UD 3: Implantación de técnicas de acceso remoto. Seguridad perimetral

Introducción a la seguridad informática

Indice

Introducción

En esta unidad didáctica se tratarán técnicas seguras de acceso remoto en sistemas informáticos.

Con ello conseguiremos proteger la integridad de redes corporativas frente a acceso no autorizados y amenazas externas.

También trataremos los elementos de seguridad perimetral, las políticas de defensa y las configuraciones de redes privadas virtuales que permiten acceso seguro desde ubicaciones remotas.

Se profundizará en la instalación y configuración de servidores de acceso remoto y en los protocolos de autenticación necesarios para verificar la identidad de los usuarios.

Elementos básicos de la seguridad perimetral

Elementos básicos de la seguridad perimetral

Es un conjunto de estrategias y configuraciones diseñadas para proteger el límite entre una red privada y una red pública.

Su objetivo principal es establecer un perímetro de seguridad que sirva de barrera entre el entorno externo de los recursos e internos de la red, permitiendo el acceso seguro de los usuarios remotos y previniendo ataques y accesos no autorizados.

Routers frontera I

- Es el primer dispositivo en el perímetro de la red interna y sirve como puerta de enlace entre la red privada y la red pública (internet)
- Es la primera línea de defensa, donde se configuran las rutas de acceso y los filtros básicos para controlar el tráfico entrante y saliente
- Las funciones del router frontera son:
  - Filtrar el tráfico de red en función de las direcciones
  - IP de origen y destino
  - Facilitar la conexión entre diferentes redes mediante el enrutamiento de paquetes de datos
  - Implementar reglas básicas de seguridad para bloquear tráfico sospecho o proveniente de direcciones desconocidas

Routers frontera II

- Las configuraciones esenciales para mejorar la seguridad del router frontera son:
  - Filtrado de paquetes: a través de Access Control List (ACL) se permite o se bloquea el tráfico basado en IP, puertos o protocolos específicos. Es importante configurar la ACL en el router para controlar que tipo de tráfico puede acceder a la red interna.
  - Nerwork Address Translation (NAT): oculta las direcciones IP internas de la red al traducirlas a una única IP pública. Esto evita que atacantes puedan conocer la estructura interna de la red.
  - Redundancia y respaldo: en redes críticas, es recomendable contar con un router de respaldo para evitar la pérdida de conectividad en caso de fallo.

Routers frontera III

- Entre las buenas prácticas con routers frontera tenemos:
  - Actualizar el firmware del router regularmente para mitigar vulnerabilidades conocidas
  - Limitar el acceso al router a través de métodos de autenticación fuertes y restringir el acceso físico y lógico a usuarios autorizados.
  - Implementar un registro de eventos para monitorizar intentos de acceso no autorizados.

Cortafuegos I

- El cortafuegos o firewall es otro componente esencial en la seguridad perimetral.
- Su función es controlar el tráfico entre diferentes segmentos de la red, permitiendo o bloqueando el acceso según políticas de seguridad previamente configuradas.
- Los cortafuegos pueden ser de tres tipos:
  - Cortafuegos de filtrado de paquetes: opera en la capa de red y evalúa cada paquete de datos en función de criterios como la dirección IP, el puerto y el protocolo.
  - Cortafuegos de inspección de estado: analiza los paquetes individuales y el estado de las conexiones.
  - Cortafuegos de aplicación: trabajan en la capa de aplicación y son capaces de analizar el tráfico específico de aplicaciones como HTTP o SMTP, para detectar patrones maliciosos.

Cortafuegos II

- Las configuraciones básicas del cortafuegos son las siguientes:
  - Definir políticas de acceso detalladas que especifiquen qué tráfico es permitido y qué tráfico es bloqueado.
  - Configurar reglas de bloqueo para el tráfico entrante que no provenga de usuarios o aplicaciones autorizadas.
  - Habilitar el registro de eventos para monitorear el tráfico sospechoso y detectar intentos de intrusión.

Redes privadas virtuales (VPN)

- Son soluciones clave en la seguridad perimetral, especialmente en entornos que requieran acceso remoto seguro.
- Una VPN permite que los usuarios accedan a la red interna desde ubicaciones remotas de manera segura encriptando el tráfico entre el usuario y la red interna.
- Una empresa puede configurar una VPN SSL en su cortafuegos perimetral, permitiendo que los usuarios remotos accedan a la red a través de un navegador seguro sin necesidad de instalar un cliente VPN adicional.
- Al implementar una VPN en una organización, se configuran los servidores de VPN en la red interna y se distribuyen certificados de acceso a los usuarios. Esto asegura que los empleados puedan acceder a los recursos internos desde ubicaciones remotas sin comprometer la seguridad

Perímetros de red I

- Es el espacio de seguridad que rodea a los recursos internos de la red y los separa de la red pública.
- Dentro del perímetro se establecen controles que permiten monitorear y restringir el tráfico de manera efectiva.
- Los distintos tipos de perímetros en función de su arquitectura son los siguientes:
  - Zona desmilitarizada (DMZ por sus siglas en inglés De-Militarized Zone): es una subred separada del resto de la red interna mediante cortafuegos adicionales. Se utiliza para alojar servicios que deben estar accesibles desde la red pública, como servidores web o de correo mientras se mantienen asilada la red interna. Su ventaja principal es que permite exponer ciertos servicios al exterior sin comprometer la seguridad de la red interna.

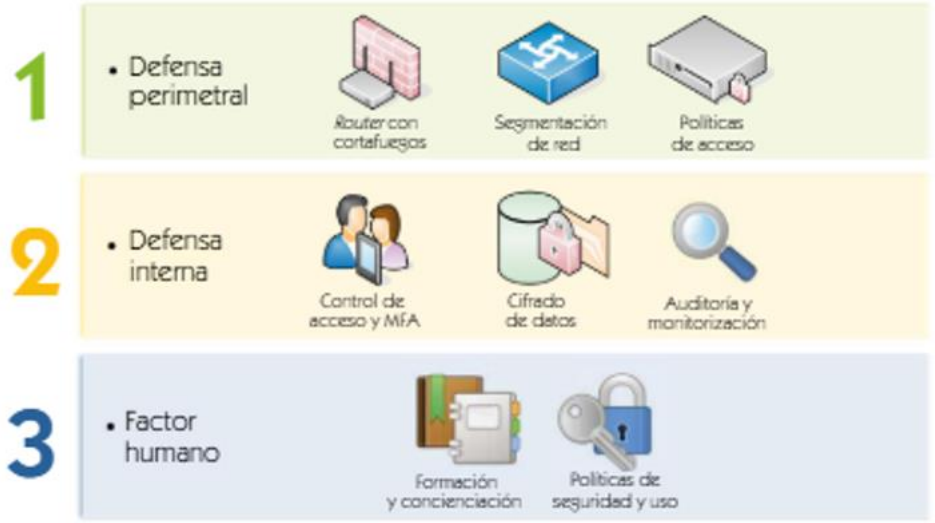
Perímetros de red II

- Arquitectura débil de subred protegida: es aquella en la que la red interna tiene pocos niveles de segmentación y se confía principalmente en un solo cortafuegos para proteger toda la red. Esta configuración puede ser suficientemente para organizaciones pequeñas, pero presenta riesgos en redes complejas o de gran tamaño.
- Arquitectura fuerte de subred protegida: implica una segmentación de la red en subredes adicionales, cada una protegida por un conjunto de cortafuegos y políticas de seguridad. Esto permite un control más granular del tráfico y limita los posibles daños en caso de un ataque en una subred específica.

Políticas de defensa en profundidad

Política de defensa en profundidad

- La defensa en profundidad es una estrategia de seguridad que se basa en implementar múltiples capas de protección para reducir la probabilidad de acceso no autorizado a los sistemas internos.
- Este enfoque asegura que, incluso si un atacante logra superar una capa de seguridad, habrá otras barreras que dificultarán su avance y mitigarán el impacto de una potencial intrusión.
- La defensa en profundidad se compone de tres áreas fundamentales: la defensa perimetral, la defensa interna y el factor humano.



Defensa perimetral I

- Constituye la primera línea de defensa de una red y se encarga de proteger el límite entre la red interna y el exterior. Esta capa incluye diversos dispositivos y tecnologías que se emplean para monitorizar, filtrar y restringir el tráfico entrante y saliente, minimizando la exposición a amenazas externas.
- Sus elementos clave son:
  - Cortafuegos: funcionan como filtros entre la red interna y las redes externas, estableciendo políticas de acceso que determinan qué tráfico es permitido. Su uso es fundamental para evitar accesos no autorizados y prevenir ciertos tipos de ataques.
  - Sistemas de detección y prevención de intrusos (IDS/IPS). Los IDS (Intrusion Detection Systems) y los IPS (Intrusion Prevention Systems) son herramientas que detectan y previenen actividades sospechosas o ataques conocidos en tiempo real. Mientras que el IDS se centra en alertar sobre actividades inusuales, el IPS actúa bloqueando de inmediato el tráfico identificado como malicioso.

Defensa perimetral II

- Segmentación de red y zonas desmilitarizadas (DZM). La segmentación de red separa los distintos componentes de la red en diferentes segmentos o subredes, permitiendo establecer diferentes niveles de acceso y seguridad. Las zonas desmilitarizadas, en particular, se utilizan para alojar servicios expuestos a la red pública, como servidores web o de correo, reduciendo la posibilidad de que un ataque en estos servicios comprometa la red interna.
- VPN (redes privadas virtuales): la VPN permiten establecer conexiones seguras entre usuarios remotos y la red interna, asegurando que los datos transmitidos sean encriptados y que el acceso esté restringido a usuarios autenticados. Esto reduce la probabilidad de interceptación de datos y ayuda a proteger el tráfico.

Defensa perimetral III

La configuración de una defensa perimetral eficaz se basa en:

- Definir políticas de acceso detalladas y actualizarlas regularmente en función de amenazas emergentes.
- Segmenta la red en zonas según el nivel de sensibilidad de los dataos y servicios alojados.
- Monitorear constantemente el tráfico de red y los registros de eventos para identificar y mitigar posibles amenazas.

En una organización que permite el acceso remoto se puede implementar una VPN para el acceso de usuarios externos utilizando un cortafuegos perimetral que solo permita conexiones a través de la VPN. Además, se podría añadir un sistema IDS para monitorizar cualquier actividad sospechosa que intente acceder al perímetro de la red.

Defensa interna I

Es una capa complementaria de la defensa en profundidad, diseñada para mitigar el impacto de un ataque en caso de que un intruso logre superar la defensa perimetra.

Se centra en la protección de los recursos y datos sensibles que residen dentro de la red corporativa.

Los componentes clave de la defensa interna son:

- Control de acceso a nivel de usuario y dispositivo: restringen el acceso a los datos y sistemas según los roles y permisos de cada usuario. Esto asegura que cada usuario solo acceda a los recursos necesarios para su función específica.
- Cifrado de datos: es importante realizarlo tanto en tránsito como en reposo. Si un atacante logra el acceso a la red interna, los datos estarán protegidos y no podrán descifrarlo sin las claves adecuadas.

Defensa interna II

- Autenticación multifactor (MFA). Añade una capa de seguridad adicional al proceso de autenticación, requiriendo que los usuarios proporcionen más de una forma de identificación.
- Listas de control de acceso (ACL) y segmentación interna. Las ACL se utilizan para limitar el acceso entre las diferentes partes de la red interna.
- Registros de auditoría y monitorización. Llevar un registro de los eventos de red interna permite analizar el comportamiento y detectar anomalías. Registra quién accedió a qué recursos y en qué momento, y es útil para identificar comportamientos maliciosos o no autorizados.

Defensa interna III

Para implementar la defensa interna se deben llevar a cabo las siguientes acciones:

- Aplicar un nuevo esquema de autenticación fuerte y limitar el acceso a datos según el principio de privilegio mínimo
- Cifrar los datos sensibles almacenados en la red interna para prevenir el uso indebido en caso de robo.
- Establecer políticas de segmentación interna y mantener un registro de auditoría completo.

En una organización de gran tamaño, la defensa interna se puede fortalecer mediante la implementación de una autenticación multifactor para todas las conexiones a sistemas sensibles, como servidores de bases de datos. Adicionalmente, se pueden cifrar los datos sensibles y registrar cada acceso a estos sistemas para detectar posibles accesos no autorizados.

Factor humano I

- Es una de las capas más importantes en la defensa en profundidad ya que los usuarios y los empleados juegan un rol crucial en la seguridad de la red.
- Los ataques de ingeniería social dependen en gran medida de la habilidad de los atacantes para manipular a las personas y obtener acceso a información confidencial.
- La formación y concienciación de los usuarios sobre buenas prácticas de seguridad son esenciales para evitar riesgos.
- El eslabón más débil de la cadena de seguridad es el factor humano.

Factor humano II

Las estrategias clave para proteger el factor humano son:

- Formación continua: es vital educar a los empleados sobre las políticas de seguridad cómo identificar ataques de ingeniería social y la importancia de mantener prácticas seguras, como no compartir contraseñas o datos sensibles.
- Concienciación sobre ingeniería social: los ataques de phishing y otros métodos de ingeniería social son una amenaza frecuente en la actualidad. Capacitar a los usuarios para que reconozcan estos ataques y no divulguen información a fuentes no verificadas ayuda a reducir la probabilidad de incidentes.
- Políticas de contraseñas seguras: la implementación de políticas de contraseñas fuertes (longitud, complejidad, periodicidad del cambio) contribuye a proteger los accesos. Es también recomendable utilizar autenticación multifactor.
- Simulaciones de ataques. Realizar simulaciones de ataques, como correos electrónicos de phishing o intento de intrusión, permite evaluar la reacción de los empleados y su preparación ante posibles ataques reales.
- Políticas de uso aceptable. Establecer políticas claras de uso aceptable de los recursos tecnológicos de la empresa, como limitar el acceso a sitios no seguros o restringir el uso de dispositivos de almacenamiento externos sin autorización.

Factor humano III

La implementación del factor humano en la seguridad se puede realizar con estas acciones:

- Invertir en programas de capacitación regulares sobre seguridad y prácticas seguras de manejo de información
- Establecer campañas de concienciación periódicas para recordar la importancia de la seguridad
- Realizar evaluaciones de conocimiento y simulaciones de ataques para medir el nivel de preparación del personal

Cifrado y tipos de VPN

Cifrado y tipos de VPN I

- Son una tecnología esencial para la conexión segura de usuarios remotos a redes internas.
- Las VPNs permiten establecer canales de comunicación seguros a través de redes públicas, como internet, de manera que los datos que circulan entre un usuario remoto y la red corporativa estén protegidos frente a accesos no autorizados.
- Para los administradores de redes, la implantación de VPN es una de las medidas de seguridad más efectivas para asegurar el acceso remoto.

Cifrados y tipos de VPN II

Las funciones de una VPN son las siguientes:

- Seguridad en el acceso remoto: las VPN protegen la información que envía a través de redes públicas mediante cifrado, garantizando que solo el usuario y el servidor de destino puedan leer los datos.
- Aislamiento de tráfico: permiten el uso compartido de la red pública sin que el tráfico de los usuarios remotos sea visible o accesible para terceros.
- Autenticación de usuarios: la VPN requieren métodos de autenticación que aseguran que solo usuarios autorizados puedan conectarse.

Beneficios y desventajas con respecto a las líneas dedicadas I

Beneficios:

- Reducción de costos: en comparación con las líneas dedicadas, como conexiones de fibra privada, las VPN son significativamente más económicas, ya que aprovechan la infraestructura de Internet sin requerir enlaces físicos costosos.
- Accesibilidad y flexibilidad: los usuarios pueden conectarse a la red interna desde prácticamente cualquier ubicación geográfica, siempre que dispongan de una conexión a Internet. Esto mejora la productividad y permite la movilidad de los trabajadores.
- Escalabilidad: a diferencia de las líneas dedicadas, donde cada enlace puede ser limitado y costoso de ampliar, las VPN pueden crecer conforme aumente el número de usuarios sin requerir cambios importantes en la infraestructura.
- Seguridad: mediante el cifrado y el uso de protocolos seguros, una VPN proteg los datos que se transmiten, reduciendo el riesgo de la interceptación y manteniendo la confidencialidad de la información.

Beneficios y desventajas con respecto a las líneas dedicadas II

Desventajas:

- Dependencia de la conexión a Internet: dado que las VPN dependen de la infraestructura de Internet, cualquier problema en la conexión pública puede afectar la calidad y la estabilidad de la comunicación.
- Latencia y rendimiento: a diferencia de las líneas dedicadas, donde el ancho de banda es constante, las VPN pueden experimentar fluctuaciones en el rendimiento debido a la congestión de la red pública.
- Riesgos de seguridad en configuraciones incorrectas: si no se configuran adecuadamente, las VPN pueden presentar vulnerabilidades que los atacantes pueden explotar, como configuraciones incorrectas en el cifrado o en la autenticación de usuarios.

Técnicas de cifrado: tipos de clave I

Cifrado de clave privada o cifrado simétrico:

- la misma clave se utiliza tanto para cifrar como para descifrar la información. Esto hace que el cifrado simétrico sea generalmente más rápido que el cifrado asimétrico.
- Es ideal para grandes volúmenes de datos
- Se requiere establecer un canal seguro para compartir la clave antes de la comunicación.
- Los algoritmos AES (Advanced Encryption Standard), DES (Data Encryption Standard) y Blow-fish son ejemplo de cifrado simétrico.
- Algunos ejemplos son:
  - Almacenamiento de datos
  - VPN

Técnicas de cifrado: tipos de clave II

Cifrado de clave pública o cifrado asimétrico:

- Utiliza un para de claves distintas: la clave pública y la clave privada. La clave pública es accesible a cualquier usuario, mientras que la clave privada es conocida únicamente por el destinatario de la comunicación:
  - Clave pública: compartida libremente y utilizada para cifrar mensajes o verificar firmas digitales.
  - Clave privada: mantenida en secreto y utilizada para descifrar mensajes o generar firmas digitales.
- Garantiza que, incluso si el mensaje cifrado es interceptado, no puede ser descifrado sin la clave privada.
- El algoritmo RSA es uno de los más utilizados en cifrado de clave pública. Otros ejemplos son DSA y ElGamal.
- Algunos ejemplos de uso son:
  - Certificados SSL/TLS
  - Firma digital

Técnicas de cifrado: tipos de clave III

Cifrado híbrido:

- Se usa para aprovechar las fortalezas de ambos métodos.
- Se utiliza en las VPN.
- Primero se utiliza el cifrado asimétrico para establecer la clave compartida de forma segura y después se usa el cifrado simétrico para el intercambio de datos, permitiendo tanto seguridad como eficiencia.
- Su funcionamiento es:
  - El remitente genera una clave de cifrado simétrica (clave de sesión) y la cifra usando la clave pública de destinatario.
  - El destinatario recibe la clave cifrada y la descifra con su clave privada.
  - Luego, ambas partes usan la clave simétrica para cifrar y descifrar el resto de la comunicación.

Técnicas de cifrado: tipos de clave IV

Cifrado híbrido:

- Muchos sistemas como SSL/TLS utilizan cifrado híbrido, combinando RSA (asimétrico) con AES (simétrico)
- Algunos ejemplos son:
  - Comunicaciones seguras en internet
  - Correos electrónicos seguros

Integridad, confidencialidad y autoría del cifrado asimétrico I

Con la arquitectura del cifrado asimétrico es posible garantizar tres pilares fundamentales en la seguridad de la información.

- Integridad: este cifrado asegura que los datos no han sido alterados durante su transmisión o almacenamiento. Esto se consigue utilizando firmas digitales:
  - Se genera un resumen (hash) del mensaje utilizando un algoritmo de resumen criptográfico (como SHA-256)
  - Este resumen se cifra con la clave privada de remitente, creando la firma digital.
  - El destinatario descifra la firma con la clave pública del remitente y compara el resumen obtenido con el generado a partir del mensaje recibido. Si coinciden, se garantiza la integridad.
- Confidencialidad: este cifrado asegura que solo los destinatarios autorizados puedan acceder el contenido de la información.
  - El remitente cifra el mensaje utilizando la clave pública del destinatario.
  - Solo el destinatario, con su clave privada, puede descifrar el mensaje.

Integridad, confidencialidad y autoría del cifrado asimétrico II

- Auditoría: el cifrado permite verificar que un mensaje o documento proviene de quien dice ser el remitente. Esto se consigue también mediante firmas digitales:
  - El remitente cifra el hash del mensaje con su clave privada, generando una firma digital.
  - El destinatario utiliza la clave pública del remitente para verificar la firma. Si la verificación es correcta, se garantiza que el remitente dice quien dice ser.

Propiedad	Mecanismo	Ejemplo de uso
Integridad	*Hash* + clave privada = firma digital	Verificar que un contrato digital no ha sido alterado.
Confidencialidad	Cifrado con clave pública del destinatario	Proteger un mensaje de acceso no autorizado.
Autoría	Cifrado con clave privada del remitente	Certificar la identidad de quien envía un mensaje.

Práctica para realizar en clase

Configura ejemplos básicos de cifrado con herramientas de línea de comandos como OpenSSL en una máquina con Linux.

Solución:

A) Cifrado simétrico con OpenSSL:

Paso 1: crea un archivo de texto llamado `mensaje.txt` con el siguiente mensaje: *"Este es un mensaje confidencial"*.

Paso 2: crea una clave privada para cifrar el mensaje, puede ser con un generador de contraseñas o una contraseña fuerte que quieras utilizar. Cambia `clave_simetrica` por tu clave.

Paso 3: utiliza OpenSSL para cifrarlo con una clave simétrica (AES) [se incluyen números de línea para facilitar la lectura, no introducir en la consola de comandos]:

```
1 openssl enc -aes-256-cbc -salt -in mensaje.txt -out mensaje_cifrado_simet.txt -k clave_simetrica
```

Paso 4: descifra el archivo cifrado:

```
1  openssl enc -d -aes-256-cbc -in mensaje_cifrado_simet.txt -out mensaje_descifrado.txt -k clave_simetrica
```

B) Cifrado asimétrico con OpenSSL:

Paso 1: genera un par de claves (pública y privada):

```
1 openssl genrsa -out clave_privada.pem 2048
2 openssl rsa -in clave_privada.pem -pubout -out clave_publica.pem
```

Paso 2: cifra `mensaje.txt` usando la clave pública:

```
1 openssl rsautl -encrypt -inkey clave_publica.pem -pubin -in mensaje.txt -out mensaje_cifrado_asim.txt
```

Paso 3: descifra el archivo cifrado usando la clave privada:

```
1 openssl rsautl -decrypt -inkey clave_privada.pem -in mensaje_cifrado_asim.txt -out mensaje_descifrado.txt
```

Tipos de VPN: VPN a nivel de enlace

- Operan en la capa de enlace de datos y crean una conexión directa entre los dos dispositivos o redes como si estuvieran físicamente conectados.
- Este tipo de VPN es ideal para conectar redes completas, ya que permite transmitir datos en bruto (frames) sin necesidad de encapsulación adicional en la red interna.
- Las características son:
  - Flexibilidad en la transmisión: los datos pueden enviarse directamente en el formato de la red local, lo que facilita la interoperabilidad entre diferentes redes.
  - Aplicación común en redes de área local (LAN): es ideal para conectar redes LAN en diferentes ubicaciones, creando una extensión virtual de la red privada.

Tipos de VPN: VPN a nivel de red

- Operan a nivel de capa de red (capa 3 del modelo OSI) y son la más utilizadas en la actualidad ya que permiten encapsular y cifrar el tráfico IP de extremo a extremo. Los protocolos más comunes son:
  - SSL (Secure Sockets Layer): este protocolo se usa para proteger conexiones web. En el contexto VPN, permite a los usuarios acceder de forma segura a aplicaciones web mediante el navegador, sin requerir la instalación de un cliente VPN adicional. La VPN SSL suelen emplearse en entornos corporativos, especialmente para accesos remotos desde dispositivos móviles.
  - IPSec (Internet Protocol Security): es un conjunto de protocolos que asegura el tráfico IP cifrándolo y autenticándolo a nivel de red. Es utilizado para la mayoría de las conexiones VPN empresariales y permite una alta compatibilidad con dispositivos de red. IPSec garantiza integridad, autenticación y confidencialidad y puede configurarse tanto en modo de transporte como en modo túnel.

Tipos de VPN: VPN a nivel de aplicación I

- Funciona en la capa de aplicación (capa 7 del modelo OSI) y se utilizan para cifrar datos específicos de aplicaciones, en lugar de todo el tráfico de la red.
- Estas VPN son útiles para usuarios que solo necesitan proteger ciertas aplicaciones o servicios y no toda la conexión.
- SSH (Secure Shell) es un protocolo que permite acceder de forma segura a sistemas remotos mediante una conexión encriptada.
- Aunque no es una VPN en el sentido tradicional, SSH se utiliza para crear túneles seguros que protegen las sesiones de usuarios. Con ella, los administradores pueden ejecutar comandos en servidores remotos de forma segura, una funcionalidad esencial para el mantenimiento y la gestión de sistemas en red.
- Un administrador de sistemas puede configurar un túnel SSH para acceder a un servidor web remoto y gestionar aplicaciones específicas si exponer toda la red a través de un VPN completo. Este tipo de acceso seguro es adecuado para tareas de mantenimiento y soporte remoto.

Tipos de VPN: VPN a nivel de aplicación II

- SSH también permite la transferencia segura de archivos mediante herramientas como SCP (Secure Copy Protocol) o SFTP (SSH File Transfer Protocol), lo que asegura que los datos transmitidos permanezcan cifrados.
- Las ventajas de VPN a nivel de aplicación son:
  - Cifrado específico: al operar a nivel de aplicación, se permite el cifrado de aplicaciones seleccionadas, en lugar de todo el tráfico de red, lo cual es útil en situaciones en las que solo es necesario proteger ciertas comunicaciones.
  - Flexibilidad: los usuarios pueden proteger solo las aplicaciones críticas sin afectar el resto de tráfico.

Servidores de acceso remoto

Servidores de acceso remoto

- Son equipos configurados específicamente para permitir el acceso seguro de usuarios externos a una red interna desde ubicaciones remotas.
- Su implementación y configuración son fundamentales para asegurar que el acceso a la red corporativa se seguro, controlado y cumpla con las políticas de la organización.
- Su uso es cada vez más común, especialmente con el aumento del teletrabajo y la necesidad de acceder a recursos en distintas ubicaciones.
- Dentro de este apartado veremos: protocolos de autenticación, configuración de parámetros de acceso y servidores de autenticación.

Protocolos de autenticación I

- Primer paso para controlar el acceso de usuarios remotos a la red corporativa.
- Existen varios protocolos de autenticación:
  - PAP (Password Authentication Protocol): es el método más básico ya que el nombre de usuario y la contraseña se envían sin cifrar. Es muy fácil de implementar, pero es muy vulnerable a la intercepción y robo de credenciales.
  - CHAP (Challenge Handshake Authentication Protocol): mejora la seguridad con respecto a la opción anterior ya que cifra la contraseña antes de enviarla por la red. Utiliza un proceso de autenticación en tres pasos, donde el servidor envía un desafío (challenge) al cliente, y el cliente responde con una respuesta encriptada. Es más segura que la anterior, pero puede no ser suficiente en entornos donde se requieren una autenticación robusta.

Protocolos de autenticación II

- RADIUS (Remote Authenticatio Dial-In User Service): protocolo de autenticación centralizada que permite la gestión y verificación de credenciales desde un servidor independiente. Es usado en redes de gran tamaño para autenticar y autorizar usuarios. Permite la autenticación centralizada y es compatible con múltiples dispositivos y servicios de red, pero requiere una configuración muy avanzada y depende de un servidor RADIUS dedicado.
- Kerberos: utiliza claves de cifrado simétrico y un servidor de autenticación centralizado. Es común en entornos Windows y UNIX. Es seguro y evita el envío de contraseñas a través de la red, pero su implementación es más compleja que la de otros protocolos y requieren sincronización horaria estricta entre cliente y servidor.
- Multi-Factor Authentication (MFA): combina múltiples métodos para validar la identidad del usuario (contraseñas, token o reconocimientos biométricos). Aumenta significativamente la seguridad, pero es menos conveniente para los usuarios.

Configuración de parámetros de acceso

- Es crucial para establecer el nivel de seguridad y personalización en el servidor de acceso remoto.
- Para ello hay que:
  - Definir políticas de acceso basadas en el rol de usuario (administrador, empelado, externos,…) especificando los niveles de permisos según el tipo de usuario.
  - Limitaciones geográficas y horarias: puede ser conveniente restringir el acceso remoto a ciertas ubicaciones geográficas o franjas horarias.
  - Restricciones por dirección IP: permitir el acceso solo desde direcciones IP específicas o rangos de IP predefinidos.
  - Reglas de autenticación y autorización: para gestionar los permisos de acceso hay que configurar las reglas de autenticación. Se realizan por grupos de usuarios.
  - Tiempo de inactividad y cierre de sesión automáticas: se recomienda establecer un tiempo de inactividad tras el cual el usuario es desconectado del sistema.

Servidores de autenticación I

- Son componentes esenciales ya que validan la identidad de los usuarios antes de permitirles el acceso a la red.
- Integran y gestionan los métodos de autenticación y se comunican con otros servidores de red para autorizar el acceso.
- Algunos tipos son:
  - RADIUS (visto anteriormente): servidor de autenticación centralizado que permite autenticar usuarios de forma segura y eficiente en entornos grandes y distribuidos.
  - TACACS+ (Terminal Access Controller Access-Control System Plus): alternativa a RADIUS, desarrollado por Cisco que permite mayor granularidad en el control de permisos y autenticación. Permite la autenticación y la autorización por separado, lo que mejora la seguridad.
  - Active Directory (AD): es uno de los métodos más utilizados en redes Windows. Permite gestionar usuarios y permisos en la red.
  - LDAP (Lightweight Directory Access Protocol) permite consultar y modificar servicios de directorio con el AD. Es común su uso en entornos heterogénos para gestionar y autenticar usuarios.

Práctica

- Configurar un servidor RADIUS en un sistema Linux e intégralo con un cliente para autenticar usuarios.
- Para ello instala en el servidor, el paquete freeradius y asegúrate de que el servidor escuche en la dirección IP correcta (para escuchar tiene que estar configurada en todas las interfaces en la dirección 0.0.0.0 o en la IP específica del servidor.
- En el caso del cliente tienes que instalar también el paquete freeradius y configurar el cliente RADIUS. Para ello tienes que editar el archivo clients.conf dentro de freeradius y agregar la configuración del servidor que has configurado en el punto anterior.
- Prueba la autenticación utilizando el comando radtest. Si la configuración es correcta, deberías ver un mensaje que indica que la autenticación fue exitosa.

Servidores de autenticación II

Una vez integrado el servidor de autenticación con el acceso remoto, es necesario establecer políticas y funciones clave como:

- Configuración de políticas de autenticación: debe configurarse el servidor para que solicite la autenticación de los usuarios a través del servidor designado (RADIUS o LDAP)
- Sistemas de log y auditoría: es importante que el servidor de autenticación almacene registros de acceso para auditoría y control, registrando intentos de acceso y el resultado de cada autenticación.
- Configuración de políticas de bloqueo: el servidor de autenticación debe establecer políticas de bloqueo automático para usuarios que intentan acceder repetidamente sin éxito. Esto ayuda a prevenir ataques de fuerza bruta.

Servidores de autenticación II

Procedimientos de autenticación multifactor:

- Token de un solo uso (OTP): añade una capa adicional de seguridad, ya que el usuario debe ingresar un código generado de forma dinámica para completar el acceso.
- Dispositivos biométricos: algunos servidores de autenticación permiten la integración de dispositivos biométricos como parte de la autenticación multifactor.
- El acceso a varios servicios puede ser unificado mediante estos sistemas:
- La autenticación federada: permite que los usuarios puedan utilizar sus credenciales en múltiples sistemas a través de diferentes aplicaciones.
- Single Sing-On (SSO): permite a los usuarios autenticarse una vez para acceder a varios sistemas. Hay que tener cuidado para no comprometer la seguridad.