

Práctica 5

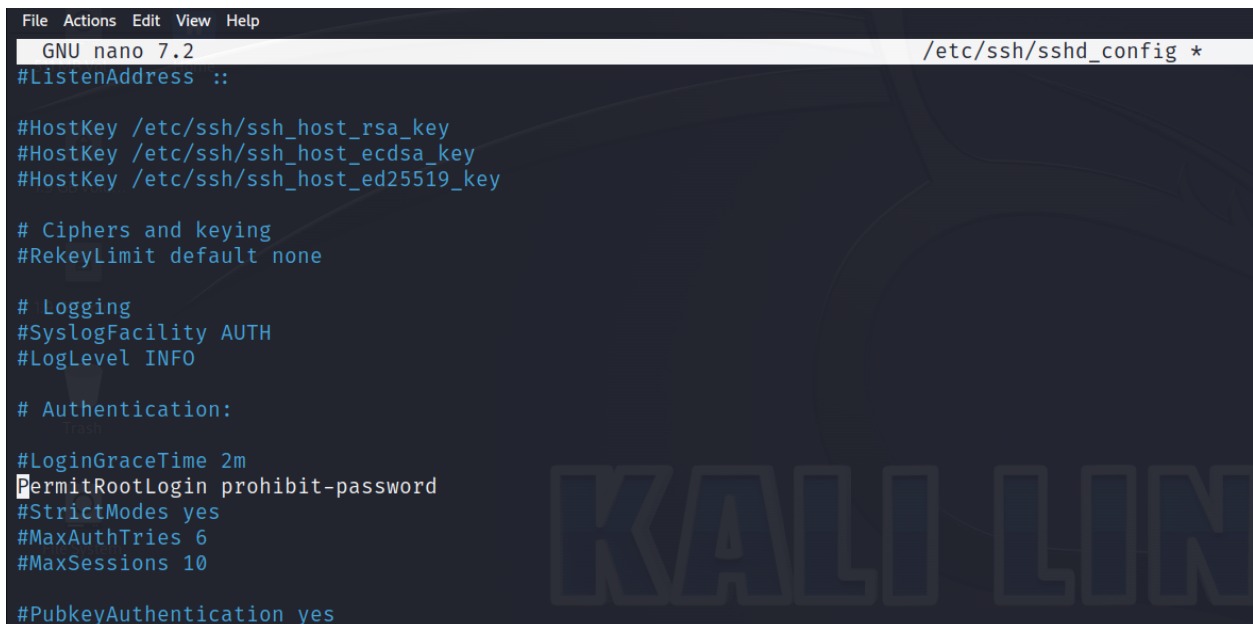
Adquisición de evidencia por la red

En situaciones en las que no disponemos del hardware adecuado, podemos realizar la extracción de evidencias a través de la red. En este escenario, se requieren dos máquinas: la máquina implicada, de la cual deseamos recuperar las evidencias, y nuestra estación forense.

A través de SSH

Podemos utilizar SSH para este propósito; únicamente necesitaremos contar con un usuario y un servidor SSH en nuestra estación forense. Además, dispondremos de una unidad donde almacenaremos las evidencias

Desde la máquina implicada, utilizaremos un entorno Kali Live y configuraremos el servidor SSH para permitir el acceso como root.



```
File Actions Edit View Help
GNU nano 7.2 /etc/ssh/sshd_config *
#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
```

Una vez configurado, podemos realizar la clonación utilizando el comando 'dd' y enviarlo a la estación forense mediante SSH desde el equipo implicado. Utilizaremos el comando '**sudo dd if=/dev/sdx | ssh user@estacion_forense "dd of=/ruta/imagen.raw"**'.

```
(kali㉿kali)-[~]
└─$ sudo dd if=/dev/sda | ssh jose@192.168.1.221 "dd of=/home/jose/clon/imagen.raw"
The authenticity of host '192.168.1.221 (192.168.1.221)' can't be established.
ED25519 key fingerprint is SHA256:yMaXyYT4L/czMYNNfMyQ7+885lHKAxIUW9zoaNiA408.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.221' (ED25519) to the list of known hosts.
jose@192.168.1.221's password:
10485760+0 records in
10485760+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 190.572 s, 28.2 MB/s
10485760+0 records in
10485760+0 records out
5368709120 bytes (5,4 GB, 5,0 GiB) copied, 185,002 s, 29,0 MB/s
(kali㉿kali)-[~]
```

Una vez completado el proceso, podemos verificar los hash y observar que coinciden con los obtenidos en la práctica 2.

```
(jose㉿jose-almiron)-[~/clon]
└─$ sudo sha512sum imagen.raw
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1ddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae  imagen.raw
```

Comandos utilizados en este apartado desde la máquina implicada:

```
(kali㉿kali)-[~]
└─$ history
 1 setxkbmap es
 2 sudo nano /etc/ssh/sshd_config
 3 sudo dd if=/dev/sda | ssh jose@192.168.1.221 "dd of=/home/jose/clon/imagen.raw"
```

A través de NetCat

En caso de no poder disponer de un servidor SSH, otra opción es utilizar la herramienta Netcat, aunque es menos recomendable. Para ello, desde la estación forense ejecutamos '**sudo nc -l -p 5000 > /ruta**'. Con esto, configuramos nuestra estación forense para escuchar en el puerto 5000 y almacenar los datos en la ruta que especifiquemos.

```
(jose@jose-almiron)-[~]  
$ sudo nc -l -p 5000 > /home/jose/clon/imagen2.raw
```

Desde el equipo implicado que se desea adquirir evidencias, ejecutaremos '**sudo dd if=/dev/sx | nc estacion_forense 5000**'. Esto llevará a cabo la clonación y enviará los datos a nuestra estación a través del puerto 5000.

```
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo dd if=/dev/sda | nc 192.168.1.221 5000
```

Una vez completado el proceso, procedemos a calcular el hash de la evidencia adquirida.

```
(jose@jose-almiron)-[~]  
$ sudo sha512sum clon/imagen2.raw  
f083c828f4c9f06f593ed470b12be44e5f2d485e0c9ad0a0da2636c071f03d881d1ddd1e2946f7b14814626075b2395222d99a92903d0f5134aaabaca5c30ae clon/  
imagen2.raw
```

Estos son los comandos utilizados desde el equipo implicado

```
(kali@kali)-[~]  
$ history  
1 setxkbmap es  
2 sudo dd if=/dev/sda | nc 192.168.1.221 5000  
(kali@kali)-[~]
```

Comandos utilizados en la estación forense

```
8  ping 192.168.1.220
9  sudo mkfs.ext4 /dev/sdb
10 mkdir clon
11 sudo mount /dev/sdb /home/jose/clon
12 sudo systemctl start ssh
13 chown jose:jose clon
14 sudo chown jose:jose clon
15 sudo sha512sum clon/imagen.raw
16 sudo nc -l -p 5000 > /home/jose/clon/imagen2.raw
17 sudo sha512sum clon/imagen2.raw
```

```
(jose@jose-almiron)-[~]
$
```