


PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 1 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Nombre y Apellidos:	EMILIO JOSÉ TOLEDO GARCÍA	Firma del Alumno:	
DNI:	45.452.080 D	Firma del Profesor:	

Apto: ☐

No Apto: ☐

Calificación:

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 540 minutos
(Temporalizados durante la Unidad de Aprendizaje 1)

El alumno/a deberá acatar las siguientes normas durante la duración de la actividad:

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486_3_E1**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)

PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 2 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Instrucciones específicas

Nombre: En esta práctica se pretende que el alumnado se familiarice con el servicio SSH y aprenda a configurarlo adecuadamente de acuerdo a los requisitos deseados mediante los archivos de configuración. Al finalizar la práctica se deberá entregar un guión que explique el proceso y los pasos seguidos para realizar todos y cada uno de los puntos.

Agrupamiento: Individual

Descripción: Los pasos que habrá que seguir para realizar la práctica son los siguientes:

1. Instalar e iniciar un servidor SSH en una máquina Linux (Preferiblemente Ubuntu)
2. Iniciar el Servidor SSH y probar a conectarte desde un cliente SSH de Windows (ejemplo: Putty) al servidor de SSH de GNU/Linux y comprueba si es posible conectarse correctamente desde cualquier equipo.
3. Cambia los protocolos SSH en cliente y servidor y comprueba si se permite la conexión. Por ejemplo, que el cliente use solo la versión 1 del protocolo y el servidor la 2.
4. Por defecto, al autenticarnos correctamente en el servidor SSH, éste nos muestra la fecha y hora de la última vez que nos conectamos. Encuentra la opción que se encarga de modificar este aspecto.
5. El servicio SSH por defecto escucha en el puerto 22. Modifícalo para que arranque en el puerto 10022 (u otro) y averigua cuál sería el comando utilizado para poder acceder al servidor. (ayuda: man ssh).
6. Configurar el servicio SSH para que no admita hacer login como root.
7. Configura el servidor SSH para que solo permita la autenticación de los usuarios que nosotros indiquemos.
8. Configura el servidor SSH para validarnos sin introducir contraseña.
9. Configura el servidor SSH de forma adecuada para que acepte la redirección X11, de tal forma que se puedan ejecutar aplicaciones gráficas de forma remota. Haz pruebas y comprueba su funcionamiento.
10. Utiliza los enlaces proporcionados para completar el trabajo, investigando qué otras opciones podrían ser útiles para la configuración de nuestro servidor SSH.

PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 3 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Instrucciones específicas

Recursos: <https://www.openssh.com/manual.html>

https://help.ubuntu.com/community/SSH/OpenSSH/Configuring?_ga=2.74147152.312157118.1647942508-1909757974.1644235693

https://manpages.ubuntu.com/manpages/xenial/man1/ssh.1.html?_ga=2.82993364.312157118.1647942508-1909757974.1644235693

<https://www.redeszone.net/tutoriales/servidores/servidor-openssh-linux-configuracion-maxima-seguridad/>

Duración: 540 minutos

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumno podrá hacer uso de internet para su realización.

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 4 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Arrancamos la presente práctica instalando el servidor SSH en nuestra máquina virtual de UBUNTU. Para ello, primeramente actualizaremos e instalaremos los programas desde los repositorios al efecto con el comando: **sudo apt-get update && upgrade**

Ahora sí, usamos la orden necesaria para instalar nuestro flamante servidor ssh.

```
emilio@emilio-VirtualBox: ~$ sudo apt install openssh-server
Leyendo lista de paquetes... Hecho
emilio@emilio-VirtualBox: ~$ sudo apt install openssh-server
[sudo] contraseña para Emilio:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  chronicon-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh_askpass
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 674 kB de archivos.
Se utilizarán 5.917 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [Y/n] y
Des:1 http://es.archive.ubuntu.com/ubuntu impish/main amd64 ncurses-term all 6.2
+20201114-2build1 [249 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu impish-updates/main amd64 openssh-sftp
```

Para comprobar que nuestro servidor ssh, está correctamente instalado y funcionando, podemos ejecutar un comando que nos reflejará si está activo:

```
emilio@emilio-VirtualBox: ~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Tue 2022-03-22 19:52:26 WET; 14min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 5725 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 5726 (sshd)
      Tasks: 1 (limit: 9482)
     Memory: 1.0M
        CPU: 39ms
    CGroup: /system.slice/ssh.service
            └─5726 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

mar 22 19:52:26 Emilio-VirtualBox systemd[1]: Starting OpenBSD Secure Shell ser
mar 22 19:52:26 Emilio-VirtualBox sshd[5726]: Server listening on 0.0.0.0 port
mar 22 19:52:26 Emilio-VirtualBox sshd[5726]: Server listening on :: port 22.
mar 22 19:52:26 Emilio-VirtualBox systemd[1]: Started OpenBSD Secure Shell serv
ESCOD
```

PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 5 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Para proteger nuestro servidor, es conveniente acceder al fichero de configuración y hacer una copia de seguridad del mismo:

```
emilio@emilio-VirtualBox:/etc/ssh$ ls
moduli          sshd_config.d      ssh_host_ed25519_key.pub
ssh_config       ssh_host_ecdsa_key  ssh_host_rsa_key
ssh_config.d     ssh_host_ecdsa_key.pub  ssh_host_rsa_key.pub
sshd_config      ssh_host_ed25519_key  ssh_import_id
emilio@emilio-VirtualBox:/etc/ssh$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.factory-defaults
emilio@emilio-VirtualBox:/etc/ssh$ ls
moduli          sshd_config.factory-defaults  ssh_host_rsa_key
ssh_config       ssh_host_ecdsa_key           ssh_host_rsa_key.pub
ssh_config.d     ssh_host_ecdsa_key.pub       ssh_import_id
sshd_config      ssh_host_ed25519_key         ssh_import_id
sshd_config.d    ssh_host_ed25519_key.pub
```

Ahora blindaremos el archivo original capando sus permisos de escritura...

```
emilio@emilio-VirtualBox:/etc/ssh$ ls
moduli          sshd_config.d      ssh_host_ed25519_key      ssh_import_id
ssh_config       sshd_config.factory-defaults  ssh_host_ed25519_key.pub
ssh_config.d     ssh_host_ecdsa_key      ssh_host_rsa_key
sshd_config      ssh_host_ecdsa_key.pub    ssh_host_rsa_key.pub
emilio@emilio-VirtualBox:/etc/ssh$ sudo chmod a-w /etc/ssh/sshd_config.factory-defaults
emilio@emilio-VirtualBox:/etc/ssh$
```

Podemos y es conveniente, modificar el puerto por defecto para aumentar la seguridad en caso de intentos de acceso por parte de intrusos:

```
ami@ami-VirtualBox:~$ sudo gedit /etc/ssh/sshd_config
```

```
1 # $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $
2
3 # This is the sshd server system-wide configuration file. See
4 # sshd_config(5) for more information.
5
6 # This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
7
8 # The strategy used for options in the default sshd config shipped with
9 # OpenSSH is to specify options with their default value where
10 # possible, but leave them commented. Uncommented options override the
11 # default value.
12
13 Include /etc/ssh/sshd_config.d/*.conf
14
15 Port 22
16 #AddressFamily any
17 #ListenAddress 0.0.0.0
18 #ListenAddress ::
19
20 #HostKey /etc/ssh/ssh_host_rsa_key
```


PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos

Fecha 04 / 03 / 2022

Página 6 de 3

Curso

7.1. MF0486_3 Seguridad en equipos informáticos

Plan de
Formación

FC-2021.1/IL000/1914256

En nuestro caso dejaremos por defecto el puerto 22 para la realización de la presente práctica, modificando el mismo cuando la ocasión lo requiera profesionalmente.

Comprobando la dirección ip de nuestro Linux Ubuntu, podemos hacer un ping desde Windows para verificar que hay comunicación entre ambos sistemas:

```

emilio@emilio-VirtualBox: /etc/ssh
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::31a9:88c2:0bd0:7313 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:28:cc:3e txqueuelen 1000 (Ethernet)
    RX packets 12427 bytes 18416469 (18.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2629 bytes 187489 (187.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.56 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:5771:c3b0:1f91:a264 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:7e:b9:5a txqueuelen 1000 (Ethernet)
    RX packets 2235 bytes 257292 (257.2 KB)
    RX errors 0 dropped 7 overruns 0 frame 0
    TX packets 293 bytes 28867 (28.8 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 275 bytes 26916 (26.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 275 bytes 26916 (26.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

emilio@emilio-VirtualBox: ~$

C:\WINDOWS\system32\ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet 3:

    Sufijo DNS específico para la conexión. . . :
    Vínculo dirección IPv4 local. . . : fe80::1c00:c722:3a80:721313
    Dirección IPv4. . . : 192.168.1.56
    Máscara de subred. . . : 255.255.255.0
    Puerta de enlace predeterminada. . . :

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo dirección IPv4 local. . . : fe80::4ca0:0075:1a1:54505317
    Dirección IPv4. . . : 192.168.1.40
    Máscara de subred. . . : 255.255.255.0
    Puerta de enlace predeterminada. . . : 192.168.1.1

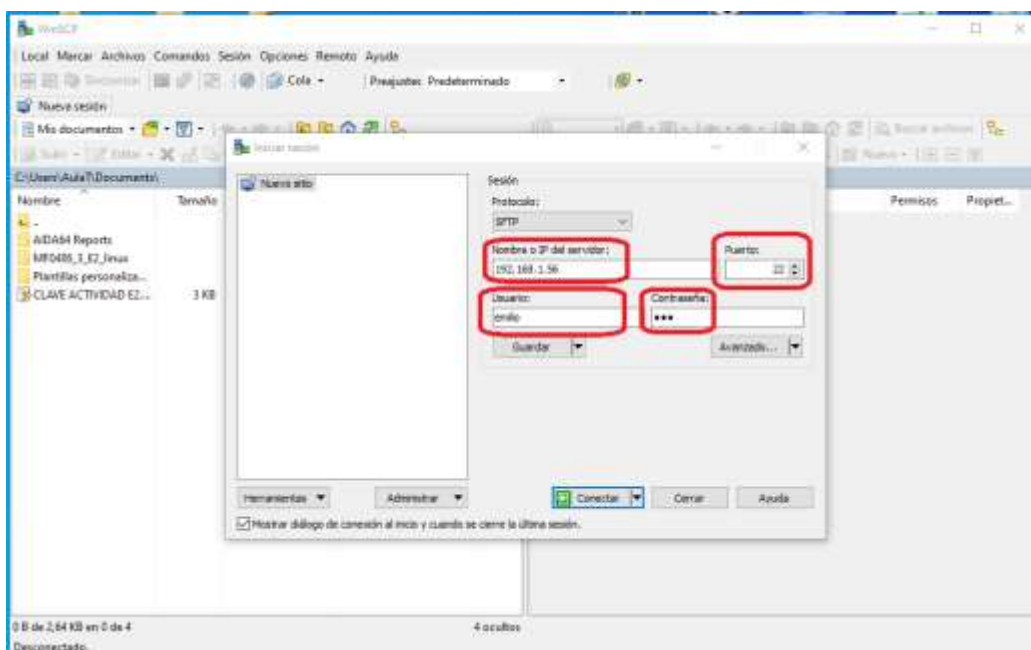
C:\WINDOWS\system32>ping 192.168.1.56

Paciendo ping a 192.168.1.56 con 32 bytes de datos:
Respuesta desde 192.168.1.56: bytes=32 tiempo=14ms TTL=64
Respuesta desde 192.168.1.56: bytes=32 tiempo=14ms TTL=64
Respuesta desde 192.168.1.56: bytes=32 tiempo=14ms TTL=64
Respuesta desde 192.168.1.56: bytes=32 tiempo=14ms TTL=64

Estadísticas de ping para 192.168.1.56:

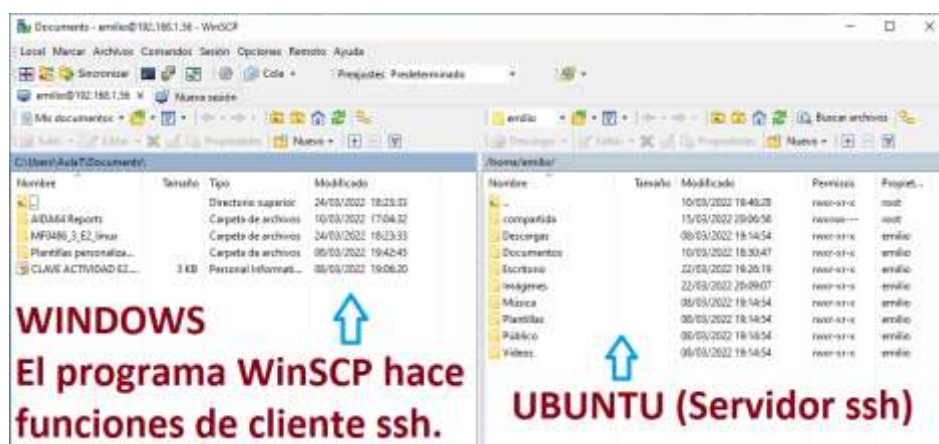
```

Con la aplicación para Windows WinSCP, podemos acceder al servidor ssh de nuestro Linux Ubuntu, introduciendo los siguientes parámetros:



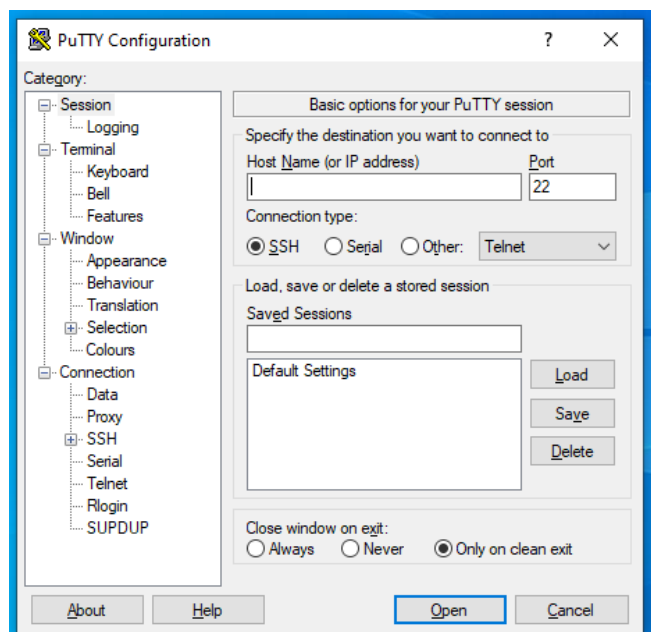
PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 7 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Si todo ha ido bien, deberíamos poder visualizar la ventana que contiene los archivos de Linux que hemos autorizado mediante ssh:



Otra fórmula para conectar desde Windows a través de SSH, es usando el programa "Putty". Podemos descargarlo desde la web <https://www.putty.org/>. Una vez instalado aparecerá en nuestra pantalla el icono correspondiente:

Al ejecutarlo, nos pedirá la dirección IP para realizar la conexión SSH, así como el puerto de conexión:



PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 8 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Solicitará entonces el nombre de usuario y la contraseña para establecer la conexión, que corresponderán en este caso con el nombre de usuario y la contraseña de nuestro usuario en Linux:

```
192.168.1.20 - PuTTY
login as: pepe
pepe@192.168.1.20's password: 
```

A continuación estaremos dentro de Ubuntu con la citada conexión SSH:

```
pepe@emilio-VirtualBox: ~
login as: pepe
pepe@192.168.1.20's password:
Welcome to Ubuntu 21.10 (GNU/Linux 5.13.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Se pueden aplicar 0 actualizaciones de forma inmediata.

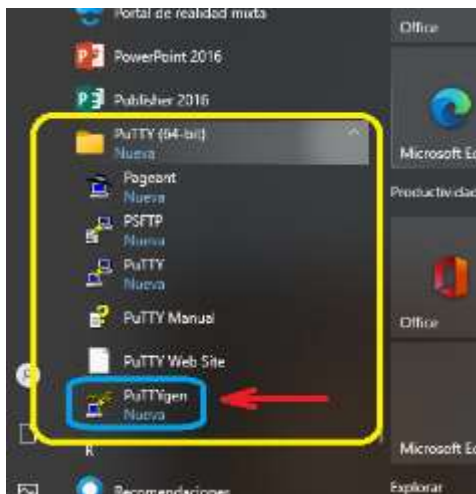
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Tue Apr  5 18:52:25 2022 from 192.168.1.50
pepe@emilio-VirtualBox:~$ ls
Descargas  Escritorio  Música      Público
Documentos Imágenes   Plantillas  Vídeos
pepe@emilio-VirtualBox:~$ 
```


PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 9 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

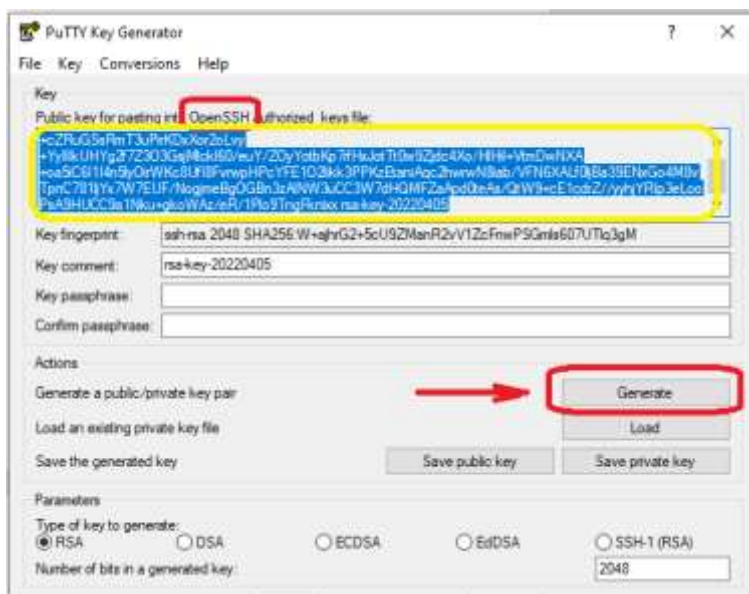
Si queremos crear una clave pública, podemos hacer uso de puttygen:

Para ejecutar PuTTYgen, vaya a Windows -> Menú Inicio -> Todos los programas -> PuTTY -> PuTTYgen.
Verá una ventana para el generador de claves PuTTY en su pantalla.

Concretamente, donde muestra la siguiente imagen:



Pinchando en “Generate”, creamos la clave pública cuyo formato es OpenSSH.



PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 10 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

Tenemos que crear un nuevo archivo con el nombre “authorized_keys”, dentro de un nuevo directorio en Ubuntu. El directorio lo creamos dentro home/usuario, en nuestro caso pepe, y llevará por nombre SSH:

```

pepe@emilio-VirtualBox: /etc/ssh
pepe@emilio-VirtualBox:~/SSH$ pwd
/home/pepe/SSH
pepe@emilio-VirtualBox:~/SSH$ ls
authorized_keys
pepe@emilio-VirtualBox:~/SSH$
  
```

Dentro del archivo “authorized_keys”, introduciremos la clave pública:

```

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQHMF2Y78henCnIuo2Zk1+c2RuG5sRNT3uPTrKDxXor2oLvy+Yy11IkuHYg2f7Z303GsJm1ck169/euY/
Z0yYotbkp7r fHxJotTt8w9Zjdc4Xo/H1HL1+VtdDwNXA+oa51C611I4n5ly0/rMKc8UFI0FvrmPHPCyFE1021lkk3PPKzEtanLAqc2hwrwN8lab/
VFN6XALf01jBa39ENxGo4MBvTpnC7B1ljYx7W7EUF/NogJneBgDGBn3zAlNW3uCC3W7dHQMFZaApd0teAs/Qtw9+cE1cdrZ//yyhJYRip3eLooPsA9HUCC9a1Nku+gkoNAZ/eR/
1Plo9Tngfkn1xx rsa-key-20220405
  
```

A continuación, editaremos las siguientes directivas del archivo sshd_config:

```

emi@emi-VirtualBox: /etc/ssh
GNU nano 5.6.1 sshd_config *
#MaxSessions 10
PubkeyAuthentication yes
  
```

```

emi@emi-VirtualBox: /etc/ssh
GNU nano 5.6.1 sshd_config *
# To disable tunneled clear text passwords, change to no
PasswordAuthentication no
#PermitEmptyPasswords no
  
```

PRÁCTICA E1: Instalar un Servidor SSH en Windows / Linux MF0486_3 Seguridad en equipos informáticos			Fecha 04 / 03 / 2022
			Página 11 de 3
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/IL000/1914256

```
emi@emi-VirtualBox: /etc/ssh
GNU nano 5.6.1 sshd_config *
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

```
emi@emi-VirtualBox: /etc/ssh
GNU nano 5.6.1 sshd_config *
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
```

Por último reiniciaremos el servidor ssh:

```
emi@emi-VirtualBox: /etc/ssh
emi@emi-VirtualBox: /etc/ssh$ sudo systemctl restart ssh
emi@emi-VirtualBox: /etc/ssh$
```

Dentro del programa Putty, introduciremos la clave privada que habremos guardado previamente cuando generamos la misma:

