will be matched. The last four bits of a supplied IP address will be ignored.
Which type of firewall is the most common and allows or blocks traffic based on Layer 3, Layer 4, and Layer 5 information?	packet filtering firewall
Which protocol or measure should be used to mitigate the vulnerability of using FTP to transfer documents between a teleworker and the company file server?	SCP
What tool is available through the Cisco IOS CLI to initiate security audits and to make recommended configuration changes with or without administrator input?	Cisco AutoSecure
Which two technologies provide enterprise-managed VPN solutions? (Choose two.)	site-to-site VPN remote access VPN
What are the three components of an STP bridge ID? (Choose three.)	the MAC address of the switch the extended system ID the bridge priority value
What are two differences between stateful and packet filtering firewalls? (Choose two.)	A stateful firewall provides more stringent control over security than a packet filtering firewall. A stateful firewall will provide more logging information than a packet filtering firewall.
Which portion of the Snort IPS rule header identifies the destination port? alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS	$HTTP_PORTS
What port state is used by 802.1X if a workstation fails authorization?	unauthorized
Which two characteristics apply to role-based CLI access superviews? (Choose two.)	A specific superview cannot have commands added to it directly. Users logged in to a superview can access all commands specified within the associated CLI views.