Borrado de Huellas

- Hay que verificar hasta que punto el potencial atacante tendría capacidad de eliminar el rastro de sus acciones y mantener el control del sistema sin ser detectado. Para ello suele ser necesaria la eliminación de registros y logs que contengan información que pueda revelar el ataque.
- Destrucción del sistema: Cuando la evidencia es tal, que no queda otra. Normalmente se inhabilita el login para causar un gran destrozo. Se suelen ejecutar los siguientes comandos:

```
rm /etc/passwd
rm /etc/shadow
rm /etc/login
rm /etc/rm
rm /etc/inetd.conf
killall login
```

- Capturando y eliminando los logs de acceso de Apache. Esta opción solo es viable si se realizó un ataque a nivel web. Los directiorios en cuestión suelen ser:

```
apache/logs/error.log
apache/logs/access.log
apache/logs/error.log
apache/logs/error.log
etc/httpd/logs/acces_log
etc/httpd/logs/error_log
etc/httpd/logs/error.log
var/www/logs/access_log
var/www/logs/access.log
usr/local/apache/logs/access_log
```

- Eliminar el historial de Bash: Eliminar .bash_history o .sh_history justo antes de salir
- Eliminar todo rastro de exploits, webshells, sniffers...
- Cuidado con Syslog: puede ser más complejo de lo habitual deshacer cambios realizados en este.
- Ficheros peligrosos:
  - utmp: Guarda un registro de los usuarios que usan el sistema mientras están conectados
    - /var/adm/utmp
    - /etc/utmp
  - wtmp: Guarda un log cada vez que un usuario entra o sale del sistema
  - lastlog: Guarda un log del momento en el que un usuario entró por última vez
  - acct o pacct: Guarda todos los comandos ejecutados por un usuario.

Búsqueda de nueva info

- Buscar las herramientas disponibles en el sistema remoto:

```
which bash
which curl
which ftp
```

```
which nc
which nmap
which ssh
which telnet
which tftp
which wget
which sftp
```

- Encontrar información sobre la red objetivo

```
ifconfig
arp
cat /etc/hosts
cat /etc/hosts.allow
cat /etc/hosts.deny
cat /etc/network/interfaces
```

- Determinar conexiones del sistema

```
netstat -an
```

- verificar los paquetes instalados en el sistema

```
dpkg -l
```

- Visualizar el repositorio de paquetes

```
cat /etc/apt/sources.list
```

- Buscar información sobre los programas y servicios

```
runlevel
ls /etc/rc2.d
```

- Buscar más información sobre el sistema

```
df -h
cd /home
ls -oaF
ls -lisa
cd /
ls -aRIF
```

- Revisar los archivos de historial y registro

```
ls -l /home
ls -la /home/user
cat /home/user/.bash_history
ls -l /var/log
tail /var/log/lastlog
tail /var/log/messages
```

- Revisar los usuarios y las credenciales

```
w
last
lastlog
ls -alG /root/.ssh
cat /root/.ssh/known_hosts
cat /etc/passwd
cat /etc/shadow
```

- Revisar configuraciones y otros archivos importantes

```
cat /etc/crontab
cat /etc/fstab
```