



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid

Bastionado Linux

Héctor Ramírez López

Índice

1.	Configuración del sistema.....	3
1.1.	Actualización y mantenimiento del sistema	3
1.2.	Eliminación de servicios	4
1.3.	Configuración segura del servicio SSH.....	6
1.4.	Configuración de firewall	8
2.	Seguridad de usuarios y contraseñas.....	10
1.1.	Políticas de contraseñas	10
3.	Validación y auditoría.....	11
3.1.	Uso de herramientas de auditoría.....	11
3.2.	Verificación mediante escaneo.....	13

1. Configuración del sistema

1.1. Actualización y mantenimiento del sistema

Lo primero que vamos a hacer es actualizar el sistema con los comandos (sudo apt update) y (sudo apt upgrade)

```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [186 kB]
Fetched 73.8 MB in 4s (17.3 MB/s)

(kali㉿kali)-[~]
$ sudo apt upgrade
The following packages were automatically installed and are no longer required:
  amass-common      libjs-jquery-ui      librav1e0.7      libwsutil16
  libbluray2        libjs-underscore    libtheoradec1   libx264-164
  libbson-1.0-0t64  libmongoc-1.0-0t64  libtheoraenc1   libxml2
  libdisplay-info2   libnet1            libudfread0     python3-bluepy
  libgeos3.14.0     libplacebo349      libwireshark18  python3-click-plugins
  libinstpatch-1.0-2 libportmidi0      libwiretap15    python3-gpg
Use 'sudo apt autoremove' to remove them.

Upgrading:
```

1.2. Eliminación de servicios

Ahora veremos como deshabilitar un servicio en caso de que no lo necesitemos, para ello ejecutaremos el comando de la imagen para ver qué servicios están habilitados.

```
(kali㉿kali)-[~]
└─$ systemctl list-unit-files | grep enabled
accounts-daemon.service          enabled      enabled
console-setup.service             enabled      enabled
cron.service                      enabled      enabled
fail2ban.service                 enabled      disabled
getty@.service                   enabled      enabled
grub-install-devices.service     enabled      disabled
haveged.service                  enabled      enabled
keyboard-setup.service           enabled      enabled
lightdm.service                  enabled      disabled
ModemManager.service              enabled      enabled
networking.service               enabled      enabled
NetworkManager-dispatcher.service enabled      disabled
NetworkManager-wait-online.service enabled      disabled
NetworkManager.service            enabled      enabled
nfs-common.service               masked      enabled
regenerate-ssh-host-keys.service enabled      enabled
rsync.service                     disabled     enabled
rtkit-daemon.service             disabled     enabled
smartmontools.service            enabled      enabled
sudo.service                      masked      enabled
systemd-confext.service          disabled     enabled
systemd-fsck-root.service        enabled-runtime disabled
```

En este caso para ver como deshabilitarlo lo haremos con el servicio de la imagen.

```
accounts-daemon.service          enabled      enabled
```

Para ello ejecutamos el siguiente comando .

```
(kali㉿kali)-[~]
└─$ sudo systemctl disable accounts-daemon.service
Removed '/etc/systemd/system/graphical.target.wants/accounts-daemon.service'.
```

Y comprobamos con el comando anterior que se ha deshabilitado.

```
(kali㉿kali)-[~]
└─$ systemctl list-unit-files | grep enabled
accounts-daemon.service           disabled
```

Ahora volveremos a habilitar el servicio con el comando siguiente .

```
(kali㉿kali)-[~]
└─$ sudo systemctl enable accounts-daemon.service
```

Volveremos a comprobar que se ha habilitado.

```
(kali㉿kali)-[~]
└─$ systemctl list-unit-files | grep enabled
accounts-daemon.service           enabled
```

1.3. Configuración segura del servicio SSH

Ahora lo primero sera editar el fichero de configuración del SSH con el comando (sudo nano /etc/ssh/sshd_config) .

```
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
```

Una vez abierto el archivo para editarlo lo veremos así .

```
GNU nano 8.6                               /etc/ssh/sshd_config

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

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

Ahora modificaremos algunos parámetros del archivo como (permitrootlogin yes) para permitir el acceso a root por SSH, (maxauthtries) para establecer el maximo de intentos para autenticarse en este caso hemos puesto 6 y (maxsessions) para limitar el número de sesiones simultaneas en este caso hemos puesto 9.

