# Cyber-weetjes

# Disclaimer

Deze presentatie is uitsluitend bedoeld voor informatieve doeleinden en is niet bedoeld om criminele activiteiten aan te moedigen. Er wordt geen verantwoordelijkheid genomen voor handelingen die voortvloeien uit de verstrekte informatie.

# Wat komt er aan bod

- Wayback Machine - The internet archive
- Basisbeveiliging.nl
- Kaspersky real time map
- Flipper Zero
- Evil Twin - malafide wifi punten

# Internet vergeet niet

# WayBackMachine


The Internet Archive is building a digital library of Internet sites and other cultural artifacts in digital form.

Like a paper library, we provide free access to researchers, historians, scholars, people with print disabilities, and the general public.

Mission: to provide Universal Access to All Knowledge.

The Internet Archive serves millions of people each day and is one of the top 300 web sites in the world.

A single copy of the Internet Archive library collection occupies 145+ Petabytes of server space (and they store at least 2 copies of everything).

The privacy is respected by avoiding storage of the IP (Internet Protocol) addresses of our readers and offer our site in https (secure) protocol.

# WayBackMachine


- Start
  - 1996
- Work
  - Archiving the Internet itself, a medium that was just beginning to grow in use. Like newspapers, the content published on the web was ephemeral - but unlike newspapers, no one was saving it.
- Today
  - 28+ years of web history accessible through the Wayback Machine supported by 1,200+ library and other partners through our Archive-It program to identify important web pages.

# WayBackMachine


Today the WayBackMachine archive contains:

- 835 billion web pages
- 44 million books and texts
- 15 million audio recordings (including 255,000 live concerts)
- 10.6 million videos (including 2.6 million Television News programs)
- 4.8 million images
- 1 million software programs

# WayBackMachine


Anyone with a free account can upload media to the Internet Archive. We work with thousands of partners globally to save copies of their work into special collections.

## Books:

Because we are a library, we pay special attention to books. Not everyone has access to a public or academic library with a good collection, so to provide universal access we need to provide digital versions of books. We began a program to digitize books in 2005 and today we scan 4,400 books per day in 20 locations around the world. Books published in or prior to 1928 are available for download, and hundreds of thousands of modern books can be borrowed through our Open Library site. One of the Internet Archive's missions is to serve people who have difficulty interacting with physical books, so most of our digitized books are available to people with print disabilities (learn about access here).

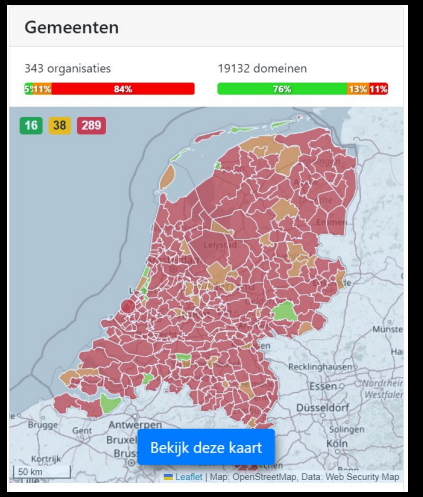
## Television:

Like the Internet, television is also an ephemeral medium. We began archiving television programs in late 2000, and our first public TV project was an archive of TV news surrounding the events of September 11, 2001. In 2009 we began to make selected U.S. television news broadcasts searchable by captions in our TV News Archive. This service allows researchers and the public to use television as a citable and sharable reference.

# Demo - WayBackMachine


[Wayback Machine (archive.org)]

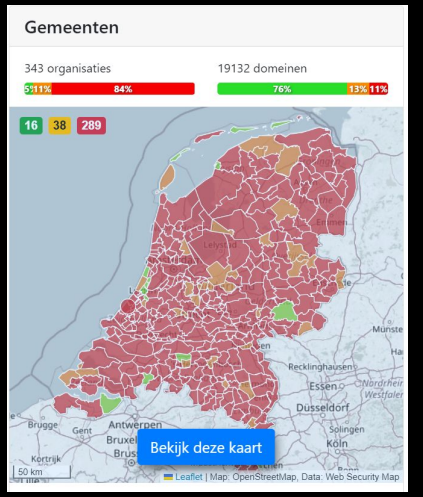
# Basisbeveiliging.nl




Deze website laat zien of belangrijke organisaties digitale basisveiligheid op orde hebben.

