Net def final

FalseFirewalls can protect against employees copying confidential data from within the network. True/False

FalseSoftware firewalls are usually more scalable than hardware firewalls. True/False

FalseStateless packet filtering keeps a record of connections that a host computer has made with other computers. True/False

FalseGenerally, connections to instant-messaging ports are harmless and should be allowed. True/False

FalseSince ICMP messages use authentication, man-in-the-middle attacks cannot be successful. True/False

FalseA dual-homed host has a single NIC with two MAC addresses. True/False

TrueA screened host has a router as part of the configuration. True/False

FalseReverse firewalls allow all incoming traffic except what the ACLs are configured to deny. True/False

FalseProxy servers take action based only on IP header information. True/False

FalseThe TCP normalization feature forwards abnormal packets to an administrator for further inspection. True/False

TrueAnother name for a VPN connection is tunnel. True/False

TrueHardware VPNs create a gateway-to-gateway VPN. True/False

FalseStandards and protocols used in VPNs are in their infancy and seldom used. True/False

TrueIPsec has become the standard set of protocols for VPN security. True/False

FalseIf you use Windows RRAS for your VPN, you will need a third-party RADIUS server if you want to use RADIUS for authentication. True/False

FalseThe term Internet and World Wide Web are different terms that mean the same thing. True/False

TrueComputers on the Internet are identified primarily by their IP address. True/False

TrueSQL injection attacks are isolated to custom applications, so administrators can prevent them. True/False

TrueThe objective of a phishing attack is to entice e-mail recipients to click a bogus link where personal information can be stolen. True/False

FalseWindows Basic Authentication requires that users enter a username and password and the password is transmitted using a hashing algorithm. True/False

C. firewall applianceThe Cisco PIX line of products is best described as which of the following? A. software firewallB. PC with firewall installedC. firewall applianceD. VPN gateway

B. not dependent on a conventional OSWhich of the following is an advantage of hardware firewalls? A. not scalable compared to software firewallsB. not dependent on a conventional OSC. less expensive than software firewallsD. easy to patch

C. data patternsWhich of the following is NOT a criteria typically used by stateless packet filters to determine whether or not to block packets. A. IP addressB. portsC. data patternsD. TCP flags

D. proxy serverWhat should a company concerned about protecting its data warehouses and employee privacy might consider installing on the network perimeter to prevent direct connections between the internal network and the Internet? A. routerB. filteringC. ICMP monitorD. proxy server

C. NATWhich element of a rule base conceals internal names and IP addresses from users outside the network? A. trackingB. filteringC. NATD. QoS

B. employees can use instant-messaging only with external network usersWhich of the following is NOT among the common guidelines that should be reflected in the rule base to implement an organization’s security policy? A. only authenticated traffic can access the internal networkB. employees can use instant-messaging only with external network usersC. the public can access the company Web serversD. employees can have restricted internet access

A. 30 rulesWhat is a suggested maximum size of a rule base? A. 30 rulesB. 300 rulesC. 10 rulesD. 100 rules

C. 80, 443Which two ports should packet-filtering rules address when establishing rules for Web access? A. 143, 80B. 25, 110C. 80, 443D. 423, 88

B. DNSWhat service uses UDP port 53? A. SMTPB. DNSC. ICMPD. TFTP

C. TCP 21 control, TCP 20 dataWhat are the to standard ports used by FTP along with their function? A. UDP 23 control, TCP 20 dataB. UDP 20 data, TCP 21 controlC. TCP 21 control, TCP 20 dataD. TCP 23 data, TCP 21 control

A. Teredo tunnelingWhich of the following is a method for supporting IPv6 on IPv4 networks until IPv6 is universally adopted? A. Teredo tunnelingB. ICMPv6 encapsulationC. IPsec tunnelingD. SMTP/S tunneling

D. load-balancing softwareWhich of the following is best described as software that prioritizes and schedules requests and then distributes them to servers based on each server’s current load and processing power. A. server pooling softwareB. traffic distribution filterC. priority server farmD. load-balancing software

C. DDoSIn what type of attack are zombies usually put to use? A. buffer overrunB. virusC. DDoSD. spoofing

D. reverse firewallWhat should you consider installing if you want to inspect packets as they leave the network? A. security workstationB. RIP routerC. filtering proxyD. reverse firewall

A. screened subnet DMZWhich type of firewall configuration protects public servers by isolating them from the internal network? A. screened subnet DMZB. dual-homed hostC. screening routerD. reverse firewall

B. proxy serverWhich type of security device can speed up Web page retrieval and shield hosts on the internal network? A. caching firewallB. proxy serverC. caching-only DNS serverD. DMZ intermediary

C. may require client configurationWhich of the following is a disadvantage of using a proxy server? A. shields internal host IP addressesB. slows Web page accessC. may require client configurationD. can’t filter based on packet content

B. a computer on the perimeter network that is highly protectedWhich of the following best describes a bastion host? A. a host with two or more network interfacesB. a computer on the perimeter network that is highly protectedC. a computer running a standard OS that also has a proxy software installedD. a computer running only embedded firmware

B. they are not routable on the InternetWhich of the following is true about private IP addresses? A. they are assigned by the IANAB. they are not routable on the InternetC. they are targeted by attackersD. NAT was designed to conserve them

B. port address translationWhich type of translation should you use if you need 50 computers in the corporate network to be able to access the Internet using a single public IP address? A. one-to-one NATB. port address translationC. one-to-many NATD. DMZ proxy translation

D. authentication serverWhich of the following is NOT an essential element of a VPN? A. VPN serverB. tunnelC. VPN clientD. authentication server

C. have more security vulnerabilities than software VPNsWhich of the following is NOT true about a hardware VPN? A. should be the first choice for fast-growing networksB. can handle more traffic than software VPNsC. have more security vulnerabilities than software VPNsD. create a gateway-to-gateway VPN

D. encapsulationWhich activity performed by VPNs encloses a packet within another packet? A. address translationB. encryptionC. authenticationD. encapsulation

C. SSLWhich VPN protocol leverages Web-based applications? A. PPTPB. L2TPC. SSLD. IPsec

B. L2TPWhich VPN protocol uses UDP port 1701 and does not provide confidentiality and authentication? A. IPsecB. L2TPC. PPTPD. SSL

C. IPsecWhich VPN protocol works at Layer 3 and can encrypt the entire TCP/IP packet? A. PPTPB. L2TPC. IPsecD. SSL

C. IPsec driverWhich IPsec component is software that handles the taks of encrypting, authenticating, decrypting and checking packets? A. ISAKMPB. IKEC. IPsec driverD. Oakley protocol

D. adds a hashed message authentication codeWhich of the following is an improvement of TLS over SSL? A. requires less processing powerB. uses a single hashing algorithm for all the dataC. uses only asymmetric encryptionD. adds a hashed message authentication code

B. VPN quarantineWhat was created to address the problem of remote clients not meeting an organization’s VPN security standards? A. split tunnelingB. VPN quarantineC. IPsec filtersD. GRE isolation

B. it was established in the mid-1960sWhich of the following is true about the Internet? A. it is the same as the World Wide WebB. it was established in the mid-1960sC. it was developed by a network of banks and businessesD. it was originally built on an extended star topology

C. NAPWhich of the following is a highly secure public facility in which backbones have interconnected data lines and routers that exchange routing and traffic data? A. ISPB. POPC. NAPD. NSF

C. anycast addressingWhat feature of the 13 DNS root servers enables any group of servers to act as a root server? A. multicast addressingB. broadcast addressingC. anycast addressingD. unicast addressing

D. SQL injectionWhat type of attack involves plaintext scripting that affects databases? A. phishingB. ActiveX controlC. Java appletD. SQL injection

B. phishingWhat type of attack displays false information masquerading as legitimate data? A. Java appletB. phishingC. buffer overflowD. SQL injection

C. use standard naming conventionsWhich of the following is NOT a step you should take to prevent attackers from exploiting SQL security holes? A. limit table accessB. use stored proceduresC. use standard naming conventionsD. place the database server in a DMZ

B. pharmingWhich variation on phishing modifies the user’s host file to redirect traffic? A. spear phishingB. pharmingC. DNS phishingD. hijacking

