Comptia security+ domain 1 practice test questions essay

Which of the following is a firewall function?-Frame Filtering-Packet Filtering-FTF hosting-encrypting-Protocol conversionPacket Filtering

You have worked as the network administrator for a company for seven months. One day all picture files on the server become corrupted. You discover that a user downloaded a virus from the Internet onto his workstation, and it propagated to the server. you successfully restore all files from backup, but your boss is adamant that this situation does not recoccur. What should you do?-Install a firewall-Allow users to access the internet only from terminals that are not attached to the main network.-Disconnect the user from the Internet-Install a network virus detection software solutionInstall a network virus detection software solution

You manage a small network at work. Users use workstations connected to your network. No portable computers are allowed. As part of your security plan, you would like to implement scanning of e-mails for all users. You want to scan the e-mails and prevent any e-mails with malicious attachments from being received by users. Your solution should minimize adminstration, allowing you to centrally manage the scan settings. Which solution should you use?-DMZ-SMTP-Network based firewall-Host based firewall-Network based firewall

As a security precaution, you have implement IPsec is used between any two devices on your network. IPsec provides encryption for traffic between devices. You would like to implement a solution that can scan the contents of the encrypted traffic to prevent any malicious attacks. Which solution should

you implement?-Protocol analyzer-VPN concentrator-Network-based IDS-Host-based IDS-Port scanner-Host-based IDS

Your company has a connection to the internet that allows users to access the Internet. You aslo have a Web sever and an e-mail server that you want to make available to the Internet users. You want to create a DMZ for these two servers. Which type of device should you use to create the DMZ? Network-based firewall

Which of the following are characteristics of a circuit-level gateway?(Select two)-Filter IP address and port-Filter based on session-Stateful-Filters based on URL-Stateless-Filter based on sessions-Stateful

Which of the following are characteristics of a packet filtering firewall?(Select two)-Stateful-Filters based on sessions-Stateless-Filters based on URL-Filters IP address and port-Stateless-Filters IP address and port

You want to install a firewall that can reject packets that are not part of an active session. Which type of firewall should you use?-Circuit-level-Packet filtering-Application level-VPN concentrator-Circuit-level

You provide Internet access for a local school. You want to control Internet access based on users, and prevent access to specific URLs. Which type of firewall should be install?-Circuit-level-Application level-IPS-Packet filtering-Application level

You are concerned about protection your network from a network-based attack from the Internet. Specifically, you are concerned about attacks that have not yet been identified or do not have prescribed protections. What

type of device should you use?-Anti-virus scanner-Signature based IDS-Network based firewall-Anomaly based IDS-Host based firewall-Anomaly based IDS

Which of the following describes how a router can be used to implement security on your network?-Use a lookup table to deny access to traffic from specific MAC address-Use an access control list to deny traffic from specific IP addresses.-Examine the packet payload to deny packets with malformed data.-Use an access control list to deny traffic sent from specific users-Use an access control list to deny traffic from specific IP addresses

What security mechanism can be used to detect attacks originating on the Internet or from within an internal trusted subnet?-Security alarm-IDS-Biometric system-Firewall-IDS

Which of the following is the best device to deploy to protect your private network from a public untrusted network?-HUB-Router-Gateway-Firewall-Firewall

Which of the following is a valid security measure to protect e-mails from viruses?-Blockers on e-mail gateways-Use PGP to sign outbound e-mail-Limit attachment to a max of 1MB-Use reverse DNS lookup-Use blockers on e-mail gateways

Virtual LAN can be created using which of the following?-Router-Switch-Gateway-HUB-Switch

What do host based intrusion detection systems often rely upon to perform their detection activities?-Network traffic-Remote monitoring tools-External sensors-Host system auditing capabilities-Host system auditing capabilities

What actions can a typical passive Intrusion Detection System(IDS) take when it detects an attack? (Select Two)-An alert is generated and delivered via e-mail, the console, or an SNMP trap.-The IDS configuration is changed dynamically and the source IP address is banned-LAN side clients are halted and removed from the domain-The IDS logs all pertinent data about the intrusion-An alert is generated and delivered via e-mail, the console, or an SNMP trap.-The IDS logs all pertinent data about the intrusion.

You have been getting a lot of phishing e-mails from the domain kenyan. msn. pl. Links within these e-mails open new browser windows at youneedit. com. pl. You want to make sure that these e-mails never reach your inbox, but that e-mail from other senders are not affected. What should you do?-Add kenyan. msn. pl to the email blacklist-add pl to the email blacklist.-add youneedit. com. pl to the email blacklist.-add msn. pl to the e-mail blacklist.-Add kenyan. msn. pl to the e-mail blacklist

Which of the following is a security service that monitors network traffic in real time or reviews the audit logs on servers looking for security violations?-firewall-switch-IDS-Padded cellIDS

Network based intrusion dectection is most suited to detect and prevent which types of attacks?-Buffer overflow exploitation of software-Application implementation flaw-Bandwidth-based denial of service-Brute force password attack-Bandwidth-based denial of service

Which of the following activities are considered passive in regards to the functioning of an intrusion detection system?(choose two)-Disconnecting a port being used by a zombie-Listening to network traffic-Transmitting FIN or RES packets to an external host-Monitoring the audit trails on a server-listening to network traffic-Monitoring the audit trails on a server

An active IDS system often performs which of the following actions? (Select two)-Request a second logon test for users performing abnormal activities.-Perform revers lookups to identify an intruder.-Trap and delay the intruder until the authorities arrive.-Update filters to block suspect traffic-Perform reverse lookup to identify an intruder-Update filters to block suspect traffic

Which of the following prevents access based on websites rating and classification?-NIDS-DMZ-Packet-filtering firewall-Content filter-Content filter

Which IDS method searches for intrusion or attack attempts by recognizing patterns or identities listed in a database?-Signature based-Heuristic based-Anomaly analysis based-Stateful inspection based-Signature based

What does an IDS that uses signature recognition use for identifying attacks?-Statistical analysis to find unusual deviations-Comparison of current statistics to past statistics-Comparison to a database of known attacks-Exceeding threshold values-Comparison to database of know attacks

You want to implement an IDS system that uses rules or statistical analysis to detect attacks. Which type of IDS should you deploy?-Anomaly-Signature-NIDS-HIDS-Anomaly

You have just installed a new network-based IDS system that uses signature recognition. What should you do on your regular basis?-Modify clipping levels-Check for backdoors-Generate a new baseline-Update the signature files-Update the signature files

Which of the following is the most common detection method used by an IDS?-Signature-Behavior-Anomaly-Heuristic-Signature

What is the most common form of hosted based IDS that employs signature or pattern matching detection methods?-Anti-virus software-Motion detectors-Honey pots-Firewalls-Anti-virus software

Which of the following devices accepts incoming client request and distributes those requests to specific servers?-Coaching engine-Load balancer-Media converter-CSU/DSU-IPSload balancer

You have a group of salesman who would like to access your private network through the Internet while they are traveling. you want to control access private network through a single server. Which solution should you implement?-IDN-VPN concentrator-RADIUS-IPS-DMZ-VPN concentrator

Which of the following devices can monitor a network and dectect potential security attacks?-Load balancer-IDS-PROXY-DNS server-CSU/DSUIDS

You want to be able to identify traffic that is being generated and sent through the network by a specific application running on a deviceWhich tool should you use?-Protocol analyzer-TDR-Multimeter-Toner probe-Certifier-Protocol analyzer

You have been given a laptop to use for work. You connect the laptop to your company network, use it form home, and use it while traveling. You want to protect the laptop from Internet-based attacks. Which solution should you use?-Host based firewall-Proxy server-VPN concentrator-Network based firewallHost based firewall

You connect your computer to a wireless network available at the local library. You find that you can access all web sites you want on the internet except for two. What could be the reason?-Router has not been configured to perform port forwarding-A firewall is blocking ports 80 and 443-A proxy server is blocing access to the web sites-Port triggering is redirecting traffic to the wrong IP address-Proxy server is blocking access to the web sites

Which of the following function are performed by proxies?(Select two)-Give users tthe ability to participate in real-based Internet discussions-Cache web pages-Block unwanted packets from entering your private network-Store client files-Filter unwanted e-mail-Block employees from accessing certain web sites-Cache web pages-Block employees from accessing certain web sites

Which of the following are true of a circuit proxy filter firewall?(Choose two)-Operates at the session layer-Operates at ring 0 at the operating system-Verifies sequencing of session packets.-Examines the entire message contents..-Operates at the network and transport layers-Operates at the application layer-Operates at the session layer-Verifies sequencing of session packets

Which of the following are security devices that perform statful inspection of packet data, looking for patterns that indicate malicious code?(choose two)-VPN-Firewall-ACL-IDS-IPS-IDS-IPS

Would like to control Internet access based on users, time of day, and web sites visited. How can you do this?-Configure the local security policy of each system to add internet restrictions.-Configure Internet zones using the Internet Options-Install a proxy server. Allow Internet access only through the proxy server.-Configure a packet-filtering firewall. Add rules to allow or deny Internet access.-Enable Windows Firewall on each system. Add or remove exception to control access.-Install a proxy server. Allow Internet access only through the proxy server.

