Chapter 6 perimeter defense

ASSIGN BUSTER

6. 1. 9 Practice ExamsWhich 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 subnetWhich of the following IPv6 addresses is equivalent to the IPv4 loopback address of 127. 0. 0. 1?:: 1Which of the following describes an IPv6 address? Eight Hexadecimal quartets

128-bit addressWhich of the following correctly describe the most common format for expressing IPv6 addresses? (Select two.)32 numbers, grouped using colons

Hexadecimal numbersWhich of the following are valid IPv6 addresses? Select all that apply. 141: 0: 0: 0: 15: 0: 0: 1

6384: 1319: 7700: 7631: 446A: 5511: 8940: 2552Which of the following is a valid IPv6 address? FEC0:: AB: 9007Routers operate at what level of the Open System Interconnect model? Network layerYou'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 two172. 17. 0. 0

172. 17. 128. 06. 2. 6 Practice ExamYou have been using SNMP on your network for monitoring and management. You are concerned about the security of this configuration. What should you do? Implement version 3 of SNMPYou 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? DNSWhich of the following protocols allows hosts to exchange messages to indicate problems with packet delivery? ICMPYou are configuring a network firewall to allow SMTP outbound e-mail

traffic, and POP3 inbound e-mail traffic. Which of the following TCP/IP ports should you open on the firewall? (Select two.)25

110Which port number is used by SNMP161Which of the following ports does FTP use to establish sessions and manage traffic? 20, 21Using 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 fileTo 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 perfume secure credit card transactions. Which ports needs to be enabled to allows secure transaction? 443Which of the following network services or protocols uses TCP/IP port 22? SSHDrag each IP port number on the left to its associated service on the rightSNMP SSH

161 TCP AND UDP 22 TCP AND UDP

TFTP SCP

69 UDP 22 TCP AND UDP

TELNET HTTPS

23 TCP 443 TCP AND UDP

HTTP FTP

80 TCP 20 TCP

SMTP POP3

25 TCP 110 TCPWhich two of the following lists accurately describes TCP and UDP? UDP: connectionless, unreliable, unsequenced, low overhead.

TCP: connection-oriented, reliable, sequenced, high overhead. You are an application developer creating applications for a wide variety of customers.

In which of two the following situations would you select a " connectionless protocol? A company connects two network through an expensive WAN link. The communication media is reliable, but very expensive. They want to minimize connection times.

A gaming company wants to create a networked version of its latest game. Communication speed and reducing packet overhead are more important than error-free delivery. You want to maintain tight security on your internal network so you restrict access to the network through certain port numbers. If you want to allow users to continue to use DNS, which port should you enable? 53Your company's network provides HTTP, HTTPS, and SSH to remote employees. Which ports must be opened on the firewall to allow this traffic to pass? 80, 433 and 22Your network recently experienced a series of attacks aimed at the Telnet and FTP services. You have rewritten the security policy to abolish the unsecured services, and now you must secure the network using your firewall and routers. Which ports must be closed to prevent traffic directed to these two services? 23, 216. 3. 8 Practice ExamWhich of the following is the main difference between DoS attack and a DDoS attack? The DDoS attack uses zombie computersAn attacker sets up 100 drone computers that flood a DNS server with invalid requests. This is an example of which kind of attack? DDoSYou suspect that an Xmas tree attack is occurring on a system. Which of the following could result if you do not stop the attack? (Select two.)The system will unavailable to respond to legitimate requests.