Dit is noodzakelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van online dienstverlening. Denk aan een veilige website of e-mail.

# Basisbeveiliging.nl

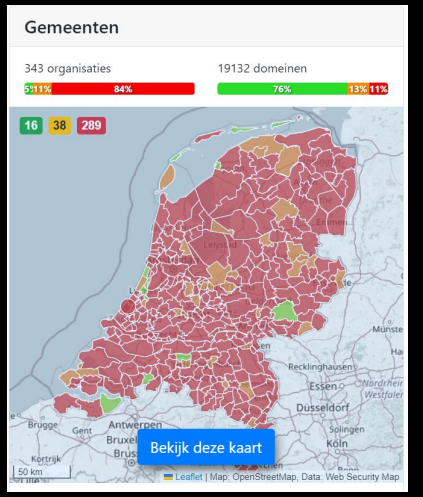



Basisbeveiliging.nl toont een actueel zicht op de veiligheid van de overheid, provincies, gemeenten, waterschappen, ziekenhuizen, GGD's, politieke partijen en cybersecuritybedrijven.

Aan deze organisaties worden door henzelf en anderen allerlei veiligheidseisen gesteld. Deze site laat zien of deze eisen worden toegepast.

De website van de Internet Cleanup Foundation

# Basisbeveiliging.nl




Hoe vinden we wat we kunnen meten?

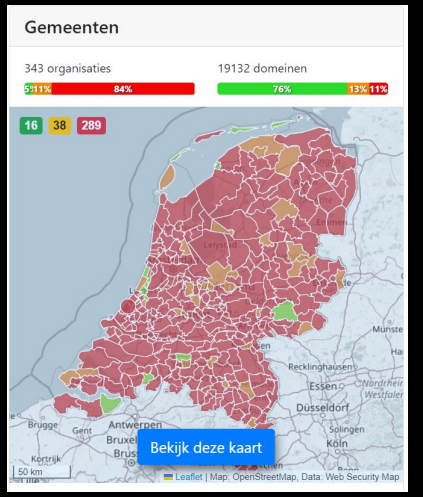
Basisbeveiliging meet veiligheid op het internet op basis van open bronnen en publieke meetinstrumenten.

Eerst wordt informatie verzameld over wat er allemaal te vinden is. Dit gebeurd onder andere met de volgende instrumenten:

- Kaartgegevens: Open Street Map
- Domeinen: Wikidata, Websiteregister rijksoverheid, Overheidsregister
- Subdomeinen: crt.sh, dnsrecon, eigen scanners
- Diensten: nmap, masscan, eigen HTTP scanner, eigen FTP scanner

Daarnaast worden domeinen toegevoegd via het helpdesksysteem, vrijwilligers en openbare databronnen.

# Basisbeveiliging.nl

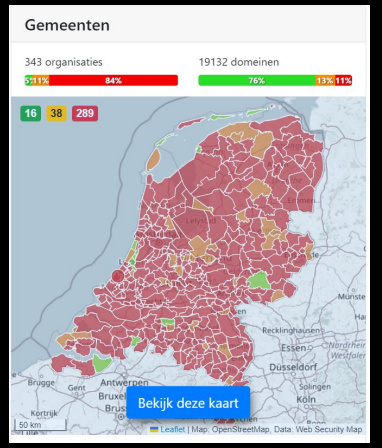



## Wat wordt er gemeten?

Metingen worden uitgevoerd met de volgende instrumenten:

- Versleuteling en kwaliteit: Qualys SSL Labs
- Veiligheid DNS: Zonemaster dnssec
- Headers van websites: Eigen scanner
- Onversleutelde FTP: Eigen scanner
- E-Mail Veiligheid: Internet.nl
- RPKI en Security.txt: Internet.nl
- Niet standaard poorten: Eigen scanner
- Ontbrekende vesleuteling: Eigen scanner
- Platform identificatie: nmap, masscan
- Screenshots: Browserless

# Basisbeveiliging.nl

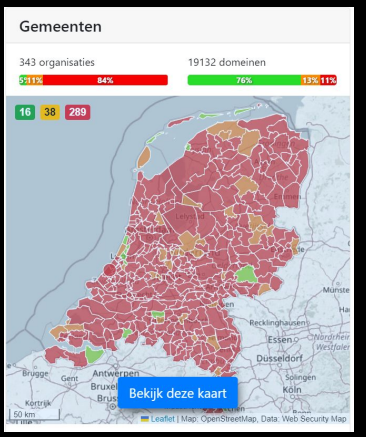



## Kan ik zelf meten?

Zelf een keer meten? Een meting controleren? Gebruik dan een van de volgende websites. Deze websites worden ook genoemd bij eventuele bevindingen.

- Open poorten: IPVoid
- Web en E-mail standaarden: internet.nl
- DNSSEC: Zonemaster
- FTP: ftptest.net
- HTTP Security Headers: securityheaders.io
- IPv6: ip6.nl
- TLS: ssllabs.com

# Basisbeveiliging.nl




## Waar vind ik meer informatie?

Op de volgende pagina's staat een heleboel achtergrondinformatie over alles wat op deze site wordt gemeten.

### Algemeen

- Poorten/Diensten, Platformidentificatie, Security.txt, DNSSEC, RPKI, IPv6: wikipedia
- Security Headers: owasp, - Clickjacking: wikipedia, - HSTS: wikipedia

### Versleuteling

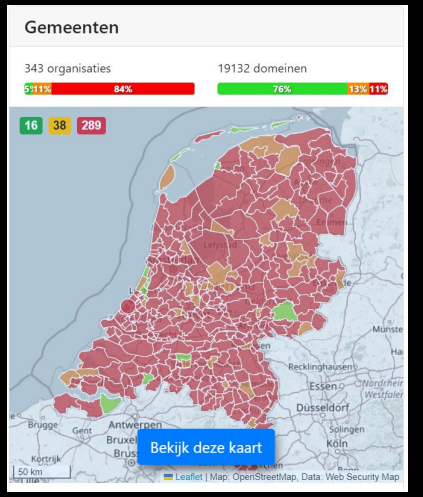
- Goede inrichting TLS op allerlei servers: cipherlist
- TLS Algemeen en TLS op niet-webservers, Secure FTP: wikipedia

### E-mail veiligheid

- Inrichten e-mail veiligheid: internet.nl
- DKIM, SPF, DMARC: wikipedia

# Demo - Basisbeveiliging.nl

- [Basisbeveiliging – Kaarten]



# Kaspersky


- Kaspersky is een internationaal bedrijf die wereldwijd actief is in bijna 200 landen en gebieden.
- Leverancier van antivirussoftware voor consumenten en bedrijven.
- Staat mondiaal in de top vier.

- Het Benelux-kantoor is gevestigd in Utrecht, Nederland.
- De R&D centers van het bedrijf zijn over de hele wereld te vinden, waaronder Europa, de Verenigde Staten, Zuid-Amerika, China, Japan en Rusland.

# Kaspersky


Web-Anti Virus
Intrusion Detection Scan (IDS)
Vulnerability Scan
Kaspersky Anti-Spam
Botnet Activity Detection
Ransomware
Mail Anti Virus
On-Demand Scan
On-Access Scan

# Kaspersky


## OAS - On-Access Scan

OAS (On-Access Scan) shows malware detection flow during On-Access Scan, i.e. when objects are accessed during open, copy, run or save operations.

## ODS - On-Demand Scan

ODS (On Demand Scanner) shows malware detection flow during On-Demand Scan, when the user manually selects the ’Scan for viruses’ option in the context menu.

## MAV - Mail Anti Virus

MAV (Mail Anti-Virus) shows malware detection flow during Mail Anti-Virus scan when new objects appear in an email application (Outlook, The Bat, Thunderbird). The MAV scans incoming messages and calls OAS when saving attachments to a disk.

# Kaspersky


## WAV - Web Anti-Virus

WAV (Web Anti-Virus) shows malware detection flow during Web Anti-Virus scan when the html page of a website opens or a file is downloads. It checks the ports specified in the Web Anti-Virus settings.

## IDS - Intrusion Detection Scan

IDS (Intrusion Detection System) shows network attacks detection flow.

## VUL - Vulnerability Scan

VUL (Vulnerability Scan) shows vulnerability detection flow.

## KAS - Kaspersky Anti-Spam

KAS (Kaspersky Anti-Spam) shows suspicious and unwanted email traffic discovered by Kaspersky's Reputation Filtering technology.

# Kaspersky


## BAD - Botnet Activity Detection

BAD (Botnet Activity Detection) shows statistics on identified IP-addresses of DDoS-attacks victims and botnet C&C servers. These statistics were acquired with the help of the DDoS Intelligence system (part of the solution Kaspersky DDoS Protection).

## RMW - Ransomware

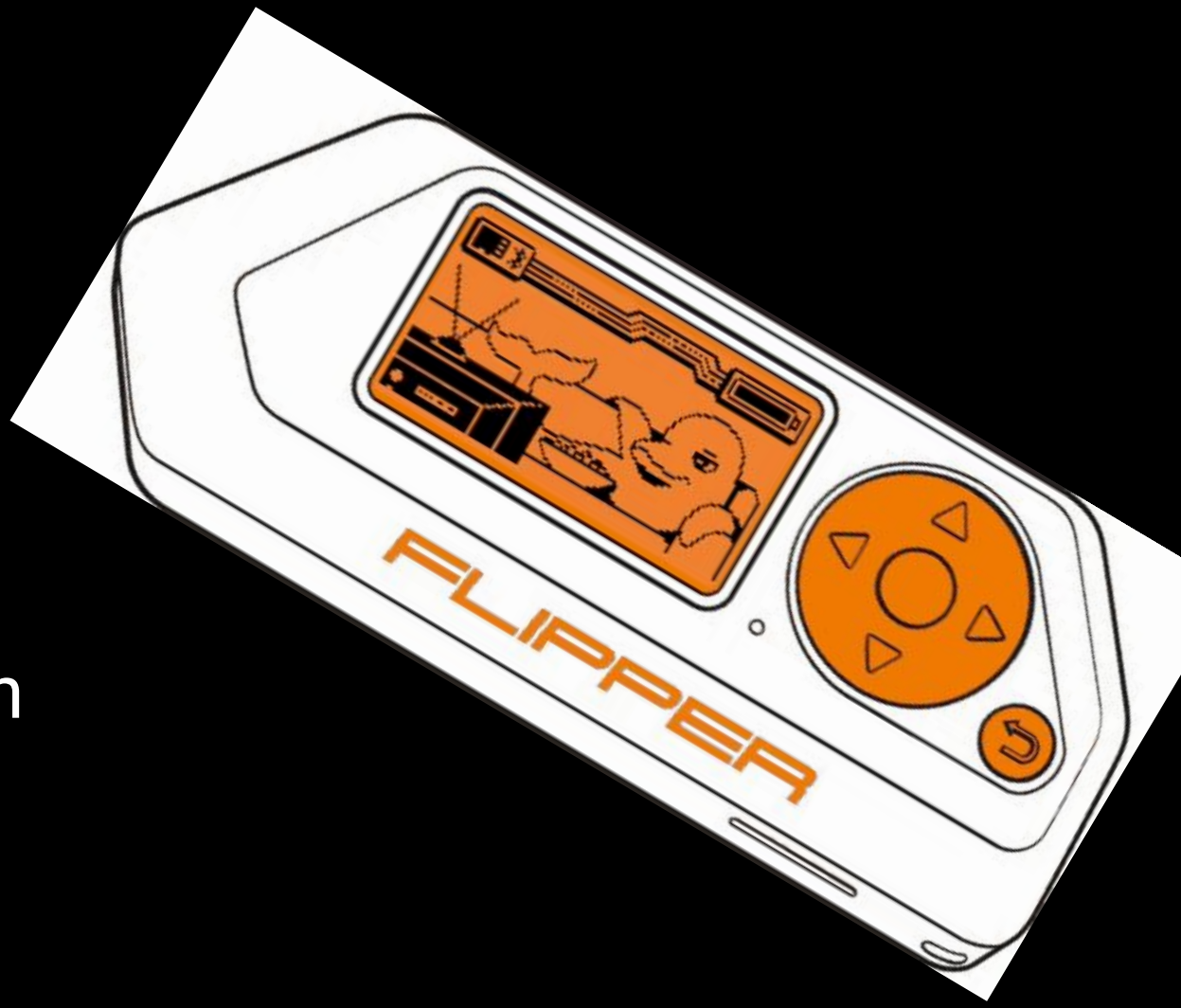
RMW (Ransomware) shows ransomware detection flow.

# Demo - Kaspersky


[MAP | Kaspersky Cyberthreat live map]

# FlipperZero

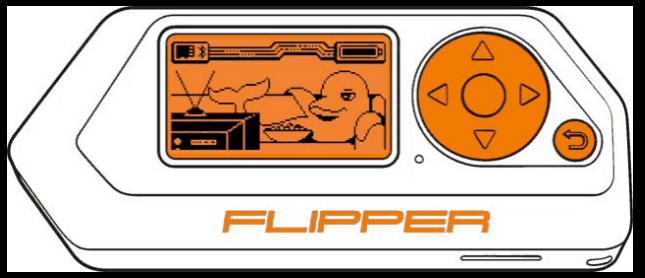
## Multi-tool Device for Geeks




Flipper Zero is een klein stukje hardware met een pictogram van een eigenwijze cyber-dolphin.

Dit apparaatje kan interacteren met andere digitale systemen in het echte leven en groeien gedurende het gebruik.

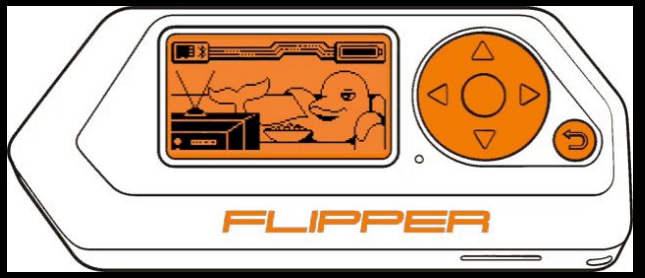
# FlipperZero




- Flipper Zero is een draagbare multitool in een speelgoedachtige behuizing.
- Gebruikt door pentesters en geeks
- Je kan er digitale dingen mee hacken, zoals radioprotocollen, toegangscontrolesystemen, hardware en meer.
- Het is volledig open-source en aanpasbaar, dus je kunt het op elke gewenste manier uitbreiden.

Flipper Zero — Portable Multi-tool Device for Geeks

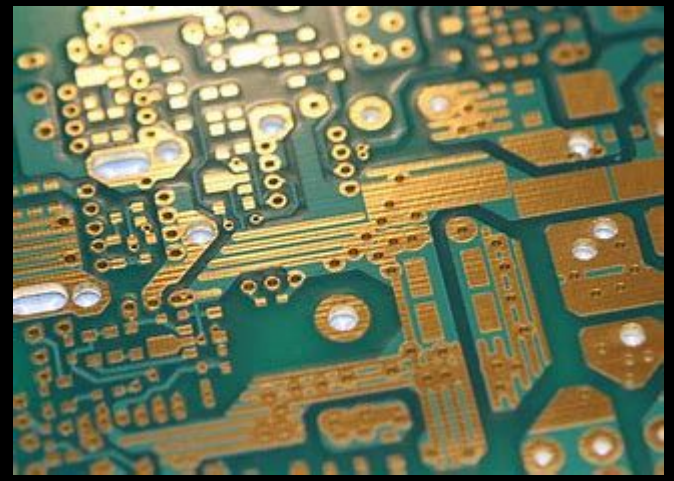
# FlipperZero



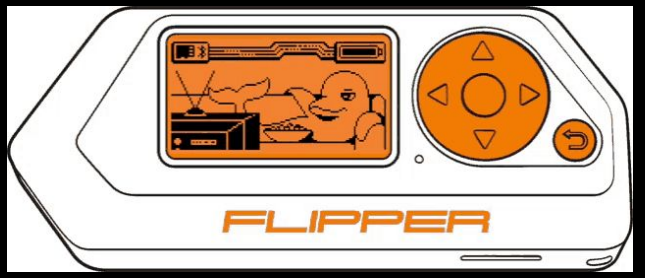

Het idee van Flipper Zero is om alle hardwaretools te combineren die je nodig hebt voor verkenning en ontwikkeling van netwerken en diverse systemen.

Flipper is geïnspireerd door het pwnagotchi-project, maar in tegenstelling tot andere doe-het-zelfborden is Flipper ontworpen met het gemak van dagelijks gebruik in gedachten: het heeft een robuuste behuizing, handige knoppen en vorm, dus er zijn geen vieze PCB's of krassende pinnen.

Flipper verandert je projecten in een spel en herinnert je eraan dat ontwikkeling altijd leuk moet zijn.



