Tema 5

Instalación, configuración y uso de servicios de acceso y administración remota

Administración de Sistemas Operativos

Índice

[Esquema 3](#_Toc169954230)

[Material de estudio 4](#_Toc169954231)

[1.1. Introducción y objetivos 4](#_Toc169954232)

[1.2.  Protocolos de acceso remoto y puertos implicados. 5](#_Toc169954233)

[1.3.  Servicios de acceso remoto del propio sistema operativo. 7](#_Toc169954234)

[1.4.  SSH. 11](#_Toc169954235)

[1.5.  Telnet. 16](#_Toc169954236)

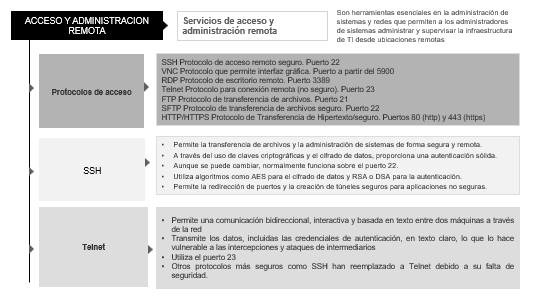
[1.6.  Referencias bibliográficas. 20](#_Toc169954237)

[A fondo 21](#_Toc169954238)

[Entrenamientos 22](#_Toc169954239)

[Test 25](#_Toc169954240)

Esquema



Material de estudio

1.1. Introducción y objetivos

Los servicios de acceso y administración remota son herramientas esenciales para los administradores de sistemas, permitiéndoles administrar y supervisar la infraestructura de TI desde ubicaciones remotas. Estos servicios, que están respaldados por una variedad de herramientas y protocolos, permiten administrar los recursos de la organización de manera segura y eficiente, lo que reduce la necesidad de acceso físico y mejora la capacidad de respuesta ante incidentes y tareas de mantenimiento. Los protocolos de acceso remoto más populares incluyen Telnet y SSH (Secure Shell), cada uno con sus propias funciones y aplicaciones. Además, los sistemas operativos modernos incluyen servicios nativos que facilitan el acceso remoto y funciones que optimizan la gestión de recursos remotos.

Los objetivos que se pretenden conseguir en este tema son:

* Comprender los protocolos de acceso remoto y los puertos implicados
  + Analizar los fundamentos de los protocolos SSH y Telnet.
  + Estudiar las diferencias entre SSH y Telnet en términos de seguridad y funcionalidad.
* Investigar los servicios de acceso remoto que ofrecen los sistemas operativos.
  + Explorar los servicios de acceso remoto proporcionados por los sistemas operativos
  + Evaluar las ventajas y limitaciones de estos servicios integrados.
* Evaluar y seleccionar las herramientas adecuadas para el acceso remoto:
  + Comparar las características y funcionalidades de SSH y Telnet, así como otros servicios nativos de acceso remoto.
  + Determinar la mejor herramienta basada en los requisitos específicos de la organización, considerando aspectos como la seguridad, el coste y la facilidad de uso.
* Instalar y configurar SSH:
  + Instalar el servidor SSH en sistemas Unix/Linux y configurar sus opciones de seguridad.
  + Conectar a sistemas remotos utilizando clientes SSH desde diferentes plataformas.
* Instalar y configurar Telnet:
  + Instalar y configurar el servicio Telnet en diferentes sistemas operativos.
  + Conectar a sistemas remotos utilizando clientes Telnet.
  + Analizar las limitaciones de seguridad de Telnet y las situaciones en las que su uso podría ser justificado.

1.2.  Protocolos de acceso remoto y puertos implicados.

Los sistemas operativos tienen varios protocolos de acceso remoto que permiten a los usuarios conectarse y controlar máquinas de forma remota. Los principales protocolos y los puertos que utilizan se describen a continuación:

1. SSH (Secure Shell, Shell Seguro)

SSH es uno de los protocolos de acceso remoto más comunes y seguros en sistemas Linux. Proporciona canales seguros a través de redes inseguras utilizando tecnología de cifrado. El puerto que utiliza es el 22. Permite acceso remoto a otra computadora y también se puede usar como servidor FTP (Protocolo de transferencia de archivos). En el sistema operativo Linux, este protocolo se configura principalmente mediante el archivo /etc/ssh/sshd\_config. Las configuraciones habituales incluyen la especificación de claves de autenticación, permisos de usuario y opciones de cifrado.

1. VNC (Virtual Network Computing , Computación en red virtual)

Usando una interfaz gráfica, VNC permite a los usuarios controlar una computadora de forma remota. Es útil para el soporte técnico y la administración. El puerto que utiliza es a partir del número 5900. En cuanto a la configuración, los servidores VNC como tightvnc, tigervnc y x11vnc tienen sus propios archivos de configuración y comandos para iniciar el servicio.

1. RDP (Remote Desktop Protocol , Protocolo de escritorio remoto)

Aunque RDP es una característica propia de Windows, se puede usar en Linux a través de aplicaciones como xrdp, que permite a los usuarios conectarse a escritorios Linux mediante un cliente RDP. Utiliza el puerto 3389. En Linux la configuración se realiza principalmente en el archivo /etc/xrdp/.

1. Telnet.

Este protocolo se utiliza principalmente para acceder a una terminal remota y realizar una conexión punto a punto a través del puerto 23. Sin embargo, la comunicación se lleva a cabo en texto plano, lo que podría poner en peligro la seguridad. La falta de cifrado ha reducido su uso en favor de SSH. Se configura a través de los directorios /etc/inetd.conf o /etc/xinetd.d/telnet y sus servicios correspondientes.

1. FTP (File Transfer Protocol , Protocolo de transferencia de archivos)

FTP es el protocolo de transferencia de archivos más utilizado, pero también se puede utilizar para acceder remotamente a los sistemas de archivos. El puerto por defecto que utiliza es 21 (TCP) para el control y una serie de puertos para la transferencia de datos, que suelen estar en el rango 1024-65535.

1. SFTP (SSH File Transfer Protocol , Protocolo de transferencia de archivos SSH)

SFTP es parte del paquete de software SSH y proporciona un método seguro para la transferencia y administración remota de archivos. Utiliza el puerto 22 (TCP).

1. HTTP/HTTPS (HyperText Transfer Protocol, o Protocolo de Transferencia de Hipertexto)

Los protocolos HTTP y HTTPS se utilizan para administrar el servidor a través de una interfaz web. HTTPS agrega una capa de seguridad mediante cifrado. Los puertos que utiliza son el 80 (TCP) para HTTP y el 443 (TCP) para HTTPS.

La interfaz de línea de comandos (CLI) se puede usar para administrar los puertos de Linux. El comando **firewall-cmd**, por ejemplo, se puede utilizar para abrir un puerto al tráfico entrante y hacer que la configuración sea persistente.

Es importante tener en cuenta que mantener abiertos los puertos puede representar un riesgo de seguridad, por lo que generalmente se recomienda mantenerlos cerrados y solo abrirlos si son necesarios para determinados servicios.

Tabla

Descripción generada automáticamente

Tabla 1. Protocolos de acceso remoto y puertos. Fuente: elaboración propia.

1.3.  Servicios de acceso remoto del propio sistema operativo.

Existen varios servicios integrados y herramientas nativas disponibles en los sistemas operativos Linux que facilitan el acceso remoto. Estos servicios son cruciales para el mantenimiento y la administración del sistema. La configuración básica de algunos de los servicios de acceso remoto más utilizados se detalla a continuación junto con una breve introducción a la instalación en el sistema operativo Linux

1. SSH

Debido a su seguridad y facilidad de uso, SSH es el servicio de acceso remoto más utilizado en Linux. Puede ejecutar comandos, transferir archivos y crear túneles seguros.

**sudo apt-get install openssh-server** # Para distribuciones basadas en Debian

**sudo yum install openssh-server** # Para distribuciones basadas en Red Hat

Estos códigos son comandos de terminal para instalar el servidor SSH en diferentes distribuciones de Linux. El comando "sudo" se utiliza para ejecutar el comando con privilegios de superusuario. El comando "apt-get install" se utiliza en distribuciones basadas en Debian, como Ubuntu, para instalar paquetes. Mientras que el comando "yum install" se utiliza en distribuciones basadas en Red Hat, como CentOS, para instalar paquetes. En este caso, se está instalando el paquete "openssh-server", que es el servidor SSH, en el sistema operativo.

Aunque SSH es muy popular en entornos Linux, es compatible con otros sistemas operativos como Windows. OpenSSH está incluido en Windows 10 y Windows Server, lo que permite a los usuarios usar SSH nativamente. Además, hay clientes y servidores SSH de terceros disponibles para Windows, como PuTTY y WinSCP.

1. VNC (Virtual Network Computing)

VNC permite acceder a un entorno gráfico de Linux de forma remota. Su instalación se realiza usando los siguientes códigos

**sudo apt-get install tightvncserver** # Para distribuciones basadas en Debian

**sudo yum install tigervnc-server** # Para distribuciones basadas en Red Hat

Estos códigos son comandos de instalación de software en sistemas operativos basados en Linux.

El primer comando "sudo apt-get install tightvncserver" es para distribuciones basadas en Debian, como Ubuntu. Este comando utiliza el gestor de paquetes APT para buscar e instalar el paquete "tightvncserver", que es un servidor VNC (Virtual Network Computing) que permite a los usuarios controlar de forma remota un escritorio o entorno gráfico.