The threat agent will obtain information about open ports on the system. You need to enumerate the devices on your network and display the configuration details of the network. Which of the following utilities should you use? NMAPAn attacker is conducting passive reconnaissance on a targeted company. Which of the following could he be doing? Browsing the organization's WebsiteWhich type of active scan turns off all flags in a TCP header? NullWhich of the following Denial of Service (DoS) attacks uses ICMP packets and will only be successful if the victim has less bandwidth than the attacker? Ping floodIn which of the following Denial of Service (DoS) attacks does the victim's system rebuild invalid UDP packets, causing the system to crash or reboot? TeardropA SYN packet is received by a server. The SYN packet has the exact same address for both the sender and receiver addresses, which is the address of the server. This is an example of what type of attack? Land attackWhich of the following is a form of denial of service attack that subverts the TCP three-way handshake process by attempting to open numerous sessions on a victim server but intentionally falling to complete the session by not sending the final required packet? SYN FloodWhich of the following is a form of denial of service attack uses spoofed ICMP packets to flood a victim with echo requests using a bounce/amplification network? SmurfA SYN attack or a SYN flood exploits or alters which element of the TCP three-way handshake? ACKWhen a Son flood is altered so that the SYN packets are spoofed in order to define the source and destination address as a single victim IP address, the attack is now called what? Land attackA surf attack requires all but which of the following elements to be implemented? Padded cellWhich of the following best describes the ping of death? An ICMP packet that is larger than 65, 536 bytes6. 4. 9 Practice ExamWhich of the following is the best countermeasure against man-in-the-middle attacks? IPSecWhat is modified in the most common form of spoofing on a typical IP Packet? Source addressWhich type of Denial of Service (DoS) attack occurs when a name server receives malicious or misleading data that the incorrectly maps host names and IP Addresses? DNS poisoningWhich of the following describes a man-in-the-middle attack? A false server intercepts communications from a client by impersonating the intended server. Capturing packets as they travel from one host to another with the intent of altering the contents of the packets is a form of which security concerns? Man-in-the-middle attackWhen the TCP/IP session state is manipulated so that a third party is able to insert alternate packets into the communications stream, what type of attack has occurred? HijackingWhat is the goal of a TCP/IP hijacking attack? Executing commands or accessing resources on a system the attacker does not otherwise have authorization to accessWhich of the following is NOT a protection against session hijacking? DHCP reservationsWhich of the following is the most effective protection against IP packet spoofing on a private network? Ingress and egress filtersWhile using the internet, you type the URL of one of your favorite sites in the browser. Instead of going to the correct site, however, the browser displays a completely different website. When you use the IP address of the Web server, the correct site displayed. Which type of attack has likely occurred. DNS poisoningWhich of the following attacks tries to associate an incorrect MAC address with a known IP address? ARP poisoningWhat are the most common network traffic captured and used in a reply attack? AuthenticationWhen a malicious user captures authentication traffic and replays it against the network later, what is the security problem you are most concerned about? An unauthorized user gained access to sensitive resourcesA router on the border of your network detects a packet with a source address that is from an internal client but the packet was received in the Internet-facing interface. This is an example of what form of attack? SpoofingAn attacker uses an exploit to push a modified host file to clients systems. This host file redirects traffic from legitimate tax preparation sites to malicious sites to gather personal and financial information. What kind of exploit has been used. DNS poisoning

Pharming6. 5. 8 Practice ExamWhich of the following is a privately controlled portion of a network that is accessible to some specific external entities? ExtranetYou 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? All-in-one security applianceYou are implementing security at a local high school that is concerned with student accessing inappropriate material on the Internet from the library's computers. The students will use the computers 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 categoriesMatch the application-aware network device on the right with the appropriate description on the left. Application-aware proxy

Improves application performanceApplication-aware firewall

Enforces security rules

Application-aware IDS

Analyzes network packets

6. 6. 5 Practice ExamYour company has a connection to the internet that allows users to access the internet. You also have a web server and an email

server that you want to make available to the internet users. You want to created a DMZ for these two servers. Which type of device should you use to create the DMZ? Network-based firewallYou 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 firewalls 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 a database server for retrieving product, customer, and order information. How should you place devices on the network to best protect the servers? (Select two.)Put the database server on the private network.

Put the Web server inside the DMZOf the following security zones, which one can serve as a buffer network between a private secured network and the untrusted Internet? DMZWhich of the following is likely to be located in a DMZ? FTP ServerMembers of the Sales team use laptops to connect to the company network. While travelling, 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 anti-virus software and the latest operating system patches have been installed. Which solution should you use? NACIn which of the following situations would you most likely implement a demilitarized zone (DMZ)? You want to protect public Web Server from attack. Which of the following terms describes a network device that is exposed to attacks and has been hardened against those attacks? Bastion or sacrificial host6. 7. 5 Practice ExamsWhich of the following is a firewall function? Packet filteringWhich of the following are characteristics of a circuit-level gateway? (Select two.)Filter based on sessions

StatefulWhich of the following are characteristics of a packet filtering firewall? (Select two.)Stateless,

Filter IP address and portYou 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-levelYou provide Internet access for a local school. You want to control Internet access based on user, and prevent access to specific URLs. Which type of firewall should you install? Application levelWhich of the following is the best device to deploy to protect your private network from a public untrusted network? FirewallYou have been given a laptop to use for work. You connect the laptop to your company network, use it from home, and use it while travelling. You want to protect the laptop from Internet-based attacks. Which solution should you use? Host based firewallYou connect your computer to a wireless network available at the local library. You find that you can access all websites you want on the Internet expect for two. What might be causing the problem? A proxy server is blocking access to the web sites. Which of the following functions are performed by proxies? (Select two.)Cache web pages

Block employees from accessing certain Web sites. Which of the following are true of a circuit proxy filter firewall? (Select two.)Verifies sequencing of session packets.

Operates at the Session LayerWhich of the following does router acting as a firewall use to control which packets are forwarded or dropped? ACLYou have a router that is configured as a firewall. The router is a layer 3 device only. Which of the following does the router use for identifying allowed or denied packets? IP addressYou 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. Port number

Source address of a packet

Destination address of a packet. 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 DMZWhich of the following firewall types can be a proxy between servers and clients? (Select two.)Circuit proxy filtering firewall

Application layer firewall6. 8. 4 Practice ExamYou 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 IP 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 NATYou 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 provided you with 5 additional registered IP addresses to support these new servers but you don't want the public to access this server 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 outside. Which method of NAT translation should you implement for these 5 servers? StaticYou 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? DynamicWhich 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. 255Which of the following networking devices or services prevents the use of IPSec in most cases? NAT6. 9. 7 Practice ExamYou 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 to the private network through a single server. Which solution should you implement? VPN concentratorA VPN is used primarily for what purpose? Support secured communications over an untrusted networkWhich VPN protocol typically employs IPSec as its data encryption mechanism? L2TPWhich statement best describes IPSec when used in tunnel mode? The entire data packet, including headers, is encapsulatedWhich IPSec sub protocol provides data encryption? ESPWhich of the following is " NOT" a VPN tunnel protocol? RADIUSWhich is the best countermeasure for someone attempting to view your network traffic? VPNPPTP (Point to Point Tunneling Protocol) is quickly becoming obsolete because of what VPN protocol? L2TP (Layer 2 Tunneling Protocol)What is the primary use of tunneling? Supporting private traffic through a public communication mediumIn addition to Authentication Header (AH), IPSec is comprised of what other service? Encapsulating Security Payload (ESP)A salesperson in your organization spends most of her time traveling between customer sites. After a customer visit she must complete various managerial task.

Which key steps should you take when implementing this configuration?

select twoConfigure the VPN connection to use IPsec

Configure the browser to send HTTPS requests through the VPN connection6. 10. 5 Practice ExamWhich of the following is a valid security measure to protect email from viruses? Use blockers on email gatewaysWhich of the following prevents access based on website ratings and classifications? Content filterDrag the web threat protection method on the left to the correct definition on the right. Prevents visiting malicious web sites

Web threat filteringPrevents outside attempts to access confidential information

Anti-phising software

Identifies and disposes of infected content

Virus blockers

Prevents unwanted email from reaching your network

Gateway email spam blocker

prevents visiting restricted websites

URL content filtering

You are investigating the use of web site URL content filtering to prevent users from visiting certain web sites. Which benefits are the result of implement this technology in your organization? choose twoEnforcement of the organizations internet usage policy

An increase in bandwidth availability6. 11. 4 Practice ExamYou have a company network with a single switch. All devices connect to the network through the switch. You want to control which devices will be able to connect to your network. For devices that do not have the latest operating system patches, you want to prevent access to all network devices except for a special server that holds the patches that the computers need to download. Which of the following components will be part of your solution? (Select two.)802. 1x authentication

Remediation serversWhich step is required to configure a NAP on a Remote Desktop (RD) Gateway server? Edit the properties for the server and select " Request clients to send a statement of health." In a NAP system, what is the function of the System Health Validator? Compare the statement of health submitted by the client to the health requirementsHow does the IPsec NAP enforcement differ from other NAP enforcement methods? Clients must be issues a valid certificate before a connection to the private network is allowed6. 12. 8 Practice ExamWhich 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 PersonalWhich of the following offers the WEAKEST form of encryption for an 802. 11 wireless network? WEPWhich of the following features are supplied by WPA2 on a wireless network? EncryptionYou need to secure your wireless network. Which security protocol would be the best choice? WPA2You need to configure a wireless network. You want to use WPA2 Enterprise. Which of the following components will be part of your design? select two802. 1x

AES encryptionWhich of the following locations will contribute the greatest amount of interference for a wireless access point? (Select two.)Near backup generators

Near cordless phonesYou need to implement a wireless network link between two buildings on a college campus. A wired network has already been implement within each buildin. The buildings are 100 meters apart. What type of wireless antennae should you use on each side of the link? select twoHigh gain

ParabolicHow does WPA2 Differ from WPA? WPA2 uses AES for encryption WPA uses TKIPYou need to configure the wireless network card to connect to your network at work. The connection should use a user name and password for authentication with AES encryption. What should you do? Configure the connection to use WPA2-Enterprise. Match the wireless networking security standards on the left to its associated characteristics on the right. Short initialization vector makes key vulnerable

WEP

Uses AES for encryption

WPA2

Uses RC4

WEP

Uses TKIP

WPA

Uses CBC-MAC

WPA2

Uses CCMP

WPA2You need to add security for your wireless network. You would like to use the most secure method. Which method should you implement? WPA2Which of the following is used on a wireless network to identify the network name? SSIDWhich of the following are true about Wi-Fi protected access 2 (WPA2)? select twoUses AES for encryption and CBC-MAC integrity

Upgrading from a network using WEP typically requires installing new hardwareWIMAX is an implementation of which IEEE committee? 802. 16You want to connect a laptop computer running windows 7 to a wireless network. What should you do? Configure the connection with a preshared key and AES encryption6. 13. 5 Practice ExamsYour company security policy states that wireless networks are not to be used because of the potential security risk they present to your network. One day you find that an employee has connected a wireless access point to the network in his office. What type of security risk is this? Rogue access pointWhich of the following describes marks that attackers place outside a building to identify an open wireless network? War chalkingThe process of walking around an office building with an 802. 11 signal detector known as what? War drivingWhich of the following best describes Bluesnarfing? Unauthorized viewing calendar, e-mails, and messages on a mobile deviceWhich of the following sends unsolicited business cards and messages to a Bluetooth device? BluejackingWhich of the following is the best protection to prevent attacks on mobile phone through the Bluetooth protocol? Disable Bluetooth on phoneYou are troubleshooting a wireless connectivity issue in a small office. You determine that the 2. 4 GHz cordless phones used in the office are interfering with the wireless network transmissions. If the cordless phones are causing the interference, which of the following wireless standard could the network be using? (Select two.)802. 11g
Bluetooth

Your organization uses an 802. 11b wireless network. Recently, other tenants installed the following equipment in your building:

A wireless television distribution system running at 2. 4Ghz

A wireless phone system running at 5. 8Ghz

A wireless phone system running at 900Mhz

An 802. 11a wireless network running in the 5. 725 - 5. 850Ghz frequency range

An 802. 11j wireless network running in the 4. 9 - 5. 0Ghz frequency range

Since this equipment was installed, your wireless network has been experiencing significant interference. Which system is to blame?

The wireless TV system. Which of the following best describes an EVIL TWIN? An access point that configured to mimic a valid access point to obtain logon credentials and other sensitive informationNetwork packet sniffing is often used to gain the information needed to conduct more specific and detailed attacks. Which of the following is the best defense against packet sniffing? EncryptionWhich of the following common network monitoring or diagnostic activity can be used as a passive malicious attack? SniffingYou are concerned that the wireless access points may have been deployed within your organization without authorization. What should you do? select twoCheck the MAC addresses of the devices connected to your wired switch
Conduct a site surveyMatch the malicious interference type on the right with the appropriate characteristic on the left. Spark Jamming
Repeatedly blasts receiving equipment with high-intensinty, short-duration RF burst at a rapid paceRandom Noise Jamming
Produces RF signals using random amplitudes and Frequencies

Random Pulse Jamming

Uses Radio signal pulses of random amplitudes and frequencies

An attacker has hidden and NFC reader behind and NFC-based kiosk in and airport. What kind of attack has occurredNFC relay attackYou are implementing a wireless network in a dentist office. The dentist practice is small, so you choose to use an inexpensive, consume-grade access point. what should you do to reduce risk? Disable WPS in the access points configurations6. 14. 9 Practice ExamWhich of the following measures will make your wireless network invisible to the casual attacker performing war driving? Disable SSID broadcastWhich remote access authentication protocol allows for the use of smart cards for authentication? EAPWhich of the following do switches and wireless access points use to control access through the device? MAC filteringYou want to implement 802. 1 x authentications on your wireless network. Where would you configure passwords that are used for authentication? On a RADIUS serverYou 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 pre-shared keys.

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 pre-shared keys.

What should you do? select twoConfigure all wireless access points with client certificates.

Configure the RADIUS server with a server certificateWhich EAP implementation is most secure? EAP-TLSWhich of the following features on a wireless network allows or rejects client connections based on the hardware address? MAC address filteringYou've just finished installing a wireless access point for a client. What should you do to prevent unauthorized users from accessing the access point (AP) configuration utility? Change the administrative password on the AP. You are concerned about sniffing attacks on your wireless network. Which of the following implementations offers the best countermeasure to sniffing? WPA2 with AESWhat is the LEAST secure place to locate an access point with an omni-directional antenna when creating a wireless cell? Near a windowWhat purpose does a wireless site survey server? (Choose two.)To identify the coverage of area and preferred placement of access points.

To identify existing or potential sources of interference, You need to place a wireless access point in your two-story building. While trying to avoid interference, which of the following is the best location for the access point? in the top floorYou are designing a wireless network implementation for a small business. The business deals with sensitive customer information, so data emanation must be reduced as much as possible. place antenna type to location. A-DIRECTIONAL

B-DIRECTIONAL

C-OMNIDIRECTIONAL

D-DIRECTIONAL

E-DIRECTIONAL

F-DIRECTIONAL

G-DIRECTIONALThe owner of a hotel has contracted with you to implement a wireless network to provide internet access for guest. what should you do?

Implement a captive portal ONCHAPTER 6 PERIMETER DEFENSE

SPECIFICALLY FOR YOUFOR ONLY$13. 90/PAGEOrder NowTags:

- Bluetooth
- Vector