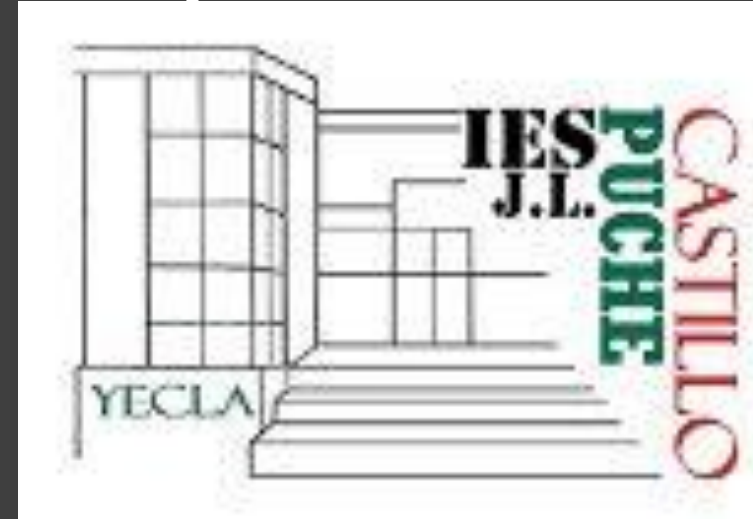




Despliegue de aplicaciones web



Unidad 1 – El servicio de control remoto.

Profesora:
blanca.palao@murciaeduca.es

Índice contenidos – Acceso remoto

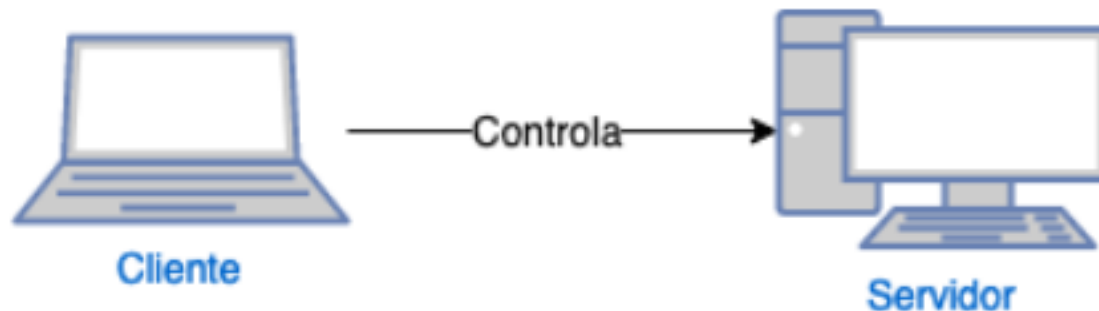
1. Seguridad en el acceso.
2. Terminales en modo texto, línea de comandos.
3. Terminales en modo gráfico.
4. Acceso remoto mediante web.
5. Administración remota entre equipos con diferente sistema operativo.
6. Instalación y configuración del servicio de acceso remoto en sistemas operativos libres y propietarios.

Introducción

Para un administrador de sistemas, el servicio de acceso remoto es fundamental, ya que permite:

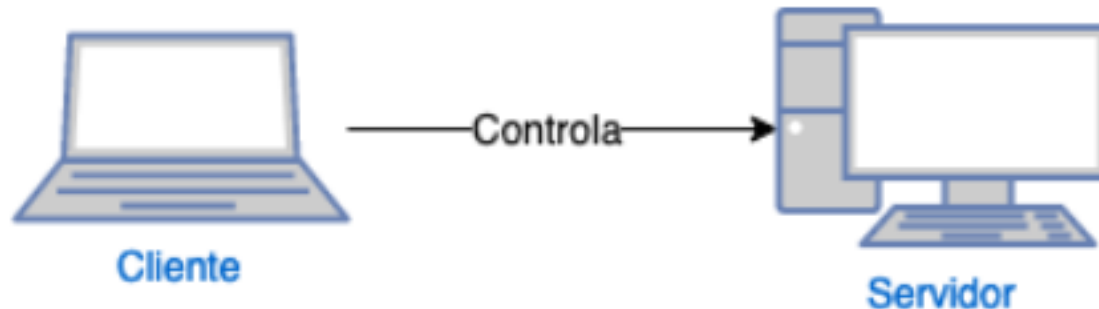
- **Administrar y resolver problemas en un servidor** o equipo sin necesidad de estar físicamente presente.
- Asesorar y ofrecer **apoyo técnico**, así como soluciones de problemas informáticos a usuarios, sin realizar ningún desplazamiento.

El esquema de funcionamiento de este servicio es muy sencillo:



Introducción

En el ordenador al que queremos acceder, le llamamos **servidor**, tenemos que tener un servicio que permita el control remoto. En el ordenador desde el que queremos acceder, le llamamos **cliente**, nos servirá para controlar el servidor, instalaremos el software cliente que permitirá acceder al servidor. Esta conexión puede realizarse en una red local o a través de la red pública. Es evidente que, especialmente si lo utilizamos a través de la red pública, tengamos muy presente la seguridad (en la asignatura de seguridad informática, profundizaréis).



1. Seguridad en el acceso. SSH.

Para los administradores de sistemas, **la seguridad en el acceso remoto es algo fundamental**. Normalmente activamos el acceso a través de una red pública, por lo que nuestra comunicación debe asegurarse todo lo posible.

- Una de las opciones más seguras es **SSH**, ya que la comunicación se encripta utilizando una combinación de claves simétricas y asimétricas (lo veis en Seguridad). Por lo tanto, cualquier agente que vigile esa conexión, únicamente accederá a información ininteligible.

1. Seguridad en el acceso. SSH.

SSH (Secure Shell) es un protocolo de acceso remoto por línea de comandos seguro, en el que la comunicación se encuentra cifrada. Por defecto, la conexión se realiza a través del puerto **22 TCP**.

-> Para instalar **un servidor SSH** en **Ubuntu**, basta con escribir:

```
sudo apt install openssh-server
```

Para controlar remotamente al servidor, basta con ejecutar en una máquina con un cliente ssh instalado el siguiente comando:

```
ssh USUARIO_SERVIDOR@IP_SERVIDOR
```

1. Seguridad en el acceso. SSH.

Podemos ver una explicación completa acudiendo al comando "**man**":

```
man ssh_config
```

Como la mayoría de los servicios en Linux, podemos ver el estado del mismo con el siguiente comando:

```
sudo service ssh status
```

Cambiando la palabra "status", podemos realizar otras acciones como pararlo (stop), iniciarlo (start) o reiniciarlo (restart).

