	Curso:	2024-2025	Ciclo:	SISTEMAS MICROINFORMÁTICOS Y REDES	
	Fecha:	14/10/2024	Módulo:	Servicios en Red	
	Tipo:	PRÁCTICA	Profesor:	Paco Gallego	
	Título:	Acceso remoto con PuTTY			
Apellidos:	Ros Abenza			Nota:	
Nombre:	Enrique				

## 1. Creamos 2 usuarios con contraseña cifrada

```

ubuntu 24.04.1 LTS sshprueba tty1
sshprueba login: mindbloom
Password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

System information as of Mon Oct 14 06:19:10 PM UTC 2024

System load:  0.83          Processes:           113
Usage of /:   94.9% of 8.02GB Users logged in:      0
Memory usage: 51%          IPv4 address for enp0s3: 10.4.200.178
Swap usage:   0%

=> / is using 94.9% of 8.02GB

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

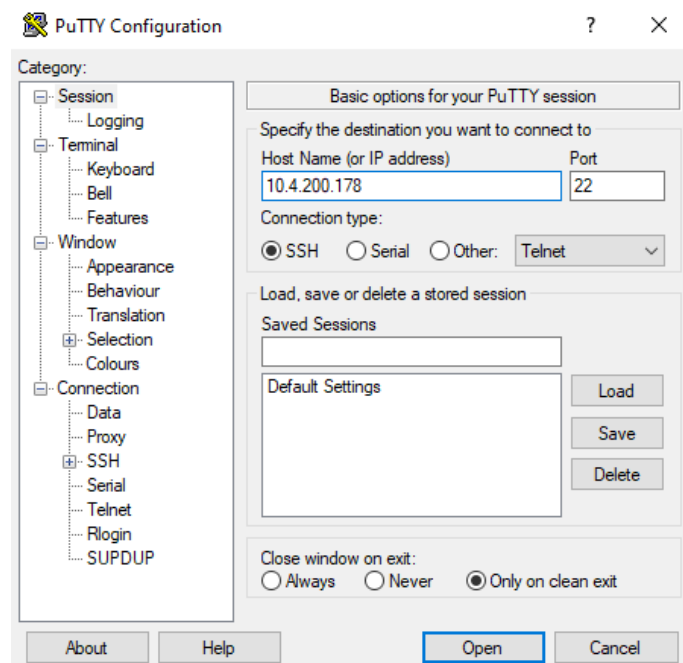
5 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

mindbloom@sshprueba:~$ sudo useradd -p "$(openssl passwd -1 'smr1')" Ros
[sudo] password for mindbloom:
mindbloom@sshprueba:~$ sudo useradd -p "$(openssl passwd -1 'smr1')" Abenza
mindbloom@sshprueba:~$ _

```

## 2. Instalamos PuTTY en nuestra maquina Windows 10 y conectamos la aplicación con la IP de nuestro servidor



	Curso:	2024-2025	Ciclo:	SISTEMAS MICROINFORMÁTICOS Y REDES	
	Fecha:	14/10/2024	Módulo:	Servicios en Red	
	Tipo:	PRÁCTICA	Profesor:	Paco Gallego	
	Título:	Acceso remoto con PuTTY			
Apellidos:	Ros Abenza			Nota:	
Nombre:	Enrique				

### 3. Tratamos de hacer un login con dichos usuarios y sus contraseñas desde PuTTY

```

10.4.200.178 - PuTTY
login as: Ros
Ros@10.4.200.178's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

System information as of Mon Oct 14 06:29:31 PM UTC 2024

System load:  0.16           Processes:           115
Usage of /:   95.2% of 8.02GB Users logged in:        1
Memory usage: 49%           IPv4 address for enp0s3: 10.4.200.178
Swap usage:   0%

=> / is using 95.2% of 8.02GB

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

```

```

10.4.200.178 - PuTTY
login as: Abenza
Abenza@10.4.200.178's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

System information as of Mon Oct 14 06:30:49 PM UTC 2024

System load:  0.63           Processes:           117
Usage of /:   95.2% of 8.02GB Users logged in:        1
Memory usage: 49%           IPv4 address for enp0s3: 10.4.200.178
Swap usage:   0%


=> / is using 95.2% of 8.02GB

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

```

	Curso:	2024-2025	Ciclo:	SISTEMAS MICROINFORMÁTICOS Y REDES	
	Fecha:	14/10/2024	Módulo:	Servicios en Red	
	Tipo:	PRÁCTICA	Profesor:	Paco Gallego	
	Título:	Acceso remoto con PuTTY			
Apellidos:	Ros Abenza			Nota:	
Nombre:	Enrique				

#### 4. Entramos al archivo de configuración de parámetros de ssh (sshd\_config) con un nano

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10


#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

mindbloom@sshprueba:~$
mindbloom@sshprueba:~$ sudo nano /etc/ssh/sshd_config
```

	Curso:	2024-2025	Ciclo:	SISTEMAS MICROINFORMÁTICOS Y REDES		
	Fecha:	14/10/2024	Módulo:	Servicios en Red		
	Tipo:	PRÁCTICA	Profesor:	Paco Gallego		
	Título:	Acceso remoto con PuTTY				
Apellidos:	Ros Abenza				Nota:	
Nombre:	Enrique					

5. Cambiamos el parámetro “PermitRootLogin” a “PermitRootLogin no” o “PermitRootLogin prohibit-password” en sistemas posteriores

```

GNU nano 7.2 /etc/ssh/sshd_config *
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes


# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

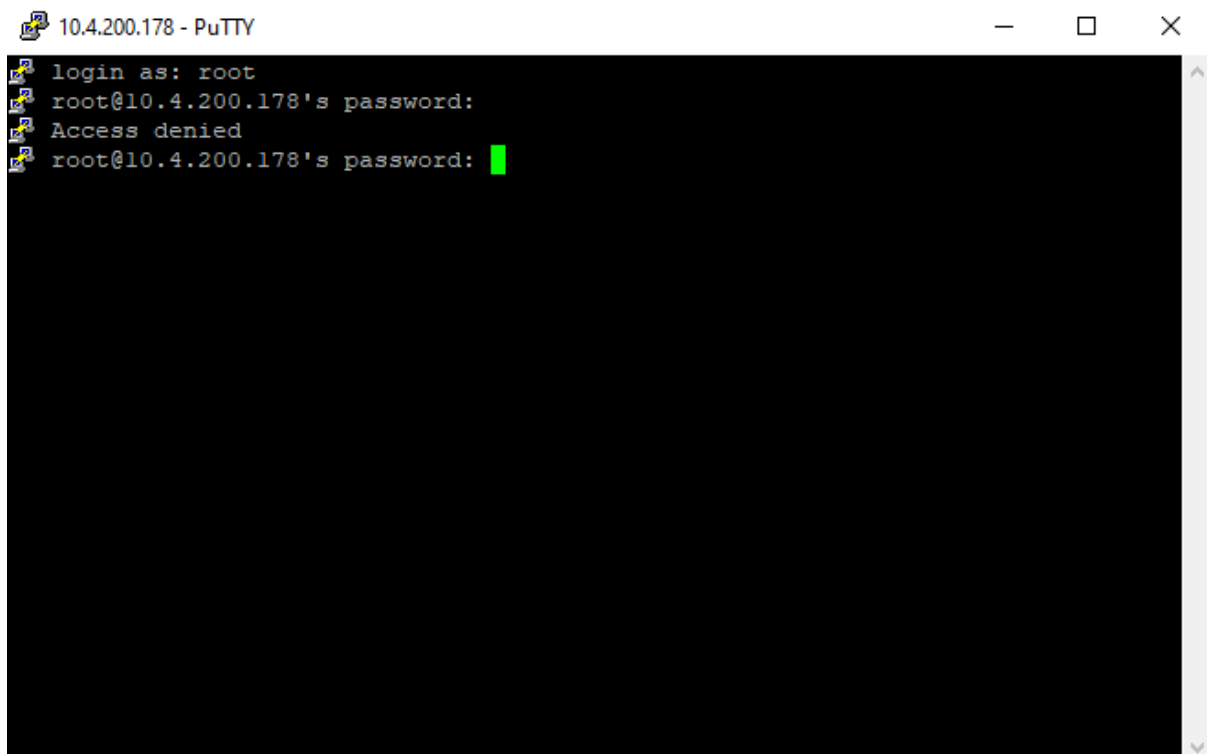
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
[ Soft wrapping of overlong lines enabled ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^I Justify    ^_ Go To Line M-F Redo     M-6 Dgou

```

	Curso:	2024-2025	Ciclo:	SISTEMAS MICROINFORMÁTICOS Y REDES	
	Fecha:	14/10/2024	Módulo:	Servicios en Red	
	Tipo:	PRÁCTICA	Profesor:	Paco Gallego	
	Título:	Acceso remoto con PuTTY			
Apellidos:	Ros Abenza			Nota:	
Nombre:	Enrique				

7. Una vez hecho esto ya no podremos acceder desde PuTTY al usuario “root” una vez cambiado el parámetro y recargado el servicio SSH de nuestra máquina



```

10.4.200.178 - PuTTY
login as: root
root@10.4.200.178's password:
Access denied
root@10.4.200.178's password:

```