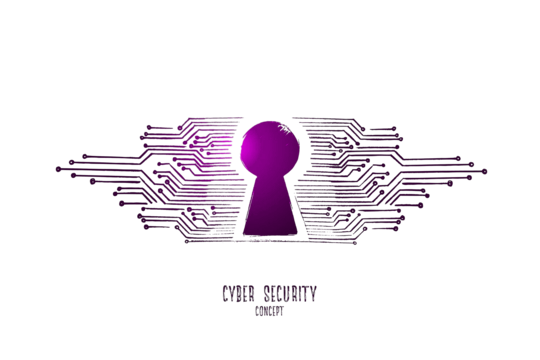
Bastionado de redes 

y sistemas.



**Protección contra intentos de accesos no autorizados y fuerza bruta**

**Francisco Iván Ramírez Ortega**

Curso 2023 - 2024

**IES El Rincón**

Curso de especialización en Ciberseguridad en entornos de las tecnologías de la información.

# Protección contra intentos de accesos no autorizados y fuerza bruta

# Introducción

Se instalará y configurará Fail2ban para proteger servidores de intentos de acceso no autorizados y ataques de fuerza bruta.

## ¿Que es [Fail2ban](https://github.com/fail2ban/fail2ban)?

Fail2Ban escanea archivos de registro como /var/log/auth.log y prohíbe las direcciones IP que realizan demasiados intentos fallidos de inicio de sesión. Lo hace actualizando las reglas del firewall del sistema para rechazar nuevas conexiones desde esas direcciones IP, durante un período de tiempo configurable. Fail2Ban viene listo para usar algunos archivos de registro estándar, como los de sshd y Apache. Es una opción gratuita para proteger frente a ataques de fuerza bruta. CrowSec sería una alternativa mejorada de pago.

### Características de Fail2Ban

## Herramientas

* Python 3.10^
* pip

## Glosario

**Cortafuegos**: sistema de seguridad que permite bloquear acceso no autorizados a un ordenador mientras permite sigue permitiendo la comunicación con otros servicio que si están autorizados.

* **Expresiones regulares**: son patrones utilizados para encontrar una determinada combinación de caracteres en un cadena texto.
* **Log** : son una grabación secuencial en un archivo o una base de datos de todos los acontecimientos que afectan a un proceso en particular ya sea una aplicación o algún servicio etc

| Instalación |
| --- |
| Linux → **sudo apt install fail2ban** |
|  |
|  |
|  |
|  |
|  |

# Bibliografía