4 - Communications and network Security

Test ID: 176805791

Question #1 of 131

Question ID: 1105243

Which protocol uses encryption to protect transmitted traffic and supports the transmission of multiple protocols?

✗ **A)** HTTP

✗ **B)** HTTPS

✓ **C)** L2TP over IPSec

✗ **D)** FTP

Explanation

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that is used to transmit traffic on virtual private network (VPN) connections. L2TP supports multiple protocols, such as Transmission Control Protocol (TCP), Internet Protocol (IP), Internetwork Packet Exchange (IPX), and Systems Network Architecture (SNA). L2TP is based on two older tunneling protocols: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F). When L2TP is implemented with Internet Protocol Security (IPSec), it also provides encryption.

Hypertext Transfer Protocol (HTTP) transmits information in clear text. Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) to encrypt HTTP traffic. HTTPS only supports the encryption of HTTP traffic. File Transfer Protocol (FTP) transmits data in clear text.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, VPN

Question #2 of 131

Question ID: 1105176

Which type of firewall is considered a second-generation firewall?

✗ **A)** packet-filtering firewall

✗ **B)** dynamic packet-filtering firewall

✗ **C)** kernel proxy firewall

✓ **D)** proxy firewall

Explanation

A proxy firewall is a second-generation firewall, meaning it was the second type created. Other types followed.

A kernel proxy firewall is a fifth-generation firewall, and a packet-filtering firewall is a first-generation firewall. A dynamic packet-filtering firewall is a fourth-generation firewall.

Third-generation firewalls typically use a system that examines the state and context of incoming packets. This type of firewall tracks protocols that are considered connectionless, such as User Datagram Protocol (UDP).

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #3 of 131

Question ID: 1105148

Consider the following IP address:

157.175.12.10/22

How many bits will be used for the host portion of this address?

✗ **A)** 22

✓ **B)** 10

✗ **C)** 6

✗ **D)** 16

Explanation

Ten bits are used for the host portion of 157.175.12.10/22.

The IP address 157.175.12.10/22 is an example of a "slash x" network, also known as Classless Interdomain Routing (CIDR) notation. CIDR is a way of applying a subnet mask to an IP address to optimize address space while ignoring

the traditional IP class categories. With classful addressing, 157.175.12.10 is a class B address, which means that 16 bits of the address are used for the network portion and 16 bits are used for the host portion of the address. With CIDR, the /22 notation at the end of the IP address means that 22 bits are used for the network portion of the address, and the host portion uses the 10 remaining bits. In turn, this would mean that this address space can be divided into smaller, more efficient blocks of space.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPv4

Network Calculators, http://www.subnetmask.info/

Question #4 of 131

Question ID: 1114720

Which protocols operate at the Transport layer of the OSI model?

a. HTTP

b. IP

c. IPX

d. TCP

e. UDP

- ✗ **A)** option d
- ✗ **B)** option a
- ✗ **C)** all of the options
- ✗ **D)** option c
- ✗ **E)** option b
- ✓ **F)** options d and e only
- ✗ **G)** option e
- ✗ **H)** options a, b, and c only

Explanation

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) both operate at the Transport layer of the Open Systems Interconnection (OSI) model. Because the Transport layer is the fourth layer in the OSI model, it is sometimes referred to as Layer 4.

Protocols that operate at the Transport layer provide transport services to higher-layer protocols, such as Hypertext Transfer Protocol (HTTP) and Trivial File Transfer Protocol (TFTP). For example, HTTP is an Application-layer protocol that uses the connection-oriented services of TCP, and TFTP is an Application-layer protocol that uses the connectionless services of UDP.

IP is a connectionless protocol in the TCP/IP protocol suite. Internetwork Packet Exchange (IPX) is a connectionless protocol in the IPX/SPX protocol suite. IP and IPX operate at the Network layer of the OSI model and provide routing and addressing services for nodes on a network.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Transport Layer

---

Question #5 of 131

Question ID: 1105142

Which function does the Session layer of the OSI model provide?

- ✗ **A)** physical network addressing
- ✓ **B)** data synchronization
- ✗ **C)** logical network addressing
- ✗ **D)** routing

Explanation

Of the choices listed, the Session layer of the Open Systems Interconnection (OSI) model provides data synchronization. The Session layer establishes and maintains the dialogue, or session, between two computers on a network. The Session layer also communicates problems, such as file transfer errors, to applications in the layers above it.

The Network layer provides logical network addressing and routing. In the TCP/IP protocol stack, IP provides network addressing. IP also provides routing and operates at the Network layer of the OSI model.

The Data Link layer provides physical network addressing. Network interface cards (NICs) are configured with media access control (MAC) addresses. A NIC's MAC address is used by a network communications protocol on Ethernet or Token Ring architectures to identify the NIC on the network.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Session Layer

---

Question #6 of 131

Question ID: 1114727

What are valid reasons for implementing subnets on an IP network?

a. to increase network security

b. to configure a greater number of hosts

c. to reduce congestion by decreasing network traffic

d. to use more than one server on each segment of an IP LAN

e. to reduce congestion by increasing network media bandwidth

- ✗ **A)** option a
- ✗ **B)** option e
- ✗ **C)** options a, c, and e only
- ✗ **D)** options b and d only
- ✗ **E)** option c
- ✗ **F)** option b
- ✗ **G)** option d
- ✓ **H)** options a and c only

Explanation

The subnet mask enables TCP/IP to find the destination host's location on either the local network or a remote location.

Subnets are used for the following reasons:

to expand the network

to reduce congestion

to reduce CPU use

to isolate network problems

to improve security

to allow combinations of media because each subnet can support a different medium

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IP Classes

---

Question #7 of 131

Question ID: 1114729

Your organization is trying to decide whether to use RSA or ECC to encryption cellular communications. What is an advantage of ECC over the RSA algorithm?

- ✓ **A)** ECC requires fewer resources.
- ✗ **B)** ECC does not deal with the intricacies of digital signatures.
- ✗ **C)** ECC uses elliptic curves instead of keys to provide security.
- ✗ **D)** ECC uses elliptic curves that improve its reliability.

Explanation

The advantage of Elliptic Curve Cryptography (ECC) over the Rivest, Shamir, and Adleman (RSA) algorithm is its improved efficiency and requirement of fewer resources than RSA. ECC has a higher strength per bit than an RSA.

ECC is a method used to implement public-key (asymmetric) cryptography. ECC serves as an alternative to the RSA algorithm and provides similar functionalities. The functions of ECC are as follows:

Digital signature generation

Secure key distribution

Encryption and decryption of data

Wireless devices, handheld computers, smart cards, and cellular telephones have limited processing power, storage, power, memory, and bandwidth compared to other systems. To ensure efficient use of resources, ECC provides encryption by using shorter key lengths. Shorter key lengths do not imply less secure systems. Therefore, ECC provides the same level of security as RSA by using a shorter key that enables easier processing by the resource-constrained devices. For example, a 224-bit ECC key provides the same level of security as the 2048-bit keys used by legacy schemes. A 3072-bit legacy key and a 256-bit ECC key provide equivalent security. This is an obvious advantage when the future lies in smaller devices and increased security.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, ECC

Question #8 of 131

Question ID: 1105244

Which technology is used to create an encrypted remote terminal connection with a Unix computer?

✗ **A)** Telnet
✗ **B)** FTP
✓ **C)** SSH
✗ **D)** SCP

Explanation

Secure Shell (SSH) is used to create an encrypted remote terminal connection with a Unix computer.

File Transfer Protocol (FTP) is used to transfer files on a TCP/IP network. FTP transmits data in clear text. Secure Copy (SCP) enables users to transfer files over a secure connection. Telnet is a protocol that enables a user to establish terminal connections with Unix computers. Telnet transmits data in clear text.

Objective:
Communication and Network Security

Sub-Objective:

Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, SSH

Secure Shell, http://searchsecurity.techtarget.com/definition/Secure-Shell

---

Question #9 of 131

Question ID: 1105166

Which applications use UDP?

✗ **A)** ARP, NFS, FTP, SMTP

✗ **B)** ICMP, ARP, FTP

✓ **C)** NFS, TFTP, SNMP

✗ **D)** NFS, FTP, TFTP

Explanation

Network applications that want to save processing time use UDP because they have very small data units to exchange and a small amount of reassembly. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP, as do Network File System (NFS) and Simple Network Management Protocol (SNMP). TFTP is a network application that is simpler than File Transfer Protocol (FTP) but less capable. It is used when user authentication and directory visibility are not required.

Simple Mail Transport Protocol (SMTP) is implemented to operate over TCP port 25. SMTP is the default protocol for sending e-mail.

FTP is used to transfer files between an FTP server and a client using IP over TCP.

Telnet and rlogin are two other protocols that use TCP.

TCP is connection-oriented, while UDP is connectionless. TCP and UDP operate at the Transport layer of the OSI model.

User Datagram Protocol (UDP) is a protocol that offers a limited amount of service when messages are exchanged between computers in a TCP/IP network. UDP is an alternative to Transmission Control Protocol (TCP). Like TCP, UDP uses Internet Protocol (IP) to actually get a packet from one computer to another. Unlike TCP, however, UDP does not divide a message into datagrams and reassemble it at the other end. UDP is implemented at the Transport layer of the TCP/IP protocol model.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Common TCP/UDP Port Numbers

---

Question #10 of 131

Question ID: 1111744

You are trying to decide which type of intrusion detection system (IDS) you should deploy to improve network security. Match the IDS description from the left with their appropriate IDS type on the right.

{UCMS id=5671067681030144 type=Activity}

Explanation

The IDS types should be matched with the descriptions in the following manner:

- Behavior-based - An IDS that uses a learned activity baseline to identify intrusion attempts
- Signature-based - An IDS that maintains an attack profile database to identify intrusion attempts
- Host-based - An IDS that only monitors a single particular device for intrusion attempts
- Network-based - An IDS that monitors an entire network segment for intrusion attempts

Many IDS solutions actually employ multiple types to provide the greatest protection.

Keep in mind that an IDS only detects intrusion attempts and employs the configured alerts to ensure that the intrusion attempts is recorded and reported. An intrusion prevention system (IPS) detects the intrusions and carries out steps to prevent the attack from being successful.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Secure Network Components

---

Question #11 of 131

Question ID: 1105233

What is a common implementation for the IPSec protocol?

✗ **A)** SSL

✗ **B)** EDI

✗ **C)** SET

✓ **D)** VPN

Explanation

Internet Protocol Security (IPSec) is a security standard commonly implemented to create virtual private networks (VPNs). IPSec allows packets to be securely exchanged over the Internet Protocol (IP) at the OSI Network layer rather than at the Application layer. The Internet Engineering Task Force (IETF) developed the standard, but Cisco has contributed to its emergence. Cisco routers have support for IPSec built into the product.

IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion of each packet but not the header information. Tunnel mode encrypts both the header and the data. For IPSec to work, the sending and receiving devices must share a public key. Another method for securing a VPN is by using Layer Two Tunneling Protocol (L2TP).

Exchange Data Interchange (EDI) is a protocol used to exchange business data in a standard format.

Secure Electronic Transfer (SET) is used to provide security for credit card transactions.

Secure Sockets Layer (SSL) is a security protocol that uses both encryption and authentication to protect data sent in network communications.

VPNs are sometimes commonly referred to as tunnels. A VPN essentially consists of a VPN server, authentication, and encryption. The VPN software encrypts the session information, as well as most message information, including File Transfer Protocol (FTP) and HyperText Transfer Protocol (HTTP) messages. The Data-link layer information remains unaltered.

The most effective attack against an IPSec-based VPN is a man in the middle attack.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPsec

VPN's: IPSec vs. SSL, http://netsecurity.about.com/cs/generalsecurity/a/aa111703.htm

Question #12 of 131

Question ID: 1192939

What are the key functions of the OSI Network layer?

a. flow control

b. path selection

c. data segmentation

d. logical addressing

e. physical addressing

- ✓ **A)** options b and d only
- ✗ **B)** options a, c, and e only
- ✗ **C)** all of the options
- ✗ **D)** option b
- ✗ **E)** optional e
- ✗ **F)** option d
- ✗ **G)** option a
- ✗ **H)** option c

Explanation

The key functions of the OSI Network layer are logical addressing and path selection. The Network layers of two systems exchange packets/datagrams. TCP/IP packets contain an IP header and the data.

Network or logical addresses contain a network portion and a host portion. Network addresses are stored in the routing table of the router and quickly determine the interface a packet needs to travel to reach the destination. Once the packets arrive at the destination network address, the local router can determine where to forward the packets based on the host address of the destination host. This header information can also be used by packet-filtering firewalls to filter traffic based on source and destination IP address.

Flow control, error notification, physical device addressing, and specification of the networking topology can take place at the Data-link layer. Note that error notification takes place at the Data-link layer, while error correction is a function of the Transport layer. The Transport layer specifies whether the delivery method is reliable or unreliable (best-effort delivery) and handles segmentation and reassembly of data into a data stream.

Physical addressing of a device occurs at the Data-link layer. The Data-link layer uses the address to determine if it is necessary to pass the message up the protocol stack and to which upper-layer stack to pass it. The Data-link layer supports both connection-oriented and connectionless services and provides for frame sequencing and flow control.

The Network layer also provides routing and related services. Some of the protocols that work at the Network layer are Internet Protocol (IP), Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Group Management Protocol (IGMP). Packet filtering firewalls operate at this layer.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Network Layer

---

Question #13 of 131

Question ID: 1105147

What is the base network ID for the address 196.11.200.71/18?

✗ **A)** 196.11.200.71
✗ **B)** 196.11.0.0
✓ **C)** 196.11.192.0
✗ **D)** 196.11.200.0
✗ **E)** 196.0.0.0

Explanation

The base network ID is 196.11.192.0.

The IP address 196.11.200.71/18 is an example of a "slash x" network, also known as Classless Interdomain Routing (CIDR) notation. CIDR is a way of applying a subnet mask to an IP address to optimize address space while ignoring the traditional IP class categories. With classful addressing, 196.11.200.71 is a class C address, which means that 24 bits of the address are used for the network portion and eight bits are used for the host portion of the address. With CIDR, the /18 notation at the end of the IP address means that 18 bits are used for the network portion of the address, and the host portion uses the 14 remaining bits. This is an example of summarization or supernetting, the opposite of subnetting. Summarizing is used to combine a collection of subnets as one for the purpose of making routing tables on the routers smaller thus improving performance.

With 18 bits used, the standard subnet mask is 11111111.11111111.11000000.00000000 or 255.255.192.0.

In turn, this means that the network portion of this address, or the base network ID, is 196.11.192.0.

The purpose of CIDR is to divide IP addresses into smaller, more efficient blocks of space.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPv4

Network Calculators, http://www.subnetmask.info/

Question #14 of 131

Question ID: 1113973

Which term best describes a program that records the activity on a computer's display?

- ✗ **A)** malware
- ✓ **B)** screen scraper
- ✗ **C)** spam
- ✗ **D)** virus

Explanation

The term screen scraper best describes a program that records the activity on a computer's display. It is used by hackers to obtain personal information.

A virus is an application that infects applications. A virus is usually programmed so that is replicates itself without the user's knowledge or permission.

Spam is a term used for unsolicited e-mail.

Malicious software (malware) is the term used for any type of malicious software. The term malware is often used when referring to viruses and Trojan horses. While a screen scraper is considered to be a type of malware, the term screen scraper best describes a program that records the activity on a computer's display.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security,VPN Screen Scraper

Screen Scraping, Trojan Horses and Passwords oh, my, http://blogs.msdn.com/b/mthree/archive/2006/03/16/screen-scraping-trojan-horses-and-passwords-oh-my.aspx

---

Question #15 of 131

Question ID: 1105191

Which statement is NOT true regarding Ethernet II frames?

- ✓ **A)** They include a two-byte Length field.
- ✗ **B)** The 802.1Q tag is optional.
- ✗ **C)** They include a two-byte Type field.
- ✗ **D)** They include both the MAC destination and source.

Explanation

Ethernet II frames do NOT include a two-byte Length field. Ethernet II frames include a two-byte Type field.

The two-byte length field is included in 802.3 frames.

All Ethernet frames, including Ethernet II and 802.3 frames, include both the MAC destination and source in the header. In addition, the 802.1Q tag, which is the virtual LAN (VLAN) tag, is optional for all Ethernet frames.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Ethernet 802.3

The Ethernet II Frame Format, http://www.firewall.cx/networking-topics/ethernet/ethernet-frame-formats/201-ethernet-ii.html

---

Question #16 of 131

Question ID: 1105160

Which protocol is used to send e-mail to a server on the Internet?

- ✗ **A)** FTP

✓ **B)** SMTP

✗ **C)** SNMP

✗ **D)** Telnet

✗ **E)** IGMP

✗ **F)** TFTP

Explanation

Simple Mail Transfer Protocol (SMTP) is an application protocol; therefore, it operates at the top layer of the OSI model. SMTP is the default protocol for sending e-mail in Microsoft operating systems.

Post Office Protocol (POP3) and Internet Message Access Protocol (IMAP) are the most popular protocols for receiving e-mail. Others include SMTP and HTTP for some types of email clients. By default, SMTP uses port 25, POP3 uses port 110, and IMAP uses port 143.

File Transfer Protocol (FTP) is a useful and powerful tool available to general users. FTP allows a user to upload and download files between local and remote hosts. Anonymous FTP access is commonly available at many sites to allow users access to public files without having to establish an account. Often a user will be required to enter a valid e-mail address as a password. By default, FTP uses ports 20 and 21.

Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. By default, SNMP uses port 161.

Trivial File Transfer Protocol (TFTP) is a network application that is simpler than FTP but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is often not implemented on networks because of its inherent security risks, namely that it is connectionless and does not require user authentication. By default, TFTP uses port 69.

Hosts and gateways use Internet Group Management Protocol (IGMP) on a single network to establish hosts' membership in particular multicast groups. The gateways use the information with a multicast routing protocol, to support IP multicasting across the Internet. Several routing protocols are used to discover multicast groups and to build routes for each group. These include Protocol-Independent Multicast (PIM), Distance-Vector Multicast Routing Protocol (DVMRP), and Multicast Open Shortest Path First (MOSPF). Because IGMP is a protocol, it is not identified by a port number but by its protocol number, which is 2.

Telnet is a user command and an underlying TCP/IP protocol for accessing remote hosts. The HTTP and FTP protocols allow you to request specific files from remote hosts but not to actually be logged on as a user of that host computer. The Telnet protocol allows you log on as a regular user with the associated privileges you have been granted to the specific application and data on that host. In other words, you appear to be locally attached to the remote system. By default, Telnet uses port 23.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, SMTP

SMTP (Simple Mail Transfer Protocol), http://searchexchange.techtarget.com/definition/SMTP

Question #17 of 131

Question ID: 1105218

What is a teardrop attack?

- ✓ **A)** It sends malformed packets to the intended victim.
- ✗ **B)** It uses UDP messages to overwhelm the intended victim.
- ✗ **C)** It is a denial of service (DoS) attack that uses oversized ICMP messages to overwhelm the intended victim.
- ✗ **D)** It uses ICMP messages to overwhelm the intended victim.

Explanation

A teardrop attack sends malformed packets to the intended victim. It takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack.

A smurf attack uses ICMP messages to overwhelm the intended victim. A fraggle attack uses UDP messages to overwhelm the intended victim. A ping of death attack is a DoS attack that uses oversized ICMP messages to overwhelm the intended victim.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Teardrop

---

Question #18 of 131

Question ID: 1105224

What is another term for a demilitarized zone (DMZ)?

