Mid2 chap6 m82

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 ff. actions is the remote system most likely to be performing? Downloading a file

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

You are an application developer creating applications for a wide variety of customers. In which of two the ff. situations would you select a “ connectionless protocol? 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. A company connects two network through an expensive WAN link. The communication media is reliable, but very expensive. They want to minimize connection times.

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

You are configuring a network firewall to allow SMTP outbound e-mail traffic, and POP3 inbound e-mail traffic. Which of the ff. TCP/IP ports should you open on the firewall? (Select two.)Port 25, Port 110

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 perfume secure credit card transactions. Which ports needs to be enabled to allows secure transaction? Port 443

Which two of the ff. lists accurately describes TCP and UDP? TCP: connection-oriented, reliable, sequenced, high overhead. UDP: connectionless, unreliable, unsequenced, low overhead.

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

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? Port 53

Which of the ff. are valid IPv6 addresses? Select all that apply. 141: 0: 0: 0: 15: 0: 0: 1, 6384: 1319: 7700: 7631: 446A: 5511: 8940: 2552

You 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 SNMP

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

Your 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? Port 80, 433 and 22

Your 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? Port 23 and 21

Routers operate at what level of the Open System Interconnect model? Network layer

An attacker sets up 100 drone computers that flood a DNS server with invalid requests. This is an example of which kind of attack? DDoS

In which of the ff. Denial of Service (DoS) attacks does the victim’s system rebuild invalid UDP packets, causing the system to crash or reboot? Teardrop

An attacker is conducting passive reconnaissance on a targeted company. Which of the ff. could he be doing? Browsing the organization’s Website

Which of the ff. attacks tries to associate an incorrect MAC address with a known IP address? ARP poisoning

Which of the ff. best describes the ping of death? An ICMP packet that is larger than 65, 536 bytes

A 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 attack

Which of the ff. is a form of denial of service attack uses spoofed ICMP packets to flood a victim with echo requests using a bounce/amplification network? Smurf

You suspect that an Xmas tree attack is occurring on a system. Which of the ff. 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.

What are the most common network traffic captured and used in a reply attack? Authentication

A SYN attack or a SYN flood exploits or alters which element of the TCP three-way handshake? ACK

A 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? Spoofing

Which of the ff. describes a man-in-the-middle attack? A false server intercepts communications from a client by impersonating the intended server.

Which of the ff. Denial of Service (DoS) attacks uses ICMP packets and will only be successful if the victim has less bandwidth than the attacker? Ping flood

Which of the ff. could easily result in a denial of service attack if the victimized system had too little free storage capacity? Spam

Which type of active scan turns off all flags in a TCP header? Null

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? All-in-one security appliance

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

You 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 categories

Which of the ff. is likely to be located in a DMZ? FTP Server

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

Of the ff. security zones, which one can serve as a buffer network between a private secured network and the untrusted Internet? 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 Web server inside the DMZ. Put the database server on the private network.

Which of the ff. terms describes a network device that is exposed to attacks and has been hardened against those attacks? Bastion or sacrificial host

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 firewalls to create a DMZ. Place the Web server inside the DMZ, and the private network behind the DMZ.

Members 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? NAC

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

Which of the ff. is the best device to deploy to protect your private network from a public untrusted network? Firewall

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. Source address of a packet, Port number, Destination address of a packet.

Which of the ff. firewall types can be a proxy between servers and clients? (Select two.)Circuit proxy filtering firewall, Application layer firewall

You 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 level

Which of the ff. does router acting as a firewall use to control which packets are forwarded or dropped? ACL

Which of the ff. are true of a circuit proxy filter firewall? (Select two.)Operates at the Session Layer. Verifies sequencing of session packets.

You 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 firewall

Which of the ff. are characteristics of a circuit-level gateway? (Select two.)Stateful, Filter based on sessions

Which of the ff. is a firewall function? Packet filtering

Which of the ff. functions are performed by proxies? (Select two.)Cache web pages, Block employees from accessing certain Web sites.

You have a router that is configured as a firewall. The router is a layer 3 device only. Which of the ff. does the router use for identifying allowed or denied packets? IP address

Which of the ff. are characteristics of a packet filtering firewall? (Select two.)Stateless, Filter IP address and port

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

You 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.

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 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 NAT

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

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

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 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? Static

Which of the ff. is “ not” a benefit of NAT? Improving the throughput rate of traffic

Which is the best countermeasure for someone attempting to view your network traffic? VPN

In addition to Authentication Header (AH), IPSec is comprised of what other service? Encapsulating Security Payload (ESP)

A VPN is used primarily for what purpose? Support secured communications over an untrusted network

Which statement best describes IPSec when used in tunnel mode? The entire data packet, including headers, is encapsulated

What is the primary use of tunneling? Supporting private traffic through a public communication medium

Which IPSec sub protocol provides data encryption? ESP

Which of the ff. is “ not” a VPN tunnel protocol? RADIUS

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 to the private network through a single server. Which solution should you implement? VPN concentrator

Which VPN protocol typically employs IPSec as its data encryption mechanism? L2TP

PPTP (Point to Point Tunneling Protocol) is quickly becoming obsolete because of what VPN protocol? L2TP (Layer 2 Tunneling Protocol)

Which of the ff. prevents access based on website ratings and classifications? Content filter

Which of the ff. is a valid security measure to protect e-mail from viruses? Use blockers on e-mail gateways1. How does IPsec Nap enforcement differ from other NAP enforcement methods? Clients must be issued a valid certificate before a connection to the private network is allowed.

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 requirements

You 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 ff. components will be part of your solution? (Select two.)802. 1x authentication, Remediation servers

Which 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.”

Which of the ff. describes marks that attackers place outside a building to identify an open wireless network? War chalking

A user calls to report that she is experiencing intermittent problems while accessing the wireless network from her laptop computer. While she normally works from her office, today she is trying to access the wireless network from a conference room which is across the hall and next to the elevator. What is the most likely cause of her connectivity problem? Interference is affecting the wireless signal.

The process of walking around an office building with an 802. 11 signal detector known as what? War driving

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

A wireless television distribution system running at 2. 4GhzA wireless phone system running at 5. 8GhzA wireless phone system running at 900MhzAn 802. 11a wireless network running in the 5. 725 – 5. 850Ghz frequency rangeAn 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 ff. best describes an evil twin? An access point that is added to the network by an internal employee to provide unauthorized network access.

Which of the ff. common network monitoring or diagnostic activity can be used as a passive malicious attack? Sniffing

Network packet sniffing is often used to gain the information needed to conduct more specific and detailed attacks. Which of the ff. is the best defense against packet sniffing? Encryption

Your 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 point

Which of the ff. is the best protection to prevent attacks on mobile phone through the Bluetooth protocol? Disable Bluetooth on phone

You 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 ff. wireless standard could the network be using?(Select two.) 802. 11b, Bluetooth

Which of the ff. best describes Bluesnarfing? Unauthorized viewing calendar, e-mails, and messages on a mobile device

Which of the ff. sends unsolicited business cards and messages to a Bluetooth device? Bluejacking

Which of the ff. features are supplied by WPA on a wireless network? Encryption

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

How does WPA2 Differ from WPA? WPA2 uses AES for encryptionWPA uses TKIP

You 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.

You are concerned about sniffing attacks on your wireless network. Which of the ff. implementations offers the best countermeasure to sniffing? WPA2 with AES

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

Which of the ff. 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.

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

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

You need to add security for your wireless network. You would like to use the most secure method. Which method should you implement? WPA2

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

WiMAX is an implementation of which IEEE committee? 802. 16

You'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.

Which of the ff. features on a wireless network allows or rejects client connections based on the hardware address? MAC address filtering

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