

資安相關

- [【Linux】禁止密碼登入\(使用金鑰\)](#)
- [【shell】deny_hack_ip.sh](#)
- [資安相關連結](#)
- [資安新聞](#)
- [Citrix 進行特定 User-Agent 的阻擋](#)

【Linux】禁止密碼登入(使用金鑰)

修改 /etc/ssh/sshd_config

```
vim /etc/ssh/sshd_config

## 修改 PubkeyAuthentication

PubkeyAuthentication yes
#使用 ssh key 登入
PasswordAuthentication no
#禁止密碼登入
```

重啟 ssh 服務

```
sudo systemctl restart sshd.service
```

【shell】 deny_hack_ip.sh

簡單阻擋 try 帳號 ip

```
#!/bin/bash
#cat /var/log/secure|awk '/Failed/{print $(NF-3)}'|sort|uniq -c|awk '{print $2="$1;}" > /root/block.txt
cat /var/log/secure|awk '/Invalid user/{print $(NF-2)}'|sort|uniq -c|awk '{print $2="$1;}" > /root/block.txt
DEFINE="10"
for i in `cat /root/block.txt`
do
    IP=`echo | awk '{split("'"${i}"'", array, "=");print array[1]}``
    NUM=`echo | awk '{split("'"${i}"'", array, "=");print array[2]}``
    if [ $NUM -gt $DEFINE ];then
        grep $IP /etc/hosts.deny > /dev/null
        if [ $? -gt 0 ];then
            echo "sshd:${IP}:deny" >> /etc/hosts.deny
        fi
    fi
done
```

資安相關連結

[Shodan Search Engine](#)

<https://1drv.ms/u/s!AjL3yZaMi0Bcgqs4uUcmVz3R78oRPQ?e=3d7QhG>

資安新聞

新聞網站名稱	RSS URL	新聞週報參考性	備註
iThome 資安頻道	https://www.ithome.com.tw/rss/security	主要來源	臺灣最大資安新聞
TWCERT/CC	https://www.twcert.org.tw/tw/rss-104-1.xml	主要來源	臺灣電腦網路危機處理技協調中心 著重於臺灣發生或是可能影響臺灣的資安事件新聞
資安趨勢部落格	http://blog.trendmicro.com.tw/?feed=rss2	主要來源	有每週資安新聞彙整
The Hacker News	http://thehackernews.com/feeds/posts/default	參考來源	
FreeBuf	http://www.freebuf.com/feed	參考來源 技術文章	有每日資安新聞彙整 有許多技術文章可以看來增進自己的技術知識
技服中心	http://www.nccst.nat.gov.tw/Services/FeedService.svc/GetFeed?lang=zh&category=news&format=rss	主要來源	國家資通安全會報技術服務中心 認為重要的新聞
安全客-安全知識	https://rsshub.app/aqk/knowledge	技術文章	
安全客-有思想的安全新媒体	https://api.anquanke.com/data/v1/rss	參考來源	
技服中心-漏洞警訊	https://www.nccst.nat.gov.tw/Services/FeedService.svc/GetFeed?lang=zh&category=vulnerability&format=rss	參考來源	國家資通安全會報技術服務中心 所通報認為對台灣影響嚴重的漏洞警訊
F-ISAC	https://fisacs.tw （這不是RSS）	主要來源	金融資安資訊分享與分析中心

Citrix 進行特定 User-Agent 的阻擋

如果需要在 Citrix ADC 上針對特定網站（例如 `api.aaa.com`）進行特定 `User-Agent` 的阻擋，可以基於虛擬服務 (Virtual Server) 或 `Host` 標頭進行精確匹配。以下是詳細步驟：

方法 1：基於虛擬服務 (Virtual Server)

假設 `api.aaa.com` 綁定到一個特定的虛擬服務，則可以直接對該虛擬服務配置 Responder Policy 或 Rewrite Policy。

步驟

1. **找到虛擬服務**
 - 登入 Citrix ADC 管理界面。
 - 前往 **Traffic Management > Load Balancing > Virtual Servers**。
 - 找到綁定 `api.aaa.com` 的虛擬服務。
2. **創建 Responder Policy**
 - 前往 **AppExpert > Responder > Policies**。
 - 點擊 **Add**，輸入以下內容：
 - **Policy Name**：例如 `BlockUserAgentForAPI`。
 - **Rule**：

```
HTTP.REQ.HEADER("Host").EQ("api.aaa.com") && HTTP.REQ.HEADER("User-Agent").CONTAINS("某關鍵字")
```

- **Action**：選擇 **DROP** 或 **Redirect**（例如引導到一個錯誤頁）。
3. **綁定到虛擬服務**
 - 編輯對應的虛擬服務。
 - 在 **Responder Policies** 部分，綁定剛創建的 Policy。
 4. **測試效果**
 - 使用工具（如 `curl` 或 Postman），模擬包含匹配的 `User-Agent` 訪問 `api.aaa.com`，應該會被阻擋。

方法 2：基於 HTTP Host Header 的精確匹配

如果 `api.aaa.com` 與其他應用共享同一虛擬服務，可以基於 `Host` 標頭進行條件判斷。

步驟

1. **創建 Responder Policy**
 - 配置條件如下：

```
HTTP.REQ.HEADER("Host").EQ("api.aaa.com") && HTTP.REQ.HEADER("User-Agent").CONTAINS("某關鍵字")
```

- 動作可以設為：
 - **DROP**：直接丟棄請求。
 - **Redirect**：引導至一個錯誤頁面，例如：

```
HTTP.REQ.URL.SET_TEXT_MODE("http://error-page.yourdomain.com")
```

2. **綁定到虛擬服務**
 - 在對應虛擬服務的 **Policies** 區域進行綁定。
3. **測試效果**

方法 3：使用 Rewrite 改寫或拒絕請求

改寫方式

如果你不想丟棄請求，而是改變特定 `User-Agent` 的行為，可以用 Rewrite Policy 改寫請求，例如修改 `User-Agent` 為通用值或添加額外標頭：

1. **Rewrite Policy 條件**

```
HTTP.REQ.HEADER("Host").EQ("api.aaa.com") && HTTP.REQ.HEADER("User-Agent").CONTAINS("某關鍵字")
```

2. **Rewrite Action**

- 替換 `User-Agent`：

```
HTTP.REQ.HEADER("User-Agent").SET_TEXT("DefaultUserAgent")
```

- 添加自定義標頭：

```
HTTP.REQ.HEADER("X-Blocked").SET_TEXT("Blocked")
```

3. 綁定到虛擬服務

方法 4：使用 Application Firewall (更高級別保護)

若已啟用 Application Firewall，可基於 `Host` 和 `User-Agent` 配置策略：

1. 創建 Application Firewall Profile

- 添加一個自定義 Profile，啟用 **Signatures**。
- 創建自定義簽名：
 - 名稱：例如 `BlockUAForAPI`
 - 條件：

```
HTTP.REQ.HEADER("Host").EQ("api.aaa.com") && HTTP.REQ.HEADER("User-Agent").CONTAINS("某關鍵字")
```

2. 綁定 Profile 至虛擬服務

測試命令範例

可以使用以下命令測試效果：

```
curl -H "Host: api.aaa.com" -H "User-Agent: 特定關鍵字" http://<你的 ADC IP>/path
```

這將模擬請求，並確認是否阻擋成功。

如果有更多需求或複雜場景，可以提供更多細節，我將協助進一步優化配置！