Parte 1: Gestión de usuarios y grupos en Linux

*Su función principal es crear automáticamente el **directorio home** del nuevo usuario que estás añadiendo.*

Al pertenecer a múltiples grupos, el usuario puede tener acceso a diferentes recursos y permisos que son específicos de cada grupo. Los grupos como desarrollo y marketing permiten que el usuario colabore con diferentes equipos. Proporciona flexibilidad en la asignación de roles. El usuario puede desempeñar diferentes funciones según el grupo al que esté accediendo en un momento dado.

Parte 2: Permisos de Archivos y Directorios en Linux

```
┌──(kali㉿kali)-[~]
└─$ sudo mkdir -p /empresa/{administracion,desarrollo,marketing,directivos}

┌──(kali㉿kali)-[~]
└─$ sudo touch /empresa/administracion/nominas.txt

┌──(kali㉿kali)-[~]
└─$ sudo touch /empresa/desarrollo/codigo.txt

┌──(kali㉿kali)-[~]
└─$ sudo touch /empresa/desarrollo/documentacion.txt

┌──(kali㉿kali)-[~]
└─$ sudo touch /empresa/marketing/publicidad2025.txt

┌──(kali㉿kali)-[~]
└─$ sudo touch /empresa/directivos/estrategia_confidencial.txt

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo chgrp desarrollo /empresa/desarrollo/*
[redacted]

┌──(kali㉿kali)-[~]
└─$ sudo chgrp directivos /empresa/directivos/*

┌──(kali㉿kali)-[~]
└─$ sudo chgrp marketing /empresa/marketing/*

┌──(kali㉿kali)-[~]
└─$ sudo chgrp administracion /empresa/administracion/*

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo chgrp directivos /empresa/directivos/*

┌──(kali㉿kali)-[~]
└─$ sudo chgrp marketing /empresa/marketing/*

┌──(kali㉿kali)-[~]
└─$ sudo chgrp administracion /empresa/administracion/*

┌──(kali㉿kali)-[~]
└─$ sudo chmod 770 /empresa/administracion

┌──(kali㉿kali)-[~]
└─$ sudo chmod 770 /empresa/desarrollo

┌──(kali㉿kali)-[~]
└─$ sudo chmod 770 /empresa/marketing

┌──(kali㉿kali)-[~]
└─$ sudo chmod 750 /empresa/directivos

┌──(kali㉿kali)-[~]
└─$ sudo chmod 770 /empresa/administracion/*
chmod: cannot access '/empresa/administracion/*': No such file or directory

┌──(kali㉿kali)-[~]
└─$ sudo chmod -R 770 /empresa/administracion/

┌──(kali㉿kali)-[~]
└─$ sudo chmod -R 770 /empresa/desarrollo/

┌──(kali㉿kali)-[~]
└─$ sudo chmod -R 770 /empresa/marketing/
```

```
┌──(kali㉿kali)-[~]
└─$ sudo chgrp -R desarrollo /empresa/desarrollo

┌──(kali㉿kali)-[~]
└─$ su - ana_dev
Password:
su: Authentication failure

┌──(kali㉿kali)-[~]
└─$ su - ana_dev
Password:
$ ls
$ cd ..
$ ls
ana_dev  director  kali  pedro_dir  raul_adm  rosa_mark  user
$ cd ..
$ ls
bin   dev      etc   initrd.img      lib    lib64       media  opt   root  sbin  swap  tmp  var      vmlinuz.old
boot  empresa  home  initrd.img.old  lib32  lost+found  mnt    proc  run   srv   sys   usr  vmlinuz
$ cd empresa
$ ls
administracion  desarrollo  directivos  marketing
$ cd desarrollo
$ ls
codigo.txt  documentacion.txt
$
```

```
$ ls
codigo.txt  documentacion.txt
$ cat codigo_fuente.txt
cat: codigo_fuente.txt: No such file or directory
$ cat codigo.txt
$ echo "nuevo codigo" >> codigo.txt
$ ls
codigo.txt  documentacion.txt
$ cd /empresa/administracion
-sh: 14: cd: can't cd to /empresa/administracion
$
```

```
┌──(kali㉿kali)-[/home]
└─$ su - director
Password:
$ cd /empresa/desarrollo
$ ls -la
total 12
drwxrwx--- 2 root desarrollo 4096 Nov  5 03:11 .
drwxr-xr-x 6 root root       4096 Nov  5 03:10 ..
-rwxrwx--- 1 root desarrollo   13 Nov 10 02:39 codigo.txt
-rwxrwx--- 1 root desarrollo    0 Nov  5 03:11 documentacion.txt
$ cd /empresa/desarrollo
$ exit

┌──(kali㉿kali)-[/home]
└─$
```

Permiso 770

- Representación: ` rwxrwx---
- Desglose:
    - rwx (propietario): *El propietario del archivo tiene permisos de lectura (r), escritura (w) y ejecución (x).*
    - rwx (grupo): *Los miembros del grupo también tienen permisos de lectura, escritura y ejecución.*
    - --- (otros): *No hay permisos para otros usuarios.*

Permiso 660

- Representación: ` rw-rw----
- Desglose:
    - rw- (propietario): *El propietario tiene permisos de lectura y escritura, pero no de ejecución.*
    - rw- (grupo): *Los miembros del grupo también tienen permisos de lectura y escritura.*
    - --- (otros): *No hay permisos para otros usuarios.*

Se deseas que el propietario tenga control total sobre el archivo o directorio, mientras que los miembros del grupo pueden leer y ejecutar, pero no modificar.

No se pudieron acceder a directorios sobre los cuales no se tenían permisos.

Sale un mensaje indicando que no puede acceder a esa carpeta.

Parte 3: Firewall con UFW en Linux

```
┌──(kali㉿kali)-[/home]
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.3 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [259 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [186 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [893 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [28.4 kB]
Fetched 74.8 MB in 17s (4,487 kB/s)
1024 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[/home]
└─$ sudo apt install ufw -y
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1024
  Download size: 169 kB
  Space needed: 880 kB / 63.2 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 0s (553 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 417218 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/sy
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(kali㉿kali)-[/home]
└─$ sudo ufw status verbose
Status: inactive
```

```
┌──(kali㉿kali)-[/home]
└─$ sudo ufw status verbose
Status: inactive

┌──(kali㉿kali)-[/home]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[/home]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

```
┌──(kali㉿kali)-[/home]
└─$ sudo ufw --force reset
Backing up 'user.rules' to '/etc/ufw/user.rules.20251110_030744'
Backing up 'before.rules' to '/etc/ufw/before.rules.20251110_030744'
Backing up 'after.rules' to '/etc/ufw/after.rules.20251110_030744'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20251110_030744'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20251110_030744'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20251110_030744'


┌──(kali㉿kali)-[/home]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw allow from 10.0.0.66 to any port 22
Rules updated

┌──(kali㉿kali)-[/home]
└─$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw allow from 127.0.0.1 to any port 3306
Rules updated

┌──(kali㉿kali)-[/home]
└─$ sudo ufw allow out 53
Rules updated
Rules updated (v6)

┌──(kali㉿kali)-[/home]
└─$ sudo ufw limit ssh
Rules updated
Rules updated (v6)
```

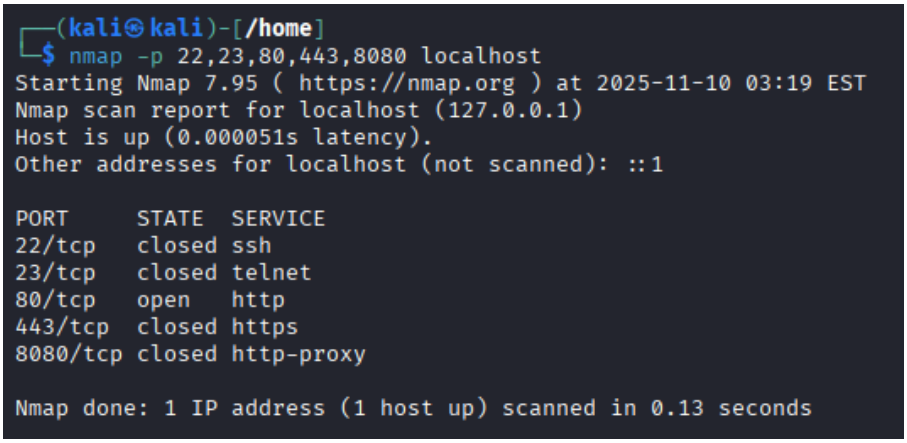
```
┌──(kali㉿kali)-[/home]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[/home]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    10.0.0.66
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
3306                       ALLOW IN    127.0.0.1
22/tcp                     LIMIT IN    Anywhere
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
22/tcp (v6)                LIMIT IN    Anywhere (v6)

