4 - Communications and network Security

Test ID: 176805791

Pregunta #1 de 131

Id. de pregunta: 1105243

¿Qué protocolo utiliza el cifrado para proteger el tráfico transmitido y admite la transmisión de múltiples protocolos?

✗ **A)** HTTP

✗ **B)** HTTPS (en)

✓ **C)** L2TP sobre IPSec

✗ **D)** FTP

explicación

El Protocolo de túnel de capa 2 (L2TP) es un protocolo de túnel que se utiliza para transmitir el tráfico en conexiones de red privada virtual (VPN). L2TP admite varios protocolos, como el Protocolo de control de transmisión (TCP), el Protocolo de Internet (IP), el Intercambio de paquetes entre redes (IPX) y la Arquitectura de red de sistemas (SNA). L2TP se basa en dos protocolos de tunelización más antiguos: Protocolo de túnel punto a punto (PPTP) y Reenvío de capa 2 (L2F). Cuando L2TP se implementa con el protocolo de seguridad de Internet (IPSec), también proporciona cifrado.

El Protocolo de transferencia de hipertexto (HTTP) transmite información en texto no cifrado. El Protocolo seguro de transferencia de hipertexto (HTTPS) utiliza capa de sockets seguros (SSL) para cifrar el tráfico HTTP. HTTPS solo admite el cifrado del tráfico HTTP. El Protocolo de transferencia de archivos (FTP) transmite datos en texto no cifrado.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, VPN

Pregunta #2 de 131

Id. de pregunta: 1105176

¿Qué tipo de firewall se considera un firewall de segunda generación?

✗ **A)** firewall de filtrado de paquetes

✗ **B)** servidor de seguridad de filtrado dinámico de paquetes

✗ **C)** firewall de proxy del núcleo

✓ **D)** servidor de seguridad proxy

explicación

Un firewall proxy es un firewall de segunda generación, lo que significa que fue el segundo tipo creado. Otros tipos siguieron.

Un firewall proxy del núcleo es un firewall de quinta generación, y un firewall de filtrado de paquetes es un firewall de primera generación. Un firewall de filtrado dinámico de paquetes es un firewall de cuarta generación.

Los firewalls de tercera generación suelen utilizar un sistema que examina el estado y el contexto de los paquetes entrantes. Este tipo de firewall realiza un seguimiento de los protocolos que se consideran sin conexión, como el Protocolo de datagramas de usuario (UDP).

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #3 de 131

Id. de pregunta: 1105148

Considere la siguiente dirección IP:

157.175.12.10/22

¿Cuántos bits se utilizarán para la parte del host de esta dirección?

✗ **A)** 22

✓ **B)** 10

✗ **C)** 6

✗ **D)** 16

explicación

Diez bits se utilizan para la porción del host de 157.175.12.10/22.

La dirección IP 157.175.12.10/22 es un ejemplo de una red "slash x", también conocida como notación de enrutamiento de interdominios sin clases (CIDR). CIDR es una forma de aplicar una máscara de subred a una dirección IP para optimizar el espacio de direcciones mientras se ignoran las categorías de clase IP tradicionales. Con el direccionamiento con clase, 157.175.12.10 es una dirección de clase B, lo que significa que se utilizan 16 bits de la dirección para la parte de red y 16 bits para la parte del host de la dirección. Con CIDR, la notación /22 al final de la dirección IP significa que se utilizan 22 bits para la parte de red de la dirección y la parte del host utiliza los 10 bits restantes. A su vez, esto significaría que este espacio de direcciones se puede dividir en bloques de espacio más pequeños y eficientes.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPv4

Calculadoras de red, http://www.subnetmask.info/

Pregunta #4 de 131

Id. de pregunta: 1114720

¿Qué protocolos operan en la capa de transporte del modelo OSI?

a. HTTP

b. P.I.

c. IPX

d. TCP

e. UDP

- ✗ **A)** Opción d
- ✗ **B)** opción A
- ✗ **C)** todas las opciones
- ✗ **D)** opción c
- ✗ **E)** opción b
- ✓ **F)** Sólo opciones D y E

✗ **G)** opción e

✗ **H)** sólo las opciones a, b y c

explicación

El Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP) funcionan en la capa de transporte del modelo de interconexión de sistemas abiertos (OSI). Debido a que la capa de transporte es la cuarta capa en el modelo OSI, a veces se conoce como capa 4.

Los protocolos que funcionan en la capa de transporte proporcionan servicios de transporte a protocolos de capa superior, como el Protocolo de transferencia de hipertexto (HTTP) y el Protocolo trivial de transferencia de archivos (TFTP). Por ejemplo, HTTP es un protocolo de nivel de aplicación que utiliza los servicios orientados a la conexión de TCP y TFTP es un protocolo de capa de aplicación que utiliza los servicios sin conexión de UDP.

IP es un protocolo sin conexión en el conjunto de protocolos TCP/IP. Internetwork Packet Exchange (IPX) es un protocolo sin conexión en el conjunto de protocolos IPX/SPX. IP e IPX operan en la capa de red del modelo OSI y proporcionan servicios de enrutamiento y direccionamiento para los nodos de una red.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red, Capa de Transporte

---

Pregunta #5 de 131

Id. de pregunta: 1105142

¿Qué función proporciona la capa Session del modelo OSI?

✗ **A)** direccionamiento de red física

✓ **B)** sincronización de datos

✗ **C)** direccionamiento de red lógico

✗ **D)** enrutamiento

explicación

De las opciones enumeradas, la capa de sesión del modelo de interconexión de sistemas abiertos (OSI) proporciona sincronización de datos. La capa Session establece y mantiene el diálogo, o sesión, entre dos equipos de una red. La

capa Session también comunica problemas, como errores de transferencia de archivos, a las aplicaciones de las capas superiores.

La capa de red proporciona enrutamiento y direccionamiento de red lógicos. En la pila de protocolos TCP/IP, IP proporciona direccionamiento de red. IP también proporciona enrutamiento y opera en la capa de red del modelo OSI.

La capa de vínculo de datos proporciona direccionamiento de red físico. Las tarjetas de interfaz de red (NIC) están configuradas con direcciones de control de acceso a medios (MAC). Una dirección MAC de una NIC es utilizada por un protocolo de comunicaciones de red en arquitecturas Ethernet o Token Ring para identificar la NIC en la red.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, capa de sesión

---

Pregunta #6 de 131

Id. de pregunta: 1114727

¿Cuáles son las razones válidas para implementar subredes en una red IP?

a. para aumentar la seguridad de la red

b. para configurar un mayor número de hosts

c. reducir la congestión disminuyendo el tráfico de red

d. para utilizar más de un servidor en cada segmento de una LAN IP

e. para reducir la congestión aumentando el ancho de banda de los medios de red

- ✗ **A)** opción A
- ✗ **B)** opción e
- ✗ **C)** sólo las opciones a, c y e
- ✗ **D)** Opciones B y D Sólo
- ✗ **E)** opción c
- ✗ **F)** opción b
- ✗ **G)** Opción d
- ✓ **H)** Sólo las opciones A y C

explicación

La máscara de subred permite a TCP/IP buscar la ubicación del host de destino en la red local o en una ubicación remota.

Las subredes se utilizan por las siguientes razones:

Para expandir la red

para reducir la congestión

para reducir el uso de cpu

Para aislar los problemas de red

para mejorar la seguridad

Para permitir combinaciones de medios porque cada subred puede admitir un medio diferente

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, Clases IP

Pregunta #7 de 131

Id. de pregunta: 1114729

Su organización está intentando decidir si desea usar RSA o ECC para encripcionar las comunicaciones celulares. ¿Cuál es una ventaja de ECC sobre el algoritmo RSA?

- ✓ **A)** Ecc requiere menos recursos.
- ✗ **B)** Ecc no se ocupa de las complejidades de las firmas digitales.
- ✗ **C)** ECC utiliza curvas elípticas en lugar de claves para proporcionar seguridad.
- ✗ **D)** ECC utiliza curvas elípticas que mejoran su fiabilidad.

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

¿Qué aplicaciones utilizan UDP?

- ✗ **A)** ARP, NFS, FTP, SMTP
- ✗ **B)** ICMP, ARP, FTP
- ✓ **C)** NFS, TFTP, SNMP
- ✗ **D)** NFS, FTP, TFTP

explicación

Las aplicaciones de red que desean ahorrar tiempo de procesamiento utilizan UDP porque tienen unidades de datos muy pequeñas que intercambiar y una pequeña cantidad de reensamblaje. El Protocolo trivial de transferencia de archivos (TFTP) utiliza UDP en lugar de TCP, al igual que el Sistema de archivos de red (NFS) y el Protocolo simple de administración de redes (SNMP). TFTP es una aplicación de red que es más simple que el Protocolo de transferencia de archivos (FTP) pero menos capaz. Se utiliza cuando no se requiere la autenticación de usuario y la visibilidad del directorio.

Protocolo simple de transferencia de correo (SMTP) se implementa para funcionar a través del puerto TCP 25. SMTP es el protocolo predeterminado para enviar correo electrónico.

FTP se utiliza para transferir archivos entre un servidor FTP y un cliente mediante IP sobre TCP.

Telnet y rlogin son otros dos protocolos que utilizan TCP.

TCP está orientado a la conexión, mientras que UDP no tiene conexión. TCP y UDP funcionan en la capa de transporte del modelo OSI.

Protocolo de datagramas de usuario (UDP) es un protocolo que ofrece una cantidad limitada de servicio cuando se intercambian mensajes entre equipos en una red TCP/IP. UDP es una alternativa al Protocolo de control de transmisión (TCP). Al igual que TCP, UDP utiliza el protocolo de Internet (IP) para obtener realmente un paquete de un equipo a otro. A diferencia de TCP, sin embargo, UDP no divide un mensaje en datagramas y lo vuelve a ensamblar en el otro extremo. UDP se implementa en el nivel de transporte del modelo de protocolo TCP/IP.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, números de puerto TCP/UDP comunes

---

Pregunta #10 de 131

Id. de pregunta: 1111744

Está intentando decidir qué tipo de sistema de detección de intrusiones (IDS) debe implementar para mejorar la seguridad de la red. Haga juego la descripción IDS de la izquierda con su tipo apropiado IDS a la derecha.

{UCMS id=5671067681030144 type=Activity}

explicación

Los tipos ids deben coincidir con las descripciones de la siguiente manera:

- Basado en el comportamiento: un IDS que utiliza una línea base de actividad aprendida para identificar los intentos de intrusión
- Basado en firmas: un IDS que mantiene una base de datos de perfiles de ataque para identificar intentos de intrusión
- Basado en host : un IDS que solo supervisa un único dispositivo en particular para los intentos de intrusión
- Basado en red: un IDS que supervisa todo un segmento de red en busca de intentos de intrusión.

Muchas soluciones IDS en realidad emplean varios tipos para proporcionar la mayor protección.

Tenga en cuenta que un IDS sólo detecta los intentos de intrusión y emplea las alertas configuradas para asegurarse de que los intentos de intrusión se registran y se notifican. Un sistema de prevención de intrusiones (IPS) detecta las intrusiones y lleva a cabo los pasos para evitar que el ataque tenga éxito.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:

Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, componentes de red seguros

---

Pregunta #11 de 131

Id. de pregunta: 1105233

¿Qué es una implementación común para el protocolo IPSec?

- ✗ **A)** SSL
- ✗ **B)** EDI
- ✗ **C)** poner
- ✓ **D)** VPN

explicación

El protocolo de seguridad de Internet (IPSec) es un estándar de seguridad comúnmente implementado para crear redes privadas virtuales (VPN). IPSec permite que los paquetes se intercambien de forma segura a través del Protocolo de Internet (IP) en la capa de red OSI en lugar de en la capa de aplicación. El Internet Engineering Task Force (IETF) desarrolló el estándar, pero Cisco ha contribuido a su aparición. Los routeres Cisco tienen soporte para el IPSec integrado en el producto.

IPSec admite dos modos de cifrado: Transporte y Túnel. El modo de transporte cifra sólo la parte de datos de cada paquete, pero no la información de encabezado. El modo de túnel cifra el encabezado y los datos. Para que IPSec funcione, los dispositivos de envío y recepción deben compartir una clave pública. Otro método para asegurar una VPN es mediante el protocolo de túnel de capa dos (L2TP).

Intercambio de datos de Exchange (EDI) es un protocolo utilizado para intercambiar datos empresariales en un formato estándar.

La transferencia electrónica segura (SET) se utiliza para proporcionar seguridad para las transacciones con tarjeta de crédito.

Capa de sockets seguros (SSL) es un protocolo de seguridad que utiliza tanto el cifrado como la autenticación para proteger los datos enviados en las comunicaciones de red.

Las VPN a veces se conocen comúnmente como túneles. Una VPN consiste esencialmente en un servidor VPN, autenticación y cifrado. El software VPN cifra la información de la sesión, así como la mayoría de la información de los mensajes, incluidos los mensajes del Protocolo de transferencia de archivos (FTP) y el Protocolo de transferencia de hipertexto (HTTP). La información de la capa de vínculo de datos permanece inalterada.

El ataque más efectivo contra una VPN basada en IPSec es un ataque de hombre en el medio.

Objetivo:

Comunicación y seguridad de la red

Subobsecución:

Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPsec

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

---

Pregunta #12 de 131

Id. de pregunta: 1192939

¿Cuáles son las funciones clave de la capa de red OSI?

a. control de flujo

b. Selección de ruta de acceso

c. Segmentación de datos

d. direccionamiento lógico

e. direccionamiento físico

- ✓ **A)** Opciones B y D Sólo
- ✗ **B)** sólo las opciones a, c y e
- ✗ **C)** todas las opciones
- ✗ **D)** opción b
- ✗ **E)** e opcional
- ✗ **F)** Opción d
- ✗ **G)** opción A
- ✗ **H)** opción c

explicación

Las funciones clave de la capa de red OSI son el direccionamiento lógico y la selección de rutas. Las capas de red de dos sistemas intercambian paquetes/datagramas. Los paquetes TCP/IP contienen un encabezado IP y los datos.

Las direcciones lógicas o de red contienen una parte de red y una parte de host. Las direcciones de red se almacenan en la tabla de enrutamiento del router y determinan rápidamente la interfaz que un paquete necesita recorrer para llegar al destino. Una vez que los paquetes llegan a la dirección de red de destino, el router local puede determinar dónde reenviar los paquetes en función de la dirección de host del host de destino. Esta información de encabezado también puede ser utilizada por los firewalls de filtrado de paquetes para filtrar el tráfico en función de la dirección IP de origen y destino.

El control de flujo, la notificación de errores, el direccionamiento de dispositivos físicos y la especificación de la topología de red pueden tener lugar en la capa de vínculo de datos. Tenga en cuenta que la notificación de errores tiene lugar en la capa de vínculo de datos, mientras que la corrección de errores es una función de la capa de transporte. La capa de transporte especifica si el método de entrega es confiable o no confiable (entrega de mejor esfuerzo) y controla la segmentación y el reensamblaje de datos en un flujo de datos.

El direccionamiento físico de un dispositivo se produce en la capa de vínculo de datos. La capa de vínculo de datos utiliza la dirección para determinar si es necesario pasar el mensaje a la pila de protocolos y a qué pila de capa superior pasarlo. La capa de vínculo de datos admite servicios orientados a la conexión y sin conexión y proporciona secuenciación de tramas y control de flujo.

La capa de red también proporciona enrutamiento y servicios relacionados. Algunos de los protocolos que funcionan en la capa de red son el Protocolo de Internet (IP), el Protocolo de mensajes de control de Internet (ICMP), el Protocolo de información de enrutamiento (RIP) y el Protocolo de administración de grupos de Internet (IGMP). Los firewalls de filtrado de paquetes funcionan en esta capa.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, capa de red

---

Pregunta #13 de 131

Id. de pregunta: 1105147

¿Cuál es el identificador de red base para la dirección 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

explicación

El identificador de red base es 196.11.192.0.

La dirección IP 196.11.200.71/18 es un ejemplo de una red "slash x", también conocida como notación de enrutamiento de interdominios sin clases (CIDR). CIDR es una forma de aplicar una máscara de subred a una dirección IP para optimizar el espacio de direcciones mientras se ignoran las categorías de clase IP tradicionales. Con el direccionamiento con clase, 196.11.200.71 es una dirección de clase C, lo que significa que se utilizan 24 bits de la dirección para la parte de red y ocho bits para la parte del host de la dirección. Con CIDR, la notación /18 al final de la dirección IP significa que se utilizan 18 bits para la parte de red de la dirección y la parte del host utiliza los 14 bits restantes. Este es un ejemplo de integración o superred, lo contrario de la subred. El resumen se utiliza para combinar una colección de subredes como una con el fin de hacer las tablas de ruteo en el Routers más pequeño así mejorando funcionamiento.

Con 18 bits utilizados, la máscara de subred estándar es 11111111.11111111.11000000.000000000 o 255.255.192.0.

A su vez, esto significa que la parte de red de esta dirección, o el identificador de red base, es 196.11.192.0.

El propósito de CIDR es dividir las direcciones IP en bloques de espacio más pequeños y eficientes.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPv4

Calculadoras de red, http://www.subnetmask.info/

Pregunta #14 de 131

Id. de pregunta: 1113973

¿Qué término describe mejor un programa que registra la actividad en la pantalla de un ordenador?

✗ **A)** malware

✓ **B)** raspador de pantalla

✗ **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

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, RASPADOR DE PANTALLA VPN

Raspado de pantalla, caballos de Troya y contraseñas oh, mi, http://blogs.msdn.com/b/mthree/archive/2006/03/16/screen-scraping-trojan-horses-and-passwords-oh-my.aspx

---

Pregunta #15 de 131

Id. de pregunta: 1105191

¿Qué afirmación NO es cierta con respecto a las tramas Ethernet II?

- ✓ **A)** Incluyen un campo length de dos bytes.
- ✗ **B)** La etiqueta 802.1Q es opcional.
- ✗ **C)** Incluyen un campo Type de dos bytes.
- ✗ **D)** Incluyen el destino MAC y la fuente.

explicación

Las tramas Ethernet II NO incluyen un campo de longitud de dos bytes. Las tramas Ethernet II incluyen un campo de tipo de dos bytes.

El campo de longitud de dos bytes se incluye en 802,3 tramas.

Todas las tramas Ethernet, incluidas las tramas Ethernet II y 802.3, incluyen el destino MAC y el origen en el encabezado. Además, la etiqueta 802.1Q, que es la etiqueta lan virtual (VLAN), es opcional para todas las tramas Ethernet.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3ª Edición),Capítulo 4: Comunicación y Seguridad de Red, Ethernet 802.3

El formato de trama Ethernet II, http://www.firewall.cx/networking-topics/ethernet/ethernet-frame-formats/201-ethernet-ii.html

---

Pregunta #16 de 131

Id. de pregunta: 1105160

¿Qué protocolo se utiliza para enviar correo electrónico a un servidor en Internet?

- ✗ **A)** FTP
- ✓ **B)** SMTP
- ✗ **C)** Snmp
- ✗ **D)** Telnet
- ✗ **E)** Igmp
- ✗ **F)** Tftp

explicación

El Protocolo simple de transferencia de correo (SMTP) es un protocolo de aplicación; por lo tanto, opera en la capa superior del modelo OSI. SMTP es el protocolo predeterminado para enviar correo electrónico en sistemas operativos de Microsoft.

El Protocolo de oficina de correos (POP3) y el Protocolo de acceso a mensajes de Internet (IMAP) son los protocolos más populares para recibir correo electrónico. Otros incluyen SMTP y HTTP para algunos tipos de clientes de correo electrónico. De forma predeterminada, SMTP usa el puerto 25, POP3 usa el puerto 110 e IMAP usa el puerto 143.

El Protocolo de transferencia de archivos (FTP) es una herramienta útil y eficaz disponible para los usuarios en general. FTP permite a un usuario cargar y descargar archivos entre hosts locales y remotos. El acceso FTP anónimo suele estar disponible en muchos sitios para permitir a los usuarios el acceso a archivos públicos sin tener que

establecer una cuenta. A menudo, se requerirá que un usuario introduzca una dirección de correo electrónico válida como contraseña. De forma predeterminada, FTP utiliza los puertos 20 y 21.

El Simple Network Management Protocol (SNMP) es el protocolo que gobierna la administración de la red y la supervisión de los dispositivos de red y de sus funciones. No se limita necesariamente a las redes TCP/IP. De forma predeterminada, SNMP utiliza el puerto 161.

El Protocolo trivial de transferencia de archivos (TFTP) es una aplicación de red que es más simple que FTP pero menos capaz. Se utiliza cuando no se requiere la autenticación de usuario y la visibilidad del directorio. TFTP utiliza el Protocolo de datagramas de usuario (UDP) en lugar del Protocolo de control de transmisión (TCP). TFTP a menudo no se implementa en las redes debido a sus riesgos de seguridad inherentes, a saber, que no tiene conexión y no requiere autenticación de usuario. De forma predeterminada, TFTP utiliza el puerto 69.

Los host y los gatewayes utilizan el Internet Group Management Protocol (IGMP) en una sola red para establecer la calidad de miembro de los host en los grupos de multidifusión particulares. Las puertas de enlace utilizan la información con un protocolo de enrutamiento de multidifusión para admitir la multidifusión IP a través de Internet. Varios Routing Protocol se utilizan para descubrir a los grupos de multidifusión y para construir las rutas para cada grupo. Éstos incluyen el Multicast Protocolo-independiente (PIM), el Protocolo de ruteo del Multicast del Vector de la Distancia (DVMRP), y el Multicast Open Shortest Path First (MOSPF). Porque el IGMP es un protocolo, no es identificado por un número de puerto sino por su número de protocolo, que es 2.

Telnet es un comando de usuario y un protocolo TCP/IP subyacente para acceder a hosts remotos. Los protocolos HTTP y FTP le permiten solicitar archivos específicos de hosts remotos, pero no iniciar sesión realmente como usuario de ese equipo host. El protocolo Telnet le permite iniciar sesión como un usuario normal con los privilegios asociados que se le han concedido a la aplicación específica y los datos en ese host. En otras palabras, parece estar conectado localmente al sistema remoto. De forma predeterminada, Telnet utiliza el puerto 23.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de red, SMTP

SMTP (Protocolo simple de transferencia de correo), http://searchexchange.techtarget.com/definition/SMTP

Pregunta #17 de 131

Id. de pregunta: 1105218

¿Qué es un ataque de lágrima?

- ✓ **A)** Envía paquetes mal formados a la víctima prevista.
- ✗ **B)** Utiliza mensajes UDP para abrumar a la víctima prevista.
- ✗ **C)** Es un ataque de denegación de servicio (DoS) que utiliza mensajes ICMP de gran tamaño para abrumar a la víctima prevista.
- ✗ **D)** Utiliza mensajes ICMP para abrumar a la víctima prevista.

explicación

Un ataque teardrop envía paquetes malformados a la víctima prevista. Aprovecha las ventajas de los puntos débiles en la funcionalidad de reensamblaje de fragmentos de la pila de protocolos TCP/IP.

Un ataque pitufo utiliza mensajes ICMP para abrumar a la víctima prevista. Un ataque fraggle utiliza mensajes UDP para abrumar a la víctima prevista. Un ping de ataque de muerte es un ataque DoS que utiliza mensajes ICMP de gran tamaño para abrumar a la víctima prevista.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red, Teardrop

---

Pregunta #18 de 131

Id. de pregunta: 1105224

¿Cuál es otro término para una zona de despeje (DMZ)?

- ✗ **A)** red privada virtual (VPN)
- ✓ **B)** subred filtrada
- ✗ **C)** firewall de doble hogar
- ✗ **D)** host con pantalla

explicación

Subred filtrada es otro término para una zona desmilitarizada (DMZ). Dos Firewall se utilizan en esta configuración: un Firewall reside entre la red pública y dmz, y el otro reside entre el DMZ y la red privada.

Un host cribado es un firewall que reside entre el router que conecta una red a Internet y la red privada. El router actúa como un dispositivo de detección, y el firewall es el host de pantalla. Este firewall emplea dos tarjetas de red y un

único enrutador de filtrado.

Un firewall de doble hogar es uno que tiene dos interfaces de red: una interfaz se conecta a Internet y la otra se conecta a la red privada. Uno de los inconvenientes más comunes de los firewalls de doble hogar es que el enrutamiento interno puede activarse accidentalmente.

Una red privada virtual (VPN) no es una red física. Como su nombre lo indica, es una red virtual que permite a los usuarios que se conectan a través de Internet acceder a los recursos de la red privada al tiempo que proporciona el máximo nivel de seguridad. Se debe usar una conexión VPN cifrada para garantizar la privacidad y la integridad de los datos que se transmiten entre entidades a través de una red pública, ya sean clientes, servidores, firewalls u otro hardware de red.

Las arquitecturas de firewall incluyen hosts bastión, firewalls de host dual, hosts cribados y subredes filtradas.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #19 de 131

Id. de pregunta: 1114737

La red contiene cuatro segmentos. ¿Qué dispositivos de red puede utilizar para conectar dos o más de los segmentos de LAN juntos?

un. concentrador

B. enrutador

c. Cambiar

d. Puente

E. repetidor

F. multiplexor

- ✗ **A)** opción f
- ✗ **B)** opción e
- ✗ **C)** sólo las opciones a, b y c

✗ **D)** sólo opciones c, d y e

✗ **E)** Opción d

✗ **F)** opción A

✗ **G)** opción b

✓ **H)** opciones b, c y d solamente

✗ **I)** opción c

explicación

Los puentes, conmutadores y enrutadores se pueden utilizar para conectar varios segmentos de LAN. Los puentes y conmutadores funcionan en la capa de vínculo de datos, utilizando la dirección de control de acceso a medios (MAC) para enviar paquetes a su destino. Los enrutadores funcionan en la capa de red mediante el uso de direcciones IP para enrutar los paquetes a su destino a lo largo de la ruta más eficaz.

Los concentradores actúan como un punto de conexión central para los dispositivos de red en un segmento de red. Trabajan en la capa física.

Los repetidores se utilizan para extender la longitud de la red más allá de la distancia máxima del segmento del cable. Toman la señal de una trama recibida y la regeneran al resto de los puertos en el repetidor. También trabajan en la capa física.

Un multiplexador inverso se utiliza para conectar varias líneas T1 entre sí con fines de tolerancia a errores. El multiplexador se coloca en ambos extremos de la conexión.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, hardware

---

Pregunta #20 de 131

Id. de pregunta: 1105177

¿Qué término se utiliza más comúnmente para describir el equipo que crea una zona desmilitarizada (DMZ)?

✓ **A)** cortafuegos

✗ **B)** enrutador

✗ **C)** concentrador activo

✗ **D)** concentrador pasivo

explicación

Un firewall se utiliza para crear una zona desmilitarizada (DMZ). Una DMZ es una zona ubicada entre la red interna de una empresa e Internet que generalmente contiene servidores a los que el público accederá. La implementación de DMZ proporciona una precaución de seguridad adicional para proteger los recursos en la red interna de la empresa. Por lo general, dos firewalls se utilizan para crear una DMZ. Un Firewall reside entre la red pública y dmz, y otro firewall reside entre el DMZ y la red privada.

Un enrutador se utiliza para crear subredes individuales en una red Ethernet. Los routers operan en la capa de red del modelo OSI. Mientras que un Firewall puede también ser un router, se refiere como Firewall cuando funciona para crear un DMZ.

Un concentrador activo se utiliza para conectar dispositivos en una topología en estrella. Un concentrador activo tiene circuitos que permiten la regeneración de la señal. En una topología con cable de estrella, los errores de terminación de cableado pueden bloquear toda la red.

Un concentrador pasivo conecta dispositivos en una topología de inicio, pero no proporciona ninguna regeneración de señal.

Un firewall se clasifica como un dispositivo de control de acceso basado en reglas. Las reglas se configuran en el firewall para permitir o denegar el paso de paquetes de una red a otra. La configuración de las reglas es una de las mayores preocupaciones para un firewall, porque las reglas pueden ser muy complejas. Una configuración incorrecta puede provocar fácilmente brechas de seguridad.

Los filtros se crean de acuerdo con la política de seguridad de la empresa.

Para proporcionar la máxima seguridad de archivos, los firewalls no deben ejecutar el sistema de archivos del Sistema de información de red (NIS). Los compiladores deben eliminarse de los firewalls.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #21 de 131

Id. de pregunta: 1105161

¿Qué término se utiliza para describir el área que está cubierta por un satélite?

✗ **A)** línea de visión

✓ **B)** huella

✗ **C)** amplitud

✗ **D)** frecuencia

explicación

El término huella se utiliza para describir el área que está cubierta por un satélite. La gran huella de un satélite puede resultar en la interceptación de la transmisión satelital. Una huella cubre un área en la Tierra durante una pequeña cantidad de tiempo.

Amplitud y frecuencia son términos de comunicación analógica. La amplitud se utiliza para describir la altura de la señal. La frecuencia se utiliza para describir el número de ondas que se transmiten durante un período de tiempo.

Línea de visión es el término utilizado para describir el requisito de que un receptor no debe tener ninguna obstrucción de la señal de satélite. Esto incluye edificios, árboles y clima.

Objetivo:
Comunicación y seguridad de la red

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)** Implemente filtros en el concentrador.

✗ **C)** Reemplace el concentrador por un repetidor.

✓ **D)** Reemplace el concentrador por un conmutador.

explicación

Debe reemplazar el concentrador por un conmutador. Esto proporcionará cierta protección contra el olfato de tráfico. En una red que utiliza concentradores, los paquetes son visibles para todos los nodos de la red. Cuando se utilizan los switches, los paquetes se reenvían sólo al host para el que está destinado el paquete porque un conmutador no reenvía paquetes hacia fuera todos sus puertos. Esto evita que la capacidad de los usuarios de la misma red vea el tráfico de los demás, lo que proporciona cierto nivel de protección contra el rastreo de tráfico. El olfato de tráfico captura paquetes de datos no pensados para el rastreador. Un sistema de detección de intrusiones (IDS) basado en la red se puede utilizar para capturar paquetes en un conmutador.

No debe reemplazar el concentrador con un repetidor. Un repetidor recibe una señal y la repite, asegurando así que la degradación de la señal no se produzca. Un repetidor no puede proteger contra el tráfico que huele por sí mismo.

No puede implementar filtros o ACL en un concentrador. La implementación de filtros y ACL en conmutadores o enrutadores proporciona un medio por el que se permite o impide el tráfico y, a continuación, se reenvía al nodo adecuado. La aplicación de filtros a los enrutadores puede proteger contra los ataques de suplantación de protocolo de Internet (IP).

El sniffing es la acción de capturar y monitorear el tráfico que pasa a través de la red. En un entorno de red normal, la información de cuenta y contraseña se pasa en texto no cifrado. Por esta razón, no es difícil comprometer toda la red poniendo una máquina en modo promiscuo y capturando todas las contraseñas.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, Switch

Rastreadores: ¿Qué son y cómo protegerse, http://www.colasoft.com/resources/sniffer.php

---

Pregunta #23 de 131

Id. de pregunta: 1114747

Va a implementar una red privada virtual (VPN) para usuarios remotos. Desea cumplir los siguientes objetivos:

La puerta de enlace de VPN debe requerir el uso del protocolo de seguridad de Internet (IPSec).

Todos los usuarios remotos deben usar IPSec para conectarse a la puerta de enlace de VPN.

Ningún host interno debe utilizar IPSec.

¿Qué modo IPSec debe utilizar?

✗ **A)** host a host

✗ **B)** puerta de enlace a puerta de enlace

✓ **C)** host a puerta de enlace

✗ **D)** Esta configuración no es posible.

explicación

Debe implementar el modo IPSec de host a puerta de enlace. En esta configuración, la puerta de enlace de VPN requiere el uso de IPSec para todos los clientes remotos. Los clientes remotos utilizan IPSec para conectarse a la puerta de enlace de VPN. Cualquier comunicación entre la puerta de enlace de VPN y los hosts de Internet en nombre de los clientes remotos no utiliza IPSec. Sólo el tráfico a través de Internet utiliza IPSec.

En el modo IPSec de host a host, cada host debe implementar IPSec. Este modo requeriría que cualquier host interno que se comunique con los clientes VPN necesitaría implementar IPSec.

En el modo IPSec de puerta de enlace a puerta de enlace, las puertas de enlace en cada extremo de la conexión proporcionan funcionalidad IPSec. Los anfitriones individuales no lo hacen. Por esta razón, la VPN es transparente para los usuarios. Esta implementación funciona mejor cuando una sucursal o empresa asociada necesita acceso a la red.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, IPSec e ISAKMP

Pregunta #24 de 131

Id. de pregunta: 1105167

¿Qué protocolo responde a las solicitudes de ping?

✓ **A)** Icmp

✗ **B)** Rarp

✗ **C)** ARP

✗ **D)** TCP

explicación

Al hacer ping a un host, el Protocolo de mensajes de control de Internet (ICMP) responderá a la solicitud. ICMP es responsable de enviar mensajes entre dispositivos de red relacionados con el estado de la red.

Si el ping es correcto, la información devuelta proporcionará información de respuesta. "Responder" significa que el host es accesible y está respondiendo a las solicitudes. Si el ping no se realiza correctamente, la información devuelta indicará el tipo de problema experimentado. Algunos códigos de error posibles podrían ser destino inalcanzable, protocolo inalcanzable y sin respuesta.

El Protocolo de resolución de direcciones (ARP) es responsable de asignar la dirección de hardware de los hosts de las redes de difusión con la dirección TCP/IP de cada host. La utilidad ARP permite que usted vea el caché ARP, que asocia cada dirección IP a una dirección física.

El Protocolo de control de transmisión (TCP) es un protocolo orientado a la conexión que opera en la capa de transporte del modelo OSI.

El Protocolo de resolución de direcciones inversas (RARP) permite que un host de una red de área local solicite su dirección IP de la tabla o caché del Protocolo de resolución de direcciones (ARP) de un servidor de puerta de enlace.

ARP y RARP asignan las direcciones de protocolo de Internet (IP) versión 4 de 32 bits a su dirección Ethernet o MAC de 48 bits correspondiente. La dirección MAC es un número codificado de forma incorrecta para la tarjeta de interfaz de red (NIC) asignada por el fabricante. La dirección IP es asignada automáticamente por el servidor DHCP de la red o manualmente por el administrador de red. ARP hace juego la dirección IP a la dirección MAC; RARP hace juego la dirección MAC a la dirección IP.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, ICMP

Pregunta #25 de 131

Id. de pregunta: 1113951

Administrar una red TCP/IP que no está en subredes. Uno de los hosts de red tiene la siguiente dirección IP:

130.250.0.10

¿Qué dirección IP es el identificador de red de la red que administra?

✗ **A)** 130.250.255.255

✗ **B)** 255.255.255.255

✗ **C)** 128.0.0.0

✓ **D)** 130.250.0.0

explicación

El identificador de red de la red que administra es 130.250.0.0. Según el escenario, la red no está en subredes y está configurada con direcciones IP de clase B. En una dirección IP de clase B, los primeros 16 bits de la dirección IP corresponden a la dirección de red y los últimos 16 bits de la dirección corresponden a la dirección del host.

En notación decimal con puntos, un número decimal representa cada parte de 8 bits, o octeto, de una dirección IP. Por lo tanto, la dirección de red para la red que administra es los dos primeros octetos seguidos de dos octetos de ceros o 130.250.0.0. La dirección 128.0.0.0 es el primer identificador de red válido en el intervalo de direcciones IP de clase B que no están en subredes. La dirección 130.250.255.255 es la dirección de difusión de la red con el identificador de red 130.250.0.0. La dirección IP 255.255.255.255 es una dirección de difusión general o universal a todas las redes de una red TCP/IP.

Antes de que se introdujera el enrutamiento de interdominios sin clases (CIDR), las redes se organizaban comúnmente por clases. En una dirección de clase B, el primer bit de la dirección se establece en uno y el segundo bit de la dirección se establece en cero.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPv4

Calculadoras de red, http://www.subnetmask.info/

Pregunta #26 de 131

Id. de pregunta: 1105136

¿En qué capa OSI funciona un concentrador activo?

✗ **A)** sesión

✗ **B)** red

✓ **C)** físico

✗ **D)** transporte

explicación

Los concentradores activos o repetidores multipuerto amplifican o regeneran las señales a todos los demás puertos del concentrador. Debido a que los concentradores activos regeneran las señales, a menudo se utilizan para extender la longitud de los segmentos más allá de sus longitudes máximas especificadas. Ellos, al igual que con todos los concentradores, se consideran dispositivos de capa física porque actúan sobre los datos a nivel de bits.

La capa física define los estándares X.25, V.35, X.21 e interfaz serie de alta velocidad (HSSI). Estos estándares definen el tipo de conector, así como el tipo de señalización utilizada. La capa física, junto con la capa de vínculo de datos y de red, proporciona compatibilidad con los componentes necesarios para transmitir el mensaje de red.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, capa de sesión

---

Pregunta #27 de 131

Id. de pregunta: 1105171

¿Qué función NO se realiza en la capa física del modelo OSI?

- ✗ **A)** definir las características eléctricas de los medios de comunicación
- ✗ **B)** Definir el tipo de conector que se utiliza
- ✓ **C)** Definir el tipo de cifrado que se utiliza para los datos
- ✗ **D)** definir el tamaño del cable Ethernet

explicación

El método de cifrado de datos que se utiliza no está definido en la capa física del modelo OSI. El cifrado de datos se admite en las capas De vínculo de datos, Red, Transporte, Sesión y Aplicación del modelo OSI.

La capa física se ocupa de los impulsos eléctricos, las señales de luz y radio, los cables físicos, las tarjetas y otros aspectos físicos del medio de comunicación. La definición del tipo de conectores que se utilizan y las limitaciones de tamaño y distancia del cable Ethernet son algunas otras funciones que se realizan en la capa física.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red. Capa física

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

Pregunta #28 de 131

Id. de pregunta: 1105190

¿En qué capa del modelo OSI funcionan los routers?

- ✗ **A)** Enlace de datos
- ✗ **B)** sesión
- ✓ **C)** red
- ✗ **D)** transporte
- ✗ **E)** físico

explicación

Los enrutadores funcionan en la capa de red del modelo de red OSI. Utilizan direcciones de origen y destino, que se encuentran en la capa de red, para enrutar paquetes. Los switches utilizan direcciones MAC, que se encuentran en la capa de enlace de datos, para reenviar tramas.

La capa Session inicia, mantiene y detiene las sesiones entre aplicaciones en diferentes dispositivos de red.

La capa física proporciona las funciones para establecer y mantener el vínculo físico entre los dispositivos de red. Los repetidores trabajan en la capa física.

La capa de transporte del modelo OSI segmenta y vuelve a ensamblar los datos en un flujo de datos y proporciona una transmisión de datos de extremo a extremo fiable y no fiable.

Los puentes funcionan en la capa Data-Link.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, Router

Pregunta #29 de 131

Id. de pregunta: 1114726

Su empresa ha decidido implementar una red inalámbrica. Los usuarios de la red inalámbrica deben poder conectarse a los recursos de la red interna, incluidos los servicios de archivo, impresión y DHCP. Todos los clientes inalámbricos ejecutarán el sistema operativo Windows.

¿Qué deberías implementar?

un. Modo de infraestructura

B. Modo ad hoc

c. Un punto de acceso inalámbrico

d. Direcciones IP estáticas

e. APIPA

- ✓ **A)** Sólo las opciones A y C
- ✗ **B)** opción c
- ✗ **C)** Opción d
- ✗ **D)** Sólo opciones B y E
- ✗ **E)** Opciones B y D Sólo
- ✗ **F)** opción b
- ✗ **G)** opción e
- ✗ **H)** opción A

explicación

Debe implementar el modo de infraestructura con un punto de acceso inalámbrico. El modo de infraestructura permite que los equipos inalámbricos se conecten a una LAN, una WAN o Internet. Esto significa que los equipos inalámbricos en modo infraestructura pueden acceder a todos los equipos de la LAN, WAN e Internet. El modo de infraestructura es mucho más costoso de implementar que el modo ad hoc porque debe configurar puntos de acceso inalámbricos. Aunque el modo de infraestructura es más difícil de instalar y configurar, es mucho más fácil de administrar que el modo ad hoc.

El modo ad hoc permite configurar equipos inalámbricos mucho más rápidamente que el modo de infraestructura. Todos los equipos inalámbricos en modo ad hoc participan en la misma red. Esto significa que los equipos inalámbricos ad hoc pueden tener acceso entre sí, pero no pueden tener acceso a los recursos de red en una LAN, WAN o Internet. El modo ad hoc es mucho más barato que el modo de infraestructura para implementar. Además, es

fácil de instalar y configurar y puede proporcionar un mejor rendimiento que el modo de infraestructura. Sin embargo, es difícil administrar una red inalámbrica en modo ad hoc.

Las direcciones IP estáticas no deben implementarse porque la red corporativa contiene un servidor DHCP. APIPA no debe utilizarse por la misma razón. Además, APIPA se utiliza sólo si no se encuentra un servidor DHCP.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, modo de infraestructura frente al modo ad hoc

Descripción del modo ad hoc, http://www.wi-fiplanet.com/tutorials/article.php/1451421

LANs inalámbricas: Ampliación del alcance de una LAN, http://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=4

Pregunta #30 de 131

Id. de pregunta: 1114740

¿Qué dispositivo de red actúa como puerta de enlace a Internet, firewall y servidor de almacenamiento en caché de Internet para una red privada?

- ✗ **A)** Identificadores
- ✓ **B)** servidor proxy
- ✗ **C)** VPN
- ✗ **D)** Ips

explicación

Un servidor proxy actúa como en la puerta de enlace a Internet, el firewall y el servidor de almacenamiento en caché de Internet para una red privada. Los hosts de la red privada se ponen en contacto con el servidor proxy con una solicitud de sitio web de Internet. El servidor proxy comprueba su caché para ver si hay disponible una copia almacenada localmente del sitio. Si no es así, el servidor proxy se comunica con su conexión a Internet para recuperar el sitio Web. El servidor proxy es prácticamente invisible para el cliente y la conexión a Internet. Un servidor proxy se puede configurar para permitir sólo el tráfico saliente de protocolo de transferencia de hipertexto (HTTP) mediante la configuración de qué usuarios tienen permisos para tener acceso a Internet a través del servidor proxy.

Una red privada virtual (VPN) es una red privada a la que los usuarios pueden conectarse a través de una red pública. Una VPN se puede implementar de las siguientes maneras:

Instalando agentes de software o hardware en el cliente o en la red

mediante la implementación de sistemas de intercambio de claves y certificados

implementando sistemas de autenticación de nodos

Un sistema de detección de intrusiones (IDS) es un dispositivo de red que detecta la intrusión en la red y registra la intrusión o se pone en contacto con el personal adecuado.

Un sistema de prevención de intrusiones (IPS) es un dispositivo de red que detecta los intentos de intrusión en la red y evita la intrusión en la red. Un IPS proporciona más seguridad que un IDS porque en realidad proporciona prevención, no solo detección.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, tipos de firewall

Servidor proxy, http://whatis.techtarget.com/definition/0,sid9_gci212840,00.html

---

Pregunta #31 de 131

Id. de pregunta: 1105181

¿Qué es SOCKS?

✗ **A)** Un servidor de seguridad de filtrado dinámico de paquetes que utiliza los puertos superiores a 1023 para establecer conexiones dinámicamente

✓ **B)** Un servidor de seguridad proxy de nivel de circuito que proporciona un canal seguro entre dos equipos

✗ **C)** Un servidor de seguridad proxy de nivel de aplicación que tiene filtros de servicio preconfigurados

✗ **D)** Un servidor de seguridad proxy del núcleo que procesa en el núcleo y crea una pila para cada paquete

explicación

SOCKS es un firewall proxy de nivel de circuito que proporciona un canal seguro entre dos equipos. SOCKS actúa como un proxy de conexión y funciona independientemente de los protocolos de aplicación TCP/IP. Las aplicaciones de red deben actualizarse para que funcionen con SOCKS.

SOCKS no es un firewall proxy de nivel de aplicación, un firewall proxy de kernel o un firewall de filtrado dinámico de paquetes.

Los firewalls proxy a nivel de circuito toman decisiones de reenvío basadas únicamente en la dirección IP y la información del puerto de servicio. Un firewall proxy de nivel de circuito es más fácil de mantener que un firewall de proxy de nivel de aplicación, pero no es tan seguro ni consume tantos recursos. A veces, los firewalls a nivel de circuito se denominan puertas de enlace a nivel de circuito.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, tipos de firewall

---

Pregunta #32 de 131

Id. de pregunta: 1105209

¿Qué dispositivo o componente de red garantiza que los equipos de la red cumplen las directivas de seguridad de una organización?

- ✗ **A)** NAT
- ✗ **B)** Dmz
- ✓ **C)** Nac
- ✗ **D)** IPSec

explicación

El Control de acceso a la red (NAC) garantiza que el equipo de la red cumpla las directivas de seguridad de una organización. Las directivas de usuario del NAC se pueden aplicar en función de la ubicación del usuario de la red, de la calidad de miembro del grupo, o de algunos otros criterios.

Traducción de direcciones de red (NAT) es un estándar IEEE que proporciona una solución de firewall transparente entre una red interna y redes externas. Con NAT, varios equipos internos pueden compartir una única interfaz de Internet y una dirección IP.

El protocolo de seguridad de Internet (IPSec) es un protocolo que protege la comunicación IP a través de una red privada o pública. IPSec se utiliza para crear una VPN. Un ejemplo es el uso de un portátil habilitado para General Packet Radio Services (GPRS) que se conecta a una intranet corporativa a través de una VPN.

Una zona desmilitarizada (DMZ) es una sección de una red que está aislada del resto de la red con firewalls. Los servidores de una DMZ son más seguros que los de la red normal.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

La parte complicada del despliegue del NAC, http://www.networkworld.com/newsletters/vpn/2008/101308nac1.html

---

Pregunta #33 de 131

Id. de pregunta: 1105135

¿Qué función OSI garantiza que se verifique la identidad del host remoto y que los datos recibidos sean auténticos?

- ✗ **A)** enrutamiento
- ✗ **B)** encriptación
- ✗ **C)** segmentación
- ✓ **D)** autenticación

explicación

La autenticación es la función OSI que garantiza que se verifica la identidad del host remoto y que los datos recibidos son auténticos. Este proceso tiene lugar en la capa Session.

El enrutamiento es la función OSI que garantiza que un paquete pueda llegar a su destino. Este proceso tiene lugar en la capa de red.

El cifrado es la función OSI que garantiza la confidencialidad de los datos mediante el cifrado de los datos. Este proceso tiene lugar en la capa Presentation.

La segmentación es la función OSI que divide los datos en paquetes de fácil transmisión. Este proceso tiene lugar en la capa de transporte.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, capa de sesión

---

Pregunta #34 de 131

Id. de pregunta: 1105241

¿Qué protocolo debe configurar en un servidor de acceso remoto para autenticar a los usuarios remotos con tarjetas inteligentes?

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

explicación

Debe utilizar el Protocolo de autenticación extensible (EAP). Mediante el uso de un protocolo de autenticación EAP, como eap-transport level security (EAP-TLS), para la autenticación, el servidor de acceso remoto puede autenticar a los usuarios remotos con tarjetas inteligentes.

Los otros protocolos de autenticación enumerados no admiten la autenticación mediante tarjetas inteligentes.

El Protocolo de autenticación de contraseña (PAP) requiere que los usuarios se autentiquen mediante una contraseña. La contraseña se transmite en texto sin formato, lo que permite una posible violación de seguridad.

El Protocolo de autenticación por desafío mutuo (CHAP) proporciona un mayor nivel de seguridad. Las contraseñas no se envían en texto sin formato. Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP) viene en dos versiones. La versión 2 proporciona una mejor seguridad porque proporciona autenticación mutua, lo que significa que se autentican ambos extremos de la conexión.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, 802.1x

---

Pregunta #35 de 131

Id. de pregunta: 1113949

Se está preparando para realizar el mantenimiento de rutina en la red. La red debe permanecer inaccesible mientras realiza este mantenimiento. Enviar un mensaje con el encabezado de paquete 135.135.255.255.

¿Qué logra esa dirección de paquete?

- ✗ **A)** Evita que otros usuarios inicien sesión en la red 135.135.
- ✗ **B)** Muestra quién está accediendo a la red 135.135.
- ✗ **C)** Visualiza cuántas estaciones están conectadas con la red 135.135.
- ✓ **D)** Transmite su mensaje a todas las estaciones de la red 135.135.

explicación

Transmite su mensaje a todas las estaciones de la red 135.135. La dirección de red 135.135.255.255 es una dirección de clase B. La dirección de nodo de 255.255 hace que este mensaje se difunda a todas las direcciones IP con una dirección IP de 135.135.x.x. Debido a que la radiodifusión se puede utilizar en algunos ataques, muchas redes han bloqueado cualquier comunicación utilizando la dirección de difusión.

Un ID de host que es todos los unos se reserva como una dirección de difusión dentro de una subred determinada para todos los hosts de esa subred. Por ejemplo, dentro de la red de clase C 192.15.28 y sin subredes, la dirección 192.15.28.255 difunde a todos los hosts de esta red. Si los bits de la parte de red son todos unos, se reserva la dirección y 255.255.255.255 es la dirección de difusión universal.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPv4

Pregunta #36 de 131

Id. de pregunta: 1105251

Usted es responsable de administrar el entorno de virtualización de su empresa. ¿Qué característica NO se debe permitir en un host de virtualización?

- ✗ **A)** implementar un firewall
- ✗ **B)** implementar IPsec
- ✗ **C)** Supervisar los registros de sucesos
- ✓ **D)** navegar por Internet

explicación

No debe permitir la exploración por Internet en un host de virtualización. Esto puede presentar una posible brecha de seguridad a través de la introducción de spyware o malware. Todo lo que afecta a un host de virtualización también afecta a todos los equipos virtuales del host. Los servidores virtuales tienen los mismos requisitos de seguridad de la información que los servidores físicos.

Debe implementar IPsec, implementar un firewall y supervisar los registros de eventos de un host de virtualización. IPsec ayuda cifrando los datos a medida que se transmiten a través de la red. Los firewalls impiden el acceso no autorizado a un equipo físico o virtual. Los registros de eventos ayudan a los administradores a detectar cuándo se han producido o se están intentando realizar infracciones de seguridad.

Un host de virtualización también se puede denominar escritorio virtual. A menudo, las aplicaciones virtuales se hospedan en un host virtual.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, virtualización

---

Pregunta #37 de 131

Id. de pregunta: 1105253

¿Cuál es la velocidad en kilobits por segundo (Kbps) de un canal D en una línea ISDN BRI?

- ✗ **A)** 56 Kbps
- ✗ **B)** 64 Kbps
- ✓ **C)** 16 Kbps

✗ **D)** 128 Kbps

explicación

El canal delta (D) en una conexión de red digital de servicios integrados (ISDN) de interfaz de velocidad básica (BRI) funciona a 16 Kbps. Una conexión BRI ISDN tiene un solo canal D y dos canales portadores (B). El canal D transporta información de señalización y control para una conexión ISDN.The D channel carries signaling and control information for an ISDN connection. Los canales B operan a 64 Kbps y transportan comunicaciones de datos o voz. Los dos canales B en una conexión BRI RDSI se pueden combinar para una velocidad total de transmisión de datos de 128 Kbps. Los módems pueden funcionar a una velocidad teórica máxima de 56 Kbps, aunque los módems rara vez pueden proporcionar esta velocidad en la práctica.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, ISDN

Pregunta #38 de 131

Id. de pregunta: 1105220

¿Qué afirmación es cierta del secuestro de direcciones de red?

✗ **A)** Implica inundar el sistema de destino con paquetes fragmentados mal formados para interrumpir las operaciones.

✗ **B)** Utiliza mensajes de eco ICMP para identificar los sistemas y servicios que están en funcionamiento.

✗ **C)** Se utiliza para identificar la topología de la red de destino.

✓ **D)** Permite al atacante redirigir el tráfico de datos de un dispositivo de red a un equipo personal.

explicación

El secuestro de direcciones de red permite a un atacante redirigir el tráfico de datos de un dispositivo de red a un equipo personal. También conocido como secuestro de sesión, el secuestro de direcciones de red permite a un atacante capturar y analizar los datos dirigidos a un sistema de destino. Esto permite a un atacante obtener acceso a recursos críticos y credenciales de usuario, como contraseñas, y a sistemas críticos de una organización. Secuestro

de sesión implica asumir el control de una conexión existente después de que el usuario ha creado correctamente una sesión autenticada.

Un ataque de análisis se utiliza para identificar la topología de la red de destino. También conocido como reconocimiento de red, el análisis implica identificar los sistemas que están en funcionamiento en la red de destino y comprobar los puertos que están abiertos, los servicios que hospeda un sistema, el tipo de sistema operativo y las aplicaciones que se ejecutan en un host de destino. El escaneo es el proceso inicial de recopilar información sobre una red para descubrir vulnerabilidades y exploits antes de que se produzca un intento real de cometer una violación de seguridad.

Un ataque pitufo utiliza mensajes de eco ICMP para identificar los sistemas y servicios que están en funcionamiento. Es un ataque de denegación de servicio (DoS) que utiliza mensajes ping de difusión falsificados para inundar un sistema de destino. En un ataque pitufo, el atacante envía una gran cantidad de paquetes de eco ICMP con la dirección IP de orígenes suplantados como la del host de destino a las direcciones de difusión IP. Esto hace que el host de destino se inunde con respuestas de eco de toda la red, lo que hace que el sistema se congele o se bloquee. Ping de la muerte, bonk, y fraggle son otros ejemplos de ataques DoS.

En un ataque teardrop, el atacante utiliza una serie de paquetes fragmentados IP, lo que hace que el sistema se congele o se bloquee mientras el host de destino está reensamblando los paquetes. Un ataque teardrop se basa principalmente en la implementación de fragmentación de IP. Para volver a montar los fragmentos en el paquete original en el destino, el host busca paquetes entrantes para asegurarse de que pertenecen al mismo paquete original. Los paquetes están mal formados. Por lo tanto, el proceso de volver a ensamblar los paquetes hace que el sistema se congele o se bloquee.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, secuestro de sesiones

---

Pregunta #39 de 131

Id. de pregunta: 1114745

¿Cuál de las siguientes directivas debe implementar para los teletrabajadores que reciben equipos portátiles de la empresa?

un. No permita que familiares o amigos usen el equipo emitido por la compañía.

B. No se conecte a redes inalámbricas no seguras.

c. Realizar una copia de seguridad del equipo emitido por la empresa fuera de la red de la empresa.

d. Utilice el ordenador emitido por la empresa como un ordenador personal.

- ✗ **A)** Opción d
- ✓ **B)** opciones A y B
- ✗ **C)** opción b
- ✗ **D)** opción A
- ✗ **E)** opción c
- ✗ **F)** Opciones C y D
- ✗ **G)** todas las opciones

explicación

Si su empresa emite equipos portátiles de empresa a teletrabajadores, debe asegurarse de que las directivas de seguridad se comunican a los teletrabajadores. Estas políticas deben incluir lo siguiente:

No permita que familiares o amigos usen el equipo emitido por la compañía.

No se conecte a redes inalámbricas no seguras.

No realice una copia de seguridad del equipo emitido por la empresa fuera de la red de la empresa.

No utilice el equipo emitido por la empresa como un equipo personal.

No modifique la configuración administrativa o de seguridad.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, tecnologías de conexión remota

---

Pregunta #40 de 131

Id. de pregunta: 1105199

Usted sabe que cualquier sistema de la zona de distensión puede verse comprometido porque la zona de distensión es accesible desde Internet.

¿Qué debes hacer debido a esto?

✗ **A)** Implemente ambos firewalls DMZ como hosts bastión.

✗ **B)** Implemente el firewall DMZ que se conecta a la red privada como un host bastión.

✓ **C)** Implemente cada equipo en la DMZ como hosts bastión.

✗ **D)** Implemente el firewall DMZ que se conecta a Internet como un host bastión.

explicación

Debe implementar cada equipo en la zona desmilitarizada (DMZ) como hosts bastión porque cualquier sistema en la DMZ puede verse comprometido. Un anfitrión bastión es, en esencia, un sistema que está endurecido para resistir los ataques.

Un host bastión no está conectado a ningún software de firewall. Sin embargo, cada firewall debe ser reforzado como un host bastión.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #41 de 131

Id. de pregunta: 1113972

¿Cuál es el término para la técnica que conecta un emisor y un receptor de red por una única ruta de acceso durante la duración de una conversación?

✗ **A)** conmutación de ruta de acceso

✓ **B)** conmutación de circuitos

✗ **C)** conmutación de paquetes

✗ **D)** conmutación de mensajes

explicación

La conmutación de circuitos es una técnica de conmutación que conecta un emisor y un receptor de red mediante una única ruta de acceso que existe durante la conversación. El equipo de envío envía una señal al equipo de destino, solicitando una conexión. Una vez que el equipo de destino ha establecido la conexión, se envía una confirmación al

equipo de envío para hacerle saber que puede continuar con su transferencia. Los teléfonos son un ejemplo de una red de conmutación de circuitos.

La conmutación de ruta no es una técnica de conmutación.

La conmutación de paquetes divide los mensajes en pequeñas unidades de datos o paquetes. Los paquetes se marcan con una dirección de origen, intermedia y de destino y se envían a su destino tomando una ruta compartida por muchos usuarios de la red. Dado que no hay una conexión dedicada establecida antes de que se envíe el paquete, este tipo de comunicación se conoce como comunicación sin conexión. Usando la dirección de destino, el paquete se envía a lo largo de la mejor ruta de muchas trayectorias posibles. Internet es un ejemplo de una red que utiliza principalmente conmutación de paquetes. Las redes de Frame Relay y X.25 también utilizan la conmutación de paquetes. Frame Relay utiliza una red pública conmutada para proporcionar una conexión de red de área extensa (WAN).

El cambio de mensajes divide la conversación en mensajes en lugar de establecer una conexión dedicada. Estos mensajes contienen una dirección de destino, que se utiliza para enviar los mensajes de un dispositivo a otro. Cada dispositivo almacena los mensajes durante un breve período y, a continuación, los reenvía al siguiente dispositivo. Esta técnica también se conoce como "almacenar y reenviar". Los servicios de soporte como el correo electrónico y el uso compartido de calendarios utilizan el cambio de mensajes.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Redes de conmutación de paquetes frente a redes de conmutación de circuitos, https://www.computerworld.com/article/2593382/networking/networking-packet-switched-vs-circuit-switched-networks.html

---

Pregunta #42 de 131

Id. de pregunta: 1105163

¿Qué método de acceso a medios especifica el estándar 802.11 para las redes inalámbricas?

✗ **A)** CSMA/CD
✗ **B)** Prioridad de la demanda
✗ **C)** Paso de tokens
✓ **D)** CSMA/CA

explicación

El estándar IEEE 802.11, que es el estándar principal para las LAN inalámbricas, especifica el uso de carrier sense multiple access/collision avoidance (CSMA/CA) para su método de acceso a medios. Al igual que una red Ethernet, que utiliza la detección múltiple de acceso/colisión por operador (CSMA/CD), las tarjetas adaptadoras inalámbricas "detectan" o escuchan el tráfico de red antes de transmitir. La diferencia es que CSMA/CA requiere un token; CSMA/CD NO requiere un token.

En CSMA/CA, si la red está libre de tráfico, la estación enviará sus datos. Sin embargo, a diferencia de una red Ethernet, las tarjetas de red inalámbricas no pueden enviar y recibir transmisiones al mismo tiempo, lo que significa que no pueden detectar una colisión. En su lugar, la estación de envío esperará a que el equipo de destino envíe un paquete de confirmación (ACK) que compruebe que se han recibido los datos. Si, después de un período de tiempo aleatorio, no se ha recibido una confirmación, la estación de envío retransmitirá los datos. El estándar 802.11 también se refiere a CSMA/CA como función de coordinación distribuida (DCF).

Las computadoras de detección de múltiples accesos/colisiones (CSMA/CD) de detección de portadora compiten por el derecho a enviar datos. En CSMA/CD, cuando se produce una colisión, los equipos que envían los datos esperan una cantidad aleatoria de tiempo antes de intentar retransmitir los datos.

Los métodos de acceso de paso de tokens solo permiten que el equipo que tiene el token transmita datos, lo que significa que no hay contención para el acceso a medios.

La prioridad de demanda es un estándar 802.12 conocido como 100VG-AnyLAN. Funciona a 100 Mbps. En caso de contención en la red, los datos de mayor prioridad se dan acceso primero.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, CSMA/CD Versus CSMA/CA

Pregunta #43 de 131

Id. de pregunta: 1105259

Su organización ha firmado un contrato con el ejército de los Estados Unidos. Como parte de este contrato, se debe proteger toda la comunicación por correo electrónico entre su organización y las fuerzas armadas de EE. UU. ¿Qué estándar de correo electrónico debe utilizar para esta comunicación?

✗ **A)** Extensión multipropósita de correo Internet (MIME)

✓ **B)** Protocolo de seguridad de mensajes (MSP)

✗ **C)** Bastante buena privacidad (PGP)

✗ **D)** Correo de privacidad mejorada (PEM)

explicación

Debe utilizar el protocolo de seguridad de mensajes (MSP). Este protocolo es utilizado por los militares para proteger los mensajes de correo electrónico. Se utiliza para firmar y cifrar mensajes y realizar funciones hash.

El estándar de correo electrónico MIME (Multipurpose Internet Mail Extension) especifica cómo se van a transferir los datos adjuntos de correo electrónico. Secure Mime (S/MIME) es un estándar de correo electrónico que amplía MIME al proporcionar un medio para cifrar datos y datos adjuntos de correo electrónico. S/MIME también proporciona firmas digitales para MIME. Ninguno de los dos es utilizado por los militares.

El correo mejorado por privacidad (PEM) proporciona cifrado de correo electrónico, pero no es utilizado por los militares.

Pretty Good Privacy (PGP) también proporciona cifrado de correo electrónico. Emplea algoritmos de clave simétrica, algoritmos de clave asimétrica, algoritmos de síntesis de mensajes, claves, etc.

Para garantizar la autenticidad y confidencialidad del mensaje de correo electrónico, el remitente debe firmar el mensaje con la clave privada del remitente y cifrar el mensaje con la clave pública del receptor, respectivamente.

La mejor manera de garantizar el no repudio de un correo electrónico es utilizar una firma digital.

Un directorio de correo electrónico no se considera seguro. Como tal, los documentos y datos confidenciales no deben almacenarse allí. Además, dado que el directorio de correo electrónico puede ser purgado en cualquier momento por el administrador de correo electrónico, los registros permanentes no deben almacenarse allí.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Correo mejorado de privacidad, 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)** Opciones A y E Solamente
- ✗ **E)** opción c
- ✗ **F)** opción b
- ✗ **G)** opción e
- ✗ **H)** opción A

explicación

El control de flujo, la notificación de errores, el direccionamiento de dispositivos físicos y la especificación de la topología de red pueden tener lugar en la capa de vínculo de datos. Tenga en cuenta que la notificación de errores tiene lugar en la capa de vínculo de datos, también denominada capa de vínculo, mientras que la corrección de errores es una función de la capa de transporte. La capa de transporte especifica si el método de entrega es confiable o no confiable, lo que se conoce como entrega de mejor esfuerzo, y controla la segmentación y el reensamblaje de datos en un flujo de datos.

Dado que el direccionamiento físico del dispositivo se produce en la capa de vínculo de datos, la capa de vínculo de datos utiliza la dirección para determinar si es necesario pasar el mensaje a la pila de protocolos y a qué pila de capa superior pasarlo. La capa de vínculo de datos admite servicios orientados a la conexión y sin conexión y proporciona secuenciación de tramas y control de flujo.

El enrutamiento se realiza en la capa de red del modelo OSI utilizando el direccionamiento lógico para determinar la ruta y la configuración. El establecimiento de los niveles de voltaje en los medios de transmisión se realiza en la capa física.

Algunos de los protocolos que funcionan en la capa de vínculo de datos son el Protocolo de Internet de línea serie (SLIP), el Protocolo punto a punto (PPP), el Protocolo de resolución de direcciones inversas (RARP) y el Reenvío de capa 2 (L2F).

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, capa de enlace de datos

---

Pregunta #45 de 131

Id. de pregunta: 1105247

¿Qué tipo de conexión de red se crea mediante la tunelización a través de una red pública?

- ✗ **A)** una WAN
- ✗ **B)** un HOMBRE
- ✓ **C)** una VPN
- ✗ **D)** una LAN

explicación

Una red privada virtual (VPN) se crea mediante la tunelización a través de una red pública, como Internet. Los protocolos de tunelización, como el Protocolo de túnel punto a punto (PPTP) y el Protocolo de túnel de capa 2 (L2TP), pueden crear un túnel, que es una conexión segura a través de una red pública.

Una conexión de red de área local (LAN) se crea normalmente mediante un protocolo de comunicación de red de capa física. Una red de área metropolitana (MAN), que abarca el área de una ciudad, se crea mediante conexiones dedicadas. Una conexión de red de área extensa (WAN) abarca una gran distancia, como la distancia entre ciudades o continentes. Una conexión WAN normalmente consta de dos o más conexiones LAN y se puede crear mediante líneas arrendadas o conexiones dedicadas.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, VPN

Pregunta #46 de 131

Id. de pregunta: 1114733

¿Qué tipo de firewall examina primero un paquete para ver si es el resultado de una conexión anterior?

✗ **A)** firewall proxy a nivel de circuito

✓ **B)** firewall con estado

✗ **C)** firewall proxy de nivel de aplicación

✗ **D)** firewall de filtrado de paquetes

explicación

Un firewall con estado examina primero un paquete para ver si es el resultado de una conexión anterior. La información sobre las conexiones anteriores se mantiene en la tabla de estados.

Ninguno de los otros firewalls examina primero un paquete para ver si es el resultado de una conexión anterior.

Con un firewall con estado, se permite un paquete si es una respuesta a una conexión anterior. Si la tabla de estados no contiene ninguna información sobre el paquete, el paquete se compara con la lista de control de acceso (ACL). Dependiendo del ACL, el paquete será remitido al host apropiado o ser caído totalmente.

Los firewalls con estado realizan las siguientes tareas:

Escanee la información de todas las capas del paquete.

Guarde la información de estado derivada de comunicaciones anteriores, como la información del puerto saliente, para que la comunicación de datos entrantes se pueda comprobar con ella.

Proporcionar compatibilidad de seguimiento para protocolos sin conexión mediante el uso de bases de datos de estado de sesión.

Permitir el acceso a la información de estado derivada de otras aplicaciones a través del firewall solo para servicios autorizados, como usuarios previamente autenticados.

Evaluar y manipular expresiones flexibles basadas en la comunicación y la información de estado derivada de la aplicación.

Los firewalls con estado se pueden utilizar para realizar un seguimiento de los protocolos sin conexión, como el Protocolo de datagramas de usuario (UDP), porque examinan más que el encabezado del paquete.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, tipos de firewall

Pregunta #47 de 131

Id. de pregunta: 1105246

¿Qué configuración de IPSec se puede utilizar para firmar y encapsular digitalmente cada paquete dentro de otro paquete?

- ✗ **A)** Protocolo ESP en modo túnel
- ✗ **B)** Protocolo ESP en modo de transporte
- ✗ **C)** Protocolo AH en modo de transporte
- ✓ **D)** Protocolo AH en modo túnel

explicación

El Protocolo de seguridad de Internet (IPSec) se puede utilizar en modo de túnel con el protocolo de encabezado de autenticación (AH) para firmar y encapsular digitalmente cada paquete enviado desde la red dentro de otro paquete. Un túnel es una construcción de comunicaciones de red que transporta paquetes encapsulados.

EL IPSec se puede utilizar en el modo de transporte con el AH para firmar y para cifrar digital los paquetes enviados entre dos host. El modo de transporte no encapsula paquetes dentro de otros paquetes. El Protocolo de seguridad encapsulador (ESP) se puede utilizar con IPSec para cifrar paquetes IPSec. ESP no se utiliza para firmar digitalmente encabezados de paquetes. ESP funciona en modo túnel y modo de transporte.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, IPSec e ISAKMP

Comprensión del modo de túnel IPSec VPN y el modo de transporte IPSec- ¿Cuál es la diferencia?, http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

---

Pregunta #48 de 131

Id. de pregunta: 1113947

¿Qué capa OSI es responsable de los servicios de archivos, impresión y mensajes?

- ✓ **A)** aplicación

✗ **B)** presentación

✗ **C)** sesión

✗ **D)** red

explicación

La capa de aplicación proporciona los protocolos necesarios para realizar los servicios de red específicos. La capa de aplicación proporciona servicios sin repudio. Por ejemplo, cuando se envía un mensaje de correo electrónico a otro usuario de la red, la capa de aplicación proporciona el Protocolo simple de transferencia de correo (SMTP) necesario para dirigir el mensaje de correo electrónico a través de la red.

Las propias aplicaciones de usuario, como Microsoft Outlook, no se encuentran en la capa de aplicación, ni tampoco otros servicios de red, como la impresión. En su lugar, las tecnologías que necesitan estas aplicaciones para acceder a los servicios de red residen en el nivel de aplicación. Los servicios de red incluyen servicios de correo electrónico, archivos, impresión, bases de datos y aplicaciones.

Algunos de los protocolos que funcionan en la capa de aplicación son SMTP, Secure Electronic Transaction (SET), HyperText Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP) y Trivial File Transfer Protocol (TFTP). El protocolo del Sistema de nombres de dominio (DNS) también funciona en esta capa.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, Aplicación

---

Pregunta #49 de 131

Id. de pregunta: 1105215

¿Qué tipo de cable es vulnerable al uso de grifos de vampiro?

✗ **A)** fibra óptica

✓ **B)** coaxial

✗ **C)** Stp

✗ **D)** Utp

explicación

El cable coaxial es vulnerable al uso de grifos de vampiros. Los grifos vampiro se colocan físicamente en el cable para permitir que los equipos no autorizados se conecten a la red. El cable coaxial consiste en un conductor cilíndrico externo hueco que rodea un solo conductor interno.

Ninguno de los otros cables de red enumerados es vulnerable al uso de grifos de vampiros. El cable UTP es susceptible a interferencias electromagnéticas (EMI) y escuchas. STP es susceptible a las escuchas. El cable de fibra óptica no es susceptible a EMI ni a las escuchas y se considera el medio de red más seguro. El cable de fibra óptica tiene una longitud utilizable efectiva mucho más larga (hasta dos kilómetros en algunos casos).

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, Coaxial

Medios de almacenamiento y redes, http://www.techexams.net/technotes/securityplus/network_storage_media.shtml

---

Pregunta #50 de 131

Id. de pregunta: 1105248

Bob administra el departamento de ventas. La mayoría de sus representantes de ventas viajan entre varios sitios de clientes. Quiere permitir que estos representantes de ventas comprueben el estado de envío de sus pedidos en línea. Esta información reside actualmente en la intranet de la empresa, pero no es accesible para nadie fuera del firewall de la empresa. Bob le ha pedido que logre esto. Decide crear una extranet para permitir que estos empleados vean el estado y el historial de pedidos de sus clientes.

¿Qué técnica podría utilizar para proteger las comunicaciones entre segmentos de red que envían datos de estado de pedidos a través de Internet?

- ✗ **A)** extranet
- ✗ **B)** Servidor de certificados
- ✓ **C)** VPN
- ✗ **D)** VLAN

explicación

Una red privada virtual (VPN) no es una red física. En una VPN, una red pública, como Internet, se utiliza para permitir la comunicación segura entre empresas que no están ubicadas juntas. Una VPN transporta datos cifrados.

Una LAN virtual (VLAN) permite segmentar las redes lógicamente sin necesidad de volver a cableado físico de la red. Un VLA N restringe la inundación solamente a esos puertos incluidos en el VLA N.

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.

Según rfc 2637, PPTP es una tecnología VPN que permite ppp para ser tunelizado a través de una red IP. Dado que la implementación de PPTP de Microsoft no incluye cifrado de forma predeterminada, cifrado punto a punto de Microsoft (MPPE) se utiliza con fines de cifrado. El PPTP utiliza un mecanismo genérico mejorado del Encapsulation de ruteo genérico (GRE) para proporcionar un servicio encapsulado flujo y congestión-controlado del datagrama para llevar los paquetes PPP. Los paquetes GRE que forman el túnel sí mismo no se protegen criptográficamente. Debido a que las negociaciones de PPP se llevan a cabo a través del túnel, puede ser posible que un atacante espiar y modificar esas negociaciones.

Al usar una VPN, una empresa evita el gasto de líneas arrendadas para una comunicación segura, pero en su lugar puede usar redes públicas para transferir datos de manera segura. Los equipos cliente pueden conectarse a la VPN mediante acceso telefónico, DSL, RDSI o módems por cable. Para garantizar la privacidad e integridad de los datos, las conexiones entre firewalls a través de redes públicas deben usar una VPN cifrada.

Una intranet es un complemento de red de área local (LAN) que está restringido a ciertos usuarios, normalmente los empleados de una empresa. Los datos contenidos en él son generalmente de naturaleza privada.

Una extranet, por otro lado, tiene un límite más amplio porque generalmente permite que dos o más empresas se comuniquen y compartan información privada.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, VPN

Pregunta #51 de 131

Id. de pregunta: 1114746

¿Qué tecnologías WAN se utilizan principalmente para permitir que los mainframes ibm se comuniquen con equipos remotos?

a. SMDS

b. SDLC

c. HDLC

d. HSSI

- ✗ **A)** opción b
- ✗ **B)** opción A
- ✗ **C)** opción c
- ✗ **D)** Sólo las opciones C y D
- ✓ **E)** Sólo opciones B y C
- ✗ **F)** Opción d
- ✗ **G)** Sólo las opciones A y B

explicación

El Control de enlace de datos sincrónico (SDLC) y el Control de enlace de datos de alto nivel (HDLC) se utilizan principalmente para permitir que los mainframes de IBM se comuniquen con equipos remotos. Un protocolo síncrono, SDLC, se utiliza sobre las redes con las conexiones permanentes. Los entornos mainframe generalmente se consideran más seguros que los entornos LAN porque hay menos puntos de entrada a un mainframe.

HDLC es una extensión de SDLC. HDLC proporciona una producción más alta que el SDLC soportando las transmisiones full-duplex. El SDLC no soporta el dúplex completo.

Switched Multimegabit Data Service (SMDS) es un protocolo de conmutación de paquetes que puede proporcionar ancho de banda según lo solicitado. Se utiliza para conectarse a través de redes públicas. Ha sido reemplazado por frame relay.

La interfaz serie de alta velocidad (HSSI) se utiliza para conectar el Routers y los multiplexores con la atmósfera, el Frame Relay, y otros servicios de alta velocidad.

Una red de área extensa (WAN) puede proporcionar acceso a segmentos de red interconectados como extranets, intranets, zonas desmilitarizadas (DMZ), red privada virtual (VPN) e Internet.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Diferencia entre HDLC y SDLC, http://www.differencebetween.com/difference-between-hdlc-and-vs-sdlc/

Pregunta #52 de 131

Id. de pregunta: 1111737

Haga coincidir cada descripción con el protocolo que mejor se adapte.

{UCMS id=5658729179512832 type=Activity}

explicación

Los protocolos deben coincidir con las descripciones de la siguiente manera:

- IPSec - Un protocolo de túnel que proporciona autenticación segura y cifrado de datos
- SNMP - Un protocolo de administración de red que permite la comunicación entre los dispositivos de red y la consola de administración
- SFTP - Un protocolo de transferencia de archivos que utiliza SSH para la seguridad
- FTPS - Un protocolo de transferencia de archivos que utiliza SSL para la seguridad

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de Red, Redes IP

Pregunta #53 de 131

Id. de pregunta: 1105242

¿Qué protocolo es un protocolo de conexión de acceso telefónico que requiere que a ambos extremos del canal de comunicación se les asigne una dirección IP?

✓ **A)** resbalar

✗ **B)** IMAP4

✗ **C)** Dlc

✗ **D)** PPP

explicación

El Protocolo de Internet de línea serie (SLIP) es un protocolo de conexión de acceso telefónico más antiguo que requiere que a ambos extremos del canal de comunicación se les asigne una dirección IP. SLIP se utilizó sobre interfaces seriales de baja velocidad.

Data Link Control (DLC) es un protocolo de conectividad que se utiliza para conectar equipos mainframe ibm con LAN y en algunos modelos anteriores, impresoras HP. Protocolo de acceso a correo de Internet versión 4 (IMAP4) es un protocolo de recuperación de correo electrónico que algunos clientes de correo electrónico utilizan para descargar mensajes de servidores de correo electrónico. DLC e IMAP4 no son protocolos de acceso telefónico.

El Protocolo punto a punto (PPP) es un protocolo de acceso telefónico más reciente con características más avanzadas que SLIP. No requiere que a ambos extremos del canal de comunicación se les asigne una dirección IP. Además, PPP admite varios protocolos de comunicaciones de red, como TCP/IP, IPX/SPX y NetBEUI.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, acceso telefónico

---

Pregunta #54 de 131

Id. de pregunta: 1113967

¿En qué tipo de ataque se interceptan los mensajes entre dos equipos?

✗ **A)** wardialing
✗ **B)** bombardeo de correo
✗ **C)** ping de la muerte
✓ **D)** hombre-en-el-medio

explicación

En un ataque de intermediario, los mensajes se interceptan entre dos equipos. El uso de firmas digitales y autenticación mutua puede ayudar a evitar este tipo de ataque.

En un ataque de bombardeo de correo, los servidores de correo electrónico y los clientes se ven abrumados por mensajes de correo electrónico no solicitados. El filtrado de correo electrónico y la retransmisión de correo electrónico pueden ayudar a evitar este tipo de ataque.

En un ataque de tutela, los hackers marcan un gran banco de números de teléfono para determinar cuál está conectado a una computadora. Mantener el número de teléfono privado e implementar un control de acceso estricto puede ayudar a prevenir este tipo de ataque.

En un ataque de ping de muerte, los paquetes ICMP de gran tamaño se envían al equipo víctima. Para evitar este tipo de ataque, debe mantenerse al día con las revisiones del sistema e implementar el filtrado de entrada.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, Man-in-the-Middle Attack

---

Pregunta #55 de 131

Id. de pregunta: 1105204

El administrador le ha pedido que mejore la seguridad de la red limitando el tráfico de datos internos confidenciales a los equipos de una subred específica mediante listas de control de acceso (ACL). ¿Dónde deben implementarse las ACL?

- ✓ **A)** Routers
- ✗ **B)** cortafuegos
- ✗ **C)** Centros
- ✗ **D)** Módems

explicación

Los ACL se deben desplegar en el Routers. Las ACL mejorarán la seguridad de la red al limitar el tráfico de datos confidenciales a los equipos de una subred específica.

Los firewalls se implementan normalmente en las interfaces de red pública. Por lo general, no están involucrados en ningún tráfico interno. Por lo tanto, las ACL de implementación en firewalls no limitarían el tráfico de datos internos confidenciales a los equipos de una subred específica. Un firewall se clasifica como un dispositivo de control de

acceso basado en reglas. Las reglas se configuran en el firewall para permitir o denegar el paso de paquetes de una red a otra.

Los concentradores se implementan normalmente para conectar hosts en una red. Los concentradores activos proporcionan regeneración de señales, mientras que los concentradores pasivos no lo hacen. Los concentradores no proporcionan la capacidad de configurar acl.

Los módems se despliegan típicamente para proporcionar las conexiones de la línea telefónica. Los módems no pueden controlar el tráfico de datos interno. Sin embargo, pueden proporcionar seguridad en la conexión de línea telefónica.

Otra respuesta válida a la pregunta que no se dio es un interruptor. Los conmutadores se implementan normalmente para crear redes de área local virtuales (VLAN). El Switch aísla el VLA N del resto de la red para proporcionar una mejor Seguridad para el VLA N. Un VLA N restringe la inundación solamente a esos puertos incluidos en el VLA N.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, Router

Mitigación de amenazas de seguridad mediante ACL, http://www.informit.com/articles/article.aspx?p=102180&seqNum=7

Pregunta #56 de 131

Id. de pregunta: 1105156

Usted necesita implementar una red inalámbrica para un cliente. Tiene dos puntos de acceso inalámbricos 802.11a, dos 802.11b y dos 802.11g.

Debe implementar tres redes inalámbricas que puedan comunicarse entre sí. ¿Qué puntos de acceso inalámbrico debe utilizar?

- ✗ **A)** Los puntos de acceso inalámbrico 802.11a y 802.11b
- ✗ **B)** Los puntos de acceso inalámbrico 802.11a y 802.11g
- ✓ **C)** Los puntos de acceso inalámbrico 802.11b y 802.11g
- ✗ **D)** Puede usarlos todos juntos.

explicación

Debe utilizar los puntos de acceso inalámbrico 802.11b y 802.11g. Estos dos estándares funcionan a la frecuencia de 2,4 GHz y se pueden utilizar indistintamente.

No puede utilizar puntos de acceso inalámbricos 802.11a con puntos de acceso inalámbricos 802.11b o 802.11g. Los puntos de acceso inalámbricos 802.11a funcionan a una frecuencia de 5 GHz. Por lo tanto, una solución que incluya 802.11a solo proporcionará dos puntos de acceso inalámbricos.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, Redes Inalámbricas

---

Pregunta #57 de 131

Id. de pregunta: 1105162

¿Qué declaración NO es verdad con respecto a la brecha del Wireless Application Protocol (WAP)?

- ✗ **A)** Los datos confidenciales se pueden capturar mientras están en la puerta de enlace.
- ✗ **B)** Ocurre cuando el gateway descifra las transmisiones WTLS y lo vuelve a cifrar con TLS/SSL.
- ✓ **C)** Ocurre cuando se implementan WAP 2.0 y anterior.
- ✗ **D)** El problema de la brecha WAP implica WTLS.

explicación

Wap Gap ocurre en las versiones de WAP antes de la versión 2.0. WTLS es substituido por TLS en WAP 2.0.

El problema de WAP Gap involucró WTLS. Ocurre cuando el gateway descifra las transmisiones WTLS y lo vuelve a cifrar con TLS/SSL. Los datos confidenciales se pueden capturar mientras están en la puerta de enlace.

El Wireless Transport Layer Security Protocol (WTLS) en la pila del Wireless Application Protocol (WAP) proporciona la Seguridad entre el cliente WAP y el gateway.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

La brecha WAP, http://sourcedaddy.com/networking/the-wap-gap.html

---

Pregunta #58 de 131

Id. de pregunta: 1111736

Haga juego las descripciones a la izquierda con las tecnologías de red a la derecha que él mejor empareja.

{UCMS id=5744477798924288 type=Activity}

explicación

Las tecnologías de red deben coincidir con las descripciones de la siguiente manera:

- DMZ - Una red que se aísla de otras redes usando un Firewall
- VLAN - Una red que se aísla de otras redes usando un Switch
- NAT : una solución de firewall transparente entre redes que permite que varios equipos internos compartan una única interfaz de Internet y dirección IP
- NAC : un servidor de red que garantiza que todos los dispositivos de red cumplan con la directiva de seguridad de una organización

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red, Canales de Comunicación Seguros

---

Pregunta #59 de 131

Id. de pregunta: 1114723

¿Qué clase de direcciones de red IP tiene un valor de entre 128 y 191 para el primer octeto?

✗ **A)** Clase A

✗ **B)** Clase D

✗ **C)** Clase C

✓ **D)** Clase B

✗ **E)** Clase E

explicación

Las direcciones de clase B van de 128 a 191 decimales, o de 10000000 a 10111111 binario. Tenga en cuenta que los tres primeros bits de una dirección de clase B siempre son 100. Las direcciones de clase B utilizan los dos primeros octetos para la dirección de red y los dos últimos octetos para la dirección de host. Con dos octetos para usar para los hosts, puede asignar las direcciones de 0.1 a 255.255 para el IDENTIFICADOR de host, que es de 00000000.000000001 a 11111111.111111111 en binario.

Los intervalos de clases de dirección se enumeran a continuación en binario y decimal:

Clase A - 00000000 - 01111111 - 0 - 126

Clase B - 10000000 - 10111111 - 128 - 191

Clase C - 11000000 - 11011111 - 192 - 223

Clase D - 11100000 - 11101111 - 224 - 239

Clase E - 11110000 - 11110111 - 240 - 255

Tenga en cuenta que la dirección de red 127 se utiliza para el bucle invertido.

Observe que el bit más significativo, que es el bit más a la izquierda, es un cero para todas las direcciones de clase A. Para las direcciones de clase B, el cero se desplaza al lugar correcto, lo que significa que los dos bits más significativos en todas las direcciones de clase B son 10. El cero cambia de nuevo para la clase C, lo que significa que los tres bits más significativos en todas las direcciones de clase C son 110. Este "cambio" continúa para la Clase D y la Clase E. Conocer este patrón le permite determinar la clase de una dirección IP binaria simplemente mirando los bits más significativos.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPv4

Calculadoras de red, http://www.subnetmask.info/

Pregunta #60 de 131

Id. de pregunta: 1113966

¿Qué debe utilizar para conectar un equipo a una red Fast Ethernet 100BaseTX?

✗ **A)** Utilice un cable RG-58 con un conector BNC.

✗ **B)** Utilice un cable de fibra óptica con un conector SC.

✗ **C)** Utilice un cable de fibra óptica con un conector ST.

✓ **D)** Utilice un cable UTP CAT5 con un conector RJ-45.

✗ **E)** Utilice un cable UTP CAT5 con un conector RJ-11.

explicación

Entre las opciones disponibles, debe utilizar el cable de par trenzado sin blindes de categoría 5 (CAT5 UTP) y los conectores RJ-45 para conectar un ordenador a una red Ethernet 100BaseTX. En una red 100BaseTX, usted puede utilizar dos pares de cable cat5 UTP o del tipo 1 blindado del par trenzado (STP). Los conectores RJ-45 normalmente conectan equipos a una red 100BaseTX. Aunque un conector RJ-45 es similar en apariencia a un conector telefónico RJ-11 estándar, un conector RJ-45 es más ancho que un conector RJ-11. Además, un conector RJ-45 admite ocho cables, mientras que un conector RJ-11 admite hasta seis cables.

El cable coaxial RG-58 y los conectores BNC, incluidos los conectores de barril BNC y los conectores BNC T, se utilizan en redes Ethernet 10Base2. Las resistencias de terminación BNC también son necesarias en ambos extremos del bus 10Base2 para evitar que las señales reboten en el cable y corrompan los datos. Algunas implementaciones coaxiales requieren un espaciado fijo entre las conexiones; el cableado de par trenzado no tiene tales requisitos.

El cable de fibra óptica, como el cable multimodo 62.5/125 y el cable monomodo 8/125, se utiliza en algunos tipos de redes Ethernet, como las redes Ethernet 10BaseFB y 100BaseFX Fast Ethernet. Los cables de fibra óptica utilizan conectores LC, SC y ST. El cable de fibra óptica tiene tres elementos físicos básicos: el núcleo, el revestimiento y la chaqueta. El núcleo es el medio de transmisión más interno, generalmente hecho de vidrio o plástico. La siguiente capa exterior, el revestimiento, también está hecha de vidrio o plástico con propiedades diferentes a las del revestimiento, y ayuda a reflejar la luz de nuevo en el núcleo. La capa más externa, la chaqueta, proporciona protección contra el calor, la humedad y otros elementos ambientales.

Los cables CAT1, CAT3, CAT5, CAT5e y CAT6 son tecnologías de par trenzado.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de Red, Par Trenzado

Pregunta #61 de 131

Id. de pregunta: 1105221

¿Qué condición pudo indicar que una red está experimentando un ataque DoS?

✗ **A)** una ligera disminución del tráfico de red

✗ **B)** un ligero aumento en el tráfico de red

✗ **C)** una disminución significativa del tráfico de red

✓ **D)** un aumento significativo del tráfico de red

explicación

Un aumento significativo en el tráfico de red podría indicar que una red está experimentando un ataque de denegación de servicio (DoS), que se produce cuando un pirata informático inunda una red con solicitudes.

Un ataque DoS impide que los usuarios autorizados tengan acceso a los recursos que están autorizados a usar. Un ejemplo de un ataque DoS es uno que hace caer un sitio Web de comercio electrónico para evitar o denegar el uso a clientes legítimos.

Una disminución significativa en el tráfico podría indicar un problema con la conectividad de red o el hardware de red, o podría indicar un ataque de pirata informático no DoS. Las redes con niveles de tráfico ligeramente fluctuantes probablemente estén funcionando normalmente.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, DoS

Descripción de los ataques de denegación de servicio, https://www.us-cert.gov/ncas/tips/ST04-015

Pregunta #62 de 131

Id. de pregunta: 1114736

Necesita resolver un problema de tráfico que se produce en una red Ethernet grande. Dentro de este gran segmento, el departamento de contabilidad está inundando la red con un alto volumen de datos, lo que hace que toda la red se ralentice.

¿Qué dispositivo es una solución rápida y de bajo costo para aislar al departamento de contabilidad?

✗ **A)** entrada

✗ **B)** enrutador

✓ **C)** puente

✗ **D)** repetidor

explicación

Un puente proporciona una solución rápida y de bajo costo para dividir una red en diferentes segmentos con el fin de reducir el tráfico de red. Los Puentes funcionan construyendo tablas de reenvío basadas en direcciones MAC. Estas tablas de reenvío permiten que los Bridges determinen qué paquetes necesitan pasar a través del Bridge a otro segmento contra qué paquetes deben permanecer en el segmento local. Los puentes tienen la capacidad de actuar como un dispositivo de almacenamiento y reenvío mediante el almacenamiento de tramas. Entre las propiedades de los puentes se incluyen las siguientes:

Reenvía los datos a todos los demás segmentos si el destino no está en el segmento local

Funciona en la capa 2, la capa de enlace de datos

Puede crear una tormenta de difusión

En este escenario, el departamento de contabilidad está compartiendo actualmente el ancho de banda de todo el segmento. El uso de un puente para colocar este departamento en su propio segmento significa que el tráfico de este segmento permanecerá en el segmento local, reduciendo así el tráfico general de la red. Solamente los paquetes destinados para otros segmentos pasarán a través del Bridge.

Un puente no es una opción óptima para reducir el tráfico intersegment. En tal caso, un router o una puerta de enlace sería una mejor opción.

Un enrutador se utiliza para conectar redes que son diferentes en topología o dirección de protocolo de Internet (IP). Podría usarse en este escenario, pero no sería una solución de bajo costo. Los enrutadores pueden ser bastante costosos de implementar. Por lo general, debe evitar el uso de dos enrutadores para conectar la red interna a una zona desmilitarizada (DMZ) porque, a continuación, proporciona varias rutas de acceso para el ataque (a veces denominado una superficie de ataque mayor).

Una puerta de enlace se utiliza para conectar redes que utilizan protocolos diferentes.

Un repetidor se utiliza para extender la longitud de la red más allá de la distancia máxima del segmento del cable. Toma la señal de una trama recibida y la regenera a el resto de los puertos en el repetidor.

Un tipo especial de enrutador, llamado enrutador de detección, funciona como un firewall de filtrado de paquetes basado en los números de puerto.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, Puente

---

Pregunta #63 de 131

Id. de pregunta: 1105214

¿Qué dispositivo convierte los mensajes entre dos aplicaciones de correo electrónico (correo electrónico) diferentes?

- ✗ **A)** traductor de correo electrónico
- ✗ **B)** servidor de correo electrónico
- ✓ **C)** gateway de correo electrónico
- ✗ **D)** conmutador de correo electrónico

explicación

Una puerta de enlace de correo electrónico convierte los mensajes entre dos aplicaciones de correo electrónico diferentes, por ejemplo, entre un servidor de Exchange y un servidor de Sendmail. Esto se logra mediante el uso del servicio Common Data Network denominado servicio de correo.

Un servidor de correo electrónico es el servidor real de la empresa que administra las transmisiones de correo electrónico de una organización, tanto entrantes como salientes. Se mantiene un directorio de correo electrónico para cada usuario de correo electrónico. Este directorio contendrá los correos electrónicos enviados y recibidos por el usuario, así como borradores de documentos, copias de documentos y documentos temporales.

Las otras dos opciones son dispositivos no válidos.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, Puerta de enlace

---

Pregunta #64 de 131

Id. de pregunta: 1113965

Está diseñando una red Ethernet. La especificación Ethernet que seleccione para la red debe admitir una velocidad de transmisión de datos de 100 megabits por segundo (Mbps) y una longitud máxima de segmento de cable de 2.000 metros (m). El cable utilizado en la especificación Ethernet que seleccione también debe ser inmune a la diafonía.

¿Qué especificación ethernet debe utilizar en la red?

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

explicación

De las especificaciones ethernet proporcionadas, debe utilizar la especificación 100BaseFX en la red. La especificación Ethernet 100BaseFX utiliza cable de fibra óptica, que es inmune a la diafonía, interferencia electromagnética (EMI) y tapping porque el cable de fibra óptica transmite luz en un cable de vidrio o plástico en lugar de transmitir electricidad en un cable de cobre.

La diafonía es la interferencia electromagnética que puede ocurrir entre los cables de cobre que están muy cerca. La diafonía puede ocurrir en cables de par trenzado sin blindaje (UTP), cables de par trenzado blindado (STP), cables coaxiales y otros tipos de cable que utilizan cable de cobre. La especificación Ethernet 100BaseFX admite una velocidad de transmisión de datos de 100 Mbps y una longitud máxima de segmento de cable de 2.000 m.

La especificación Ethernet 10Base2 utiliza el cable coaxial RG-58. La especificación Ethernet 10Base2 admite una velocidad de transmisión de datos de 10 Mbps y una longitud máxima de segmento de cable de 185 m. La especificación Ethernet 10BaseT admite una velocidad de transmisión de datos de 10 Mbps y una longitud máxima de segmento de cable de 100 m. La especificación 10BaseT requiere un cable UTP. La especificación Ethernet 100BaseTX es una versión de Fast Ethernet a través de cable UTP de categoría 5 (CAT5) o cable STP de tipo 1. La especificación Fast Ethernet 100BaseTX admite una velocidad de transmisión de datos de 100 Mbps y una longitud máxima de segmento de cable de 100 m.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, Fibra óptica

Pregunta #65 de 131

Id. de pregunta: 1105137

¿Qué capa del modelo TCP/IP corresponde a la capa de transporte del modelo OSI?

- ✗ **A)** Internet
- ✓ **B)** transporte
- ✗ **C)** Acceso a la red
- ✗ **D)** aplicación

explicación

La capa de transporte del modelo TCP/IP corresponde a la capa de transporte del modelo OSI.

La capa de aplicación del modelo TCP/IP corresponde a las capas Aplicación, Presentación y Sesión del modelo OSI.

La capa de Internet del modo TCP/IP corresponde a la capa de red del modelo OSI. El protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP) funcionan en el nivel de Internet.

La capa de acceso a la red del modelo TCP/IP corresponde a las capas De enlace de datos y Física del modelo OSI.

El modelo OSI tiene siete capas; el modelo TCP/IP tiene cuatro capas.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, modelo TCP/IP

Pregunta #66 de 131

Id. de pregunta: 1113975

Ha implementado un módem para permitir que los usuarios remotos se conecten a la red. Debe asegurarse de que solo los usuarios de ubicaciones específicas puedan acceder a su red mediante el módem. ¿Qué debe implementar?

- ✗ **A)** radio
- ✗ **B)** NAT
- ✗ **C)** TACACS
- ✓ **D)** Callback

explicación

Debe implementar la devolución de llamada. La devolución de llamada se asegurará de que sólo los usuarios de ubicaciones específicas puedan acceder a su red mediante el módem. La característica configura el módem para desconectarse del usuario una vez que se ha producido la autenticación y para devolver la llamada al usuario en un número predefinido.

El Servicio de autenticación remota telefónica de usuario (RADIUS) es un servicio que realiza la autenticación y las cuentas de usuario remoto. La implementación de un servidor RADIUS no garantiza que sólo los usuarios de ubicaciones específicas puedan acceder a la red mediante el módem. El sistema de control de acceso del controlador de acceso de terminal (TACACS) es una tecnología similar al RADIUS.

La traducción de direcciones de red (NAT) proporciona una solución de firewall transparente entre una red interna y redes externas. Con NAT, varios equipos internos pueden compartir una única interfaz de Internet y una dirección IP. El propósito principal de NAT es ocultar los hosts internos de la red pública. NAT no garantiza que sólo los usuarios de ubicaciones específicas puedan acceder a la red mediante el módem.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Devolución de llamada, http://technet.microsoft.com/en-us/library/cc784461.aspx

---

Pregunta #67 de 131

Id. de pregunta: 1114725

¿Qué tecnología WLAN admite un máximo de transmisión de datos de 11 Mbps?

- ✓ **A)** 802.11b
- ✗ **B)** 802.11e
- ✗ **C)** 802,11 g
- ✗ **D)** 802.11a

explicación

La tecnología de red de área local inalámbrica (WLAN) 802.11b admite velocidades de datos máximas de 11 Mbps.

Los clientes de la red inalámbrica (WLAN) del 802.11b, los Puntos de acceso, y los Bridges utilizan el espectro separado de la secuencia directa (DSSS) para la transmisión a través de los puertos RF. La transmisión radioeléctrica DSSS proporciona velocidades de datos entre 1 Mbps y 11 Mbps. El DSSS utiliza tres tipos de esquemas de modulación para la modulación radioeléctrica:

Binary Phase Shift Keying (BPSK) para transmitir velocidades de datos a 1 Mbps.

Quadrature Phase Shift Keying (QPSK) para transmitir velocidades de datos a 2 Mbps.

Complementary Code Keying (CCK) para transmitir velocidades de datos a 5,5 Mbps y 11 Mbps.

Las redes inalámbricas (WLAN) 802.11a trabajan en la banda de frecuencia industrial, científica y médica (ISM) de 5 GHz con multiplexación por división de frecuencia ortogonal (MDFO). OFDM admite una velocidad de datos máxima de 54 Mbps.

802.11e proporciona calidad de servicio (QoS) y soporte para el tráfico multimedia. Esta implementación utiliza las bandas de 2,4 GHz (lo mismo que 802.11b) o 5,8 GHz (lo mismo que 802.11a). Por lo tanto, puede funcionar a 11 Mbps o 54 Mbps.

802.11f proporciona capacidades de itinerancia para redes inalámbricas a 54 Mbps.

802.11g es una extensión de 802.11b. 802.11g aumenta la capacidad de velocidad a 54 Mbps.

802.11h es una extensión de 802.11a. 802.11h añade capacidad europea al estándar 802.11a.

802.11i agrega el protocolo de red segura robusta (RSN) para aumentar la seguridad de las redes inalámbricas.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, 802.11b

LAN inalámbricas: Ampliación del alcance de una LAN, http://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=2

Pregunta #68 de 131

Id. de pregunta: 1105229

Ha descubierto que el servidor de archivos de su organización se ha visto abrumado por los paquetes de difusión UDP, lo que ha provocado un bloqueo del servidor. ¿Qué ataque se ha producido?

✗ **A)** pitufo

✓ **B)** fraggle

✗ **C)** lágrima

✗ **D)** ping de la muerte

explicación

Se ha producido un ataque de fraggle. Un ataque de fragmentación ahoga los recursos de procesamiento del host víctima al inundar la red con paquetes UDP falsificados. Fraggle es un ataque de denegación de servicio (DoS) que envía grandes cantidades de paquetes UDP de difusión falsificados a direcciones de difusión IP. Esto hace que el host de destino se inunde con respuestas de eco de toda la red, lo que hace que el sistema se congele o se bloquee.

Un ataque pitufo es similar a un ataque fraggle, pero suplanta la dirección IP de origen en un paquete de difusión ICMP ECHO en lugar de en paquetes UDP. Pitufo es un ataque DoS que utiliza mensajes de ping de difusión falsificados para inundar un sistema de destino. En un ataque de este tipo, el atacante envía una gran cantidad de paquetes de eco ICMP con una dirección IP de origen falsificada similar a la del host de destino a direcciones de difusión IP. Esto hace que el host de destino se inunde con respuestas de eco de toda la red, lo que hace que el sistema se congele o se bloquee. Otros ejemplos de ataques DoS son SYN Flood, Bonk y Ping de ataques de muerte.

En un ataque teardrop, el atacante utiliza una serie de paquetes fragmentados IP, haciendo que el sistema se congele o se bloquee mientras los paquetes están siendo vueltos a montar por el host víctima. Un ataque teardrop se basa principalmente en la implementación de fragmentación de IP. Para volver a montar los fragmentos en el paquete original en el destino, el host comprueba los paquetes entrantes para asegurarse de que pertenecen al mismo paquete original. Los paquetes están mal formados. Por lo tanto, el proceso de volver a ensamblar los paquetes hace que el sistema se congele o se bloquee.

Un ping de muerte es otro tipo de ataque DoS que implica inundar el equipo de destino con paquetes de gran tamaño, superando el tamaño aceptable durante el proceso de reensamblaje y haciendo que el equipo de destino se congele o se bloquee. Otros ataques de denegación de servicio son pitufo y fraggle.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Red Fraggle

---

Pregunta #69 de 131

Id. de pregunta: 1114724

¿Qué notación es el prefijo de red que se utiliza para denotar una dirección IP de clase C sin subnetefacción?

✗ **A)** /16

✗ **B)** /8

✗ **C)** /32

✓ **D)** /24

explicación

El prefijo de red /24 se utiliza para denotar una dirección IP de clase C no subneteada. Las direcciones IP basadas en clases fueron los primeros tipos de direcciones asignadas en Internet. El primer octeto de una dirección IP de clase A es de 1 a 126 en notación decimal; el primer octeto de una dirección IP de clase A es la dirección de red. El primer octeto de una dirección IP de Clase B es de 128 a 191 en notación decimal; los dos primeros octetos de una dirección IP de clase B son la dirección de red. El primer octeto de una dirección IP de clase C es de 191 a 223; los tres primeros octetos de una dirección IP de clase C son la dirección de red.

La creación de subredes se introdujo para permitir un uso más eficiente del espacio de direcciones IP. En las subredes, algunos bits de host de una dirección IP basada en clases se utilizan como bits de dirección de red para permitir la creación de agrupaciones más pequeñas de direcciones IP que las agrupaciones ofrecidas por las direcciones IP basadas en clases. Por ejemplo, tiene una oficina con 200 equipos que residen en cuatro redes independientes que consta de 50 equipos cada uno. Si a cada red se le ha asignado su propio intervalo de direcciones IP de clase C, no se utilizarán 204 direcciones IP en cada intervalo, para un total de 816 direcciones IP desperdiciadas. Con la creación de subredes, un único intervalo de direcciones IP de clase C puede proporcionar direcciones IP para los hosts de las cuatro redes. Si ha subredes de un único intervalo de direcciones IP de clase C, solo se desperdiciarán 48 direcciones IP.

Antes de que se introdujera el enrutamiento de interdominios sin clases (CIDR), las redes se organizaban comúnmente por clases. En una dirección de clase C, los dos primeros bits de la dirección se establecen en uno y el tercer bit de la dirección se establece en cero.

Una máscara de subred es un número binario de 32 bits que se puede comparar con una dirección IP para determinar qué parte de la dirección IP es la dirección de host y qué parte de la dirección IP es la dirección de red. Cada 1 bit en una máscara de subred indica un bit en la dirección de red y cada 0 bit en la máscara de subred indica un bit en la dirección del host. Por ejemplo, en una red que utiliza un intervalo de direcciones IP de clase C sin subnetted, la dirección IP 192.168.0.1 tiene una máscara de subred de 255.255.255.0. En notación binaria, 255 se representa como 11111111. En notación binaria, la máscara de subred 255.255.255.0 se representa como 11111111 11111111 11111111 00000000. La representación binaria de la dirección IP 192.168.0.1 es 11000000 10101000 000000000 00000001. La siguiente es una comparación de la máscara de subred binaria y la dirección IP binaria:

11111111 11111111 11111111 00000000 Máscara de subred

11000000 10101000 000000000 00000001 dirección IP

De esta comparación, usted puede ver que los primeros 24 bits de la dirección IP, o 192.168.0 en notación decimal, son la dirección de red y los ocho bits pasados de la dirección IP, o 1 en notación decimal, son la dirección del host.

Otro método, denominado prefijo de red, también se utiliza para determinar qué parte de una dirección IP es la dirección de red y qué parte de una dirección IP es la dirección de host. El método de prefijo de red anexa un carácter de barra diagonal (/) y un número después de la dirección IP, como en el ejemplo siguiente:

192.168.0.1/24

En este ejemplo, el prefijo de red indica que los primeros 24 bits de la dirección IP, o 192.168.0 en notación decimal, son la dirección de red y los últimos 8 bits de la dirección IP son la dirección de host. Esto a veces se conoce como notación CIDR.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, IPv4

Calculadoras de red, http://www.subnetmask.info/

Pregunta #70 de 131

Id. de pregunta: 1113952

¿Qué capa del modelo OSI también se conoce como Capa 4?

- ✗ **A)** la capa Presentation
- ✗ **B)** la capa de red
- ✗ **C)** la capa Session
- ✓ **D)** la capa de transporte

explicación

La capa de transporte del modelo de interconexión de sistemas abiertos (OSI) también se conoce como capa 4. La capa de transporte del modelo OSI es responsable de las comunicaciones orientadas a la conexión o sin conexión. Los protocolos de comunicaciones orientados a la conexión, como el Protocolo de control de transmisión (TCP) en el conjunto de protocolos TCP/IP, establecen una conexión virtual entre el host de envío y el host receptor para proporcionar una entrega de datos fiable y sin errores. Los protocolos sin conexión, como UDP, no proporcionan el mismo servicio garantizado, pero crean menos sobrecarga. Aunque ambos tipos de protocolos de transporte funcionan

en este nivel, muchos gráficos etiquetan esta capa como orientada a la conexión, ya que esta es la única capa donde se produce el transporte orientado a la conexión.

Algunos de los protocolos que funcionan en la capa de transporte son TCP, protocolo de datagramas de usuario (UDP) e intercambio de paquetes secuenciados (SPX). Capa de sockets seguros (SSL) se compone de dos protocolos: uno funciona en la capa de sesión y el otro funciona en la capa de transporte. SSL se considera un protocolo de capa de transporte.

La capa de transporte no proporciona confidencialidad, pero las capas de presentación, red y sesión sí. La capa de transporte administra la velocidad de control de las transferencias de paquetes. Proporciona servicios de extremo a extremo.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, Transporte

---

Pregunta #71 de 131

Id. de pregunta: 1105258

Recientemente, su organización se ha vuelto cada vez más preocupada por los hackers. Se le ha encomendado específicamente la tarea de prevenir los ataques man-in-the-middle. ¿Qué protocolo NO es capaz de prevenir este tipo de ataque?

✗ **A)** Protocolo de seguridad de Internet (IPSec)
✓ **B)** Shell remoto (rsh)
✗ **C)** HTTP seguro (HTTPS)
✗ **D)** Shell seguro (SSH)

explicación

El protocolo de shell remoto (rsh) NO es capaz de prevenir ataques man-in-the-middle (MITM). El protocolo de shell remoto (rsh) se utiliza para iniciar sesión en equipos remotos y puede ser fácilmente explotado por un ataque de tipo "Man in the middle" porque no proporciona cifrado ni autenticación de datos. En un ataque de tipo "Man in the middle", un intruso captura el tráfico de una conexión establecida para interceptar los mensajes que se intercambian entre el remitente y el receptor. El protocolo rsh no proporciona seguridad porque el tráfico fluye en texto no cifrado y no en texto cifrado.

Secure shell (SSH) proporciona seguridad mediante la autenticación antes del intercambio de claves secretas. SSH también se conoce como telnet cifrado porque proporciona cifrado del tráfico intercambiado entre el remitente y el receptor. Debido a que SSH utiliza cifrado, SSH puede prevenir ataques de tipo "Man in the middle" mejor que rsh.

HTTP Seguro (HTTPS) se basa en el protocolo secure socket layer (SSL). SSL es un protocolo de dos capas que contiene el protocolo de registro SSL y el protocolo de protocolo de enlace SSL. El protocolo de enlace SSL proporciona un mecanismo de autenticación antes del intercambio de credenciales y evita ataques, como ataques de tipo "Man in the middle", y usa certificados para validar las identidades de ambas partes. HTTPS se utiliza para las transacciones en línea.

El protocolo de seguridad de Internet (IPSec) es un marco de seguridad establecido para proteger la comunicación a través de redes inseguras, como Internet. IPSec implementa un intercambio de claves de Internet (IKE) para el intercambio de claves y la administración. IKE administra la primera fase del acuerdo de negociación de claves y el intercambio seguro de claves como parte del marco IPSec. IPSec evita los ataques de tipo "Man in the middle" mediante el cifrado y la autenticación.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, inicio de sesión remoto (rlogin), shell remoto (rsh), copia remota (rcp)

Pregunta #72 de 131

Id. de pregunta: 1105173

¿Qué tipo de firewall afecta más negativamente al rendimiento de la red?

- ✗ **A)** firewall con estado
- ✗ **B)** firewall proxy a nivel de circuito
- ✓ **C)** firewall proxy de nivel de aplicación
- ✗ **D)** firewall de filtrado de paquetes

explicación

Un firewall proxy de nivel de aplicación afecta de forma más perjudicial al rendimiento de la red porque requiere más procesamiento por paquete.

El firewall de filtrado de paquetes proporciona un alto rendimiento. Los firewalls proxy con estado y a nivel de circuito, aunque más lentos que los firewalls de filtrado de paquetes, ofrecen un mejor rendimiento que los firewalls de nivel de aplicación.

Los firewalls proxy del kernel ofrecen un mejor rendimiento que los firewalls de nivel de aplicación.

Un firewall de nivel de aplicación crea un circuito virtual entre los clientes de firewall. Cada protocolo tiene su propia parte dedicada del firewall que sólo se ocupa de cómo filtrar correctamente los datos de ese protocolo. A diferencia de un firewall de nivel de circuito, un firewall de nivel de aplicación no examina la dirección IP y el puerto del paquete de datos. A menudo, estos tipos de firewalls se implementan como un servidor proxy.

Un firewall basado en proxy proporciona un mayor aislamiento de red que un firewall con estado. Un firewall con estado proporciona un mayor rendimiento que un firewall basado en proxy. Además, un firewall con estado proporciona alguna configuración de reglas dinámicas con el uso de la tabla de estado.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #73 de 131

Id. de pregunta: 1105158

Sospecha que un equipo cliente de Windows en la red se ha visto comprometida. Debe ver la información de la dirección IP del equipo. ¿Qué herramienta debe utilizar?

✗ **A)** Señal
✗ **B)** tracert
✗ **C)** netstat
✓ **D)** ipconfig

explicación

Debe utilizar la herramienta ipconfig para ver la información de dirección IP de un equipo Con Windows. Esta herramienta muestra la dirección IP, la máscara de subred y la puerta de enlace predeterminada de un equipo. También se puede utilizar para liberar y renovar una concesión de dirección IP del Protocolo de host de configuración dinámica (DHCP).

La herramienta ping se utiliza para probar la disponibilidad de un equipo a través de una red. Puede hacer ping a los equipos en función de su nombre de host DNS o dirección IP.

La herramienta tracert se utiliza para determinar la ruta que toma un paquete a través de una red IP de Windows. Los equipos UNIX tienen una herramienta similar llamada traceroute.

La herramienta netstat muestra las conexiones de red entrantes y salientes, las tablas de enrutamiento y las estadísticas de la interfaz de red.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

La sintaxis y las opciones para utilizar la utilidad de diagnóstico ipconfig para conexiones de red, https://technet.microsoft.com/en-us/library/cc940124.aspx

---

Pregunta #74 de 131

Id. de pregunta: 1105174

¿Qué tipo de firewall sólo examina la información del encabezado del paquete?

- ✗ **A)** firewall con estado
- ✗ **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

Pregunta #77 de 131

Id. de pregunta: 1113945

Haga juego el protocolo de la izquierda con el puerto predeterminado que utiliza a la derecha. Mueva los elementos correctos de la columna izquierda a la columna de la derecha para que coincida con el protocolo con el puerto predeterminado correcto.

{UCMS id=5752530594168832 type=Activity}

explicación

Los protocolos dados utilizan estos puertos predeterminados:

- Puerto 20 - FTP
- Puerto 23 - Telnet
- Puerto 25 : SMTP
- Puerto 53 : DNS
- Puerto 80 - HTTP

FTP también utiliza el puerto 21, pero no se ha enumerado en este escenario.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de Red, Redes IP

Pregunta #78 de 131

Id. de pregunta: 1114735

¿Qué categoría de par trenzado sin blindes (UTP) consta de cuatro pares trenzados de cable de cobre y está certificada para velocidades de transmisión de hasta 100 Mbps?

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

explicación

El cableado UTP de categoría 5 es la categoría más utilizada de cable UTP. Permite velocidades de transmisión de hasta 100 Mbps, y es la categoría más alta de cableado UTP.

Las tasas de transmisión UTP son las siguientes:

Categoría 1 - hasta 4 Mbps

Categoría 2 - hasta 4 Mbps

Categoría 3 - hasta 10 Mbps

Categoría 4 - hasta 16 Mbps

Categoría 5 - hasta 100 Mbps

Categoría 5e - hasta 1000 Mbps (1 Gbps)

Categoría 6 - hasta 1000 Mbps (1 Gbps)

Categoría 6e - hasta 1000 Mbps (1 Gbps)

Categoría 7 - hasta 10 Gbps

El cableado de categoría 1 consiste en dos pares de alambre de cobre trenzado. Está clasificado para el grado de voz, no la comunicación de datos. Es el cableado UTP más antiguo y se utiliza para la comunicación en la red telefónica conmutada (RTC).

El cableado de categoría 2 consta de cuatro pares de cable de cobre trenzado y es adecuado para comunicaciones de datos de hasta 4 Mbps.

El cableado de categoría 3 consiste en cuatro pares de alambre de cobre trenzado con tres giros por pie. Es adecuado para la comunicación de datos de 10 Mbps. Ha sido el estándar UTP más utilizado desde mediados de la década de 1980, especialmente para redes Ethernet.

El cableado de categoría 4 consta de cuatro pares de cable de cobre trenzado y está clasificado para 16 Mbps. Fue diseñado con redes Token Ring de 16 Mbps en mente.

El cableado de categoría 5 consiste en cuatro pares trenzados de cable de cobre terminados por conectores RJ-45. El cableado de categoría 5 puede admitir frecuencias de hasta 100 MHz y velocidades de hasta 100 Mbps. Se puede utilizar para atm, token ring, 1000Base-T, 100Base-T, y redes 10Base-T.

NOTA: El cable de categoría 5e es el cable más utilizado para las nuevas implementaciones de UTP. La "e" en el cable de categoría 5e significa "mejorado". Esta especificación mejorada admitirá anchos de banda de hasta 350 MHz.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red. Par trenzado

Transmisión de datos - Cableado, http://en.kioskea.net/contents/transmission/transcabl.php3

Pregunta #79 de 131

Id. de pregunta: 1114719

¿Qué proceso OSI garantiza que cada capa OSI en el remitente agregue su propia información al paquete y cada capa OSI en el receptor elimine su información correspondiente?

✗ **A)** negociación

✓ **B)** encapsulación

✗ **C)** compresión

✗ **D)** encriptación

explicación

La encapsulación es el proceso OSI que garantiza que cada capa OSI en el remitente agregue su propia información a los paquetes y cada capa OSI en el receptor elimine su información correspondiente. La encapsulación ajusta los datos de una capa alrededor de un paquete de datos de una capa contigua.

La negociación es el proceso mediante el cual se negocia el canal de comunicación. Esto solo ocurre en la capa Session del modelo OSI.

La compresión es el proceso mediante el cual los datos se comprimen en un formato más pequeño para mejorar el tiempo de transmisión. Esto solo ocurre en la capa presentation del modelo OSI.

El cifrado es el proceso mediante el cual los datos se cifran para garantizar la confidencialidad. Esto solo ocurre en la capa presentation del modelo OSI. Las capas Red, Vínculo de datos y Transporte admiten el cifrado.

El modelo OSI está definido por siete capas de protocolo. Su propósito principal es proporcionar un modelo estándar para la comunicación de red para permitir que las redes disímiles se comuniquen. Las siete capas son las siguientes:

Capa 1 Capa física (la más alejada del usuario)

Capa de enlace de datos de capa 2

Capa 3 Capa de red

Capa de transporte de capa 4

Capa de sesión de capa 5

Capa de presentación de capa 6

Capa de aplicación de capa 7 (la más cercana al usuario)

OSI proporciona servicios de autenticación, confidencialidad, registro, aplicación, compresión, cifrado, comunicación, transmisión, direccionamiento y monitoreo. Incluye estándares de técnicas de seguridad, estándares de seguridad de capas, estándares de protocolo y estándares específicos de la aplicación.

Los sistemas que se basan en el marco OSI se consideran sistemas abiertos porque se construyen con protocolos y estándares internacionalmente aceptados para comunicarse fácilmente con otros sistemas.

Objetivo:

Comunicación y seguridad de la red

Subobsecución:

Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, encapsulación y deencapsulación

---

Pregunta #80 de 131

Id. de pregunta: 1114741

Va a implementar una red privada virtual (VPN) para usuarios remotos. Ha decidido implementar la puerta de enlace de VPN en su propia zona desmilitarizada (DMZ) detrás del firewall externo.

¿Cuáles son las ventajas de esta implementación?

un. El firewall puede proteger la puerta de enlace de VPN.

B. El firewall puede inspeccionar el texto sin formato de la VPN.

c. El firewall puede inspeccionar todas las comunicaciones de la VPN.

d. El firewall necesitará rutas especiales a la puerta de enlace de VPN configurada.

- ✗ **A)** Sólo opciones B y C
- ✗ **B)** Opción d
- ✗ **C)** opción A
- ✗ **D)** opción c
- ✗ **E)** opción b
- ✗ **F)** Sólo las opciones C y D
- ✓ **G)** Sólo las opciones A y B

explicación

Al implementar una puerta de enlace de VPN en su propia dmz detrás del firewall externo, recibirá las siguientes ventajas:

El firewall puede proteger la puerta de enlace de VPN.

El firewall puede inspeccionar el texto sin formato de la VPN.

La conectividad a Internet no depende de la puerta de enlace de VPN.

En esta implementación, se experimentan los siguientes inconvenientes:

El firewall necesitará rutas especiales a la puerta de enlace de VPN configurada.

El soporte de cliente de itinerancia es difícil de lograr.

Un firewall SOLO puede inspeccionar y registrar texto sin formato de la VPN. No puede inspeccionar todas las comunicaciones porque la mayor parte de la comunicación se cifrará. Un firewall no puede inspeccionar el tráfico cifrado.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

Registre las sesiones de puerta de enlace de VPN SSL de acceso remoto seguro > proteger la red interna, http://www.petri.co.il/record-secure-remote-access-ssl-vpn-gateway-sessions.htm

---

Pregunta #81 de 131

Id. de pregunta: 1105249

¿Cuál es otro término usado para el servicio telefónico viejo llano (POTS)?

- ✗ **A)** IPSec
- ✗ **B)** Im
- ✗ **C)** VoIP
- ✓ **D)** Pstn

explicación

La red telefónica conmutada pública (RTC) es otro término utilizado para POTS. Esta es la red de voz de conmutación de circuitos estándar utilizada para la mayoría de los teléfonos públicos en los Estados Unidos.

La voz sobre IP (VoIP) es una tecnología que permite que las transmisiones de voz viajen a través de una red IP.

El protocolo de seguridad de Internet (IPSec) es un protocolo de seguridad utilizado en redes IP.

La mensajería instantánea (MI) es un mecanismo de chat basado en texto que permite que los mensajes de texto se transmitan a través de redes.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, PSTN (POTS, PBX)

Pregunta #82 de 131

Id. de pregunta: 1105189

Un cliente se pone en contacto con usted en relación con un problema de servidor de correo electrónico. Al investigar el problema, observa que hay un número extremadamente grande de mensajes de correo electrónico en la carpeta saliente. Esto ha hecho que el disco duro se llene. Detener temporalmente el servidor de correo electrónico, eliminar los mensajes de correo electrónico y reinicie el servidor de correo electrónico. Inmediatamente, la carpeta de correo saliente comienza a llenarse de nuevo.

¿Qué está causando el problema que está experimentando?

- ✗ **A)** ataque zombie
- ✗ **B)** infección por virus
- ✓ **C)** Retransmisión SMTP
- ✗ **D)** Infección por caballo de Troya

explicación

El problema está causado por la retransmisión SMTP. Hasta que deshabilite la retransmisión SMTP en el servidor de correo electrónico, la carpeta de correo saliente seguirá llenándose.

Ninguno de los otros problemas haría que la carpeta de correo saliente se llenara inmediatamente.

Los zombis son programas controlados por control remoto que los hackers pueden utilizar para atacar redes. Los zombis a menudo están programados para hacer que un ataque de hackers parezca como si se originó en un equipo diferente.

Un caballo de Troya es un malware que se disfraza como una utilidad útil, pero contiene código malicioso incrustado. Cuando se ejecuta la utilidad disfrazada, el caballo de Troya realiza actividades maliciosas en segundo plano y proporciona una utilidad útil en el front-end. Los caballos de Troya utilizan canales encubiertos para realizar actividades maliciosas, como eliminar archivos del sistema y plantar una puerta trasera en un sistema.

Un virus es un software malicioso (malware) que se basa en otros programas de aplicación para ejecutar e infectar un sistema. El criterio principal para clasificar un fragmento de código ejecutable como un virus es que se propaga por medio de hosts. Los hosts podrían ser cualquier aplicación o archivo en el sistema. Un virus infecta un sistema al replicarse a sí mismo a través de hosts de aplicaciones. Los virus suelen incluir un mecanismo de replicación y un mecanismo de activación diseñado con un objetivo particular en mente.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, seguridad del correo electrónico

¿Cuáles son los principales problemas de seguridad relacionados con la retransmisión SMTP?, http://searchexchange.techtarget.com/expert/KnowledgebaseAnswer/0,sid43_gci947777,00.html

---

Pregunta #83 de 131

Id. de pregunta: 1113954

¿Qué afirmación NO es cierta con respecto a la tecnología ETHERNET LAN?

- ✗ **A)** Es compatible con transmisiones full duplex.
- ✗ **B)** Está definido por IEEE 802.3
- ✗ **C)** Utiliza el acceso múltiple del detección del portador con la detección de la colisión (CSMA/CD).
- ✓ **D)** Utiliza una unidad de acceso multiestación (MAU) como su dispositivo central.

explicación

La tecnología Ethernet LAN NO utiliza una unidad de acceso multiestación (MAU) como su dispositivo central. Este es el dispositivo central utilizado en la tecnología Token Ring. Las redes Token Ring fueron definidas por IEEE 802.5. Token Ring soporta la transmisión dúplex completa usando el acceso múltiple del detección portadora con la evitación de colisiones (CSMA/CA).

Ethernet admite transmisiones de dúplex completo. Utiliza el acceso múltiple del detección del portador con la detección de la colusión (CSMA/CD). Está definido por IEEE 802.3.

Full-duplex puede transmitir y recibir información en ambas direcciones simultáneamente. Las transmisiones pueden ser asíncronas o síncronas. En la transmisión asíncrona, se utiliza un bit de inicio para indicar el comienzo de la

transmisión. El bit inicial va seguido de bits de datos y, a continuación, le siguen uno o dos bits de parada para indicar el final de la transmisión. Porque los bits del comienzo y de la parada se envían con cada unidad de datos, la velocidad de transmisión de datos real es más baja que semidúplex porque los bits de tara se utilizan para la sincronización y no llevan la información. En este modo, los datos se envían sólo cuando están disponibles y los datos no se transmiten continuamente. En la transmisión síncrona, el transmisor y el receptor tienen relojes sincronizados y los datos se envían en un flujo continuo. Los relojes se sincronizan mediante transiciones en los datos y, por lo tanto, los bits de inicio y detención no son necesarios para cada unidad de datos enviada.

Las transmisiones semidúplex son transmisiones en las que la información puede transmitirse en dos direcciones, pero sólo en una dirección a la vez. Las transmisiones símplex son la comunicación que tiene lugar en una sola dirección.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3ª Edición),Capítulo 4: Comunicación y Seguridad de Red, Ethernet 802.3

Pregunta #84 de 131

Id. de pregunta: 1114739

¿Qué dispositivo de red proporciona una solución de firewall transparente entre una red interna y redes externas?

- ✗ **A)** servidor proxy
- ✗ **B)** concentrador
- ✓ **C)** Enrutador NAT
- ✗ **D)** enrutador

explicación

Un enrutador de traducción de direcciones de red (NAT) proporciona una solución de firewall transparente entre una red interna y redes externas. Con NAT, varios equipos internos pueden compartir una única interfaz de Internet y una dirección IP. El propósito principal de NAT es ocultar los hosts internos de la red pública. Al implementar NAT, la red privada debe usar uno de los intervalos de direcciones de red privada:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

El NAT puede utilizar la traducción estática o dinámica. La traducción estática tiene asignaciones estáticas para la comunicación NAT; la traducción dinámica tiene una tabla dinámica que se configura mientras que los host intentan utilizar el NAT. El NAT puede causar los problemas con un túnel de la red privada virtual (VPN) IPSec debido a los cambios realizados al encabezado IP. NAT sólo se admite con IPSec cuando se ejecuta en modo nat traversal.

Un servidor proxy a menudo se confunde como un servidor NAT. Sin embargo, un servidor proxy no es una solución transparente. Un servidor proxy funciona en la capa 4 o superior del modelo OSI (la capa de transporte o superior). NAT actúa en la capa de red (capa 3) del modelo OSI.

Un enrutador es un dispositivo de red que divide una red de área local en subredes más pequeñas. Los routers operan en la capa de red (Capa 3) del modelo OSI. Mientras que un Firewall puede también ser un router, se refiere como Firewall cuando funciona para crear un DMZ.

Un concentrador es un dispositivo de red que conecta varias redes entre sí.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, direcciones IP públicas frente a direcciones IP privadas

Cómo funciona la traducción de direcciones de red, http://computer.howstuffworks.com/nat5.htm

---

Pregunta #85 de 131

Id. de pregunta: 1105238

¿Qué implementación de línea de suscriptor digital (DSL) ofrece velocidades de hasta 8 megabits por segundo (Mbps) y proporciona una velocidad de descarga más rápida que la velocidad de carga?

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

explicación

Asymmetrical Digital Subscriber Line (ADSL) ofrece velocidades de hasta 8 megabits por segundo (Mbps) y proporciona una velocidad de descarga más rápida que la velocidad de carga.

Dsl de alta velocidad de bits (HDSL) ofrece velocidades de hasta 1,544 Mbps a través de cable UTP normal.

ISDN DSL (IDSL) ofrece velocidades de hasta 128 kilobits por segundo (Kbps).

Symmetrical DSL (SDSL) ofrece velocidades de hasta 1,1 Mbps. Los datos viajan en ambas direcciones a la misma velocidad.

Otro tipo de DSL es la línea de suscriptor digital de velocidad de bits muy alta (VDSL). VDSL transmite a velocidades súper aceleradas de 52 Mbps aguas abajo y 12 Mbps en sentido ascendente.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, DSL

Pregunta #86 de 131

Id. de pregunta: 1105230

¿Qué condición podría indicar que un hacker está atacando una red?

- ✗ **A)** un enrutador que está transmitiendo tráfico
- ✗ **B)** un ligero aumento en el tráfico de red
- ✓ **C)** un aumento importante en el tráfico ICMP
- ✗ **D)** una ligera disminución del tráfico de red

explicación

Un aumento importante en el tráfico del Protocolo de mensajes de control de Internet (ICMP) indica que un pirata informático podría estar atacando una red con un ataque de denegación de servicio (DoS) de ping.

Se espera un ligero aumento o disminución en la línea de base del tráfico de red en las operaciones de red generales. Los aumentos o disminuciones importantes o repentinos en el tráfico de red pueden indicar que una red está siendo atacada por un pirata informático. Un enrutador es un dispositivo diseñado para transmitir tráfico entre redes.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:

Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, DoS

Pregunta #87 de 131

Id. de pregunta: 1302571

Debe proponer un esquema de cableado para la nueva ubicación de su empresa. Varios departamentos están ubicados en el mismo piso con una distancia máxima de 61 metros (200 pies) entre departamentos. Desea una instalación relativamente fácil y de bajo costo con conexiones simples.

¿Qué tipo de cableado propondrías?

- ✗ **A)** ThickNet
- ✗ **B)** Fibra óptica
- ✗ **C)** ThinNet
- ✓ **D)** Par trenzado

explicación

El cableado de par trenzado es el medio de cableado menos costoso. Debido a que el par trenzado sin blindes (UTP) se usa comúnmente en sistemas telefónicos, se produce en masa, lo que lo hace barato y ampliamente disponible. Además, el cableado de par trenzado es muy fácil de trabajar, lo que significa que se requiere muy poca capacitación para su instalación.

Al igual que en los sistemas telefónicos, el cableado de par trenzado utiliza conectores de conectores de conectores registrados (RJ) para conectar cables a los componentes. Las redes de computadoras utilizan los conectores RJ-45 más grandes, que son muy similares a los conectores RJ-11 comúnmente conocidos utilizados en los sistemas telefónicos; esto se suma a la simplicidad de instalar twisted-pair.

Twisted-pair tiene una longitud máxima de 100 metros (328 pies), lo que funcionará para la compañía en el escenario porque las oficinas están ubicadas a menos de 61 metros (200 pies) entre sí. Es importante tener en cuenta que el par trenzado es el tipo de cable de red más susceptible a la atenuación, por lo que su distancia máxima es de 100 metros (328 pies).

La siguiente es una tabla de comparaciones de medios de red:

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

Objetivo:

Comunicación y seguridad de la red

Subobsecución:

Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red. Par trenzado

CCNA: Tipos de medios de red > cable de par trenzado, http://www.ciscopress.com/articles/article.asp?p=31276

Pregunta #88 de 131

Id. de pregunta: 1113948

Desea utilizar el intervalo de direcciones IP privadas designadas por IANA que el intervalo de direcciones IP privadas con un máximo de 16 bits para proporcionar direcciones IP de host.

¿Qué dirección IP es una dirección IP de host válida en este intervalo?

✗ **A)** 11.0.1.0

✗ **B)** 172.30.250.10

✗ **C)** 10.251.250.100

✓ **D)** 192.168.0.1

explicación

De las direcciones IP enumeradas, 192.168.0.1 es una dirección de host válida dentro del intervalo de direcciones IP privadas designadas por IANA que proporcionan un máximo de 16 bits por dirección de host. La dirección IP 11.0.1.0 es una dirección IP pública o externa.

El Grupo de Trabajo de Ingeniería de Internet (IETF) es un grupo de trabajo que crea estándares para Internet. El IETF se divide en una serie de comités más pequeños, incluida la Asociación de Números Asignados de Internet (IANA), que decide cómo se utiliza el espacio de direcciones IP. La IANA ha reservado tres espacios de direcciones para el direccionamiento IP privado o interno. Las direcciones IP internas nunca son asignadas por la IANA para su uso en la Internet pública. Los intervalos de direcciones IP privadas son los siguientes: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16. Tenga en cuenta que el número después del carácter de barra diagonal (/) se conoce como el prefijo de dirección de red, que indica el número de bits en la dirección de red.

Las direcciones IP privadas en el intervalo 192.168.0.0/16 se pueden utilizar como un espacio de direcciones de clase B con una dirección de red de 16 bits y una dirección de host de 16 bits, o se pueden convertir en subredes en direcciones de clase C. Las direcciones IP de host válidas en este espacio de direcciones van desde 192.168.0.1 hasta 192.168.255.254. Los primeros 16 bits de la dirección corresponden a la dirección de red y los últimos 16 bits de la dirección corresponden a la dirección del host.

El intervalo de direcciones IP internas 10.0.0.0/8 proporciona direcciones IP con una dirección de red de 8 bits y una dirección de host de 24 bits. Los primeros 8 bits de una dirección IP interna 10.0.0.0/8 corresponden a la dirección de red y los últimos 24 bits corresponden a la dirección del host. Las direcciones IP de host válidas en este espacio de direcciones van de 10.0.0.1 a 10.255.255.254. La dirección 10.251.250.100 es una dirección IP de host válida en este intervalo.

El intervalo de direcciones IP privadas 172.16.0.0/12 proporciona una dirección de red de 12 bits y una dirección de host de 20 bits. Las direcciones IP en el intervalo de 172.16.0.1 a 172.31.255.254 son direcciones IP de host válidas para este espacio de direcciones; los primeros 12 bits corresponden a la dirección de red y los últimos 20 bits corresponden a la dirección del host. La dirección IP 172.30.250.10 es una dirección IP de host válida en el intervalo 172.16.0.0/12.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, direcciones IP públicas frente a direcciones IP privadas

¿Qué es una dirección IP privada?, http://compnetworking.about.com/od/workingwithipaddresses/f/privateipaddr.htm

---

Pregunta #89 de 131

Id. de pregunta: 1105195

En la red de Windows de su organización, ha implementado directivas que permiten a los usuarios iniciar sesión en la red solo desde determinadas estaciones de trabajo. ¿Qué concepto representa esta acción?

- ✓ **A)** ruta de acceso forzada
- ✗ **B)** dominio de seguridad
- ✗ **C)** ruta de acceso de confianza
- ✗ **D)** kernel de seguridad

explicación

Una ruta de acceso forzada es un método de control de acceso que limita las rutas de acceso a través de las cuales un usuario puede tener acceso a los recursos. Un ejemplo de una ruta de acceso forzada es cuando una organización configura directivas que permiten a los usuarios iniciar sesión en la red únicamente desde determinadas estaciones de trabajo.

Una ruta de acceso de confianza es un mecanismo que permite a un usuario comunicarse con la base informática de confianza (TCB). Un dominio de seguridad es un conjunto de recursos administrados por la misma directiva de seguridad y grupo de seguridad. Un núcleo de seguridad es el hardware, firmware y recursos de software de un TCB.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Ruta de acceso forzada, http://www.yourwindow.to/information-security/gl_enforcedpath.htm

---

Pregunta #90 de 131

Id. de pregunta: 1114744

¿Qué trabajo NO proporciona un analizador de protocolos de red?

- ✓ **A)** Detectar virus activos o malware en la red
- ✗ **B)** proporcionar estadísticas de actividad de red
- ✗ **C)** identificar las fuentes y destinos de las comunicaciones
- ✗ **D)** identificar los tipos de tráfico en la red

explicación

Un analizador de protocolo de red no detecta virus activos ni malware en la red.

La mayoría de los analizadores de protocolo de red proporcionan las siguientes funciones:

Proporcionar estadísticas de actividad de red.

Identificar las fuentes y destinos de las comunicaciones.

Identifique los tipos de tráfico en la red.

Detectar un nivel inusual de tráfico.

Detectar características de patrón específicas.

Un analizador de protocolo de red puede determinar si las contraseñas se transmiten a través de la red en texto no cifrado. También se puede utilizar para leer el contenido de cualquier paquete de protocolo de transferencia de archivos (FTP), incluida una solicitud FTP GET. WireShark es un analizador de protocolo de red comercial.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, ataques de red

Analizador de red, http://searchnetworking.techtarget.com/sDefinition/0,sid7_gci1196637,00.html

---

Pregunta #91 de 131

Pregunta con id.: 1105200

¿Cuál es la desventaja de un firewall de hardware al compararlo con un firewall de software?

- ✗ **A)** Tiene menor capacidad de rendimiento que un firewall de software.

✓ **B)** Tiene un número fijo de interfaces disponibles.

✗ **C)** Es más fácil cometer errores de configuración que en un firewall de software.

✗ **D)** Proporciona una menor seguridad en comparación con un firewall de software.

explicación

Se adquiere un firewall de hardware con un número fijo de interfaces disponibles. Con un firewall de software, agregar interfaces es tan fácil como agregar y configurar otra tarjeta de interfaz de red (NIC).

Un firewall de hardware supera a un firewall de software. Es más fácil cometer errores de configuración en un firewall de software, no en un firewall de hardware. La mayoría de los firewalls de hardware se anuncian como soluciones "llave en mano", lo que significa que los problemas de instalación y configuración de software son mínimos. Los firewalls de hardware generalmente proporcionan una mayor seguridad sobre los firewalls de software.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

Comparación de características de firewall, http://www.windowsecurity.com/articles/Comparing_Firewall_Features.html

---

Pregunta #92 de 131

Id. de pregunta: 1105254

¿En qué tipo de red la confianza NO es una preocupación principal?

✗ **A)** dominios del servicio de directorio

✗ **B)** entorno distribuido

✓ **C)** red privada virtual (VPN)

✗ **D)** Kerberos

explicación

La confianza NO es una preocupación principal en una red privada virtual (VPN). Una VPN es una red privada segura que está aislada de la red privada interna de una organización. La VPN permite a los usuarios conectarse a ella a través de una red pública, como Internet.

La confianza es una preocupación principal en dominios de servicio de directorio, entornos Kerberos y entornos distribuidos.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, VPN

Pregunta #93 de 131

Id. de pregunta: 1105236

¿Qué opción mejor describió un hombre?

- ✓ **A)** una red troncal que conecta LANs con WAN
- ✗ **B)** Una red que conecta otras redes más pequeñas a través de una conexión internacional
- ✗ **C)** Una red que proporciona un túnel privado a través de una red pública
- ✗ **D)** Una red que conecta un solo edificio o grupo de edificios para compartir recursos

explicación

Una red de área metropolitana (MAN) es una red troncal de red que conecta las redes de área local (LAN) con las redes de área extensa (WAN).

Hay tres tipos principales de redes de datos: LANs, MANs, y WAN.

Una LAN es una red que conecta un solo edificio o grupo de edificios para compartir recursos. Una WAN es una red que conecta otras redes más pequeñas a través de una conexión internacional. Una red privada virtual (VPN) es una red que proporciona un túnel privado a través de una red pública.

Una LAN inalámbrica (WLAN) es una red de área local inalámbrica. Una red privada virtual (VPN) es una red privada a la que se accede a través de una red pública, como Internet.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:

Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, MAN

Pregunta #94 de 131

Id. de pregunta: 1114734

¿Cuáles son las características del método de conmutación de corte?

un. Los marcos se descartan si son runts o gigantes.

B. Tiene menos latencia que el método de almacenamiento y reenvío.

c. La comprobación de redundancia cíclica (CRC) se calcula después de que una trama se copie al búfer del Switch.

d. Solamente la dirección de destino se copia en el buffer del Switch antes de que una trama se remita a su destino.

- ✗ **A)** Sólo las opciones A y C
- ✗ **B)** opción A
- ✗ **C)** Opción d
- ✓ **D)** Opciones B y D Sólo
- ✗ **E)** opción c
- ✗ **F)** opción b

explicación

El método de corte copia la dirección de destino de una trama en el búfer del conmutador y, a continuación, envía la trama a su destino. Este método da como resultado una latencia reducida en comparación con los conmutadores que utilizan el método de almacenamiento y reenvío. El tiempo de espera es esencialmente el retardo que ocurre mientras que la trama atraviesa el Switch. El método de transferencia de corte a través tiene generalmente menos latencia y mantiene una latencia constante, ya que el conmutador reenvía la trama tan pronto como lea la dirección de destino. Esto da lugar a un procesamiento de trama más rápido a través del switch. Sin embargo, los switches configurados para utilizar el método de corte no realizan ninguna comprobación de errores.

El método de almacenamiento y reenvío copia una trama completa en su búfer, calcula la comprobación de redundancia cíclica (CRC) y descarta las tramas que contienen errores, así como las tramas runt (menos de 64 bytes) y las tramas gigantes (mayores de 1.518 bytes). Porque el Switch debe recibir la trama entera antes de remitir, el tiempo de espera a través del Switch varía con la longitud de trama. Esto causa más latencia en comparación con los conmutadores que utilizan el método de corte.

Debe basar su decisión en cuanto a qué método de conmutación utilizar en una red en si la comprobación de errores o la latencia constante es la mayor preocupación. Configure los conmutadores para que usen el método de conmutación de almacenamiento y reenvío en lugar del método de conmutación de corte cuando desee que los conmutadores realicen comprobaciones de errores y no le importe una latencia incoherente o un rendimiento más lento. Configure los conmutadores para que utilicen el método de conmutación de corte cuando necesite una latencia constante o un rendimiento más rápido y no necesite comprobación de errores.

Además de los dos métodos de conmutación principales, cut-through y store-and-forward, también hay un método de corte modificado conocido como "sin fragmentos". Porque las colisiones ocurren normalmente dentro de los primeros 64 bytes de una trama, fragmento-libre lee estos bytes antes de remitir la trama. Esto permite que el método sin fragmentos filtre las tramas de colisión.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cómo funcionan los conmutadores LAN, https://computer.howstuffworks.com/lan-switch.htm

---

Pregunta #95 de 131

Id. de pregunta: 1105206

¿Qué tipo de firewall oculta el verdadero origen de un paquete antes de enviarlo a través de otra red?

- ✗ **A)** host bastión
- ✓ **B)** servidor de seguridad proxy
- ✗ **C)** firewall de filtrado de paquetes
- ✗ **D)** firewall con estado

explicación

Un firewall proxy oculta el verdadero origen de un paquete antes de enviarlo a través de otra red. La característica de seguridad principal de un firewall proxy es que oculta la información del cliente. Es el único equipo de una red que se comunica con equipos que no son de confianza.

Un host bastión es un sistema reforzado que generalmente reside en una zona desmilitarizada (DMZ) y se accede con frecuencia.

Un firewall con estado reenvía paquetes en nombre del cliente. Examina cada paquete y permite o deniega su paso basándose en muchos factores, incluida la tabla de estados. La tabla de estados se utiliza para realizar un seguimiento de dónde está una conexión en el protocolo de enlace TCP para que se puedan descartar las tramas que llegan que se reciben fuera de la secuencia normal (un indicador de posible actividad maliciosa). Este tipo de firewall también se conoce a menudo como firewall de inspección con estado.

Un firewall de filtrado de paquetes reenvía los paquetes en función de las reglas que definen qué tráfico se permite y se deniega en la red. Un firewall de filtrado de paquetes examina el paquete de datos para obtener información sobre las direcciones de origen y destino de un paquete entrante, el protocolo de comunicaciones de la sesión (TCP, UDP o ICMP) y el puerto de aplicación de destino de origen para el servicio deseado.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, tipos de firewall

---

Pregunta #96 de 131

Id. de pregunta: 1114738

¿Qué características se aplican a las redes Fast Ethernet 100Base-TX?

a. Velocidad de transmisión de datos de 100 Mbps

B. Dos pares de cableado UTP de categoría 5

c. Cuatro pares de cableado UTP de categoría 3, 4 o 5

d. Longitud máxima del segmento de 100 metros (328 pies)

E. Longitud máxima del segmento de 412 metros (1.352 pies) semidúplex

- ✗ **A)** opción b
- ✗ **B)** Opción d
- ✗ **C)** sólo las opciones a, c y e
- ✗ **D)** opción A
- ✗ **E)** opciones a, b y e solamente
- ✗ **F)** opción e
- ✓ **G)** opciones a, b y d solamente

✗ **H)** opción c

✗ **I)** sólo las opciones a, c y d

explicación

100Base-TX, conocido como Fast Ethernet, utiliza dos pares de cable UTP de categoría 5. Se utilizan conectores RJ-45 estándar. 100Base-TX transmite datos a 100 Mbps utilizando el tipo de señalización de banda base. Su distancia máxima de segmento es de 100 metros (328 pies).

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, par trenzado

---

Pregunta #97 de 131

Id. de pregunta: 1105219

Usted es el administrador de seguridad de su organización. Un usuario del departamento de TI le informa de que un servidor de impresión fue recientemente víctima de un ataque de lágrimas. ¿Qué instrucción define correctamente el ataque que se ha producido?

✗ **A)** Implica el uso de paquetes no válidos que tienen las mismas direcciones de origen y destino.

✗ **B)** Implica aprovechar los paquetes ICMP de gran tamaño y hacer que el sistema se congele o se bloquee.

✗ **C)** Inunda el host de destino con paquetes SYN falsificados y hace que el host se congele o se bloquee.

✓ **D)** Implica el uso de paquetes fragmentados con formato incorrecto y hace que el sistema de destino se congele o se bloquee.

explicación

En un ataque teardrop, el atacante utiliza una serie de paquetes fragmentados de protocolo de Internet (IP) y hace que el sistema se congele o se bloquee mientras el host de destino vuelve a ensamblar los paquetes. Un ataque teardrop se basa principalmente en la implementación de fragmentación de IP. Para volver a montar los fragmentos en el paquete original en el destino, el host busca paquetes entrantes para asegurarse de que pertenecen al mismo paquete

original. Los paquetes están mal formados. Por lo tanto, el proceso de volver a ensamblar los paquetes hace que el sistema se congele o se bloquee.

En un ataque de tierra, se utilizan paquetes no válidos que tienen las mismas direcciones de origen y destino. Un ataque terrestre implica el envío de un paquete TCP SYN falsificado con la dirección IP del host de destino y un puerto abierto que sirve como origen y destino al host de destino en un puerto abierto. El ataque a tierra hace que el sistema se congele o se bloquee porque la máquina responde continuamente a sí misma.

En un ataque de inundación SYN, el atacante inunda el objetivo con paquetes IP falsificados y hace que se congele o se bloquee. El Protocolo de control de transmisión (TCP) utiliza los paquetes de sincronización (SYN) y confirmación (ACK) para establecer la comunicación entre dos equipos host. El intercambio de los paquetes SYN, SYN-ACK y ACK entre dos equipos host se conoce como protocolo de enlace. Los atacantes inundan los equipos de destino con una serie de paquetes SYN a los que responde el equipo host de destino. A continuación, el equipo host de destino asigna recursos para establecer una conexión. La dirección IP está falsificada. Por lo tanto, el equipo host de destino nunca recibe una respuesta válida en forma de paquetes de confirmación desde el equipo atacante. Cuando el equipo de destino recibe muchos de estos paquetes SYN, se queda sin recursos para establecer una conexión con los usuarios legítimos y se vuelve inalcanzable para el procesamiento de solicitudes válidas.

En un ataque de denegación de servicio (DoS), el equipo de destino se inunda con numerosos paquetes de protocolo de mensajes de control de Internet (ICMP) o protocolo de datagramas de usuario (UDP) de gran tamaño. Estos paquetes, que consumen el ancho de banda de la red de destino o sobrecargan los recursos computacionales del sistema de destino, causan la pérdida de conectividad de red y servicios. Ping de la muerte, pitufo, bonk, y fraggle son ejemplos de ataques DoS.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red, Teardrop

---

Pregunta #98 de 131

Id. de pregunta: 1114731

¿Qué tipo de firewall examina primero un paquete para ver si es el resultado de una conexión anterior?

- ✗ **A)** firewall proxy de nivel de aplicación
- ✗ **B)** firewall proxy a nivel de circuito
- ✓ **C)** firewall con estado

✗ **D)** firewall de filtrado de paquetes

explicación

Un firewall con estado examina primero un paquete para ver si es el resultado de una conexión anterior. La información sobre las conexiones anteriores se mantiene en la tabla de estados.

Ninguno de los otros firewalls examina primero un paquete para ver si es el resultado de una conexión anterior.

Con un firewall con estado, se permite un paquete si es una respuesta a una conexión anterior. Si la tabla de estados no contiene ninguna información sobre el paquete, el paquete se compara con la lista de control de acceso (ACL). Dependiendo del ACL, el paquete será remitido al host apropiado o ser caído totalmente.

Los firewalls con estado realizan las siguientes tareas:

Escanee la información de todas las capas del paquete.

Guarde la información de estado derivada de comunicaciones anteriores, como la información del puerto saliente, para que la comunicación de datos entrantes se pueda comprobar con ella.

Proporcionar compatibilidad de seguimiento para protocolos sin conexión mediante el uso de bases de datos de estado de sesión.

Permitir el acceso a la información de estado derivada de otras aplicaciones a través del firewall solo para servicios autorizados, como usuarios previamente autenticados.

Evaluar y manipular expresiones flexibles basadas en la comunicación y la información de estado derivada de la aplicación.

Los firewalls con estado se pueden utilizar para realizar un seguimiento de los protocolos sin conexión, como el Protocolo de datagramas de usuario (UDP), porque examinan más que el encabezado del paquete.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #99 de 131

Id. de pregunta: 1114730

¿Qué tipo o tipos de firewalls operan en la capa de red del modelo OSI?

a. Firewall con estado

b. Firewall proxy del núcleo

c. Servidor de seguridad de filtrado de paquetes

d. Firewall proxy a nivel de circuito

e. Firewall proxy de nivel de aplicación

- ✗ **A)** opción e
- ✗ **B)** opciones b, d y e solamente
- ✗ **C)** opción A
- ✗ **D)** todas las opciones
- ✗ **E)** opción b
- ✓ **F)** Sólo las opciones A y C
- ✗ **G)** Opción d
- ✗ **H)** opción c

explicación

Los firewalls con estado y de filtrado de paquetes funcionan en la capa de red y transporte del modelo OSI. Los firewalls con estado también funcionan en la capa de enlace de datos.

Los firewalls proxy a nivel de circuito funcionan en la capa session.

El proxy del kernel y los firewalls proxy de nivel de aplicación funcionan en el nivel de aplicación del modelo OSI.

Los firewalls conectan redes privadas y públicas. Su propósito principal es proteger la red privada de las brechas de seguridad mediante la creación de puntos de control de seguridad en los límites entre las redes privadas y públicas. Los firewalls crean cuellos de botella entre las redes privadas y públicas porque deben examinar los paquetes que pasan a través de ellos. Si existe un firewall dedicado en su red, permitirá la centralización de los servicios de seguridad.

Los firewalls proporcionan filtrado de paquetes, traducción de direcciones de red (NAT), proxy y servicios de túnel cifrados, entre otras cosas. Los servicios de túnel cifrados son probablemente el servicio menos importante proporcionado por los firewalls.

La mayoría de los firewalls incluyen un componente de filtrado de protocolos que permite a los administradores de seguridad configurar el comportamiento del firewall en función de los protocolos que encuentra. El motor de aplicación de reglas de un firewall garantiza que se aplican las reglas configuradas por el administrador de seguridad. La mayoría de los firewalls incluyen una función de registro extendida que permite a los administradores de seguridad auditar las actividades del firewall.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #100 de 131

Id. de pregunta: 1105178

¿Qué arquitectura de firewall tiene dos interfaces de red?

- ✗ **A)** host con pantalla
- ✓ **B)** firewall de doble hogar
- ✗ **C)** host bastión
- ✗ **D)** subred filtrada

explicación

Un firewall de doble hogar tiene dos interfaces de red. Una interfaz se conecta a la red pública, normalmente a Internet. La otra interfaz se conecta a la red privada. La función de reenvío y enrutamiento debe deshabilitarse en el firewall para asegurarse de que se produce la segregación de red.

Un host bastión es un equipo que reside en una red que está bloqueada para proporcionar la máxima seguridad. Estos tipos de hosts residen en la primera línea de los sistemas de seguridad de red de una empresa. La configuración de seguridad de esta entidad es importante porque se expone a entidades que no son de confianza. Cualquier servidor que resida en una zona desmilitarizada (DMZ) debe configurarse como host bastión. Un host bastión tiene instalado el software de firewall, pero también puede proporcionar otros servicios.

Un host cribado es un firewall que reside entre el router que conecta una red a Internet y la red privada. El router actúa como un dispositivo de detección, y el firewall es el host de pantalla.

Subred filtrada es otro término para una zona desmilitarizada (DMZ). Dos Firewall se utilizan en esta configuración: un Firewall reside entre la red pública y dmz, y el otro reside entre el DMZ y la red privada.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, arquitectura de firewall

---

Pregunta #101 de 131

Id. de pregunta: 1113968

¿Qué tecnología centraliza la autenticación, las estadísticas y la autorización por comando?

- ✗ **A)** radio
- ✓ **B)** TACACS+
- ✗ **C)** anuncio
- ✗ **D)** LDAP

explicación

El sistema de control de acceso del controlador de acceso de terminal (TACACS+) centraliza la autenticación, las estadísticas, y la autorización por comando. TACACS+ habilita la autenticación de dos factores, permite que un usuario cambie las contraseñas y resincroniza los tokens de seguridad.

El Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) ofrece un sistema centralizado para la autenticación. El RADIUS no ofrece las estadísticas centralizadas o la autorización por comando, pero se soporta más extensamente que el TACACS+.

Active Directory (AD) es un servicio de directorio compatible con redes Windows. El Protocolo ligero de acceso a directorios (LDAP) se utiliza para crear una conexión entre servicios de directorio o entre un servicio de directorio y un cliente.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, RADIUS y TACACS+

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

---

Pregunta #102 de 131

Id. de pregunta: 1114728

Usted ha descubierto que los hackers están obteniendo acceso a su red inalámbrica WEP. Después de investigar, descubres que los hackers están utilizando la conducción de guerra. Es necesario protegerse contra este tipo de ataque.

¿Qué debes hacer?

un. Cambie el identificador de conjunto de servicios (SSID) predeterminado.

B. Inhabilite las difusiones SSID.

c. Configure la red para utilizar el acceso autenticado solamente.

d. Configure el protocolo WEP para utilizar una clave de 128 bits.

- ✗ **A)** opción c
- ✗ **B)** Opción d
- ✗ **C)** opción A
- ✗ **D)** Sólo las opciones A y B
- ✗ **E)** todas las opciones
- ✗ **F)** opción b
- ✓ **G)** sólo las opciones a, b y c

explicación

Debe completar todos los pasos siguientes para protegerse contra los ataques de conducción de guerra:

Cambie el SSID predeterminado.

Inhabilite las difusiones SSID.

Configure la red para que utilice solo el acceso autenticado.

Algunos otros pasos sugeridos incluyen:

Implemente el acceso protegido Wi-Fi (WPA) o WPA2 en lugar de WEP.

Reduzca la intensidad de la señal del punto de acceso.

La conducción de guerra es un método para descubrir redes inalámbricas 802.11 conduciendo con una computadora portátil y buscando redes inalámbricas abiertas. NetStumbler es una herramienta común de conducción de guerra.

Anteriormente, una de las formas de protegerse contra este ataque era configurar el protocolo WEP para utilizar una clave de 128 bits. Sin embargo, desde entonces se ha demostrado que todas las versiones de WEP son susceptibles a los ataques.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

El conducir de la guerra, https://searchmobilecomputing.techtarget.com/definition/war-driving

---

Pregunta #103 de 131

Id. de pregunta: 1114748

Su empresa consta de 75 empleados. Su empresa ha entrado en una asociación con otra empresa que se encuentra en todo el país. Los usuarios de su empresa deben poder conectarse a la red del socio de forma rápida y fiable. Se requiere soporte para transmisiones de voz, datos e imágenes y un enlace dedicado las 24 horas. La solución debe ser lo más económica posible y, al mismo tiempo, proporcionar suficiente ancho de banda para los empleados de su empresa.

¿Qué tecnología debe implementar?

- ✗ **A)** ISDN
- ✗ **B)** tiestos
- ✓ **C)** T1
- ✗ **D)** cajero
- ✗ **E)** Fddi

explicación

Las líneas T1 pueden proporcionar conexiones digitales rápidas de hasta 1,544 Mbps, transmitiendo voz, datos y vídeo. Una línea T1 también proporciona una conexión dedicada, lo que significa que proporciona un enlace de 24 horas. Una línea T1 es más costosa que una conexión de acceso telefónico mediante plain old telephone service (POTS) o una conexión de red digital de servicios integrados (ISDN), pero esta compañía necesita suficiente ancho de banda para acomodar a sus 75 usuarios, lo que justifica el costo adicional. Si el ancho de banda completo del T1 demuestra demasiado costoso o innecesario, el T1 fraccionario está disponible. Con un T1 fraccionario, puede suscribirse a uno o más de los 24 canales disponibles a un costo menor que el T1.

El Asynchronous Transfer Mode (ATM) es un tipo de enlace de conmutación de paquetes de alta velocidad que transmite hasta 2,488 Mbps. ATM requiere equipos costosos para su implementación. Por lo tanto, es una alternativa costosa y es utilizada típicamente por las espinas dorsales de Internet.

Fiber Distributed Data Interface (FDDI) es una red Token Ring de alta velocidad que utiliza cables de fibra óptica que transmiten hasta 100 Mbps. Aunque ofrece velocidad, está limitado a una distancia de anillo de 100 kilómetros o 62 millas. Incluso si la distancia no fuera un factor, el medio de fibra hace que esta alternativa sea demasiado costosa.

La red digital de servicios integrados (ISDN) proporciona una conexión digital directa punto a punto a una velocidad de hasta 2 Mbps. Sin embargo, normalmente, las velocidades de 128 Kbps se ven con la ISDN. Sin embargo, es una conexión de acceso telefónico; por lo tanto, no proporcionaría un vínculo dedicado las 24 horas.

Plain Old Telephone Service (POTS) utiliza cableado telefónico estándar, lo que lo convierte en una solución de bajo costo, pero no ofrecería la conexión rápida deseada, ni ofrecería un enlace dedicado las 24 horas, ya que es una conexión de acceso telefónico.

Las tecnologías de conmutación de paquetes incluyen X.25, ATM, Frame Relay y Voz sobre IP (VoIP). Las tecnologías de conmutación de paquetes tienen las siguientes propiedades:

A los paquetes se les asignan números de secuencia.

Se produce un tráfico de ráfaga.

La red no tiene conexión.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, Líneas T

Pregunta #104 de 131

Id. de pregunta: 1111740

Haga coincidir las descripciones de la izquierda con los tipos de ataque de la derecha.

{UCMS id=5733523484835840 type=Activity}

explicación

Los ataques deben coincidir con las descripciones de la siguiente manera:

- Ataque de fuerza bruta : se produce cuando un hacker intenta todos los valores posibles para variables como nombres de usuario y contraseñas
- Envenenamiento por DNS : se produce cuando se dan direcciones IP y nombres de host con el objetivo de desviar el tráfico

- Ataque de tipo "Man in the middle": se produce cuando un pirata informático intercepta mensajes de un remitente, los modifica y los envía a un receptor legítimo.
- Pitufo : se produce cuando una combinación de suplantación de protocolo de Internet (IP) y mensajes de protocolo de mensajes de control de Internet (ICMP) satura una red

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Glosario

Pregunta #105 de 131

Id. de pregunta: 1105223

Un cliente se pone en contacto con usted en relación con un problema de servidor de correo electrónico. Al investigar el problema, observa que hay un número extremadamente grande de mensajes de correo electrónico en la carpeta saliente. Esto ha hecho que el disco duro se llene. Detener temporalmente el servidor de correo electrónico, eliminar los mensajes de correo electrónico y reinicie el servidor de correo electrónico. Inmediatamente, la carpeta de correo saliente comienza a llenarse de nuevo.

¿Qué tipo de problema está experimentando?

✗ **A)** ataque zombie
✗ **B)** Infección por caballo de Troya
✓ **C)** Retransmisión SMTP
✗ **D)** infección por virus

explicación

Retransmisión SMTP es el problema que está experimentando, hasta que deshabilite la retransmisión SMTP en el servidor de correo electrónico, la carpeta de correo saliente seguirá llenándose.

Ninguno de los otros problemas haría que la carpeta de correo saliente se llenara inmediatamente.

Los zombis son programas controlados por control remoto que los hackers pueden utilizar para atacar redes. Los zombis a menudo están programados para hacer que un ataque de hackers parezca como si se originó en un equipo diferente.

Un caballo de Troya es un malware que se disfraza como una utilidad útil, pero contiene código malicioso incrustado. Cuando se ejecuta la utilidad disfrazada, el caballo de Troya realiza actividades maliciosas en segundo plano y proporciona una utilidad útil en el front-end. Los caballos de Troya utilizan canales encubiertos para realizar actividades maliciosas, como eliminar archivos del sistema y plantar una puerta trasera en un sistema.

Un virus es un software malicioso (malware) que se basa en otros programas de aplicación para ejecutar e infectar un sistema. El criterio principal para clasificar un fragmento de código ejecutable como un virus es que se propaga por medio de hosts. Los hosts podrían ser cualquier aplicación o archivo en el sistema. Un virus infecta un sistema al replicarse a sí mismo a través de hosts de aplicaciones. Los virus suelen incluir un mecanismo de replicación y un mecanismo de activación diseñado con un objetivo particular en mente.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, Spam

¿Cuáles son los principales problemas de seguridad relacionados con la retransmisión SMTP?, http://searchexchange.techtarget.com/expert/KnowledgebaseAnswer/0,sid43_gci947777,00.html

---

Pregunta #106 de 131

Id. de pregunta: 1105139

¿Qué capa OSI es responsable de dar formato a los datos?

- ✓ **A)** presentación
- ✗ **B)** aplicación
- ✗ **C)** red
- ✗ **D)** Vínculo de datos

explicación

La capa de presentación, o capa 6, es normalmente una parte del sistema operativo. Sus principales responsabilidades incluyen el formato de datos, el cifrado de datos y la traducción de paquetes que recibe. Esta capa se traduce entre los formatos de datos de aplicación y de red.

La capa Presentación funciona para transformar los datos en la forma que la capa de aplicación puede aceptar. Formatea y cifra los datos que se enviarán a través de una red, lo que proporciona la libertad de problemas de

compatibilidad. Un ejemplo de un protocolo que opera en esta capa es el protocolo de música digital MIDI.

Las capas Presentación y Sesión proporcionan seguridad de extremo a extremo de TCP/IP.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de la Red, Presentación

---

Pregunta #107 de 131

Id. de pregunta: 1192940

¿Qué puertos se conocen como los puertos conocidos?

- ✓ **A)** Puertos del 0 al 1023
- ✗ **B)** Puertos 49152 a 65535
- ✗ **C)** Puertos 1024 a 49151
- ✗ **D)** Puertos 1024 a 65535

explicación

Los puertos 0 a 1023 son los puertos conocidos. La Autoridad de números asignados de Internet (IANA) asigna estos puertos. No todos estos números de puerto se asignan a un protocolo.

Los puertos 1024 a 65535 se conocen como puertos dinámicos porque los sistemas operativos pueden asignarlo según sea necesario. Los puertos 1024 a 49151 son puertos registrados, lo que significa que varias aplicaciones y servicios han registrado su uso con la IANA. La mayoría de las empresas limitan los puertos dinámicos a los que numeran del 49152 al 65535 para no interferir con los reservados por ciertas aplicaciones y servicios.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, números de puerto TCP/UDP comunes

Pregunta #108 de 131

Id. de pregunta: 1105257

Una organización desea implementar un servidor de acceso telefónico remoto para garantizar que el personal pueda conectarse a la red de la organización desde ubicaciones remotas. El protocolo de autenticación debe incluir cifrado para evitar que los piratas informáticos accedan a la red. ¿Qué protocolo se debe utilizar?

✓ **A)** tipo

✗ **B)** papilla

✗ **C)** savia

✗ **D)** LDAP

explicación

El Protocolo de autenticación por desafío mutuo (CHAP) utiliza un método de desafío-respuesta para autenticar a un usuario. La autenticación cifrada aplica un algoritmo de firma digital a los bits de datos que se envían desde el reclamante al verificador. En CHAP, se envía una solicitud de inicio de sesión desde el usuario al servidor de autenticación. El servidor responde enviando un desafío con un valor aleatorio al usuario. El usuario cifra este desafío con una contraseña predefinida. El servidor deniega o concede acceso al usuario descifrando la respuesta de desafío y comparándola con el valor recibido del usuario.

El Protocolo de autenticación de contraseña (PAP) es un protocolo de autenticación utilizado para autenticar a los usuarios a través de redes de protocolo punto a punto (PPP). PAP identifica y autentica a los usuarios que intentan acceder a la red desde ubicaciones remotas. PAP envía las credenciales en texto no cifrado a través de la red. PAP no utiliza ninguna forma de cifrado durante la autenticación y no se utiliza muy a menudo debido a sus problemas de seguridad.

Service Advertisement Protocol (SAP) es un protocolo IPX. Los servidores de archivos e impresión anuncian sus direcciones y servicios a través de SAP cada 60 segundos. Los enrutadores escuchan los anuncios de SAP y crean una tabla de todos los servicios conocidos junto con sus direcciones de red. Esta información se anuncia a través de SAP cada 60 segundos. El enrutador local responde a la consulta de servicio de archivo, impresora o puerta de enlace con la dirección de red del servicio solicitado. El cliente puede ponerse en contacto directamente con el servicio. SAP no proporciona autenticación cifrada.

El Protocolo ligero de acceso a directorios (LDAP) es un protocolo de red. Consulta y modifica los servicios de directorio que se ejecutan a través de TCP/IP. Un cliente inicia una sesión LDAP conectándose al puerto TCP 389 en el servidor LDAP. El servidor responde a las solicitudes de operación del cliente de forma secuencial. LDAP no proporciona autenticación cifrada.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, protocolos de autenticación remota

Cisco- Comprensión y configuración de la autenticación CHAP PPP, http://www.cisco.com/warp/public/471/understanding_ppp_chap.html

---

Pregunta #109 de 131

Id. de pregunta: 1105225

¿Qué protocolo utiliza el puerto 1812 para comunicarse con los usuarios de acceso telefónico?

- ✓ **A)** radio
- ✗ **B)** TACACS
- ✗ **C)** resbalar
- ✗ **D)** PPP

explicación

El Servicio de autenticación remota telefónica de usuario (RADIUS) utiliza el puerto 1812 para comunicarse con los usuarios de acceso telefónico. Es un protocolo basado en UDP.

El Point-to-Point Protocol (PPP) es un protocolo de encapsulación usado para transmitir los datos sobre las líneas telefónicas. No utiliza ningún puerto porque la información de encapsulación PPP se quita cuando los datos llegan a una red informática.

Serial Line Internet Protocol (SLIP) es un más viejo encapsulation protocol que fue utilizado antes de que el PPP fuera creado. Su funcionamiento es similar al PPP pero no proporciona la corrección de errores y no proporciona diversos métodos de autenticación.

El sistema de control de acceso del controlador de acceso de terminal (TACACS) utiliza el puerto 49 para comunicarse con los usuarios de acceso telefónico. Es un protocolo basado en UDP. El TACACS+ utiliza el puerto 65 para comunicar con los usuarios de acceso telefónico. Es un protocolo basado en TCP.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, RADIUS y TACACS+

Números de puerto, http://www.iana.org/assignments/port-numbers

---

Pregunta #110 de 131

Id. de pregunta: 1114732

Ha configurado los siguientes filtros en el firewall de filtrado de paquetes de su empresa:

Permita todo el tráfico hacia y desde los hosts locales.

Permitir todas las conexiones TCP entrantes.

Permita que todo el tráfico SSH linux1.kaplanit.com.

Permitir que todo el tráfico SMTP smtp.kaplanit.com.

¿Qué regla probablemente resultará en una violación de seguridad?

- ✗ **A)** Permitir que todo el tráfico SMTP smtp.kaplanit.com.
- ✓ **B)** Permitir todas las conexiones TCP entrantes.
- ✗ **C)** Permita todo el tráfico hacia y desde los hosts locales.
- ✗ **D)** Permita que todo el tráfico SSH linux1.kaplanit.com.

explicación

Lo más probable es que la regla Permitir todas las conexiones TCP entrantes dé lugar a una infracción de seguridad. Esta regla es una que no verá en la mayoría de las configuraciones de firewall. Simplemente permitiendo todas las conexiones TCP entrantes, no está limitando los hosts remotos a ciertos protocolos. Se producirán infracciones de seguridad debido a esta configuración incorrecta. Solo debe permitir los protocolos que necesiten los hosts remotos. Usted debe dejar caer todos los demás.

En la mayoría de los casos, permitir todo el tráfico hacia y desde hosts locales es una regla de firewall común. Si configura reglas de firewall con respecto al tráfico de host local, debe extremar las precauciones. Es difícil predecir el tipo de tráfico que se origina con los hosts locales. Si decide eliminar ciertos tipos de tráfico, los usuarios pueden quejarse de no poder llegar a los hosts remotos.

Limitar ciertos tipos de tráfico, como el tráfico SSH y SMTP, a determinados equipos es una configuración de firewall común. Mediante este tipo de regla, puede proteger los demás equipos de la red de infracciones de seguridad mediante esos protocolos o puertos.

Otros filtros de paquetes de firewall comunes incluyen la eliminación de paquetes entrantes con la opción Enrutamiento de origen establecida, la eliminación de protocolos de intercambio de información de enrutador y la

eliminación de paquetes entrantes con una dirección IP de origen interna. En su mayor parte, no se utilizan filtros que bloquean los paquetes salientes con una dirección IP de destino externa específica.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Reglas de firewall y NAT (PDF),
https://www.cisco.com/c/en/us/td/docs/video/cuvc/design/guides/desktop/5_5/cuvc_design_guide/firewallrules.pdf

---

Pregunta #111 de 131

Id. de pregunta: 1105252

Su organización necesita implementar un sistema mediante el cual los usuarios remotos puedan marcar a la red para transmitir pequeñas cantidades de datos de ventas. Desea que este sistema proporcione la máxima seguridad para evitar que los piratas informáticos se conecten a la red. ¿Qué tecnología debe implementar?

- ✗ **A)** Implemente un sistema de devolución de llamada con llamada en espera.
- ✗ **B)** Implemente el identificador de llamadas con desvío de llamadas.
- ✗ **C)** Implemente el identificador de llamadas con llamadas de tres vías.
- ✓ **D)** Implemente un sistema de devolución de llamada con identificador de llamada.

explicación

Debe implementar un sistema de devolución de llamada con identificador de llamada. El identificador de llamadas funciona junto con un sistema de devolución de llamada para proporcionar la máxima seguridad. El sistema de identificador de llamadas puede comprobar que el usuario está llamando desde un número de teléfono aprobado. Si se realiza un intento de conexión desde un número de teléfono no aprobado, la conexión se termina antes de que la seguridad se vea comprometida.

No debe implementar un sistema de devolución de llamada con llamada en espera. La implementación de llamadas en espera realmente causaría problemas con las conexiones remotas porque la implementación de llamadas en espera podría interrumpir una conexión correcta.

La implementación del identificador de llamada con cualquier otra tecnología no es adecuada en este escenario.

Un sistema de devolución de llamada es un mecanismo de protección de acceso remoto que limita las conexiones de acceso telefónico llamando al usuario a un número de teléfono predefinido o asegurándose de que el usuario

conectado desde un número de teléfono aprobado está utilizando el identificador de llamada.

La implementación más segura de un sistema de devolución de llamada implica la entrada de un ID de usuario y un número de identificación personal (PIN) cuando el usuario se conecta. Una vez que se verifica al usuario, el sistema de devolución de llamada devuelve la llamada al usuario como el número de teléfono que corresponde con el ID de usuario.

Algunas implementaciones de un sistema de devolución de llamada permiten al sistema volver a llamar a un usuario en función de la entrada del usuario en el momento de la conexión. Se trata de una implementación menos segura de la devolución de llamada y solo debe implementarse con entidades de confianza.

Cuando se utiliza la devolución de llamada para las conexiones de acceso telefónico remoto, un autor de la llamada puede atacar conectándose y, a continuación, no colgando. Si el autor de la llamada se autenticó previamente y ha completado la sesión, se seguiría manteniendo una conexión a la red remota. Además, un usuario remoto no autenticado puede mantener la línea abierta, actuando como si se hubiera producido la autenticación de devolución de llamada. Por lo tanto, se debe completar una desconexión activa en el lado de la línea del recurso informático.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Identificador de llamadas y devolución de llamada, http://technet.microsoft.com/en-us/library/cc778189(v=WS.10).aspx

---

Pregunta #112 de 131

Id. de pregunta: 1111742

Haga juego las descripciones a la izquierda con los problemas de seguridad inalámbrica correspondientes a la derecha.

{UCMS id=5688086354722816 type=Activity}

explicación

Los problemas de seguridad inalámbrica deben coincidir con las descripciones de la siguiente manera:

- Agrietamiento WEP/WPA - Los algoritmos matemáticos se utilizan para determinar la clave previamente compartida usada en el Punto de acceso.
- Warchalking - SSID y otros detalles de autenticación con respecto a una red inalámbrica se anotan en un lugar público prominente.
- Gemelo malvado - Un Punto de acceso rogue se configura con el mismo SSID que un Punto de acceso válido.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Glosario

Pregunta #113 de 131

Id. de pregunta: 1105193

Está explicando a un administrador junior sobre el escaneo de puertos. ¿Cuál de las siguientes afirmaciones es verdadera?

- ✗ **A)** Hay más de 65.000 puertos conocidos.
- ✗ **B)** Hay 1.024 puertos que son vulnerables en una red TCP/IP.
- ✗ **C)** Sólo los puertos UDP son vulnerables en una red TCP/IP.
- ✓ **D)** Hay más de 65.000 puertos que son vulnerables en una red TCP/IP.

explicación

En una red TCP/IP, hay más de 65.000 puertos que son vulnerables.

Los primeros 1.024 puertos son los puertos conocidos responsables de servicios conocidos, como el Sistema de nombres de dominio (DNS) y el Protocolo de configuración dinámica de host (DHCP). Los números de puerto comienzan en 0 y pasan por 65.535.

Los puertos TCP y UDP son vulnerables en una red TCP/IP.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

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

Introducción al escaneo de puertos, http://netsecurity.about.com/cs/hackertools/a/aa121303.htm

---

Pregunta #114 de 131

Id. de pregunta: 1113953

Está dando servicio a un equipo Windows que está conectado a la red Ethernet de su empresa. Debe determinar el fabricante de la NIC del equipo. Emita el comando ipconfig /all en la ventana del símbolo del sistema y registre la dirección MAC de la NIC, que es 00-20-AF-D3-03-1B.

¿Qué parte de la dirección MAC le ayudará a determinar el fabricante de la NIC?

- ✗ **A)** D3-03-1B
- ✗ **B)** AF-D3-03
- ✓ **C)** 00-20-AF
- ✗ **D)** 20-AF-D3

explicación

Una dirección de control de acceso a medios (MAC) es un número único de 48 bits que está integrado en una NIC que se conecta a una red Ethernet. Una dirección MAC se divide en seis octetos, cada uno de los cuales representa 8 bits de la dirección como un número hexadecimal de dos dígitos. Los tres primeros octetos de una dirección MAC son asignados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) a cada fabricante de tarjeta de interfaz de red (NIC); estos tres octetos identifican de forma única a cada fabricante de NIC. En este escenario, la secuencia 00-20-AF identifica el fabricante de la NIC como 3Com.

Otros fabricantes populares de NIC incluyen Cisco, a la que se le ha asignado la secuencia 00-00-0C, y Hewlett-Packard, a la que se le ha asignado la secuencia 08-00-09.

Los tres últimos octetos de una dirección MAC se utilizan para identificar de forma única cada NIC que produce un fabricante.

Originalmente, una dirección MAC se agregaba permanentemente a una NIC, pero los procesos de fabricación más recientes permiten que la dirección MAC se vuelva a configurar a un valor diferente. La capacidad de reconfigurar una dirección MAC permite a los administradores asignar direcciones de su elección. Sin embargo, el cambio de direcciones MAC debe hacerse con cuidado porque tener dos tarjetas con la misma dirección MAC en la misma red siempre causará problemas de comunicaciones.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, direccionamiento MAC

Dirección MAC IEEE, http://www.banalyzer.de/ban/HTML/P_LAYER2/Eng/P_lay207.html

Pregunta #115 de 131

Id. de pregunta: 1113946

Usted es un consultor. Uno de sus clientes le ha pedido que establezca hosts de red para su red. Esta red está conectada a Internet.

¿Cuál es el número máximo de hosts que esta empresa puede tener con una dirección de red de 208.15.208.0 utilizando la máscara de subred predeterminada?

- ✗ **A)** 62
- ✗ **B)** 16,382
- ✗ **C)** 16,777,214
- ✗ **D)** 510
- ✓ **E)** 254
- ✗ **F)** 65,534

explicación

Esta dirección IP es una dirección de clase C. Una red de clase C tiene 254 hosts por red. El número de hosts por red se calcula determinando el número de bits disponibles para el identificador de red.

En una dirección IP de clase C, los tres primeros octetos (24 bits) se asignan al ID de red y el último octeto, que es de ocho bits, se asigna al ID de host. Sabiendo que ocho bits están asignados al ID de host, puede determinar el número de hosts disponibles. Para calcular esto, convierta los ocho bits en binarios.

Para hacer esto con una calculadora, escriba ocho en la calculadora en formato binario, luego convierta ese número a decimal. El resultado debe ser 255 hosts por red. Dado que 255 está reservado para las difusiones de red, el número real de hosts posibles es 254.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, Clases IP

Calculadoras de red, http://www.subnetmask.info/

Pregunta #116 de 131

Id. de pregunta: 1105183

¿Qué procedimiento es un ejemplo de un control operativo?

- ✓ **A)** un control de copia de seguridad
- ✗ **B)** un sistema de gestión de bases de datos
- ✗ **C)** identificación y autenticación
- ✗ **D)** un plan de continuidad del negocio

explicación

Los controles de copia de seguridad, las pruebas de software y la administración antivirus son componentes de los controles de software operativos. Los controles de software operativos comprueban el software para averiguar si el software está comprometiendo la seguridad o no. Los procedimientos de recuperación de confianza, las pistas de auditoría, los niveles de recorte, la garantía operativa y del ciclo de vida, la administración de la configuración y los controles de medios y sistemas son ejemplos de controles operativos.

Un plan de continuidad de las actividades se refiere a los procedimientos emprendidos para hacer frente a la falta de disponibilidad a largo plazo de los procesos institucionales. La planeación de la continuidad del negocio difiere de la recuperación ante desastres. La recuperación ante desastres tiene como objetivo minimizar el impacto de un desastre.

Un sistema de gestión de bases de datos (DBMS) es una colección de software que gestiona y procesa grandes cantidades de datos almacenados en un formato estructurado. Un DBMS es un ejemplo de un control de aplicación y no un control operativo.

La identificación y autenticación de los empleados son ejemplos de controles técnicos que se definen bajo el control de administración de seguridad.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, SP 800-53 Rev. 4

Pregunta #117 de 131

Id. de pregunta: 1113970

¿Qué tecnología atacarán los phreakers?

✗ **A)** NAT

✗ **B)** cortafuegos

✓ **C)** VoIP

✗ **D)** Servidores web

explicación

Phreakers atacará voz sobre protocolo de Internet (VoIP). Los phreakers atacan generalmente el equipo PBX usado para las líneas telefónicas.

Los phreakers no atacan firewalls, servidores web o NAT. Los hackers atacan estas tecnologías. Los cortafuegos se utilizan para proteger las redes locales y crear zonas desmilitarizadas (DMZ). Los servidores web proporcionan servicios web a los usuarios, incluidos sitios web, sitios FTP y sitios de noticias. La traducción de direcciones de red (NAT) proporciona una solución de firewall transparente entre una red interna y redes externas.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cómo proteger su red VoIP, http://www.networkworld.com/research/2006/051506-voip-guide-security.html?ts

---

Pregunta #118 de 131

Id. de pregunta: 1105192

¿Qué métrica utiliza el protocolo de protocolo de información de enrutamiento (RIP) versión 2 para determinar la ruta de acceso de red?

✗ **A)** ancho de banda

✗ **B)** convergencia

✓ **C)** recuento de saltos

✗ **D)** demorar

explicación

Las versiones 1 y 2 del RIP utilizan el recuento de saltos como la métrica principal para determinar la ruta de red más deseable. Una métrica es un valor variable asignado a las rutas y es un mecanismo utilizado por los enrutadores para elegir la mejor ruta cuando hay varias rutas al mismo destino. Cada router atravesado por un paquete de la fuente al

destino constituye un salto. Cuanto menor sea el recuento de saltos, mayor será la preferencia dada a esa ruta de acceso. Con RIP, el recuento de saltos se limita a 15 saltos. Marcan a cualquier router más allá de este número de saltos como inalcanzable.

RIP no utiliza el retardo como su métrica principal. El retardo refiere al tiempo que un paquete del Internet Protocol (IP) toma viajar de la fuente al destino. Algunos protocolos dinámicos, tales como Interior Gateway Routing Protocol (IGRP), utilizan el retardo conjuntamente con otros parámetros para determinar la mejor trayectoria al destino.

RIP no utiliza el ancho de banda como su métrica principal. El ancho de banda refiere a la producción alcanzable máxima en un link. Esta métrica es utilizada como parte del cálculo métrico por algunos Routing Protocol, tales como IGRP y ENHANCED IGRP (EIGRP).

RIP no utiliza la convergencia como su métrica principal. La convergencia refiere a la cantidad de tiempo que toma para que las actualizaciones de ruteo sean propagadas a todo el Routers a través de la red.

RIP v1, RIP v2 e IGRP se consideran protocolos de vector de distancia. Open Shortest Path First (OSPF) es un protocolo de estado de vínculo. EIGRP es un protocolo híbrido equilibrado, también conocido como protocolo avanzado de vector de distancia. Los protocolos de ruteo de vector de distancia comúnmente difunden su información de tabla de ruteo al resto del routers cada minuto.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, RIP

Protocolo de información de enrutamiento TCP/IP,
http://www.tcpipguide.com/free/t_TCPIPRoutingInformationProtocolRIPRIP2andRIPng.htm

---

Pregunta #119 de 131

Id. de pregunta: 1111738

Haga coincidir cada descripción con el protocolo que mejor se adapte.

{UCMS id=5659415703191552 type=Activity}

explicación

Los protocolos deben coincidir con las descripciones de la siguiente manera:

- SSH - Un protocolo que utiliza un canal seguro para conectar un servidor y un cliente

- SSL : un protocolo que protege los mensajes entre la capa de aplicación y transporte
- SCP - Un protocolo que permite que los archivos se copien a través de una conexión segura
- ICMP - Un protocolo usado para probar e informar sobre la información de la trayectoria entre los dispositivos de red

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de Red, Redes IP

Pregunta #120 de 131

Id. de pregunta: 1113969

¿Qué es el envenenamiento por DNS?

✗ **A)** La práctica de muchos equipos que transmiten paquetes con formato incorrecto al servidor DNS para hacer que el servidor se bloquee

✗ **B)** la práctica de enviar continuamente mensajes de sincronización de un servidor DNS con paquetes falsificados

✗ **C)** La práctica de un equipo que transmite paquetes con formato incorrecto al servidor DNS para hacer que el servidor se bloquee

✓ **D)** la práctica de dispensar direcciones IP y nombres de host con el objetivo de desviar el tráfico

explicación

El envenenamiento por DNS es la práctica de dispensar direcciones IP y nombres de host con el objetivo de desviar el tráfico. La seguridad DNS configurada correctamente (DNSSEC) en el servidor DNS puede proporcionar validación de mensajes, lo que, a su vez, evitaría el envenenamiento de DNS.

Una inundación SYN es la práctica de enviar continuamente mensajes de sincronización de un servidor DNS con paquetes falsificados. Una inundación SYN puede ocurrir cuando se establece un gran número de conexiones se entreabiertas a un solo equipo.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y red, envenenamiento de caché DNS

Pregunta #121 de 131

Id. de pregunta: 1111739

Mueva los elementos correctos de la columna izquierda a la columna de la derecha para que coincida con el protocolo con el puerto predeterminado correcto.

{UCMS id=5693803627282432 type=Activity}

explicación

Los protocolos dados utilizan estos puertos predeterminados:

- Puerto 21 - FTP
- Puerto 110 - POP3
- Puerto 143 - IMAP
- Puerto 443 - HTTPS
- Puerto 3389 - RDP

FTP también utiliza el puerto 20, pero no se muestra en este escenario.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de Red, Redes IP

Pregunta #122 de 131

Id. de pregunta: 1105164

¿Qué tecnología de transmisión de radio especifica el estándar 802.11b?

✗ **A)** multiplexación por división de frecuencia ortogonal (MDFO)

✗ **B)** espectro ensanchado de salto de frecuencia (FHSS)

✗ **C)** espectro de banda estrecha

✓ **D)** espectro ensanchado de secuencia directa (DSSS)

explicación

El estándar 802.11b es una adición al estándar IEEE 802.11 para LAN inalámbricas. Mientras que la norma 802.11 original incluía tecnologías de transmisión de radiocomunicaciones de espectro ensanchado de secuencia directa (DSSS) y espectro ensanchado de salto de frecuencia (FHSS), la norma 802.11b especifica únicamente DSSS. Tanto el DSSS como el FHSS son tecnologías de espectro ensanchado, lo que significa que emiten señales a través de una gama de radiofrecuencias.

DSSS transmite una señal que es una combinación de una señal artificial y una real. El extremo receptor utiliza la señal adicional para mantener la integridad de la señal real cuando se experimenta interferencia. Ambos extremos deben acordar el método para generar la señal. DSSS ofrece un alcance superior, la capacidad de bloquear interferencias y una velocidad de transmisión de 11 Mbps.

El espectro de banda estrecha significa que las señales se transmiten a través de una frecuencia. Por ejemplo, una estación de radio transmite sus señales a través de una frecuencia o estación de radio.

FHSS transmite señales a través de frecuencias que cambian continuamente. Ambos extremos deben estar sincronizados para saber qué frecuencia se está utilizando. Las señales FHSS son difíciles de captar para los usuarios malintencionados. La velocidad de transmisión es de 1 Mbps.

La multiplexación por división de frecuencia ortogonal (MDFO) es un esquema de modulación utilizado con redes en el estándar IEEE 802.11a.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 4: Comunicación y seguridad de la red, 802.11b

---

Pregunta #123 de 131

Id. de pregunta: 1114742

La política de seguridad de su empresa establece que debe proporcionar protección contra los phreakers. ¿A qué entidad atacarían con mayor probabilidad?

✗ **A)** una red Token Ring

✗ **B)** una red Ethernet

✗ **C)** un dispositivo de acceso biométrico

✓ **D)** un sistema telefónico PBX

explicación

Lo más probable es que los phreakers ataquen un sistema telefónico de central de conmutación (PBX).

Los phreakers no atacarán una red Ethernet, una red Token Ring o un dispositivo de acceso biométrico.

Phreaking es el uso fraudulento de los servicios telefónicos. Un sistema telefónico PBX es en realidad un conmutador telefónico privado instalado en la ubicación de una empresa. Cuando se instala un sistema PBX, se deben tomar varias precauciones para reducir el fraude:

Cambie las contraseñas predeterminadas del sistema PBX.

Revise la factura de teléfono PBX regularmente.

Bloquear llamadas remotas después del horario comercial

Cambiar las contraseñas predeterminadas del sistema PBX se asegurará de que los phreakers no puedan entrar en el sistema utilizando la contraseña predeterminada dada en el momento de la instalación. Phreakers comúnmente utilizan este método para entrar en los sistemas.

Revisar la factura telefónica de PBX regularmente le permitirá reconocer el fraude más rápidamente. La factura telefónica de PBX mostrará una lista de las llamadas realizadas desde el sistema y la hora de las llamadas. Muchas veces, los phreakers utilizarán el sistema PBX después de horas para hacer llamadas telefónicas ilegales.

El bloqueo de llamadas remotas fuera de horario asegurará que los phreakers no puedan hacer llamadas telefónicas ilegales después de horas. La característica del acceso directo al sistema interno (DISA) de un sistema PBX permite a los usuarios marcar adentro al sistema PBX remotamente y hacer las llamadas telefónicas interurbanas dentro del sistema después de ingresar un código de acceso.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, PBX

Pregunta #124 de 131

Id. de pregunta: 1113957

Tiene dos redes inalámbricas en su edificio. Las redes inalámbricas no se superponen. Ambos utilizan acceso protegido Wi-Fi (WPA).

Desea asegurarse de que no se establezcan puntos de acceso inalámbrico no autorizados. ¿Qué debes hacer?

- ✗ **A)** Cambie las dos redes inalámbricas a WPA2.
- ✓ **B)** Complete periódicamente una encuesta sobre el sitio.
- ✗ **C)** Cambie las dos redes inalámbricas a WEP.
- ✗ **D)** Deshabilite las difusiones SSID para las dos redes inalámbricas.

explicación

Debe completar periódicamente una encuesta sobre el sitio para asegurarse de que no se establezcan puntos de acceso inalámbricos no autorizados. Las encuestas de sitio generalmente producen información sobre los tipos de sistemas en uso, los protocolos en uso y otra información crítica. Debe asegurarse de que los piratas informáticos no puedan usar encuestas de sitios para obtener esta información. Para protegerse contra encuestas de sitio no autorizadas, debe cambiar el identificador de conjunto de servicios (SSID) predeterminado y deshabilitar las difusiones de SSID. Inmediatamente después de descubrir un punto de acceso inalámbrico mediante una encuesta sobre el sitio, debe localizar físicamente el dispositivo y desconectarlo.

Para asegurarse de que no se establecen puntos de acceso inalámbrico no autorizados, no debe cambiar las dos redes inalámbricas a WPA2. Esto aumentaría la seguridad de las dos redes y evitaría que los hackers accedan a las redes. Sin embargo, no impediría que un atacante configurara un nuevo punto de acceso inalámbrico.

No debe deshabilitar las difusiones SSID para las dos redes inalámbricas para asegurarse de que no se establecen puntos de acceso inalámbrico no autorizados. La razón por la que deshabilitaría las transmisiones de SSID es para proteger una red inalámbrica de los piratas informáticos y para evitar encuestas de sitios no autorizadas. La desactivación de la difusión de SSID en una red existente NO PUEDE impedir el establecimiento de nuevos puntos de acceso inalámbricos.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, Encuestas de sitio

Pasos de la encuesta del sitio, http://www.wi-fiplanet.com/tutorials/article.php/1116311

Pregunta #125 de 131

Id. de pregunta: 1113964

¿Qué entidad de red utiliza una dirección IP pública y actúa como interfaz entre una red de área local e Internet?

✗ **A)** enrutador

✗ **B)** VPN

✗ **C)** cortafuegos

✓ **D)** NAT

explicación

La traducción de direcciones de red (NAT) actúa como la interfaz entre una red de área local e Internet utilizando una dirección IP pública.

Una VPN es una red privada que se implementa a través de una red pública, como Internet.

Un enrutador es un dispositivo de red que divide una red de área local en subredes más pequeñas. Los routers operan en la capa de red del modelo OSI (Capa 3). Mientras que un Firewall puede también ser un router, se refiere como Firewall cuando funciona para crear un DMZ.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de la red, direcciones IP públicas frente a direcciones IP privadas

Soluciones de seguridad de enrutador NAT, http://www.grc.com/nat/nat.htm

---

Pregunta #126 de 131

Id. de pregunta: 1105232

¿Qué declaración NO es verdadera con respecto a las transmisiones de multidifusión?

✗ **A)** Los protocolos utilizan direcciones de clase D.

✗ **B)** Se pueden transmitir clips de datos, multimedia, vídeo y voz.

✗ **C)** Un paquete se transmite a un grupo específico de dispositivos.

✓ **D)** Un mensaje tiene una dirección de origen y de destino.

explicación

En las transmisiones de multidifusión, un mensaje NO tiene una dirección de origen y de destino. Esta es una descripción de las transmisiones de unidifusión.

Los paquetes de transmisión de multidifusión se transmiten a un grupo específico de dispositivos. Los protocolos de multidifusión utilizan direcciones de clase D. Los clips de datos, multimedia, vídeo y voz se pueden transmitir mediante multidifusión. Es una transmisión de uno a muchos.

Los tres tipos de métodos de transmisión son: unidifusión, multidifusión y difusión.

Las transmisiones de unidifusión están pensadas para un solo dispositivo. Es una transmisión uno a uno.

Las transmisiones de difusión están pensadas para todos los dispositivos de una subred. Es una transmisión de uno a todos.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, unidifusión, multidifusión y difusión

---

Pregunta #127 de 131

Id. de pregunta: 1105145

Está configurando un equipo para conectarse a Internet. ¿Qué información debe tener un ordenador de una red antes de poder comunicarse con Internet?

- ✗ **A)** la clave pública, la dirección del servidor proxy y la dirección MAC del enrutador
- ✗ **B)** la dirección IP, la puerta de enlace predeterminada y el servidor DNS
- ✗ **C)** la dirección MAC del router, la máscara de subred y la dirección del servidor FTP
- ✗ **D)** la dirección IP, la máscara de subred y la dirección MAC del router
- ✓ **E)** la dirección IP, la puerta de enlace predeterminada y la máscara de subred

explicación

Antes de que cualquier equipo de una red pueda comunicarse con Internet, necesitará una dirección IP, una puerta de enlace predeterminada y una máscara de subred. Puede proporcionar esta información manualmente o puede utilizar un servidor DCHP para proporcionar automáticamente esta información.

La dirección IP es un número binario de 32 dígitos que se necesita para identificar cada dispositivo, o host, en Internet. La dirección IP proporciona una dirección lógica para cada dispositivo.

La máscara de subred se utiliza para bloquear una parte de la dirección IP. El propósito del bloqueo es distinguir el identificador de red del identificador de host. También se utiliza para identificar si la dirección IP del host de destino está en la subred local o en una subred remota.

El equipo no necesita ninguno de los otros componentes enumerados para comunicarse en Internet.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y seguridad de red, DHCP/BOOTP

Pregunta #128 de 131

Id. de pregunta: 1105245

¿Qué carga útil se produce mediante IPSec en modo de túnel con el protocolo AH?

- ✗ **A)** Un paquete encapsulado cifrado
- ✓ **B)** Un paquete encapsulado firmado digitalmente
- ✗ **C)** Un paquete no cifrado
- ✗ **D)** Un paquete sin tapar firmado digitalmente

explicación

El protocolo de seguridad de Internet (IPSec) en modo de túnel con el protocolo de encabezado de autenticación (AH) produce un paquete encapsulado que está firmado digitalmente. AH firma digitalmente un paquete para los propósitos de la autenticación. El modo de túnel encapsula un paquete dentro de otro paquete.

El Protocolo de seguridad encapsulador (ESP) cifra los paquetes IPSec. El modo de transporte envía paquetes IPSec entre dos equipos sin encapsular paquetes. AH y ESP funcionan en modo de transporte y modo túnel.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:

Implementar canales de comunicación seguros de acuerdo con el diseño

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, IPSec e ISAKMP

Comprensión del modo de túnel IPSec VPN y el modo de transporte IPSec- ¿Cuál es la diferencia?, http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

---

Pregunta #129 de 131

Id. de pregunta: 1114743

Debe implementar contramedidas de seguridad para protegerse de los ataques que se implementan contra su sistema PBX a través del mantenimiento remoto. ¿Qué directivas proporcionan protección contra los ataques de PBX de mantenimiento remoto?

un. Desactive las funciones de mantenimiento remoto cuando no sea necesario.

B. Utilice la autenticación segura en los puertos de mantenimiento remoto.

c. Mantenga los terminales PBX en un área cerrada y restringida.

d. Reemplazar o deshabilitar los inicios de sesión y contraseñas incrustados.

- ✗ **A)** opción c
- ✓ **B)** todas las opciones
- ✗ **C)** Sólo las opciones A y B
- ✗ **D)** sólo las opciones a, b y c
- ✗ **E)** opción b
- ✗ **F)** opción A
- ✗ **G)** Opción d

explicación

Debe implementar todas las directivas dadas para proporcionar protección contra ataques pbx de mantenimiento remoto.

Debe desactivar las características de mantenimiento remoto cuando no sea necesario e implementar una directiva en la que se requiera la interacción local para la administración remota.

Debe utilizar la autenticación segura en los puertos de mantenimiento remoto. Esto se asegurará de que el tráfico de autenticación no pueda ser comprometido.

Debe mantener los terminales PBX en un área restringida y bloqueada. Si bien se trata más bien de un problema de seguridad física, también puede afectar a los ataques de mantenimiento remoto. Si la seguridad física de un sistema PBX se ve comprometida, el atacante puede volver a configurar el sistema PBX para permitir el mantenimiento remoto.

Debe reemplazar o deshabilitar los inicios de sesión y las contraseñas incrustados. Estos generalmente son configurados por el fabricante para permitir el acceso de puerta trasera al sistema.

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, PBX

Análisis de vulnerabilidades de PBX, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

---

Pregunta #130 de 131

Id. de pregunta: 1105182

¿Cuál es la principal vulnerabilidad de seguridad del uso del Protocolo de transferencia de archivos (FTP)?

- ✗ **A)** Pueden producirse tanto cargas como descargas.
- ✗ **B)** Se permite el inicio de sesión anónimo.
- ✗ **C)** La sesión entre el cliente y el servidor no está cifrada.
- ✓ **D)** El ID de usuario y la contraseña se envían en texto no cifrado.

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

Subobsecución:
Implementar principios de diseño seguro en arquitecturas de red

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de red, FTP, FTPS, SFTP, TFTP

Pregunta #131 de 131

Id. de pregunta: 1113960

Haga juego las descripciones a la izquierda con los protocolos de encripción inalámbrica a la derecha.

{UCMS id=5657176146182144 type=Activity}

explicación

Los protocolos de cifrado inalámbricos deben coincidir con las descripciones de la siguiente manera:

- WEP - Utiliza una clave de 40 bits o 104 bits
- WPA/WPA2 Personal - Utiliza una clave previamente compartida de 256 bits
- WPA/WPA2 Enterprise - Requiere un servidor RADIUS

Objetivo:
Comunicación y seguridad de la red

Subobsecución:
Componentes de red seguros

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, Redes Inalámbricas