```
GNU nano 8.6                               /etc/ssh/sshd_config

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

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

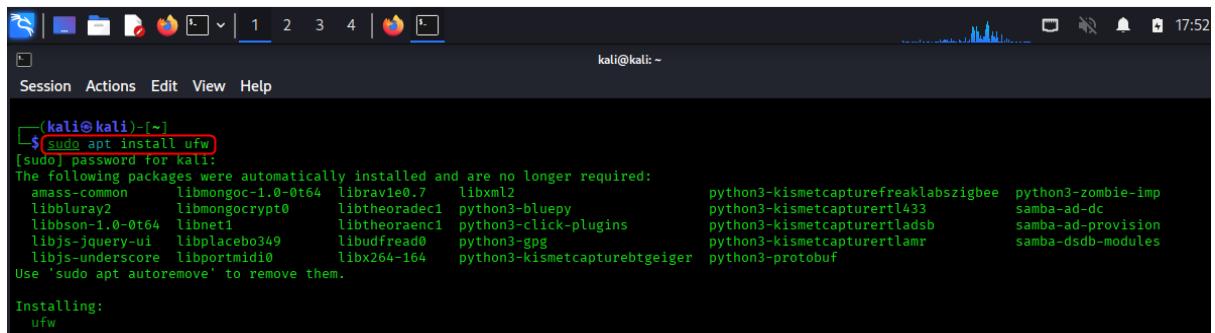
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
MaxAuthTries 6
MaxSessions 9
```

1.4. Configuración de firewall

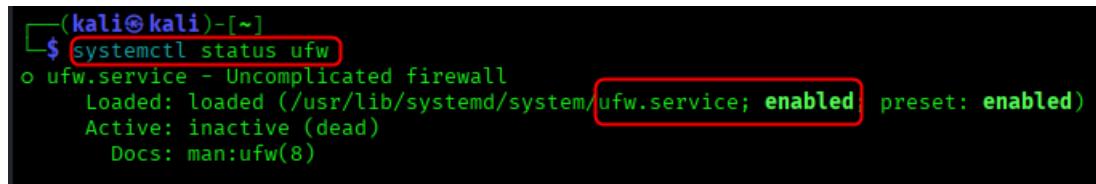
Lo primero que haremos en este punto será instalar el firewall con el comando (sudo apt install ufw).



```
(kali㉿kali)-[~]
$ sudo apt install ufw
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  amass-common   libmongoc-1.0-0t64  librav1e0.7  libxml2
  libblury2     libmongocrypt0    libtheoradec1 python3-bluepy
  libbson-1.0-0t64 libnetl1      libtheoraenc1  python3-click-plugins
  libjs-jquery-ui libplacebo349   libubfread0   python3-gpg
  libjs-underscore libportmid10   libx264-164   python3-kismetcapturebtgeiger
  Use 'sudo apt autoremove' to remove them.

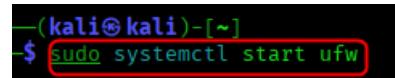
Installing:
  ufw
```

Una vez instalado nos aseguramos de que el servicio UFW este habilitado lo vemos con el comando (systemctl status ufw) como se observa en la imagen está habilitado.



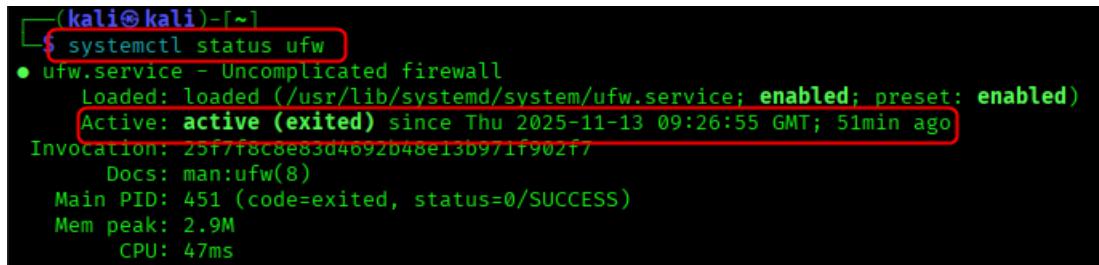
```
(kali㉿kali)-[~]
$ systemctl status ufw
● ufw.service - Uncomplicated firewall
  Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: enabled)
  Active: inactive (dead)
    Docs: man:ufw(8)
```

El siguiente paso es activar el servicio con el comando (sudo systemctl start ufw).



```
(kali㉿kali)-[~]
$ sudo systemctl start ufw
```

Comprobaremos que está activo con el comando anterior.



```
(kali㉿kali)-[~]
$ systemctl status ufw
● ufw.service - Uncomplicated firewall
  Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: enabled)
  Active: active (exited) since Thu 2025-11-13 09:26:55 GMT; 51min ago
    Invocation: 25f1f8c8e83d4692d48e13d971f902f/
      Docs: man:ufw(8)
    Main PID: 451 (code=exited, status=0/SUCCESS)
    Mem peak: 2.9M
      CPU: 47ms
```

Ahora procederemos a aplicar una regla al firewall para que rechace las conexiones entrantes lo haremos con el comando (sudo ufw default deny incoming).

```
(kali㉿kali)-[~]
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

Realizaremos lo mismo, pero para que permita las conexiones salientes, esto se hace con el comando (sudo ufw default allow outgoing).

```
(kali㉿kali)-[~]
$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

2. Seguridad de usuarios y contraseñas

1.1. Políticas de contraseñas

Para este punto instalaremos con (`sudo apt install libpam_pwquality`) para crear la política de contraseñas.

```
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install libpam-pwquality
The following packages were automatically installed and are no longer required:
  amass-common      libmongoc-1.0-0t64   libravie0.7    libxml2
  libbluray2        libmongocrypt0     libtheoradec1  python3-bluepy
  libbison-1.0-0t64 libnet1           libtheoraenc1  python3-click-plugins
  libjs-jquery-ui   libplacebo349     libudfread0    python3-gpg
  libjs-underscore  libportmidi0     libx264-164   python3-kismetcapturebtgeiger
                                         python3-kismetcapturefreer
                                         python3-kismetcapturertl4
                                         python3-kismetcapturertl
                                         python3-kismetcapturertl
                                         python3-kismetcapturebtgeiger
                                         python3-protobuf
Use 'sudo apt autoremove' to remove them.

Installing:
  libpam-pwquality
```

Tendremos que ajustar los criterios para establecer la complejidad de las contraseñas editaremos el fichero con (`sudo nano /etc/security/libpam-pwquality.conf`) y añadiríamos tres líneas (`minlen 12`) que sería el mínimo de caracteres que debe tener la contraseña, (`dcredit -1`) requiere al menos un numero en la contraseña y (`lcredit -1`) debe tener al menos 1 minúscula.

```
Session Actions Edit View Help /etc/security/libpam-pwquality.conf *  
GNU nano 8.6  
minlen 12  
dcredit -1  
(credit -1)
```

3. Validación y auditoría

3.1. Uso de herramientas de auditoría

Instalaremos la herramienta de auditoria Lynis con (sudo apt intall lynis).

```
[kali㉿kali] ~
$ sudo apt install lynis
[sudo] password for kali:
lynis is already the newest version (3.1.4-1).
The following packages were automatically installed
  amass-common      libmongoc-1.0-0t64   libravie0.7
  libbluray2        libmongocrypt0    libtheorade
  libsson-1.0-0t64   libnet1          libtheoraen
  libvdpau1         libnisi1         libtiff5
  libvdpau1         libnisi1         libtiff5
```

Ejecutaremos la herramienta con el comando (`sudo lnyis audit system`).

```
[kali㉿kali)-[~] $ sudo llynis audit system
```

Tras ejecutar este comando nos realizará una auditoría y nos dará los resultados. Nos da un 63 de hardening index es decir una puntuación media y nos recomienda: Configurar políticas más estrictas de contraseñas y permisos, activar un antivirus o escáner de malware, fortalecer el firewall y asegurar servicios de red innecesarios.

```
Lynis security scan details:

Hardening index : 63 [#####
Tests performed : 276
Plugins enabled : 1

Components:
- Firewall          [V]
- Malware scanner   [X]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status    [?]
- Security audit       [V]
- Vulnerability scan   [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat

=====
Lynis 3.1.4

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2024, CISOfy - https://cisofty.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
```

3.2. Verificación mediante escaneo

Aquí mostramos el escaneo localhost realizado con nmap se ha realizado con el comando (nmap 127.0.0.1) nos dice que nmap ha escaneado 1000 puertos, pero no ha encontrado ninguno abierto.

```
(kali㉿kali)-[~]
$ nmap 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 11:23 GMT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid