**Tema V. Fail2ban**

Sistemes de Gestió Empresarial | 2023-2024

Andreu Sanz Sanz

Tabla de continguts

[1. Comprobar que ssh está instalado (o comprobar que esté instalado) 2](#_Toc152178118)

[2. Probar la conexión a través de ssh desde WIndows a Ubuntu Server (WinSCP, Putty..) 2](#_Toc152178119)

[3. ¿Qué es un ataque de fuerza bruta? 2](#_Toc152178121)

[4. ¿Para qué sirve y qué es FAIL2BAN? 3](#_Toc152178122)

[5. ¿Qué hace FAIL2BAN con el fichero de logs? 3](#_Toc152178123)

[6. ¿Qué son los jails? 3](#_Toc152178124)

[7. ¿Qué se puede hacer con FAIL2BAN? 3](#_Toc152178125)

[8. Instala Fail2BAN en Ubuntu Server. 3](#_Toc152178127)

[9. Habilita Fail2ban para que arranque automáticamente 3](#_Toc152178128)

[10. Comprobar que el servicio fail2ban está activo 3](#_Toc152178129)

[11. ¿Qué muestra sudo fail2ban-client status? ¡Explícalo! 4](#_Toc152178131)

[12. ¿Cuál es el archivo de configuración? Explica los parámetros: bantime y maxretry. 4](#_Toc152178132)

[13. ¿Cuál es el jail activado por defecto? (CAPTURA) 5](#_Toc152178134)

[14. Accede al fichero de logs. (CAPTURA) 5](#_Toc152178135)

[Ejercicio 1 6](#_Toc152178136)

[Ejercicio 2 7](#_Toc152178144)

[Ejercicio 3 7](#_Toc152178145)

## REQUISITOS PREVIOS

# Comprobar que ssh está instalado (o comprobar que esté instalado)

Texto

Descripción generada automáticamente

# Probar la conexión a través de ssh desde WIndows a Ubuntu Server (WinSCP, Putty..)

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

## PREGUNTAS CONTEXTUALES FAIL2BAN

# ¿Qué es un ataque de fuerza bruta?

Un ataque de fuerza bruta es un método en el que un atacante intenta descifrar una contraseña o clave mediante la prueba sistemática de todas las combinaciones posibles. Este enfoque es intensivo en recursos y lleva tiempo.

# ¿Para qué sirve y qué es FAIL2BAN?

Fail2Ban es una herramienta de prevención de intrusiones en servidores GNU/Linux, escrita en Python. Se utiliza para defender contra ataques de fuerza bruta en servicios abiertos al exterior.

# ¿Qué hace FAIL2BAN con el fichero de logs?

Fail2Ban monitoriza ficheros de logs, como /var/log/auth.log, en busca de intentos de acceso fallidos. Detecta patrones de autenticación incorrecta y toma medidas como bloquear la IP del atacante.

# ¿Qué son los jails?

Los "jails" en Fail2Ban son conjuntos de reglas y acciones específicas asociadas a cada servicio que se quiere proteger. Cada jail se configura para defender un servicio particular, como sshd o apache-auth.

# ¿Qué se puede hacer con FAIL2BAN?

Fail2Ban puede bloquear automáticamente las direcciones IP que superan el umbral de intentos de acceso fallidos, añadiendo reglas al cortafuegos. Aunque no es infalible, sirve como una importante primera línea de defensa contra ataques y puede trabajar en conjunto con otras medidas de seguridad.

## CONFIGURACIÓN FAIL2BAN

# Instala Fail2BAN en Ubuntu Server. (CAPTURA)

comand: sudo apt install fail2ban

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

# Habilita Fail2ban para que arranque automáticamente (CAPTURA)

# Comprobar que el servicio fail2ban está activo (CAPTURA)

Tras ejecutar el comando sudo systemctl enable fail2ban.service he reiniciado el servidor con reboot y despues he ejecutado sudo systemctl status fail2ban.service para comprobar que el Fail2ban estava arrancado.

Texto

Descripción generada automáticamente

## CARACTERÍSTICAS

# ¿Qué muestra sudo fail2ban-client status? ¡Explícalo! (CAPTURA)

Muestra el numero de jails que estan actualmente habilitados y el detalle de cada uno de ellos.

Diagrama

Descripción generada automáticamente

# ¿Cuál es el archivo de configuración? Explica los parámetros: bantime y maxretry. (CAPTURA)

Texto

Descripción generada automáticamente

# Texto Descripción generada automáticamente

El archivo de configuración es /etc/fail2ban/jail.conf.

- bantime es el numero de segundos que el host sea baneado

- maxretry es la cantidad de fallos antes de que se prohíba un host.

# ¿Cuál es el jail activado por defecto? (CAPTURA)

Por defecto, el unico jail que suele estar habilitado es el correspondiente al servicio sshd

Texto

Descripción generada automáticamente

# Accede al fichero de logs. (CAPTURA)

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

## Ejercicio 1

# Paso 1

# Interfaz de usuario gráfica, Texto Descripción generada automáticamente

# Paso 2



# Paso 3

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

# Paso 4



# Paso 5

Texto

Descripción generada automáticamente

# Paso 6



## Ejercicio 2

Texto

Descripción generada automáticamente

## Ejercicio 3

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente