Herramientas de acceso remoto.

Caso práctico

Stockbyte. (Uso educativo nc)

Recordaras a Juan y María, trabajadores de la empresa de mantenimiento de equipos informáticos, entre los clientes de su empresa, tienen varias **PYME** (pequeñas y medianas empresas).

Hace tiempo se dieron cuenta de que muchos errores, consultas, configuraciones, chequeo con antivirus, etc., se podían resolver utilizando la conexión remota. De esta forma ahorran tiempo y dinero, además de dar un servicio más rápido para cubrir las necesidades de sus clientes.

-¡Buenos días, María!

-¡Buenos días, Juan! , ¿Qué tenemos para hoy?

-La dirección de la empresa, ha decidido que tenemos que empezar a trabajar con acceso remoto en varias PYME a las que damos servicio –dijo Juan.

-¡Ya era hora! –respondió María-. No veas la de tiempo y dinero que perdemos en desplazamientos a las empresas para resolver cosas que en 5 minutos lo podrías solucionar desde aquí con un acceso remoto.

-Estoy de acuerdo contigo -dijo Juan-, ¡Ya era hora!, esto será un ahorro considerable, con este sistema vamos ha ahorrar mucho dinero y tiempo.

-Y el servicio que damos a los clientes también mejorará, -dijo María-. Vamos a resolverles muchas incidencias casi en el momento, estoy segura que lo agradecerán y les será de gran ayuda.

-¿Y por cual empiezo? -preguntó María-.

-Tenemos una asesoría, un instituto, una empresa de transporte y otros clientes que tienen empresas en sitios mal comunicados. Decide tú por cual empiezas.

-Empezaré por el instituto –dijo María-.

-De acuerdo, me parece una buena idea –dijo Juan.

Debes conocer

Existen programas comerciales (algunos gratuitos y otros de pago, o con versiones "profesionales" de pago), que permiten realizar conexiones a escritorios remotos, y son muy usados en entornos de soporte técnico o supervisión de

sistemas. El más conocido es **Teamviewer** (https://www.teamviewer.com/es). También se utilizan otras herramientas como **Skype** (https://www.skype.com/es/), **Webex** (https://www.webex.es/) o **Zoom** (https://zoom.us/) para reuniones online y compartir el escritorio durante videoconferencias.

1.- Gestión de acceso remoto.

Caso práctico

Stockbyte. (Uso educativo nc)

María llegó al instituto esa misma mañana, se puso al habla con el coordinador del mantenimiento de equipos del **IES** Montes Claros, llamado Alberto.

-Creo que ya te han informado, desde la dirección de mi empresa, que algunas consultas, configuraciones, eliminación de virus, etc. se pueden hacer por control remoto, desde las oficinas de mi empresa, así no nos tenemos que desplazar continuamente aquí y eso le da agilidad a la resolución de incidencias -dijo María.

-Sí, ya estoy informado y me parece muy bien. He estado pensando que este sistema también nos vale para visualizar una presentación de todos los equipos de la red -dijo Alberto.

-Así es, lo incluyo en los requerimientos, y si tienes alguna necesidad especial más me lo dices -dijo María-.

-De acuerdo -dijo Juan-. De todas formas me gustaría que cuando tengas un rato, me expliques más detalles sobre este servicio. Yo se más o menos en qué consiste, pero no conozco todo el alcance que puede llegar a tener. Y esto me sería de utilidad para saber si puedo incluir algún requerimiento más.

-Pues ahora mismo te explico…

Voy a explicarte en qué consiste este servicio. Sobre la redes, se han diseñado varios servicios de conexión remota, que permite acceder desde un ordenador a otro o a un recurso ubicado en este último. Esto se puede hacer a través de una red local o externa (Internet). Estos servicios facilitan la gestión de los equipos de una red, pero pueden suponer una amenaza, si están activos en un equipo con acceso a Internet, ya que permiten que desde el exterior, controlen directamente nuestro equipo. La mayor parte de estos servicios utilizan el protocolo **TCP** (siglas en inglés de Transmission Control Protocol, en español Protocolo de Control de Transmisión) como nivel de transporte.

Podemos clasificar los sistemas de conexión remota en tres tipos:

Conexión remota mediante una terminal virtual en modo texto.
Conexión remota mediante una terminar virtual de forma gráfica.
Conexión remota mediante web.

Remotamente puedes acceder prácticamente a cualquier recurso que ofrece un ordenador. Puedes acceder a archivos, impresoras, configuraciones, etc. Por ejemplo, se puede configurar un servidor de forma remota.

Autoevaluación

El servicio que permite acceder desde un ordenador a otro ordenador se llama:

Enviar

Es el acceso remoto, permite acceder desde un ordenador a otro o a un recurso ubicado en este último.

2.- Terminales en modo texto.

Caso práctico

María empezó a probar los diferentes productos existentes para implementar el servicio de acceso remoto. Empezó por los servicios en Modo texto.

Stockbyte. (Uso educativo nc)

"Esta forma era la más común hasta hace poco, cuando los sistemas operativos no eran tan gráficos como ahora y por eso es la que menos recursos necesita –pensó María".

"Casi todos los sistemas operativos incluyen un programa de conexión mediante el protocolo **TELNET**. En los sistemas **UNIX,** aparte del servicio **TELNET,** también podemos encontrar **RLOGIN** y el **SSH** –siguió reflexionando María".

"Lo más destacable de **SSH**, es la característica de confidencialidad ya que la información viaja protegida y, además, se ajusta un poco a lo que busco" –concluyó mentalmente María.

¿Qué tal hasta ahora? Imagino que piensas que es interesante y muy útil este servicio ¿no? Vas a ver ahora los servicios básicos o de modo texto.

Existen 3 servicios básicos o protocolos de conexión o de terminal remota modo texto:

TELNET (Siglas en inglés de Telecommunication NETwork, significa Redes de Comunicaciones), utiliza el puerto 23 **TCP.**
RLOGIN (Siglas en inglés de Remote Login, significa conectarse a distancia), utiliza el puerto 513 **TCP.**
SSH (**S**ecure **SH**ell, en español: intérprete de órdenes segura), por el puerto 22 **TCP.**

RFC (Siglas en inglés de Request for Comments, significa Petición de Comentario), son una serie de documentos con una propuesta oficial para un nuevo protocolo en Internet. Este se explica con detalle y tiene que ser aceptado.

Cualquiera puede enviar una propuesta de **RFC** a la **IETF** (siglas en inglés de Internet Engineering Task Force, en español Grupo Especial sobre Ingeniería de Internet), pero es ésta la que decide si el documento se convierte en un **RFC.**

Cada **RFC** tiene un titulo y un número asignado, que no puedo repetirse, ni eliminarse aunque el documento quede obsoleto.

Autoevaluación

Podemos clasificar los servicios de clasificación remota en varios tipos que son:

- ○ Modo texto y modo gráfico.
- ○ Modo texto, modo gráfico y web.
- ○ Modo gráfico y web.
- ○ Modo texto, modo gráfico y modo internet.

Error. Pero casi lo consigues.

Muy bien. Esta era la respuesta esperada.

Incorrecto. Tienes que repasar el punto anterior.

No es correcto. Tienes que repasar.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

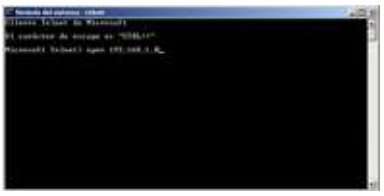
2.1.- TELNET.

Ahora vas a entrar a ver más en profundidad el protocolo **TELNET**. Era el método más utilizados hasta hace unos años, utiliza una conexión **TCP** sobre el puerto 23.

Este protocolo está disponible en todos los sistemas operativos y no tienes que configurar nada, se maneja en modo comando. Los comandos más habituales son:

Comandos habituales.

open <dirección IP o nombre de host>	Establece una conexión con el host.
close	Cierra la conexión.
quit	Termina el programa.
<ctrl>z	Suspende temporalmente el programa.
status	Muestra el estado actual.



Alicia Galán Gutiérrez. (Copyright (Cita))

Una vez establecida la conexión el sistema remoto solicita un login (Nombre de usuario) y una password (Contraseña) para poder acceder al sistema.

Para poder introducir estos comandos una vez que estas conectado debes pulsar un carácter de escape *ctrl.-]* y esperar aparezca el indicador ***telnet>***, para que la orden tecleada sea procesada por el programa **TELNET** y no por el host remoto.

Uno de lo parámetros más importantes de la configuración de programa cliente Telnet es la **emulación de terminal**. Este parámetro determina la forma que el host va a interpretar los caracteres especiales que enviaremos: Movimiento del cursor, teclas de función, paginación, etc. Ya que cada tipo de terminal suele tener distintos códigos de teclado. Los tipos de terminal más comunes son **VT-100**, **ANSI**, **XTERM.**

El programa **TELNET** permite establecer conexiones utilizando otros puertos distintos de 23, esto te permite conectarte directamente a otros servicios como **FTP**, **SMTP** o incluso **HTTP** y trabajar directamente las órdenes del protocolo. También permite establecer un fichero de registro donde se guardan todas las operaciones que se han realizado durante la conexión.

Actualmente, el servicio Telnet sólo se suele usar en conexiones en intranet al **ser un protocolo poco seguro**, pues no encripta la tramas. Se utiliza en algunos casos en Internet para acceder a servicios de bases de datos de bibliotecas y de otros centros de documentación, aunque en su gran mayoría ha sido sustituidos por servicios Web.

Muchos equipos de interconexión de redes, como switch o router, se pueden administrar mediante telnet.

