

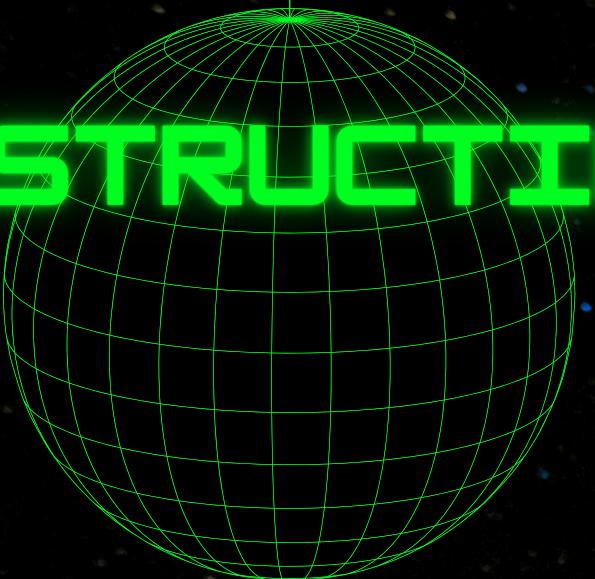


**SS/US**

Twin Evil

**BONUS >**

## INSTRUCTION



Nell'azienda Theta, sono state installate delle lampadine IoT per migliorare l'efficienza energetica e l'automazione degli uffici. Tuttavia, un abile attaccante ha sfruttato una tecnica sofisticata chiamata "Twin Evil" per ottenere accesso non autorizzato alla rete aziendale.

L'intruso ha lasciato un messaggio inquietante: "Ya airgeddoned!" su ogni server e client, compromettendo la sicurezza di tutta l'infrastruttura digitale di Theta.

# STUPIDE LAMPADINE!



Gli attaccanti hanno sfruttato la tecnica "Twin Evil" per ottenere accesso non autorizzato alla rete tramite lampadine IoT. Il messaggio "Ya airgeddoned!" fa riferimento all'uso del tool Airgeddon.

Da questo messaggio sappiamo che l'attacco ha coinvolto tecniche sofisticate di penetration testing. La nostra missione è investigare a fondo su questo attacco.

# LET'S TOUCH BASES

Illustriamo all'azienda Theta, evidentemente a digiuno di nozioni basilari, i principi di una connessione WiFi; Nonostante le misure di sicurezza, le reti Wi-Fi possono essere vulnerabili a diversi tipi di attacchi, come:

## Evil Twin

*Un attacco in cui un malintenzionato crea un access point falso con lo stesso SSID di uno legittimo.*

## Deauth Attack

*Utilizzato per disconnettere forzatamente i dispositivi dalla rete, spesso preludio ad altri attacchi come Evil Twin.*

## Packet Sniffing

*La cattura e analisi del traffico di rete per ottenere informazioni sensibili.*

# INSICUREZZA ONDE RADIO



Nella serie tv Mr Robot, Elliot fa visita a Fernando Vera in prigione, portando con sé il suo telefono su cui ha installato un'app di scansione Wi-Fi. Con quello scanner, può vedere tutti gli AP wireless e vedere che sono tutti protetti con WPA2.

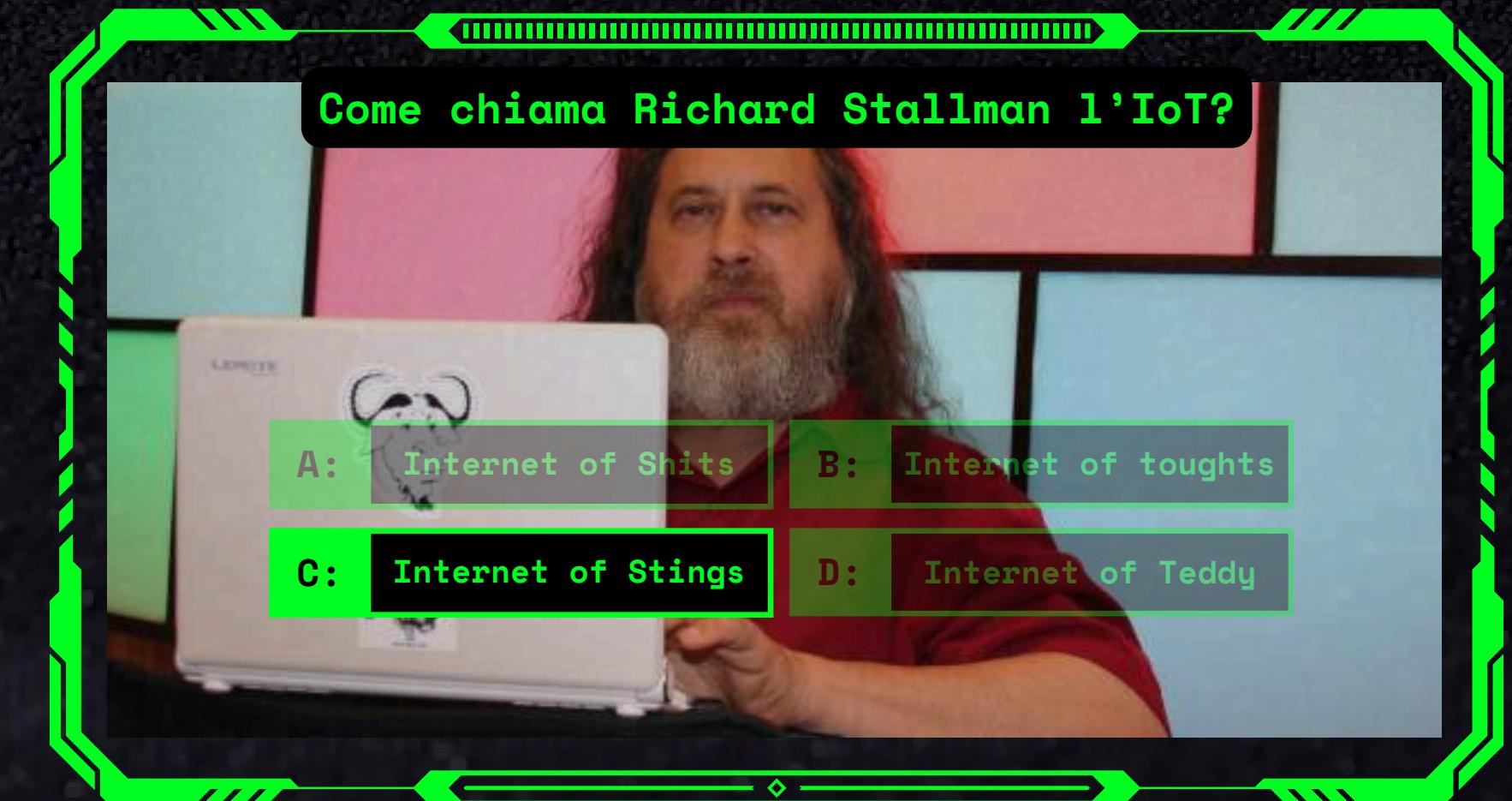
Sebbene sappia di poter violare WPA2, riconosce che il breve lasso di tempo con cui sta lavorando è inadeguato per forzare brute-force WPA2. La strategia di Elliot quindi, in questo caso è quella di falsificare la connessione Bluetooth dell'auto della polizia alla sua tastiera.

Con l'avvento dell'IoT (Internet of Things) la situazione è letteralmente sfuggita di mano. Con miliardi di dispositivi connessi, dai frigoriferi alle lampadine, la superficie di attacco per i malintenzionati è aumentata esponenzialmente.

Questo ha reso il bisogno di sicurezza più urgente che mai. Come sottolinea Stallman, l'IoT può trasformarsi in una trappola di vulnerabilità se non si adottano misure di sicurezza adeguate. La realtà è che ogni dispositivo connesso rappresenta un potenziale punto di ingresso per gli attaccanti, e quindi la protezione di questi sistemi è diventata una priorità assoluta.

Come chiama Richard Stallman l'IoT?

- A: Internet of Shits
- B: Internet of tougths
- C: Internet of Stings
- D: Internet of Teddy



# HOW TO CRACK 101

PER POTER ESEGUIRE ATTACCHI BASATI SU WIFI, SERVONO ADATTATORI WI-FI CHE SUPPORTINO REQUISITI FONDAMENTALI:

**CONTROLLO A  
BASSO LIVELLO:**

**MODALITA' MONITOR  
E INJECTION:**

Gli hacker necessitano di adattatori Wi-Fi particolari, poiché quelli comuni non permettono il controllo a basso livello richiesto per attacchi sofisticati.

Questi adattatori devono supportare modalità monitor e injection per catturare tutti i pacchetti di rete e inviare pacchetti manipolati.

# HOW TO HACK 101

PER POTER ESEGUIRE ATTACCHI BASATI SU WIFI, SERVONO ADATTATORI WI-FI CHE SUPPORTINO REQUISITI FONDAMENTALI:

## CHIPSET PREFERITI:

I chipset Atheros e Realtek sono frequentemente scelti per queste capacità avanzate.

## COMPATIBILITA' SOFTWARE:

Devono essere compatibili con software di attacco come Aircrack-ng e Airgeddon, utilizzati su sistemi operativi come Linux.

# HOW TO HACK 101

PER POTER ESEGUIRE ATTACCHI BASATI SU WIFI, SERVONO ADATTATORI WI-FI CHE SUPPORTINO REQUISITI FONDAMENTALI:

## PRODUTTORI SPECIALIZZATI :

- Aziende come Hak5 producono hardware specifico, come le famose Wi-Fi Pineapple, utilizzate anche da blackhats.

- Link utili: [Hak5 Shop](#) e [Wi-Fi Pineapple](#)

## COMPATIBILITA' SOFTWARE:

- Alcuni hacker preferiscono auto-costruirsi questi dispositivi con l'ausilio di mini-board come i Raspberry Pi o dispositivi come il Flipper Zero per la loro versatilità.
- Link: [Flipper Zero](#)



# HOW TO HACK 101

PER POTER ESEGUIRE ATTACCHI BASATI SU WIFI, SERVONO ADATTATORI WI-FI CHE SUPPORTINO REQUISITI FONDAMENTALI:

## List Chipset Adatti:

- Per una lista esaustiva dei chipset adatti, consultare il sito di Aircrack.
- Link: [Aircrack Chipsets](#)

### What is the best wireless card to buy ?

Which card to purchase is a hard question to answer. Each person's criteria is somewhat different, such as one may require 802.11ax capability, or may require it to work via virtualization. However, having said that, then the following cards are considered the best in class:

- Alfa AWUS036AXML (a/b/g/n/ac/ax, WiFi 6E) is the best performing card, with a stable driver
- Alfa AWUS036AXM (a/b/g/n/ac/ax, WiFi 6E) has been reported as a bit less sensitive than the AWUS036AXML

#### Runner ups:

- Alfa AWUS036ACH (a/b/g/n/ac) is the best performing card, but the driver can be unstable enough to crash your kernel
- Alfa AWUS036ACM (a/b/g/n/ac) is the highest performing of the STABLE devices, but it requires kernel 4.19.5 or higher, and the driver doesn't work on the Raspberry Pi 3 yet; it works on the Raspberry Pi 4.

#### Older adapters:

- Alfa AWUS036H [b/g USB]
- Ubiquiti SRC [a/b/g Cardbus]
- Ubiquiti SRX [a/b/g ExpressCard]
- Airpcap series [USB]
- TP-Link TL-WNT722N v1 [b/g/n USB] - Beware, if version is not specified by vendor, it is NOT v1
- Alfa AWUS036NHA [b/g/n USB]
- Alfa AWUS051NH V2 [a/b/g/n USB]
- MiniPCIe: anything that uses [ath9k](#), especially AR92xx and AR93xx (ability to do [spectral scan](#))

Also read [this](#) first before purchasing. There are many available on the market for fairly low prices. You are simply trading off distance, sensitivity and performance for cost.

