



GUARD

¿Qué es SSHGUARD?

Es un programa que protege a hosts frente a ataques de fuerza bruta o DOS contra SSH y otros servicios.

Analiza los logs del sistema, detecta ataques y procede a bloquear a los atacantes.

¿Contra qué tipos de ataque protege?

SSHGuard protege contra ataques de fuerza bruta y DOS a:

- SSH
- FTP
- IMAP/POP
- ..."

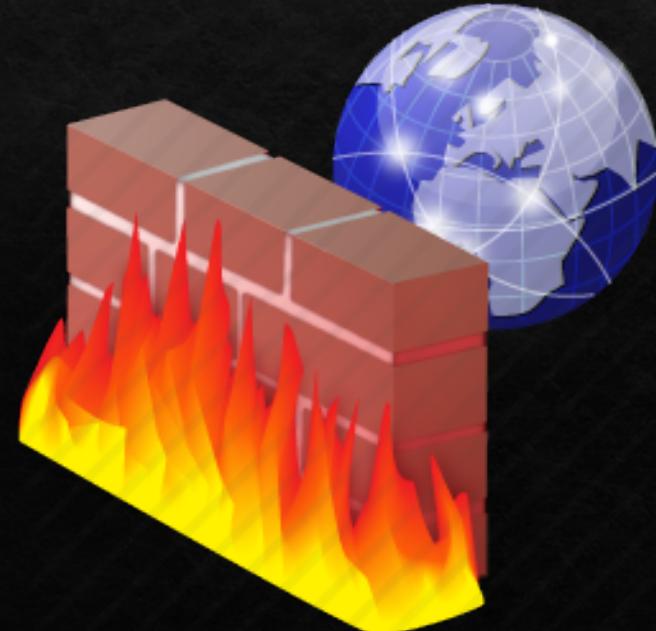
¿Cómo protege?

1. Consulta logs del sistema.
2. Si reconoce un ataque, bloquea la IP del atacante.
3. Después de un tiempo determinado desbloquea al supuesto atacante.

Todo lo que sshguard considere como un ataque, es bloqueado mediante el backend del firewall (iptables, PF, FirewallID, etc.).

Configuración (Linux)

1. Crear cadenas en el firewall:
 1. `iptables -N sshguard`
 2. `iptables -A INPUT -j sshguard #Todos los puertos`
 3. `iptables -A INPUT -m multiport -p tcp --destination-ports 21,22,80,110 #Algunos puertos`
2. Reiniciar firewall y sshguard.
3. Comandos:
 1. `-a`: umbral de puntuación para bloqueo.
 2. `-p`: tiempo de bloqueo.
 3. `-s`: tiempo de detección.
 4. `-w`: whitelist.





Created by Ioar Crespo and Guillermo Berasategui

Running on OSX system

[!] WARNING! This script only will work if sshguard is already installed.

----- MAIN MENU -----

Select option:

- [1] Set protected ports.
- [2] Whitelist addresses.
- [3] Set attack score threshold.
- [4] Set blocktime.
- [5] Set detection time.

Script en Pyhton

Hemos creado un script en Python para configurar SSHGuard de forma sencilla.

PROS y CONTRAS

PROS:

- Robusto. Hace lo que tiene que hacer y lo hace bien.
- Gratuito y de código abierto.
- Tiene opciones para configurar parámetros de bloqueo (listas blancas, tiempo de bloqueo, umbral de bloqueo...)

CONTRAS:

- Poca y mala documentación (funcionamiento y configuración).
- Desactualización. ¿Seguridad? ¿Nuevos ataques?



FAIL2BAN

¿Qué es y como funciona?

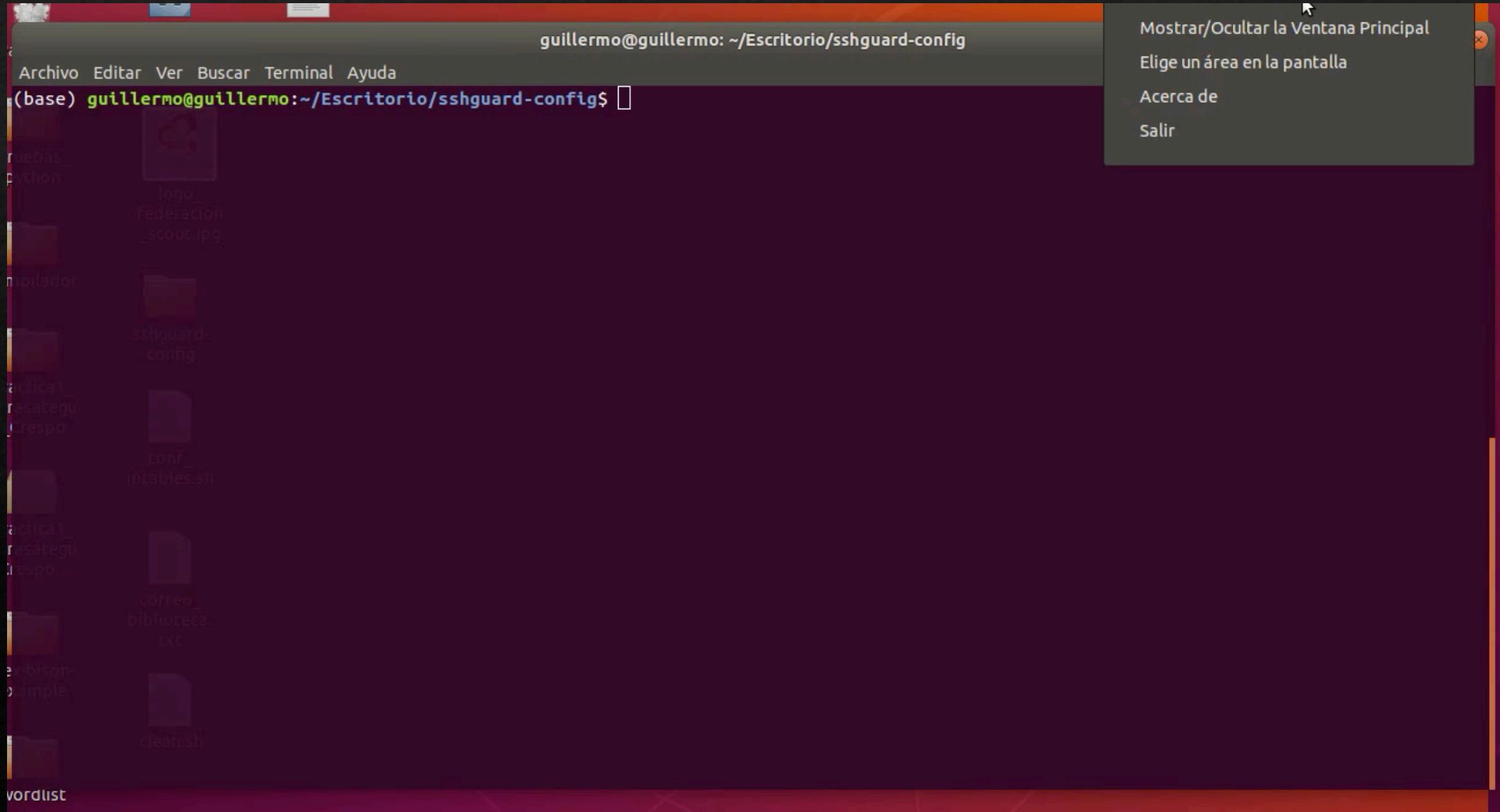
- Protección contra ataques fuerza bruta y DoS
- Desarrollado en Python
- Protección contra multiples servicios