El protocolo TELNET está especificado en el **RFC 854** y sus parámetros de configuración van del 855 al 861.

2.2.- RLOGIN.

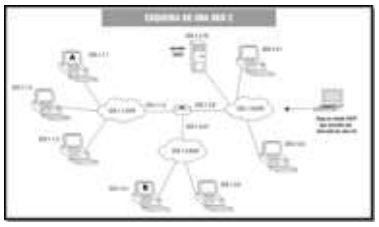
El siguiente servicio que vas a ver es el rlogin, que forma parte del conjunto de utilidades desarrolladas en la versión **BSD** de **UNIX** (rlogin, rsh, rcp, rexec) que permite establecer conexiones entre distintos servidores de forma similar a telnet, ejecutar programas en distintas máquinas (rsh o rexec) o copiar ficheros entre máquinas (rcp).

Ejemplo de uso de comando rcp, para copiar entre mi maquina y la maquina remota maquina2, en la cuenta del usuario operador en el directorio datos.

Ej.- $rcp mensajes.* operador@maquina:/home/usuario01/datos

Estas órdenes pueden ejecutarse sin necesidad de contraseña si tenemos configurados los archivos:

/etc/hosts.equiv. Fichero de configuración general que guarda las máquinas que no precisan autorización, para conectarnos a la nuestra.
.rhosts. Fichero de configuración particular de cada usuario que guarda las máquinas remotas que no precisan autorización, para conectarnos a la nuestra si ya estoy previamente registrado en la maquina remota.



Ministerio de Educación (Uso educativo nc)

El programa **rlogin** provee un servicio de terminal remoto similar al proveído por Telnet. **rlogin** es el comando de sesión remota de Unix. Su sintaxis básica es la siguiente:

rlogin *nombre_de_host*

Autoevaluación

Cual de los siguientes protocolos es de acceso remoto en modo gráfico.

- ○ RLOGIN.
- ○ SSH.
- ○ TELNET.
- ○ RDP.

Error. Este es un protocolo en modo texto para Unix.

Incorrecta. Este no es en modo gráfico.

No es correcta. Este protocolo es en modo texto, típico de Windows.

Efectivamente, es un protocolo de acceso remoto en modo gráfico.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

Para saber más

En este enlace puedes encontrar más información sobre este servicio:
Login remoto.

2.3.- SSH.

Vas a ver ahora el último de los protocolos en modo texto, que viene a resolver la falta de seguridad de los servicios anteriores. Por ejemplo, si tenemos un programa capturador de tramas (sniffer) en la red, como el conocido "wireshark" podemos ver cada una de las órdenes incluidas las contraseñas que se intercambian utilizando telnet o rlogin.

LordT. (CC BY-SA)

SSH está basado en el protocolo SSL (siglas en inglés de Secured Socket Level), desarrollado por Netscape y utiliza un esquema de encriptación asimétrica mediante la generación e intercambio de claves públicas y privadas. SSL es un protocolo que se intercala entre el nivel de transporte y el protocolo de aplicación. Tiene la ventaja de enviar toda la información encriptada. Por otra parte, permite la autentificación tanto del usuario que se conecta como del servidor al cual nos conectamos, con lo que se dificulta la suplantación del servidor o la interceptación de la información.

Aparte de servicios **SSH** existen herramientas como sftp y scp que permiten el intercambio de ficheros al igual que RCP y FTP pero de forma segura.

Un configuración del servicio **SSH**, se realiza editando los ficheros de configuración /etc/ssh/sshd_config (para el servidor) y /etc/ssh/ssh_config (para el cliente), en el mismo directorio encontramos las claves públicas y privadas de nuestro servidor. El fichero **sshd_config** incluye una serie de parámetros que rigen el funcionamiento del servicio.

El servicio SSH soporta dos métodos de autentificación:

- El tradicional basado en **contraseñas** del usuario del sistema.
- Otro basado en claves **públicas y privadas**.

Parámetros básicos.
Puesto de escucha, se puede cambiar por motivos de seguridad: *Port 22.*
IP de escucha, si el equipo tiene varias IP podemos indicar por cual realizaras la escucha del servicio: *ListenAddress 192.168.20.30.*
Versión del protocolo: *Protocol 2.*
Fichero donde se guardan las claves del servidor:
HostKey /etc/ssh/ssh_host_rsa_key.
HostKey /etc/ssh/ssh_host_dsa_key.
Indica si está permita la conexión del superusuario:
PermitRootLogin no.
Permitir el Modo de autentificación mediante clave RSA y clave pública:
RSAAuthentication yes.
PubkeyAuthentication yes.
Modo de autentificación por host (equipo) no por usuario:
HostbasedAuthentication no.
Permitir el túnel del protocolo X-windows por SSH:
X11Forwarding yes.
Permitir o denegar el acceso a determinados usuarios o grupos desde determinadas
máquinas, si un usuario no está en la lista de permitidos se deniega:
AllowUsers fulano@maquina1 mengano@maquina2.
AllowGroups 2esi administradores.
Podemos utilizar la política de denegar:
DenyUsers invitado Pepito.
DenyGroups hacke.

Para saber más

Existe un proyecto de código abierto de programas SSH en la siguiente página Web:

SSH.

2.4.- PuTTY

Trabajando con Microsoft Windows puedes utilizar un software libre llamado “**PuTTY”.** Este permite realizar conexiones con los tres protocolos anteriores y tiene una versión portable.

Alicia Galán Gutiérrez. (Uso educativo nc)

Ahora también lo tienes disponible en varias plataformas Unix, y se está desarrollando la versión para **Mac OS** clásico y **Mac OS** X. Otra gente ha contribuido con versiones no oficiales para otras plataformas, tales como Symbian para teléfonos móviles. Es software beta escrito y mantenido principalmente por Simon Tatham, open source y licenciado bajo la Licencia **MIT** (Massachusetts Institute of Technology, Instituto de Tecnología de Massachusetts).

El nombre **PuTTY** proviene de las siglas **Pu**: Port unique y **TTY**: terminal type. Su traducción al castellano sería: Puerto único para tipos de terminal.

Algunas características de PuTTY son:

El **almacenamiento** de hosts y preferencias para uso posterior.
Control sobre la clave de cifrado SSH y la versión de protocolo.
Clientes de línea de comandos SCP y SFTP, llamados "pscp" y "psftp" respectivamente.
Control sobre el redireccionamiento de puertos con SSH, incluyendo manejo empotrado de reenvío X11.
Completos **emuladores** de terminal XTERM, VT102, y ECMA-48.
Soporte **IPv6.**
Soporte **3DES, AES, RC4, Blowfish, DES.**
Soporte de **autenticación** de clave pública.
Soporte para **conexiones** de puerto serie local.

Para saber más

Aquí tienes el enlace de la página oficial de PuTTy, donde puedes descargarte las diferentes versiones:

PuTTY.

Autoevaluación

SSH está basado en el protocolo:

Enviar

El servicio SSH está basado en el protocolo SSL, desarrollado por Netscape.

La **licencia MIT** es una de tantas licencias de software que ha empleado el Instituto Tecnológico de Massachusetts a lo largo de su historia, y quizás debería llamarse más correctamente **licencia X11**, ya que es la licencia que llevaba este software de muestra de la información de manera gráfica X Window System originario del **MIT** en los años 1980. Pero ya sea como **MIT** o **X11**, su texto es idéntico.

El texto de la licencia **no tiene copyright**, lo que permite su modificación. No obstante, esto puede no ser recomendable e incluso muchas veces dentro del movimiento del software de código abierto desaconsejan el uso de este texto para una licencia. A no ser que se indique que es una modificación y no la versión original. La licencia **MIT** es muy parecida a la licencia **BSD** en cuanto a efectos.

3.- Terminales remotos en modo gráfico.

Caso práctico

Stockbyte. (Uso educativo nc)

María ha descartado el uso de herramientas en modo texto, lo que sí que parece interesarla es Putty, una herramienta que sirve para administración remota, en su versión portable, para llevarla en el pendrive USB.

"Para los usuarios inexpertos usar programas en entorno gráfico es mucho más sencillo" -pensó María.

"En el instituto necesitan compartir una pantalla, con una presentación para varios ordenadores y va a ser más fácil para ellos si les facilito un entorno gráfico" –reflexionó María.

"Voy a revisar los diversos programas que me permiten manejar un equipo de forma remota en modo gráfico" –se puso como tarea María.

"Hay algunos muy versátiles y otros más específicos. Tengo que ver cuales se acoplan mejor en cada una de las empresas en las que voy a instalar este servicio".

"Para el Instituto podría ir bien una versión portable, así no hace falta instalarlo en todos los ordenadores y cuando lo necesiten en un aula lo pueden llevar en el pendrive".

"En el periódico usan frecuentemente unidades PDA, tendré que pensar sobre esto también".

"Empezare buscando uno apropiado para el instituto…" –empezó a actuar María.

Los anteriores sistemas de conexión remota permiten establecer un terminal en modo texto, donde un usuario normal o un administrador pueden introducir los comandos que necesite. Con el incremento de la velocidad de la redes se han creado nuevas herramientas que permiten la conexión gráfica con las mismas características del entorno remoto: resolución, escritorio, uso del ratón, etc...

Existen diversos programas que nos permiten manejar un equipo desde otro, de forma remota, si están conectados en red. Algunos transmiten la imagen remota de la pantalla del servidor, mientras que otros solo envían las coordenadas X e Y del cursor, simulando el sistema operativo anfitrión.

Autoevaluación

¿Cuál es el protocolo de acceso remoto en modo texto más seguro?

- ○ TELNET.
- ○ RLOGIN.
- ○ SSH.
- ○ Ninguno es seguro.