53                         ALLOW OUT   Anywhere
53 (v6)                    ALLOW OUT   Anywhere (v6)
```

```
┌──(kali㉿kali)-[/home]
└─$ sudo systemctl start apache2

┌──(kali㉿kali)-[/home]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-11-10 03:12:59 EST; 11s ago
 Invocation: c3e3dc1ff52f4315a2ec3a0f7aa728f9
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 55916 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 55932 (apache2)
      Tasks: 6 (limit: 5067)
     Memory: 20.7M (peak: 21.1M)
        CPU: 177ms
     CGroup: /system.slice/apache2.service
             ├─55932 /usr/sbin/apache2 -k start
             ├─55943 /usr/sbin/apache2 -k start
             ├─55944 /usr/sbin/apache2 -k start
             ├─55945 /usr/sbin/apache2 -k start
             ├─55946 /usr/sbin/apache2 -k start
             └─55947 /usr/sbin/apache2 -k start

Nov 10 03:12:58 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 10 03:12:59 kali apachectl[55931]: AH00558: apache2: Could not reliably determine the s
Nov 10 03:12:59 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
... skipping ...
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-11-10 03:12:59 EST; 11s ago
 Invocation: c3e3dc1ff52f4315a2ec3a0f7aa728f9
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 55916 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
```

```
┌──(kali㉿kali)-[/home]
└─$ telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
```

```
┌──(kali㉿kali)-[/home]
└─$ nmap -p 23 localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 03:17 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000053s latency).
Other addresses for localhost (not scanned): ::1

PORT   STATE  SERVICE
23/tcp closed telnet

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

```
┌──(kali㉿kali)-[/home]
└─$ telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```



El puerto 80 esta open, resultado esperado

Al intentar conectar con el puerto 23 la conexión es rechazada

Reglas mas útiles:

LIMIT IN 22/tcp si hay demasiadas conexiones fallidas, bloquea temporalmente la IP atacante.

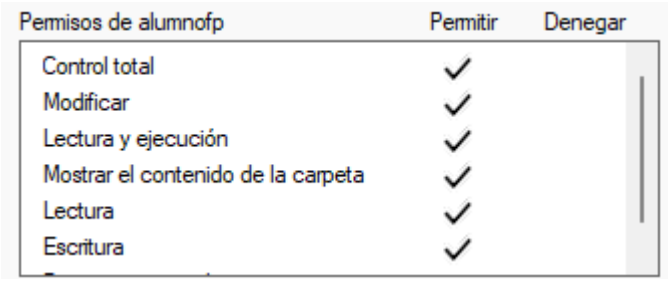
Allow 80/tcp y 443/tcp si usas un servidor web.

3306 solo desde 127.0.0.1 muy buena práctica: MySQL solo accesible localmente.

Parte 4: Controles de Acceso y Firewall en Windows

```
PS C:\Users\alumnofp> Get-LocalUser

Name               Enabled Description
----               ------- -----------
Administrador      False   Cuenta integrada para la administración del equipo o dominio
alumnofp           True
DefaultAccount     False   Cuenta de usuario administrada por el sistema.
Invitado           False   Cuenta integrada para el acceso como invitado al equipo o dominio
Usuario            True
WDAGUtilityAccount False   Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de ap...


PS C:\Users\alumnofp> Get-LocalGroup

Name                                Description
----                                -----------
Administradores                     Los administradores tienen acceso completo y sin restricciones al equi...
Administradores de Hyper-V          Los miembros de este grupo tienen acceso completo y sin restricciones ...
Duplicadores                        Pueden replicar archivos en un dominio
IIS_IUSRS                           Grupo integrado usado por Internet Information Services.
Invitados                           De forma predeterminada, los invitados tienen el mismo acceso que los ...
Lectores del registro de eventos    Los miembros de este grupo pueden leer registros de eventos del equipo...
Operadores criptográficos           Los miembros tienen autorización para realizar operaciones criptográfi...
Operadores de asistencia de control de acceso Los miembros de este grupo pueden consultar de forma remota los atribu...
Operadores de configuración de red  Los miembros en este equipo pueden tener algunos privilegios administr...
Operadores de copia de seguridad    Los operadores de copia de seguridad pueden invalidar restricciones de...
Operadores de hardware en modo usuario Los miembros de este grupo pueden operar con hardware desde el modo de...
Propietarios del dispositivo        Los miembros de este grupo pueden cambiar la configuración de todo el ...
System Managed Accounts Group       Los miembros de este grupo los administra el sistema.
Usuarios                            Los usuarios no pueden hacer cambios accidentales o intencionados en e...
Usuarios avanzados                  Los usuarios avanzados se incluyen para la compatibilidad con versione...
Usuarios COM distribuidos           Los miembros pueden iniciar, activar y usar objetos de COM distribuido...
Usuarios de administración remota   Los miembros de este grupo pueden acceder a los recursos de WMI median...
Usuarios de escritorio remoto       A los miembros de este grupo se les concede el derecho de iniciar sesi...
Usuarios de OpenSSH                 Los miembros de este grupo pueden conectarse a este equipo mediante SSH.
Usuarios del monitor de sistema     Los miembros de este grupo tienen acceso a los datos del contador de r...
Usuarios del registro de rendimiento Los miembros de este grupo pueden programar contadores de registro y r...
```

```
PS C:\Users\alumnofp> Get-Acl "C:\Users\alumnofp" | Format-List


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\alumnofp
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administradores Allow  FullControl
         FPB06\alumnofp Allow  FullControl
         S-1-15-3-65536-599108337-2355189375-1353122160-3480128286-3345335107-485756383-4087318168-230526575 Allow
         ExecuteFile, Synchronize
Audit  :
Sddl   : O:SYG:SYD:P(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-3421037145-133781885-1423182514-1002)(A;;0x10
         0020;;;S-1-15-3-65536-599108337-2355189375-1353122160-3480128286-3345335107-485756383-4087318168-230526575)
```



Los permisos coinciden.

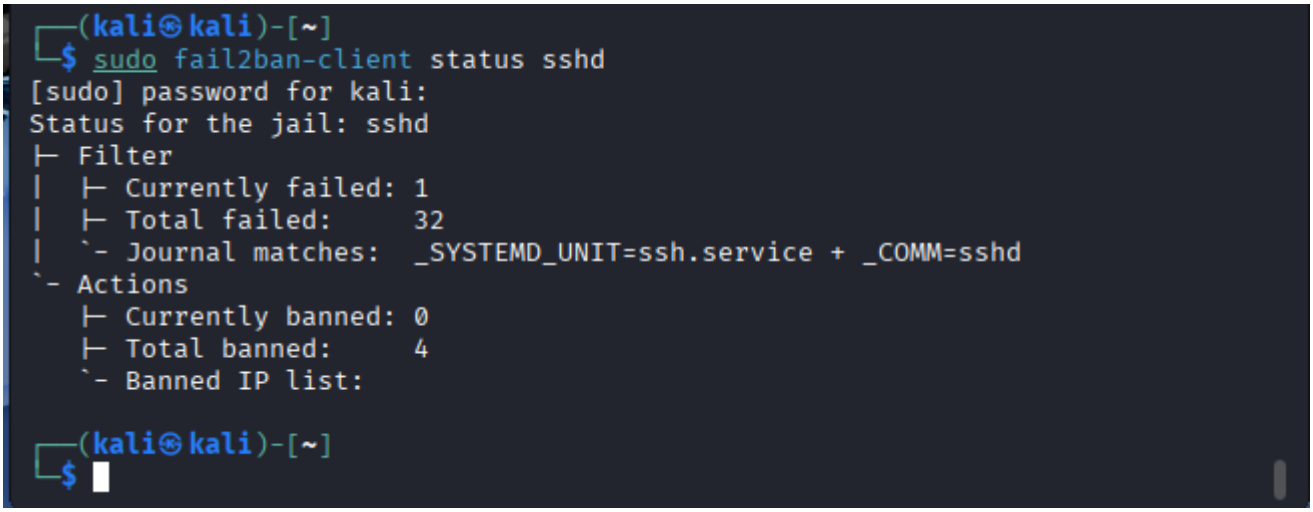
Parte 5: Detección de Intrusiones con Fail2ban

```
┌──(kali㉿kali)-[/home]
└─$ sudo apt install fail2ban -y
[sudo] password for kali:
Installing:
  fail2ban

Installing dependencies:
  python3-systemd
```

```
┌──(kali㉿kali)-[/home]
└─$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

┌──(kali㉿kali)-[/home]
└─$ sudo systemctl start ssh

┌──(kali㉿kali)-[/home]
└─$ sudo systemctl status fail2ban
○ fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:fail2ban(1)

┌──(kali㉿kali)-[/home]
└─$ sudo systemctl start fail2ban

┌──(kali㉿kali)-[/home]
└─$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-11-11 03:22:21 EST; 3s ago
 Invocation: 2c34e574e6734307b1e5217bcef7b432
       Docs: man:fail2ban(1)
   Main PID: 66955 (fail2ban-server)
      Tasks: 5 (limit: 5067)
     Memory: 15M (peak: 15.4M)
        CPU: 969ms
     CGroup: /system.slice/fail2ban.service
             └─66955 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 11 03:22:21 kali systemd[1]: Started fail2ban.service - Fail2Ban Service.
Nov 11 03:22:23 kali fail2ban-server[66955]: Server ready
```

```
┌──(kali㉿kali)-[/home]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.28/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 28730sec preferred_lft 28730sec
    inet6 fd17:625c:f037:2:294b:e0b3:2abc:ae3f/64 scope global dynamic noprefixroute
       valid_lft 86054sec preferred_lft 14054sec
    inet6 fe80::ced7:cdcd:f756:f622/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
C:\Users\alumnofp>ssh usuario_falso@10.0.0.66
ssh: connect to host 10.0.0.66 port 22: Connection timed out

C:\Users\alumnofp>ssh usuario_falso@10.0.0.28
The authenticity of host '10.0.0.28 (10.0.0.28)' can't be established.
ED25519 key fingerprint is SHA256:11JOgyYpco2p37ABaV1r+JAhGQxGmac0UrTGuq+ks0g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.0.28' (ED25519) to the list of known hosts.
usuario_falso@10.0.0.28's password:
Permission denied, please try again.
usuario_falso@10.0.0.28's password:
Permission denied, please try again.
usuario_falso@10.0.0.28's password:
usuario_falso@10.0.0.28: Permission denied (publickey,password).
```



Funcionamiento:

Monitorea los archivos de log del sistema

Detecta intentos fallidos repetidos

Acción: bloquea la IP maliciosa automáticamente

Ante un ataque:

- Registra el número de fallos de la IP
- Si supera el límite → detecta ataque
- Ejecuta una acción (banear IP)
- Añade una regla de firewall para bloquear tráfico
- Notifica en su log
- Mantiene el bloqueo durante cierto tiempo
- Luego elimina el bloqueo automáticamente

1. Protección contra fuerza bruta

Un servidor con SSH expuesto es atacado todos los días por bots automáticos.
Sin Fail2ban:

- podrían probar miles de contraseñas
- podrían entrar por fuerza bruta
- podrían causar un DoS por demasiadas conexiones

Fail2ban corta esos intentos rápidamente.

2. Reduce el ruido y la carga del servidor

Bloquear bots que intentan entrar constantemente:

- reduce uso de CPU
- reduce conexiones abiertas
- evita logs masivos

3. Capa adicional de seguridad

Fail2ban actúa como un sistema reactivo que se activa solo cuando hay un ataque real.

4. Protege múltiples servicios

No solo sirve para SSH:

- Apache / Nginx (ataques web)
- Servidores FTP
- MySQL
- Postfix / Dovecot (correo)
- APIs
- Paneles de administración

Cualquier servicio que genere logs puede ser protegido.