Bloque 6: Recursos en red

Contenido

Introducción

Cada vez más, se ofrecen recursos en red para intentar no duplicar servicios o aplicaciones y poder controlar las aplicaciones en red. Un ejemplo es: Tener una impresora para cada dispositivo vs tener una impresora en red para todos los dispositivos.

En Windows, vamos a estudiar aspectos que determinan cómo un usuario inicia sesión, además de sus privilegios específicos una vez se han autentificado. Esto utiliza los GPO (Archivos y plantillas de configuración de política de grupos). Se utiliza la Consola de Administración de Microsoft.

También se van a estudiar los servidores, cómo configurarlos, herramientas de Software para compartir y gestionar el acceso a los recursos.

Se van a ver a parte las herramientas de conexión remota, ya que se van a acceder a servidores que no tienen una conexión física directa (muy útil actualmente para teletrabajo)

Las herramientas de seguridad complementarias, como el cifrado, ya vaya a ir sobre archivos o almacenamiento, o los cortafuegos, que controlan el tráfico entrante y saliente de la red. Además, están los sistemas de detección de intrusos (IDS), y las herramientas de administración y análisis.

Permisos

Cuando un usuario intenta acceder al sistema, primero tiene que autenticarse, generalmente a través de un usuario y una clave.

Una vez dentro, el usuario accede a los recursos siempre que esté autorizado. Para esta parte, se usan los permisos. Los permisos son herramientas de protección de los recursos.

Los objetos son estructuras de datos que representan recursos, como archivos, carpetas, procesos, impresoras… Estos recursos están restringidos por medio de los permisos.

Los permisos definen el tipo de acceso concedido a un usuario o un grupo de usuarios a unos recursos concretos. Un usuario tiene ciertos permisos, pero si pertenece a un grupo, también tendrá asignado esos permisos de grupo.

En Windows, los recursos constan de un propietario, que concede o deniega los permisos de usuarios o grupos. Se conoce como principios de seguro (Security Principals), identificados con un SID.

El propietario de un objeto es su creador, y puede modificar, siempre que posea permiso para ello, quién va a pasar el propietario. Ese permiso se conoce como “Toma de Posesión”.

Por defecto, los administradores de sistema y los propietarios de sistema van a tener ese permiso. Por otro lado, el propietario va a tener control total sobre el objeto. Las acciones y los permisos que pueden realizar los security principals van a tener diferentes puntos dependiendo del tipo de objeto: modificar, cambiar propietario, eliminar y lectura como típicos en todos.

Permisos básicos NTFS:

- **Carpetas:**
    - Mostrar contenido en la carpeta: Listar su contenido

    - **Lectura:** Ver el contenido de la carpeta, permisos, propietario y atributos
    - **Escritura:** Posibilita crear nuevos archivos y su carpeta, ver propietario, modificar atributos y permisos
    - **Lectura y ejecución:** Permite navegar por las subcarpetas más permisos de lectura y mostrar contenido
    - **Modificar:** Permite eliminar la carpeta más los permisos de lectura y ejecución
    - **Control total:** Permite todos los permisos previos además de cambiar permisos y tomar posesión.
    - **Permisos especiales.**
- **Archivos:**
    - **Lectura:** Permite ver el archivo, propietarios, permisos y atributos
    - **Escritura:** Permite modificar el contenido y atributos, asi como ver el propietario, permisos y atributos
    - **Lectura y ejecución:** Permite ejecutar el archivo mas el permiso de lectura
    - **Modificar:** Permite modificar y eliminar archivos mas permisos de lectura y ejecución
    - **Control total:** Permite todos los permisos previos además de cambiar permisos y tomar posesión.
    - **Permisos especiales**

Permisos especiales:

- **Atravesar carpeta/ejecutar archivos:** Permite moverse por carpetas, aunque no tenga permiso de acceso, y permite ejecutar archivos
- **Mostrar carpetas/leer datos:** Permite ver el nombre de archivos y subcarpetas, y permite ver el contenido de los archivos
- **Leer atributos:** Ver atributos de un archivo o carpeta como lectura y oculto
- **Leer atributos:** Permite ver los atributos extendidos
- **Crear archivos/escribir datos:** Permite crear archivos y modificar el contenido de archivos
- **Crear carpetas/anexar datos:** Permite crear carpetas y añadir datos sin sobrescribir otros en archivos
- **Escribir atributos:** Modificar atributos
- **Escribir atributos extendidos**
- **Eliminar**
- **Permisos de lectura:** Permite leer los permisos
- **Cambiar permisos**
- **Tomar posesión**

Un usuario tiene sus permisos propios por ser usuario y, además, los permisos asignados por ser miembro de un grupo.