El segundo comando "sudo yum install tigervnc-server" es para distribuciones basadas en Red Hat, como Fedora o CentOS. Este comando utiliza el gestor de paquetes YUM para buscar e instalar el paquete "tigervnc-server", que es similar al tightvncserver pero específico para distribuciones Red Hat.

En resumen, estos comandos sirven para instalar un servidor VNC en sistemas Linux, pero varían dependiendo de la distribución del sistema operativo.

1. RDP (Remote Desktop Protocol)

Este protocolo se utiliza para el acceso remoto al escritorio en sistemas Windows. Para usarlo, se debe activar la opción de Escritorio Remoto en la configuración del sistema.

Para permitir el envío de datos de ida y vuelta entre las máquinas conectadas, como el escritorio remoto y la computadora utilizada, el protocolo Remote Desktop Protocol (RDP) abre un canal de red específico. Para lograrlo, siempre usa el puerto de red 3389. Este canal transmite datos como movimientos de ratón, pulsaciones de teclas, visualizaciones de escritorio y otros datos necesarios a través de TCP/IP, el protocolo de transporte que se utiliza para la mayoría de los tipos de tráfico de Internet. Para mejorar la seguridad de las conexiones a Internet pública, RDP también cifra todos los datos.

La utilidad Remote Desktop presente en los sistemas operativos Windows utiliza este protocolo RDP.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 1. Conexión a escritorio remoto. Fuente: elaboración propia.

Aunque RDP es un protocolo de Microsoft, en Linux se puede usar a través de xrdp.

Para realizar su instalación en Linux se utilizan los comandos

**sudo apt-get install xrdp** # Para distribuciones basadas en Debian

**sudo yum install xrdp** # Para distribuciones basadas en Red Hat

El comando "sudo apt-get install xrdp" se utiliza en distribuciones basadas en Debian, para instalar el paquete xrdp, que es un servidor de escritorio remoto para Linux.

El comando "sudo yum install xrdp" se utiliza en distribuciones basadas en Red Hat, para instalar el mismo paquete xrdp.

1. Telnet

Telnet se utiliza principalmente para tareas de administración de red o redes privadas porque es menos seguro que SSH. Para proceder a su instalación utilizaremos:

**sudo apt-get install telnetd** # Para distribuciones basadas en Debian

**sudo yum install telnet-server** # Para distribuciones basadas en Red Hat

Los siguientes comandos se deben usar para abrir los puertos específicos para permitir el tráfico de diferentes servicios a través del firewall. El uso del comando "sudo" antes de cada uno indica que se está ejecutando con privilegios de superusuario necesarios para poder realizar cambios en la configuración del firewall.

**sudo ufw allow 22/tcp** # Permitir SSH

**sudo ufw allow 5900/tcp** # Permitir VNC

**sudo ufw allow 3389/tcp** # Permitir RDP

**sudo ufw allow 80/tcp** # Permitir HTTP

**sudo ufw allow 443/tcp** # Permitir HTTPS

1.4.  SSH.

Secure Shell – SSH es un protocolo de red criptográfico para operar servicios de red seguros sobre una red no segura como por ejemplo Internet. Aunque SSH se utiliza principalmente para el acceso a un servidor remoto y la ejecución segura de comandos, también se puede utilizar para la transferencia de archivos y para el enrutamiento seguro de la red.

Proporciona un método seguro para acceder y administrar remotamente servidores y otros dispositivos de red. El uso de SSH permite la transferencia segura de archivos entre dispositivos. SSH es la base de protocolos como SCP (Protocolo de copia segura) y SFTP (Protocolo de transferencia de archivos SSH).

El uso de SSH permite la creación de túneles seguros en una red, esto puede ser beneficioso para redirigir puertos y acceder a servicios de red internos que no se pueden acceder directamente desde fuera de la red.

**Protocolo y puerto**

- El SSH funciona normalmente a través del puerto 22.

- Utiliza criptografía de clave pública para autenticar el servidor y en algunos casos al cliente. Utiliza algoritmos como RSA o DSA para la autenticación y AES para el cifrado de datos. SSH.

**Componentes principales**

- Cliente SSH: es la aplicación que inicia una conexión SSH.

- Servidor de SSH: es la aplicación que acepta conexiones SSH.

- Shell Remoto: la interfaz de línea de comandos proporcionada al cliente por el servidor.

1.4. 1.  Instalación y configuración.

**Instalación del cliente:**

* En sistemas basados en Linux/Unix generalmente se encuentra preinstalado
* Para Windows es posible usar aplicaciones como PuTTY o activar el cliente OpenSSH en versiones más recientes.