If you want to know if your existing card is compatible then use this page: [Tutorial: Is My Wireless Card Compatible?](#)

### What tutorials are available ?

The [Tutorials](#) page has many tutorials specific to the aircrack-ng suite. If your question is not answered

- How do I crack a static WEP key ?
- How many IVs are required to crack WEP ?
- How can I know what is the key length ?
- How do I know my WEP key is correct ?
- How can I crack a WPA-PSK network ?
- Where can I find good wordlists ?
- How do I recover my WEP/WPA key in windows ?
- Will WPA be cracked in the future ?
- How do I learn more about WPA/WPA2 ?
- How do I decrypt a capture file ?
- What are the authentication modes for WEP ?
- How do I merge multiple capture files ?
- Can I convert cap files to ivs files ?
- Can I use Wireshark/Ethereal to capture 802.11 packets ?
- Can Wireshark/Ethereal decode WEP or WPA data packets ?
- What are the different wireless filter expressions ?
- How do I change my card's MAC address ?
- Is my card compatible with airodump-ng / airoplay-ng ?
- Can I have multiple instance of airoplay-ng running at the same time ?
- How to use spaces, double quote and single quote, etc. in AP names ?
- What is the size of ARP packets ?
- How can I resolve MAC addresses to IP addresses ?

Users' rating	Gen	Chipset	Card/s using it	Band/s	Interface
😡	Wifi6e	Mediatek MT7921AUN	Alfa AWUS036AXML	2.4Ghz / 5Ghz / 6Ghz	USB
😡	Wifi6e	Mediatek MT7921AUN	Alfa AWUS036AXM	2.4Ghz / 5Ghz / 6Ghz	USB
😡	Wifi5	MediaTek MT7612U	Alfa AWUS036ACM	2.4Ghz / 5Ghz	USB

- [Wayland](#)
- [Consistent Network Device Naming](#)
  - [Kali Nethunter](#)
- [Essential Tools](#)
- [Optional Tools](#)
  - [BeEF Tips](#)
  - [Hashcat Tips](#)
  - [Bettercap Tips](#)
- [Update Tools](#)
- [Internal Tools](#)
- [Known Incompatibilities](#)

#### Getting Started

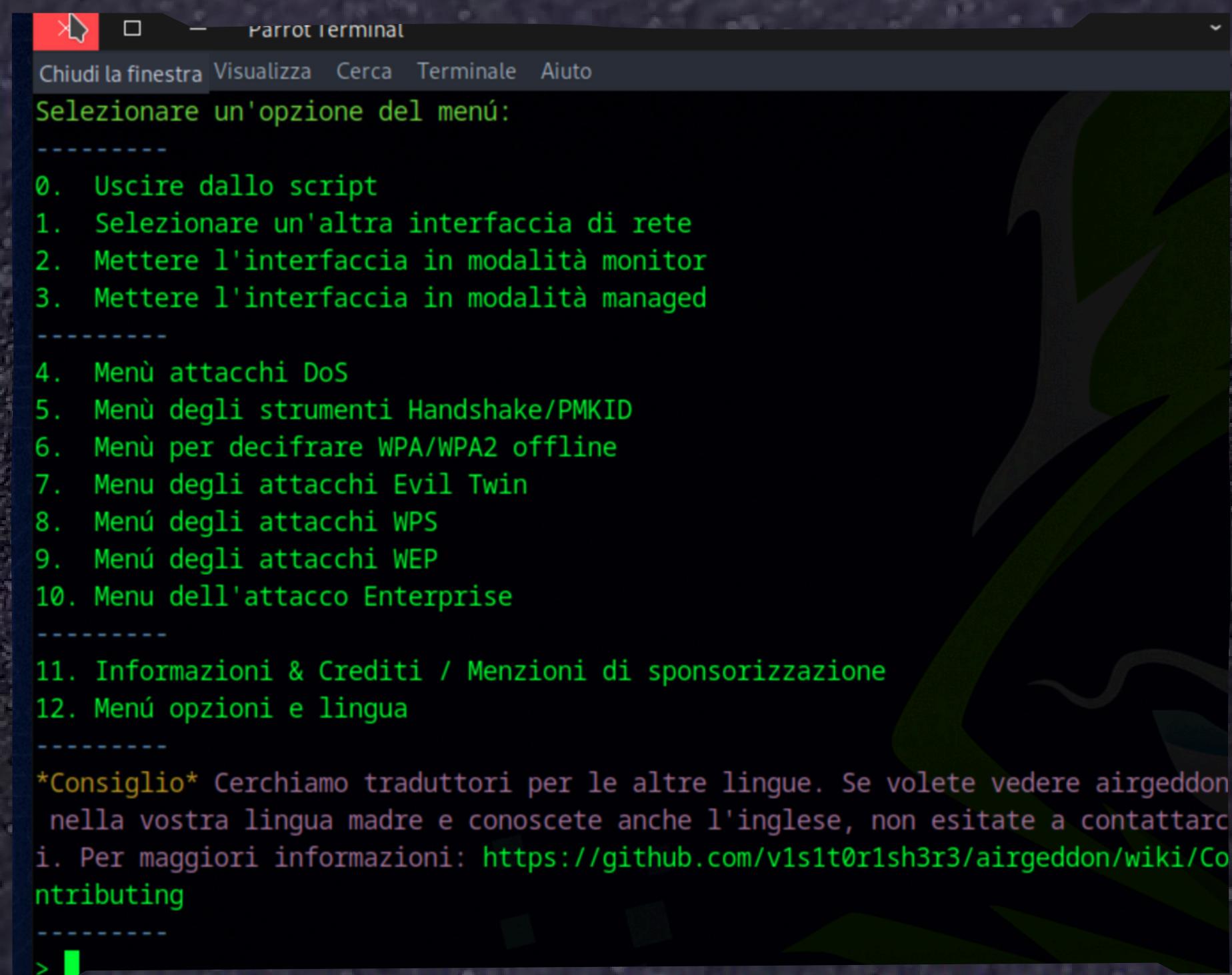
- [Installation & Usage](#)
- [Options](#)
- [Docker](#)
  - [Linux](#)
  - [Mac OSX](#)
  - [Windows](#)
- [Other Sources](#)
- [FAQ & Troubleshooting](#)

#### Project & Development

- [Plugins system](#)
  - [Plugins development](#)
  - [Plugins Hall of Fame](#)
- [Supported Languages](#)
- [Contributing & Code of Conduct](#)
- [Merchandising Online Shop](#)
- [Changelog](#)
- [Disclaimer & License](#)
- [Contact](#)

#### Acknowledgments & References

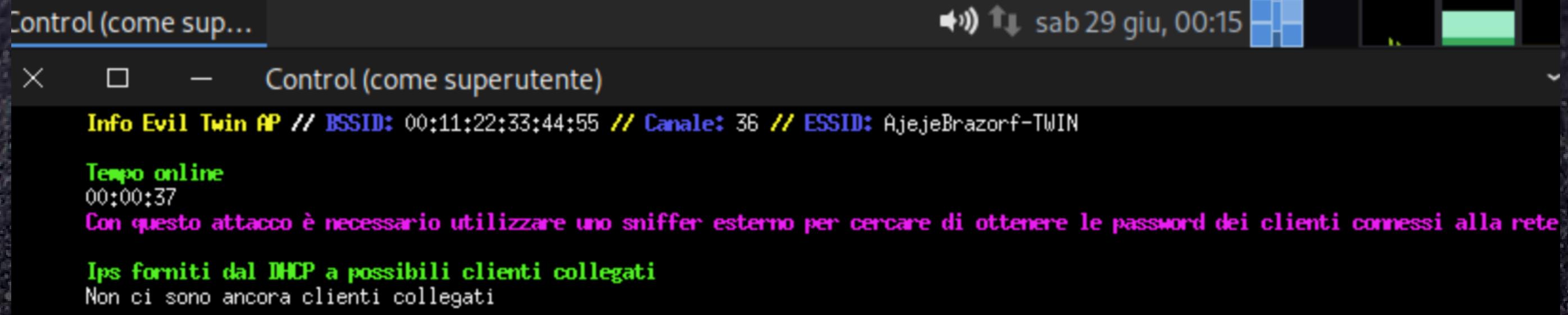
# DEAUTH ATTACK



```
Parrot terminal
Chiudi la finestra Visualizza Cerca Terminale Aiuto
Selezionare un'opzione del menù:
-----
0. Uscire dallo script
1. Selezionare un'altra interfaccia di rete
2. Mettere l'interfaccia in modalità monitor
3. Mettere l'interfaccia in modalità managed
-----
4. Menù attacchi DoS
5. Menù degli strumenti Handshake/PMKID
6. Menù per decifrare WPA/WPA2 offline
7. Menu degli attacchi Evil Twin
8. Menù degli attacchi WPS
9. Menù degli attacchi WEP
10. Menu dell'attacco Enterprise
-----
11. Informazioni & Crediti / Menzioni di sponsorizzazione
12. Menù opzioni e lingua
-----
*Consiglio* Cerchiamo traduttori per le altre lingue. Se volete vedere airgeddon
nella vostra lingua madre e conoscete anche l'inglese, non esitate a contattarc
i. Per maggiori informazioni: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Co
ntributing
----->
```

Grazie ad airgeddon, gli hacker hanno utilizzato la tecnica **Deauth Attack** in modo che le lampadine si scollegassero forzatamente dalla rete Wifi.

# EVIL TWIN



Dopodiché con l'attacco evil twin hanno creato una rete gemella a cui tutte le lampadine si sono ricollegate senza capire che fosse quella degli attaccanti.

# SNIFFING E MANIPOLAZIONE DEI PACCHETTI

Gli hacker hanno poi cominciato ad intercettare il traffico sulla rete, e hanno sniffato informazioni sensibili al fine di aumentare la superficie d'attacco con attacchi mirati e ingegneria sociale attraverso il phishing.

```
192.168.1.33.8149 > 192.168.1.1.53: 24181+ A? api.facebook.com
192.168.1.33.22837 > 192.168.1.1.53: 24181+ A? api.facebook.com
192.168.1.33.30641 > 192.168.1.1.53: 5979+ A? api.facebook.com
192.168.1.33.26870 > 192.168.1.1.53: 5979+ A? api.facebook.com
192.168.1.33.23081 > 192.168.1.1.53: 59541+ A? cnn.com
192.168.1.33.24663 > 192.168.1.1.53: 9351+ A? cnn.com
192.168.1.33.59880 > 192.168.1.1.53: 17819+ A? connectivitycheck.gstatic.com
192.168.1.33.51177 > 192.168.1.1.53: 61721+ A? connectivitycheck.gstatic.com
192.168.1.33.35957 > 192.168.1.1.53: 14523+ A? www.google.com
192.168.1.33.49829 > 192.168.1.1.53: 24947+ A? connectivitycheck.gstatic.com
```

# TIPS TO SAVE YOU

- 1 Rimuovere le lampadine IoT (se non strettamente necessarie)
- 2 Utilizzo di WPA3 al posto di WPA2
- 3 Segmentare la rete e isolare le WLAN (Wireless LAN)
- 4 Formazione del personale



# TRAIN YOUR PEOPLE!

Architettura di reti gsm, funzionamento e attacchi su IMSI Catcher, femtocelle e protezioni relative.

Il personale tecnico deve essere fortemente istruito sull'utilizzo del Wifi.

Si raccomanda di redarre un piano didattico contenente i seguenti argomenti:

Reti Wi-fi e onde radio: funzionamento interno, minacce, attacchi e mitigazioni.

Analisi e studio di altri tools simili ad airgeddon: aircrack, bettercap (integrato in molti di questi tools), e il relativo funzionamento.

# EVERYBODY CAN CRACK!

Come si chiama il celebre strumento che ti aiuta a crackare in maniera divertente le reti WIFI in giro per il mondo?

A: Pwnagotchi

C: Cracking Mama

B: Tamagochi

D: Trackingochi

Il Pwnagotchi è un progetto open-source assestante che riprende il concetto del Tamagotchi, alterandolo. Si basa su un Raspberry Pi (preferibilmente Pi Zero W) sfruttando la potenza di calcolo per esaminare e catturare le vulnerabilità delle reti Wi-Fi.

Infatti, l'idea basata sul prendersi cura dell'animaletto viene rivisistata. Il Pwnagotchi è progettato per diventare felice quando esplora il mondo, connettendosi e compromettendo le varie reti Wi-Fi circostanti. In base alla quantità di reti Wi-Fi compromesse, il Pwnagotchi svilupperà una personalità diversa.

**DISCLAIM**

# NIENTE PAURA!

Per questa ricerca, nessuna delle vostre reti Wi-Fi è stata maltrattata, stressata, o sfruttata per testare attacchi Evil Twin o qualsiasi altro trucco hacker.

Tutti i nostri esperimenti sono stati condotti nel pieno rispetto delle regole (e della vostra banda larga)!