Los permisos que no estén otorgados explícitamente, están denegados

La denegación de permisos tiene prioridad sobre la concesión (Si hay dos grupos que se contradicen, tiene prevalencia lo más restrictivo)

Los permisos sobre ficheros prevalecen sobre los de carpeta

Permisos en red y locales

En Windows se pueden compartir archivos o carpetas y asignar **permisos de red**. Igual que de forma local, se aplican los más restrictivos si hay conflicto.

Al compartir, dándole al uso compartido avanzado, se establecen una serie de permisos a usuarios o en general (**Todos**).

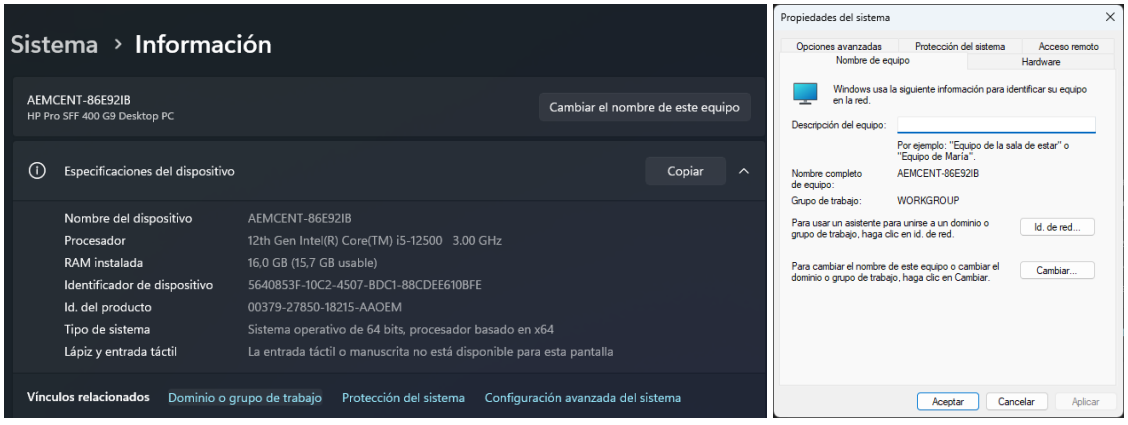
Compartir archivos o carpetas

Hace falta cumplir unos **requisitos de compartición de archivos o carpetas:**

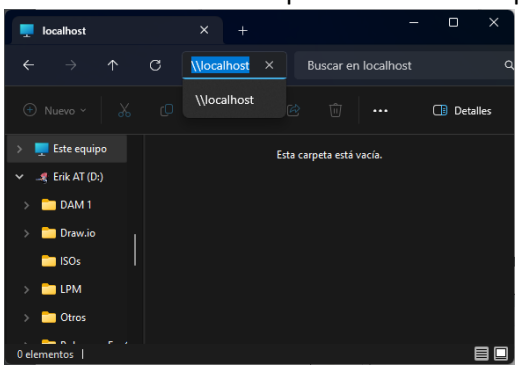
- **Los equipos tienen que estar en la misma subred**
- **Se activa la detección de redes y uso compartido en configuración**

- **Tienen que estar en el mismo grupo de trabajo** tanto el equipo con el recurso como el equipo que quiere acceder (se puede usar el comando ping con las IPs locales)

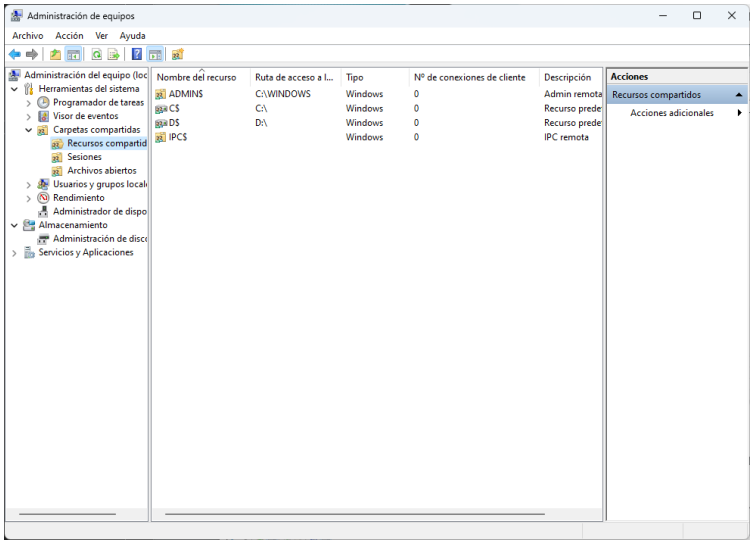
Para ver el grupo de trabajo en Windows:



