ModSecurity

臺灣大學計資中心

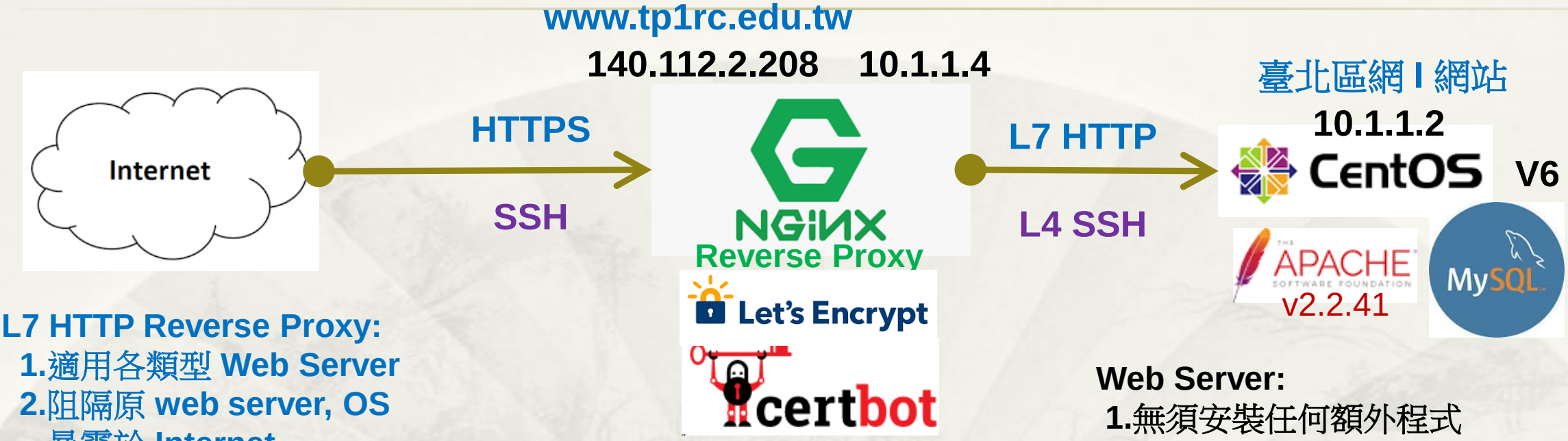
網路組

游子興

網頁攻擊事件

* 2022/08/02 美國國會議員裴洛西訪台
* 遭受對岸網軍進行**網頁置換攻擊**
* 區網首頁潛在風險
  * PHP + MySQL ：歷史悠久、維護人員更迭
  * 動態網頁：公佈欄、連線單位資訊資料庫
  * 網頁後台管理系統
* 解決方案
  * 純靜態網頁: 無後台管理功能、無動態程式功能
  * 公版網頁範本
  * **商用WAF: 經費有限**

區網網頁新架構



L7 HTTP Reverse Proxy:

1.適用各類型 Web Server
2.阻隔原 web server, OS 暴露於 Internet.
3.額外提供 Load Balance、Content Cache、WAF 功能.

L4 SSH Reverse Proxy:

1. SSH 遠端登入
2. sftp 異地備份

Let's Encrypt 免費憑證：

1.Certbot 安裝於NGINX，不影響原 Web Server
2.憑證到期自動 Renew
3.減輕後端 Web Server SSL/TLS 加解密 Loading
4.後端已解密封包可進行 IDS/IPS 流量分析

Web Server:

1.無須安裝任何額外程式
2.原 MRTG 服務(需內對外連線)，移至別台機器.
3.改用虛擬 IP，移除 Gateway IP 設定

※避免未知後門/木馬(如:Reverse Shell)持續運作.

區網網頁新架構

ModSecurity:

1.Open Source WAF Project

2.支援 Apache、IIS、NGINX 等網站伺服器

3.支援多種阻擋規則

(1)OWASP ModSecurity Core Rule Set

(2)Atomicorp's Free ModSecurity Rule

(3)Comodo Free ModSecurity Rules

(4)WordPress ModSecurity Rule Set (WPRS)

OWASP Core Rule Set(CRS)

OWASP 撰寫之阻擋規則

Docker 架構

1.跨平台相容

2,部署簡單快速

ModSecurity

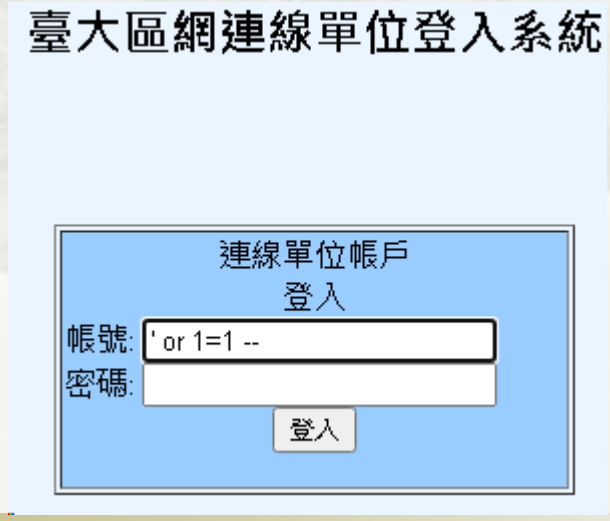
- Open Source Web Application Firewall(WAF) Project
  - Library that handles HTTP filtering
- 版本演進
  - v1.x Only for Apache Module
  - v2.x Support IIS and NGINX
  - v3.x Standalone Engine, Called “libModSecurity”.
    - no longer dependent on the Apache web server
    - 目前僅提供 CentOS 6/7, Amazon Linux 1/2, Ubuntu, Mac OSX 用 Source 安裝的方法。
    - 目前連接器(Connector)僅支援 NGINX

ModSecurity Rule Set

- OWASP ModSecurity Core Rule Set
  - https://coreruleset.org/
- Atomicorp's Free ModSecurity Rule
  - https://atomicorp.com/free-modsecurity-rules/
- Comodo Free ModSecurity Rules
  - https://modsecurity.comodo.com/
- WordPress ModSecurity Rule Set (WPRS)
  - https://github.com/Rev3rseSecurity/wordpress-modsecurity-ruleset

Command/SQL Injection
XSS 測試

- Command Injection
  - https://www.tp1rc.edu.tw/index.php?a=/bin/sh
- 連線單位登入系統、管理後台
  - https://www.tp1rc.edu.tw/https/data_sys/login.php
  - SQL Injection: ‘ or 1=1 --
  - XSS(Cross-Site Script): <script>alert(1)</script>



Web Shell Backdoor
測試

- https://github.com/backdoorhub/shell-backdoor-list
- Simple Shell
  - https://github.com/backdoorhub/shell-backdoor-list/raw/master/shell/php/simple-shell.php
  - 一句話木馬
    - <?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
- B374K Shell
  - https://github.com/backdoorhub/shell-backdoor-list/raw/master/shell/php/b374k.php

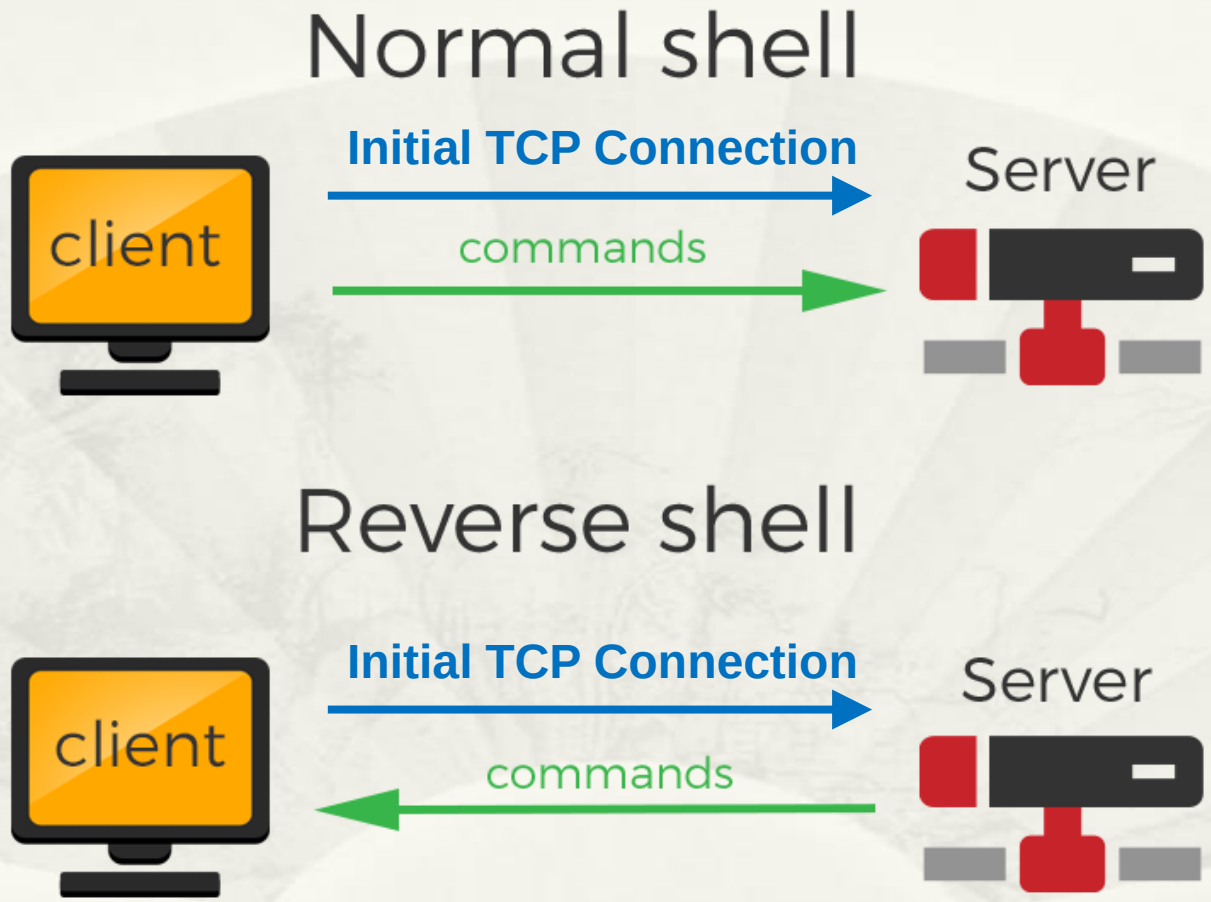
Simple Shell
一句話木馬

* 有效阻擋
  * http://10.1.1.2/https/simple-shell.php?cmd=cat+/etc/passwd
  * http://www.tp1rc.edu.tw/https/simple-shell.php?cmd=cat+/etc/passwd
* 阻擋無效
  * http://10.1.1.2/https/simple-shell.php?cmd=ls
  * http://www.tp1rc.edu.tw/https/simple-shell.php?cmd=ls

B374K Shell

* default password : b374k
* 可順利登入，但大部分功能無法運作
  * http://10.1.1.2/https/b374k.php
  * http://www.tp1rc.edu.tw/https/b374k.php

Reverse Shell
測試



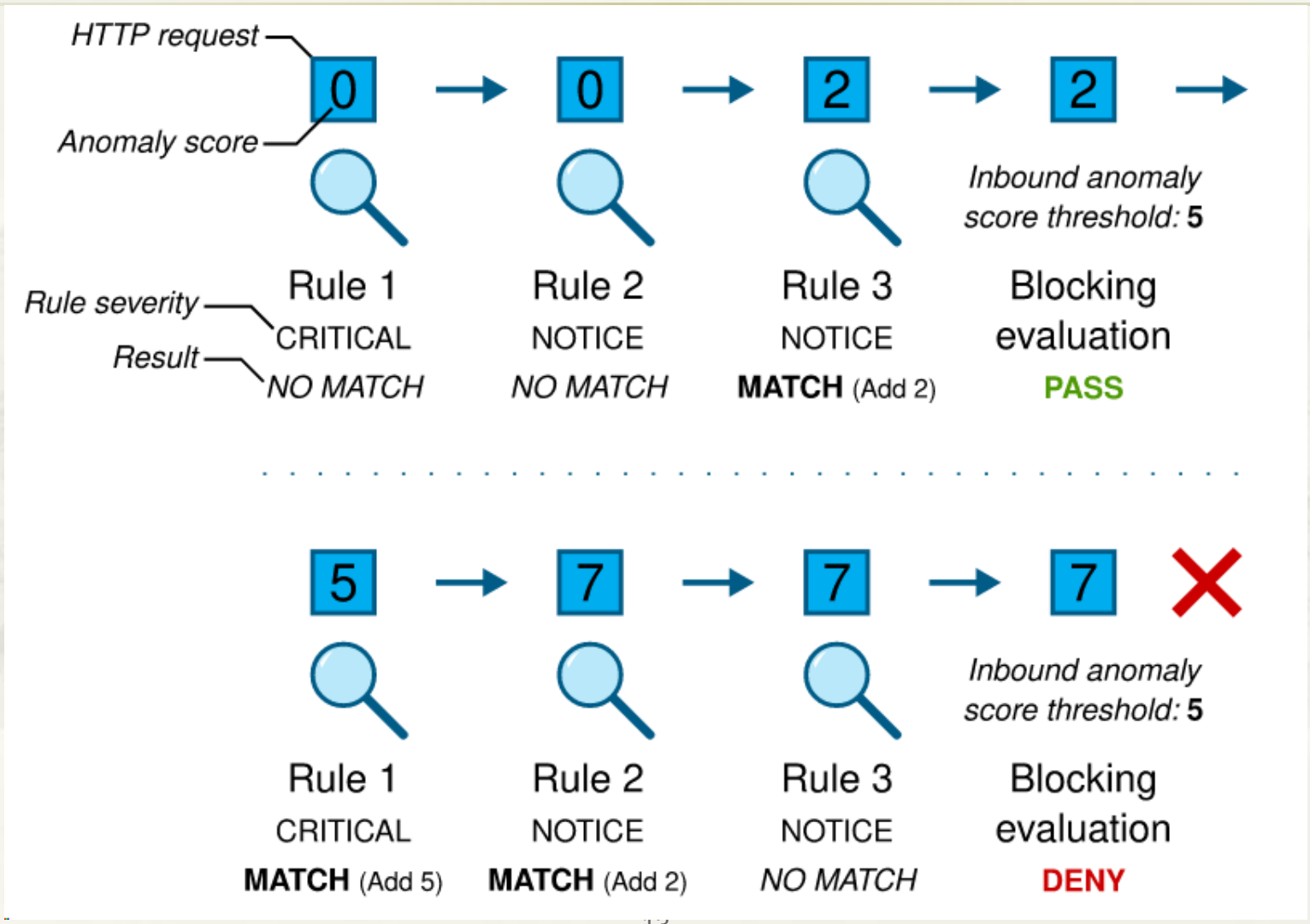
圖片來源: https://medium.com/@rietesh/python-reverse-shell-hack-your-neighbours-552561336ca8

區網 Web Server

- 使用虛擬 IP 且無內對外連線 Internet 需求
- 建議移除 Gateway IP 設定
  - 無法連線 Internet，可避免後門程式(如:Reverse Shell) 繼續運作

```
[root@tp1rc ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.1.1.0        *               255.255.255.0   U     0      0        0 eth0
link-local      *               255.255.0.0     U     1002   0        0 eth0
[root@tp1rc ~]# ping 8.8.8.8
connect: Network is unreachable
```

OWASP Core Rule Set(CRS)



OWASP Core Rule Set(CRS)

* Severity Level

Severity Level	Default Anomaly Score
CRITICAL	5
ERROR	4
WARNING	3
NOTICE	2

簡報完畢
謝謝