**Instalación del servidor:**

* Para Linux/Unix se usa `apt-get install openssh-server` para distribuciones basadas en Debian;
* En todos los sistemas, es necesario realizar una configuración básica del servidor en ` /etc/ssh/sshd\_config`.

1.4. 2.  Ejemplo de conexión básica

Si queremos realizar una conexión desde un terminal con sistema operativo Windows a un terminal de Linux, por ejemplo Ubuntu, realizaremos los siguientes pasos:

* Desde el terminal cliente, el que tiene sistema operativo Windows, abriremos una consola de comandos.
* En la consola de comandos indicaremos usuario@ipdestino, por ejemplo [usuario@192.168.230.19](mailto:usuario@192.168.230.19), donde usuario es el nombre del usuario con el que queremos conectar a la maquina servidora con la ip indicada.
* A continuación, nos pedirá la contraseña del usuario
* Una vez introducida la contraseña y validada estaremos conectándonos remotamente a la maquina servidora. Podemos verlo en la consola de comandos porque muestra el prompt de la máquina de Ubuntu.

Texto

Descripción generada automáticamente

Figura 2. Conexión por SSH a máquina remota desde consola comandos. Fuente: elaboración propia.

Para salir de la conexión, escribiremos **exit** en la máquina cliente, lo que rompe la conexión con la maquina servidora.

* Hay que tener en cuenta que en la máquina servidora debe estar instalado el servicio ssh. De no ser así ( el error ssh.service not found lo indica) instalaremos openssh-server.

Texto

Descripción generada automáticamente

Figura 3. Instalación de SSH en Ubuntu. Fuente: elaboración propia.

Los comandos **sudo service ssh status** nos indica la situación en la que se encuentra el servicio ssh y el comando **sudo service ssh start** lo arranca si estuviera caído.

En el apartado A Fondo puedes encontrar un vídeo explicativo de cómo conectar vía SSH desde un sistema Windows a un sistema Ubuntu

A continuación, vamos a ver algunos de los usos prácticos que se le dan al servicio SSH.

* Transferencia de archivos. Una vez abierta una conexión ssh podemos realizar el copiado de archivos de forma segura entre el cliente y el servidor, para ello utilizaremos el comando

**scp archivo\_local usuario@direccion\_ip\_del\_servidor:/ruta/destino.** En el ejemplo siguiente, se va a copiar desde la máquina Windows el fichero fichero1.txt a la máquina servidora Ubuntu, a una carpeta llamada dirUsuario previamente creada.

**scp fichero1.txt** [**usuario@192.168.230.19:/home/usuario**](mailto:usuario@192.168.230.19:/home/usuario)**/dirUsuario**

* Cambiar el Puerto por defecto. Como se ha comentado anteriormente, el puerto por defecto en el que está escuchando el servicio ssh es el 22 pero podemos modificarlo a otro puerto distinto, esto nos dará un nivel más de seguridad.

En la maquina servidora ejecutaremos **sudo nano /etc/ssh/sshd\_config** lo que abre el fichero de configuración del servicio ssh . En este fichero hay que localizar donde indica el puerto actual (#PORT 22), lo cambiaremos al nuevo puerto (#PORT 222) y guardaremos el fichero con Ctrl+O.

Texto

Descripción generada automáticamente

Figura 4. Edición del fichero de configuración de ssh en Ubuntu. Fuente: elaboración propia.

Una vez realizado el cambio es necesario reiniciar el servicio ssh con el comando **sudo systemctl restart sshd.**

Es probable que se tenga que modificar el firewall, si existe, para abrir el nuevo puerto si no lo estuviera.

* Creación de túneles SSH: El uso de SSH permite la creación de túneles seguros en una red. Puede ser beneficioso para redirigir puertos y acceder a servicios de red internos que no se pueden acceder directamente desde fuera de la red.

En este ejemplo vamos a crear un túnel de tipo local que es un túnel que conecta un puerto local a otro en una máquina remota. Es útil para acceder a una base de datos que está detrás de un firewall, por ejemplo.

**ssh -L 3307:192.168.230.19:3306** [**usuario@host\_ssh.com**](mailto:usuario@host_ssh.com)

En este caso se redirige el puerto 3307 de la máquina local al puerto 3306 de 192.168.230.19 a través de host\_ssh.com. Con este comando se puede acceder al puerto 3306 conectando a localhost:3307.

En conclusión, para facilitar la administración remota y brindar acceso seguro a servidores, SSH es una herramienta esencial para cualquier profesional de la informática. La comprensión y el uso efectivo de SSH mejoran la seguridad y la eficiencia operativa en entornos de TI.

En el apartado A Fondo puedes encontrar un vídeo explicativo de cómo crear un túnel con SSH.