✗ **A)** virtual private network (VPN)

✓ **B)** screened subnet

✗ **C)** dual-homed firewall

✗ **D)** screened host

Explanation

Screened subnet is another term for a demilitarized zone (DMZ). Two firewalls are used in this configuration: one firewall resides between the public network and DMZ, and the other resides between the DMZ and private network.

A screened host is a firewall that resides between the router that connects a network to the Internet and the private network. The router acts as a screening device, and the firewall is the screen host. This firewall employs two network cards and a single screening router.

A dual-homed firewall is one that has two network interfaces: one interface connects to the Internet, and the other connects to the private network. One of the most common drawbacks to dual-homed firewalls is that internal routing may accidentally become enabled.

A virtual private network (VPN) is not a physical network. As its name implies, it is a virtual network that allows users connecting over the Internet to access private network resources while providing the maximum level of security. An encrypted VPN connection should be used to ensure the privacy and integrity of data that is transmitted between entities over a public network, whether those entities are clients, servers, firewalls, or other network hardware.

Firewall architectures include bastion hosts, dual-homed firewalls, screened hosts, and screened subnets.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #19 of 131

Question ID: 1114737

Your network contains four segments. Which network devices can you use to connect two or more of the LAN segments together?

a. Hub

b. Router

c. Switch

d. Bridge

e. Repeater

f. Multiplexer

- ✗ **A)** option f
- ✗ **B)** option e
- ✗ **C)** options a, b, and c only
- ✗ **D)** options c, d, and e only
- ✗ **E)** option d
- ✗ **F)** option a
- ✗ **G)** option b
- ✓ **H)** options b, c, and d only
- ✗ **I)** option c

Explanation

Bridges, switches, and routers can be used to connect multiple LAN segments. Bridges and switches operate at the Data Link layer, using the Media Access Control (MAC) address for sending packets to their destination. Routers operate at the Network layer by using IP addresses to route packets to their destination along the most efficient path.

Hubs act as a central connection point for network devices on one network segment. They work at the Physical layer.

Repeaters are used to extend the length of network beyond the cable's maximum segment distance. They take a received frame's signal and regenerate it to all other ports on the repeater. They also work at the Physical layer.

An inverse multiplexer is used to connect several T1 lines together for fault tolerance purposes. The multiplexer is placed at both ends of the connection.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Hardware

Question #20 of 131

Question ID: 1105177

Which term is most commonly used to describe equipment that creates a demilitarized zone (DMZ)?

- ✓ **A)** firewall
- ✗ **B)** router
- ✗ **C)** active hub
- ✗ **D)** passive hub

Explanation

A firewall is used to create a demilitarized zone (DMZ). A DMZ is a zone located between a company's internal network and the Internet that usually contains servers that the public will be accessing. The DMZ implementation provides an extra security precaution to protect the resources on the company's internal network. Usually two firewalls are used to create a DMZ. One firewall resides between the public network and DMZ, and another firewall resides between the DMZ and private network.

A router is used to create individual subnetworks on an Ethernet network. Routers operate at the Network layer of the OSI model. While a firewall can also be a router, it is referred to as a firewall when it functions to create a DMZ.

An active hub is used to connect devices in a star topology. An active hub has circuitry that allows signal regeneration. In a star-wired topology, cabling termination errors can crash the entire network.

A passive hub connects devices in a start topology, but it does not provide any signal regeneration.

A firewall is classified as a rule-based access control device. Rules are configured on the firewall to allow or deny packet passage from one network to another. The configuration of the rules is one of the biggest concerns for a firewall, because the rules can be very complex. Misconfiguration can easily lead to security breaches.

Filters are created according to the company's security policy.

To provide maximum file security, firewalls should not run the Network Information System (NIS) file system. Compilers should be deleted from firewalls.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

Question #21 of 131

Question ID: 1105161

Which term is used to describe the area that is covered by a satellite?

- ✗ **A)** line of sight
- ✓ **B)** footprint
- ✗ **C)** amplitude
- ✗ **D)** frequency

Explanation

The term footprint is used to describe the area that is covered by a satellite. The large footprint of a satellite can result in the interception of the satellite transmission. A footprint covers an area on Earth for a small amount of time.

Amplitude and frequency are analogue communication terms. Amplitude is used to describe the height of the signal. Frequency is used to describe the number of waves that are transmitted during a period of time.

Line of sight is the term used to describe the requirement that a receiver must not have any obstruction of the satellite signal. This includes buildings, trees, and weather.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

What is the meaning of a satellites footprint (coverage)?, https://techbaron.com/what-is-the-meaning-of-a-satellites-footprint-coverage/

Question #22 of 131

Question ID: 1105205

You manage the security for a small corporate network that includes a hub and firewall. You want to provide protection against traffic sniffing. What should you do?

- ✗ **A)** Implement access control lists (ACLs) on the hub.
- ✗ **B)** Implement filters on the hub.
- ✗ **C)** Replace the hub with a repeater.
- ✓ **D)** Replace the hub with a switch.

Explanation

You should replace the hub with a switch. This will provide some protection against traffic sniffing. In a network that uses hubs, packets are visible to every node on the network. When switches are used, the packets are forwarded only to the host for which the packet is intended because a switch does not forward packets out all of its ports. This prevents the ability of users on the same network from viewing each other's traffic, thereby providing some level of protection against traffic sniffing. Traffic sniffing captures data packets not intended for the sniffer. A network-based intrusion detection system (IDS) can be used to capture packets on a switch.

You should not replace the hub with a repeater. A repeater receives a signal and repeats it, thereby ensuring the signal degradation does not occur. A repeater cannot protect against traffic sniffing by itself.

You cannot implement filters or ACLs on a hub. Implementing filters and ACLs on switches or routers provides a means whereby traffic is allowed or prevented, and then forwarded to the appropriate node. Applying filters to routers can protect against Internet Protocol (IP) spoofing attacks.

Sniffing is the action of capturing and monitoring the traffic going over the network. In a normal networking environment, account and password information is passed in clear text. For this reason, it is not hard to compromise the entire network by putting a machine into promiscuous mode and capturing all the passwords.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Switch

Sniffers: What They Are and How to Protect Yourself, http://www.colasoft.com/resources/sniffer.php

---

Question #23 of 131

Question ID: 1114747

You are deploying a virtual private network (VPN) for remote users. You want to meet the following goals:

The VPN gateway should require the use of Internet Protocol Security (IPSec).

All remote users must use IPSec to connect to the VPN gateway.

No internal hosts should use IPSec.

Which IPSec mode should you use?

✗ **A)** host-to-host

✗ **B)** gateway-to-gateway

✓ **C)** host-to-gateway

✗ **D)** This configuration is not possible.

Explanation

You should deploy host-to-gateway IPSec mode. In this configuration, the VPN gateway requires the use of IPSec for all remote clients. The remote clients use IPSec to connect to the VPN gateway. Any communication between the VPN gateway and the internet hosts on behalf of the remote clients does not use IPSec. Only the traffic over the Internet uses IPSec.

In host-to-host IPSec mode, each host must deploy IPSec. This mode would require that any internal hosts that communicate with the VPN clients would need to deploy IPSec.

In gateway-to-gateway IPSec mode, the gateways at each end of the connection provide IPSec functionality. The individual hosts do not. For this reason, the VPN is transparent to the users. This deployment best works when a branch office or partner company needs access to your network.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, IPSec and ISAKMP

Question #24 of 131

Question ID: 1105167

Which protocol responds to ping requests?

✓ **A)** ICMP

✗ **B)** RARP

✗ **C)** ARP

✗ **D)** TCP

Explanation

When you ping a host, Internet Control Message Protocol (ICMP) will respond to the request. ICMP is responsible for sending messages between network devices regarding network health.

If the ping is successful, the information returned will give reply information. "Reply" means that the host is reachable, and is responding to requests. If the ping is unsuccessful, the information returned will state the type of problem experienced. Some possible error codes could be destination unreachable, protocol unreachable, and no reply.

Address Resolution Protocol (ARP) is responsible for mapping the hardware address of the hosts on broadcast networks with the TCP/IP address of each host. The ARP utility allows you to view the ARP cache, which maps each IP address to a physical address.

Transmission Control Protocol (TCP) is a connection-oriented protocol operating at the Transport layer of the OSI model.

Reverse Address Resolution Protocol (RARP) allows a host on a local area network to request its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache.

ARP and RARP map the 32-bit Internet Protocol (IP) version 4 addresses to their corresponding 48-bit Ethernet, or MAC, address. The MAC address is a hard-coded number for the network interface card (NIC) that is assigned by the manufacturer. The IP address is assigned automatically by the network's DHCP server or manually by the network administrator. ARP matches IP address to MAC address; RARP matches MAC address to IP address.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, ICMP

Question #25 of 131

Question ID: 1113951

You administer a TCP/IP network that is not subnetted. One of the network hosts has the following IP address:

130.250.0.10

Which IP address is the network ID of the network you administer?

- ✗ **A)** 130.250.255.255
- ✗ **B)** 255.255.255.255
- ✗ **C)** 128.0.0.0

✓ **D)** 130.250.0.0

Explanation

The network ID of the network you administer is 130.250.0.0. According to the scenario, your network is not subnetted and is configured with Class B IP addresses. In a Class B IP address, the first 16 bits of the IP address correspond to the network address, and the last 16 bits of the address correspond to the host address.

In dotted-decimal notation, a decimal number represents each 8-bit portion, or octet, of an IP address. Therefore, the network address for the network you administer is the first two octets followed by two octets of zeroes, or 130.250.0.0. The address 128.0.0.0 is the first valid network ID in the range of Class B IP addresses that are not subnetted. The address 130.250.255.255 is the broadcast address for the network with the network ID 130.250.0.0. The IP address 255.255.255.255 is a general or universal broadcast address to all networks on a TCP/IP network.

Before Classless Interdomain Routing (CIDR) was introduced, networks were commonly organized by classes. In a Class B address, the first bit of the address is set to one and the second bit of the address is set to zero.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPv4

Network Calculators, http://www.subnetmask.info/

Question #26 of 131

Question ID: 1105136

At which OSI layer does an active hub function?

✗ **A)** Session

✗ **B)** Network

✓ **C)** Physical

✗ **D)** Transport

Explanation

Active hubs or multiport repeaters amplify or regenerate signals to all other ports on the hub. Because active hubs regenerate signals, they are often used to extend the length of segments beyond their maximum specified lengths.

They, as with all hubs, are considered Physical layer devices because they act on the data at the bit level.

The Physical layer defines the X.25, V.35, X.21, and High-Speed Serial Interface (HSSI) standards. These standards define the type of connector as well as the type of signaling used. The Physical layer, along with the Data-Link and Network layer, provides support to the components that are necessary to transmit the network message.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Session Layer

---

Question #27 of 131

Question ID: 1105171

Which function is NOT performed at the Physical layer of the OSI model?

- ✗ **A)** defining the electrical features of the communication media
- ✗ **B)** defining the type of connector being used
- ✓ **C)** defining the type of encryption being used for the data
- ✗ **D)** defining the size of the Ethernet cable

Explanation

The data encryption method being used is not defined at the Physical layer of the OSI model. Data encryption is supported at the Data-Link, Network, Transport, Session, and Application layers of the OSI model.

The Physical layer deals with electrical impulses, light and radio signals, physical cables, cards, and other physical aspects of the communication medium. Defining the type of connectors being used and the size and distance limitations of the Ethernet cable are some other functions performed at the Physical layer.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security. Physical layer

OSI model, http://www.tech-faq.com/osi-model.html

Question #28 of 131

Question ID: 1105190

At which layer of the OSI model do routers operate?

- ✗ **A)** Data-link
- ✗ **B)** Session
- ✓ **C)** Network
- ✗ **D)** Transport
- ✗ **E)** Physical

Explanation

Routers operate at the Network layer of the OSI networking model. They use source and destination addresses, which are located at the Network layer, to route packets. Switches use MAC addresses, which are located at the Data-link layer, to forward frames.

The Session layer starts, maintains, and stops sessions between applications on different network devices.

The Physical layer provides the functions to establish and maintain the physical link between network devices. Repeaters work at the Physical layer.

The Transport layer of the OSI model segments and reassembles data into a data stream and provides reliable and unreliable end-to-end data transmission.

Bridges work at the Data-Link layer.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Router

---

Question #29 of 131

Question ID: 1114726

Your company has decided to implement a wireless network. The wireless network users must be able to connect to resources on your internal network, including file, print, and DHCP services. All wireless clients will run the Windows operating system.

What should you implement?

a. Infrastructure mode

b. Ad hoc mode

c. A wireless access point

d. Static IP addresses

e. APIPA

- ✓ **A)** options a and c only
- ✗ **B)** option c
- ✗ **C)** option d
- ✗ **D)** options b and e only
- ✗ **E)** options b and d only
- ✗ **F)** option b
- ✗ **G)** option e
- ✗ **H)** option a

Explanation

You should implement infrastructure mode with a wireless access point. Infrastructure mode allows wireless computers to connect to a LAN, a WAN, or the Internet. This means that infrastructure mode wireless computers can access all computers on the LAN, WAN, and Internet. Infrastructure mode is much more expensive to implement than ad hoc mode because you must configure wireless access points. While infrastructure mode is harder to set up and configure, it is much easier to manage than ad hoc mode.

Ad hoc mode allows wireless computers to be configured much more quickly than infrastructure mode. Ad hoc mode wireless computers all participate in the same network. This means that the ad hoc wireless computers can access each other, but cannot access network resources on a LAN, WAN, or Internet. Ad hoc mode is much cheaper than infrastructure mode to implement. In addition, it is easy to set up and configure and can provide better performance than infrastructure mode. However, it is difficult to manage an ad hoc mode wireless network.

Static IP addresses should not be implemented because the corporate network contains a DHCP server. APIPA should not be used for the same reason. In addition, APIPA is utilized only if a DHCP server is not found.

Objective:

Communication and Network Security

Sub-Objective:

Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Infrastructure Mode Versus Ad Hoc Mode

Understanding Ad Hoc Mode, http://www.wi-fiplanet.com/tutorials/article.php/1451421

Wireless LANs: Extending the Reach of a LAN, http://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=4

Question #30 of 131

Question ID: 1114740

Which network device acts as an Internet gateway, firewall, and Internet caching server for a private network?

✗ **A)** IDS

✓ **B)** proxy server

✗ **C)** VPN

✗ **D)** IPS

Explanation

A proxy server acts as in Internet gateway, firewall, and Internet caching server for a private network. Hosts on the private network contact the proxy server with an Internet Web site request. The proxy server checks its cache to see if a locally stored copy of the site is available. If not, the proxy server communicates with its Internet connection to retrieve the Web site. The proxy server is virtually invisible to the client and the Internet connection. A proxy server can be configured to allow only outgoing Hypertext Transfer Protocol (HTTP) traffic by configuring which users have permissions to access the Internet via the proxy server.

A virtual private network (VPN) is a private network that users can connect to over a public network. A VPN can be implemented in the following ways:

by installing software or hardware agents on the client or network

by implementing key and certificate exchange systems

by implementing node authentication systems

An intrusion detection system (IDS) is a network device that detects network intrusion and either logs the intrusion or contacts the appropriate personnel.

An intrusion prevention system (IPS) is a network device that detects network intrusion attempts and prevents the network intrusion. An IPS provides more security than an IDS because it actually provides prevention, not just detection.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Types

Proxy server, http://whatis.techtarget.com/definition/0,sid9_gci212840,00.html

---

Question #31 of 131

Question ID: 1105181

What is SOCKS?

- ✗ **A)** a dynamic packet-filtering firewall that uses the ports higher than 1023 to establish connections dynamically
- ✓ **B)** a circuit-level proxy firewall that provides a secure channel between two computers
- ✗ **C)** an application-level proxy firewall that has preconfigured service filters
- ✗ **D)** a kernel proxy firewall that processes in the kernel and creates a stack for each packet

Explanation

SOCKS is a circuit-level proxy firewall that provides a secure channel between two computers. SOCKS acts as a connection proxy and works independent of TCP/IP application protocols. Network applications need to be updated to work with SOCKS.

SOCKS is not an application-level proxy firewall, a kernel proxy firewall, or a dynamic packet-filtering firewall.

Circuit-level proxy firewalls make forwarding decisions based solely on IP address and service port information. A circuit-level proxy firewall is easier to maintain than an application-level proxy firewall, but it is not as secure or as resource intensive. Sometimes circuit-level firewalls are called circuit-level gateways.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Types

---

Question #32 of 131

Question ID: 1105209

Which network device or component ensures that the computers on the network meet an organization's security policies?

✗ **A)** NAT
✗ **B)** DMZ
✓ **C)** NAC
✗ **D)** IPSec

Explanation

Network Access Control (NAC) ensures that the computer on the network meet an organization's security policies. NAC user policies can be enforced based on the location of the network user, group membership, or some other criteria.

Network Address Translation (NAT) is an IEEE standard that provides a transparent firewall solution between an internal network and outside networks. Using NAT, multiple internal computers can share a single Internet interface and IP address.

Internet Protocol Security (IPSec) is a protocol that secures IP communication over a private or public network. IPSec is used to create a VPN. An example is the use of a General Packet Radio Services (GPRS)-enabled laptop that connects to a corporate intranet via a VPN.

A demilitarized zone (DMZ) is a section of a network that is isolated from the rest of the network with firewalls. Servers in a DMZ are more secure than those on the regular network.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

The Tricky Part of NAC Deployment, http://www.networkworld.com/newsletters/vpn/2008/101308nac1.html

---

Question #33 of 131

Question ID: 1105135

Which OSI function ensures that the identity of the remote host is verified and that the data received is authentic?

- ✗ **A)** routing
- ✗ **B)** encryption
- ✗ **C)** segmentation
- ✓ **D)** authentication

Explanation

Authentication is the OSI function that ensures that the identity of the remote host is verified and that the data received is authentic. This process takes place at the Session layer.

Routing is the OSI function that ensures that a packet can reach its destination. This process takes place at the Network layer.

Encryption is the OSI function that ensures data confidentiality by encrypting the data. This process takes place at the Presentation layer.

Segmentation is the OSI function that divides data into easily transmitted packets. This process takes place at the Transport layer.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Session Layer

---

Question #34 of 131

Question ID: 1105241

Which protocol should you configure on a remote access server to authenticate remote users with smart cards?

- ✓ **A)** EAP
- ✗ **B)** CHAP
- ✗ **C)** PAP
- ✗ **D)** MS-CHAP

Explanation

You should use the Extensible Authentication Protocol (EAP). By using an EAP authentication protocol, such as EAP-Transport Level Security (EAP-TLS), for authentication, the remote access server can authenticate remote users with smart cards.

The other authentication protocols listed do not support authentication using smart cards.

Password Authentication Protocol (PAP) requires that users authenticate using a password. The password is transmitted in plain text, thereby allowing a possible security breach.

Challenge Handshake Authentication Protocol (CHAP) provides a higher level of security. Passwords are not sent in plain text. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) comes in two versions. Version 2 provides better security because it provides mutual authentication, meaning both ends of the connection are authenticated.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, 802.1x

---

Question #35 of 131

Question ID: 1113949

You are preparing to perform routine maintenance on the network. The network must remain inaccessible while you are performing this maintenance. You send a message with the packet header 135.135.255.255.

What does that packet address accomplish?

- ✗ **A)** It prevents any further users from logging in to the 135.135 network.
- ✗ **B)** It displays who is accessing the 135.135 network.
- ✗ **C)** It displays how many stations are connected to the 135.135 network.

✓ **D)** It broadcasts your message to all stations on the 135.135 network.

Explanation

It broadcasts your message to all stations on the 135.135 network. The network address 135.135.255.255 is a class B address. The node address of 255.255 causes this message to be broadcast to all IP addresses with an IP address of 135.135.x.x. Because broadcasting can be used in some attacks, many networks have blocked any communication using the broadcast address.

A host ID that is all ones is reserved as a broadcast address within a given subnetwork for all hosts on that subnetwork. For example, within the class C network 192.15.28 and with no subnetting, the address 192.15.28.255 broadcasts to all hosts on this network. If the bits in the network portion are all ones, the address is reserved, and 255.255.255.255 is the universal broadcast address.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPv4

Question #36 of 131

Question ID: 1105251

You are responsible for managing your company's virtualization environment. Which feature should NOT be allowed on a virtualization host?

✗ **A)** implementing a firewall

✗ **B)** implementing IPsec

✗ **C)** monitoring the event logs

✓ **D)** browsing the Internet

Explanation

You should not allow Internet browsing on a virtualization host. This can present a possible security breach through the introduction of spyware or malware. Anything that affects a virtualization host also affects all virtual computers on the host. Virtual servers have the same information security requirements as physical servers.

You should implement IPsec, implement a firewall, and monitor the event logs of a virtualization host. IPsec helps by encrypting data as it transmits across the network. Firewalls prevent unauthorized access to a physical or virtual

computer. Event logs help administrators to detect when security breaches have occurred or are being attempted.

A virtualization host can also be referred to as a virtual desktop. Often virtual applications are hosted on a virtual host.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Virtualization

---

Question #37 of 131

Question ID: 1105253

What is the speed in kilobits per second (Kbps) of a D channel on a BRI ISDN line?

✗ **A)** 56 Kbps

✗ **B)** 64 Kbps

✓ **C)** 16 Kbps

✗ **D)** 128 Kbps

Explanation

The delta (D) channel on a basic rate interface (BRI) integrated services digital network (ISDN) connection operates at 16 Kbps. A BRI ISDN connection has a single D channel and two Bearer (B) channels. The D channel carries signaling and control information for an ISDN connection. The B channels operate at 64 Kbps and carry data or voice communications. The two B channels in a BRI ISDN connection can be combined for a total data transmission speed of 128 Kbps. Modems can operate at a maximum theoretical speed of 56 Kbps, although modems are rarely able to provide this speed in practice.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, ISDN

Question #38 of 131

Question ID: 1105220

Which statement is true of network address hijacking?

✗ **A)** It involves flooding the target system with malformed fragmented packets to disrupt operations.

✗ **B)** It uses ICMP echo messages to identify the systems and services that are up and running.

✗ **C)** It is used for identifying the topology of the target network.

✓ **D)** It allows the attacker to reroute data traffic from a network device to a personal computer.

Explanation

Network address hijacking allows an attacker to reroute data traffic from a network device to a personal computer. Also referred to as session hijacking, network address hijacking enables an attacker to capture and analyze the data addressed to a target system. This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to critical systems of an organization. Session hijacking involves assuming control of an existing connection after the user has successfully created an authenticated session.

A scanning attack is used to identify the topology of the target network. Also referred to as network reconnaissance, scanning involves identifying the systems that are up and running on the target network and verifying the ports that are open, the services that a system is hosting, the type of operating system, and the applications running on a target host. Scanning is the initial process of gathering information about a network to find out vulnerabilities and exploits before an actual attempt to commit a security breach takes place.

A smurf attack uses ICMP echo messages to identify the systems and services that are up and running. It is a denial-of-service (DoS) attack that uses spoofed broadcast ping messages to flood a target system. In a smurf attack, the attacker sends a large amount of ICMP echo packets with spoofed sources IP address as that of the target host to IP broadcast addresses. This results in the target host being flooded with echo replies from the entire network, causing the system to either freeze or crash. Ping of death, bonk, and fraggle are other examples of DoS attacks.

In a teardrop attack, the attacker uses a series of IP fragmented packets, causing the system to either freeze or crash while the target host is reassembling the packets. A teardrop attack is primarily based on the fragmentation implementation of IP. To reassemble the fragments in the original packet at the destination, the host looks for incoming packets to ensure that they belong to the same original packet. The packets are malformed. Therefore, the process of reassembling the packets causes the system to either freeze or crash.

Objective:
Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Session Hijacking

---

Question #39 of 131

Question ID: 1114745

Which of the following policies should you implement for telecommuters who are issued company notebook computers?

a. Do not allow family or friends to use the company-issued computer.

b. Do not connect to unsecured wireless networks.

c. Back up the company-issued computer outside the company network.

d. Use the company-issued computer as a personal computer.

- ✗ **A)** option d
- ✓ **B)** options a and b
- ✗ **C)** option b
- ✗ **D)** option a
- ✗ **E)** option c
- ✗ **F)** options c and d
- ✗ **G)** all of the options

Explanation

If your company issues company notebook computers to telecommuters, you should ensure that security policies are communicated to the telecommuters. These policies should include the following:

Do not allow family or friends to use the company-issued computer.

Do not connect to unsecured wireless networks.

Do not back up the company-issued computer outside the company network.

Do not use the company-issued computer as a personal computer.

Do not alter security or administrative settings.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Remote Connection Technologies

---

Question #40 of 131

Question ID: 1105199

You are aware that any system on the demilitarized zone (DMZ) can be compromised because the DMZ is accessible from the Internet.

What should you do because of this?

- ✗ **A)** Implement both DMZ firewalls as bastion hosts.
- ✗ **B)** Implement the DMZ firewall that connects to the private network as a bastion host.
- ✓ **C)** Implement every computer on the DMZ as bastion hosts.
- ✗ **D)** Implement the DMZ firewall that connects to the Internet as a bastion host.

Explanation

You should implement every computer on the demilitarized zone (DMZ) as bastion hosts because any system on the DMZ can be compromised. A bastion host is, in essence, a system that is hardened to resist attacks.

A bastion host is not attached to any firewall software. However, every firewall should be hardened like a bastion host.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #41 of 131

Question ID: 1113972

What is the term for the technique that connects a network sender and receiver by a single path for the duration of a conversation?

✗ **A)** path switching

✓ **B)** circuit switching

✗ **C)** packet switching

✗ **D)** message switching

Explanation

Circuit switching is a switching technique that connects a network sender and receiver by a single path that exists for the duration of the conversation. The sending computer sends a signal to the destination computer, requesting a connection. Once the destination computer has established the connection, an acknowledgement is sent to the sending computer to let it know that it can proceed with its transfer. Telephones are an example of a circuit-switched network.

Path switching is not a switching technique.

Packet switching breaks messages down into small units of data, or packets. The packets are marked with a source, intermediate, and destination address and sent to their destination taking a path that is shared by many network users. Because there is not a dedicated connection established before the packet is sent, this type of communication is known as connectionless communication. Using the destination address, the packet is sent along the best route of many possible paths. The Internet is an example of a network that uses mainly packet switching. Frame relay and X.25 networks also use packet switching. Frame relay uses a public switched network to provide a wide area network (WAN) connection.

Message switching divides the conversation into messages rather than establishing a dedicated connection. These messages contain a destination address, which is used to send the messages from device to device. Each device stores the messages for a brief period and then forwards it to the next device. This technique is also known as "store and forward." Support services such as e-mailing and calendar sharing use message switching.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

Packet-Switched vs. Circuit-Switched Networks,
https://www.computerworld.com/article/2593382/networking/networking-packet-switched-vs-circuit-switched-networks.html

Question #42 of 131

Question ID: 1105163

Which media-access method does the 802.11 standard specify for wireless networks?

✗ **A)** CSMA/CD

✗ **B)** Demand priority

✗ **C)** Token-passing

✓ **D)** CSMA/CA

Explanation

The IEEE 802.11 standard, which is the main standard for wireless LANs, specifies using Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) for its media access method. Like an Ethernet network, which uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD), wireless adapter cards "sense," or listen, for network traffic before transmitting. The difference is that CSMA/CA requires a token; CSMA/CD does NOT require a token.

In CSMA/CA, if the network is free of traffic, the station will send its data. However, unlike an Ethernet network, wireless network cards cannot send and receive transmissions at the same time, which means that they cannot detect a collision. Instead, the sending station will wait for an acknowledgement packet (ACK) to be sent by the destination computer verifying that the data was received. If, after a random amount of time, an acknowledgement has not been received, the sending station will retransmit the data. The 802.11 standard also refers to CSMA/CA as Distributed Coordination Function (DCF).

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) computers compete for the right to send data. In CSMA/CD, when a collision occurs, the computers sending the data wait a random amount of time before attempting to retransmit the data.

Token-passing access methods allow only the one computer that has the token to transmit data, meaning there is no contention for media access.

Demand priority is an 802.12 standard known as 100VG-AnyLAN. It operates at 100 Mbps. In the event of contention on the network, the higher-priority data is given access first.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, CSMA/CD Versus CSMA/CA

Question #43 of 131

Question ID: 1105259

Your organization has signed a contract with the United States military. As part of this contract, all e-mail communication between your organization and the U.S. military must be protected. Which e-mail standard must you use for this communication?

✗ **A)** Multipurpose Internet Mail Extension (MIME)

✓ **B)** Message Security Protocol (MSP)

✗ **C)** Pretty Good Privacy (PGP)

✗ **D)** Privacy-Enhanced Mail (PEM)

Explanation

You should use the message security protocol (MSP). This protocol is used by the military to secure e-mail messages. It is used to sign and encrypt messages and perform hashing functions.

The Multipurpose Internet Mail Extension (MIME) e-mail standard specifies how e-mail attachments are to be transferred. Secure Mime (S/MIME) is an e-mail standard that extends MIME by providing a means to encrypt e-mail data and attachments. S/MIME also provides digital signatures for MIME. Neither is used by the military.

Privacy-Enhanced Mail (PEM) provides e-mail encryption but is not used by the military.

Pretty Good Privacy (PGP) also provides e-mail encryption. It employs symmetric key algorithms, asymmetric key algorithms, message digest algorithms, keys, and so on.

To ensure e-mail message authenticity and confidentiality the sender should sign the message using the sender's private key and encrypt the message using the receiver's public key, respectively.

The best way to ensure non-repudiation of an e-mail is to use a digital signature.

An e-mail directory is not considered secure. As such, confidential documents and data should not be stored there. In addition, because the e-mail directory can be purged at any time by the e-mail administrator, permanent records should not be stored there.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

Privacy-Enhanced Mail, https://neodean.wordpress.com/tag/message-security-protocol/

Question #44 of 131

Question ID: 1114722

Which functions can take place at the Data-link layer of the OSI model?

a. routing

b. flow control

c. error notification

d. physical addressing

e. setting voltage levels in transmission media

- ✗ **A)** all of the options
- ✗ **B)** option d
- ✓ **C)** option b, c, and d only
- ✗ **D)** options a and e only
- ✗ **E)** option c
- ✗ **F)** option b
- ✗ **G)** option e
- ✗ **H)** option a

Explanation

Flow control, error notification, physical device addressing, and specification of the networking topology can take place at the Data-link layer. Note that error notification takes place at the Data-link layer, also referred to as the Link layer, whereas error correction is a function of the Transport layer. The Transport layer specifies whether the delivery method is reliable or unreliable, referred to as best-effort delivery, and handles segmentation and reassembly of data into a data stream.

Because the physical addressing of the device occurs at the Data-link layer, the Data-link layer uses the address to determine whether it is necessary to pass the message up the protocol stack and to which upper-layer stack to pass it. The Data-link layer supports both connection-oriented and connectionless services and provides for frame sequencing and flow control.

Routing is performed at the Network layer of the OSI model using logical addressing to determine the path and setting. Setting voltage levels in transmission media is performed at the Physical layer.

Some of the protocols that work at the data-link layer are Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), Reverse Address Resolution Protocol (RARP), and Layer 2 Forwarding (L2F).

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Data Link Layer

---

Question #45 of 131

Question ID: 1105247

Which type of network connection is created by tunneling through a public network?

✗ **A)** a WAN
✗ **B)** a MAN
✓ **C)** a VPN
✗ **D)** a LAN

Explanation

A virtual private network (VPN) is created by tunneling through a public network, such as the Internet. Tunneling protocols, such as Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP), can create a tunnel, which is a secure connection through a public network.

A local area network (LAN) connection is typically created by a Physical layer network communication protocol. A metropolitan area network (MAN), which spans the area of a city, is created by dedicated connections. A wide area network (WAN) connection spans a large distance, such as the distance between cities or continents. A WAN connection typically consists of two or more LAN connections and can be created by using either leased-lines or dedicated connections.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, VPN

Question #46 of 131

Question ID: 1114733

Which type of firewall first examines a packet to see if it is the result of a previous connection?

✗ **A)** circuit-level proxy firewall

✓ **B)** stateful firewall

✗ **C)** application-level proxy firewall

✗ **D)** packet-filtering firewall

Explanation

A stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table.

None of the other firewalls first examines a packet to see if it is the result of a previous connection.

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Stateful firewalls perform the following tasks:

Scan information from all layers in the packet.

Save state information derived from previous communications, such as the outgoing port information, so that incoming data communication can be verified against it.

Provide tracking support for connectionless protocols through the use of session state databases.

Allow state information derived from other applications access through the firewall for authorized services only, such as previously authenticated users.

Evaluate and manipulate flexible expressions based on communication and application derived state information.

Stateful firewalls can be used to track connectionless protocols, such as the User Datagram Protocol (UDP), because they examine more than the packet header.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Types

Question #47 of 131

Question ID: 1105246

Which IPSec configuration can be used to digitally sign and encapsulate each packet within another packet?

✗ **A)** ESP protocol in tunnel mode

✗ **B)** ESP protocol in transport mode

✗ **C)** AH protocol in transport mode

✓ **D)** AH protocol in tunnel mode

Explanation

Internet Protocol Security (IPSec) can be used in tunnel mode with the Authentication Header (AH) protocol to digitally sign and encapsulate each packet sent from the network within another packet. A tunnel is a network communications construct that transports encapsulated packets.

IPSec can be used in transport mode with AH to digitally sign and encrypt packets sent between two hosts. Transport mode does not encapsulate packets within other packets. Encapsulating Security Protocol (ESP) can be used with IPSec to encrypt IPSec packets. ESP is not used to digitally sign packet headers. ESP works in tunnel mode and transport mode.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, IPSec and ISAKMP

Understanding VPN IPSec Tunnel Mode and IPSec Transport Mode - What's the Difference?, http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

Question #48 of 131

Question ID: 1113947

Which OSI layer is responsible for file, print, and message services?

✓ **A)** Application

✗ **B)** Presentation

✗ **C)** Session

✗ **D)** Network

Explanation

The Application layer provides the protocols necessary to perform the specific network services. The Application layer provides non-repudiation services. For example, when an e-mail message is sent to another user in the network, the Application layer provides the Simple Mail Transfer Protocol (SMTP) needed to direct the e-mail message across the network.

User applications themselves, such as Microsoft Outlook, are not found in the Application layer, nor are other network services, such as printing. Rather, the technologies needed by these applications to access network services reside at the Application layer. Network services include e-mail, file, print, database, and application services.

Some of the protocols that work at the Application layer are SMTP, Secure Electronic Transaction (SET), HyperText Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP). The Domain Name System (DNS) protocol also operates at this layer.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Application

---

Question #49 of 131

Question ID: 1105215

Which cable type is vulnerable to the use of vampire taps?

✗ **A)** fiber optic

✓ **B)** coaxial

✗ **C)** STP

✗ **D)** UTP

Explanation

Coaxial cable is vulnerable to the use of vampire taps. Vampire taps are physically placed on the cable to allow rogue computers to connect to your network. Coaxial cable consists of a hollow outer cylindrical conductor surrounding a

single inner conductor.

None of the other network cables listed is vulnerable to the use of vampire taps. UTP cable is susceptible to electromagnetic interference (EMI) and eavesdropping. STP is susceptible to eavesdropping. Fiber-optic cable is not susceptible to EMI or eavesdropping and is considered the safest network media. Fiber-optic cable has a much longer effective usable length (up to two kilometers in some cases).

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Coaxial

Network and Storage Media, http://www.techexams.net/technotes/securityplus/network_storage_media.shtml

---

Question #50 of 131

Question ID: 1105248

Bob manages the Sales department. Most of his sales representatives travel among several client sites. He wants to enable these sales representatives to check the shipping status of their orders online. This information currently resides on the company intranet, but it is not accessible to anyone outside the company firewall. Bob has asked you to accomplish this. You decide to create an extranet to allow these employees to view their customers' order status and history.

Which technique could you use to secure communications between network segments sending order-status data via the Internet?

- ✗ **A)** Extranet
- ✗ **B)** Certificate server
- ✓ **C)** VPN
- ✗ **D)** VLAN

Explanation

A virtual private network (VPN) is not a physical network. In a VPN, a public network, such as the Internet, is used to allow secure communication between companies that are not located together. A VPN transports encrypted data.

A Virtual LAN (VLAN) allows networks to be segmented logically without physically rewiring the network. A VLAN restricts flooding to only those ports included in the VLAN.

An extranet enables two or more companies to share information and resources. While an extranet should be configured to provide the shared data, an extranet is only a Web page. It is not actually responsible for data transmission.

A certificate server provides certificate services to users. Certificates are used to verify user identity and protect data communication.

VPNs use what is known as a tunneling protocol for the secure transfer of data using the Internet. A common tunneling protocol for this purpose is Point-to-Point Tunneling Protocol (PPTP). The term "tunnel" refers to how the information is privately sent. Data being sent is encapsulated into what are called network packets. Packets are encrypted from where they originate before they are sent via the Internet. The information travels in an encrypted, or non-readable, form. Once the information arrives at its destination, it is then decrypted.

According to RFC 2637, PPTP is a VPN technology that allows PPP to be tunneled through an IP network. Because Microsoft's implementation of PPTP does NOT include encryption by default, Microsoft Point-to-Point Encryption (MPPE) is used for encryption purposes. PPTP uses an enhanced Generic Routing Encapsulation (GRE) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets. The GRE packets forming the tunnel itself are not cryptographically protected. Because the PPP negotiations are carried out over the tunnel, it may be possible for an attacker to eavesdrop on and modify those negotiations.

By using a VPN, a company avoids the expense of leased lines for secure communication, but instead can use public networks to transfer data in a secure way. Client computers can connect to the VPN by dial-up, DSL, ISDN, or cable modems. To ensure the privacy and integrity of the data, connections between firewalls over public networks should use an encrypted VPN.

An intranet is a local area network (LAN) add-on that is restricted to certain users, usually a company's employees. The data contained on it is usually private in nature.

An extranet, on the other hand, has a wider boundary because it usually allows two or more companies to communicate and share private information.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, VPN

Question #51 of 131

Question ID: 1114746

Which WAN technologies are primarily used to enable IBM mainframes to communicate with remote computers?

a. SMDS

b. SDLC

c. HDLC

d. HSSI

- ✗ **A)** option b
- ✗ **B)** option a
- ✗ **C)** option c
- ✗ **D)** options c and d only
- ✓ **E)** options b and c only
- ✗ **F)** option d
- ✗ **G)** options a and b only

Explanation

Synchronous Data Link Control (SDLC) and High-level Data Link Control (HDLC) are primarily used to enable IBM mainframes to communicate with remote computers. A synchronous protocol, SDLC, is used over networks with permanent connections. Mainframe environments are generally considered more secure than LAN environments because there are fewer entry points to a mainframe.

HDLC is an extension of SDLC. HDLC provides higher throughput than SDLC by supporting full-duplex transmissions. SDLC does not support full duplex.

Switched Multimegabit Data Service (SMDS) is a packet-switching protocol that can provide bandwidth as demanded. It is used to connect across public networks. It has been replaced by frame relay.

High-Speed Serial Interface (HSSI) is used to connect routers and multiplexers to ATM, frame relay, and other high-speed services.

A wide area network (WAN) may provide access to interconnected network segments such as extranets, intranets, demilitarized zones (DMZs), virtual private network (VPNs), and the Internet.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

Difference Between HDLC and SDLC, http://www.differencebetween.com/difference-between-hdlc-and-vs-sdlc/

Question #52 of 131

Question ID: 1111737

Match each description with the protocol that it BEST fits.

{UCMS id=5658729179512832 type=Activity}

Explanation

The protocols should be matched with the descriptions in the following manner:

- IPSec - A tunneling protocol that provides secure authentication and data encryption
- SNMP - A network management protocol that allows communication between network devices and the management console
- SFTP - A file transferring protocol that uses SSH for security
- FTPS - A file transferring protocol that uses SSL for security

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IP Networking

Question #53 of 131

Question ID: 1105242

Which protocol is a dial-up connection protocol that requires both ends of the communication channel be assigned an IP address?

✓ **A)** SLIP

✗ **B)** IMAP4

✗ **C)** DLC

✗ **D)** PPP

Explanation

Serial Line Internet Protocol (SLIP) is an older dial-up connection protocol that requires both ends of the communication channel be assigned an IP address. SLIP was used over low-speed serial interfaces.

Data Link Control (DLC) is a connectivity protocol that is used to connect IBM mainframe computers with LANs and in some earlier models, HP printers. Internet Mail Access Protocol version 4 (IMAP4) is an e-mail retrieval protocol that some e-mail clients use to download messages from e-mail servers. DLC and IMAP4 are not dial-up protocols.

Point-to-Point Protocol (PPP) is a newer dial-up protocol with more advanced features than SLIP. It does not require that both ends of the communication channel be assigned an IP address. In addition, PPP supports several network communications protocols, such as TCP/IP, IPX/SPX, and NetBEUI.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Dial-up

---

Question #54 of 131

Question ID: 1113967

In which type of attack are messages intercepted between two computers?

✗ **A)** wardialing
✗ **B)** mail bombing
✗ **C)** ping of death
✓ **D)** man-in-the-middle

Explanation

In a man-in-the-middle attack, messages are intercepted between two computers. Using digital signatures and mutual authentication can help prevent this type of attack.

In a mail bombing attack, e-mail servers and clients are overwhelmed with unrequested e-mail messages. E-mail filtering and e-mail relay can help prevent this type of attack.

In a wardialing attack, hackers dial a large bank of phone numbers to determine which is connected to a computer. Keeping telephone number private and implementing tight access control can help prevent this type of attack.

In a ping-of-death attack, oversized ICMP packets are sent to the victim computer. To prevent this type of attack, you should stay up to date with system patches and implement ingress filtering.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Man-in-the-Middle Attack

---

Question #55 of 131

Question ID: 1105204

Your manager has asked you to improve network security by confining sensitive internal data traffic to computers on a specific subnet using access control lists (ACLs). Where should the ACLs be deployed?

✓ **A)** routers
✗ **B)** firewalls
✗ **C)** hubs
✗ **D)** modems

Explanation

The ACLs should be deployed on the routers. The ACLs will improve network security by confining sensitive data traffic to computers on a specific subnet.

Firewalls are typically deployed on the public network interfaces. They typically are not involved in any internal traffic. Therefore, deployment ACLs on firewalls would not confine sensitive internal data traffic to computers on a specific subnet. A firewall is classified as a rule-based access control device. Rules are configured on the firewall to allow or deny packet passage from one network to another.

Hubs are typically deployed to connect hosts in a network. Active hubs provide signal regeneration, while passive hubs do not. Hubs do not provide the ability to configure ACLs.

Modems are typically deployed to provide phone line connections. Modems cannot control internal data traffic. However, they can provide security on the phone line connection.

Another valid answer to the question that was not given is a switch. Switches are typically deployed to create virtual local area networks (VLANs). The switch isolates the VLAN from the rest of the network to provide better security for the VLAN. A VLAN restricts flooding to only those ports included in the VLAN.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Router

Mitigating Security Threats Using ACLs, http://www.informit.com/articles/article.aspx?p=102180&seqNum=7

Question #56 of 131

Question ID: 1105156

You need to implement a wireless network for a client. You have two 802.11a, two 802.11b, and two 802.11g wireless access points.

You need to implement three wireless networks that can communicate with each other. Which wireless access points should you use?

- ✗ **A)** the 802.11a and 802.11b wireless access points
- ✗ **B)** the 802.11a and 802.11g wireless access points
- ✓ **C)** the 802.11b and 802.11g wireless access points
- ✗ **D)** You can use all of them together.

Explanation

You should use the 802.11b and 802.11g wireless access points. These two standards operate at the 2.4 GHz frequency and can be used interchangeably.

You cannot use 802.11a wireless access points with 802.11b or 802.11g wireless access points. 802.11a wireless access points operate at the 5 GHz frequency. Therefore, a solution that includes 802.11a will only provide two wireless access points.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Wireless Networks

Question #57 of 131

Question ID: 1105162

Which statement is NOT true regarding Wireless Application Protocol (WAP) Gap?

- ✗ **A)** Sensitive data can be captured while it is on the gateway.
- ✗ **B)** It occurs when the gateway decrypts WTLS transmissions and re-encrypts it with TLS/SSL.
- ✓ **C)** It occurs when WAP 2.0 and earlier are implemented.
- ✗ **D)** The WAP Gap issue involves WTLS.

Explanation

WAP Gap occurs in versions of WAP prior to version 2.0. WTLS is replaced by TLS in WAP 2.0.

The WAP Gap issue involved WTLS. It occurs when the gateway decrypts WTLS transmissions and re-encrypts it with TLS/SSL. Sensitive data can be captures while it is on the gateway.

The Wireless Transport Layer Security Protocol (WTLS) in the Wireless Application Protocol (WAP) stack provides for security between the WAP client and the gateway.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

The WAP Gap, http://sourcedaddy.com/networking/the-wap-gap.html

Question #58 of 131

Question ID: 1111736

Match the descriptions on the left with the network technologies on the right that it BEST matches.

{UCMS id=5744477798924288 type=Activity}

Explanation

The network technologies should be matched with the descriptions in the following way:

- DMZ - A network that is isolated from other networks using a firewall
- VLAN - A network that is isolated from other networks using a switch
- NAT - A transparent firewall solution between networks that allows multiple internal computers to share a single Internet interface and IP address
- NAC - A network server that ensures that all network devices comply with an organization's security policy

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Secure Communication Channels

---

Question #59 of 131

Question ID: 1114723

Which class of IP network addresses has a value of between 128 and 191 for the first octet?

✗ **A)** Class A
✗ **B)** Class D
✗ **C)** Class C
✓ **D)** Class B
✗ **E)** Class E

Explanation

Class B addresses range from 128 to 191 decimal, or 10000000 to 10111111 binary. Note that the first three bits in a class B address are always 100. Class B addresses use the first two octets for the network address and the last two octets for the host address. With two octets to use for the hosts, you can assign the addresses 0.1 through 255.255 for the host ID, which is 00000000.00000001 through 11111111.11111111 in binary.

The address class ranges are listed below in binary and decimal:

Class A - 00000000 - 01111111 - 0 - 126

Class B - 10000000 - 10111111 - 128 - 191

Class C - 11000000 - 11011111 - 192 - 223

Class D - 11100000 - 11101111 - 224 - 239

Class E - 11110000 - 11110111 - 240 - 255

Note that The 127 network address is used for loopback.

Notice that the most significant bit, which is the left-most bit, is a zero for all Class A addresses. For Class B addresses, the zero shifts to the right one place, which means that the two most significant bits in all Class B addresses are 10. The zero shifts again for Class C, which means that the three most significant bits in all Class C addresses are 110. This "shifting" continues for Class D and Class E. Knowing this pattern allows you to determine the class of a binary IP address simply by looking at the most significant bits.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPv4

Network Calculators, http://www.subnetmask.info/

Question #60 of 131

Question ID: 1113966

What should you use to connect a computer to a 100BaseTX Fast Ethernet network?

- ✗ **A)** Use an RG-58 cable with a BNC connector.
- ✗ **B)** Use a fiber-optic cable with an SC connector.
- ✗ **C)** Use a fiber-optic cable with an ST connector.
- ✓ **D)** Use a CAT5 UTP cable with an RJ-45 connector.
- ✗ **E)** Use a CAT5 UTP cable with an RJ-11 connector.

Explanation

Among the available choices, you should use Category 5 unshielded twisted-pair (CAT5 UTP) cable and RJ-45 connectors to connect a computer to a 100BaseTX Ethernet network. On a 100BaseTX network, you can use two pairs of either CAT5 UTP or Type 1 shielded twisted-pair (STP) cable. RJ-45 connectors typically connect computers to a 100BaseTX network. Although an RJ-45 connector is similar in appearance to a standard RJ-11 telephone connector, an RJ-45 connector is wider than an RJ-11 connector. Additionally, an RJ-45 connector supports eight wires, whereas an RJ-11 connector supports up to six wires.

RG-58 coaxial cable and BNC connectors, including BNC barrel connectors and BNC T connectors, are used on 10Base2 Ethernet networks. BNC terminating resistors are also required on both ends of the 10Base2 bus to prevent signals from bouncing back into the cable and corrupting data. Some coaxial implementations require fixed spacing between the connections; twisted pair cabling has no such requirements.

Fiber-optic cable, such as 62.5/125 multimode cable and 8/125 single-mode cable, is used on some types of Ethernet networks, such as 10BaseFB Ethernet and 100BaseFX Fast Ethernet networks. Fiber-optic cables use LC, SC, and ST connectors. Fiber optic cable has three basic physical elements: the core, the cladding, and the jacket. The core is the innermost transmission medium, usually made of glass or plastic. The next outer layer, the cladding, is also made of glass or plastic with different properties than the cladding, and helps to reflect the light back into the core. The outermost layer, the jacket, provides protection from heat, moisture, and other environmental elements.

CAT1, CAT3, CAT5, CAT5e, and CAT6 cable are all twisted pair technologies.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Twisted pair

---

Question #61 of 131

Question ID: 1105221

Which condition might indicate that a network is undergoing a DoS attack?

- ✗ **A)** a slight decrease in network traffic
- ✗ **B)** a slight increase in network traffic
- ✗ **C)** a significant decrease in network traffic
- ✓ **D)** a significant increase in network traffic

Explanation

A significant increase in network traffic might indicate that a network is undergoing a denial of service (DoS) attack, which occurs when a hacker floods a network with requests.

A DoS attack prevents authorized users from accessing resources they are authorized to use. An example of a DoS attack is one that brings down an e-commerce Web site to prevent or deny usage to legitimate customers.

A significant decrease in traffic might indicate a problem with network connectivity or network hardware, or it might indicate a non-DoS hacker attack. Networks with slightly fluctuating traffic levels are probably operating normally.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, DoS

Understanding Denial-of-service attacks, https://www.us-cert.gov/ncas/tips/ST04-015

Question #62 of 131

Question ID: 1114736

You need to solve a traffic problem occurring on a large Ethernet network. Within this large segment, the accounting department is flooding the network with a high volume of data, which causes the entire network to slow down.

Which device is a quick and low-cost solution to isolating the accounting department?

✗ **A)** gateway
✗ **B)** router
✓ **C)** bridge
✗ **D)** repeater

Explanation

A bridge provides a quick and low-cost solution for dividing a network into different segments for the purposes of reducing network traffic. Bridges work by building forwarding tables based on MAC addresses. These forwarding tables enable bridges to determine which packets need to pass through the bridge to another segment versus which packets are to stay on the local segment. Bridges have the capacity to act as a store-and-forward device by storing frames. Properties of bridges include the following:

Forwards the data to all other segments if the destination is not on the local segment

Operates at Layer 2, the Data Link layer

Can create a broadcast storm

In this scenario, the Accounting department is currently sharing the bandwidth of the entire segment. Using a bridge to place this department on its own segment means the traffic of this segment will stay on the local segment, thus

reducing the overall traffic of the network. Only packets destined for other segments will pass through the bridge.

A bridge is not an optimal choice for reducing intersegment traffic. In such a case, a router or gateway would be a better choice.

A router is used to connect networks that are dissimilar in either topology or Internet Protocol (IP) address. It could be used in this scenario, but it would not be a low-cost solution. Routers can be rather costly to implement. Generally you should avoid using two routers to connect your internal network to a demilitarized zone (DMZ) because it then provides multiple paths for attack (sometimes called an increased attack surface).

A gateway is used to connect networks that use different protocols.

A repeater is used to extend the length of network beyond the cable's maximum segment distance. It takes a received frame's signal and regenerates it to all other ports on the repeater.

A special type of router, called a screening router, functions like a packet-filtering firewall based upon port numbers.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Bridge

---

Question #63 of 131

Question ID: 1105214

Which device converts messages between two dissimilar electronic mail (e-mail) applications?

- ✗ **A)** e-mail translator
- ✗ **B)** e-mail server
- ✓ **C)** e-mail gateway
- ✗ **D)** e-mail switch

Explanation

An e-mail gateway converts messages between two dissimilar e-mail applications, for example, between an Exchange server and a Sendmail server. It accomplishes this through the use of the Common Data Network service called mail service.

An e-mail server is the actual company server that manages the e-mail transmissions for an organization, both incoming and outgoing. An e-mail directory is maintained for each e-mail user. This directory will contain the user's sent and received e-mails, as well as document drafts, document copies, and temporary documents.

The other two options are invalid devices.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Gateway

---

Question #64 of 131

Question ID: 1113965

You are designing an Ethernet network. The Ethernet specification you select for the network should support a data transmission rate of 100 megabits per second (Mbps) and a maximum cable segment length of 2,000 meters (m). The cable used in the Ethernet specification you select should also be immune to crosstalk.

Which Ethernet specification should you use on the network?

- ✗ **A)** 100BaseTX
- ✓ **B)** 100BaseFX
- ✗ **C)** 10BaseT
- ✗ **D)** 10Base2

Explanation

Of the Ethernet specifications provided, you should use the 100BaseFX specification on the network. The 100BaseFX Ethernet specification uses fiber-optic cable, which is immune to crosstalk, electromagnetic interference (EMI), and tapping because fiber-optic cable transmits light on a glass or plastic cable rather than transmitting electricity on a copper cable.

Crosstalk is electromagnetic interference that can occur between copper wires that are in close proximity. Crosstalk can occur in unshielded twisted-pair (UTP) cables, shielded twisted-pair (STP) cables, coaxial cables, and other types of cable that use copper wire. The 100BaseFX Ethernet specification supports a data transmission rate of 100 Mbps and a maximum cable segment length of 2,000 m.

The 10Base2 Ethernet specification uses RG-58 coaxial cable. The 10Base2 Ethernet specification supports a data transmission rate of 10 Mbps and a maximum cable segment length of 185 m. The 10BaseT Ethernet specification supports a data transmission rate of 10 Mbps and a maximum cable segment length of 100 m. The 10BaseT specification requires UTP cable. The 100BaseTX Ethernet specification is a version of Fast Ethernet over either Category 5 (CAT5) UTP cable or Type 1 STP cable. The 100BaseTX Fast Ethernet specification supports a data transmission rate of 100 Mbps and a maximum cable segment length of 100 m.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Fiber optic

---

Question #65 of 131

Question ID: 1105137

Which layer of the TCP/IP model corresponds to the Transport layer of the OSI model?

✗ **A)** Internet
✓ **B)** Transport
✗ **C)** Network access
✗ **D)** Application

Explanation

The Transport layer of the TCP/IP model corresponds to the Transport layer of the OSI model.

The Application layer of the TCP/IP model corresponds to the Application, Presentation, and Session layers of the OSI model.

The Internet layer of the TCP/IP mode corresponds to the Network layer of the OSI model. Internet protocol (IP), address resolution protocol (ARP), and Internet control message protocol (ICMP) operate at the Internet layer.

The Network access layer of the TCP/IP model corresponds to the Data-Link and Physical layers of the OSI model.

The OSI model has seven layers; the TCP/IP model has four layers.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, TCP/IP Model

---

Question #66 of 131

Question ID: 1113975

You have deployed a modem to allow remote users to connect to your network. You need to ensure that only users from specific locations can access your network using the modem. What should you deploy?

✗ **A)** RADIUS
✗ **B)** NAT
✗ **C)** TACACS
✓ **D)** Callback

Explanation

You should deploy callback. Callback will ensure that only users from specific locations can access your network using the modem. The feature configures the modem to disconnect from the user once authentication has occurred and to call back the user at a pre-defined number.

Remote Authentication Dial-In User Service (RADIUS) is a service that performs remote user authentication and accounting. Deploying a RADIUS server does not ensure that only users from specific locations can access your network using the modem. Terminal Access Controller Access Control System (TACACS) is a technology similar to RADIUS.

Network Address Translation (NAT) provides a transparent firewall solution between an internal network and outside networks. Using NAT, multiple internal computers can share a single Internet interface and IP address. The primary purpose of NAT is to hide internal hosts from the public network. NAT does not ensure that only users from specific locations can access your network using the modem.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

Callback, http://technet.microsoft.com/en-us/library/cc784461.aspx

---

Question #67 of 131

Question ID: 1114725

Which WLAN technology supports maximum of 11 Mbps data transmission?

- ✓ **A)** 802.11b
- ✗ **B)** 802.11e
- ✗ **C)** 802.11g
- ✗ **D)** 802.11a

Explanation

The 802.11b wireless local area network (WLAN) technology supports maximum data rates of 11 Mbps.

802.11b WLAN clients, access points, and bridges use the Direct Sequence Spread Spectrum (DSSS) for transmission through RF ports. DSSS radio transmission provides data rates between 1 Mbps and 11 Mbps. DSSS uses three types of modulation schemes for Radio Modulation:

Binary Phase Shift Keying (BPSK) for transmitting data rates at 1 Mbps.

Quadrature Phase Shift Keying (QPSK) for transmitting data rates at 2 Mbps.

Complementary Code Keying (CCK) for transmitting data rates at 5.5 Mbps and 11 Mbps.

802.11a WLANs work in the 5-GHz Industrial, Scientific and Medical (ISM) frequency band with Orthogonal Frequency Division Multiplexing (OFDM). OFDM supports a maximum data rate of 54 Mbps.

802.11e provides Quality of Service (QoS) and support for multimedia traffic. This deployment uses the 2.4 GHz (the same as 802.11b) or 5.8 GHz (the same as 802.11a) bands. Therefore, it can operate at 11 Mbps or 54 Mbps.

802.11f provides roaming capabilities for wireless networks at 54 Mbps.

802.11g is an extension of 802.11b. 802.11g increases the speed capability to 54 Mbps.

802.11h is an extension of 802.11a. 802.11h adds European capability to the 802.11a standard.

802.11i adds the Robust Secure Network (RSN) protocol to increase security for wireless networks.

Objective:
Communication and Network Security

Sub-Objective:

Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, 802.11b

Wireless LANs: Extending the Reach of a LAN, http://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=2

Question #68 of 131

Question ID: 1105229

You have discovered that your organization's file server has been overwhelmed by UDP broadcast packets, resulting in a server crash. Which attack has occurred?

✗ **A)** smurf

✓ **B)** fraggle

✗ **C)** teardrop

✗ **D)** ping of death

Explanation

A fraggle attack has occurred. A fraggle attack chokes the processing resources of the victim host by flooding the network with spoofed UDP packets. Fraggle is a denial-of-service (DoS) attack that sends large amounts of spoofed broadcast UDP packets to IP broadcast addresses. This results in the target host being flooded with echo replies from the entire network, causing the system to either freeze or crash.

A smurf attack is similar to a fraggle attack, but it spoofs the source IP address in an ICMP ECHO broadcast packet instead of in UDP packets. Smurf is a DoS attack that uses spoofed broadcast ping messages to flood a target system. In such an attack, the attacker sends a large amount of ICMP echo packets with spoofed source IP address similar to that of the target host to IP broadcast addresses. This results in the target host being flooded with echo replies from the entire network, causing the system to freeze or crash. Other examples of DoS attacks are SYN Flood, Bonk, and Ping of death attacks.

In a teardrop attack, the attacker uses a series of IP fragmented packets, causing the system to either freeze or crash while the packets are being reassembled by the victim host. A teardrop attack is primarily based on the fragmentation implementation of IP. To reassemble the fragments in the original packet at the destination, the host checks the incoming packets to ensure that they belong to the same original packet. The packets are malformed. Therefore, the process of reassembling the packets causes the system to either freeze or crash.

A ping of death is another type of DoS attack that involves flooding the target computer with oversized packets, exceeding the acceptable size during the process of reassembly and causing the target computer to either freeze or crash. Other denial of service attacks are smurf and fraggle.

Objective:

Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Fraggle

---

Question #69 of 131

Question ID: 1114724

Which notation is the network prefix that is used to denote an unsubnetted Class C IP address?

✗ **A)** /16

✗ **B)** /8

✗ **C)** /32

✓ **D)** /24

Explanation

The network prefix /24 is used to denote an unsubnetted Class C IP address. Class-based IP addresses were the first types of addresses assigned on the Internet. The first octet of a Class A IP address is from 1 through 126 in decimal notation; the first octet of a Class A IP address is the network address. The first octet of a Class B IP address is from 128 through 191 in decimal notation; the first two octets of a Class B IP address are the network address. The first octet of a Class C IP address is from 191 through 223; the first three octets of a Class C IP address are the network address.

Subnetting was introduced to enable more efficient use of the IP address space. In subnetting, some host bits of a Class-based IP address are used as network address bits to enable smaller groupings of IP addresses to be created than the groupings offered by Class-based IP addresses. For example, you have an office with 200 computers that reside on four separate networks that consists of 50 computers each. If each network has been assigned its own Class C IP address range, then 204 IP addresses will not be used in each range, for a total of 816 wasted IP addresses. With subnetting, a single Class C IP address range can provide IP addresses for the hosts on all four networks. If you subnetted a single Class C IP address range, then only 48 IP addresses would be wasted.

Before Classless Interdomain Routing (CIDR) was introduced, networks were commonly organized by classes. In a Class C address, the first two bits of the address are set to one, and the third bit of the address is set to zero.

A subnet mask is a 32-bit binary number that can be compared to an IP address to determine which part of the IP address is the host address and which part of the IP address is the network address. Every 1 bit in a subnet mask

indicates a bit in the network address, and every 0 bit in the subnet mask indicates a bit in the host address. For example, on a network that uses an unsubnetted Class C IP address range, the IP address 192.168.0.1 has a subnet mask of 255.255.255.0. In binary notation, 255 is represented as 11111111. In binary notation, the subnet mask 255.255.255.0 is represented as 11111111 11111111 11111111 00000000. The binary representation of the IP address 192.168.0.1 is 11000000 10101000 00000000 00000001. The following is a comparison of the binary subnet mask and the binary IP address:

11111111 11111111 11111111 00000000 Subnet Mask

11000000 10101000 00000000 00000001 IP Address

From this comparison, you can see that the first 24 bits of the IP address, or 192.168.0 in decimal notation, are the network address and the last eight bits of the IP address, or 1 in decimal notation, are the host address.

Another method, called a network prefix, is also used to determine which part of an IP address is the network address and which part of an IP address is the host address. The network prefix method appends a slash (/) character and a number after the IP address, as in the following example:

192.168.0.1/24

In this example, the network prefix indicates that the first 24 bits of the IP address, or 192.168.0 in decimal notation, are the network address and the last 8 bits of the IP address are the host address. This is sometimes referred to as CIDR notation.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IPv4

Network Calculators, http://www.subnetmask.info/

Question #70 of 131

Question ID: 1113952

Which layer of the OSI model is also referred to as Layer 4?

- ✗ **A)** the Presentation layer
- ✗ **B)** the Network layer
- ✗ **C)** the Session layer

✓ **D)** the Transport layer

Explanation

The Transport layer of the Open Systems Interconnection (OSI) model is also referred to as Layer 4. The Transport layer of the OSI model is responsible for connection-oriented or connectionless communications. Connection-oriented communications protocols, such as Transmission Control Protocol (TCP) in the TCP/IP protocol suite, establish a virtual connection between the sending host and the receiving host to provide reliable, error-free data delivery. Connectionless protocols, such as UDP, do not provide the same guaranteed service but create less overhead. Although both types of transport protocols operate at this level, many charts label this layer as connection-oriented since this is the only layer where connection-oriented transport occurs.

Some of the protocols that work at the Transport layer are TCP, User Datagram Protocol (UDP), and Sequenced Packet Exchange (SPX). Secure Sockets Layer (SSL) is comprised of two protocols: one works at the Session layer, and the other works at the Transport Layer. SSL is considered a Transport layer protocol.

The Transport layer does not provide confidentiality, but the Presentation, Network, and Session layers do. The Transport layer manages the control rate of packet transfers. It provides end-to-end services.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Transport

---

Question #71 of 131

Question ID: 1105258

Recently, your organization has become increasingly concerned about hackers. You have been specifically tasked with preventing man-in-the-middle attacks. Which protocol is NOT capable of preventing this type of attack?

✗ **A)** Internet Protocol Security (IPSec)

✓ **B)** Remote shell (rsh)

✗ **C)** HTTP Secure (HTTPS)

✗ **D)** Secure shell (SSH)

Explanation

The remote shell (rsh) protocol is NOT capable of preventing man-in-the-middle (MITM) attacks. The remote shell (rsh) protocol is used to log on to remote computers and can be easily exploited by a man-in-the middle attack because it provides neither encryption nor authentication of data. In a man-in-the-middle attack, an intruder captures the traffic of an established connection to intercept the messages being exchanged between the sender and the receiver. The rsh protocol does not provide security because the traffic flows in cleartext and not ciphertext.

Secure shell (SSH) provides security by authenticating before the exchange of secret keys. SSH is also known as encrypted telnet because it provides encryption of traffic exchanged between the sender and the receiver. Because SSH uses encryption, SSH can prevent man-in-the-middle attacks better than rsh can.

HTTP Secure (HTTPS) is based on the secure socket layer (SSL) protocol. SSL is a two-layered protocol that contains the SSL Record Protocol and the SSL Handshake Protocol. SSL handshake provides an authentication mechanism before the exchange of credentials and prevents attacks, such as man-in-the-middle attacks, and uses certificates to validate the identities of both parties. HTTPS is used for online transactions.

Internet Protocol Security (IPSec) is a security framework established to secure communication over insecure networks, such as the Internet. IPSec deploys an Internet key exchange (IKE) for key exchange and management. IKE manages the first phase of the key negotiation agreement and the secure exchange of keys as a part of the IPSec framework. IPSec prevents man-in-the-middle attacks through encryption and authentication.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Remote Log-in (rlogin), Remote Shell (rsh), Remote Copy (rcp)

Question #72 of 131

Question ID: 1105173

Which type of firewall most detrimentally affects network performance?

- ✗ **A)** stateful firewall
- ✗ **B)** circuit-level proxy firewall
- ✓ **C)** application-level proxy firewall
- ✗ **D)** packet-filtering firewall

Explanation

An application-level proxy firewall most detrimentally affects network performance because it requires more processing per packet.

The packet-filtering firewall provides high performance. Stateful and circuit-level proxy firewalls, while slower than packet-filtering firewalls, offer better performance than application-level firewalls.

Kernel proxy firewalls offer better performance than application-level firewalls.

An application-level firewall creates a virtual circuit between the firewall clients. Each protocol has its own dedicated portion of the firewall that is concerned only with how to properly filter that protocol's data. Unlike a circuit-level firewall, an application-level firewall does not examine the IP address and port of the data packet. Often, these types of firewalls are implemented as a proxy server.

A proxy-based firewall provides greater network isolation than a stateful firewall. A stateful firewall provides greater throughput and performance than a proxy-based firewall. In addition, a stateful firewall provides some dynamic rule configuration with the use of the state table.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #73 of 131

Question ID: 1105158

You suspect that a Windows client computer on your network has been compromised. You need to view the IP address information for the computer. Which tool should you use?

- ✗ **A)** ping
- ✗ **B)** tracert
- ✗ **C)** netstat
- ✓ **D)** ipconfig

Explanation

You should use the ipconfig tool to view the IP address information for a Windows computer. This tool displays a computer's IP address, subnet mask, and default gateway. It can also be used to release and renew a Dynamic Configuration Host Protocol (DHCP) IP address lease.

The ping tool is used to test the availability of a computer over a network. You can ping computers based on their DNS host name or IP address.

The tracert tool is used to determine the route a packet takes across a Windows IP network. UNIX computers have a similar tool called traceroute.

The netstat tool displays incoming and outgoing network connections, routing tables, and network interface statistics.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

The Syntax and Options for using the Ipconfig Diagnostic Utility for Network Connections, https://technet.microsoft.com/en-us/library/cc940124.aspx

---

Question #74 of 131

Question ID: 1105174

Which type of firewall only examines the packet header information?

- ✗ **A)** stateful firewall
- ✗ **B)** kernel proxy firewall
- ✓ **C)** packet-filtering firewall
- ✗ **D)** application-level proxy firewall

Explanation

A packet-filtering firewall only examines the packet header information.

A stateful firewall usually examines all layers of the packet to compile all the information for the state table. A kernel proxy firewall examines every layer of the packet, including the data payload. An application-level proxy firewall examines the entire packet.

Packet-filtering firewalls are based on access control lists (ACLs). They are application independent and operate at the Network layer of the OSI model. They cannot keep track of the state of the connection.

A packet-filtering firewall only looks at a data packet to obtain the source and destination addresses and the protocol and port used. This information is then compared to the configured packet-filtering rules to decide if the packet will be dropped or forwarded to its destination.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #75 of 131

Question ID: 1113974

Which function does start and stop bits provide?

✗ **A)** They mark the beginning and ending of synchronous communication.

✗ **B)** They translate analog signal into digital signals and vice versa using modulation.

✓ **C)** They mark the beginning and ending of asynchronous communication.

✗ **D)** They mark the beginning and ending of a data packet.

Explanation

Start and stop bits mark the beginning and ending of asynchronous communication.

Start and stop bits are not used to mark the beginning and ending of a data packet.

Synchronous communication has no need of start and stop bits because data is transferred as a stream of bits instead of as separate frames.

A modem translates analog signals into digital signals and vice versa. An analog signal produces an infinite waveform. An analog signal can be varied by amplification. A digital signal produces a saw-tooth waveform. Both types of signals can be used to transmit data.

Isochronous data is synchronous data transmitted without a clocking source, with the bits sent continuously and no start or stop bits. All bits are of equal importance and are anticipated to occur at regular time intervals. Pleisiochronous transmission is a transmission method that uses more than one timing source, sometimes running at different speeds. This method may require master and slave clock devices.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Asynchronous Versus Synchronous

---

Question #76 of 131

Question ID: 1111743

Match the descriptions from the left with the attack types on the right.

{UCMS id=5687979517411328 type=Activity}

Explanation

The attack types should be matched with the descriptions in the following manner:

- Dictionary attack - occurs when a hacker tries to guess passwords using a list of common words
- DoS attack - occurs when a server or resource is overloaded so that legitimate users cannot access it
- Pharming attack - occurs when traffic is redirected to a site that looks identical to the intended site
- Phishing attack - occurs when confidential information is requested by an entity that appears to be legitimate

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Glossary

Question #77 of 131

Question ID: 1113945

Match the protocol from the left with the default port it uses on the right. Move the correct items from the left column to the column on the right to match the protocol with the correct default port.

{UCMS id=5752530594168832 type=Activity}

Explanation

The protocols given use these default ports:

- Port 20 - FTP
- Port 23 - Telnet
- Port 25 - SMTP
- Port 53 - DNS
- Port 80 - HTTP

FTP also uses port 21, but it was not listed in this scenario.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IP Networking

---

Question #78 of 131

Question ID: 1114735

Which unshielded twisted-pair (UTP) category consists of four twisted pairs of copper wire and is certified for transmission rates of up to 100 Mbps?

✗ **A)** Category 4
✗ **B)** Category 1
✗ **C)** Category 2
✓ **D)** Category 5
✗ **E)** Category 3

Explanation

Category 5 UTP cabling is the most widely used category of UTP cable. It enables transmission rates of up to 100 Mbps, and it is the highest category of UTP cabling.

UTP transmission rates are as follows:

Category 1 - up to 4 Mbps

Category 2 - up to 4 Mbps

Category 3 - up to 10 Mbps

Category 4 - up to 16 Mbps

Category 5 - up to 100 Mbps

Category 5e - up to 1000 Mbps (1 Gbps)

Category 6 - up to 1000 Mbps (1 Gbps)

Category 6e - up to 1000 Mbps (1 Gbps)

Category 7 - up to 10 Gbps

Category 1 wiring consists of two pairs of twisted copper wire. It is rated for voice grade, not data communication. It is the oldest UTP wiring and is used for communication on the Public Switched Telephone Network (PSTN).

Category 2 wiring consists of four pairs of twisted copper wire and is suitable for data communications of up to 4 Mbps.

Category 3 wiring consists of four pairs of twisted copper wire with three twists per foot. It is suitable for 10 Mbps data communication. It has been the most widely used UTP standard since the mid-1980s, especially for Ethernet networks.

Category 4 wiring consists of four pairs of twisted copper wire and is rated for 16 Mbps. It was designed with 16 Mbps Token Ring networks in mind.

Category 5 wiring consists of four twisted pairs of copper wire terminated by RJ-45 connectors. Category 5 cabling can support frequencies of up to 100 MHz and speeds of up to 100 Mbps. It can be used for ATM, Token Ring, 1000Base-T, 100Base-T, and 10Base-T networking.

NOTE: Category 5e cable is the most commonly used cable for new UTP implementations. The "e" in Category 5e cable stands for "enhanced." This enhanced specification will support bandwidths of up to 350 MHz.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security. Twisted Pair

Data Transmission - Cabling, http://en.kioskea.net/contents/transmission/transcabl.php3

Question #79 of 131

Question ID: 1114719

Which OSI process ensures that each OSI layer at the sender adds its own information to the packet and each OSI layer at the receiver strips off its corresponding information?

✗ **A)** negotiation

✓ **B)** encapsulation

✗ **C)** compression

✗ **D)** encryption

Explanation

Encapsulation is the OSI process that ensures that each OSI layer at the sender adds its own information to the packets and each OSI layer at the receiver strips off its corresponding information. Encapsulation wraps data from one layer around a data packet from an adjoining layer.

Negotiation is the process whereby the communication channel is negotiated. This only occurs at the Session layer of the OSI model.

Compression is the process whereby data is compressed into a smaller format to improve transmission time. This only occurs at the Presentation layer of the OSI model.

Encryption is the process whereby data is encrypted to ensure confidentiality. This only occurs at the Presentation layer of the OSI model. The Network, Data-Link, and Transport layers all support encryption.

The OSI model is defined by seven protocol layers. Its primary purpose is to provide a standard model for network communication to allow dissimilar networks to communicate. The seven layers are as follows:

Layer 1 Physical layer (farthest from user)

Layer 2 Data-Link layer

Layer 3 Network layer

Layer 4 Transport layer

Layer 5 Session layer

Layer 6 Presentation layer

Layer 7 Application layer (closest to user)

OSI provides authentication, confidentiality, logging, application, compression, encryption, communication, transmission, addressing, and monitoring services. It includes security technique standards, layer security standards, protocol standards, and application-specific standards.

Systems that are built on the OSI framework are considered open systems because they are built with internationally accepted protocols and standards to easily communicate with other systems.

Objective:
Communication and Network Security

Sub-Objective:

Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Encapsulation and Deencapsulation

---

Question #80 of 131

Question ID: 1114741

You are deploying a virtual private network (VPN) for remote users. You have decided to deploy the VPN gateway in its own demilitarized zone (DMZ) behind the external firewall.

What are the benefits of this deployment?

a. The firewall can protect the VPN gateway.

b. The firewall can inspect plain text from the VPN.

c. The firewall can inspect all communications from the VPN.

d. The firewall will need special routes to the VPN gateway configured.

- ✗ **A)** options b and c only
- ✗ **B)** option d
- ✗ **C)** option a
- ✗ **D)** option c
- ✗ **E)** option b
- ✗ **F)** options c and d only
- ✓ **G)** options a and b only

Explanation

When you deploy a VPN gateway in its own DMZ behind the external firewall, you receive the following benefits:

The firewall can protect the VPN gateway.

The firewall can inspect plain text from the VPN.

Internet connectivity does not depend on the VPN gateway.

In this deployment, the following drawbacks are experienced:

The firewall will need special routes to the VPN gateway configured.

Roaming client support is hard to achieve.

A firewall can ONLY inspect and log plain text from the VPN. It cannot inspect all communications because most of the communication will be encrypted. A firewall cannot inspect encrypted traffic.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

Record Secure Remote Access SSL VPN Gateway Sessions > Protecting the Internal Network, http://www.petri.co.il/record-secure-remote-access-ssl-vpn-gateway-sessions.htm

---

Question #81 of 131

Question ID: 1105249

What is another term used for Plain Old Telephone Service (POTS)?

✗ **A)** IPSec
✗ **B)** IM
✗ **C)** VoIP
✓ **D)** PSTN

Explanation

Public-switched telephone network (PSTN) is another term used for POTS. This is the standard circuit-switched voice network used for most public telephones in the United States.

Voice over IP (VoIP) is a technology that allows voice transmissions to travel over an IP network.

Internet Protocol Security (IPSec) is a security protocol used on IP networks.

Instant Messaging (IM) is a text-based chatting mechanism that allows text messages to be transmitted over networks.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, PSTN (POTS, PBX)

Question #82 of 131

Question ID: 1105189

A client contacts you regarding an e-mail server problem. When you research the problem, you notice that there is an extremely large number of e-mail messages in the outbound folder. This has caused the hard drive to fill up. You temporarily stop the e-mail server, delete the e-mail messages, and restart the e-mail server. Immediately, the outbound mail folder starts to fill up again.

What is causing the problem you are experiencing?

- ✗ **A)** zombie attack
- ✗ **B)** virus infection
- ✓ **C)** SMTP relay
- ✗ **D)** Trojan horse infection

Explanation

The problem is caused by SMTP relay. Until you disable SMTP relay on the e-mail server, the outbound mail folder will continue to fill up.

None of the other problems would cause the outbound mail folder to immediately fill up.

Zombies are remote-controlled programs that hackers can use to attack networks. Zombies are often programmed to make a hacker attack seem as if it originated from a different computer.

A Trojan horse is malware that is disguised as a useful utility, but contains embedded malicious code. When the disguised utility is run, the Trojan horse performs malicious activities in the background and provides a useful utility at the front end. Trojan horses use covert channels to perform malicious activities, such as deleting system files and planting a back door into a system.

A virus is malicious software (malware) that relies upon other application programs to execute and infect a system. The main criterion for classifying a piece of executable code as a virus is that it spreads itself by means of hosts. The hosts could be any application or file on the system. A virus infects a system by replicating itself through application hosts. Viruses usually include a replication mechanism and an activation mechanism designed with a particular objective in mind.

Objective:
Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Email security

What are the major security issues involved with SMTP relay?, http://searchexchange.techtarget.com/expert/KnowledgebaseAnswer/0,sid43_gci947777,00.html

---

Question #83 of 131

Question ID: 1113954

Which statement is NOT true regarding the Ethernet LAN technology?

- ✗ **A)** It supports full duplex transmissions.
- ✗ **B)** It is defined by IEEE 802.3
- ✗ **C)** It uses carrier sense multiple access with collision detection (CSMA/CD).
- ✓ **D)** It uses a multistation access unit (MAU) as its central device.

Explanation

The Ethernet LAN technology does NOT use a multistation access unit (MAU) as its central device. This is the central device used in the Token Ring technology. Token Ring networks were defined by IEEE 802.5. Token Ring supports full duplex transmission using carrier sense multiple access with collision avoidance (CSMA/CA).

Ethernet supports full duplex transmissions. It uses carrier sense multiple access with collusion detection (CSMA/CD). It is defined by IEEE 802.3.

Full-duplex can transmit and receive information in both directions simultaneously. The transmissions can be asynchronous or synchronous. In asynchronous transmission, a start bit is used to indicate the beginning of transmission. The start bit is followed by data bits, and then one or two stop bits follow to indicate the end of the transmission. Because start and stop bits are sent with every unit of data, the actual data transmission rate is lower than half-duplex because the overhead bits are used for synchronization and do not carry information. In this mode, data is sent only when it is available and the data is not transmitted continuously. In synchronous transmission, the transmitter and receiver have synchronized clocks and the data is sent in a continuous stream. The clocks are synchronized by using transitions in the data and, therefore, start and stop bits are not required for each unit of data sent.

Half-duplex transmissions are transmissions in which information can be transmitted in two directions, but only one direction at a time. Simplex transmissions are communication that takes place in one direction only.

Objective:

Communication and Network Security

Sub-Objective:

Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Ethernet 802.3

Question #84 of 131

Question ID: 1114739

Which network device provides a transparent firewall solution between an internal network and outside networks?

✗ **A)** proxy server

✗ **B)** hub

✓ **C)** NAT router

✗ **D)** router

Explanation

A Network Address Translation (NAT) router provides a transparent firewall solution between an internal network and outside networks. Using NAT, multiple internal computers can share a single Internet interface and IP address. The primary purpose of NAT is to hide internal hosts from the public network. When implementing NAT, your private network should use one of the private network address ranges:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

NAT can use static or dynamic translation. Static translation has static mappings for the NAT communication; dynamic translation has a dynamic table that is configured as hosts attempt to use NAT. NAT can cause problems with a IPSec virtual private network (VPN) tunnel because of changes made to the IP header. NAT is only supported with IPSec when running in NAT traversal mode.

A proxy server is often mistaken as a NAT server. However, a proxy server is not a transparent solution. A proxy server operates at Layer 4 or higher of the OSI model (the Transport layer or above). NAT operates at the Network layer (Layer 3) of the OSI model.

A router is a network device that divides a local area network into smaller subnetworks. Routers operate at the Network layer (Layer 3) of the OSI model. While a firewall can also be a router, it is referred to as a firewall when it functions to

create a DMZ.

A hub is a network device that connects multiple networks together.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Public Versus Private IP Addresses

How Network Address Translation Works, http://computer.howstuffworks.com/nat5.htm

---

Question #85 of 131

Question ID: 1105238

Which Digital Subscriber Line (DSL) implementation offers speeds up to 8 megabits per second (Mbps) and provides faster download speed than upload speed?

✗ **A)** SDSL
✓ **B)** ADSL
✗ **C)** IDSL
✗ **D)** HDSL

Explanation

Asymmetrical Digital Subscriber Line (ADSL) offers speeds up to 8 megabits per second (Mbps) and provides faster download speed than upload speed.

High-bit-rate DSL (HDSL) offers speeds up to 1.544 Mbps over regular UTP cable.

ISDN DSL (IDSL) offers speeds up to 128 kilobits per second (Kbps).

Symmetrical DSL (SDSL) offers speeds up to 1.1 Mbps. Data travels in both directions at the same rate.

Another type of DSL is Very high bit-rate Digital Subscriber Line (VDSL). VDSL transmits at super-accelerated rates of 52 Mbps downstream and 12 Mbps upstream.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, DSL

Question #86 of 131

Question ID: 1105230

Which condition might indicate that a hacker is attacking a network?

- ✗ **A)** a router that is transmitting traffic
- ✗ **B)** a slight increase in network traffic
- ✓ **C)** a major increase in ICMP traffic
- ✗ **D)** a slight decrease in network traffic

Explanation

A major increase in Internet Control Message Protocol (ICMP) traffic indicates that a hacker might be attacking a network with a ping of death denial-of-service (DoS) attack.

A slight increase or decrease in the baseline of network traffic is expected in general network operations. Major or sudden increases or decreases in network traffic might indicate that a network is under attack by a hacker. A router is a device that is designed to transmit traffic between networks.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, DoS

Question #87 of 131

Question ID: 1302571

You must propose a cabling scheme for your company's new location. Several departments are located on the same floor with a maximum distance of 61 meters (200 feet) between departments. You want a relatively easy, low-cost installation with simple connections.

Which type of cabling would you propose?

- ✗ **A)** ThickNet
- ✗ **B)** Fiber-optic
- ✗ **C)** ThinNet
- ✓ **D)** Twisted-pair

Explanation

Twisted-pair cabling is the least expensive cabling media. Because unshielded twisted-pair (UTP) is commonly used in telephone systems, it is mass-produced, making it inexpensive and widely available. In addition, twisted-pair cabling is very easy to work with, meaning that very little training is required for its installation.

As in telephone systems, twisted-pair cabling uses Registered Jack (RJ) connectors to connect cables to components. Computer networks use the larger RJ-45 connectors, which are very similar to the commonly known RJ-11 connectors used in telephone systems; this adds to the simplicity of installing twisted-pair.

Twisted-pair has a maximum length of 100 meters (328 feet), which will work for the company in the scenario because the offices are located within 61 meters (200 feet) of each other. It is important to note that twisted-pair is the networking cable type most susceptible to attenuation, which is why its maximum distance is 100 meters (328 feet).

The following is a table of network media comparisons:

Cable Name	Type	Data Rate	Max Length
10Base2	Coaxial	10 Mbps	185 m
10Base5	Coaxial	10 Mbps	500 m
10BaseT	UTP	10 Mbps	100 m
10BaseF	Fiber-optic	10 Mbps	2 km
100BaseT	UTP	100 Mbps	100 m
100BaseT4	UTP	100 Mbps	100 m
100BaseTX	UTP/STP	100 Mbps	100 m
100BaseFX	Fiber-optic	100 Mbps	412 m - multi-mode, half duplex 2 km - multi-mode, full duplex 10 km - single-mode, full duplex
100VG-AnyLAN	UTP	100 Mbps	100 m (Cat 3) 213 m (Cat 5
1000BaseT	UTP	1 Gbps	100 m
1000BaseSX	multi-mode fiber-optic	1 Gbps	275 m - 62.5 micron multi-mode, half duplex 316 m - 50 micron multi-mode, half duplex 275 m - 62.5 micron multi-mode, full duplex 550 m - 50 micron multi-mode, full duplex
1000BaseLX/LH	Fiber-optic	1 Gbps	316 m - multi-mode / single-mode, half duplex 550 m - multi-mode, full duplex 5 km - single-mode, full duplex
1000BaseZX	single-mode fiber-optic	1 Gbps	100 m
1000BaseCX	STP	1 Gbps	25 m
10GBaseSR	multi-mode fiber-optic	10 Gbps	300 m - 50 micron, multi-mode, half duplex
10GBaseLR	single-mode fiber-optic	10 Gbps	10 km - single-mode only
10GBaseER	single-mode fiber-optic	10 Gbps	40 km - single-mode only
10GBaseSW	multi-mode fiber-optic	10 Gbps	33 m - 62.5 micron, multi-mode, half duplex
10GBaseLW	single-mode fiber-optic	10 Gbps	10 km - single-mode only
10GBaseEW	single-mode fiber-optic	10 Gbps	40 km - single-mode only
10GBaseT	UTP, STP	10 Gbps	55 m - Cat 6 100 m - Cat 6a

Objective:

Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security. Twisted Pair

CCNA: Network Media Types > Twisted-Pair Cable, http://www.ciscopress.com/articles/article.asp?p=31276

Question #88 of 131

Question ID: 1113948

You want to use the IANA-designated private IP address range that private IP address range with a maximum of 16 bits to provide host IP addresses.

Which IP address is a valid host IP address in this range?

✗ **A)** 11.0.1.0

✗ **B)** 172.30.250.10

✗ **C)** 10.251.250.100

✓ **D)** 192.168.0.1

Explanation

Of the IP addresses listed, 192.168.0.1 is a valid host address within the range of IANA-designated private IP addresses that provide a maximum of 16 bits per host address. The IP address 11.0.1.0 is a public, or external, IP address.

The Internet Engineering Task Force (IETF) is a working group that creates standards for the Internet. The IETF is divided into a number of smaller committees, including the Internet Assigned Numbers Association (IANA), which decides how the IP address space is used. The IANA has reserved three address spaces for private or internal IP addressing. Internal IP addresses are never assigned by the IANA for use on the public Internet. The private IP address ranges are as follows: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Note that the number after the slash (/) character is referred to as the network address prefix, which indicates the number of bits in the network address.

Private IP addresses in the range 192.168.0.0/16 can be used as a Class B address space with a 16-bit network address and a 16-bit host address, or they can be subnetted into Class C addresses. Valid host IP addresses in this address space range from 192.168.0.1 through 192.168.255.254. The first 16 bits in the address correspond to the network address, and the last 16 bits in the address correspond to the host address.

The internal IP address range 10.0.0.0/8 provides IP addresses with an 8-bit network address and a 24-bit host address. The first 8 bits of a 10.0.0.0/8 internal IP address correspond to the network address, and the last 24 bits correspond to the host address. Valid host IP addresses in this address space range from 10.0.0.1 through 10.255.255.254. The address 10.251.250.100 is a valid host IP address in this range.

The 172.16.0.0/12 private IP address range provides a 12-bit network address and a 20-bit host address. IP addresses in the range of 172.16.0.1 through 172.31.255.254 are valid host IP addresses for this address space; the first 12 bits correspond to the network address, and the last 20 bits correspond to the host address. The IP address 172.30.250.10 is a valid host IP address in the range 172.16.0.0/12.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Public Versus Private IP Addresses

What is a Private IP Address?, http://compnetworking.about.com/od/workingwithipaddresses/f/privateipaddr.htm

Question #89 of 131

Question ID: 1105195

In your organization's Windows network, you have implemented policies that allow users to only log in to the network from certain workstations. What concept does this action represent?

- ✓ **A)** enforced path
- ✗ **B)** security domain
- ✗ **C)** trusted path
- ✗ **D)** security kernel

Explanation

An enforced path is an access control method that limits the paths through which a user can access resources. An example of an enforced path is when an organization configures policies that allow users to only log in to the network from certain workstations.

A trusted path is a mechanism that allows a user to communicate with the trusted computing base (TCB). A security domain is a set of resources that are managed by the same security policy and security group. A security kernel is the hardware, firmware, and software resources of a TCB.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

Enforced path, http://www.yourwindow.to/information-security/gl_enforcedpath.htm

Question #90 of 131

Question ID: 1114744

Which job is NOT provided by a network protocol analyzer?

- ✓ **A)** detect active viruses or malware on the network
- ✗ **B)** provide network activity statistics
- ✗ **C)** identify the sources and destinations of communications

✗ **D)** identify the types of traffic on the network

Explanation

A network protocol analyzer does not detect active viruses or malware on the network.

Most network protocol analyzers provide the following functions:

Provide network activity statistics.

Identify the sources and destinations of communications.

Identify the types of traffic on the network.

Detect unusual level of traffic.

Detect specific pattern characteristics.

A network protocol analyzer can determine if passwords are being transmitted over the network in clear text. It can also be used to read the contents of any File Transfer Protocol (FTP) packet, including an FTP GET request. WireShark is a commercial network protocol analyzer.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Network Attacks

Network analyzer, http://searchnetworking.techtarget.com/sDefinition/0,sid7_gci1196637,00.html

---

Question #91 of 131

Question ID: 1105200

What is a disadvantage of a hardware firewall when comparing it to a software firewall?

✗ **A)** It has lower performance capability than a software firewall.

✓ **B)** It has a fixed number of interfaces available.

✗ **C)** It is easier to make configuration errors than in a software firewall.

✗ **D)** It provides decreased security as compared to a software firewall.

Explanation

A hardware firewall is purchased with a fixed number of interfaces available. With a software firewall, adding interfaces is as easy as adding and configuring another network interface card (NIC).

A hardware firewall outperforms a software firewall. It is easier to make configuration errors in a software firewall, not a hardware firewall. Most hardware firewalls are advertised as "turn-key" solutions, meaning software installation and configuration issues are minimal. Hardware firewalls generally provide increased security over software firewalls.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

Comparing Firewall Features, http://www.windowsecurity.com/articles/Comparing_Firewall_Features.html

---

Question #92 of 131

Question ID: 1105254

In which type of network is trust NOT a primary concern?

- ✗ **A)** directory service domains
- ✗ **B)** distributed environment
- ✓ **C)** virtual private network (VPN)
- ✗ **D)** Kerberos

Explanation

Trust is NOT a primary concern in a virtual private network (VPN). A VPN is a secure, private network that is isolated from an organization's internal private network. The VPN allows users to connect to it over a public network, such as the Internet.

Trust is a primary concern in directory service domains, Kerberos environments, and distributed environments.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, VPN

Question #93 of 131

Question ID: 1105236

Which option BEST described a MAN?

- ✓ **A)** a network backbone that connects LANs to WANs
- ✗ **B)** a network that connects other smaller networks over an international connection
- ✗ **C)** a network that provides a private tunnel over a public network
- ✗ **D)** a network that connects a single building or group of buildings to share resources

Explanation

A metropolitan area network (MAN) is a network backbone that connects local area networks (LANs) to wide area networks (WANs).

There are three main types of data networks: LANs, MANs, and WANs.

A LAN is a network that connects a single building or group of buildings to share resources. A WAN is a network that connects other smaller networks over an international connection. A virtual private network (VPN) is a network that provides a private tunnel over a public network.

A wireless LAN (WLAN) is a wireless local area network. A virtual private network (VPN) is a private network that is accessed via a public network, such as the Internet.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, MAN

Question #94 of 131

Question ID: 1114734

What are characteristics of the cut-through switching method?

a. Frames are discarded if they are runts or giants.

b. It has less latency than the store-and-forward method.

c. The cyclic redundancy check (CRC) is computed after a frame is copied to the switch's buffer.

d. Only the destination address is copied into the switch's buffer before a frame is forwarded to its destination.

✗ **A)** options a and c only
✗ **B)** option a
✗ **C)** option d
✓ **D)** options b and d only
✗ **E)** option c
✗ **F)** option b

Explanation

The cut-through method copies a frame's destination address to the switch's buffer and then sends the frame to its destination. This method results in reduced latency compared to switches using the store-and-forward method. Latency is essentially the delay that occurs while the frame traverses the switch. The cut-through switching method generally has less latency, and maintains constant latency since the switch forwards the frame as soon as it reads the destination address. This results in faster frame processing through the switch. However, switches configured to use the cut-through method do not perform any error checking.

The store-and-forward method copies an entire frame to its buffer, computes the cyclic redundancy check (CRC), and discards frames containing errors as well as runt frames (less than 64 bytes) and giant frames (greater than 1,518 bytes). Because the switch must receive the entire frame before forwarding, latency through the switch varies with the frame length. This causes more latency compared to switches using the cut-through method.

You should base your decision as to which switching method to use on a network on whether error checking or consistent latency is the bigger concern. Configure your switches to use the store-and-forward switching method rather than the cut-through switching method when you want the switches to perform error checking and you do not mind inconsistent latency or slower throughput. Configure your switches to use the cut-through switching method when you need constant latency or faster throughput, and do not need error checking.

In addition to the two main switching methods, cut-through and store-and-forward, there is also a modified cut-through method known as "fragment-free." Because collisions normally occur within the first 64 bytes of a frame, fragment-free reads these bytes before forwarding the frame. This allows the fragment-free method to filter out collision frames.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

How LAN switches work, https://computer.howstuffworks.com/lan-switch.htm

---

Question #95 of 131

Question ID: 1105206

Which type of firewall hides a packet's true origin before sending it through another network?

- ✗ **A)** bastion host
- ✓ **B)** proxy firewall
- ✗ **C)** packet-filtering firewall
- ✗ **D)** stateful firewall

Explanation

A proxy firewall hides a packet's true origin before sending it through another network. The primary security feature of a proxy firewall is that it hides the client information. It is the only computer on a network that communicates with untrusted computers.

A bastion host is a hardened system that usually resides on a demilitarized zone (DMZ) and is accessed frequently.

A stateful firewall forwards packets on behalf of the client. It examines each packet and permits or denies it passage based on many factors, including the state table. The state table is used to track where in the TCP handshake a connection is so that any frames that arrive that are received out of normal sequence (an indicator of possible malicious activity) can be dropped. This type of firewall is also often referred to as a stateful-inspection firewall.

A packet-filtering firewall forwards packets based on rules that define which traffic is permitted and denied on the network. A packet filtering firewall examines the data packet to get information about the source and destination addresses of an incoming packet, the session's communications protocol (TCP, UDP or ICMP), and the source destination application port for the desired service.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Types

Question #96 of 131

Question ID: 1114738

Which characteristics apply to Fast Ethernet 100Base-TX networks?

a. 100 Mbps data-transmission rate

b. Two pairs of Category 5 UTP cabling

c. Four pairs of Category 3, 4, or 5 UTP cabling

d. Maximum segment length of 100 meters (328 feet)

e. Maximum segment length of 412 meters (1,352 feet) half-duplex

- ✗ **A)** option b
- ✗ **B)** option d
- ✗ **C)** options a, c, and e only
- ✗ **D)** option a
- ✗ **E)** options a, b, and e only
- ✗ **F)** option e
- ✓ **G)** options a, b, and d only
- ✗ **H)** option c
- ✗ **I)** options a, c, and d only

Explanation

100Base-TX, known as Fast Ethernet, uses two pairs of Category 5 UTP cable. Standard RJ-45 connectors are used. 100Base-TX transmits data at 100 Mbps using the baseband signaling type. Its maximum segment distance is 100 meters (328 feet).

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Twisted Pair

Question #97 of 131

Question ID: 1105219

You are the security administrator for your organization. A user in the IT department informs you that a print server was recently the victim of a teardrop attack. Which statement correctly defines the attack that has occurred?

✗ **A)** It involves the use of invalid packets that have the same source and destination addresses.

✗ **B)** It involves taking advantage of the oversized ICMP packets and causing the system to either freeze or crash.

✗ **C)** It floods the target host with spoofed SYN packets and causes the host to either freeze or crash.

✓ **D)** It involves the use of malformed fragmented packets and causes the target system to either freeze or crash.

Explanation

In a teardrop attack, the attacker uses a series of fragmented Internet Protocol (IP) packets and causes the system to either freeze or crash while the packets are being reassembled by the target host. A teardrop attack is primarily based on the fragmentation implementation of IP. To reassemble the fragments in the original packet at the destination, the host seeks incoming packets to ensure that they belong to the same original packet. The packets are malformed. Therefore, the process of reassembling the packets causes the system to either freeze or crash.

In a land attack, invalid packets having the same source and destination addresses are used. A land attack involves sending a spoofed TCP SYN packet with the target host's IP address and an open port serving as the source and destination both to the target host on an open port. The land attack causes the system to freeze or crash because the machine continuously replies to itself.

In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. The Transmission Control Protocol (TCP) uses the synchronize (SYN) and acknowledgment (ACK) packets to establish communication between two host computers. The exchange of the SYN, SYN-ACK, and ACK packets between two host computers is referred to as handshaking. The attackers flood the target computers with a series of SYN packets to which the target host computer replies. The target host computer then allocates resources to establish a connection. The IP address is spoofed. Therefore, the target host computer never receives a valid response in the form of ACK packets from the attacking computer. When the target computer receives many such SYN packets, it runs out of resources to establish a connection with the legitimate users and becomes unreachable for processing of valid requests.

In a denial-of-service (DoS) attack, the target computer is flooded with numerous oversized Internet Control Message Protocol (ICMP) or User Datagram Protocol (UDP) packets. These packets, which either consume the bandwidth of the target network or overload the computational resources of the target system, cause loss of network connectivity and services. Ping of death, smurf, bonk, and fraggle are examples of DoS attacks.

Objective:

Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Teardrop

---

Question #98 of 131

Question ID: 1114731

Which type of firewall first examines a packet to see if it is the result of a previous connection?

- ✗ **A)** application-level proxy firewall
- ✗ **B)** circuit-level proxy firewall
- ✓ **C)** stateful firewall
- ✗ **D)** packet-filtering firewall

Explanation

A stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table.

None of the other firewalls first examine a packet to see if it is the result of a previous connection.

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Stateful firewalls perform the following tasks:

Scan information from all layers in the packet.

Save state information derived from previous communications, such as the outgoing port information, so that incoming data communication can be verified against it.

Provide tracking support for connectionless protocols through the use of session state databases.

Allow state information derived from other applications access through the firewall for authorized services only, such as previously authenticated users.

Evaluate and manipulate flexible expressions based on communication and application derived state information.

Stateful firewalls can be used to track connectionless protocols, such as the User Datagram Protocol (UDP), because they examine more than the packet header.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #99 of 131

Question ID: 1114730

Which type or types of firewalls operate at the Network layer of the OSI model?

a. stateful firewall

b. kernel proxy firewall

c. packet-filtering firewall

d. circuit-level proxy firewall

e. application-level proxy firewall

- ✗ **A)** option e
- ✗ **B)** options b, d, and e only
- ✗ **C)** option a
- ✗ **D)** all of the options
- ✗ **E)** option b
- ✓ **F)** options a and c only
- ✗ **G)** option d
- ✗ **H)** option c

Explanation

Stateful and packet-filtering firewalls operate at the Network and Transport layer of the OSI model. Stateful firewalls also operate at the data-link layer.

Circuit-level proxy firewalls operate at the Session layer.

Kernel proxy and application-level proxy firewalls operate at the Application layer of the OSI model.

Firewalls connect private and public networks. Their primary purpose is to protect the private network from security breaches by creating security checkpoints at the boundaries between the private and public networks. Firewalls create bottlenecks between the private and public networks because they must examine the packets that pass through them. If a dedicated firewall exists on your network, it will allow the centralization of security services.

Firewalls provide packet filtering, Network Address Translation (NAT), proxy, and encrypted tunnel services, among other things. The encrypted tunnel services are probably the least important service provided by firewalls.

Most firewalls include a protocol-filtering component that allows security administrators to configure firewall behavior based on protocols it encounters. The rule enforcement engine of a firewall ensures that the rules configured by the security administrator are enforced. Most firewalls include an extended logging function that allows security administrators to audit firewall activities.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #100 of 131

Question ID: 1105178

Which firewall architecture has two network interfaces?

- ✗ **A)** screened host
- ✓ **B)** dual-homed firewall
- ✗ **C)** bastion host
- ✗ **D)** screened subnet

Explanation

A dual-homed firewall has two network interfaces. One interface connects to the public network, usually the Internet. The other interface connects to the private network. The forwarding and routing function should be disabled on the firewall to ensure that network segregation occurs.

A bastion host is a computer that resides on a network that is locked down to provide maximum security. These types of hosts reside on the front line in a company's network security systems. The security configuration for this entity is

important because it is exposed to un-trusted entities. Any server that resides in a demilitarized zone (DMZ) should be configured as a bastion host. A bastion host has firewall software installed, but can also provide other services.

A screened host is a firewall that resides between the router that connects a network to the Internet and the private network. The router acts as a screening device, and the firewall is the screen host.

Screened subnet is another term for a demilitarized zone (DMZ). Two firewalls are used in this configuration: one firewall resides between the public network and DMZ, and the other resides between the DMZ and private network.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Firewall Architecture

---

Question #101 of 131

Question ID: 1113968

Which technology centralizes authentication, accounting, and per-command authorization?

✗ **A)** RADIUS
✓ **B)** TACACS+
✗ **C)** AD
✗ **D)** LDAP

Explanation

Terminal Access Controller Access Control System (TACACS+) centralizes authentication, accounting, and per-command authorization. TACACS+ enables two-factor authentication, enables a user to change passwords, and resynchronizes security tokens.

Remote Authentication Dial-In User Service (RADIUS) offers a centralized system for authentication. RADIUS does not offer centralized accounting or per-command authorization, but is more widely supported than TACACS+.

Active Directory (AD) is a directory service supported on Windows networks. Lightweight Directory Access Protocol (LDAP) is used to create a connection between directory services or between a directory service and a client.

Objective:

Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, RADIUS and TACACS+

TACACS+ and RADIUS Comparison,
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

---

Question #102 of 131

Question ID: 1114728

You have discovered that hackers are gaining access to your WEP wireless network. After researching, you discover that the hackers are using war driving. You need to protect against this type of attack.

What should you do?

a. Change the default Service Set Identifier (SSID).

b. Disable SSID broadcasts.

c. Configure the network to use authenticated access only.

d. Configure the WEP protocol to use a 128-bit key.

- ✗ **A)** option c
- ✗ **B)** option d
- ✗ **C)** option a
- ✗ **D)** options a and b only
- ✗ **E)** all of the options
- ✗ **F)** option b
- ✓ **G)** options a, b, and c only

Explanation

You should complete all of the following steps to protect against war-driving attacks:

Change the default SSID.

Disable SSID broadcasts.

Configure the network to use authenticated access only.

Some other suggested steps include:

Implement Wi-Fi Protected Access (WPA) or WPA2 instead of WEP.

Reduce the access point signal strength.

War driving is a method of discovering 802.11 wireless networks by driving around with a laptop and looking for open wireless networks. NetStumbler is a common war-driving tool.

Previously, one of the ways to protect against this attack was to configure the WEP protocol to use a 128-bit key. However, it has since been proven that all versions of WEP are susceptible to attacks.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

War driving, https://searchmobilecomputing.techtarget.com/definition/war-driving

---

Question #103 of 131

Question ID: 1114748

Your company consists of 75 employees. Your company has entered into a partnership with another company that is located across the country. Your company's users must be able to connect to the partner's network quickly and reliably. Support for voice, data, and imaging transmissions and a dedicated 24-hour link are required. Your solution must be as inexpensive as possible while providing enough bandwidth for your company's employees.

Which technology should you implement?

- ✗ **A)** ISDN
- ✗ **B)** POTS
- ✓ **C)** T1
- ✗ **D)** ATM
- ✗ **E)** FDDI

Explanation

T1 lines can provide fast, digital connections of up to 1.544 Mbps, transmitting voice, data, and video. A T1 line also provides a dedicated connection, which means that it provides a 24-hour link. A T1 line is more expensive than a dial-

up connection using Plain Old Telephone Service (POTS) or an Integrated Services Digital Network (ISDN) connection, but this company needs enough bandwidth to accommodate its 75 users, which justifies the additional cost. If the full bandwidth of the T1 proves too costly or unnecessary, fractional T1 is available. With a fractional T1, you can subscribe to one or more of the 24 available channels at a lower cost than T1.

Asynchronous Transfer Mode (ATM) is a high-speed, packet-switching link type transmitting up to 2.488 Mbps. ATM requires expensive equipment to implement. Therefore, it is a costly alternative and is typically used by Internet backbones.

Fiber Distributed Data Interface (FDDI) is a high-speed, Token Ring network that uses fiber-optic cable transmitting up to 100 Mbps. Although it does offer speed, it is limited to a ring distance of 100 kilometers or 62 miles. Even if distance were not a factor, the fiber medium makes this alternative too costly.

Integrated Services Digital Network (ISDN) provides a direct, point-to-point digital connection at a speed of up to 2 Mbps. Usually though, speeds of 128 Kbps are seen with ISDN. However, it is a dial-up connection; therefore, it would not provide a dedicated 24-hour link.

Plain Old Telephone Service (POTS) uses standard telephone wiring, which makes it a low-cost solution, but it would not offer the fast connection desired, nor would it offer a dedicated 24-hour link, as it is a dial-up connection.

Packet-switching technologies include X.25, ATM, frame relay, and Voice over IP (VoIP). Packet-switching technologies have the following properties:

Packets are assigned sequence numbers.

Burst traffic occurs.

Network is connectionless.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, T Lines

---

Question #104 of 131

Question ID: 1111740

Match the descriptions on the left with the attack types on the right.

{UCMS id=5733523484835840 type=Activity}

Explanation

The attacks should be matched with the descriptions in the following manner:

- Brute force attack - occurs when a hacker tries all possible values for such variables as user names and passwords
- DNS poisoning - occurs when IP addresses and host names are given out with the goal of traffic diversion
- Man-in-the-middle attack - occurs when a hacker intercepts messages from a sender, modifies those messages, and sends them to a legitimate receiver
- Smurf - occurs when a combination of Internet Protocol (IP) spoofing and Internet Control Message Protocol (ICMP) messages saturates a network

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Glossary

Question #105 of 131

Question ID: 1105223

A client contacts you regarding an e-mail server problem. When you research the problem, you notice that there is an extremely large number of e-mail messages in the outbound folder. This has caused the hard drive to fill up. You temporarily stop the e-mail server, delete the e-mail messages, and restart the e-mail server. Immediately, the outbound mail folder starts to fill up again.

Which type of problem are you experiencing?

✗ **A)** zombie attack
✗ **B)** Trojan horse infection
✓ **C)** SMTP relay
✗ **D)** virus infection

Explanation

SMTP relay is the problem you are experiencing, Until you disable SMTP relay on the e-mail server, the outbound mail folder will continue to fill up.

None of the other problems would cause the outbound mail folder to immediately fill up.

Zombies are remote-controlled programs that hackers can use to attack networks. Zombies are often programmed to make a hacker attack seem as if it originated from a different computer.

A Trojan horse is malware that is disguised as a useful utility, but contains embedded malicious code. When the disguised utility is run, the Trojan horse performs malicious activities in the background and provides a useful utility at the front end. Trojan horses use covert channels to perform malicious activities, such as deleting system files and planting a back door into a system.

A virus is malicious software (malware) that relies upon other application programs to execute and infect a system. The main criterion for classifying a piece of executable code as a virus is that it spreads itself by means of hosts. The hosts could be any application or file on the system. A virus infects a system by replicating itself through application hosts. Viruses usually include a replication mechanism and an activation mechanism designed with a particular objective in mind.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Spam

What are the major security issues involved with SMTP relay?,
http://searchexchange.techtarget.com/expert/KnowledgebaseAnswer/0,sid43_gci947777,00.html

---

Question #106 of 131

Question ID: 1105139

Which OSI layer is responsible for formatting data?

- ✓ **A)** Presentation
- ✗ **B)** Application
- ✗ **C)** Network
- ✗ **D)** Data Link

Explanation

The Presentation layer, or Layer 6, is normally a part of the operating system. Its main responsibilities include formatting data, encrypting data, and translating packets it receives. This layer translates between application and network data formats.

The Presentation layer works to transform data into the form that the Application layer can accept. It formats and encrypts data to be sent across a network, providing freedom from compatibility problems. An example of a protocol that operates at this layer is the MIDI digital music protocol.

Both the Presentation and Session layers provide TCP/IP end-to-end security.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Presentation

---

Question #107 of 131

Question ID: 1192940

Which ports are known as the well-known ports?

- ✓ **A)** ports 0 through 1023
- ✗ **B)** ports 49152 through 65535
- ✗ **C)** ports 1024 through 49151
- ✗ **D)** ports 1024 through 65535

Explanation

Ports 0 through 1023 are the well-known ports. The Internet Assigned Numbers Authority (IANA) assigns these ports. Not all of these port numbers are assigned to a protocol.

Ports 1024 through 65535 are known as dynamic ports because they can be assigned by operating systems as needed. Ports 1024 through 49151 are registered ports, meaning that various applications and services have registered their use with the IANA. Most companies limit dynamic ports to those numbering 49152 through 65535 so as not to interfere with those reserved by certain applications and services.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Common TCP/UDP Port Numbers

---

Question #108 of 131

Question ID: 1105257

An organization wants to implement a remote dial-in server to ensure that personnel can connect to the organization's network from remote locations. The authentication protocol must include encryption to prevent hackers from accessing the network. Which protocol should be used?

✓ **A)** CHAP

✗ **B)** PAP

✗ **C)** SAP

✗ **D)** LDAP

Explanation

Challenge Handshake Authentication Protocol (CHAP) uses a challenge-response method to authenticate a user. Encrypted authentication applies a digital signature algorithm to the data bits that are sent from the claimant to the verifier. In CHAP, a logon request is sent from the user to the authentication server. The server responds by sending a challenge with a random value to the user. The user encrypts this challenge with a predefined password. The server denies or grants access to the user by decrypting the challenge response and comparing it to the value received from the user.

Password Authentication Protocol (PAP) is an authentication protocol used to authenticate users over Point-to-Point Protocol (PPP) networks. PAP identifies and authenticates users who attempt to access the network from remote locations. PAP sends credentials in clear text over the network. PAP does not use any form of encryption during authentication and is not used very often because of its security concerns.

Service Advertisement Protocol (SAP) is an IPX protocol. File and print servers advertise their addresses and services through SAP every 60 seconds. The routers listen to SAP advertisements and build a table of all known services along with their network addresses. This information is advertised through SAP every 60 seconds. The local router responds to the file, printer, or gateway service query with the network address of the requested service. The client can directly contact the service. SAP does not provide encrypted authentication.

Lightweight Directory Access Protocol (LDAP) is a networking protocol. It queries and modifies directory services running over TCP/IP. A client initiates an LDAP session by connecting to the TCP port 389 on the LDAP server. The server responds to the operation requests from the client in a sequential manner. LDAP does not provide encrypted authentication.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Remote Authentication Protocols

Cisco- Understanding and Configuring PPP CHAP Authentication,
http://www.cisco.com/warp/public/471/understanding_ppp_chap.html

---

Question #109 of 131

Question ID: 1105225

Which protocol uses port 1812 to communicate with dial-up users?

- ✓ **A)** RADIUS
- ✗ **B)** TACACS
- ✗ **C)** SLIP
- ✗ **D)** PPP

Explanation

Remote Authentication Dial-In User Service (RADIUS) uses port 1812 to communicate with dial-up users. It is a UDP-based protocol.

Point-to-Point Protocol (PPP) is an encapsulation protocol used to transmit data over telephone lines. It does not use any ports because PPP encapsulation information is removed when the data reaches a computer network.

Serial Line Internet Protocol (SLIP) is an older encapsulation protocol that was used before PPP was created. Its operation is similar to PPP but does not provide error correction and does not provide different authentication methods.

Terminal Access Controller Access Control System (TACACS) uses port 49 to communicate with dial-up users. It is a UDP-based protocol. TACACS+ uses port 65 to communicate with dial-up users. It is a TCP-based protocol.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, RADIUS and TACACS+

Port Numbers, http://www.iana.org/assignments/port-numbers

Question #110 of 131

Question ID: 1114732

You have configured the following filters on your company's packet-filtering firewall:

Permit all traffic to and from local hosts.

Permit all inbound TCP connections.

Permit all SSH traffic to linux1.kaplanit.com.

Permit all SMTP traffic to smtp.kaplanit.com.

Which rule will most likely result in a security breach?

- ✗ **A)** Permit all SMTP traffic to smtp.kaplanit.com.
- ✓ **B)** Permit all inbound TCP connections.
- ✗ **C)** Permit all traffic to and from local hosts.
- ✗ **D)** Permit all SSH traffic to linux1.kaplanit.com.

Explanation

The Permit all inbound TCP connections rule will most likely result in a security breach. This rule is one you will not see in most firewall configurations. By simply allowing all inbound TCP connections, you are not limiting remote hosts to certain protocols. Security breaches will occur because of this misconfiguration. You should only allow those protocols that remote hosts need. You should drop all others.

In most cases, permitting all traffic to and from local hosts is a common firewall rule. If you configure firewall rules regarding local host traffic, you should use extreme caution. It is hard to predict the type of traffic originating with your local hosts. If you decide to drop certain types of traffic, users may complain about being unable to reach remote hosts.

Limiting certain types of traffic, such as SSH and SMTP traffic, to certain computers is a common firewall configuration. By using this type of rule, you can protect the other computers on your network from security breaches using those protocols or ports.

Other common firewall packet filters include dropping inbound packets with the Source Routing option set, dropping router information exchange protocols, and dropping inbound packets with an internal source IP address. For the most part, filters blocking outbound packets with a specific external destination IP address are not used.

Objective:

Communication and Network Security

Sub-Objective:

Implement secure design principles in network architectures

References:

Firewall and NAT rules (PDF),
https://www.cisco.com/c/en/us/td/docs/video/cuvc/design/guides/desktop/5_5/cuvc_design_guide/firewallrules.pdf

---

Question #111 of 131

Question ID: 1105252

Your organization needs to implement a system whereby remote users can dial in to the network to transmit small amounts of sales data. You want this system to provide maximum security to prevent hackers from connecting to the network. Which technology should you implement?

- ✗ **A)** Implement a callback system with call waiting.
- ✗ **B)** Implement caller ID with call forwarding.
- ✗ **C)** Implement caller ID with three-way calling.
- ✓ **D)** Implement a callback system with caller ID.

Explanation

You should implement a callback system with caller ID. Caller ID works in conjunction with a callback system to provide maximum security. The caller ID system can verify that the user is calling from an approved telephone number. If a connection attempt is made from an unapproved telephone number, the connection is terminated before security is compromised.

You should not implement a callback system with call waiting. Implementing call waiting would actually cause problems with remote connections because the call waiting implementation could interrupt a successful connection.

Implementing caller ID with any other technologies is not appropriate in this scenario.

A callback system is a remote access protection mechanism that limits dial-up connections by calling back the user at a predefined telephone number or by ensuring that the user connected from an approved telephone number is using caller ID.

The most secure implementation of a callback system involves entry of a user ID and personal identification number (PIN) when the user connects. Once the user is verified, the callback system calls back the user as the telephone number that corresponds with the user ID.

Some implementations of a callback system allow the system to call a user back based on the user's input at the time of connection. This is a less secure implementation of callback, and should only be implemented with trusted entities.

When callback is used for remote dial-up connections, a caller may attack by connecting and then not hanging up. If the caller was previously authenticated and has completed the session, a connection into the remote network would still be maintained. Also, an unauthenticated remote user may hold the line open, acting as if callback authentication has taken place. Thus, an active disconnect should be completed at the computing resource's side of the line.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

Caller ID and callback, http://technet.microsoft.com/en-us/library/cc778189(v=WS.10).aspx

---

Question #112 of 131

Question ID: 1111742

Match the descriptions on the left with the corresponding wireless security issues on the right.

{UCMS id=5688086354722816 type=Activity}

Explanation

The wireless security issues should be matched with the descriptions in the following way:

- WEP/WPA cracking - Mathematical algorithms are used to determine the pre-shared key used on the access point.
- Warchalking - SSID and other authentication details regarding a wireless network are written down in a prominent public place.
- Evil twin - A rogue access point is configured with the same SSID as a valid access point.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Glossary

Question #113 of 131

Question ID: 1105193

You are explaining to a junior administrator about port scanning. Which of the following statements is true?

- ✗ **A)** There are over 65,000 well-known ports.
- ✗ **B)** There are 1,024 ports that are vulnerable on a TCP/IP network.
- ✗ **C)** Only UDP ports are vulnerable on a TCP/IP network.
- ✓ **D)** There are over 65,000 ports that are vulnerable on a TCP/IP network.

Explanation

On a TCP/IP network, there are over 65,000 ports that are vulnerable.

The first 1,024 ports are the well-known ports responsible for well-known services, such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP). The port numbers start at 0 and go through 65,535.

Both TCP and UDP ports are vulnerable on a TCP/IP network.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Port Scanning

Introduction to Port Scanning, http://netsecurity.about.com/cs/hackertools/a/aa121303.htm

---

Question #114 of 131

Question ID: 1113953

You are servicing a Windows computer that is connected to your company's Ethernet network. You need to determine the manufacturer of the computer's NIC. You issue the ipconfig /all command in the command prompt window and record the NIC's MAC address, which is 00-20-AF-D3-03-1B.

Which part of the MAC address will help you to determine the NIC's manufacturer?

- ✗ **A)** D3-03-1B
- ✗ **B)** AF-D3-03
- ✓ **C)** 00-20-AF

✗ **D)** 20-AF-D3

Explanation

A media access control (MAC) address is a unique 48-bit number that is built into a NIC that connects to an Ethernet network. A MAC address is divided into six octets, each of which represents 8 bits of the address as a two-digit hexadecimal number. The first three octets of a MAC address are assigned by the Institute of Electrical and Electronics Engineers (IEEE) to each network interface card (NIC) manufacturer; these three octets uniquely identify each NIC manufacturer. In this scenario, the sequence 00-20-AF identifies the NIC's manufacturer as 3Com.

Other popular manufacturers of NICs include Cisco, which has been assigned the sequence 00-00-0C, and Hewlett-Packard, which has been assigned the sequence 08-00-09.

The last three octets of a MAC address are used to uniquely identify each NIC that a manufacturer produces.

Originally, a MAC address was permanently added to a NIC, but more recent manufacturing processes allow the MAC address to be reconfigured to a different value. The ability to reconfigure a MAC address allows administrators to assign addresses of their choosing. However, changing MAC addresses must be done with care because having two cards with the same MAC address on the same network will always cause communications problems.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, MAC Addressing

IEEE MAC Address, http://www.banalyzer.de/ban/HTML/P_LAYER2/Eng/P_lay207.html

---

Question #115 of 131

Question ID: 1113946

You are a consultant. One of your clients has asked you to establish network hosts for its network. This network is connected to the Internet.

What is the maximum number of hosts that this company can have with a network address of 208.15.208.0 using the default subnet mask?

✗ **A)** 62

✗ **B)** 16,382

✗ **C)** 16,777,214

✗ **D)** 510

✓ **E)** 254

✗ **F)** 65,534

Explanation

This IP address is a class C address. A class C network has 254 hosts per network. The number of hosts per network is calculated by determining the number of bits available for the network ID.

In a class C IP address, the first three octets (24 bits) are assigned to the network ID, and the last octet, which is eight bits, is assigned to the host ID. Knowing that eight bits are assigned to the host ID, you can determine the number of hosts available. To calculate this, convert the eight bits to binary.

To do this with a calculator, type eight ones into the calculator in binary form, then convert that number to decimal. The result should be 255 hosts per network. Because 255 is reserved for network broadcasts, the actual number of possible hosts is 254.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IP Classes

Network Calculators, http://www.subnetmask.info/

Question #116 of 131

Question ID: 1105183

Which procedure is an example of an operational control?

✓ **A)** a backup control

✗ **B)** a database management system

✗ **C)** identification and authentication

✗ **D)** a business continuity plan

Explanation

Backup controls, software testing, and anti-virus management are components of operational software controls. Operational software controls check the software to find whether the software is compromising security or not. Trusted

recovery procedures, audit trails, clipping levels, operational and life-cycle assurance, configuration management, and media and system controls are all examples of operational controls.

A business continuity plan refers to the procedures undertaken for dealing with long-term unavailability of business processes. Business continuity planning differs from disaster recovery. Disaster recovery aims at minimizing the impact of a disaster.

A database management system (DBMS) is a collection of software that manages and processes large amounts of data stored in a structured format. A DBMS is an example of an application control and not an operational control.

Identification and authentication of employees are examples of technical controls that are defined under the security administration control.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, SP 800-53 Rev. 4

Question #117 of 131

Question ID: 1113970

Which technology will phreakers attack?

✗ **A)** NAT
✗ **B)** firewalls
✓ **C)** VoIP
✗ **D)** Web servers

Explanation

Phreakers will attack Voice over Internet Protocol (VoIP). Phreakers generally attack PBX equipment used for telephone lines.

Phreakers do not attack firewalls, Web servers, or NAT. Hackers attacks these technologies. Firewalls are used to protect local networks and create demilitarized zones (DMZs). Web servers provide Web services to users, including Web sites, FTP sites, and news sites. Network Address Translation (NAT) provides a transparent firewall solution between an internal network and outside networks.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

How to Protect Your VoIP Network, http://www.networkworld.com/research/2006/051506-voip-guide-security.html?ts

---

Question #118 of 131

Question ID: 1105192

Which metric is used by the Routing Information Protocol (RIP) Version 2 protocol to determine the network path?

✗ **A)** bandwidth
✗ **B)** convergence
✓ **C)** hop count
✗ **D)** delay

Explanation

Both Versions 1 and 2 of RIP use hop count as the primary metric to determine the most desirable network path. A metric is a variable value assigned to routes and is a mechanism used by routers to choose the best path when there are multiple routes to the same destination. Each router traversed by a packet from the source to the destination constitutes one hop. The lower the hop count, the higher the preference given to that path. Using RIP, the hop count is limited to 15 hops. Any router beyond this number of hops is marked as unreachable.

RIP does not use delay as its primary metric. Delay refers to the time an Internet Protocol (IP) packet takes to travel from source to destination. Some dynamic protocols, such as Interior Gateway Routing Protocol (IGRP), use delay in combination with other parameters to determine the best path to the destination.

RIP does not use bandwidth as its primary metric. Bandwidth refers to the maximum attainable throughput on a link. This metric is used as a part of the metric calculation by some routing protocols, such as IGRP and Enhanced IGRP (EIGRP).

RIP does not use convergence as its primary metric. Convergence refers to the amount of time it takes for routing updates to be propagated to all routers throughout the network.

RIP v1, RIP v2, and IGRP are considered distance vector protocols. Open Shortest Path First (OSPF) is a link-state protocol. EIGRP is a balanced hybrid protocol, also referred to as an advanced distance vector protocol. Distance vector routing protocols commonly broadcast their routing table information to all other routers every minute.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, RIP

TCP/IP Routing Information Protocol,
http://www.tcpipguide.com/free/t_TCPIPRoutingInformationProtocolRIPRIP2andRIPng.htm

---

Question #119 of 131

Question ID: 1111738

Match each description with the protocol that it BEST fits.

{UCMS id=5659415703191552 type=Activity}

Explanation

The protocols should be matched with the descriptions in the following manner:

- SSH - A protocol that uses a secure channel to connect a server and a client
- SSL - A protocol that secures messages between the Application and Transport layer
- SCP - A protocol that allows files to be copied over a secure connection
- ICMP - A protocol used to test and report on path information between network devices

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IP Networking

---

Question #120 of 131

Question ID: 1113969

What is DNS poisoning?

- ✗ **A)** the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash
- ✗ **B)** the practice of continually sending a DNS server synchronization messages with spoofed packets
- ✗ **C)** the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash
- ✓ **D)** the practice of dispensing IP addresses and host names with the goal of traffic diversion

Explanation

DNS poisoning is the practice of dispensing IP addresses and host names with the goal of traffic diversion. Properly configured DNS security (DNSSEC) on the DNS server can provide message validation, which, in turn, would prevent DNS poisoning.

A SYN flood is the practice of continually sending a DNS server synchronization messages with spoofed packets. A SYN flood can transpire when a high number of half-open connections are established to a single computer.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network, DNS Cache Poisoning

---

Question #121 of 131

Question ID: 1111739

Move the correct items from the left column to the column on the right to match the protocol with the correct default port.

{UCMS id=5693803627282432 type=Activity}

Explanation

The protocols given use these default ports:

- Port 21 - FTP
- Port 110 - POP3
- Port 143 - IMAP

- Port 443 - HTTPS
- Port 3389 - RDP

FTP also uses port 20, but it was not listed in this scenario.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, IP Networking

---

Question #122 of 131

Question ID: 1105164

Which radio transmission technology does the 802.11b standard specify?

✗ **A)** orthogonal frequency-division multiplexing (OFDM)
✗ **B)** frequency hopping spread spectrum (FHSS)
✗ **C)** narrowband spectrum
✓ **D)** direct sequence spread spectrum (DSSS)

Explanation

The 802.11b standard is an addition to the IEEE 802.11 standard for wireless LANs. While the original 802.11 standard included both direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) radio transmission technologies, 802.11b specifies only DSSS. Both DSSS and FHSS are spread-spectrum technologies, which means that they broadcast signals over a range of radio frequencies.

DSSS transmits a signal that is a combination of an artificial and a real signal. The receiving end utilizes the additional signal to maintain the integrity of the real signal when interference is experienced. Both ends must agree upon the method for generating the signal. DSSS offers superior range, the ability to block interference, and a transmission rate of 11 Mbps.

Narrowband spectrum means that signals are transmitted over one frequency. For example, a radio station transmits its signals over one radio frequency or station.

FHSS transmits signals over continually changing frequencies. Both ends must be synchronized to know which frequency is being used. FHSS signals are difficult for malicious users to pick up. The transmission rate is 1 Mbps.

Orthogonal frequency-division multiplexing (OFDM) is a modulation scheme used with networks in the IEEE 802.11a standard.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, 802.11b

---

Question #123 of 131

Question ID: 1114742

Your company's security policy states that you must provide protection against phreakers. Which entity would they most likely attack?

- ✗ **A)** a Token Ring network
- ✗ **B)** an Ethernet network
- ✗ **C)** a biometric access device
- ✓ **D)** a PBX phone system

Explanation

Phreakers will most likely attack a Private Branch Exchange (PBX) phone system.

Phreakers will not attack an Ethernet network, Token Ring network, or a biometric access device.

Phreaking is the fraudulent use of telephone services. A PBX phone system is actually a private telephone switch installed at a company's location. When a PBX system is installed, several precautions should be taken to reduce fraud:

Change the default PBX system passwords.

Review the PBX phone bill regularly.

Block remote calling after business hours

Changing the default PBX system passwords will ensure that phreakers cannot break into the system using the default password given at installation time. Phreakers commonly use this method to break into systems.

Reviewing the PBX phone bill regularly will allow you to recognize fraud more quickly. The PBX phone bill will list the calls made from the system and the time of the calls. Many times, phreakers will use the PBX system after hours to make illegal phone calls.

Blocking remote calling after hours will ensure that phreakers cannot make illegal phone calls after hours. The Direct Inward System Access (DISA) feature of a PBX system allows users to dial in to the PBX system remotely and make long-distance phone calls from within the system after entering an access code.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, PBX

Question #124 of 131

Question ID: 1113957

You have two wireless networks in your building. The wireless networks do not overlap. Both of them use Wi-Fi Protected Access (WPA).

You want to ensure that no unauthorized wireless access points are established. What should you do?

- ✗ **A)** Change the two wireless networks to WPA2.
- ✓ **B)** Periodically complete a site survey.
- ✗ **C)** Change the two wireless networks to WEP.
- ✗ **D)** Disable SSID broadcasts for the two wireless networks.

Explanation

You should periodically complete a site survey to ensure that no unauthorized wireless access points are established. Site surveys generally produce information on the types of systems in use, the protocols in use, and other critical information. You need to ensure that hackers cannot use site surveys to obtain this information. To protect against unauthorized site surveys, you should change the default Service Set Identifier (SSID) and disable SSID broadcasts. Immediately upon discovering a wireless access point using a site survey, you should physically locate the device and disconnect it.

To ensure that no unauthorized wireless access points are established, you should not change the two wireless networks to WPA2. This would increase the security for the two networks and prevent hackers from accessing the

networks. However, it would not prevent an attacker from setting up a new wireless access point.

You should not disable SSID broadcasts for the two wireless networks to ensure that no unauthorized wireless access points are established. The reason you would disable SSID broadcasts is to protect a wireless network from hackers and to prevent unauthorized site surveys. Disabling the SSID broadcast on an existing network CANNOT prevent the establishment of new wireless access points.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Site Surveys

Site Survey Steps, http://www.wi-fiplanet.com/tutorials/article.php/1116311

Question #125 of 131

Question ID: 1113964

Which network entity uses one public IP address and acts as the interface between a local area network and the Internet?

- ✗ **A)** router
- ✗ **B)** VPN
- ✗ **C)** firewall
- ✓ **D)** NAT

Explanation

Network Address Translation (NAT) acts as the interface between a local area network and the Internet using one public IP address.

A VPN is a private network that is implemented over a public network, such as the Internet.

A router is a network device that divides a local area network into smaller subnetworks. Routers operate at the Network layer of the OSI model (Layer 3). While a firewall can also be a router, it is referred to as a firewall when it functions to create a DMZ.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Public Versus Private IP Addresses

NAT Router Security Solutions, http://www.grc.com/nat/nat.htm

---

Question #126 of 131

Question ID: 1105232

Which statement is NOT true regarding multicast transmissions?

- ✗ **A)** The protocols use Class D addresses.
- ✗ **B)** Data, multimedia, video, and voice clips can be transmitted.
- ✗ **C)** A packet is transmitted to a specific group of devices.
- ✓ **D)** A message has one source and destination address.

Explanation

In multicast transmissions, a message does NOT have one source and destination address. This is a description of unicast transmissions.

Multicast transmission packets are transmitted to a specific group of devices. Multicast protocols use Class D addresses. Data, multimedia, video, and voice clips can be transmitted using multicast. It is a one-to-many transmission.

The three types of transmission methods are: unicast, multicast, and broadcast.

Unicast transmissions are intended for a single device. It is a one-to-one transmission.

Broadcast transmissions are intended for all devices on a subnet. It is a one-to-all transmission.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Unicast, Multicast, and Broadcast

Question #127 of 131

Question ID: 1105145

You are configuring a computer to connect to the Internet. Which information must a computer on a network have before it can communicate with the Internet?

- ✗ **A)** the public key, proxy server address, and MAC address of the router
- ✗ **B)** the IP address, default gateway, and DNS server
- ✗ **C)** the MAC address of the router, subnet mask, and FTP server address
- ✗ **D)** the IP address, subnet mask, and MAC address of the router
- ✓ **E)** the IP address, default gateway, and subnet mask

Explanation

Before any computer on a network can communicate with the Internet, it will need an IP address, a default gateway, and a subnet mask. You can supply this information manually, or you can use a DCHP server to automatically supply this information.

The IP address is a 32-digit binary number that is needed to identify each device, or host, on the Internet. The IP address provides a logical address for each device.

The subnet mask is used to block out a portion of the IP address. The purpose of the blocking is to distinguish the network ID from the host ID. It is also used to identify whether the IP address of the destination host is on the local subnet or on a remote subnet.

The computer does not need any of the other listed components to communicate on the Internet.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, DHCP/BOOTP

Question #128 of 131

Question ID: 1105245

Which payload is produced by using IPSec in tunnel mode with the AH protocol?

- ✗ **A)** an encapsulated packet that is encrypted
- ✓ **B)** an encapsulated packet that is digitally signed
- ✗ **C)** an unencapsulated packet that is encrypted
- ✗ **D)** an unencapsulated packet that is digitally signed

Explanation

Internet Protocol Security (IPSec) in tunnel mode with the Authentication Header (AH) protocol produces an encapsulated packet that is digitally signed. AH digitally signs a packet for authentication purposes. Tunnel mode encapsulates a packet within another packet.

Encapsulating Security Protocol (ESP) encrypts IPSec packets. Transport mode sends IPSec packets between two computers without encapsulating packets. AH and ESP work in transport mode and tunnel mode.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure communication channels according to design

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, IPSec and ISAKMP

Understanding VPN IPSec Tunnel Mode and IPSec Transport Mode - What's the Difference?, http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

---

Question #129 of 131

Question ID: 1114743

You need to implement security countermeasures to protect from attacks being implemented against your PBX system via remote maintenance. Which policies provide protection against remote maintenance PBX attacks?

a. Turn off the remote maintenance features when not needed.

b. Use strong authentication on the remote maintenance ports.

c. Keep PBX terminals in a locked, restricted area.

d. Replace or disable embedded logins and passwords.

- ✗ **A)** option c

- ✓ **B)** all of the options
- ✗ **C)** options a and b only
- ✗ **D)** options a, b, and c only
- ✗ **E)** option b
- ✗ **F)** option a
- ✗ **G)** option d

Explanation

You should implement all of the given policies to provide protection against remote maintenance PBX attacks.

You should turn off the remote maintenance features when not needed and implement a policy whereby local interaction is required for remote administration.

You should use strong authentication on the remote maintenance ports. This will ensure that authentication traffic cannot be compromised.

You should keep PBX terminals in a locked, restricted area. While this is more of a physical security issue, it can also affect remote maintenance attacks. If the physical security of a PBX system is compromised, the attacker can then reconfigure the PBX system to allow remote maintenance.

You should replace or disable embedded logins and passwords. These are usually configured by the manufacturer to allow back door access to the system.

Objective:
Communication and Network Security

Sub-Objective:
Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, PBX

PBX Vulnerability Analysis, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

---

Question #130 of 131

Question ID: 1105182

What is the major security vulnerability of using File Transfer Protocol (FTP)?

- ✗ **A)** Both uploads and downloads can occur.
- ✗ **B)** Anonymous logon is allowed.

✗ **C)** The session between the client and server is not encrypted.

✓ **D)** The user ID and password are sent in clear text.

Explanation

The major security vulnerability of using FTP is that the user ID and password are sent in clear text. This allows it to be subject to packet capture. The only way to protect against this is to implement Secure FTP (SFTP) or to implement FTP with Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

You can configure FTP to use anonymous logon, but this is not a major security vulnerability. Any administrators who use anonymous logon must be willing to accept the risk that comes with it. However, anonymous logon is not enabled by default.

While the FTP session is not encrypted, this is not considered a major vulnerability. Compromising the logon credentials is more of a security vulnerability than compromising the FTP data.

FTP can be configured to allow both uploads and downloads. This is not considered a security vulnerability because either of these functions can be disabled.

Objective:
Communication and Network Security

Sub-Objective:
Implement secure design principles in network architectures

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, FTP, FTPS, SFTP, TFTP

Question #131 of 131

Question ID: 1113960

Match the descriptions on the left with the Wireless Encryption Protocols on the right.

{UCMS id=5657176146182144 type=Activity}

Explanation

The Wireless Encryption Protocols should be matched with the descriptions in the following way:

- WEP - Uses a 40-bit or 104-bit key
- WPA/WPA2 Personal - Uses a 256-bit pre-shared key
- WPA/WPA2 Enterprise - Requires a RADIUS server

Objective:

Communication and Network Security

Sub-Objective:

Secure network components

References:

CISSP Cert Guide (3rd Edition), Chapter 4: Communication and Network Security, Wireless Networks