Redes

Unidad 4: Seguridad, Equipos y Medios de Transmisión.

1. ¿Cuáles son las principales características, ventajas y desventajas de los medios de transmisión por cobre, fibra óptica e inalámbricos?.

Los medios de transmisión son fundamentales para la comunicación moderna, y cada uno tiene sus propias características, ventajas y desventajas.

Medios de transmisión por cobre:

Características: Utilizan cables de cobre para transmitir señales eléctricas.

Ventajas: Costo relativamente bajo, fácil instalación y mantenimiento, y es compatible con tecnologías existentes.

Desventajas: Velocidad de transmisión limitada (hasta 1 Gbps), distancia limitada (hasta 100 metros sin amplificador) y susceptible a interferencias eléctricas.

Medios de transmisión por fibra óptica:

Características: Utilizan cables de fibra óptica para transmitir señales luminosas.

Ventajas: Velocidad de transmisión alta (hasta 100 Gbps), distancia larga (miles de kilómetros sin amplificador) y es resistente a interferencias eléctricas y enviromentales.

Desventajas: Costo más alto que los cables de cobre y tienen Instalación y mantenimiento más complejos

Medios de transmisión inalámbricos:

Características: Utilizan ondas radioélectricas para transmitir señales sin cables.

Ventajas: Fácil instalación y movilidad, no requiere cables o infraestructura física y tiene costo reducido en áreas remotas o difíciles de alcanzar.

Desventajas: Velocidad de transmisión limitada (hasta 1 Gbps), susceptible a interferencias ambientales (ruidos, obstáculos, etc.) y pueden ser interceptadas o hackeadas.

2. ¿Qué diferencias existen entre los dispositivos de red activos y pasivos? Menciona ejemplos de cada uno.

En una red, los dispositivos se clasifican en activos y pasivos según su función y capacidad para procesar y transmitir información.

Dispositivos de red activos:

Características:

Pueden procesar y transmitir información.

Tienen una inteligencia propia para tomar decisiones.

Pueden realizar tareas como routing, switching, firewall, etc.

Ejemplos:

Routers (directores de red): dirigen el tráfico de red hacia su destino.

Switches (interruptores): conectan dispositivos en una red local y dirigen el tráfico.

Firewalls (paredes de fuego): protegen la red de amenazas y ataques.

Servidores: almacenan y proporcionan acceso a recursos y servicios en la red.

Dispositivos de red pasivos:

Características:

No pueden procesar o transmitir información por sí mismos.

Solo reciben y transmiten información según las instrucciones recibidas.

No tienen inteligencia propia para tomar decisiones.

Ejemplos:

Cables: transportan señales eléctricas o ópticas entre dispositivos.

Conectores: permiten la conexión física entre dispositivos.

Cardes de red: permiten la conexión de un dispositivo a una red.

3. ¿Qué es un firewall, cómo funciona y qué tipos existen (hardware y software)?.

Firewall: ¿qué es y cómo funciona?

Los firewalls son un componente fundamental para la seguridad de las redes y dispositivos. Es importante elegir el tipo adecuado según las necesidades específicas

Un firewall es un sistema de seguridad de red que controla y gestiona el tráfico de red entrante y saliente en una red o dispositivo. Su función principal es proteger la red y los dispositivos conectados a ella de amenazas y ataques de seguridad, como virus, malware, ataques de phishing y otros tipos de ataques cibernéticos.

Cómo funciona un firewall:

a) Monitoreo del tráfico: El firewall monitorea todo el tráfico de red que entra y sale de la red o dispositivo.

b) Análisis de reglas: El firewall analiza las reglas de seguridad configuradas para determinar si el tráfico es seguro o no.

c) Bloqueo o permitido: Si el tráfico no cumple con las reglas de seguridad, el firewall lo bloquea. De lo contrario, lo permite.

Tipos de firewalls: hardware y software

Firewalls de hardware: Son dispositivos físicos que se conectan entre la red y los dispositivos que se quieren proteger.

Ejemplos:

Firewalls dedicados para redes empresariales.

Routers con firewall incorporado.

Firewalls de software: Son programas que se instalán en un dispositivo para controlar el tráfico de red.

Ejemplos:

Windows Defender Firewall (integrado en Windows).

Firewall de Linux (iptables).

Software de firewall comercial, como FortiGuard.

4. ¿Cómo contribuyen los antivirus a la seguridad de una red y cuáles son los más utilizados actualmente?.

Los antivirus son programas de software diseñados para detectar, prevenir y eliminar malware (software malicioso) en un dispositivo o red.

¿ Como Contribuyen a la seguridad de una red?

a) Detección de malware: Los antivirus analizan los archivos y programas que se ejecutan en la red para detectar patrones de malware conocidos.

b) Prevenimiento de ataques: Los antivirus pueden bloquear el acceso de programas maliciosos a la red y a los recursos del sistema.

c) Elimination de amenazas: Los antivirus pueden eliminar malware detectado en la red.

Los Antivirus más utilizados actualmente son:

Norton Antivirus: Ofrece protección contra malware, phishing y otros tipos de ataques.

Kaspersky Antivirus: Conocido por su eficacia en detectar y eliminar malware.

Avast Antivirus: Ofrece protección contra malware, phishing y otros tipos de ataques.

McAfee Antivirus: Conocido por su capacidad para detectar y eliminar malware avanzado.

Bitdefender Antivirus: Ofrece protección contra malware, phishing y otros tipos de ataques.

5. ¿Qué recomendaciones se deben seguir para crear y mantener contraseñas seguras en entornos personales y laborales?.

Las contraseñas son una de las barreras de seguridad más importantes para proteger los datos personales y laborales.

Algunas de las ecomendaciones más comunes pueden ser:

Longitud: Utiliza contraseñas de al menos 12 caracteres.

Complejidad: Incluye una combinación de:

* Letras mayúsculas y minúsculas.

* Números.

* Caracteres especiales (!, @, #, $, etc.).

Unicidad: Utiliza contraseñas únicas para cada cuenta o servicio.

No compartir: Nunca teñas que compartir tus contraseñas con nadie.

Utiliza un gestor de contraseñas: Considera utilizar un gestor de contraseñas como LastPass o 1Password para generar y almacenar contraseñas seguras.

Actualiza tus contraseñas regularmente**: Cambia tus contraseñas cada 60-90 días

No escribes tus contraseñas en papel**: Evita escribir tus contraseñas en papel o en lugares visibles.

6. ¿Qué son el malware, phishing, sniffing y spoofing? ¿Cómo afectan a la seguridad de una red y cómo se pueden prevenir?.

Malware (software malicioso): Es un Software diseñado para causar daño o obtener acceso no autorizado a una red o dispositivo. Puede causar pérdida de datos, interrupción de servicios, robo de información sensible, entre otros. Estos pueden ser Vírus, troyanos, ransomware, spyware, adware, entre otros.

Para prevenir se debe instalar antivirus y software de seguridad actualizado, evitar abrir archivos desconocidos, utilizar firewalls.

Phishing: Es la técnica de engaño para obtener información sensible, como contraseñas o datos personales. Puede causar pérdida de datos sensibles, robo de identidad, entre otros. Los métodos para emplearlos pueden ser Emails, mensajes de texto o llamadas telefónicas que solicitan información sensible.

Para prevenir se debe no responder a solicitudes de información sensible por email o mensaje de texto, verificar la autenticidad de las solicitudes.

Sniffing: Es una tecnica para interceptar y analizar el tráfico de red para obtener información sensible. Puede causar pérdida de datos sensibles, como contraseñas o información financiera. Sus Métodos son, utilizar software o hardware para capturar y analizar el tráfico de red.

Para prevenir se debe utilizar VPNs (Redes Privadas Virtuales), cifrar el tráfico de red, utilizar firewalls.

Spoofing: Es técnica para masquear como un dispositivo o usuario legítimo para obtener acceso no autorizado a una red. Puede causar pérdida de datos sensibles, interrupción de servicios, entre otros. Se obtiene cuando se utilizan direcciones IP falsas, direcciones MAC falsas, entre otros.

Para prevenir se debe utilizar autenticación de doble factor (2FA), verificar la autenticidad de las solicitudes.

7. ¿Cuáles son las buenas prácticas básicas para garantizar la seguridad en una red doméstica? ¿Y en una red empresarial?.

a) Configurar el router correctamente:

Cambia la contraseña predeterminada del router.

Activa la autenticación WPA2 (o WPA3 si es posible).

Configura el firewall del router.

b) Utilizar una red segura:

Utiliza una red Wi-Fi segura y cifrada.

Evita utilizar redes públicas o no seguras.

c) Instalar software de seguridad:

Instala un antivirus y software de seguridad actualizado en tus dispositivos.

Actualiza regularmente el software de seguridad.

e) Crear contraseñas fuertes:

Utiliza contraseñas únicas y fuertes para tus cuentas en línea.

Evita utilizar la misma contraseña para varias cuentas.

f) Actualizar dispositivos y software:

Actualiza regularmente tus dispositivos y software para patchar vulnerabilidades.

8. ¿Qué pasos básicos se deben seguir para configurar una red Wi-Fi de forma segura (SSID, cifrado, contraseña, etc.)?.

Configurar una red Wi-Fi de forma segura es crucial para proteger los dispositivos y datos.

Paso 1: Configurar el SSID (Nombre de la red)

Elige un nombre de red único y no relacionado con tu nombre o dirección. Asegúrate de que el SSID sea visible para que los dispositivos puedan encontrar la red.

Paso 2: Configurar el cifrado

Elige WPA2 (o WPA3 si es posible) como tipo de cifrado. Asegúrate de que el cifrado esté activado para proteger el tráfico de red.

Paso 3: Configurar la contraseña

Elige una contraseña fuerte y única para tu red Wi-Fi. Asegúrate de que la contraseña sea compleja y incluya letras mayúsculas y minúsculas, números y caracteres especiales.

Paso 4: Configurar la autenticación

Elige un método de autenticación como WPA2-PSK (Pre-Shared Key) o WPA2-802.1X.Se debe asegurar de que la autenticación esté configurada correctamente para proteger el acceso a la red.

Paso 5: Configurar el firewal

Activa el firewall del router para bloquear tráfico no autorizado. Se debe connfigurar las reglas del firewall para permitir sólo el tráfico autorizado.

Paso 6: Actualizar el firmware del router

Verifica si hay actualizaciones disponibles para el firmware del router. Actualiza el firmware para patchar vulnerabilidades.

Paso 7: Monitorear la red

Utiliza herramientas de monitoreo para detectar anomalías en la red. Realiza análisis de seguridad regulares para detectar vulnerabilidades.

9. ¿Cómo se puede proteger una red inalámbrica contra accesos no autorizados y ataques comunes?.

Proteger una red inalámbrica es crucial para evitar accesos no autorizados y ataques comunes.

Medidas de seguridad básicas

Cambiar la contraseña predeterminada del router: Cambia la contraseña predeterminada del router para evitar que se pueda acceder fácilmente.

Activar el cifrado: Activa el cifrado WPA2 (o WPA3 si es posible) para proteger el tráfico de red.

Configurar el firewall: Configura el firewall del router para bloquear tráfico no autorizado.

Actualizar el firmware del router: Actualiza el firmware del router regularmente para patchar vulnerabilidades.

Medidas de seguridad avanzadas

Implementar autenticación de doble factor (2FA): Implementa autenticación de doble factor para agregar una capa adicional de seguridad.

Utilizar un sistema de gestión de redes: Utiliza un sistema de gestión de redes para monitorear y controlar la red.

Configurar una lista de dispositivos autorizados: Configura una lista de dispositivos autorizados para acceder a la red.

Utilizar un sistema de detección de intrusiones: Utiliza un sistema de detección de intrusiones para detectar y responder a ataques.

10. ¿Cuál es la importancia de la educación del usuario final en la prevención de ataques informáticos y brechas de seguridad?.

¿Por qué es importante la educación del usuario final?

a) Conocer las amenazas: Los usuarios deben conocer las amenazas comunes, como phishing, malware y ransomware, para evitarlas.

b) Toma de decisiones informadas: Los usuarios deben tomar decisiones informadas sobre la seguridad de sus datos y dispositivos.

c) Prevenir errores humanos: La educación puede prevenir errores humanos que pueden llevar a brechas de seguridad.

d) Incrementar la conciencia: La educación incrementa la conciencia sobre la importancia de la seguridad informática.

Beneficios de la educación del usuario final:

a) Reducir los riesgos: La educación reduce los riesgos de ataques informáticos y brechas de seguridad.

b) Incrementar la seguridad: La educación incrementa la seguridad de los dispositivos y datos.

c) Mejorar la respuesta a incidentes: La educación ayuda a los usuarios a responder adecuadamente a incidentes de seguridad.