使用 Fail2Ban 自動阻擋攻擊者

```
vi /etc/fail2ban/jail.local
```

加入

```
[nginx-http-auth]
enabled  = true
filter   = nginx-http-auth
action   = iptables[name=HTTP, port=http, protocol=tcp]
logpath  = /var/log/nginx/error.log
bantime  = 3600
findtime = 600
maxretry = 5
```

重新啟動服務

```
systemctl restart fail2ban
```

檢查當前被封的 IP

```
fail2ban-client status
```

額外再加入

```
[nginx-primary-script]
enabled = true
filter = nginx-primary-script
action = iptables[name=PrimaryScript, port=http, protocol=tcp]
logpath = /var/log/nginx/error.log
maxretry = 3
bantime = 3600
```

防止攻擊腳本

```
[Definition]
failregex = .*FastCGI sent in stderr: "Primary script unknown".*request: ".*installer\.php.*
            .*FastCGI sent in stderr: "Primary script unknown".*request: ".*WordPress/installer\.php.*
```

```
        .*FastCGI sent in stderr: "Primary script unknown".*request: ".*phpinfo\.php.*
        .*FastCGI sent in stderr: "Primary script unknown".*request: ".*info\.php.*

# 常見入侵腳本和工具
        .*GET /wp-admin.*                  # WordPress 管理面板攻擊
        .*GET /wp-login\.php.*             # WordPress 登錄攻擊
        .*GET /xmlrpc\.php.*               # WordPress XML-RPC 攻擊
        .*GET /phpMyAdmin/.*               # phpMyAdmin 攻擊
        .*GET /pma/.*                      # phpMyAdmin 縮寫攻擊
        .*GET /myadmin/.*                  # 其他管理工具探測
        .*GET /config\.php.*               # 嘗試訪問配置文件
        .*GET /setup\.php.*                # 安裝腳本
        .*GET /install\.php.*              # 安裝腳本
        .*GET /adminer.*                   # Adminer 攻擊

# 常見惡意腳本探測
        .*GET /shell\.php.*                # 後門探測
        .*GET /cmd\.php.*                  # 命令執行腳本
        .*GET /console\.php.*              # 惡意工具腳本
        .*GET /backdoor\.php.*             # 後門腳本探測
        .*GET /wp-content/uploads/shell.*  # WordPress 上傳漏洞
        .*GET /eval-stdin.*                # eval 利用腳本

# 文件探測攻擊
        .*GET /\.env.*                     # Laravel 或其他框架配置文件
        .*GET /\.git/config.*              # Git 配置文件
        .*GET /backup.*                    # 嘗試下載備份
        .*GET /dump.*                      # 嘗試訪問數據庫轉儲
        .*GET /debug.*                     # 調試工具
        .*GET /error_log.*                 # 日誌檔案

# 特定漏洞利用
        .*GET /HNAP1/.*                    # HNAP 協議漏洞 (常針對路由器)
        .*GET /boaform/admin/formLogin.*   # IOT 設備漏洞
        .*GET /invoker/JMXInvokerServlet.* # JBoss 漏洞
        .*GET /webdav.*                    # WebDAV 攻擊
        .*GET /manager/html.*              # Tomcat 管理界面探測
```

直接封某個 IP

```
fail2ban-client set nginx-primary-script banip xxx.xxx.xxx.xxx
```

如果封錯想解除

```
fail2ban-client set nginx-primary-script unbanip 192.168.1.100
```

白名單　　寫在　/etc/fail2ban/jail.local

```
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1 192.168.1.100
```

做完任何設定都要記得重啟

```
systemctl restart fail2ban
```

修訂版本　　#4
由 tainan 建立於　26 十一月　2024 08:23:57
由 tainan 更新於　27 十一月　2024 07:39:13