Speedrun!
傳送到 Linux 賜福處的最短攻擊路徑！

CYCRAFT

whoami

- 小趴 / freetsubasa
- 法環白金玩家，最近在成為白笛的路上
- 貓奴 / 遊戲宅 / 我有 PS5 我超強
- 目前為奧義智慧科技的資安研究員

Agenda

- 攻擊！
  - 常見進入 Linux 系統的管道
  - 試圖提權
  - 橫向移動
  - 掌握權力
- 防禦！
  - SELinux/AppArmor
  - Rookit 的調查
- 重建家園

攻擊！水鳥亂舞！

如何進入一台 Linux Server

作業系統漏洞

第三方套件漏洞

服務伺服器漏洞

前端安全

Web 框架漏洞

Web 框架漏洞

- ThinkPHP RCE
  - 最近大量衛服部釣魚網站利用此框架架設
- Wordpress RCE
  - plugin 百百種，總是會有讓你被打進去的那一種

套件服務漏洞 - shellsock

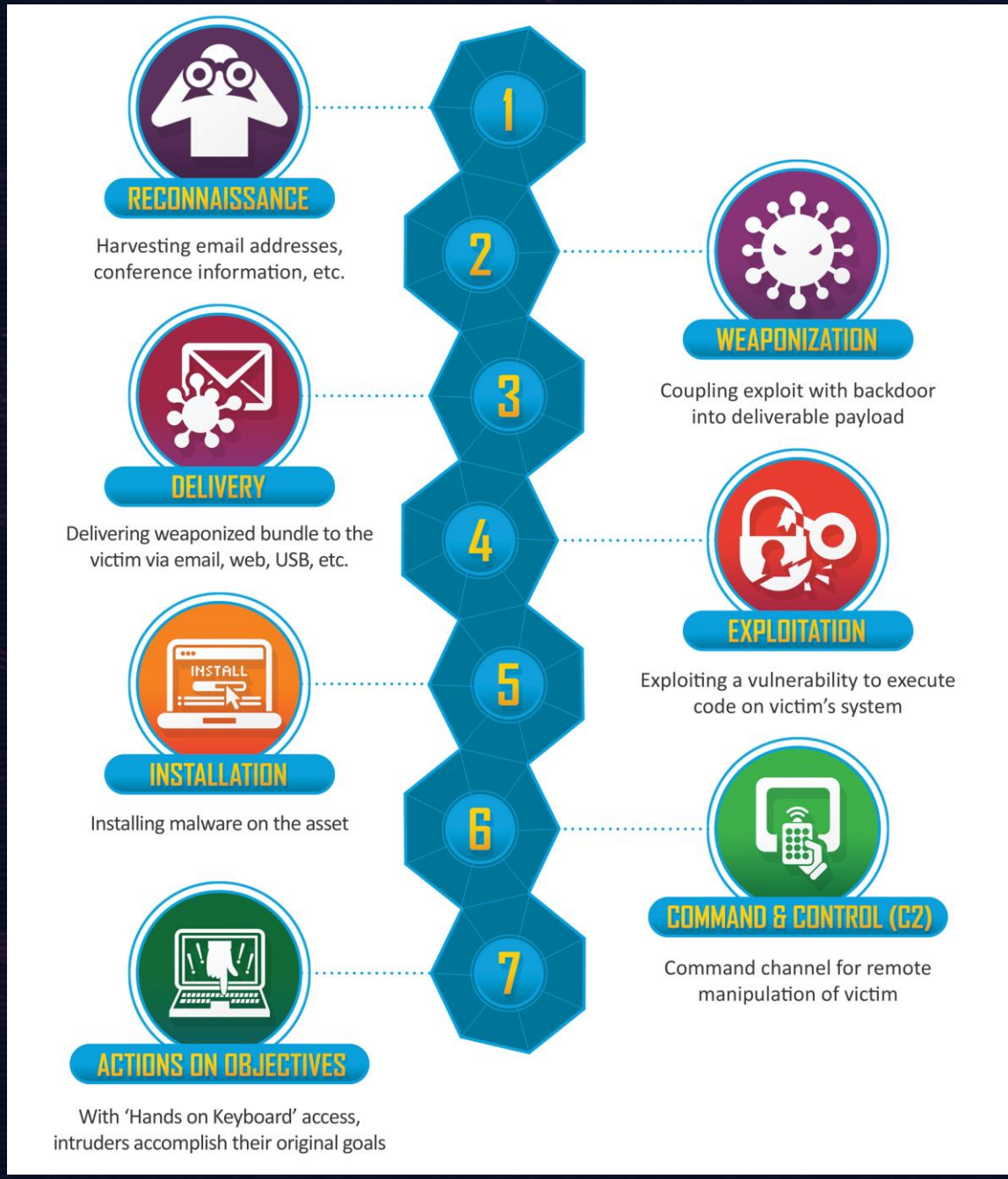
- 攻擊語法簡單，只要一行指令，就能對系統進行操作
- 範圍廣大，bash 為多款作業系統預設 shell
  - 例如 CentOS、Fedora、RHEL

```
() { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'
```

然後呢？
可以成為艾爾登之王了嗎？

那我們可以做些什麼？

- 提權
- 獲取機敏資訊
- 橫向移動
- 權限維持
- 清理痕跡
- 或是更多你想做的



Linux Kill Chain

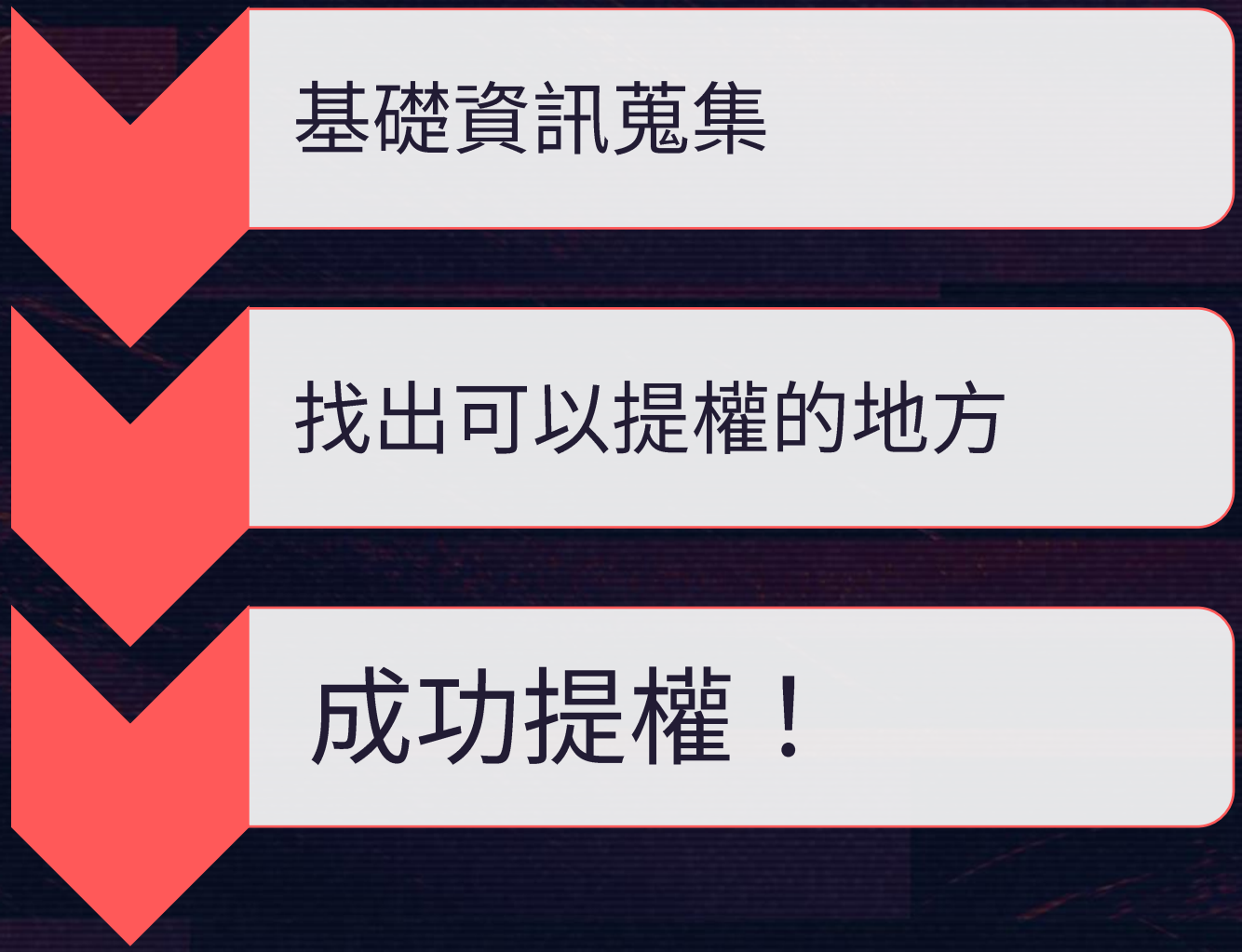
- 一開始取得的帳號通常是低權限，需透過攻擊手法提升權限來達成目標，盡可能擴張控制範圍，最終抵達目標機器進行計畫

Linux Kill Chain

- 先講提權！

如何提權

- Linux Kernel 提權
- 第三方服務提權
- 密碼收集提權
- 環境變量提權
- suid 提權
- sudo 提權
- 配置錯誤提權



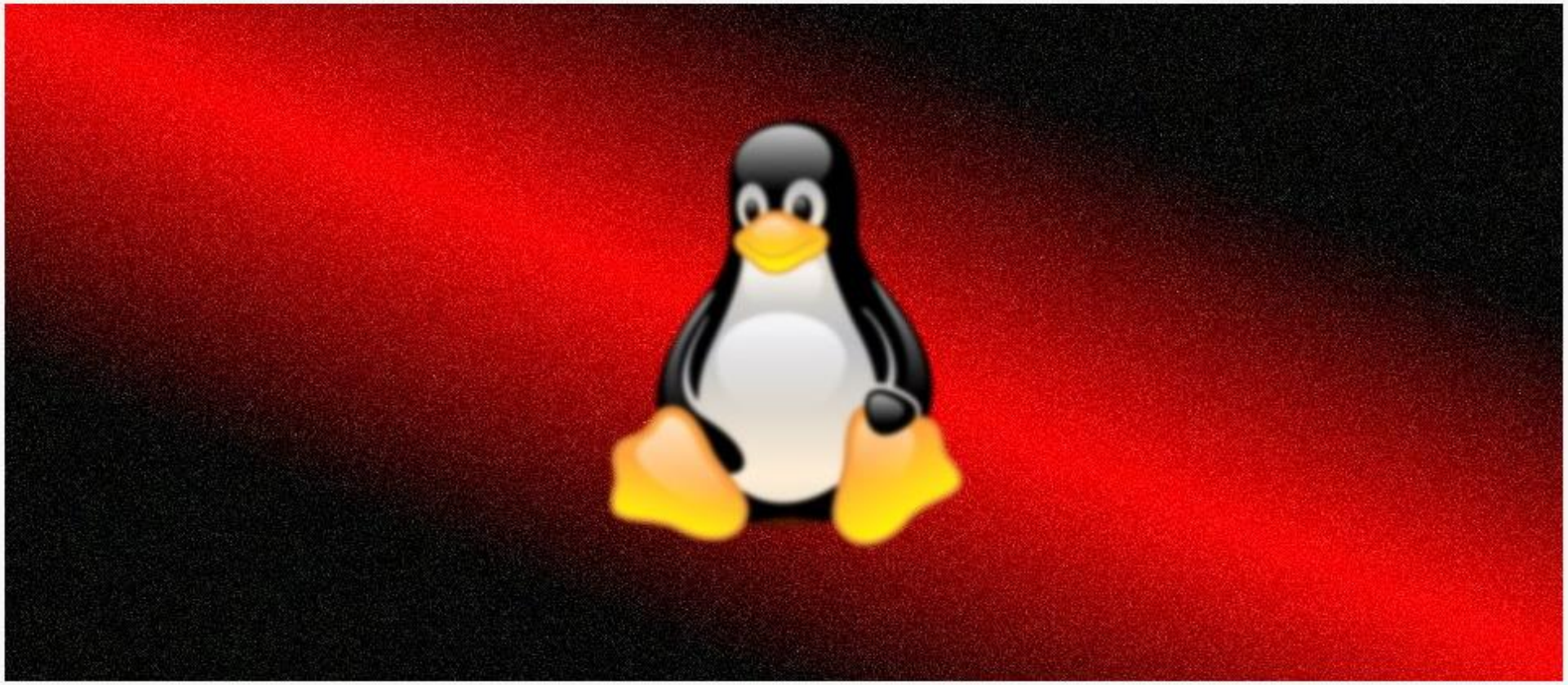
Linux Kernel 提權

- kernel 提權有機會會造成伺服器當機重開，謹慎使用
- kernel 通殺漏洞較為少見
  - 但管理者可能較少會去升級 kernel，有些較為古老的漏洞仍有機會
- 懶人用法：搭配 kali 自帶的 SearchSploit 搜尋相關漏洞

Linux漏洞Dirty Pipe波及Linux核心5.8以及之後的所有版本

針對藏匿於Linux核心的CVE-2022-0847，官方於2月23日釋出Linux 5.16.11、5.15.25及5.10.102以完成修補，同樣受到這項漏洞波及的Android，Google也在2月24日將修補程式併入Android核心

文/ 陳曉莉 | 2022-03-08 發表



一名軟體工程師Max Kellermann本周揭露了一個藏匿於Linux核心的安全漏洞CVE-2022-0847，該漏洞允許駭客覆蓋任何唯讀檔案，由於它牽涉到行程間通訊機制Pipe，使得Kellermann把它稱為Dirty Pipe漏洞，並說它比2016年出現的

Linux Kernel 提權 - Dirty Pipe

- 是個權限擴張漏洞，不是直接的權限提升
- 但我們可以將資料寫入只有 root 才可以改動的檔案

是不是有點想法了？

Linux Kernel 提權 - Dirty Pipe

- 既然我們有 root 權限改檔案，那我們直接改 root 密碼！
  - 但改完之後記得再把原本的 passwd 檔案放回去 XD
- 或是找到其他 SUID 為 root 或是以 root 身分跑的程式
  - 我們可以想法 inject 並且複寫他們！

Sudo 提權 - CVE-2021-3156

- 只要能登入機器，就有機會可以得到 root 權限
- sudoedit -s 在處理 \ 結尾的時候出現問題，出現 heap overflow

套件提權 - PwnKit

- 號稱所有駭客夢寐以求的漏洞
  - 預設安裝
  - 自從 2009 年就存在至今
  - 即使背景沒有 polkit 相關程序進行也可以利用
- 幾乎通殺所有版本的 Linux 發行版
- 利用簡單！

小結一下

關於提權

- 能進入伺服器已經贏了一半
- 透過觀察伺服器上的服務，盡量進行資訊蒐集
- 套件、Kernel 漏洞有機會就可以嘗試，要注意是否會影響服務
- 提權方式不只上述幾種，還有各種奇技淫巧可以各種嘗試
- 追最新的漏洞發布，隨時都有機會可以得到 root！

橫向移動！獵犬步法！

AD 可以橫向移動
我們也可以嗎？

Linux Kill Chain

Linux 橫向移動

- 嘗試可以連線到哪些內網
- 內網 port 掃描
- SSH 帳密
  - 根據前面提權，我們是無法知道 root 本來的密碼的
  - 管理員可能就幾組密碼輪流
  - 可以擷取密碼 hash 嘗試爆破
  - 利用 strace 監聽 ssh 登入服務嘗試得到密碼

Linux 橫向移動 - SSH 部分

- 私鑰洩漏，利用指令搜尋私鑰
- 得到私鑰後根據以下文件找到對應的伺服器連線
  - /etc/hosts
  - /etc/ssh/ssh_config
  - ~/.known_hosts
  - ~/.bash_history
  - ~/.ssh/config

Linux 橫向移動 - SSH 部分

- 如果只有密碼 hash 呢？
- 可以試試看 John the rapper 或是 hashcat 等工具爆破密碼

小結一下

關於橫向移動

- 能做的事情還是很多！
- 確認這台機器能連去哪個機器很重要
- 可以搜尋使用者有沒有存多把私鑰
- 如果可以最好能知道管理者的密碼
  - 不同的機器但同一個管理者可能會有相同密碼

持續掌握權限
那股力量正是成王的關鍵

Linux Kill Chain

隱藏

- 隱藏檔案
- 隱藏權限
- 隱藏操作紀錄
- 隱藏 port
- 隱藏 process

} 今天會著重在後面四個部分！

隱藏權限 – chatter

- 利用 chatter 這個指令達成隱藏權限的目的

```
papa@papa:/tmp/cybertest$ touch a.php
papa@papa:/tmp/cybertest$ ls -all
total 8
drwxrwxr-x  2 papa papa 4096 Sep 13 20:49 .
drwxrwxrwt 13 root root 4096 Sep 13 20:50 ..
-rw-rw-r--  1 papa papa    0 Sep 13 20:50 a.php
papa@papa:/tmp/cybertest$ sudo chattr +i a.php
papa@papa:/tmp/cybertest$ ls -all
total 8
drwxrwxr-x  2 papa papa 4096 Sep 13 20:49 .
drwxrwxrwt 13 root root 4096 Sep 13 20:51 ..
-rw-rw-r--  1 papa papa    0 Sep 13 20:50 a.php
papa@papa:/tmp/cybertest$ rm -rf a.php
rm: cannot remove 'a.php': Operation not permitted
papa@papa:/tmp/cybertest$
```

隱藏操作紀錄 – space

- 開啟 shell 的隱藏模式！
  - [space]set +o history
  - 這個命令後就再也不會記錄，包含這的指令
- 想只刪除特定關鍵字
  - history | grep "keyword“
  - 搭配 history -d 一起服用

隱藏 port

- 網管可能會利用 netstat 等等工具檢查
- 我們可以使用各種工具來隱藏我們連回機器的 port
- SSLH
  - 可以讓 https 與 ssh 公用同一個 port
- iptables
  - 利用 rule 達成 port 的重複使用

隱藏 process

- 總不能讓網管一查 ps aux process 就被發現
- 總是會有隱藏 process 的辦法
- 靠工具 libprocesshider
  - 透過 ld_preload 載入預先邊好的 library

既然都這樣了還是我們直接放個 rootkit？！

什麼是 Rootkit

- 有分成兩種 user mode 跟 kernel mode
- rootkit 三要素：隱藏、操縱、收集數據
- 本身不會像病毒或蠕蟲那樣影響伺服器
- 類似悄悄潛伏在機器裡的間諜，會偷偷回傳資料給我們
- 這種類型的攻擊通常不會觸發自動執行的網路安全控制功能

Rootkit 介紹

> 以 Reptile 為例，大致功能會有前面提及的各種隱藏術

Features

- Give root to unprivileged users
- Hide files and directories
- Hide processes
- Hide himself
- Hide TCP/UDP connections
- Hidden boot persistence
- File content tampering
- Some obfuscation techniques
- ICMP/UDP/TCP port-knocking backdoor
- Full TTY/PTY shell with file transfer
- Client to handle Reptile Shell
- Shell connect back each X times (not default)

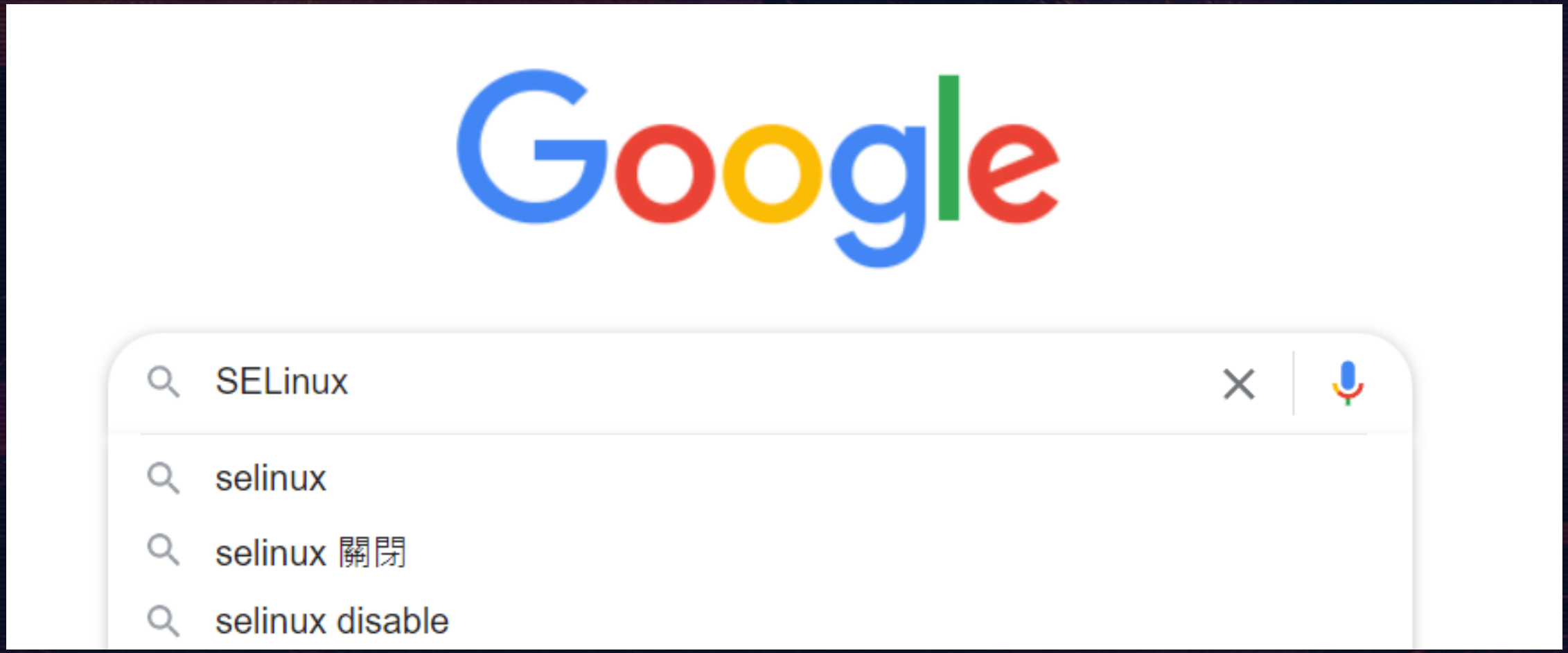
再來小結一下

關於持續使用

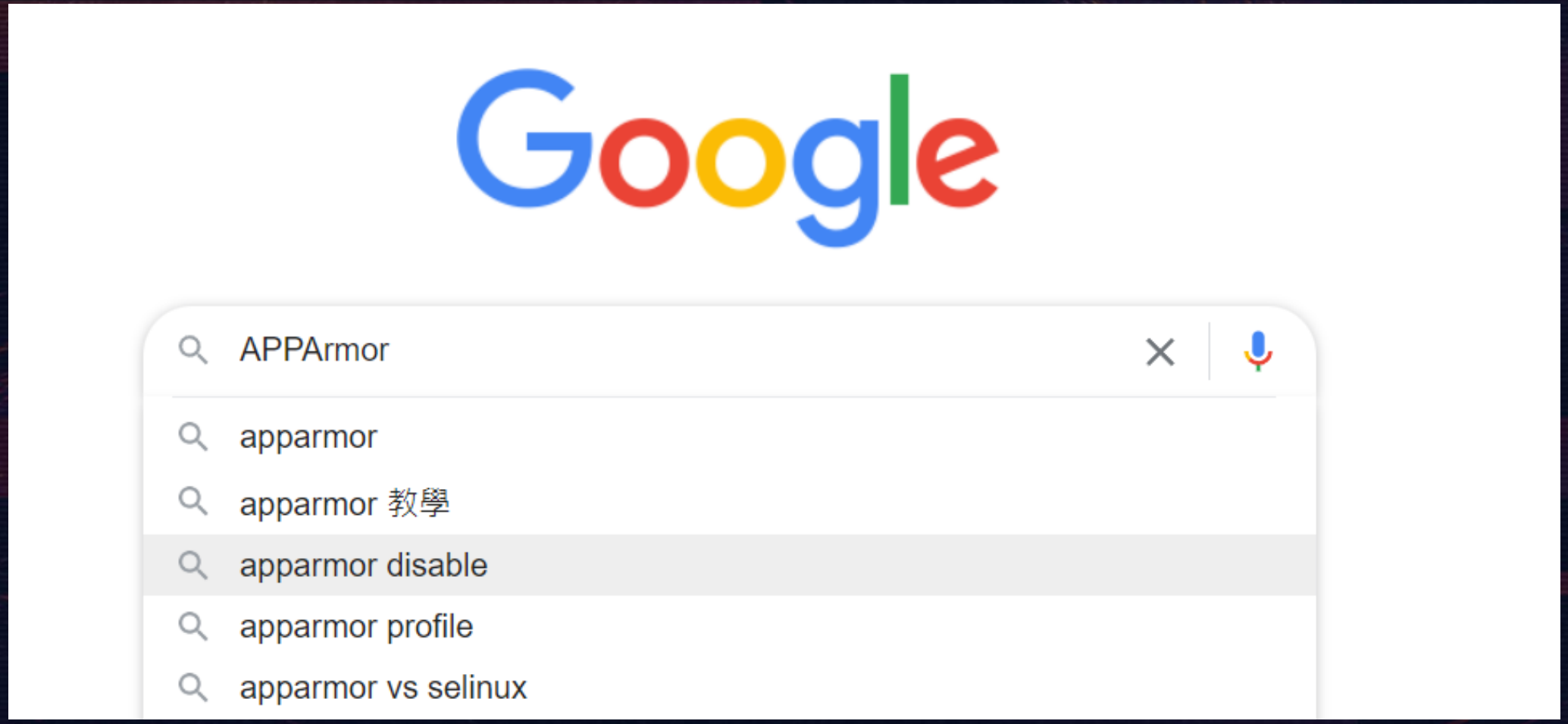
- 隱藏檔案 / process / port 的手法還有很多
- rootkit 的加入會讓管理員更難以發現你的行蹤

防禦！指紋石盾！

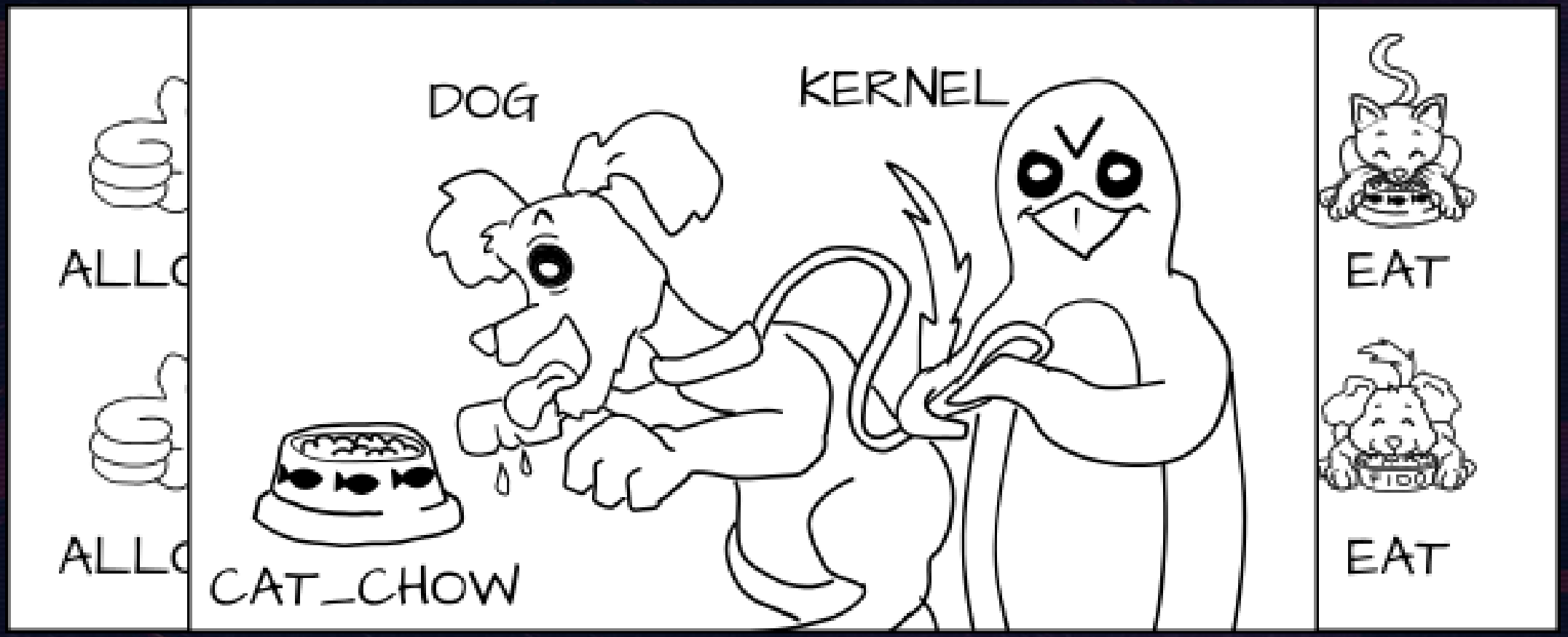
SELinux



AppArmor



SELinux



AppArmor

- 是 ubuntu 自帶的安全工具
- 可以限制、應用、控制檔案、目錄、網路的能力
- 有分兩種模式
  - enforcement 會完全遵照規則，格殺勿論
  - complain 只是對違反的行為進行 log 紀錄

那 rootkit 呢 ... ?

- 雖然很難，但還是有些辦法
- RKHunter
  - 檢查套件的 sha256 是否有變動
  - 檢查是否有常見的 rootkit 元件
  - 檢查是否有異常權限的文件
  - 檢查 kernel module 是否有奇怪的文字
  - 檢查隱藏檔案
- chkrootkit
  - 檢測常用的一些指令是否有被替換

再來小結一下

關於防禦

- SELinux 與 AppArmor 可增設規則，就算入侵也可以降低損傷
- 只要設定正確，他們也可以不用被關閉
- 定期的套件升級與確認安全性更新必不可少
- rootkit 雖然難防，但凡走過必留下痕跡，法網恢恢疏而不漏
  - 注意連線狀態
  - 注意隱藏的檔案
  - 應該要可以刪掉卻刪除不了的檔案
  - 利用工具確認常用指令使否已被 inject

重建家園！修復法環！

重建的第一步 - 確認損失範圍

- 調查駭客是從哪裡入侵的
  - 調查網頁 log、防火牆資訊、服務伺服器 log
- 駭客入侵後做了什麼？
  - 查 bash_history 等等確認災害範圍
  - 如果沒有 bash 歷史資料就查其他地方的 log

重建的第二步 – 修復城牆

- 套件問題請升級
- 密碼問題請更新新密碼，並保持一定的密碼強度
- 網頁前端的各種漏洞也需要一一修復

重建的第三步 – 清理家園

- 利用 chkrootkit 等服務確認是否還有遺留的檔案

```
papa@papa:/tmp/cybertest$ sudo chkrootkit
ROOTDIR is '/'
Checking 'amd'...                                           not found
Checking 'basename'...                                      not infected
Checking 'biff'...                                          not found
Checking 'chfn'...                                          not infected
Checking 'chsh'...                                          not infected
Checking 'cron'...                                          not infected
Checking 'crontab'...                                       not infected
Checking 'date'...                                          not infected
Checking 'du'...                                            not infected
Checking 'dirname'...                                       not infected
Checking 'echo'...                                          not infected
Checking 'egrep'...                                         not infected
Checking 'env'...                                           not infected
Checking 'find'...                                          not infected
Checking 'fingerd'...                                       not found
Checking 'gpm'...                                           not found
Checking 'grep'...                                          not infected
Checking 'hdparm'...                                        not infected
Checking 'su'...                                            not infected
Checking 'ifconfig'...                                      not infected
Checking 'inetd'...                                         not infected
Checking 'inetdconf'...                                     not found
Checking 'identd'...                                        not found
Checking 'init'...                                          not infected
```

重建的第三步 – 清理家園

- 利用 RKHunter 確認常被 inject 的執行檔案室否正常

```
Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                               [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                        [ None foun
    Checking for preloaded libraries                         [ None foun
    Checking LD_LIBRARY_PATH variable                        [ Not found

  Performing file properties checks
    Checking for prerequisites                               [ OK ]
    /usr/sbin/adduser                                        [ OK ]
    /usr/sbin/chroot                                         [ OK ]
    /usr/sbin/cron                                           [ OK ]
    /usr/sbin/depmod                                         [ OK ]
    /usr/sbin/fsck                                           [ OK ]
    /usr/sbin/groupadd                                       [ OK ]
    /usr/sbin/groupdel                                       [ OK ]
    /usr/sbin/groupmod                                       [ OK ]
    /usr/sbin/grpck                                          [ OK ]
    /usr/sbin/ifconfig                                       [ OK ]
    /usr/sbin/init                                           [ OK ]
    /usr/sbin/insmod                                         [ OK ]
    /usr/sbin/ip                                             [ OK ]
    /usr/sbin/lsmod                                          [ OK ]
    /usr/sbin/modinfo                                        [ OK ]
    /usr/sbin/modprobe                                       [ OK ]
    /usr/sbin/nologin                                        [ OK ]
    /usr/sbin/pwck                                           [ OK ]
    /usr/sbin/rmmod                                          [ OK ]
    /usr/sbin/route                                          [ OK ]
    /usr/sbin/rsyslogd                                       [ OK ]
    /usr/sbin/runlevel                                       [ OK ]
    /usr/sbin/sshd                                           [ OK ]
    /usr/sbin/sulogin                                        [ OK ]
    /usr/sbin/sysctl                                         [ OK ]
    /usr/sbin/useradd                                        [ OK ]
```

再來小結一下

關於修復

- 破壞總是比建造快，需要耐心去找駭客粗心留下的線索
- 先確認損害範圍，以利找出修補方式
- 如果不幸被放 rootkit 還是可以嘗試刪除留下來的 payload
- 多注意是否有可疑的連線
  - 不管是對外網或是內網

恭喜成為新的艾爾登之王

我們可以做些什麼

- 伺服器定期升級系統，確認服務是否有安全性更新
- 確認帳號權限，維持最小權限原則
- 密碼常保更新，且盡量善用密碼片語及 MFA 機制
- SELinux/AppArmor 可以學習基本設定，降低被入侵後的風險
- 隨時監控系統執行檔是否有變化，有的話可能有被放 rootkit
- 災後復原之路通常道阻且長，平時應多加注意伺服器狀況