Multiples acciones de defensa

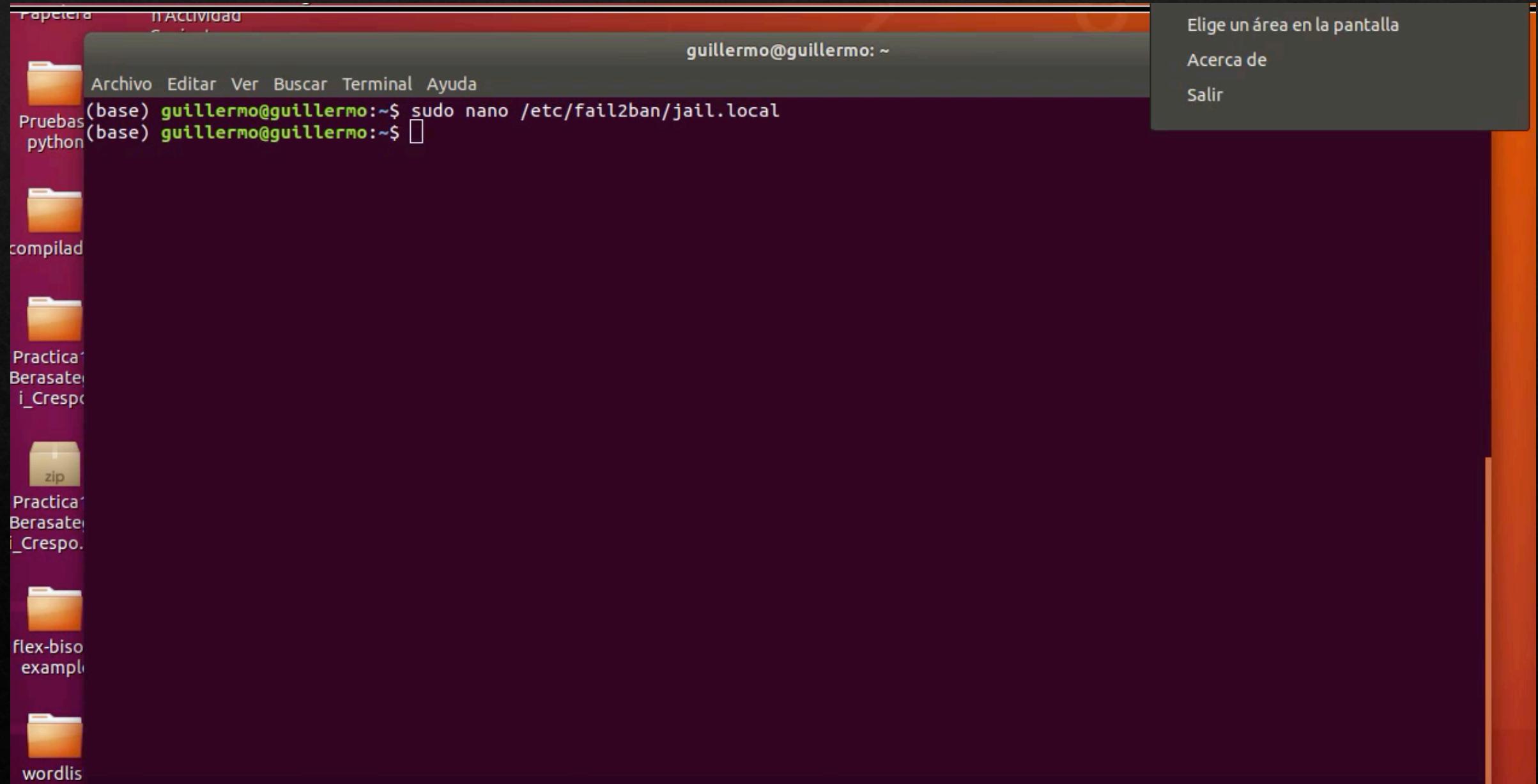
- Banear IP
- Banear IP +
Correo electrónico
- Script de Python
- ...



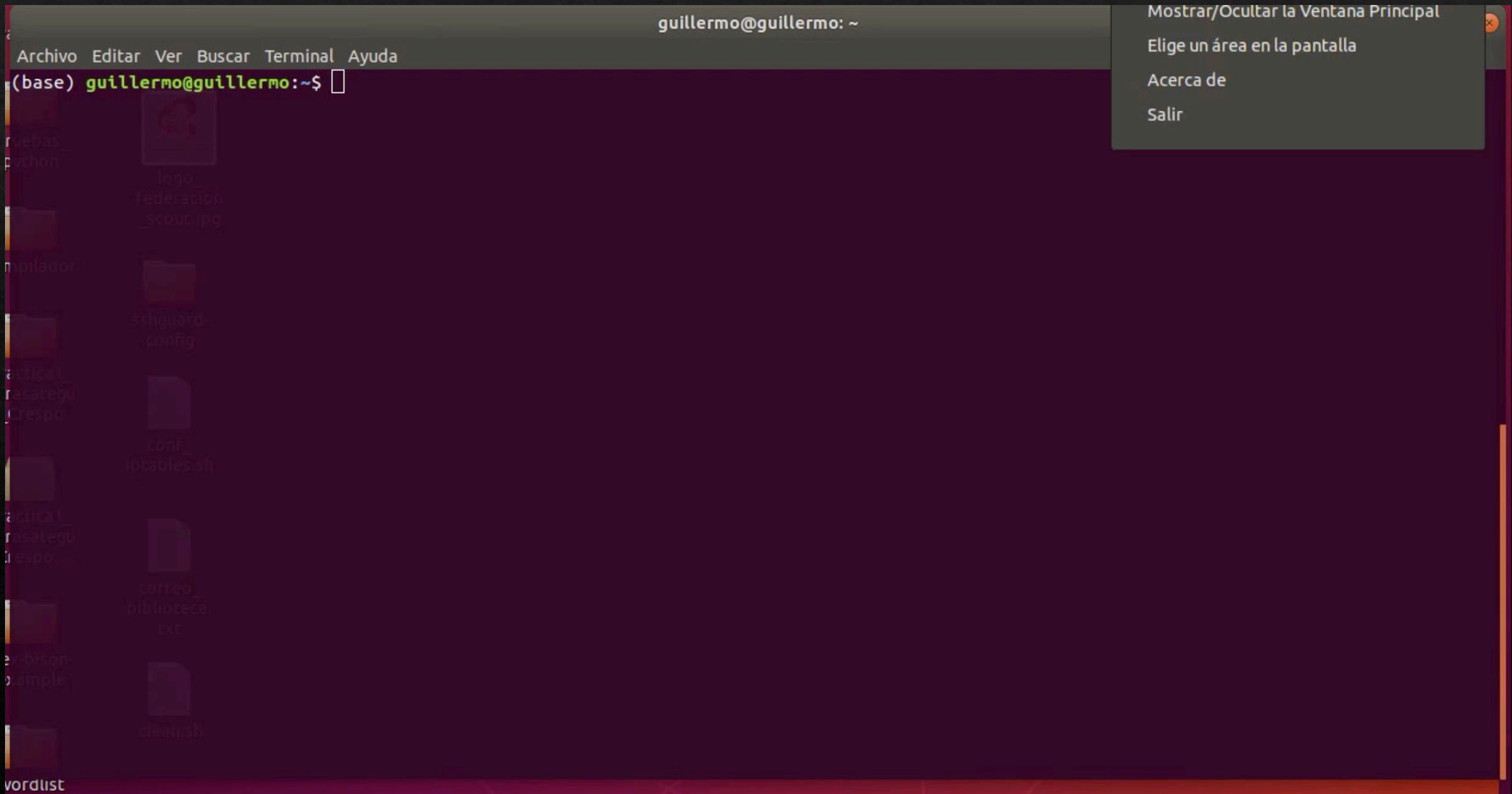
Configuración (I)



Configuración (II)



Ataque + baneo



Mail recibido

para mi ▾ ...

XA inglés ▾ > español ▾ Traducir mensaje Desactivar para: inglés ×

Hi,

The IP 192.168.1.139 has just been banned by Fail2Ban after 5 attempts against sshd.

Here is more information about 192.168.1.139 :

```
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/  
#  
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.  
#
```

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: [192.168.0.0/16](https://www.arin.net/resources/registry/whois/inaccuracy_reporting/)