Para ver el recurso compartido desde el explorador de Windows:



Para administrarlo en la administración de equipos:



Todas las direcciones ocultas acaban en $

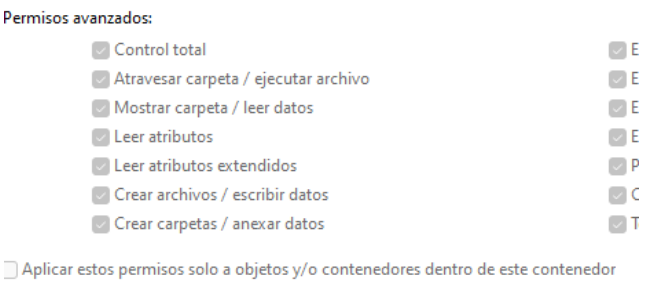
Herencia

Windows permite la herencia de permisos de objetos primarios (contenedores) a secundarios (subcarpetas y archivos dentro del contenedor). Los secundarios heredan los permisos de los primarios

El propietario controla cómo se heredan los permisos que controlan. Los permisos de carpetas o archivos pueden heredar implícitamente los permisos de la carpeta que los contiene.

La herencia es dinámica: **Las modificaciones en los permisos primarios afectan a los secundarios**. Aun así, los permisos explícitos tienen más prioridad que los heredados

La herencia de permisos se puede editar para cada permiso, es decir, se elige desde ahí a quién se aplica cada permiso.



ACL (Lista de Control de Accesos)

Van a contener los usuarios, grupos, y equipos que tienen el acceso a los objetos. Cada objeto tiene un ACL, donde se muestran los permisos de usuarios. Existe una ACE (Entrada de Control de Accesos) en la ACL

Derechos de usuarios

Los derechos de usuarios, conocidos como privilegios, determinan las acciones que un usuario o grupo puede realizar en un sistema.

Los derechos de los usuarios se relacionan directamente con los usuarios, no con los objetos.

- **Derechos de inicio de sesión**: Quién inicia sesión en un sistema y de qué modo (login y contraseña)
- **Privilegios específicos**: Establecen los derechos de usuario una vez entran al sistema

Los derechos de los usuarios prevalecen sobre los permisos de los objetos y, al igual que con los permisos, al asignar derechos a grupos, se le asignará automáticamente esos derechos a sus usuarios miembros

Directivas de seguridad. Objetos y ámbito de directivas

Son herramientas que establecen reglas de seguridad para usuarios y equipos. Se definen mediante objetos de directivas de grupo (GPO, Group Policy Object) y contienen una serie de configuraciones que controlan el entorno de trabajo.

Con esto, se centralizan políticas de los usuarios, como roles, entornos gráficos

Se definen en 2 grupos:

- GPO Locales: Utilizadas para equipos que no forman parte de un dominio, entendiendo dominio como una administración de los recursos de una organización o empresa. Las directivas que configura las GPO se dividen en 2:
    - Directivas de Configuración de Equipo (Aglutinan la configuración a nivel de equipo y se inician en el arranque del sistema)
    - Directivas de Configuración de Usuario (Aglutinan la configuración a nivel usuario, y se inician cuando el usuario inicia sesión)

  Ambas se dividen en 3 partes:

    - Configuración de Software: Permite la configuración del software ya instalado y la instalación automatizada de software.
    - Configuración de Windows: Está relacionada a la configuración de seguridad y a Windows
    - Plantillas administrativas: Incluyen políticas basadas en la configuración y ajustes del equipo (inicio, red, panel de control, componentes, apagado…)

- GPO no locales: Utilizadas en equipos que forman parte de un dominio, utilizando Active Directory

Para ver las políticas que se utilizan en un sistema, se puede usar el comando gpresult /r

Cuando se quiere establecer una GPO, se tiene que elegir su nivel. Por ejemplo, en “Directiva de seguridad Local” La GPO se encuentra en ‘Configuracion del usuario’, ‘Plantillas administrativas’ y ‘Panel de control’.

Las opciones para aplicar son:

- No configurada: no se ha editado
- Habilitada
- Deshabilitada

Se pueden añadir comentarios en la GPO, además de tener el apartado de ‘Compatible con:’, donde aparecen los sistemas operativos que cuentan con esa GPO.

Ejercicio 6.4: Active Directory

Active Directory es un servicio de directorios que almacena la información acerca de los objetos de una red y facilita su uso por parte de los usuarios y administradores.

Incluye:

- Reglas que definen las clases de objetos y atributos en el directorio, restricciones y limites de las instancias de los objetos
- Un catálogo que contiene información acerca de los objetos y permite a los usuarios buscar información del directorio independientemente del dominio.
- Un mecanismo para consultar y publicar tanto los objetos como sus propiedades, además de buscar por usuarios o aplicaciones red
- Un servicio de replicación

Plantillas

Las plantillas administrativas nos permiten definir la configuración de registro de Windows para administrar aplicaciones tanto del sistema operativo como otras de terceros para establecer el GPO

Las plantillas se pueden agregar o quitar de las aplicaciones sobre las que estemos trabajando en las GPOs

Requisitos de seguridad del sistema y datos. Seguridad a nivel de usuarios y equipos

Requisitos del sistema: Windows utiliza unas políticas que se implementan en gran medida por medio de los permisos de los recursos y las directivas de seguridad aplicadas a usuarios y equipos

Se va a gestionar por la consola de administración de Microsoft (MMC). Se podrá aplicar directivas de seguridad de manera selectiva y gestionar las herramientas administrativas.

Con MMC se administra de forma centralizada, rápida y cómoda distintas GPO a grupos, usuarios y equipos

Servidores

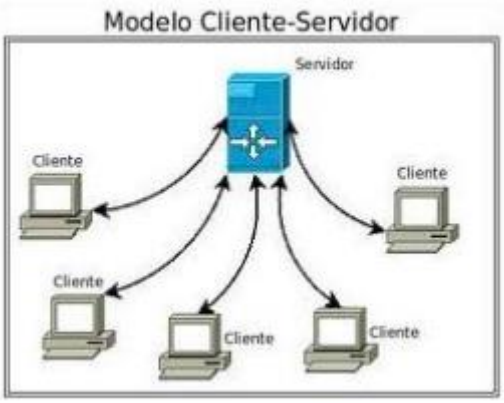
Los servidores permiten compartir los recursos en red. El servidor va a tener complementos de software del Sistema operativo y el software necesario para compartir recursos en red.

Tienen que ser:

- Disponibles: Estar activo de forma permanente
- Escalables: El sistema puede ser ampliado en cualquier momento, es decir, se pueden añadir hosts sin problema.
- Buen mantenimiento: El sistema tiene que estar preparado para realizar tareas de mantenimiento, sin afectar en ningún momento a la disponibilidad del servidor (en su funcionamiento vaya)

Los servidores se utilizan en el modelo cliente-servidor.

Los servidores están siempre en funcionamiento, esperando que los clientes realicen peticiones.
Cuando un cliente realiza una petición, el servidor dará una respuesta oportuna.



Servidor de ficheros (ftp)

Gestionan el almacenamiento de los ficheros que tienen los clientes. Sirve para:

- Facilitar la compartición: Se pueden compartir los ficheros
- Trabajar sobre los permisos de acceso en vez de trabajar en los permisos de cada fichero en cada host
- Registrar las conexiones de quienes entran.
- Realizar copias de seguridad.
- Controlar versiones de archivos.

Se usan los protocolos FTP (File Transfer Protocol), FTPS (FTP SSL para tema de filtrado de datos) y SFTP (SSH FTP)

Windows facilita la instalación de un servidor FTP a través de sus características. Se puede acceder a servidores FTP por medio del sistema de archivos o la aplicación FileZilla Client.

Servidor de impresión

Posibilitan la conectividad con impresoras, sin depender de un host concreto. Los servidores de impresión se conectan a la red directamente y funcionan como puente de enlace con las impresoras

Según la localización hay servidores externos o internos:

- Extenos: Fuera de la impresora y se conectan a un puerto de la misma
- Internos: Está incluido en la propia impresora

En Windows, yendo a panel de control -> hardware y sonido -> dispositivos e impresoras -> impresoras y escáneres y la impresora que queramos, en sus propiedades tendremos la opción de compartir la impresora en la red (no todas tienen esta opción).

Clientes de impresión

Con los servidores de impresoras y su centralización puedes agregar drivers, y de esa forma los clientes pueden usar esos servidores de impresión, además de agregar nuevas impresoras y modificar la cola de impresión

Servidor de aplicaciones

Alojan y ejecutan programas a petición de los clientes en red. Generalmente se utilizan cuando queremos conseguir reducir el tamaño de las aplicaciones cliente, dirigir el flujo de datos para aumentar el rendimiento y controlar la seguridad de los datos.

Los clientes realizan peticiones y reciben respuestas de un servidor web por el protocolo HTTP/S, y este servidor web coge datos del servidor de aplicaciones, quien a su vez coge datos de la base de datos

Se divide en tres capas:

- Nivel 1: **Presentación o interfaz gráfica (GUI, Graphic User Interface):** El usuario se conecta al servidor de aplicación por medio de un navegador o una aplicación cliente específica.
- Nivel 2: **Aplicación o servidor de aplicaciones:** Se encarga de ejecutar el procesamiento de la información, y actúa de intermediario entre los clientes y la capa de datos
- Nivel 3: **Datos:** Su misión es alojar el conjunto de datos necesarios para procesar las peticiones que reciben los clientes.

Un ejemplo:

1. Accedo desde mi ordenador a la web de AirEuropa.
2. Esa misma web está siendo dada por el servidor de aplicación de AirEuropa
3. Ese servidor recoge los datos de la base de datos
4. El servidor le pasa los datos a la web y la web responde a la consulta de mi ordenador

Los ejemplos más comunes son Oracle WebLogic, WebSphere (IBM), WildFly, Apache Gerónimo o GlassFish

Windows facilita la instalación de un servidor Web a través de sus características (Herramintas de administración web y Servicios WorldWideWeb de ISS)

Conexión remota. Herramientas

Permiten conectar un equipo a otros sin necesidad de tener acceso físico al dispositivo en concreto. Se puede usar en soportes como mantenimiento o campos como el teletrabajo.

Hay muchas herramientas que permiten acceso remoto, como AnyDesk o la *Conexión a Escritorio Remoto* de Windows, en las propiedades del sistema.

Para conectarse remotamente a un equipo, es necesario saber su dirección IP

En Ubuntu, existe la aplicación cliente de escritorio remoto Remmina: Solo hace falta añadir un nuevo perfil, con el usuario, la contraseña y el servidor al que conectarse

Herramientas de seguridad

Los sistemas en red deben estar cubiertos ante la vasta cantidad de amenazas que pueden tener. Para ello, se implantan una serie de herramientas complementarias para defender el sistema, además del antivirus.

Todo va a depender de qué nivel busca cada empresa

Cifrado

Garantizan la confidencialidad, autenticidad e integridad de los datos, mediante convertir los datos originales a un formato codificado

En Windows, se permite cifrar mediante EFS sobre los NTFS (en versiones avanzadas). Garantiza que los archivos que se cifren se asocien únicamente con el usuario que los ha cifrado, es decir, que no pueden acceder los usuarios.
Hay que dar al archivo, ir a sus propiedades -> general -> avanzadas -> cifrar contenido para proteger datos. Windows recomienda cifrar carpetas, ya que estas son recursivas.
Una vez se ha cifrado, desde las opciones permite acceder a otros usuarios.

- Otra forma de cifrar contenido, es con la herramienta BitLocker. Este actúa sobre los volúmenes. Asegura la privacidad e integridad de volúmenes enteros, además de ser más potentes que el cifrado EFS por ser más segura

En Ubuntu, hay muchas herramientas como GPG (GNU Privacy Guard), que emplea una encriptación simétrica y asimétrica

- Usa además Seahorse, que gestiona las claves y las contraseñas del propio GPG

Administración y análisis

El tratamiento y el flujo de una red puede ser muy complejo. Por ello, hay muchas aplicaciones que valen para monitorizar la red de forma global, buscando estudiar la red a largo plazo y de forma concreta, valorar la optimización de la red, y detectar tráfico malintencionado.

Un ejemplo es PandoraFMS, una herramienta de análisis y administración, encargada de monitorizar la red corporativa. Puede trabajar sobre distintos protocolos, aplicaciones, sistemas operativos, bases de datos…

Cortafuegos (Firewall)

Controla el tráfico entrante y saliente de la red. Se filtra así las posibles amenazas que pueden entrar en un equipo.

Sus filtrados pueden ser por paquetes con direcciones IP y MAC (determinar que IP o MAC no tienen acceso a la red), por aplicaciones atendiendo al puerto, y direcciones URL

Usan el protocolo NAT para traducir las IP y proteger las IP privadas de los dispositivos que protege.

Pueden ser de dos tipos:

- Firewall dedicado: Dispositivos hardware específicos que se usan para analizar el tráfico a gran velocidad
- Firewall integrado: Dispositivos hardware que se encuentra integrado en el router SOHO (Small Office Home Office)

- Firewall por software: Aplicaciones software que realizan funciones de firewall. Hay dos tipos.
    - Firewall servidor: Para SO en red sobre ámbito de clientes
    - Firewall personal: Para SO en red que filtra el tráfico de la red entre el equipo y el resto de la red. Es el que se piensa normalmente.

El firewall trabaja con unas reglas que los usuarios deben definir. Dichas reglas dicen qué conexión se autoriza (allow) y qué se bloquea (deny). Los sistemas operativos permiten configurar el firewall por medio de la terminal e incluso por interfaces gráficas

Ubuntu utiliza el firewall UFW, que funciona sobre iptables (tablas de IP). Se carga en el kernel de Linux y filtra paquetes por medio de reglas establecidas. Existe una aplicación gráfica para configurarlo: GUFW (necesita instalarse). Las reglas se pueden añadir de forma preconfigurada y se elige si la configuración es avanzada o simple.

En **Windows**, el cortafuegos es el de Windows Defender, ubicado en Panel de Control -> Sistema y Seguridad -> Firewall de Windows Defender.

En la barra lateral, se puede activar o desactivar el firewall. En esa ventana, además, permite notificar cuando el firewall bloquee una nueva aplicación

Si se da a "Permitir aplicaciones comunicarse a través del firewall", aparece un menú con las aplicaciones del sistema, además de si están permitidas o no en las redes públicas y privadas

En opciones avanzadas, permite configurar las reglas de entrada y salida, viendo las bloqueadas y las permitidas

Ejercicio: Se desea establecer una regla para abrir un puerto que escucha solicitudes de entrada HTTP en el puerto 80:

Se crea una nueva regla de entrada, por puerto, elegimos que aplique a TCP (mas seguro que UDP), y aplica al puerto local específico (80). Se elige cuándo se permite la conexión o si se bloquea y el dominio al que afecta (publico, privado, dominio). Para acabar, se elige un nombre para identificar la recha.

Sistemas de detección de intrusión (IDS, Intrude Detection System)

Monitorizan los eventos y actividades en una red en busca de accesos sin permiso. Se clasifican de varias formas:

- Según el **sistema de detección de intrusiones:**
    - Detección mediante firmas: Detecta los problemas por patrones conocidos por dar problemas
    - Detección mediante anomalías: Detecta comportamientos usuales de la red en base a los puertos, conexiones, usuarios, etc. Y se comparan con alteraciones en un momento dado.
- Según el tipo de respuesta ante un ataque
    - Pasivos: Informan a los administradores para que tomen medidas
    - Activos: Actúan automáticamente, sin tener que informar a los administradores
- Según la fuente del análisis
    - NIDS (Sistemas de Detección de Intrusión en Red): Analiza una parte concreta de la red en busca de problemas

- HIDS (Sistemas de Detección de Intrusión de Host): Analiza las actividades de un host mediante sus conexiones, registros y programas.

En Ubuntu, se conoce Security Onion, un conjunto de herramientas orientadas a la seguridad y el análisis forense

OpenSSH

Secure Shell (SSH) y OpenSSH son herramientas que pueden acceder de forma remota y segura. Se usa en servidores.

Se tiene que instalar el servidor OpenSSH, instalándolo con el sudo apt en Ubuntu. Se configura en Ubuntu en el archivo /etc/ssh. Una vez hecho todo, se reinicia el sistema para que comience el servidor

En Windows, se utiliza PuTTY como cliente. Es muy rápida, porque, con poner la IP y el puerto, ya se abre la conexión.

Si además se está utilizando otro sistema Ubuntu como cliente e integra ssh, solo hace falta el comando ssh -p puerto usuario@servidor.