Incorrecto. No es nada seguro, la información no viaja protegida.

Error. No es seguro, cualquiera puede ver la información que viaja por la red.

Correcta. Es el más seguro.

No es correcto. SSH es más seguro que los demás.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

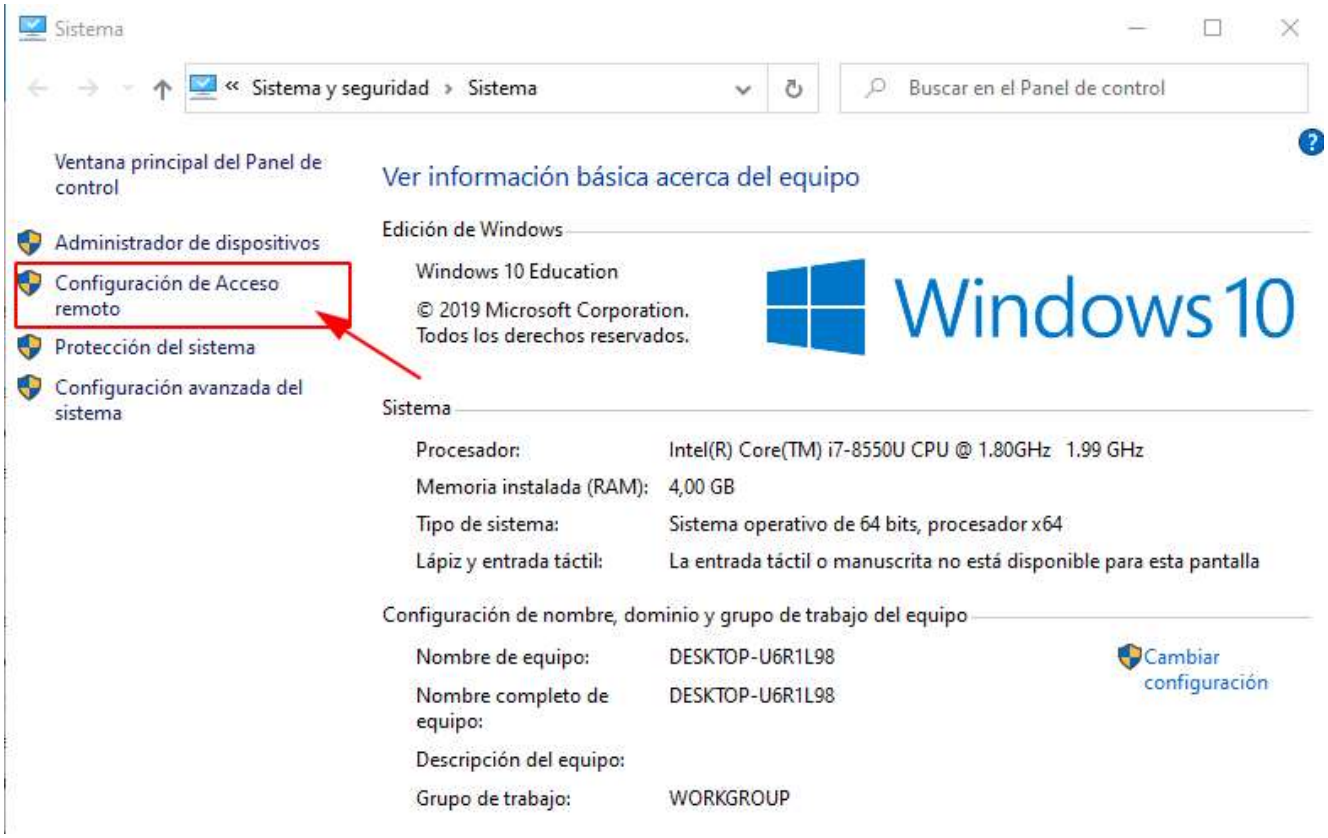
3.1.- Servicios remotos de Windows: Terminal Server, Escritorio Remoto, RDP.

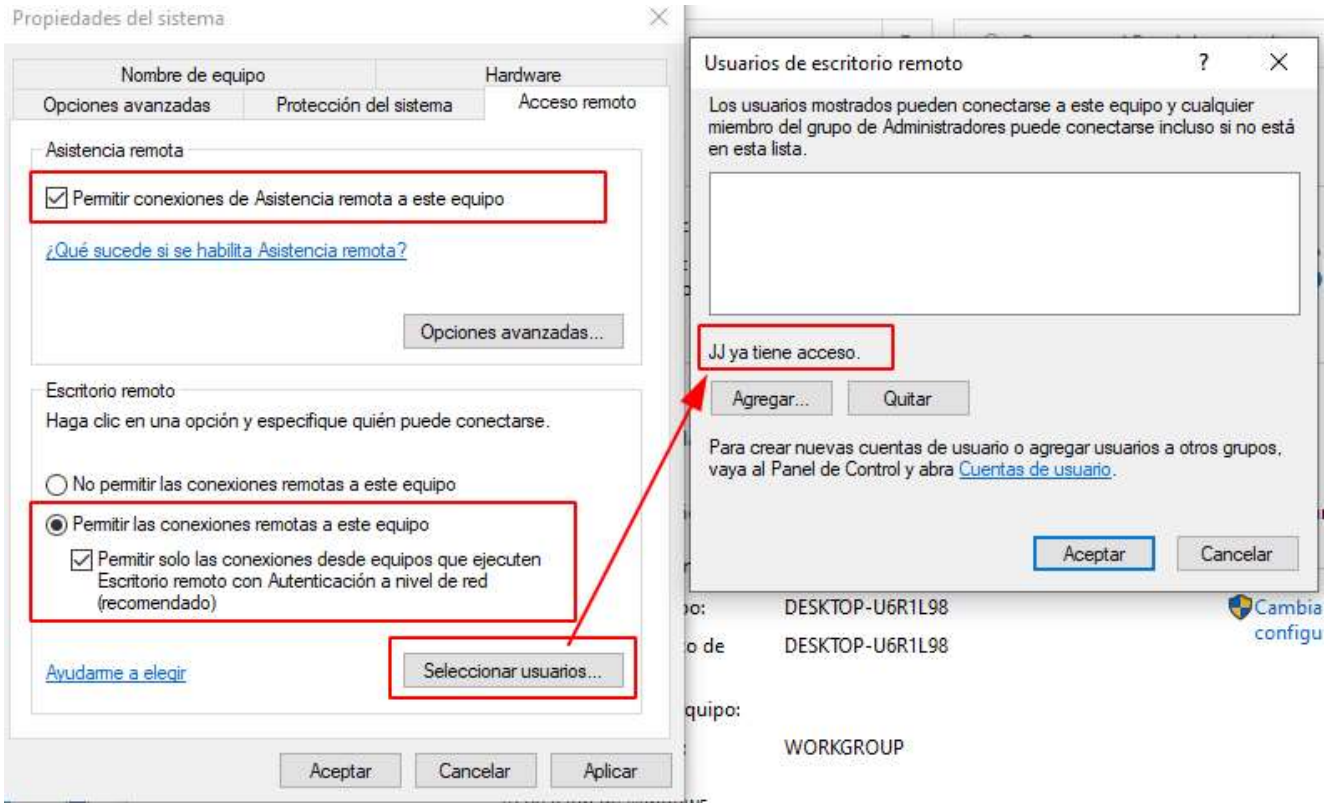
Terminal Server es una herramienta de Windows que permite la conexión remota de usuarios a un servidor Windows mediante el protocolo RDP (Remote Desktop Protocol). Utiliza el puerto 3389. Este protocolo no permite la conexión desde más de un cliente, salvo en Windows Server.

La información gráfica que genera el servidor es convertida a un formato propio de RDP y enviada a través de la red al terminal, que interpretará la información contenida en el paquete del protocolo para reconstruir la imagen a mostrar en la pantalla del terminal.

En cuanto a la introducción de órdenes en el terminal por parte del usuario, las teclas que pulse éste en el teclado del terminal, así como los movimientos y pulsaciones del ratón son redirigidos al servidor. El protocolo proporciona dos características importantes: cifrado y compresión de los datos por motivos de seguridad, y para un mejor rendimiento en las redes de menor velocidad.

Para este ejemplo usaremos un sistema con Windows 10. Desde el explorador de Windows, pulsamos con el botón derecho del ratón para acceder a las “Propiedades” de “Este equipo” y vemos la siguiente pantalla:



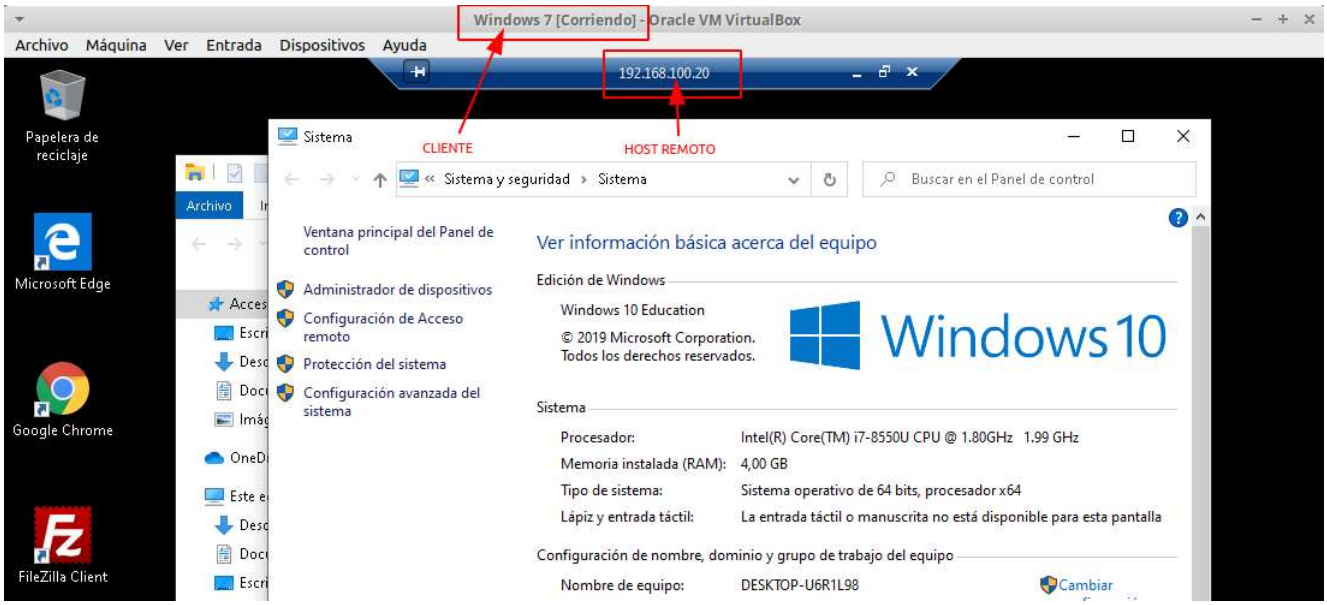


José A. Jiménez (CC0)

Desde otro sistema (por ejemplo, Windows 7) abrimos la herramienta de conexión a escritorio remoto.

El sistema nos preguntará la contraseña remota y a continuación cargará el entorno gráfico del entorno anfitrión, pero en el caso de Windows 10 (o cualquier versión que no sea Server) cerrará cualquier otra conexión abierta:

José A. Jiménez (CC0)



José A. Jiménez (CC0)

3.2.- Sistemas Unix-Linux (X Windows System).

Y ahora le toca el turno a los sistemas Unix-linux. En este apartado vas a conocer **X Windows System** (Sistema de ventanas X). La versión actual de este protocolo es 11 por lo cual se le suele llamar **X11.**

El sistema de **ventanas X** también llamado "Servidor de las X", es el encargado de los entornos visuales en los sistemas operativos basados en Unix-Linux. Fue el resultado de un proyecto académico llamado **"Athena"** en el Instituto de Tecnología de Massachusetts (**MIT**) a mediados de los 80. Actualmente, las implementaciones principales son *Xfree86* y *X.org.*
X fue diseñado con una arquitectura **cliente-servidor**:

> El **Servidor** X es el que mantiene el control exclusivo de la pantalla y es el encargado de comunicarse con el dispositivo utilizado para la visualización de los gráficos.
> El **cliente** se comunica con el servidor y le indica cosas básicas como: "Trazar una línea de aquí para acá", "Colar un punto aquí".

Lo característico de esta arquitectura radica principalmente en que no se limita a un cliente que esté en el mismo equipo que el servidor, sino a clientes remotos por medio de protocolos de comunicación como el **TCP/IP**. En los sistemas UNIX Linux, las aplicaciones gráficas utilizan, normalmente, un protocolo de red denominado X-Windows (Puerto 6000) que permite que un programa pueda ser manejado desde cualquier ordenador de la red que disponga de este servicio.

Alicia Galán Gutiérrez. (Uso educativo nc)

En este sistema cualquier programa que trabaja con el entorno gráfico es un **cliente** de X y cualquier máquina que disponga de un terminal gráfico es un **servidor** de X.

Para configurar el equipo remoto en Ubuntu primero tienes que habilitar la opción que permite utilizarlo. Accedes a Sistema, Preferencias, Escritorio remoto y seleccionas **Permitir a otros usuarios ver mi escritorio**. Si queremos que el usuario remoto pueda controlar dicho escritorio debemos seleccionar de forma adicional **Permitir a otro usuario controlar su escritorio.** También podemos confirmar cada acceso y/o requerir que el usuario introduzca una contraseña, dentro de las opciones de **Seguridad.**

Si te vas a conectar desde otro sistema que no es Ubuntu, necesitas un cliente de escritorio remoto, como por ejemplo **VNC** viewer. Si estás en Ubuntu, debes ir a Aplicaciones, seleccionar Internet y, por ultimo, hacer clic en **Visor de escritorios remotos.**

Massachusetts Institute of Technology (MIT o Instituto Tecnológico de Massachusetts) es una de las instituciones dedicadas a la docencia y la investigación más importantes de Estados Unidos. MIT es considerada como una de las mejores universidades de ciencia e ingeniería del mundo. Esta situado en Cambridge, Massachusetts y cuenta con numerosos premios Nóbel.

Autoevaluación

¿Qué puerto utiliza el protocolo RDP?

- 9833.
- 3389.
- 3388.
- 6000.

Incorrecto. Si lo hubieras puesto al revés…

Correcta. Ya veo que no se te escapa un detalle.

Has fallado. Por un número.

Error. Está lejos de la solución.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

3.3.- Servicios RDP en Linux

Cliente RDP para Linux

Además de clientes windows, también es posible conectarse a Terminal Server con un cliente Linux mediante el escritorio remoto. Existen diferentes clientes, como “freerdp”:

```
$ sudo apt install freerdp
```

Y desde el cliente nos podemos conectar al servidor Windows de esta forma:

```
profesor@randomax90:~/Escritorio$ xfreerdp -u JJ 192.168.100.20
WARNING: Using deprecated command-line interface!
connected to 192.168.100.20:3389
Password:
```

Servidor RDP para Linux

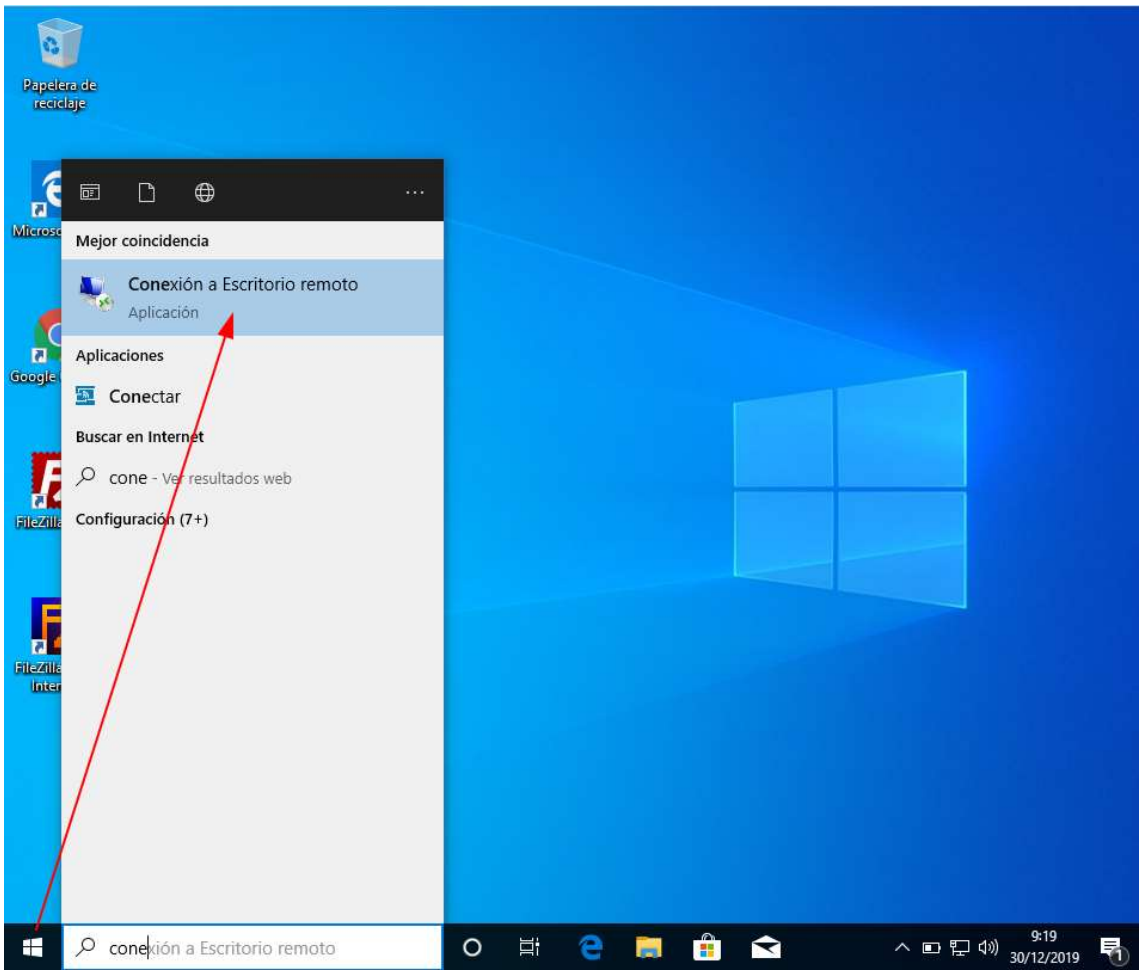
Igualmente, podemos instalar un Servidor RDP (por ejemplo, xrdp) para tener acceso remoto a nuestro sistema Linux desde un sistema Windows:

```
$ sudo apt install xrdp
```