You are the office manager of a small financial credit business. Your company handles personal, financial information for clients seeking small loans over the Internet. you are aware of your obligation to secure clients records, but budget is an issue. Which item would provide the best security for this situation?-Proxy server with access controls-All in one security appliance-Firewall on your gateway server to the Internet-Network access control systemAll in one security appliance

You are implementing security at a local high school that is concerned with students accessing inappropriate material on the Internet form the library’s computers. The students will use the computes to search the Internet for research paper content. The school budget is limited. Which content filtering option would you choose?-Restrict content based on content categories-Block specific DNS domain names-Block all content except for contect you

have identified as permitted-Allow all content except for the content you have identified as restricted.-Restrict content based on content categories

Which of the following solutions would you implement to track which websites that network users are accessing?-Tarpit-NIDS-Packet-filtering firewall-Proxy-Proxy

When configuring VLANs on a switch, what is used to identify VLAN membership of a device?-Switch port-Hostname-Mac address-IP address-Switch port

Which of the following does a router acting as a firewall use to control which packets are forwarded or dropped?-IPsec-VNC-ACL-RDP-PPP-ACL

You have a router that is configured as a firewall. The router is a layer 3 devices only. Which of the following does the router use for identify allowed or denied packets?-Session ID-MAC address-Username and password-IP address-IP address

You want to increase the security of your network by allowing only authenticated users to be able to access network devices through a switch. Which of the following should you implement?-IPsec-Spanning tree-802. 1x-Port security-802. 1x

Which of the following application typically use 802. 1x authentication? (Select two)-Controlling access through a switch-Authentication remote access clients-Controlling access through a wireless access point-Authenticating VPN users through the Internet-Controling access through a switch-Controling access through a wireless access point

Which of the following attacks, if successful, causes a switch to function like a hub?-Replay-ARP poisoning-MAC spoofing-Mac flooding-Mac flooding

You manage a network that uses a single switch. All ports within your building connect through the single switch. In the lobby of your building are three RJ-45 ports connected to the switch. You want to allow vistors to plug into these ports to gain Internet access, but they should not have access to any other devices on your private network. Employees, connected throughout the rest of your building should have private and Internet access. Which feature should you implement?-NAT-port authentication-VLANs-DMZ-VLANs

You have just installed a packet filtering firewall on your network. What options will you be able to set on your firewall? Select all that apply.-Digital signature-Destination address of a packet-Checksum-Sequence number-Port number-Acknowledgement number-Source address of a packet-Destination address of a packet-Port number-Source address of a packet

Which configuring VLANs on a switch, what type of switch ports are members of all VLANs defined on the switch?-Any port not assigned to a VLAN-Each port can only be a member of a single VLAN-Trunk ports-Gigabit and higer Ethernet ports-Uplink ports-Trunk ports

Which of the following is most important thing to do to prevent console access to the router?-Implement an access list to prevent console connections.-Keep the router in a locked room-Set console and enable secret passwords.-Disconnect the console cable when not in use-Keep the router in a locked room

Which of the following describes how access lists can be used to improve network security?-An access list filters based on the frame header such as source or destination MAC-AN access list identifies traffic that must use authentication or encryption-An access list looks for patterns of traffic between multiple packets and take action to stop detected attacks.-An access list filters traffic based on the IP header information such as source or destination IP address, protocol, or socket numbers.-An access list filters traffic based on the IP header or destination IP address, protocol, or socket numbers

You manage a network that uses switches. In the lobby of your building are three RJ-45 ports connected to a switch. You want to make sure that vistors cannot plug in their computers to the free network jacks and connect to the network. However, employees who plug into those same jacks should be able to coneect to the network. What feature should you configure?-Bonding-Spanning tree-Port authentication-Mirroring-VLANs-Port authentication

Which of the following solutions would you implement to eliminate switching loops?-Inner-vlan routing-Auto-duplex-Spanning tree-CSMA/CD-Spanning tree

You manage a single subnet with three switches. The switches are connected to provide redundant paths between the switches. Which feature prevents switching loops and ensures there is only a single active path between any two switches?-PoE-Trunking-802. 1x-Spanning tree-Spanning tree

You manage a network that uses multiple switches. You want to provide mulitple paths between switches so that if one link goes down, an alternate

path is available. Which feature should your switch support?-PoE-Mirroring-OSPF-Spanning tree-Trunking-Spanning tree

In which of the following situations would you use port security?-You want to restrict the device that could connect through a switch port.– You want to prevent MAC address spoffing-You want to control the packets sent and received by a router-You want to prevent sniffing attacks on the network. You want to restrict the devices that could connect through a switch port

You are the network administrator for a city library. Throughout the library are several groups of computers that provide public access to the Internet. Supervision of these computers has been difficult. You've had problems with patrons bringing personal laptops into the library and disconnecting the network cables from the library computers to connect their laptops to the internet.

The library computers are in groups of four. Each group of four computers is connected to a hub that is connected to the library network through an access port on a switch. You want to restrict access to the network so only the library computers are permitted connectivity to the internet. What can you do?-Create static Mac address for each computer-Configure port security on the switch.-Create a VLAN for each group of four computers.-Remove the hub and place each library computer on its own access port

-Configure port security on the switch

You want to ensure that all users in the Development OU have a common set of network communication security settings applied.

Which should you do?-Create a GPO folder policy for the folders containing the files.-Create a GPO computer policy for the computers in the Development OU-Create a GPO user for the development OU-Create a GPO computer policy for the computers container

-Create a GPO computer policy for the computers in the Development OU

Computer policies include a special category called user rights. Whcih action do they allow an administrator to perform?-Identify users who can perform maintenance task on computers in an OU-Specify the registry for users on specified computers in an OU-Designate a basic set of rights for all users in an OU-Identify users who can perform maintenance tasks on computer in an OU

Which statement is true regarding application of GPO settings?(Flip for answer. Too much to write)If a setting is defined in the local group policy on the computer and not defined in the GPO linked to the OU, the setting will be applied

Which step is required to configured a NAP on a RD gateway server?-Configure the server to issue a valid statement of health certificate-Configure the enforcement point as a RADIUS client to the NAP server-On the 802. 1x switch, define the RD gateway server as a compliant network VLAN-Edit the properties for the server and select REQUST CLIENT TO SEND A STATEMENT OF HEALTHEdit the properties for the server and select REQUST CLIENT TO SEND A STATEMENT OF HEALTH

LABAdd an HTTP Firewall Rule that allows traffic from the WAN to the Web server in the DMZ Hide Details

From Zone: UNSECURE (WAN)

To Zone: DMZ

Service: HTTP

Action: Allow Always

Source Hosts: Any

Internal IP Address: 172. 16. 2. 100

External IP Address: Dedicated WAN

Add an HTTPS Firewall Rule that allows traffic from the WAN to the Web server in the DMZ Hide Details

From Zone: UNSECURE (WAN)

To Zone: DMZ

Service: HTTPS

Action: Allow Always

Source Hosts: Any

Internal IP Address: 172. 16. 2. 100

External IP Address: Dedicated WAN

Add an FTP Firewall Rule that allows traffic from the administrator workstation to the Web server in the DMZ Hide Details

From Zone: SECURE (LAN)

To Zone: DMZ

Service: FTP

Action: Allow Always

Source Address: 192. 168. 1. 200

Destination Address: 172. 16. 2. 100

Add an SSH (TCP) Firewall Rule that allows traffic from the administrator workstation to the Web server in the DMZ Hide Details

From Zone: SECURE (LAN)

To Zone: DMZ

Service: SSH (TCP)

Action: Allow Always

Source Address: 192. 168. 1. 200

Destination Address: 172. 16. 2. 100

Explanation

To configure the Firewall, complete the following steps: 1. In the Security Appliance Configuration Utility, select Firewall > IPv4 Rules. 2. Click Add…. 3. Enter Firewall Rule parameters as required by the scenario and click Apply. 4. Repeat steps 2 and 3 for additional firewall rules

You have a company network that is connected to the Internet. You want all users to have Internet access, but need to protect your private network and users. You also need to make a Web server publicly available to Internet users. Which solution should you use?-Use single firewall. Put the Web server in front of the firewall, and the private network behind the firewall.-Use firewall to create a DMZ. Place the Web server inside the DMZ, and the private network behind the DMZ-Use firewall to create a DMZ. Place the Web server and the private network inside the DMZ-Use a single firewall. Put the Web server and the private network behind the firewall-Use firewall to create a DMZ. Place the web server inside the DMZ, and the private network behind the DMZ.

You have used firewalls to create a demilitarized zone. You have a web server that needs to be accessible to Internet users. The Web server must communicate with database server for retrieving product, customer, and order information. How should you place devices on the network to best protect the severs?(SELECT TWO)-Put the web server inside the DMZ-Put the database server on the private network

Of the following security zones, which one can serve as a buffer network between a private secured network and the untrusted internet?-Padded cell-DMZ-Extranet-Intranet-DMZ

Which of the following is likely to be located in a DMZ?-FTP server-User workstation-Domain controller-Backup server-FTP server

You run a small network for your business that has a single router connected to the internet and a single switch. You keep sensitive documents on a computer that you would like to keep isolated from other computers on the network. Other hosts on the network should not be able to communicate with the computer through the switch, but you still need to access the network through the computer? What should you use for the situation?-VPN-Port security-Spanning tree-VLAN-VLAN

Which of the following best describe the concept of a virtual LAN? Devices on the same network logically grouped as if they were on separate networks

You have a small network at home that is connected to the Internet. On your home network you have a server with the IP address of 192. 168. 55. 199/16. You have a single public address that is shared by all hosts on your private network. You want to configure the server as a Web server and allow Internet hosts to contact the server to browse a personal Web site. What should you use to allow access? Static NAT

You are the network administrator for a small company that implements NAT to access the Internet. However, you recently acquired 5 servers that must be accessible from outside your network. Your ISP has provided you with 5 additional registered IP addresses to support these new servers but you don’t want the public to access these servers directly. You want to place these servers behind your firewall on the inside network yet still allow them

to be accessible to the public from the outside. Which method of NAT translation should you implement for these 5 servers? Static

You want to connect your small company network to the Internet. Your ISP provides you with a single IP address that is to be shared between all hosts on your private network. You do not want external hosts to be able to initiate connection to internal hosts. What type of Network Address Translation (NAT) should you implement? Dynamic

Which of the following is not one of the ranges of IP addresses defined in RFC 1918 that are commonly used behind a NAT server? 169. 254. 0. 0 – 169. 254. 255. 255

Which of the following is a privately controlled portion of a network that is accessible to some specific external entities? Extranet

Members of the Sales team use laptops to connect to the company network. While traveling, they connect their laptops to the Internet through airport and hotel networks. You are concerned that these computers will pick up viruses that could spread to your private network. You would like to implement a solution that prevents the laptops from connecting to your network unless antivirus software and the latest operating system patches have beeninstalled. Which solution should you use? NAC

You manage a network with a single switch. All hosts connect to the network through the switch. You want to increase the security of devices that are part of the accounting department. You want to make sure that broadcast traffic sent by an accounting computer is only received by other accounting

computers, and you want to implement ACLs to control traffic sent to accounting computers through the network. What should you do? Use a router to configure a subnet for the accounting computers

When designing a firewall, what is the recommended approach for opening and closing ports? Close all ports; open only ports required by applications inside the DMZ.

Which of the following networking devices or services prevents the use of IPSec in most cases? NAT

In which of the following situations would you most likely implement a demilitarized zone (DMZ)? You want to protect a public Web server from attack.

Which of the following best describes the purpose of using subnets? Subnets divide an IP network address into multiple network addresses.

Which of the following is not a reason to use subnets on a network? Combine different media type on to the same subnet.

You want to set up a service to allow multiple users to dial in to the office server from modems on their home computers. What service should you implement? RAS

You often travel away from the office. While traveling, you would like to use a modem on your laptop computer to connect directly to a server in your office and access files on that server that you need. Remote access

The presence of unapproved modems on desktop systems gives rise to the LAN being vulnerableto which of the following? War dialing

Which of the following phone attacks adds unauthorized charges to a telephone bill? Cramming

Which of the following cloud computing solutions will deliver software applications to a client either over the Internet or on a local area network? SaaS

Which of the following best describes the Platform as a Service (PaaS) cloud computing service model? PaaS delivers everything a developer needs to build an application onto the cloudinfrastructure.

Which of the following is not true regarding cloud computing? Cloud computing requires enduser knowledge of the physical location andconfiguration of the system that delivers the services.

Which of the following are true concerning the Virtual Desktop Infrastructure (VDI)? (Select two.)In the event of a widespread malware infection, the administrator can quickly reimage all user desktops on a few central servers.

User desktop environments are centrally hosted on servers instead of on individualdesktop systems.

You are purchasing a hard disk over the Internet from an online retailer. What does your browser use to ensure that others cannot see your credit card number on the Internet? SSL

IPSec is implemented through two separate protocols. What are these protocols called? AH and ESP

Which of the following network layer protocols provides authentication and encryption services for IP based network traffic? IPSec

Which of the following protocols can be used to securely manage a network device from a remote connection? SSH

Which of the following protocols are often added to other protocols to provide securetransmission of data? (Select two.)TLS and SSL

What is the primary function of the IKE protocol used with IPSec? Create a security association between communicating partners

FTPS uses which mechanism to provide security for authentication and data transfer? SSL

Which of the following protocols can TLS use for key exchange? (Select two.)DiffieHellman and RSA

SFTP uses which mechanism to provide security for authentication and data transfer? SSH

Which of the following is a secure alternative to FTP that uses SSL for encryption? FTPS

Which of the following is the best countermeasure against man-in-the-middle attacks? IPSec

Which protocol uses traps to send notifications from network devices? SNMP

You have been using SNMP on your network for monitoring and management. You areconcerned about the security of this configuration. Implement version 3 of SNMP.

Which of the following are improvements to SNMP that are included within SNMP version 3? (Select two.)Authentication for agents and managersEncryption of SNMP messages

Which of the following tools allow for remote management of servers? (Select two.)SSHTelnet

Which network service would you use to get the IP address from the FQDN hostname? DNS

You want to implement a protocol on your network that allows computers to find the IP address of a host from a logical name. Which protocol should you implement? DNS

Which protocol does HTTPS use to offer greater security in Web transactions? SSL

Which TCP/IP protocol is a secure form of HTTP that uses SSL as a sublayer for security? HTTPS

Which protocol is used for securely browsing a Web site? HTTPS

As network administrator you are asked to recommend a secure method of transferring data between hosts on a network. Which of the following protocols would you recommend? (Select two.)SFTPSCP

Which of the following protocols allows hosts to exchange messages to indicate problems with packet delivery? ICMP

Which of the following IPv6 addresses is equivalent to the IPv4 loopback address of 127. 0. 0. 1?:: 1

Which of the following describes an IPv6 address? (Select two.)Eight hexadecimal quartets128bit address

Which of the following correctly describe the most common format for expressing IPv6 addresses? (Select two.)32 numbers, grouped using colonsHexadecimal numbers

Which of the following are valid IPv6 addresses? Select all that apply. 141: 0: 0: 0: 15: 0: 0: 16384: 1319: 7700: 7631: 446A: 5511: 8940: 2552

Which of the following is a valid IPv6 address? FEC0:: AB: 9007

You are configuring a network firewall to allow SMTP outbound email traffic, and POP3 inbound email traffic. Which of the following TCP/IP ports should you open on the firewall? (Select two.)25110

Which port number is used by SNMP? 161

You want to close all ports associated with NetBIOS on your network firewalls to prevent attacks directed against NetBIOS. Which ports should you close? 135, 137139

Which of the following protocols uses port 443? HTTPS

Which of the following ports does FTP use to establish sessions and manage traffic? 20, 21

To transfer files to your company’s internal network from home, you use FTP. The administrator has recently implemented a firewall at the network perimeter and disabled as many ports aspossible. Now you can no longer make the FTP connection. You suspect the firewall is causing the issue. Which ports need to remain open so you can still transfer the files? (Select two.)2120

Using the Netstat command, you notice that a remote system has made a connection to your Windows Server 2008 system using TCP/IP port 21. Which of the following actions is the remote system most likely to be performing? Downloading a file

To access your company’s internal network from home, you have used Telnet. Security policy now prohibits the use of unsecure protocols such as Telnet. The administrator has recently implemented a firewall at the network perimeter and disabled many ports. Which port needs to be closed to prevent Telnet access from home? 23

You administer a Web server on your network. The computer has multiple IP addresses. They are 192. 168. 23. 8 to 192. 168. 23. 17. The name of the computer is www. westsim. com. You configured the Web site as follows:

• IP address: 192. 168. 23. 8• HTTP Port: 1030• SSL Port: 443

Users complain that they can’t connect to the Web site when they type www. westsim. com. What is the most likely source of the problem?

The HTTP port should be changed to 80.

To increase security on your company’s internal network, the administrator has disabled as many ports as possible. Now, however, though you can browse the Internet, you are unable to perform secure credit card transactions. Which port needs to be enabled to allow secure transactions?
443

Which of the following network services or protocols uses TCP/IP port 22?
SSH

Drag each IP port number on the left to its associated service on the right. Be aware that someport numbers may be used more than once. SNMP161 TCP and UDP

SSH22 TCP and UDP

TFTP69 UDP

SCP22 TCP and UDP

Telnet23 TCP

HTTPS443 TCP and UDP

HTTP80 TCP

FTP20 TCP

SMTP25 TCP

POP3110 TCP

Which of the following specifications identify security that can be added to wireless networks? (Select two.)802. 11i802. 1x

Which of the following wireless security methods uses a common shared key configured on the wireless access point and all wireless clients? WEP, WPA Personal, and WPA2 Personal

What is the least secure place to locate an access point with an omnidirectional antenna when creating a wireless cell? Near a window

What purposes does a wireless site survey serve? (Choose two.)To identify existing or potential sources of interference. To identify the coverage area and preferred placement of access points.

Which of the following offers the weakest form of encryption for an 802. 11 wireless network? WEP

Which of the following wireless network protection methods prevents the broadcasting of the wireless network name? SSID broadcast

Which of the following measures will make your wireless network invisible to the casual attacker performing war driving? Disable SSID broadcast

What encryption method is used by WPA for wireless networks? TKIP

Which of the following provides security for wireless networks? WPA

Which of the following features are supplied by WPA2 on a wireless network? Encryption

You need to secure your wireless network. Which security protocol would be the best choice? WPA2

On a wireless network that is employing WEP, which type of users are allowed to authenticate through the access points? Users with the correct WEP key

Which remote access authentication protocol allows for the use of smart cards forauthentication? EAP

Which of the following do switches and wireless access points use to control access through thedevice? MAC filtering

You have physically added a wireless access point to your network and installed a wireless networking card in two laptops running Windows. Neither laptop can find the network and you have come to the conclusion that you must manually configure the wireless access point (AP). Which of the following values uniquely identifies the network AP? SSID

You have a small wireless network that uses multiple access points. The network uses WPA and broadcasts the SSID. WPA2 is not supported by the wireless access points. You want to connect a laptop computer to the wireless network. Which of the followingparameters will you need to configure on the laptop? (Select two.)TKIP encryptionPreshared key

You need to configure a wireless network. You want to use WPA2 Enterprise. Which of the following components will be part of your design? (Select two.)AES encryption802. 1x

Which of the following locations will contribute the greatest amount of interference for a wireless access point? (Select two.)Near backup generatorsNear cordless phones

You need to place a wireless access point in your twostory building. While trying avoidinterference, which of the following is the best location for the access point? In the top floor

Which of the following recommendations should you follow when placing access points to provide wireless access for users within your company building? Place access points above where most clients are.

You want to implement 802. 1x authentication on your wireless network. Which of the following will be required? RADIUS

You want to implement 802. 1x authentication on your wireless network. Where would youconfigure passwords that are used for authentication? On a RADIUS server

You are the wireless network administrator for your organization. As the size of the organization has grown, you've decide to upgrade your wireless network to use 802. 1x authentication instead of preshared keys. You've decided to use LEAP to authenticate wireless clients. To do this, you configured a Cisco RADIUS server and installed the necessary Cisco client software on each RADIUS client. Which of the following is true concerning this implementation? The system is vulnerable because LEAP is susceptible to dictionary attacks.

You are the wireless network administrator for your organization. As the size of the organization has grown, you've decide to upgrade your wireless network to use 802. 1x authentication instead of preshared keys. To do this, you need to configure a RADIUS server and RADIUS clients. You want the server and the clients to mutually authenticate with each other. What should you do? (Select two. Each response is a part of the complete solution.)Configure all wireless access points with client certificates. Configure the RADIUS server with a server certificate.

Which EAP implementation is most secure? EAPTLS

Match each description on the left with the appropriate cloud technology on the right. Public cloudProvides cloud services to just about anyone.

Private cloudProvides cloud services to a single organization.

Community cloudAllows cloud services to be shared by several organizations.

Hybrid cloudIntegrates one cloud service with other cloud services.

You’ve decided to use a subnet mask of 255. 255. 192. 0 on the 172. 17. 0. 0 network to create four separate subnets. Which network IDs will be assigned to these subnets in this configuration? (Select two.)172. 17. 128. 0172. 17. 0. 0

Your organization uses a Web server to host an ecommerce site. Because this Web server handles financial transactions, you are concerned that it could become a prime target for exploits. You want to implement a network security control that will analyze the contents of each packet going to or from the Web server. The security control must be able to identify malicious payloads and block them. What should you do? Implement an applicationaware IPS in front of the Web server.

Drag the Web threat protection method on the left to the correct definition on the right. Prevents visiting malicious Web sitesWeb threat filtering

Prevents outsided attempts to access confidential informationAntiphishing software

Identifies and disposes of infected contentVirus blockers

Prevents unwanted email from reaching your networkGateway email spam blockers

Prevents visiting restricted Web sitesURL content filtering

Match the applicationaware network device on the right with the appropriate description on the left. Each description may be used once, more than once, or not at all. Applicationaware proxyImproves application performance

Applicationaware firewallEnforces security rules based on the application that is generating network traffic, instead ofthe traditional port and protocol

Applicationaware IDSAnalyzes network packets to detect malicious payloads targeted at applicationlayer services

You are investigating the use of Web site and URL content filtering to prevent users from visiting certain Web sites. Which benefits are the result of implementing this technology in your organization? (Choose two.)Enforcement of the organization’s Internet usage policyAn increase in bandwidth availability

You’ve just deployed a new Cisco router that connects several network segments in your organization. The router is physically located in a server room that requires an ID card to gain access. You’ve backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using a Telnet client with a user name of admin and a password of admin. You have used the MD5 hashing algorithm to protect the password. What should you do to increase the security of this device? (Select two.)Change the default administrative user name and password. Use an SSH client to access the router configuration.

You’ve just deployed a new Cisco router that connects several network segments in your organization. The router is physically located in a cubicle near your office. You’ve backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using an SSH client with a user name of

admin01 and apassword of You have used the MD5 hashing algorithm to protect the password. What should you do to increase the security of this device? Use SCP to back up the router configuration to a remote location.

You can use a variety of methods to manage the configuration of a network router. Match the management option on the right with its corresponding description on the left. (Each option can be used more than once.)SSLUses publickey cryptography

HTTPTransfers data in clear text

SSHUses publickey cryptography

TelnetTransfers data in clear text

Console portCannot be sniffed

Match the Active Directory component on the left with the appropriate description on the right. Each component may be used once, more than once, or not at all. Holds a copy of the Active Directory databaseDomain Controller

Manages access for a workstationComputer Object

Manages access for an employeeUser Object

Can be created to logically organize network resourcesOrganizational Unit

Cannot be moved, renamed, or deletedGeneric Container

Defines a collection of network resources that share a common directory databaseDomain

The owner of a hotel has contracted with you to implement a wireless network to provide Internet access for guests. The owner has asked that you implement security controls such that only paying guests are allowed to use the wireless network. She wants guests to be presented with a login page when they initially connect to the wireless network. After entering a code provided by the concierge atcheckin, guests should then be allowed full access to the Internet. If a user does not provide the correct code, they should not be allowed to access the Internet. What should you do? Implement a captive portal.

You need to implement a wireless network link between two buildings on a college campus. A wired network has already been implemented within each building. The buildings are 100 meters apart. What type of wireless antennae should you use on each side of the link? (Select two.)ParabolicHighgain

A salesperson in your organization spends most of her time traveling between customer sites. After a customer visit, she must complete various managerial tasks, such as updating your organization’s order database. Because she rarely comes back to your home office, she usually accesses the network from her notebook computer using WiFi access provided by hotels, restaurants, and airports. Many of these locations provide unencrypted public WiFi access, and you are concerned that sensitive data could be exposed. To remedy this situation, you decide to configure her notebookto use a VPN when accessing the home network over an open

wireless connection. Which key steps should you take when implementing this configuration? (Select two.)Configure the browser to send HTTPS requests through the VPN connection.

Configure the VPN connection to use IPsec.