

Tema 3 – Entorno seguro Servidor SSH

Ayuda para la práctica

Administración de Sistemas Operativos

Instalación y configuración inicial

```
# sudo -i
```

```
# apt-get update
```

```
# apt-get install openssh-server
```

```
# /etc/init.d/ssh stop|start|restart|reload
```

```
# service ssh stop|start|restart|reload
```

- Configuración: `/etc/ssh/sshd_config`

`PermitRootLogin prohibit-password`

`PermitRootLogin yes`

Port 22 → 4776 (cambiar puerto por seguridad)

Uso básico del cliente SSH

```
# ssh <host>
```

```
# ssh <user>@<host>
```

```
# ssh -p <port> <user>@<host>
```

```
# ssh -p <port> -l <user> <host>
```

```
# ssh <host> <command>
```

```
# ssh <user>@<host> <command>
```

```
# ssh -p <port> <user>@<host> <command>
```

```
# ssh -p <port> -l <user> <host> <command>
```

Creando grupo de acceso por SSH

```
# groupadd hostusers
```

```
# useradd -g hostusers -d /hosting/testuser/home
```

```
-s /sbin/nologin testuser
```

```
# passwd testuser
```

```
# grep testuser /etc/passwd
```

- **Editamos /etc/ssh/sshd_config**

```
#Subsystem sftp /usr/lib/openssh/sftp-server
```

```
Subsystem sftp internal-sftp
```

Restringimos ámbito del grupo

- **Editamos /etc/ssh/sshd_config**

```
#Subsystem sftp /usr/lib/openssh/sftp-server
```

```
Subsystem sftp internal-sftp
```

```
Match Group hostusers
```

```
ChrootDirectory /hosting/%u
```

```
ForceCommand internal-sftp
```

Restringimos ámbito del grupo

- **Creamos los directorios**

```
# mkdir -p /hosting/testuser/home/public_html
```

- **Cambiamos los directorios de usuario y grupo**

```
# chown testuser:hostusers /hosting/testuser/home
```

- **Reiniciamos el servicio**

```
# service ssh restart
```

- **Probamos a conectarnos**

```
# ssh -p 4776 testuser@192.168.56.101
```

```
# sftp -P 4776 testuser@192.168.56.101
```