CONEXIÓN Y GESTIÓN DE RECURSOS EN RED

6.1 Seguridad en las redes informáticas

En los Sistemas informáticos hay que preservar la integridad, la disponibilidad y la privacidad de la información.

La seguridad la podemos distinguir en dos tipos:

- Medidas de seguridad activa: Se utilizan para detectar las amenazas y generar acciones contra ellas. Como el uso del control de acceso o el sistema de detección de intrusos.
- Medidas de seguridad pasivas: Intentan que el impacto sea menor una vez producido el ataque, como tener una buena pacificación de las copias de seguridad.

6.1.1 Control de acceso

Se puede limitar el el acceso de algún usuario a algún equipo de la red, se pueden permitir y denegar varias opciones como la de ejecutar mandos…

También se pueden encontrar medidas de acceso físico a los edificios donde se encuentran los sistemas como los CPD con controles de acceso.

6.1.2 Cortafuegos (firewall)

Se encargan de proteger los sistemas o las redes informáticas de las amenazas que pueden llegar a trabes de la red, impidiendo el acceso no autorizado y permitiendo el tráfico autorizado tanto entrante como saliente.

Cortafuegos hardware

Están conectados a el router o pueden estar integrados en el. Una de las utilidades de los cortafuegos es crear las DMZ dentro de una red.

DMZ o Zona Desmilitarizada

Es una zona dentro de una red aislada de el resto de la red. En esta están los servidores y los recursos de la red que podrán ser accesibles desde internet.

La DMZ se puede conectar con el exterior, pero no con la red interna que esta fuera de su zona; sin embargo, los equipos de dentro de la red si pueden acceder a las DMZ.

Cortafuegos Software

Linux y Windows tren incorporados varias aplicaciones de cortafuegos como en Linux (ufw, iptables, nftables) y en Windows (Windows Defender).

Cortafuegos en Linux

Se puede gestionar con el comando ufw. Esta herramienta utiliza las iptables su sucesor las nftables que son el firewall en Linux.

Cortafuegos en Windows

Se puede acceder desde diferentes sitios, tanto a las propiedades básicas como a la las avanzadas.

- Firewall y protección de red = Configuración → Actualización y seguridad → Seguridad de Windows.
- Firewall de Windows Defender = Es accesible desde el Panel de control o escribiendo lo desde el Inicio
- Windows Defender Firewall con seguridad avanzada = Escribiendo **wf.msc** en Inicio o en Ejecutar. Dentro se ven los perfiles de las redes privadas y de las redes publicas o invitadas.

Dentro de cada perfil se pueden ver los siguientes elementos:

- Estado de firewall de Widows defender: puede estar activado o desactivado
- Conexiones entrantes: se pueden bloquear excepto las admitidas.
- Redes privadas y publicas o invitadas: En una red privada se conocen a los dispositivos que esta en ella. Y en las publicas o invitadas se puede conectar cualquier dispositivo
- Estado de notificación: si el usuario quiere recibir una notificación cuando se bloquee una aplicación.

Detalles:

- En activar o desactivar el Firewall de Windows defender se pueden activar o desactivar el firewall a de mas de configurar el bloqueo de las conexiones entrantes y las notificaciones.
- La red del dominio es aquella que tiene un controlador de dominio dentro de Active Directory.
- En Configuración avanzada se pueden poner reglas para cada tipo de red: estas se pueden aplicar dentro de un dominio, perfil publico o perfil privado. Estas reglas pueden ser de entrada, de salida o de seguridad de conexión entre dos equipos.

6.1.3 Sistemas de detección de intrusión

Son herramientas que monitorizan y detectan las intrusiones, como los sistemas IDS, IPS y SIEM. Los tres son sistemas para proteger las comunicaciones pero funcionan de manera distinta.

- **IDS:** Sistemas que detecta accesos no autorizados a equipos o a redes.
- **IPS:** Protege al sistema de la intrusión. Se encarga de monitorizar las entradas y salidas en busca de ataques cibernéticos y de malware.
- **SIEM:** Sistemas que analiza los eventos de seguridad en una red. Se complementa con los anteriores y centraliza la información, descartando falsos positivos.

6.1.4 Herramienta de cifrado y seguridad

Hay herramientas que permiten encriptar archivos y carpetas, así como la información que viaja por la red. Utilizan algoritmos de cifrado.

- OpenSSL: Es un paquete que ofrece herramientas de seguridad para TLS y SSL.
- LibreSSL: Es una bifurcación de OpenSSL. Ofrece varias utilidades, como libcrypto, libssl o libtls que son bibliotecas de criptografías y utilidades para TLS

Comando:

openssl req → Se utiliza para crear certificados auto firmados.

OpenSSH

Paquete que ayuda a la seguridad ofreciendo herramienta SSH y otras aplicaciones para cifrar comunicaciones en una red.

Certificados

Se utilizan en ciertos sitios, como en servidores web para garantizar la identidad de el servidor.

Existen compañías dedicadas a ofrecer y validar certificados. El usuario también puede crear certificados pero al no estar validado por una autoridad de certificación es posible tener problemas al no reconocer que es un certificado.

Hay diferentes tipos de certificados pero la mayoría se basan en el estándar X.509 v3.

Los certificados generan una clave publica y una privada. LA clave privada la maniene en el servidor, mientras que la publica se envía a el cliente y asegura la identidad del servidor.

Las extensiones o formatos son : .CSR, .KEY, .CRT, .CERT, .CER, .PEM… Es posible convertir un tipo de certificado en otro.

En un sitio web podemos ver si es seguro si tiene el candad en la barra de búsqueda.

Comprobación de certificados instados en Windows

- Ejecutar certmgr.msc para ver los certificados del usuario actual
- Ejecutar certlm.msc para ver los certificados del usuario actual

Comprobación de certificados instados en Linux

En Linux los certificados están en /etc/ssl/certs. Aquí están con el fichero ca-certificates.crt.

Si queremos configurar una app para usar un certificado de una autoridad certificadora tenemos que añadir el certificado al archivo ca-certificates.crt

Let's Encrypt

Herramienta con la que se puede conseguir un certificado digital de forma gratuita y valido para usarlo en web con HTTPS.

6.1.5 Configuración del router

Para acceder al router necesitamos tener la dirección IP, el nombre de usuario y la contraseña.

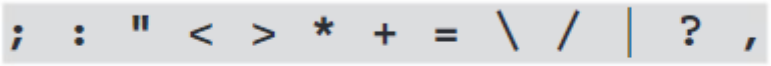
Si es una red pequeña el router también es el que ofrece la salida a la red a través de un un módem, este puede tener integrado el firewall y un servidor DHCP. Por defecto tiene la IP 192.168.1.1 o 192.168.0.1 aunque se puede modificar.

Con los comandos tracert (Windows) o traceroute (Linux) podemos ver el camino que siguen los datos.

6.2 Recursos compartidos

6.2.1 Identificación de los equipos dentro de una red.

Los equipos dentro de una red deben tener una dirección IP única y un nombre único. El nombre tiene que tener 15 caracteres máximo y o se pueden utilizar los siguientes caracteres:



Los equipos dentro de una red se añadirán a un grupo de trabajo o a un domino. Los grupos de trabajo no tienen administrador y el dominio si.

- Los grupos de trabajo son mas útiles en redes pequeñas. Los ordenadores tienen que estar en la misma red y la administración se hará en cada equipo.
- En los dominios existe una cuenta de Administrador y un equipo que hará de controlador de dominio. Los usuarios podrán iniciar sesión en cualquier equipo del dominio si están autorizados para ello.

Los equipos dentro de una red pueden tener: un nombre de host o de equipo, o un nombre completo o FQDN "tiene dos partes: la parte del host y el nombre de dominio".

Para acceder al equipo por una red local organizada en grupos de trabajo se accede mediante la IP o el nombre del host.

6.2.2 Conexión de ordenadores en red

Para conectar dos ordenadores en red es necesario que se vean a través de ella. Para eso usamos el comando **ping** este comando enviá y recibe paquetes mientras no se le corte el proceso. Por defecto envía 4 paquetes.

6.2.3 Compartición de recursos en red

Es una de las principales ventajas de las redes informáticas. Al compartir recursos en red podemos acceder a ellos con mayor facilidad. Esto evita tener información duplicada.

Windows

Se comparte la carpeta por red. “Como siempre”

Linux

Hay que instalar el servicio samba si no esta instalado para poder compartir los recursos con el protocolo SMB/CIFS.

Para compartir la carpeta le daremos encima de esta al botón derecho y pulsaremos la opción de Recurso compartido de red local.

6.3 Lista de control de acceso

Las ACL sirven para ampliar el control sobre los permisos asignados y el acceso de los usuarios a diferentes recursos tanto locales como a través de la red.

Estas se pueden utilizar para ampliar los permisos básicos en los sistemas de archivos.

A los usuarios que acceden al sistema a través de la red también se le pueden aplicar las ACL.

Las listas de control de acceso pueden ser:

- DACL: indica que usuarios y grupos pueden utilizar un objeto y con que permisos.
- SACL: indica que accesos al objeto serán auditados por el sistema.

Una ACL contiene una lista de ACE que indica que permisos tendrá cada usuario. Los permisos se pueden permitir, denegar y auditar a un usuario o grupo de usuarios y podrán ser explícitos o heredados.

Linux

Getfacl → Obtiene la ACL de un fichero o directorio.

Setfacl → Modifica o elimina la ACL de un fichero o directorio.

Windows

En Windows el sistema de archivos debe ser NTFS no se puede implementar en el sistema FAT.

Las ACL se pueden gestionar en la pantalla Seguridad o con el comando

icacls → Este crea, muestra y modifica las listas de acceso DACL para archivos y directorios. También puede realizar copias de las mismas y restaurarlas.

También se pueden utilizar los comandos de PowerShell Get-Acl y Set-Acl, que obtienen o cambian las listas de control de acceso de un recurso.

6.4 Acceso Remoto

Permiten realizar acciones sobre un equipo accediendo desde otro, bien para trabajar con el o para hacer trabajos de administración.

6.4.1 Escritorio remoto

Con el escritorio remoto se puede acceder y trabajar de modo grfico desde un ordenador remoto como si estuviera trabajando con ese ordenador física mente.

Los protocolos para trabajar con los escritorios remotos son RDP en Windows(XRDP si se quiere acceder desde Linux) y VNC que es el protocolo para utilizar el escritorio remoto en Linux.

6.4.2 Conexión remota

Se puede acceder de forma remota a otro equipo utilizando conexiones de solo tipo texto, para ejecutar algún comando o tareas de administración.

Es lo ams recomendable ya que es mas rapido que acceder mediante el escritorio remoto y porque lo mas probable es que si nos conectamos a un servidor no tenga entorno grafico.

Telnet

Trabaja sobre la capa de aplicación del protocolo TCP/IP, por defecto utiliza el puerto 23. Solo se utiliza para acceder en modo texto. Al trabajar los datos circulan de manera no cifrada, por eso se ha sustituido por SSH.

SSH

Trabaja en la capa de aplicación del protocolo TCP/IP, utiliza el puerto 22 y sustituyó a Telnet, ya que la comunicación es segura y la información viaja de manera cifrada. Para poder acceder a un sistema mediante SSH, hay que tener instalado y en funcionamiento el corta fuego del servidor SSH.

APLICACIONES PARA EL ACCESO REMOTO

PuTTY

Esta herramienta permite acceder a equipos remotos, utilizando los protocolos Telnet, SSH o Rlogin.

6.4.3 Copias remotas

Se utilizan para realizar copias de archivos en equipos remotos, o copiar archivos desde un equipo remoto.

rsync → Realiza copias rápidas, en carpetas remotas y locales.

scp → Copia archivos entre dos máquinas de una red, de forma segura, utilizando el protocolo SSH.