1.5.  Telnet.

Telnet fue uno de los protocolos de red más antiguos y esenciales que permitió la comunicación remota entre dispositivos. El estudio de Telnet proporciona una comprensión profunda de los fundamentos de la administración remota de sistemas y la evolución de la seguridad en redes. Este capítulo analiza la arquitectura, el uso y los problemas de seguridad de Telnet, así como sus alternativas actuales.

En los años 80 y 90, Telnet se convirtió en una herramienta vital para desarrolladores y administradores de sistemas. Sin embargo, a medida que las redes se volvían más accesibles y complejas, la falta de mecanismos de seguridad adecuados comenzó a ser una preocupación.

Actualmente, Telnet ha sido parcialmente sustituido por SSH (Secure Shell) y otras tecnologías seguras, aunque aún se emplea en algunos sistemas.

Telnet no solo se refiere al protocolo, sino también al programa utilizado para establecer la conexión remota con otros ordenadores, sistemas o dispositivos.

**Protocolo y puerto**

El uso de este protocolo permite la conexión remota a otros equipos y la gestión de dispositivos de red.

Telnet utiliza el protocolo de control de transmisión (TCP), que usa el puerto 23 por defecto.

A diferencia de SSH, que utiliza criptografía de clave pública, Telnet transmite los datos sin encriptar lo que supone vulnerabilidades en términos de seguridad.

**Componentes principales**

* Cliente Telnet: El cliente Telnet es un programa que permite que el usuario se conecte al servidor Telnet e interactúe con el sistema remoto.
* Servidor Telnet: Es un software que recibe conexiones Telnet entrantes y ejecuta comandos del cliente en un sistema remoto.

El uso de este protocolo y programa solo es posible en modo comando. Para establecer una conexión con Telnet entre dos sistemas, primero debemos tener un cliente en un ordenador y un servidor en la máquina a la que pretendemos acceder. Para realizar la conexión entre los dos extremos necesitaremos tener el puerto 23 abierto en la máquina remota.

1.5. 1.  Ejemplo de conexión básica

Las conexiones que se realicen usando este protocolo siguen varios pasos:

1. Configuración de conexión: El cliente Telnet establece una conexión TCP con el servidor Telnet en el puerto 23.

2. Negociación: El cliente y el servidor acuerdan el tipo de terminal, el tamaño de la pantalla y el manejo de caracteres especiales en el terminal.

3. Transmisión de Datos: una vez que se establece la conexión, el cliente envía comandos al servidor, y el servidor devuelve el comando que se ha ejecutado.

4. Cierre de conexión: Cuando el usuario cierra la conexión u ocurre un error, la sesión termina.

Para saber si el cliente Telnet está habilitado en nuestro PC abriremos una consola de comandos en modo administrador y escribiremos telnet seguido de la ip destino y puerto a la que queremos conectar.

**Texto

Descripción generada automáticamente**

Figura 5. Conexión usando protocolo Telnet. Fuente: elaboración propia.

En este caso es necesario habilitar el servicio. Para ello, en un sistema Windows, hay que navegar a *Panel de control>Programas>Programas y características>Activar o Desactivar características de Windows* y activar “Cliente Telnet”

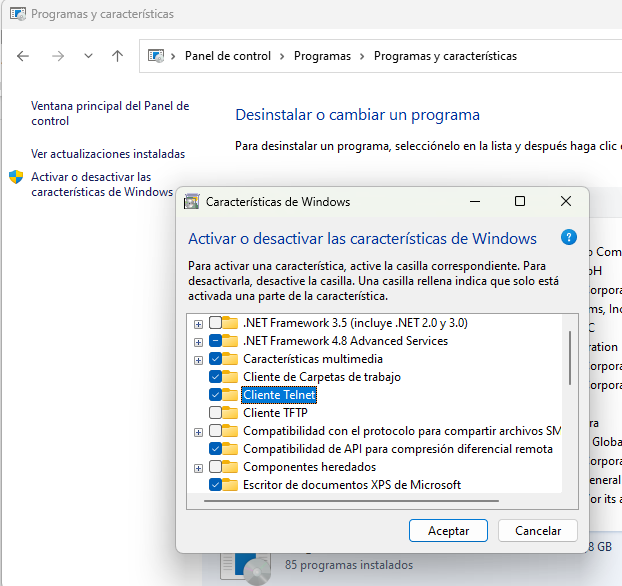


Figura 6. Activar Cliente Telnet en Windows. Fuente: elaboración propia.

Este paso realiza una breve instalación de las características y una vez finalizada podremos usar telnet desde nuestro sistema Windows.