1. Seguridad en el acceso. SSH.

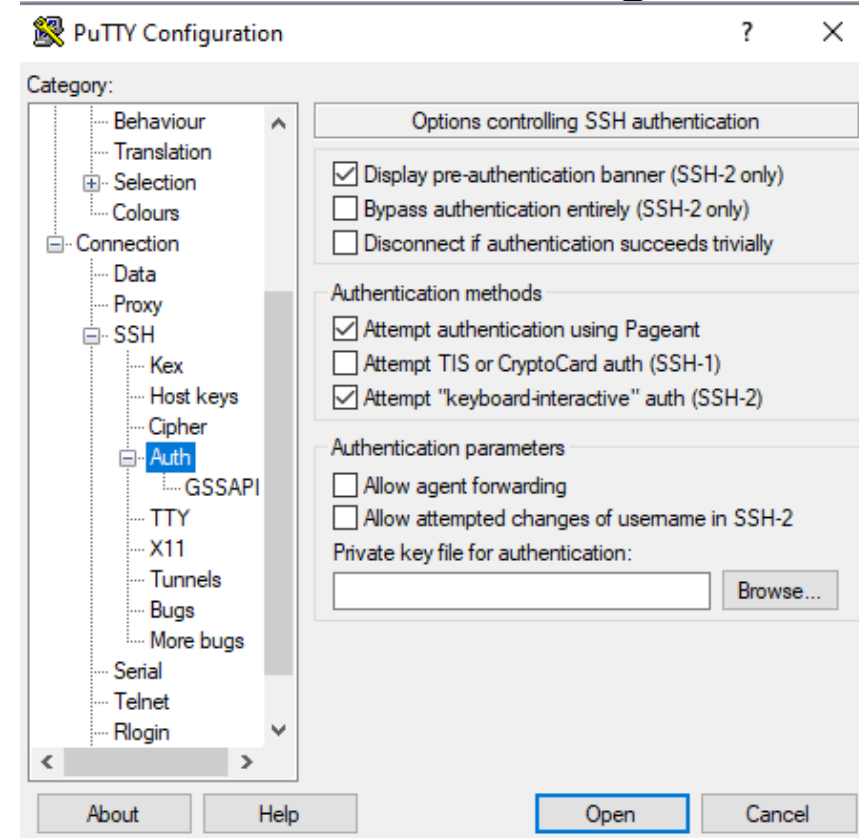
En **Windows** puede usarse el cliente **Putty** (también se puede instalar en Unix) para establecer la conexión <https://www.putty.org/>

En un archivo de configuración típico de ssh podemos encontrar algunos parámetros configurables como:

- El puerto de escucha para la conexión -> **Port**
- La versión del protocolo -> **Protocol**



PuTTY

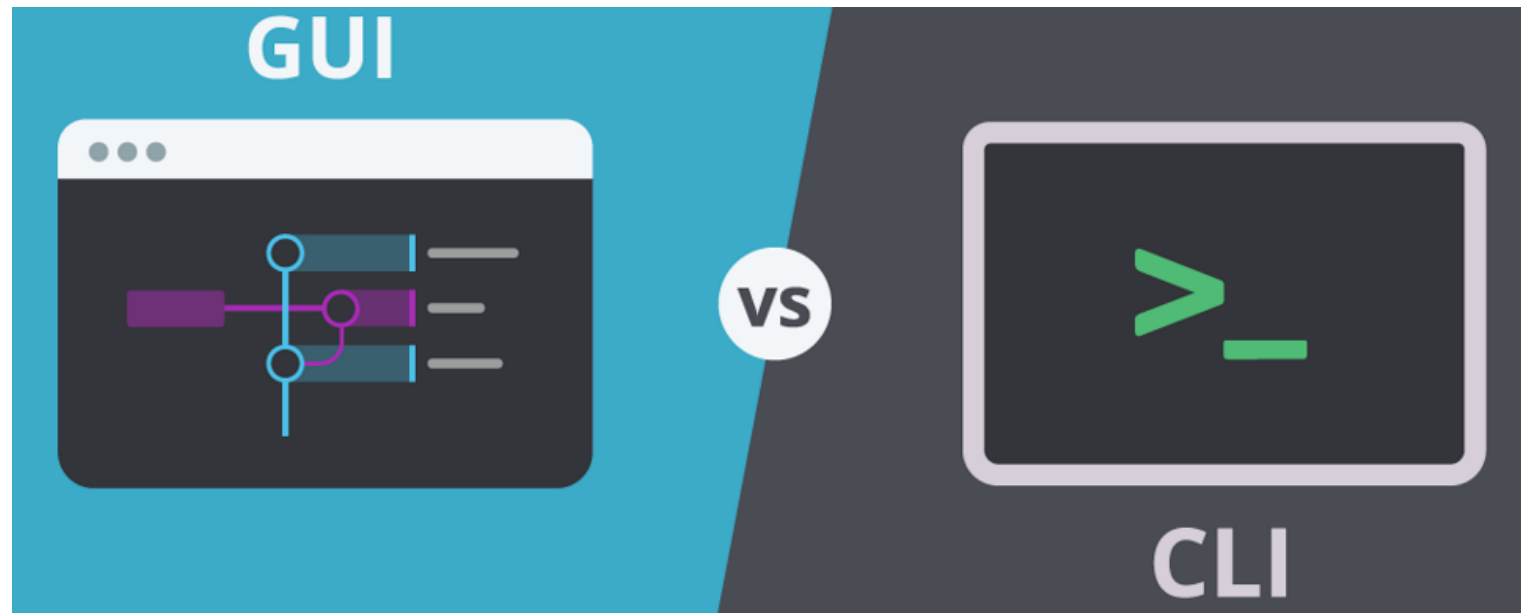


2. Terminales en modo texto, línea de comandos.

Podemos clasificar el acceso remoto en tres métodos:

- Mediante terminal (línea de comandos).
- Mediante interfaz gráfica.
- Mediante web.

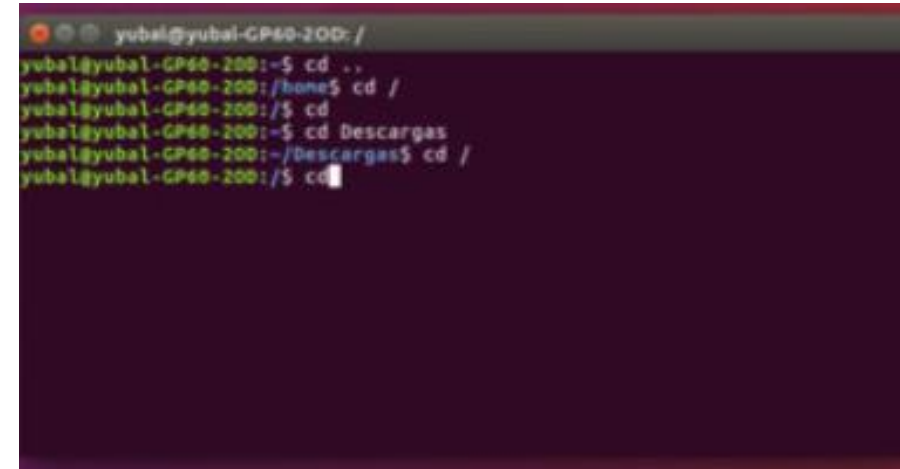
Interfaces gráficas (**GUI**)
Línea comandos (**CLI**)



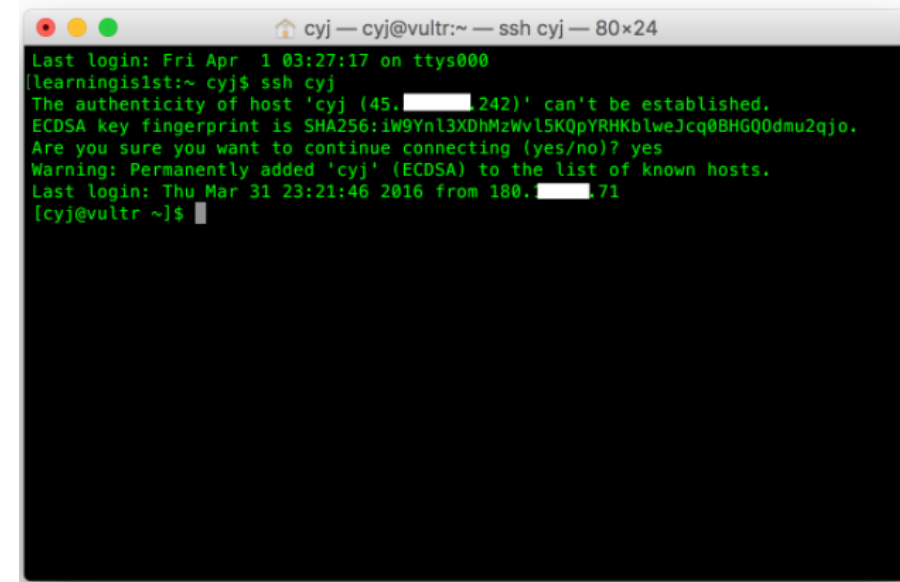
2.1. Acceso remoto mediante terminal.

Este tipo de acceso remoto **permite abrir una sesión de terminal** (línea de comandos) en un servidor, permitiendo a un cliente **ejecutar comandos** en el mismo.

Es el modo de acceso remoto **más utilizado** por los administradores de sistemas cuando controlan a distancia un servidor.



```
yubal@yubal-CP60-200: /  
yubal@yubal-CP60-200:~$ cd ..  
yubal@yubal-CP60-200:/home$ cd /  
yubal@yubal-CP60-200:/$ cd  
yubal@yubal-CP60-200:~$ cd Descargas  
yubal@yubal-CP60-200:~/Descargas$ cd /  
yubal@yubal-CP60-200:/$ cd
```



```
cyj — cyj@vultr:~ — ssh cyj — 80x24  
Last login: Fri Apr 1 03:27:17 on ttys000  
[learningis1st:~ cyj$ ssh cyj  
The authenticity of host 'cyj (45.██████████242)' can't be established.  
ECDSA key fingerprint is SHA256:iW9Ynl3X0hMzWv15K0pYRHkblweJcq0BHGQ0dmu2qjo.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'cyj' (ECDSA) to the list of known hosts.  
Last login: Thu Mar 31 23:21:46 2016 from 180.██████████171  
[cyj@vultr ~]$
```

2.1. Acceso remoto mediante terminal.

Algunos protocolos más populares son:

- **SSH**. Protocolo del que hemos hablado.
- **Telnet**: Es uno de los **primeros protocolos** de acceso remoto por línea de comandos utilizado. Es muy fácil de configurar y además es **compatible** con la mayoría de los sistemas. Utiliza por defecto el puerto **23 TCP**.

La conexión por Telnet se realiza sin cifrar, por lo que es inseguro utilizarlo, sobre todo a través de una red pública.

2.1. Acceso remoto mediante terminal.

- **Telnet.**

En un dispositivo con un cliente Telnet instalado, podemos **iniciar una conexión** simplemente escribiendo en una terminal:

```
telnet IP_SERVIDOR
```

Nos pedirá el usuario y la contraseña. **Recuerda** que ambas credenciales se enviarán a través de la red en texto plano (sin cifrar). Es una la razón por la que su uso está en desuso.

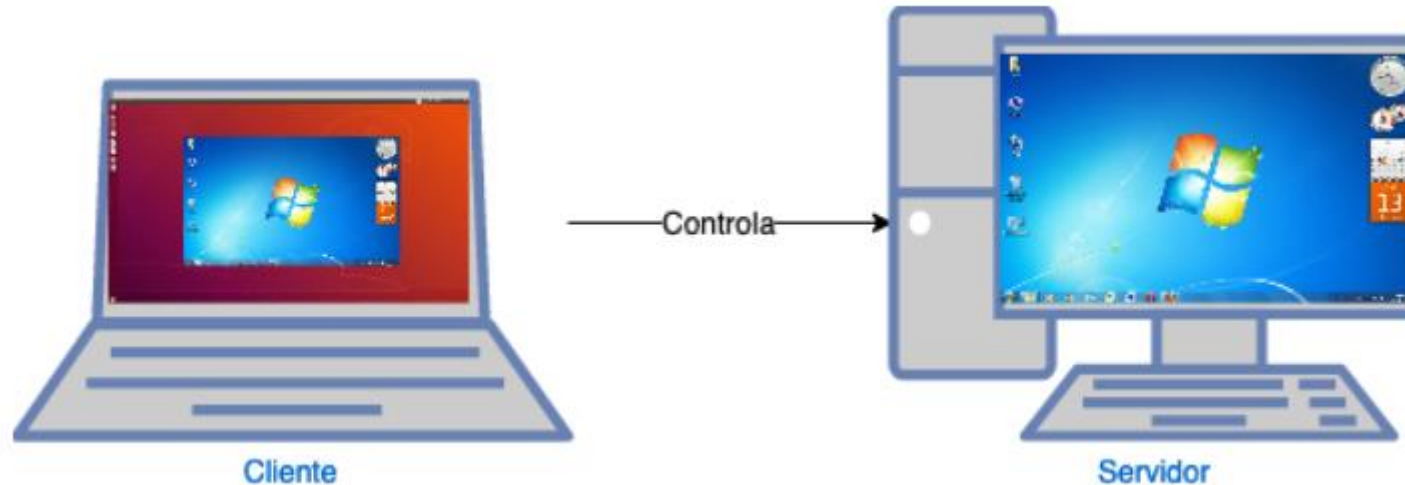
2.1. Acceso remoto mediante terminal.

Resumen

- **SSH**, **Telnet** y **Rlogin** son tres formas de hacer lo mismo: iniciar sesión en una computadora multiusuario desde otra computadora, a través de una red.
- **SSH**, **Telnet** y **Rlogin** son protocolos de red que le permiten hacer conexiones remotas. En la computadora en la que se sienta, ejecuta un cliente, que establece una conexión de red a la otra computadora (el servidor). La conexión de red transmite las pulsaciones de teclas y los comandos del cliente al servidor y le devuelve las respuestas del servidor.

3. Acceso remoto mediante interfaz gráfica.

Cuando accedemos remotamente a un equipo mediante este procedimiento, **visualizaremos** en nuestro dispositivo (el cliente) la pantalla gráfica del servidor, como si lo **tuviéramos delante** y le conectáramos un monitor.



3. Acceso remoto mediante interfaz gráfica.

Los protocolos más conocidos son:

- Remote Desktop Protocol (**RDP**). Es un protocolo propietario de Microsoft, utilizado para controlar remotamente sistemas Windows. A no ser que sea Windows Server, únicamente se permite la conexión de un cliente. En esta conexión no se ve lo que está haciendo un usuario en el servidor, sino que abre una nueva sesión para el cliente. Por defecto, utiliza el puerto **TCP 3389** para la conexión.

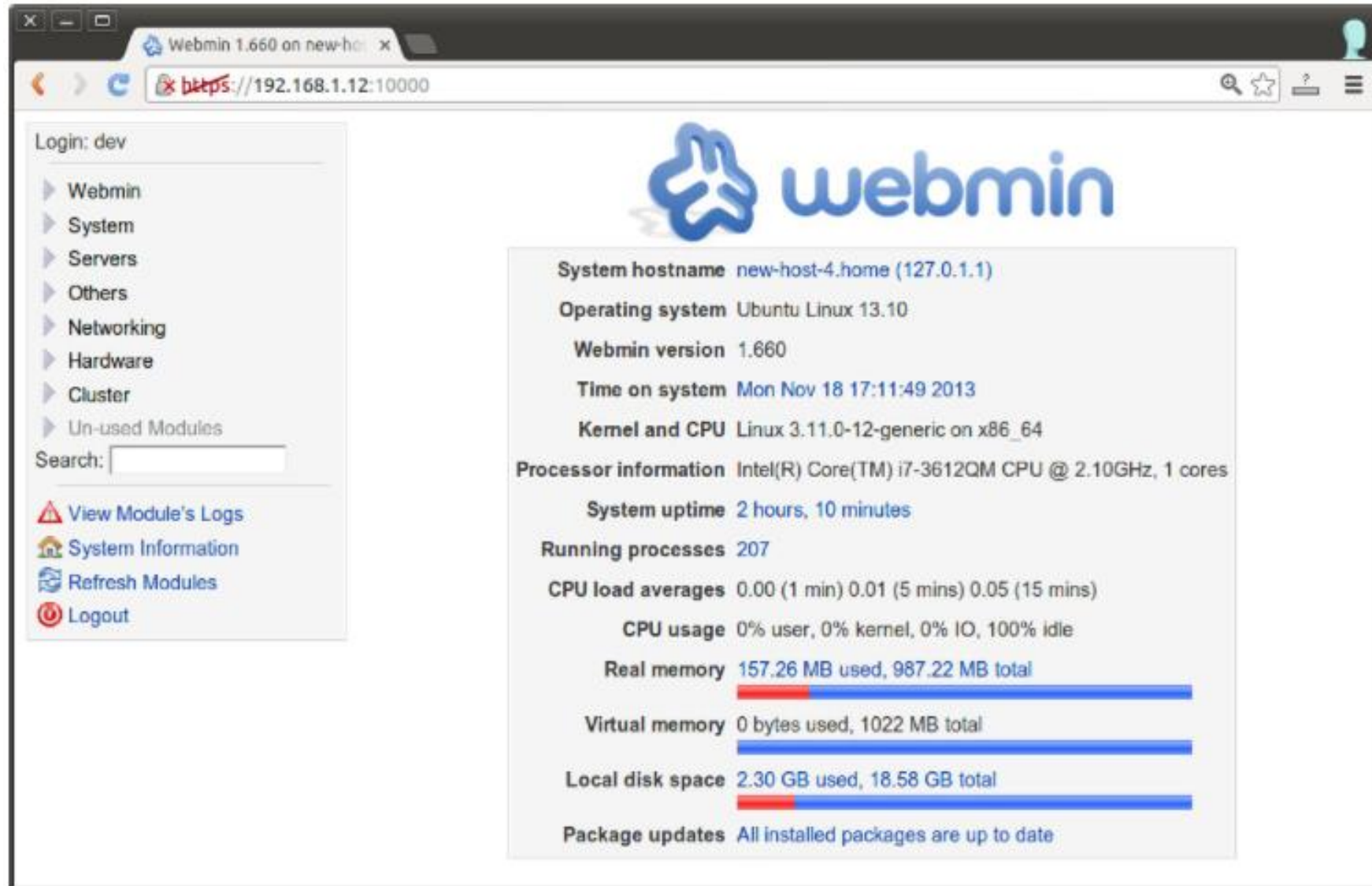


3. Acceso remoto mediante interfaz gráfica.

Algunos de los **programas** más conocidos para controlar remotamente un ordenador de forma gráfica son:

- [Ultra VNC](#)
- [TightVNC](#)
- [NoMachine](#)
- [AnyDesk](#)
- [TeamViewer](#)
- [LogMeIn](#)

4. Accesso remoto mediante web.



The screenshot displays the Webmin 1.660 web interface in a browser window. The address bar shows the URL `https://192.168.1.12:10000`. The interface includes a left sidebar with navigation links and a main content area displaying system status.

Left Sidebar:

- Login: dev
- Webmin
- System
- Servers
- Others
- Networking
- Hardware
- Cluster
- Un-used Modules
- Search:
- [View Module's Logs](#)
- [System Information](#)
- [Refresh Modules](#)
- [Logout](#)

Main Content Area:

System hostname [new-host-4.home \(127.0.1.1\)](#)

Operating system Ubuntu Linux 13.10

Webmin version 1.660

Time on system [Mon Nov 18 17:11:49 2013](#)

Kernel and CPU Linux 3.11.0-12-generic on x86_64

Processor information Intel(R) Core(TM) i7-3612QM CPU @ 2.10GHz, 1 cores

System uptime [2 hours, 10 minutes](#)

Running processes [207](#)

CPU load averages 0.00 (1 min) 0.01 (5 mins) 0.05 (15 mins)

CPU usage 0% user, 0% kernel, 0% IO, 100% idle

Real memory [157.26 MB used, 987.22 MB total](#)

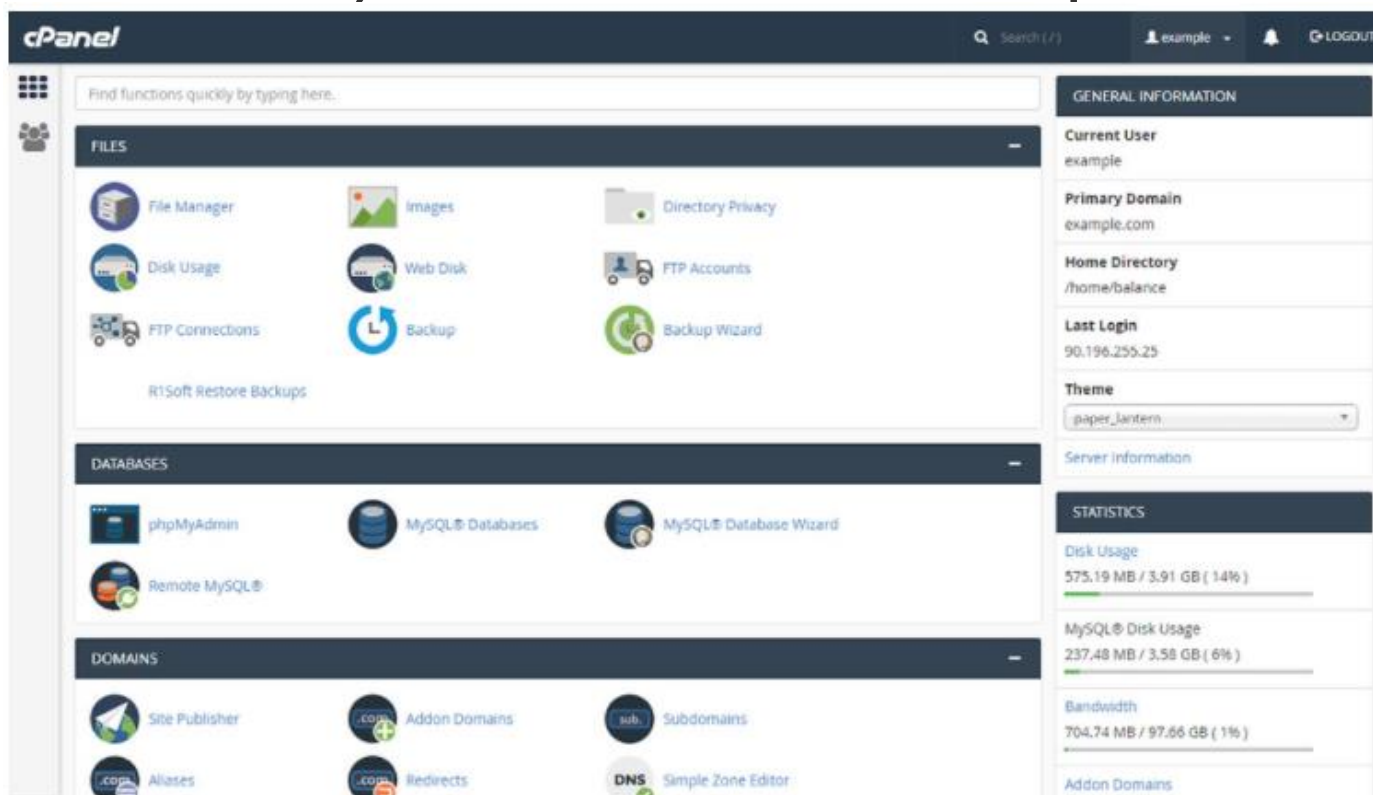
Virtual memory [0 bytes used, 1022 MB total](#)

Local disk space [2.30 GB used, 18.58 GB total](#)

Package updates [All installed packages are up to date](#)

4. Acceso remoto mediante web.

Los paneles de control remoto a través de la web son muy utilizados sobre todo cuando **contratamos un hosting**, ya que es la forma predeterminada con la que **administramos el servidor** que nos asignan. Normalmente, el software utilizado para ello es **cpanel**.



En la administración de sistemas, el software **webmin** es muy conocido y nos permite controlar remotamente un servidor a través de un navegador utilizando una interfaz muy amigable.

Actividad guiada 1 – Conectar por SSH

Todas las máquinas virtuales están aisladas entre sí, por lo que hay riesgo de conflicto y se pueden repetir las Ips.

1º Configurar adaptador de red

Configuración de Red > Cableado > IPv4 > Manual y añadir una dirección privada dentro del rango.

Rangos Redes Locales	
Desde	Hasla
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255



Actividad guiada 1 – Conectar por SSH

Cada vez que tengáis que instalar algo nuevo en Ubuntu, previamente:

> *sudo apt-get update*

> *apt-get upgrade*

apt-get update: actualiza la lista de paquetes disponibles y sus versiones, pero no instala o actualiza ningún paquete. Esta lista la coge de los servidores con repositorios que tenemos definidos en el sources.list.

apt-get upgrade: una vez el comando anterior ha descargado la lista de software disponible y la versión en la que se encuentra, podemos actualizar dichos paquetes usando este comando: apt-get upgrade. Instalará las nuevas versiones respetando la configuración del software cuando sea posible (esta es la maravilla de este tipo de sistemas).

Actividad guiada 1 – Conectar por SSH

> *sudo apt-get install openssh-server* [instalación del servicio]

> *sudo service ssh status* [comprobamos que esté activo]

Instalación...