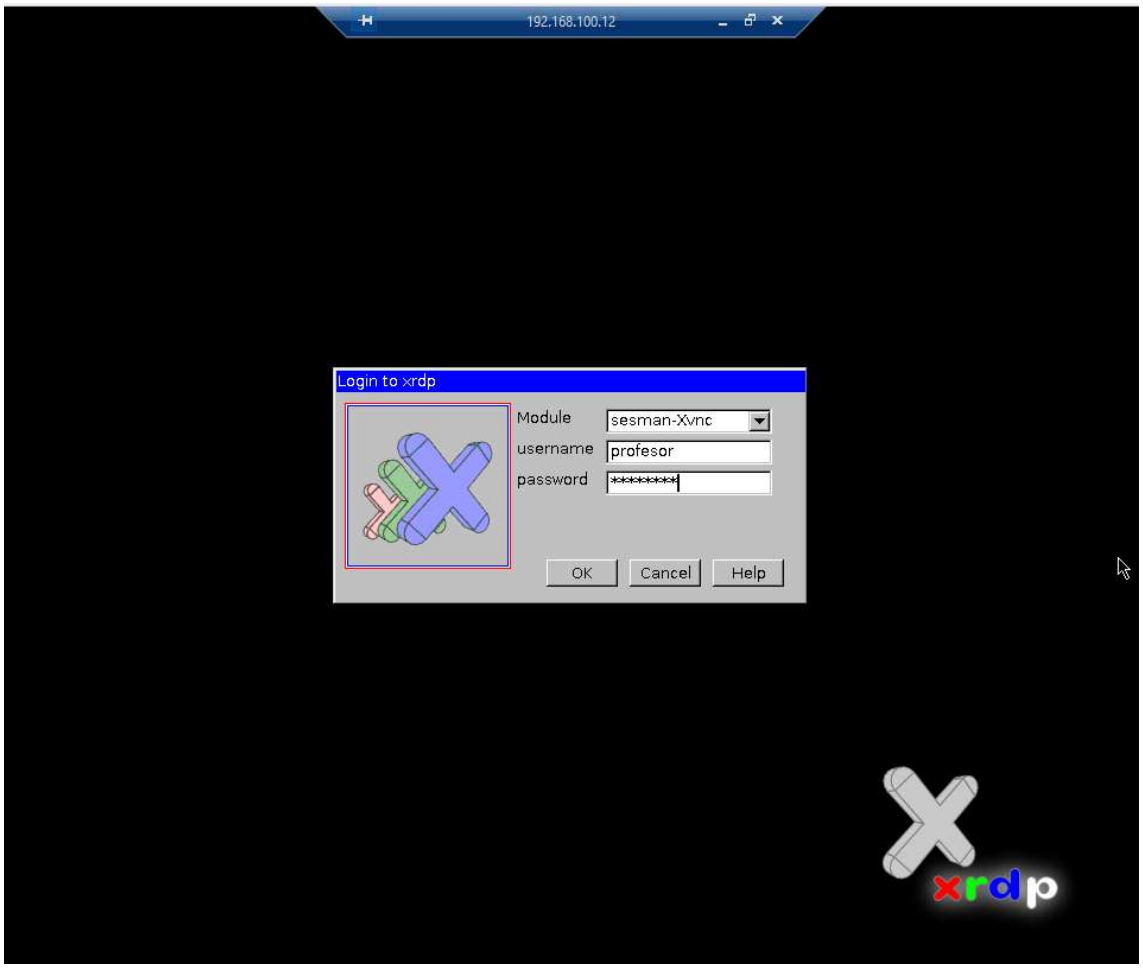
Y ahora podremos conectarnos en modo gráfico a nuestro servidor Linux desde cualquier equipo de la red.

Cliente de Escritorio Remoto desde Windows

Desde una máquina Windows también podemos abrir una **Conexión a Escritorio Remoto** que nos permitirá conectar con nuestro servidor Linux:



José A. Jiménez (CC0)



Esta herramienta nos permite realizar múltiples accesos concurrentes al servidor.

3.4.- Otros Accesos: Teamviewer y VNC.

Alicia Galán Gutiérrez. (Uso educativo nc)

Para conectar a un equipo remoto desde cualquier sistema operativo, también se puede utilizar software no incluido en los sistemas operativos de Microsoft. Uno de los más utilizados es el VNC (son las siglas en inglés de Virtual Network Computing, traducido Computación Virtual en Red).

El software viene incluido en el paquete de aplicaciones y servicios que por defecto traen la mayoría de las distribuciones de linux, con lo que no necesitas instalarlo. Sin embargo, en los sistemas Windows sí tienes que instalarlo a través de los ficheros correspondientes de cliente y/o servidor.

Otra opción no menos interesante, muy práctica y sencilla de utilizar, es el software **TeamViewer**.

En la siguiente dirección Web, puedes bajar el software, tanto en su versión cliente como en la de servidor:

VNC.

Para saber más

En este enlace puedes ver la documentación oficial de TeamViewer para su instalación, configuración y uso:

Documentación sobre acceso remoto con TeamViewer.

3.5.- Servicio VNC.

VNC son las siglas en inglés de Virtual Network Computing (Computación Virtual en Red). El servidor utiliza el puerto 5900, los clientes de Windows el puerto 5800, y los de Linux y Mac OS el terminal que no estén usando (si solo has activado un terminal, el siguiente puede acceder desde el puerto 5801, si tenemos activados cuatro debemos conectarnos por el puerto 5804, etc.).

Alicia Galán Gutiérrez. (Uso educativo nc)

VNC es un servicio de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente. VNC no impone restricciones en el sistema operativo del servidor: se puede compartir la pantalla de una máquina con cualquier sistema operativo que admita VNC conectándose desde otro ordenador o dispositivo que disponga del cliente VNC.

La versión original del VNC se desarrolló en los laboratorios AT&T Olivetti Research Laboratory, en Cambridge. El programa era de código abierto, por lo que cualquiera podía modificarlo. Existen hoy en día varios programas para el mismo uso, muchos de cuyos derivados son software libre con licencia GPL.

El programa servidor suele tener la opción de funcionar como servidor HTTP para mostrar la pantalla compartida en un navegador con java. En este caso el usuario remoto (cliente) no tiene que instalar un programa cliente de VNC sino que es descargado por el navegador automáticamente.

VNC es independiente de la plataforma. Un cliente VNC de un sistema operativo puede conectarse a un servidor VNC del mismo sistema operativo o de cualquier otro. Hay clientes y servidores tanto para muchos sistemas operativos basados en GUI como para java. Varios clientes pueden conectarse a un servidor VNC al mismo tiempo. Los usos populares de esta tecnología incluyen ayuda técnica remota y acceso a los archivos presentes en el ordenador del trabajo desde la computadora de la casa o viceversa.

Hay una serie de variantes de VNC que ofrecen, aparte de las funciones típicas de VNC, funciones particulares; por ejemplo, algunos están optimizados para Microsoft Windows; otros disponen de transferencia de archivos, (que no es propiamente parte de VNC), etc. Muchos son compatibles (sin funciones adicionales) con el propio VNC en el sentido de que un usuario de una variante de VNC puede conectar con un servidor de otra, mientras que otros se basan en el código fuente de VNC, pero no son compatibles con el estándar VNC.

Las características más importantes de **VNC** son:

Permite crear **pantallas virtuales** en Linux y Mac OS, pero solo puede compartir la pantalla actual en Windows.
En algunas versiones puede **compartir la pantalla** con varios clientes a la vez.
Permite **compartir impresoras**.
Permite **FTP seguro**.
Permite **chat seguro.**
Puede **compartir aplicaciones** con servidores Windows.

VNC es un escritorio remoto útil para muchos propósitos, ocupa muy poco y sirve para cualquier sistema operativo.

Autoevaluación

Para instalar el servidor VNC en Linux, lo hacemos desde el paquete:

Enviar

Para los servidores **VNC**, desde Linux, ejecutas **vcnserver.**

A continuación veremos un pequeño ejemplo con una de las formas de usar VNC posibles:

Configuración VNC en Servidor:

```
$ sudo apt install x11vnc
$ sudo ufw allow 5900/tcp
$ xhost +
$ x11vnc -usepw
```

Configuración VNC en Cliente:

En cualquier dispositivo se puede utilizar un software cliente como "vncviewer". Si el cliente está en Linux, se lanza con:

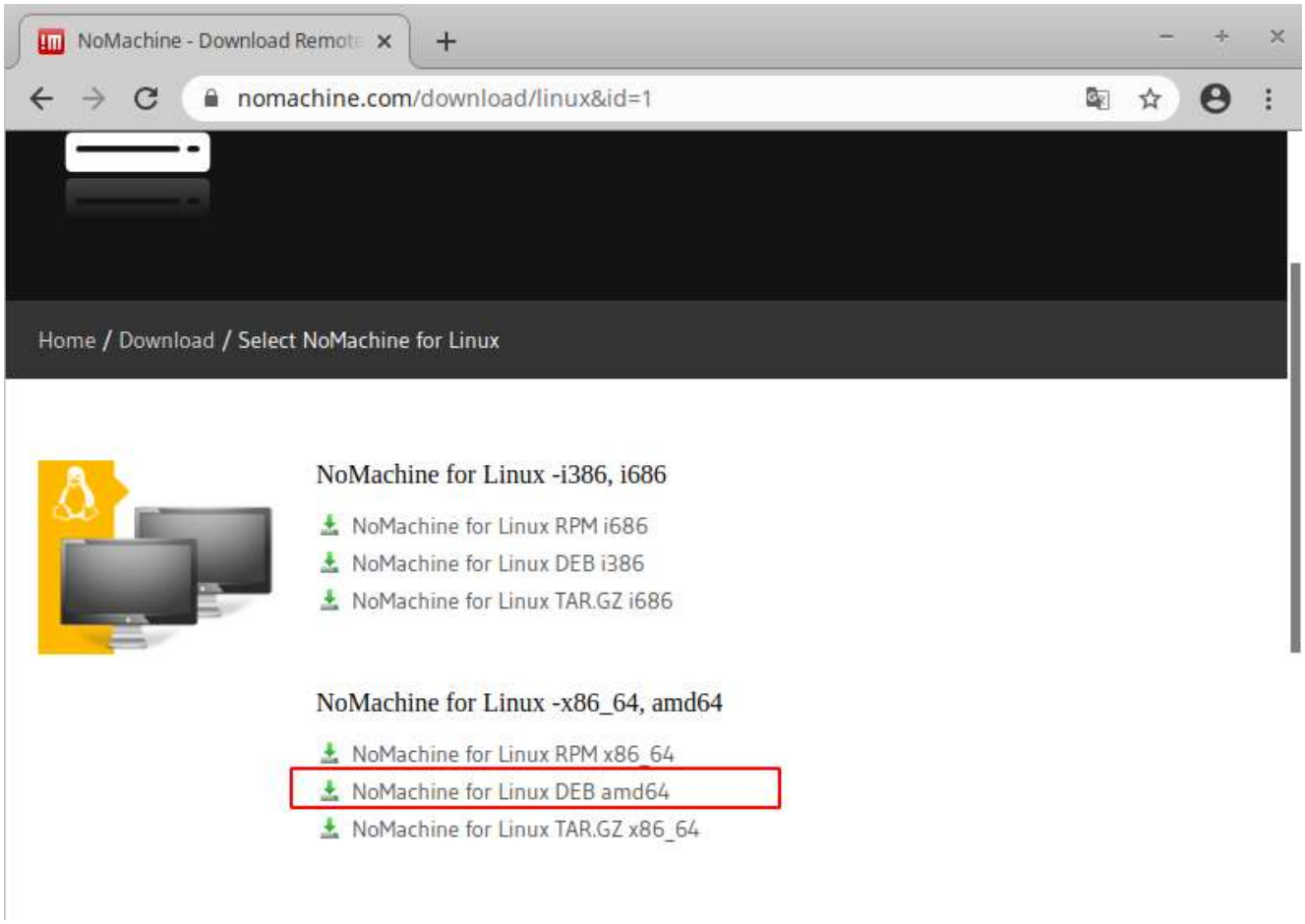
```
$ vncviewer <IP>:0
```

Como ejemplo, el siguiente vídeo muestra cómo configurar el servidor x11vnc en un sistema Linux Ubuntu 18.04 y acceder a él desde diferentes clientes, como un iPad

https://www.youtube.com/embed/ACr82ZaeWYk

3.5.- Tecnología NX

La **tecnología NX** permite realizar conexiones remotas X11 muy rápidas a través de las cuales los usuarios pueden acceder a escritorios remotos de Linux o Unix incluso bajo conexiones que no sean demasiado potentes. NX realiza una compresión directa del protocolo X11, lo que permite una mayor eficiencia que VNC. La información se envía mediante SSH, por lo que toda la información que se intercambian servidor y cliente está cifrada.
Existe una implementación libre de esta aplicación, llamada **FreeNX**. El software puede descargarse de www.nomachine.com.



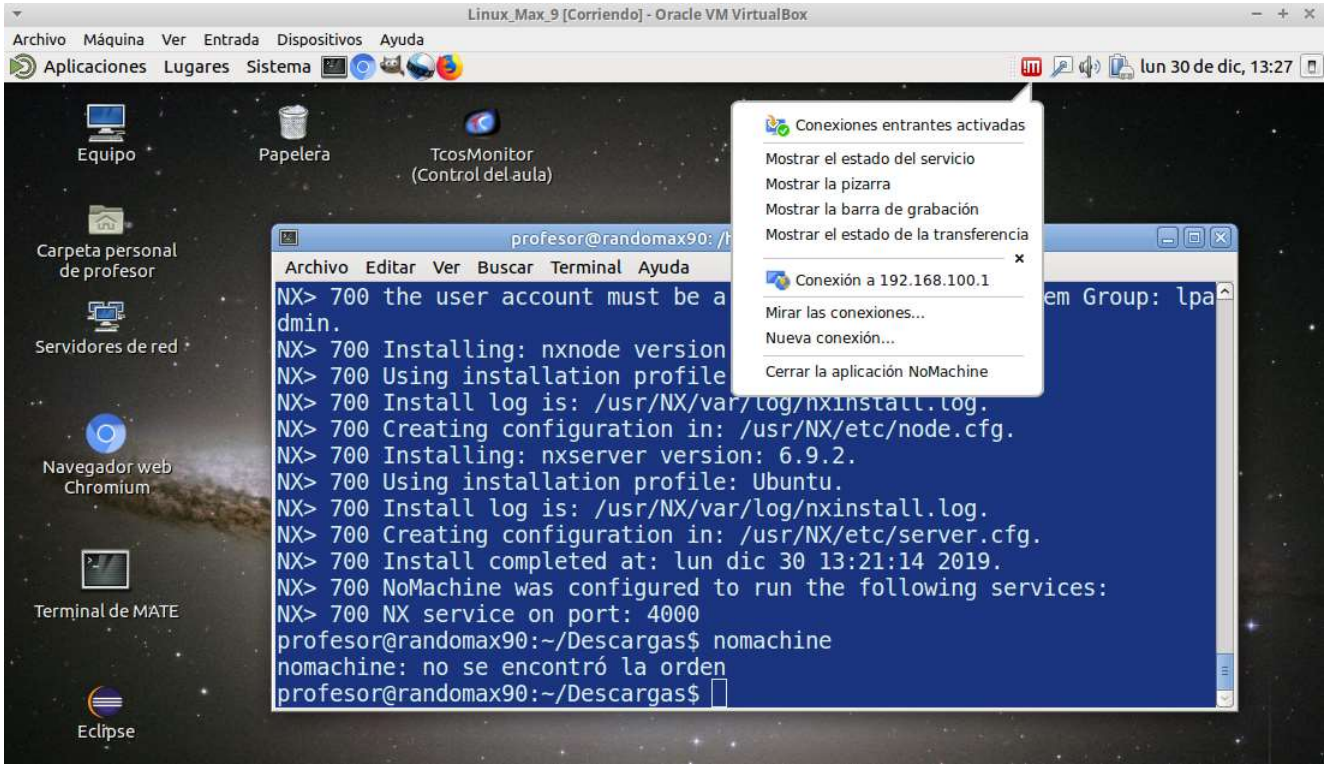
José A. Jiménez (CC0)

Y una vez descargado, se instala con:

```
profesor@clientedns:~/Descargas$ sudo dpkg -i nomachine_6.9.2_1_amd64.deb
```

Instalaremos la aplicación en dos sistemas diferentes, uno hará de servidor y el otro de cliente. En ambos tendremos la aplicación instalada y accesible desde el menú principal.

Utilizaremos como servidor un equipo que, en nuestro ejemplo, tiene la IP 192.168.100.12:

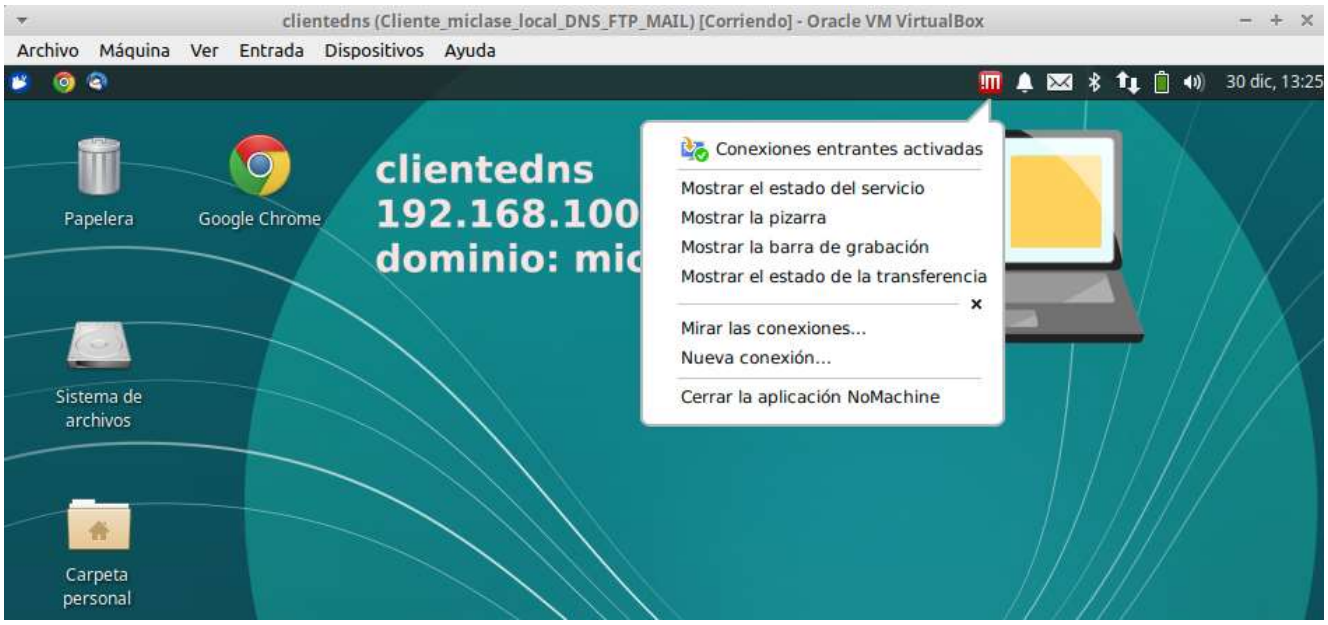


José A. Jiménez (CC0)

Pulsamos en “Mostrar el estado del servicio” para verificar que está activo, y vemos que así es:

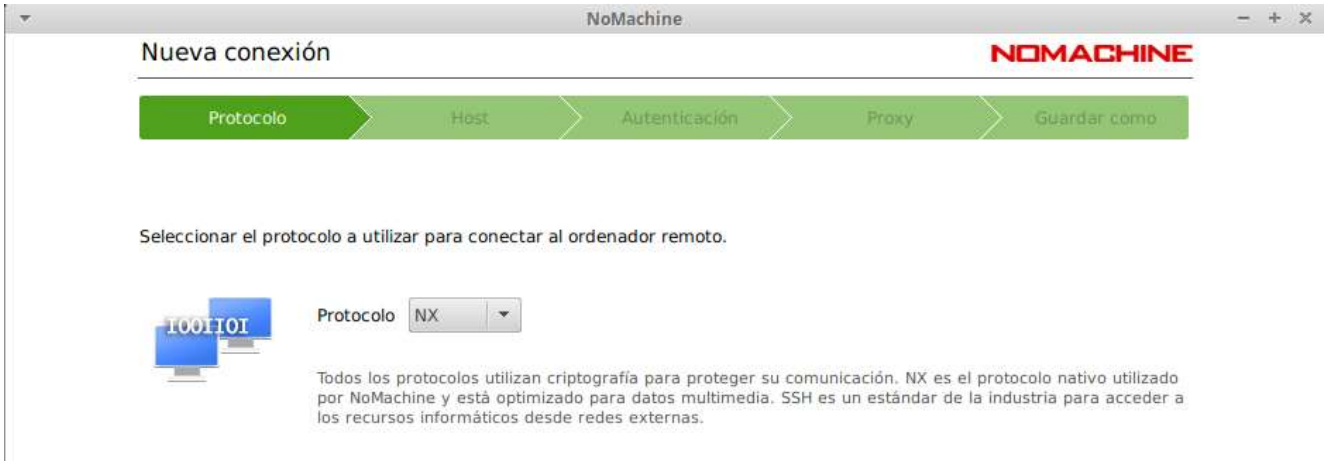
José A. Jiménez (CC0)

Desde el cliente, donde también hemos instalado la aplicación, abrimos el menú “Nueva conexión”:

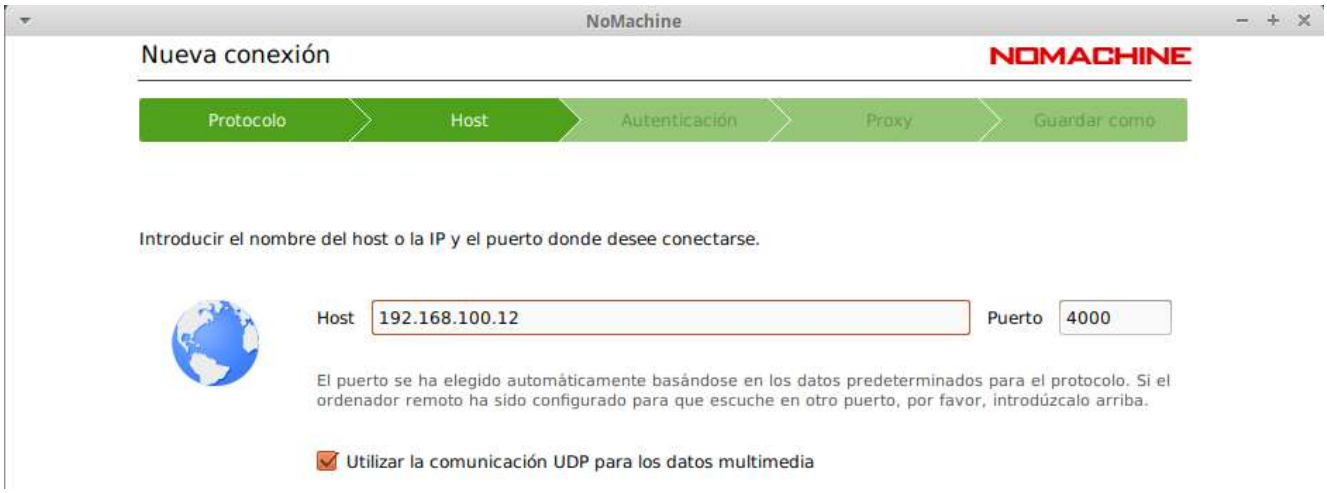


José A. Jiménez (CC0)

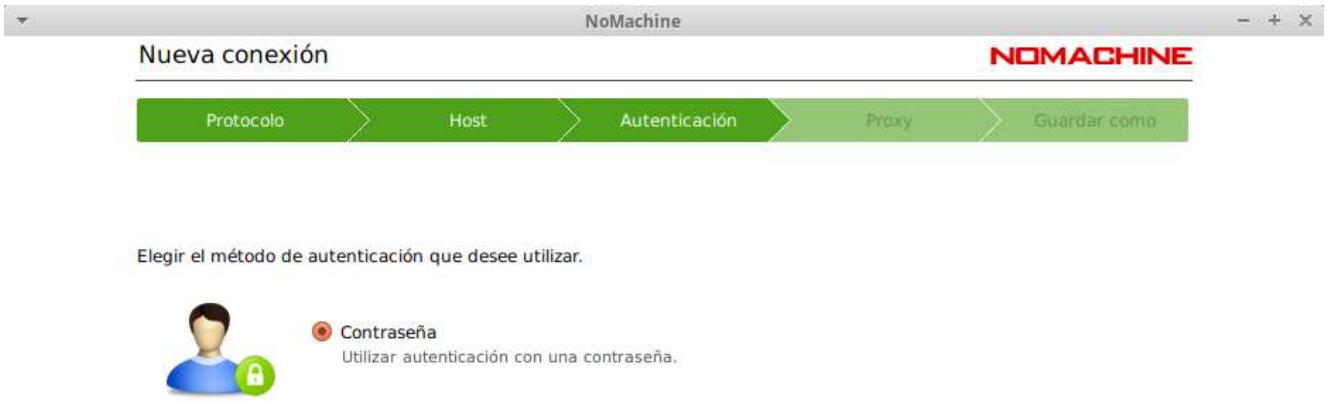
Seguimos los pasos del configurador automático:



José A. Jiménez (CC0)

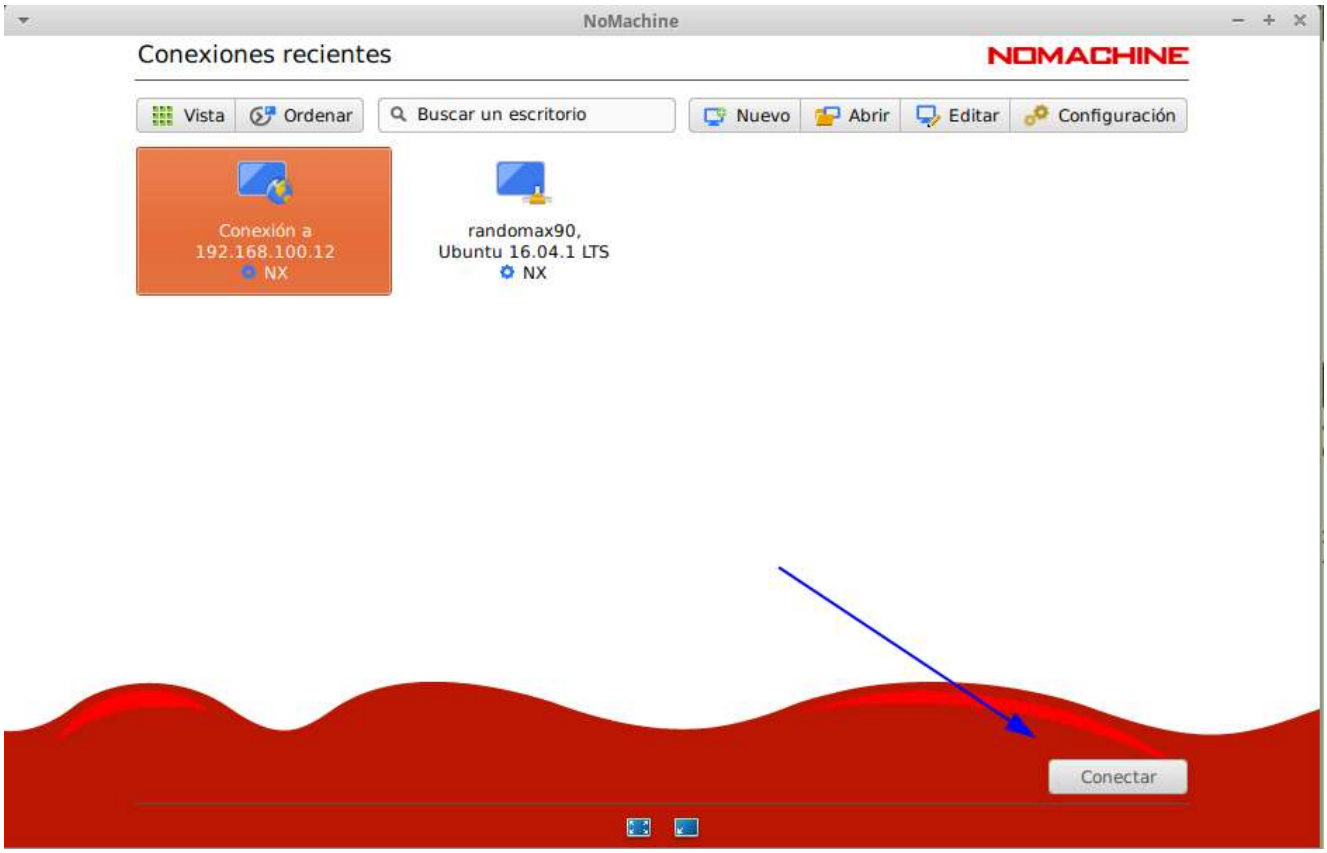


José A. Jiménez (CC0)



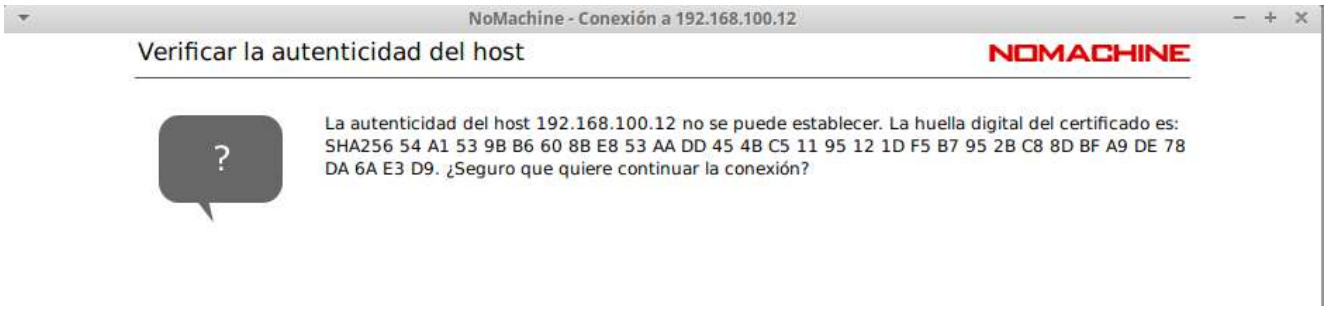
José A. Jiménez (CC0)

A continuación nos permitirá crear un icono en el escritorio para realizar la conexión directamente, y nos presentará la pantalla de conexiones:

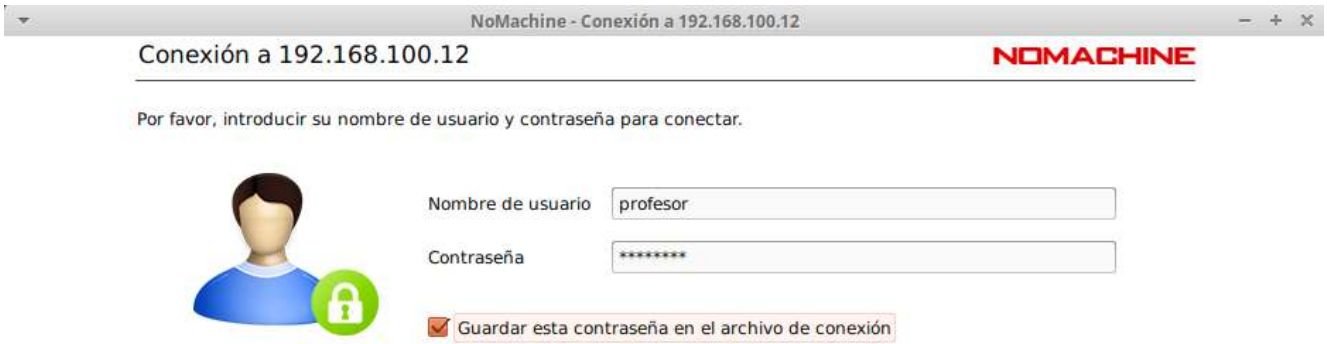


José A. Jiménez (CC0)

La primera vez que accedemos, la aplicación necesitará instalar un certificado, después nos preguntará las credenciales de acceso y finalmente estará lista para establecer la conexión:

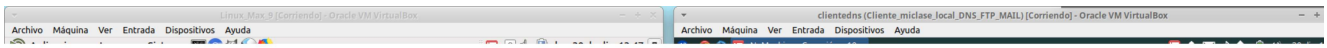


José A. Jiménez (CC0)



José A. Jiménez (CC0)

Y en este momento, desde el cliente tendremos una ventana que replicará literalmente el aspecto del servidor:



José A. Jiménez (CC0)

También existe el software cliente NX para Windows y para Mac. Puedes acceder a la página de descargas de la aplicación para obtener la versión que necesites:

https://www.nomachine.com/download

Autoevaluación

Para conectar el equipo remoto Ubuntu desde Windows XP, se usa el programa:

- ○ NVC.
- ○ VNC.
- ○ logMein.
- ○ No se puede.

No es correcto, pero casi aciertas. Fíjate un poco más.

Correcta. Ya veo que no se te escapa un detalle.

No, no. Has fallado.

Si se puede. Has fallado.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

4.- Seguridad en el acceso.

Caso práctico

Para María, como para la mayoría de las administradoras y los administradores de una red, es tan importante o mas, la seguridad en el acceso remoto como mantener actualizadas las definiciones de virus.

Stockbyte. (Uso educativo nc)

"Tengo que estudiar el tema de la seguridad para dar soporte a las empresas desde mi oficina y quiero hacerlo por Internet" -pensó María-. "Los datos transmitidos por Internet viajan de forma más vulnerable que cuando lo hacen por una red interna".

"Para curarme en salud lo mejor sería que toda la información viajara encriptada. Pero bueno, quizá el coste es muy alto según las necesidades de cada caso" –reflexionó María.

"Tengo que buscar soluciones para cada empresa…"

"Los protocolos de seguridad que tiene, por ejemplo, una central nuclear son muy diferentes a los de una oficina" –recordó María, añorando su época de becaria en una conocida central nuclear del país.

Como puedes imaginar esta es una cuestión importante a tener en cuenta, sobre todo si la información a la que se accede desde un acceso remoto es confidencial. Las principales prioridades y preocupaciones de los administradores de red son:

- La seguridad en el acceso remoto.
- Las actualizaciones de seguridad.
- El parcheado de los sistemas.
- La monitorización de intrusiones.
- La transferencia segura de archivos.
- Los planes de contingencia y recuperación del servicio.

Por lo tanto, ya sabes qué es lo que te puede quitar el sueño, cuando seas administrador o administradora de una red.

Como sabes por lo leído anteriormente, en los protocolos de conexión o de terminal remota **en modo texto, el único que ofrece seguridad es SSH**, Tiene la ventaja de enviar toda la información encriptada. Por otra parte, permite la autentificación tanto del usuario que se conecta como del servidor al cual nos conectamos, con lo que se dificulta la suplantación del servidor o la interceptación de la información.

Para saber más

La Versión 1 de SSH se creo en 1995 pero ya no se utiliza porque emplea mucho procesador. El protocolo SSH-2 está especificado en RCF 4651 y sus parámetros van del 4652 al 4656. Para saber más sobre la encriptación de la clave pública te aconsejamos que leas el RCF 4716 y para los tipos de encriptación el 4344. Todas estas normas están en inglés en el siguiente enlace:

RFC.

4.1.- Seguridad en el acceso. Soluciones.

El problema de la seguridad en el acceso remoto te surge cuando éste se hace por Internet. En la estructura básica de cualquier empresa, son las redes de área local (**LAN**) las que realizan la conexión entre los diferentes equipos. Estas redes se conectan cada vez más a Internet mediante un equipo de interconexión, denominado router. En muchas ocasiones, las empresas tienen la necesidad de comunicarse con sus sucursales, con su clientela o con los comerciales que viajan constantemente y que están alejados geográficamente.

Stockbyte. (Uso educativo nc)

Sin embargo, los datos transmitidos a través de Internet viajan de forma más vulnerable que cuando lo hacen por la red interna y pueden ser interconectados por alguna persona ajena a la entidad, ya que la ruta tomada no está definida por anticipado. Esto significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo de la línea, un usuario escuche la red y se apropie de los datos. Es por esto que la información de una organización o empresa no debe ser enviada bajo estas condiciones de inseguridad, sobre todo si son datos confidenciales.

Existen **dos posibles soluciones** para este problema:

Utilizar **redes dedicadas** para establecer una comunicación segura entre dos puntos alejados geográficamente. Sin embargo, esta solución no es fácil ni económica, se hace inviable para la mayoría de las empresas.
Otra posible solución es utilizar el medio inseguro de Internet como medio de transmisión, con un **protocolo túnel**, que nos aporte seguridad y privacidad en los datos transmitidos. Esto significa que los datos se van a encapsular, antes de ser enviados de manera cifrada. El término **Red privada virtual**, en ingles Virtual Private Network, abreviado **VPN,** se utiliza para hacer referencia a este tipo de **red artificial**. El termino **virtual** hace referencia a la conexión de dos redes físicas de área local a través de una conexión poco fiable como es Internet y el término **privada** porque solo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden acceder a los datos y recursos de la red del otro lado de la red privada virtual.

Así, las redes privadas virtuales dan la posibilidad de una conexión segura a bajo coste, ya que no requieren una línea dedicada contratada a una empresa de comunicaciones. No obstante, no garantizan una calidad de servicio similar a una línea dedicada, ya que la **red es pública** y, por lo tanto, no es segura del todo.

El funcionamiento de una red privada virtual se basa en un protocolo de **túnel**, este protocolo cifra los datos que se transmiten desde un lado de la VPN hacia el otro. En la unidad 8 estudiarás más en detalle este tipo de redes.

Autoevaluación

Existen dos soluciones para la seguridad en accesos remotos. Uno es el uso de redes dedicadas y el otro es el uso de un protocolo de:

Enviar

Son los protocolos de túnel que encapsulan los datos antes de ser enviados.