Si en una consola de comandos Windows indicamos el siguiente comando

**telnet 192.168.230.19 222**

y el sistema remoto no tiene abierto el puerto 222 el resultado de la ejecución será:

**Conectándose a 192.168.230.19...No se puede abrir la conexión al host, en puerto 222: Error en la conexión**

En cambio, si el puerto 222 estuviera abierto, el resultado es una consola con el prompt de Telnet.

Texto

Descripción generada automáticamente

Figura 7. Acceso vía protocolo Telnet. Fuente: elaboración propia.

En el apartado A Fondo puedes encontrar información sobre cómo comprobar puertos usando Telnet.

En resumen, Telnet es un protocolo (y programa) muy extendido que lleva mucho tiempo utilizándose. Los datos transferidos entre dos sistemas usando este protocolo, incluidos los nombres de usuario y contraseñas, se transmiten a través en texto plano, lo que los hace susceptibles a la intercepción y lectura por atacantes que utilizan técnicas de espionaje de red. Debido a esta vulnerabilidad de seguridad el uso de este protocolo ha sido limitado siendo sustituido en gran parte por SSH.

1.6.  Referencias bibliográficas.

Microsoft. (s.f.). *Understanding Remote Desktop Protocol. Microsoft Learn.* https://learn.microsoft.com/es-es/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

Microsoft. (s.f.). *Cómo usar Escritorio remoto. Microsoft Support.* https://support.microsoft.com/es-es/windows/c%C3%B3mo-usar-escritorio-remoto-5fe128d5-8fb1-7a23-3b8a-41e636865e8c

Profesional Review. (20 de Enero 2019). *Telnet: ¿Qué es?.* https://www.profesionalreview.com/2019/01/20/telnet-que-es/

Redessy. (s.f.). *Cómo instalar, configurar y habilitar el servicio SSH en Linux.* https://redessy.com/como-instalar-configurar-y-habilitar-el-servicio-ssh-en-linux/

Red Hat. (s.f.). *Controlling ports using CLI. Red Hat Enterprise Linux 8 documentation.* https://access.redhat.com/documentation/es-es/red\_hat\_enterprise\_linux/8/html/securing\_networks/controlling-ports-using-cli\_controlling-network-traffic-using-firewalld

A fondo

Conexión SSH Windows-Ubuntu

El Rincón del Hacker. (03 de diciembre de 2021). *Cómo Hacer CONEXIÓN via SSH Desde WINDOWS a LINUX* [Vídeo]. Youtube. https://www.youtube.com/watch?v=isqtKUFfV4k

En este vídeo puedes comprobar los pasos necesarios para conectar vía ssh un sistema Windows con un sistema operativo Ubuntu que se encuentra en una máquina virtual en VirtualBox.

Cómo crear un túnel SSH

Tony Teaches Tech. (17 de mayo de 2022). *How to Make an SSH Proxy Tunnel* [Vídeo]. Youtube. https://www.youtube.com/watch?v=F-ubwghsWPM

Aprende a configurar un servidor proxy de túnel SSH que conecta un ordenador local con un servidor remoto que contiene un recurso accesible.

Comprobar puertos TCP remotos con un cliente Telnet

DaveTutoriales. (18 de febrero de 2020). *Como Probar puertos de comunicación TCP remotamente habilitando Cliente Telnet en WindowsWorkstation* [Vídeo]. Youtube. https://www.youtube.com/watch?v=vUURv74OPMU

Conoce los pasos y la activación del cliente Telnet, para comprobar puertos TCP en máquinas remotas desde un sistema operativo Windows.

Entrenamientos

Los siguientes entrenamientos se han realizado desde una máquina cliente con sistema operativo Windows hacia una máquina servidora con sistema operativo Ubuntu.

Entrenamiento 1

* Crea una conexión Telnet a la máquina remota desde un sistema Windows para conectarnos a su puerto 2224
* Desarrollo paso a paso
  + Abrir una consola de comandos usando cmd en modo administrador.
  + Utilizaremos el comando telnet direccion\_ip\_o\_hostname puerto
  + Es posible que puede que solicite usuario o contraseña
* Solución

telnet 192.168.230.19 2224

Entrenamiento 2

* El objetivo del ejercicio es conectar de forma segura a un servidor remoto utilizando SSH (Secure Shell) desde una máquina cliente y realizar una serie de operaciones:
  + Establecer la conexión SSH.
  + Cambiar el puerto predeterminado de SSH en el servidor remoto.
* Desarrollo paso a paso
  + Paso 1: Establecer la Conexión SSH usando el comando ssh username@server\_ip\_or\_hostname. Para ello abriremos una consola con cmd en modo administrador.
  + Paso 2: Cambiar el Puerto Predeterminado de SSH. Para ello hay que editar el archivo de configuración del servidor SSH (sshd\_config) con un editor, por ejemplo, nano.
* Solución

ssh [usario@192.168.230.19](mailto:usario@192.168.230.19)

sudo nano /etc/ssh/sshd\_config

Modificar el puerto donde se indica #Port 22 y cambiar el número 22 por el nuevo puerto

Guardar fichero con Ctrl+O.

Entrenamiento 3

* Abre una conexión SSH usando el nuevo puerto indicado en el ejercicio anterior y cierra la conexión
* Desarrollo paso a paso
  + Para abrir una conexión SSH usando un puerto que no es el de por defecto se utiliza el comando
    - ssh -p 222 usuario@direccion\_ip\_o\_hostname
  + Donde
    - -p 222 especifica el puerto SSH al que deseas conectarte (en este caso, el puerto 222).
    - usuario es el nombre de usuario en el servidor al que quieres acceder.
    - direccion\_ip\_o\_hostname es la dirección IP o el nombre de host del servidor al que quieres conectarte.
* Solución

ssh -p 222 [usuario@192.168.230.19](mailto:usuario@192.168.230.19)

exit

Entrenamiento 4

* Usando la conexión SSH segura de los ejercicios anteriores crea un directorio en la máquina destino y dentro de ese directorio copia un fichero que tengas en tu máquina local.
* Desarrollo paso a paso
  + Establecer una conexión SSH con el servidor de destino usando el nuevo puerto
  + Crear un Directorio en el Servidor Destino. Una vez que estés conectado al servidor destino a través de SSH, crea un directorio donde copiaremos el archivo desde la máquina local, usando el comando mkdir. Una vez creado salimos de la conexión SSH.
  + Copiar un Archivo desde la Máquina Local al Directorio en el Servidor Destino, Ahora, copiaremos un archivo desde la máquina local al directorio que acabamos de crear en el servidor destino. Utilizaremos el comando scp para esta tarea.
* Solución

ssh [usuario@192.168.230.19](mailto:usuario@192.168.230.19) -p 222

mkdir ~/nuevo\_directorio # crea el dir en home/usuario

exit # sale de la conexión ssh

scp /ruta/al/archivo/local.txt usuario@192.168.230.19:/home/usuario/nuevo\_directorio/

Test

1. ¿Cuál es el puerto predeterminado utilizado por el protocolo SSH?

A. 20

B. 21

\_ C. 22

D. 23

El puerto por defecto del protocolo SSH es el 22.

1. ¿Qué protocolo se utiliza principalmente para la administración remota segura de dispositivos de red?:

\_ A. SSH.

B. FTP.

C. Telnet.

D. HTTP.

La administración remota de dispositivos en una red puede realizarse usando SSH y Telnet pero SSH lo hace de forma segura ya que Telnet tiene vulnerabilidades de seguridad. El resto de los protocolos no son válidos para administraciones remotas.

1. ¿Cuál es el puerto predeterminado utilizado por el protocolo Telnet por defecto?

A. 20

B. 21

C. 22

\_D. 23

El puerto por defecto del protocolo Telnet es el 23.

1. ¿Cuál de los siguientes protocolos no transfiere los datos cifrados?:

A. SSH

B. SFTP.

\_C. Telnet.

D. HTTPS.

Telnet es un protocolo de administración remota que transfiere los datos sin encriptar, en texto plano.

1. ¿Cuál es la utilidad de acceso remoto predeterminada en Windows?

A. Terminal.

B. Putty.

C. FTP.

\_ D. Remote Desktop

Remote Desktop es la utilidad de los sistemas operativos Windows que permite a un usuario conectarse a través de un escritorio remoto a otro ordenador desde un cliente.

1. ¿Qué comando se utiliza en sistemas Windows para establecer una conexión Telnet?:

A. ssh.

B. rdp.

C. connect.

\_D. Ninguna de las anteriores.

En sistemas operativos Windows el comando que se usa para una conexión es Telnet. Para ello es necesario abrir una consola de comandos y escribir el comando telnet ipdestino puerto para conectar a una máquina en un puerto concreto.

1. ¿Qué puerto utiliza el servicio Remote Desktop Protocol en Windows?

A. 21

B.22

\_C. 3389

D. 80

El puerto por defecto usado por RDP es el 3389. El puerto 21 se usa para transferencia de ficheros (FTP), el puerto 22 es el utilizado por el protocolo SSH y el puerto 80 es el que se usa para tráfico web.

1. ¿Cuál es el principal objetivo del protocolo SSH?

A. Transferir archivos sin cifrado

\_B. Proporcionar una conexión remota cifrada

C. Navegar por internet de manera segura

D. Acceder a bases de datos

El objetivo principal de SSH es proporcionar una conexión a una máquina remota de forma segura por la que los datos vayan cifrados.

1. ¿Qué algoritmo se utiliza comúnmente para la autenticación en SSH?

A. MD5

B. DES

C. Ninguno porque los datos no están cifrados

\_D. RSA

Los datos transferidos usando el protocolo SSH van cifrados. El algoritmo que suele utilizarse es el RSA.

1. ¿Cuál de los siguientes es un beneficio de usar SSH sobre Telnet?

A. SSH es más rápido

B. SSH utiliza menos recursos

\_C. SSH cifra las comunicaciones

D. SSH es compatible con todos los sistemas operativos

Tanto SSH como Telnet son protocolos que se utilizan para la administración de máquinas remotas, en cambio Telnet envía los datos sin cifrar mientras que SSH los manda cifrados.

1. ¿Qué puerto debe abrirse en un firewall para permitir conexiones Telnet?

A. 21

\_B. 23

C. 25

D. 110

El puerto utilizado por Telnet es el puerto 23 por defecto.

1. ¿Qué protocolo ha reemplazado mayoritariamente a Telnet para conexiones seguras?
2. FTP

B. HTTP

\_C. SSH

D. SMTP

Tanto Telnet como SSH se utilizan para realizar conexiones remotas, pero SSH cifra las comunicaciones. El resto de los protocolos tienen otras funcionalidades distintas.

1. ¿Cuál es el propósito principal de VNC (Virtual Network Computing)?

A. Transferir archivos entre dos computadoras

\_B. Proporcionar acceso remoto usando la interfaz gráfica de un sistema

C. Monitorizar el rendimiento de la red

D. Cifrar comunicaciones entre dos dispositivos

VNC es un sistema que permite a los usuarios controlar otra computadora remotamente a través de una red mediante una interfaz gráfica.

1. ¿Cuál es la función principal del protocolo FTP?

A. Enviar correos electrónicos

\_B. Transferir archivos entre un cliente y un servidor

C. Proporcionar acceso remoto a una interfaz gráfica

D. Cifrar datos entre dos dispositivos

El protocolo FTP(File Transfer Protocol ) se utiliza para transferencia de ficheros.

1. ¿En qué se diferencia SFTP de FTP?

A. SFTP utiliza una interfaz gráfica

B. SFTP es más rápido que FTP

\_C. SFTP cifra las transferencias de archivos

D. SFTP solo se utiliza en redes locales

Los protocolos FTP y SFTP se utilizan para la transferencia de ficheros entre dos sistemas. La diferencia radica en que, mientras FTP no utiliza cifrado, SFTP sí lo hace.

1. ¿Qué característica distingue HTTPS de HTTP?

\_A. HTTPS cifra las comunicaciones

B. HTTPS es más rápido

C. HTTPS utiliza un puerto diferente

D. HTTPS es compatible solo con navegadores modernos

HTTP y HTTPs son dos protocolos para la transferencia de hipertexto, pero https utiliza TLS (SSL) para encriptar las peticiones y respuestas.

1. ¿Cuál es el propósito principal del comando scp en el contexto de SSH?

A. Conectar de forma remota a una interfaz gráfica

B. Ejecutar comandos de shell en un servidor remoto

\_ C. Transferir archivos de manera segura entre dos computadoras

D. Monitorizar el rendimiento del servidor

Una vez abierta una conexión ssh podemos realizar el copiado de archivos de forma segura entre el cliente y el servidor.

1. ¿Cuál es la función principal de un túnel SSH?

\_A. Cifrar y encapsular tráfico de red para protegerlo durante la transmisión

B. Transferir archivos sin cifrado entre dos computadoras

C. Permitir conexiones remotas a una base de datos

D. Monitorizar el uso de la CPU en un servidor remoto

Los túneles SSH que se crean sirven para poder transferir tráfico de forma segura dentro de una red.

1. ¿Cómo se cambia el puerto predeterminado de SSH en un servidor Linux?

A. Editando el archivo /etc/ssh/ssh\_config

B. Utilizando el comando ssh-change-port

\_C. Editando el archivo /etc/ssh/sshd\_config

D. Reiniciando el servicio SSH con un nuevo puerto

El archivo /etc/ssh/sshd\_config tiene una línea dedicada al puerto por defecto que se utiliza en SSH. Para modificarlo hay que editarlo y cambiar el puerto 22 por defecto por el puerto deseado.

1. ¿Cuál es el uso principal de PuTTY?

A. Transferir archivos entre dos sistemas sin cifrado

B. Proporcionar una interfaz gráfica para la administración de bases de datos

C. Monitorizar el rendimiento del hardware del servidor

\_D. Conectar de forma segura a una línea de comandos remota mediante SSH

Putty es una herramienta que se utiliza para realizar conexiones remotas usando el protocolo SSH.