A continuación abrimos el fichero de configuración con un **editor** (vim, atom, nano, kate)

> *sudo gedit /etc/ssh/sshd_config*

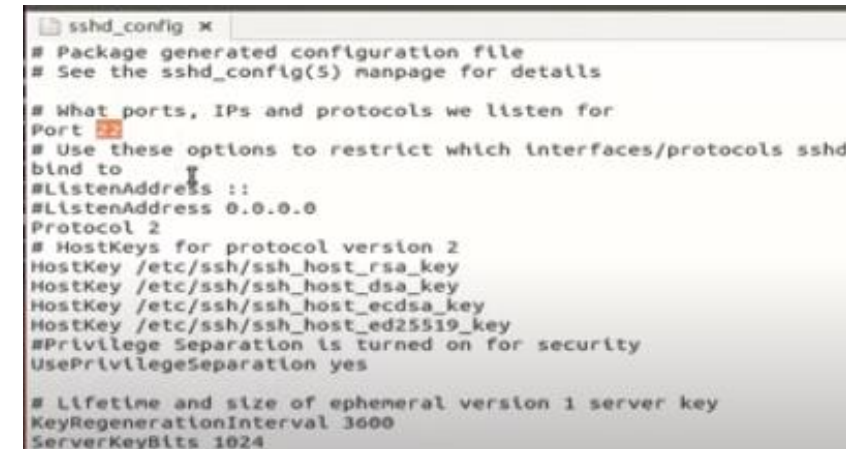
Comprobamos que el puerto sea el 22, y el protocolo sea el 2.

Si se han hecho cambios, hay que reiniciar el servicio con:

> *sudo /etc/init.d/ssh restart*

Cread en vuestro escritorio un documento con vuestro nombre.

Con esto dejamos las máquinas con un servidor activo y esperando peticiones de un cliente.

A screenshot of a text editor window titled 'sshd_config'. The file content shows standard SSH daemon configuration. The 'Port' is set to 22, and 'Protocol' is set to 2. The 'HostKey' section lists several keys: /etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_dsa_key, /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_ed25519_key. The 'PrivilegeSeparation' is set to 'yes'. At the bottom, 'KeyRegenerationInterval' is 3600 and 'ServerKeyBits' is 1024.

```
sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd
bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024
```

Actividad guiada 1 – Conectar por SSH terminal

Ahora, localizamos nuestra IP:

> ifconfig

Ahora con el compañero de al lado, compartimos nuestra IP. Con la IP del compañero, nuestro puesto sería el cliente que se conecta al servidor así: `ssh -p 22 user@IP + pass`. ¡el user y pass es el del ordenador cliente!

> ssh -p 22 alumno@IP_COMPAÑERO

> cd Escritorio/ [Para movernos a un directorio concreto]

> touch creo_desde_servidor.txt [Para crear un archivo vacío]

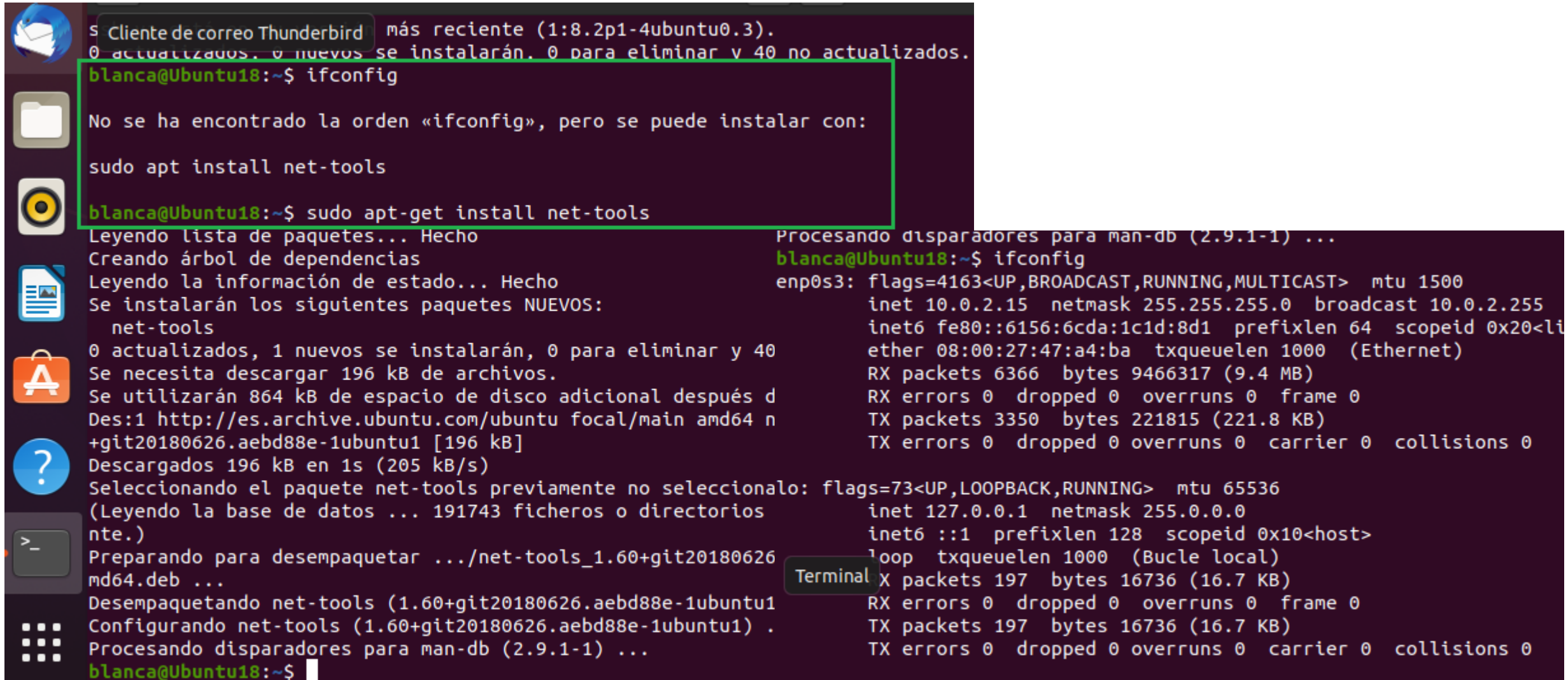
> ls [Para listar]

> rm nombre_fichero_creado_por_compañero [Borrar un archivo]

> mkdir ejemplo [Para crear carpeta]

Actividad guiada 1 – Conectar por SSH terminal

Solución **error** *ifconfig* -> *sudo apt-get install net-tools*



```
blanca@Ubuntu18:~$ ifconfig
No se ha encontrado la orden «ifconfig», pero se puede instalar con:
sudo apt install net-tools

blanca@Ubuntu18:~$ sudo apt-get install net-tools
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  net-tools
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 40
Se necesita descargar 196 kB de archivos.
Se utilizarán 864 kB de espacio de disco adicional después d
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 n
+git20180626.aebd88e-1ubuntu1 [196 kB]
Descargados 196 kB en 1s (205 kB/s)
Seleccionando el paquete net-tools previamente no seleccionalo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
(Leyendo la base de datos ... 191743 ficheros o directorios
nte.)
Preparando para desempaquetar .../net-tools_1.60+git20180626
md64.deb ...
Desempaquetando net-tools (1.60+git20180626.aebd88e-1ubuntu1
Configurando net-tools (1.60+git20180626.aebd88e-1ubuntu1) .
Procesando disparadores para man-db (2.9.1-1) ...
blanca@Ubuntu18:~$
```

Procesando disparadores para man-db (2.9.1-1) ...

```
blanca@Ubuntu18:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::6156:6cda:1c1d:8d1 prefixlen 64 scopeid 0x20<li
ether 08:00:27:47:a4:ba txqueuelen 1000 (Ethernet)
RX packets 6366 bytes 9466317 (9.4 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3350 bytes 221815 (221.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Bucle local)
RX packets 197 bytes 16736 (16.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 197 bytes 16736 (16.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Actividad guiada 1 – Conectar por SSH terminal

Posibles soluciones al **error**:

```
ssh: connect to host 10.0.2.15 port 22: No route to host
```

sudo service ssh status -> ver que está activo

sudo lsof -nP -iTCP -sTCP:LISTEN -> ver que el Puerto 22 está abierto.

ping 10.0.2.16 -> el host debe de ser alcanzable

Actividad guiada 1 – Conectar por SSH con terminal

Probad a conectar desde vuestro PC a la Ubuntu VirtualBox.

1º NAT + Reenvío de puertos

Red

Adaptador 1 | Adaptador 2 | Adaptador 3 | Adaptador 4

☒ Habilitar adaptador de red

Conectado a: NAT

Nombre:

Avanzadas

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Permitir todo

Dirección MAC: 08002747A4BA

☒ Cable conectado

Reenvío de puertos

Reglas de reenvío de puertos

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
SSH	TCP	127.0.0.2	2222	10.0.2.15	22

interfaz loopback

IP Ubuntu

Actividad guiada 1 – Conectar por SSH con terminal

Probad a conectar desde vuestro PC a la Ubuntu VirtualBox.

VirtualBox Ubuntu ➡

↓ Ordenador sobremesa

```
blanca@Ubuntu18: ~/Escritorio
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

Se pueden aplicar 25 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

blanca@Ubuntu18:~$ ls
Descargas  Escritorio  Música      Público
Documentos Imágenes   Plantillas  Videos
blanca@Ubuntu18:~$ cd Escritorio
blanca@Ubuntu18:~/Escritorio$ ls
testDesdePutty
blanca@Ubuntu18:~/Escritorio$
```

```
Actividades  Terminal  26 de sep 22:44
blanca@Ubuntu18: ~/Escritorio

etadata [354 kB]
Des:9 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11
Metadata [2.464 B]
Des:10 http://es.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-1
1 Metadata [944 B]
Des:11 http://es.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-1
1 Metadata [10,4 kB]
Descargados 1.068 kB en 3s (424 kB/s)
Leyendo lista de paquetes... Hecho
blanca@Ubuntu18:~$ sudo apt-get install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssh-server ya está en su versión más reciente (1:8.2p1-4ubuntu0.3).
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
U Ayuda «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 31 no actualizados.
blanca@Ubuntu18:~$ ls
Descargas  Escritorio  Música      Público
Documentos Imágenes   Plantillas  Videos
blanca@Ubuntu18:~$ cd Escritorio
blanca@Ubuntu18:~/Escritorio$ mkdir testDesdePutty
blanca@Ubuntu18:~/Escritorio$ ls
testDesdePutty
blanca@Ubuntu18:~/Escritorio$
```

Actividades guiadas en Aula Virtual

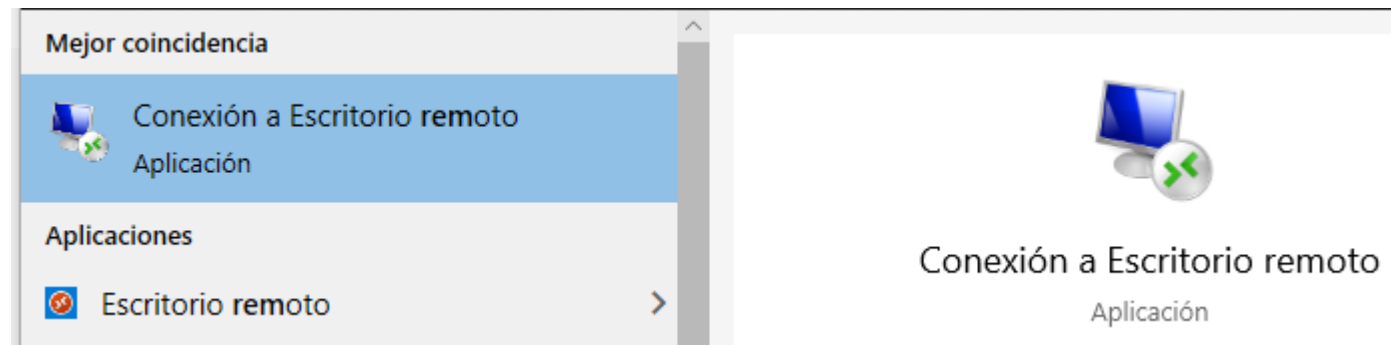
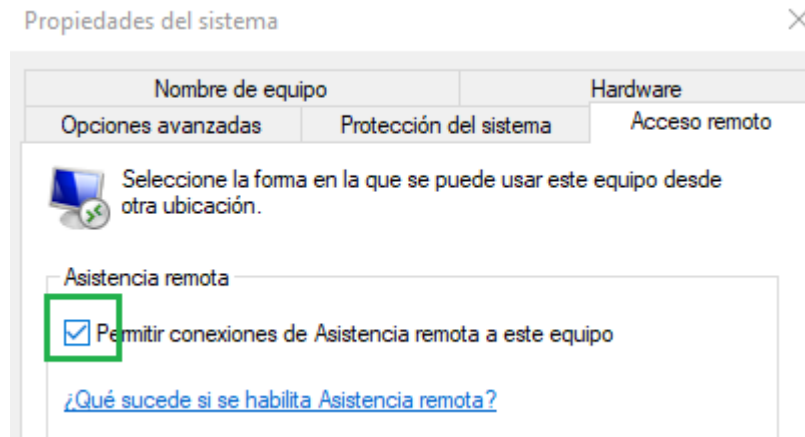
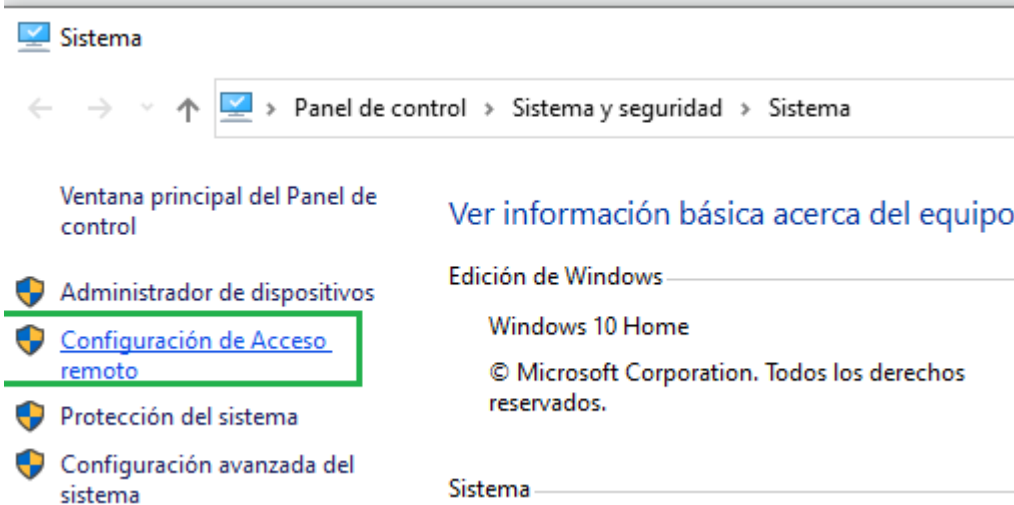
- **Windows. Conexión remota utilizando PuTTY.**
- **Linux. Conexión terminal ssh.**

Actividad guiada – Remote Desktop Connection

Utilizad una de las máquinas virtuales de Windows que tengáis en VirtualVox

RDC:Remote Desktop Connection de Windows

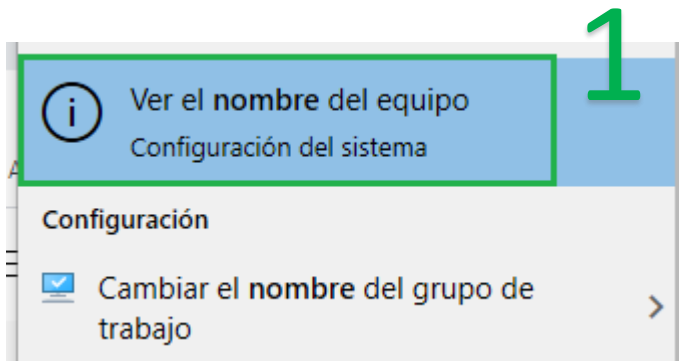
Start > Settings > System > Remote Desktop > Enable Remote Desktop.



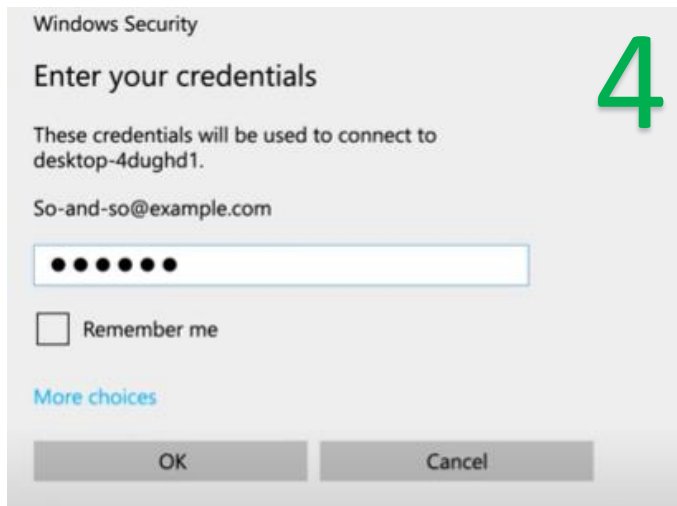
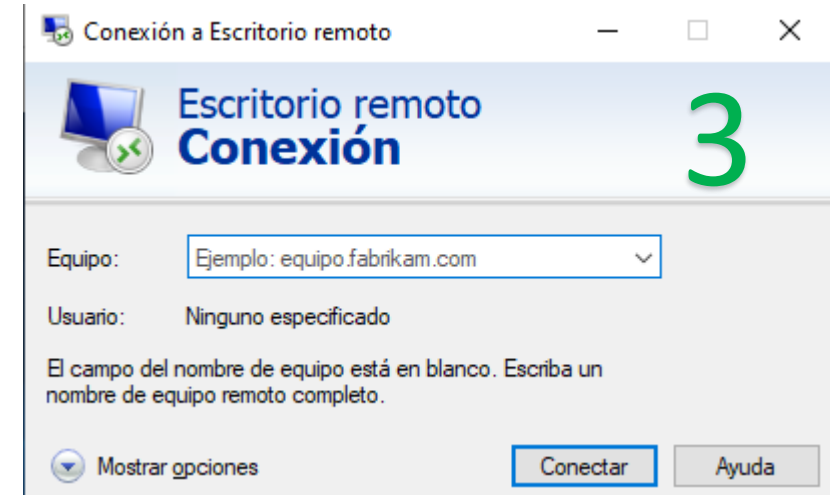
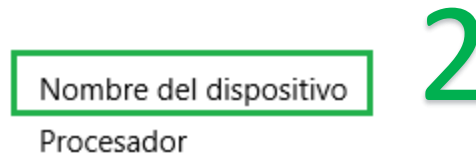
Actividad guiada 2 – Remote Desktop Connection

Utilizad una de las máquinas virtuales de Windows que tengáis en VirtualVox

RDC:Remote Desktop Connection de Windows



Especificaciones del dispositivo



Práctica 1 – SSH

Revisad fecha de entrega en aula virtual.

Acceso al detalle de la práctica en Aula Virtual.

¡Preguntas, dudas!