A. primaryWhat type of DNS server is authoratative for a specific domain? A. primaryB. secondaryC. read-onlyD. initial

B. updating a secondary DNS serverWhat is a zone transfer? A. the movement of e-mail from one domain to anotherB. updating a secondary DNS serverC. backing up an SQL data fileD. coping host file data to another system

D. split-DNS architectureWhat type of DNS configuration prevents internal zone information from being stored on an Internet-accessible server? A. read-only zoneB. anti-phishing DNSC. caching DNS zoneD. split-DNS architecture

C. use the default standard Web page error messagesWhich of the following is NOT a recommended security setting for Apache Web servers? A. harden the underlying OSB. create Web groupsC. use the default standard Web page error messagesD. disable HTTP traces

perimeterA firewall can consist of all devices postioned on the network _____.

ruleACLs filter packets by using a _____ base to determine whether to allow a packet to pass.

handshakeThe ACK flag is normally sent at the end of the three-way _____ to indicate that a connection is established.

filterA primary objective of a rule base is to _____ communications based on complex rules.

DMZThe rule base should permit access to public servers in the _____ and enable users to access the Internet.

screeningA _____ router determines whether to allow or deny packets based on their source and destination IP addresses.

hostIn a screened _____ setup, a router is added between the host and the Internet to carry out IP packet filtering.

publiclyA DMZ is a subnet of _____ accessible servers placed outside the internal network.

hardenYou can _____ a bastion host by removing unnecessary accounts and services.

endpointsNetwork gateways are _____ of the VPN connection.

ExchangeThe Internet Key _____ protocol enables computers to make an SA.

XORTLS splits the input data in half and recombines it using a(n) _____ function.

NAPsThe internet tier system starts with a backbone network connected via _____ to regional Internet service providers.

Routers_____ direct network traffic to its destionation on the Internet using tables and protocols.

spoofingThe lack of authentication for computers on the Internet make IP _____ possible, which is change in the IP addresses in the headers of malicious packets.

cacheDNS _____ poisoning streers unsuspecting victims to a server of the attacker’s choice instead of the intended Web site.

Botnets_____ are networks of zombie computers that magnify the scope and intensity of an attack.

stackA critical buffer component is the function _____ and buffer overflows are usually aimed at this component.

JavaA _____ applet is a small program sometimes used as embedded code in Web pages.

DNSSECThe goal of _____ is to provide authentication of DNS data and ensure integrity of DNS data.

proxy serversoftware that forwards network packets and caches Web pages to speed up network performance

socketthe end point of a computer-to-computer connection defined by an IP address and port address

cleanup rulea packet-filtering rule that comes last in a rule base and covers any packets that have not been covered by preceding rules

firewall appliancehardware devices with firewall functionality

stateless packet filterssimple filters that determine whether to allow or block packets based on information in protocol headers

rule basethe collection of rules that filter traffic at an interface of a firewall

many-to-one NATa process that uses the source and destination TCP and UDP port addresses to map traffic between internal and external hosts

one-to-one NATthe process of mapping one internal IP address to one external IP address

dual-homed hosta computer configured with more than one network interface

screened hosta host in which one interface is connected to an internal network and the other interface is connected to a router to an untrusted network

load-balancing softwaresoftware that prioritizes and schedules requests and then distributes them to servers in a server clusted based on each server’s current load and processing power

screening routera router placed between an untrusted network and an internal network

IKEa form of key exchange used to encrypt and decrypt data as it passes though a VPN tunnel

Kerberosan IETF standard for secure authentication of requests for resource access

ESPan IPsec protocol that encrypts the header and data components of TCP/IP packets

SSLa protocol developed by Netscape Communications Corporation as a way of enabling Web servers and browsers to exchange encrypted information

IPseca set of standard procedures that the IETF developed for enabling secure communication on the Internet

GREa nonproprietary tunneling protocol that can encapsulate a variety of Network layer protocols

anycast addressinga network addressing scheme that allows DNS services to be decentralized among a group of servers, regardless of their location

split brain DNS architecturea network architecture that uses a single DNS domain with a DNS server on the organization’s DNZ for Internet services and a DNS server on the internal network for service to internal hosts