# Demo - FlipperZero



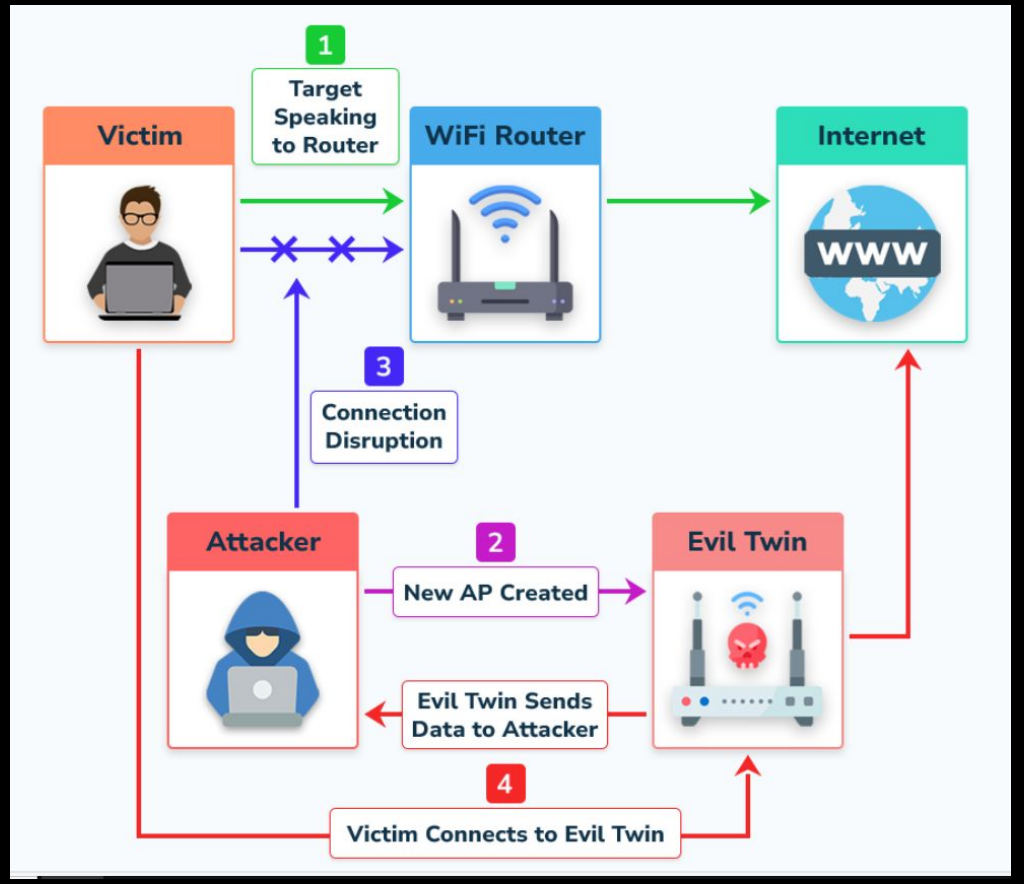

[Bing Video's]

# FlipperZero



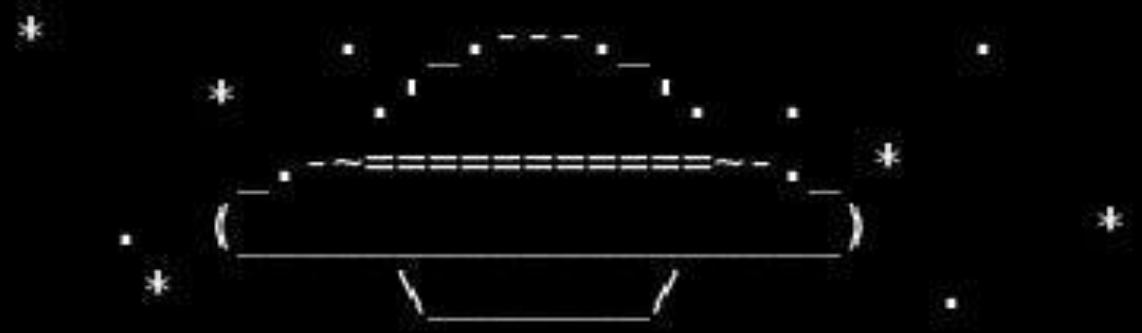

# Evil Twin aanval

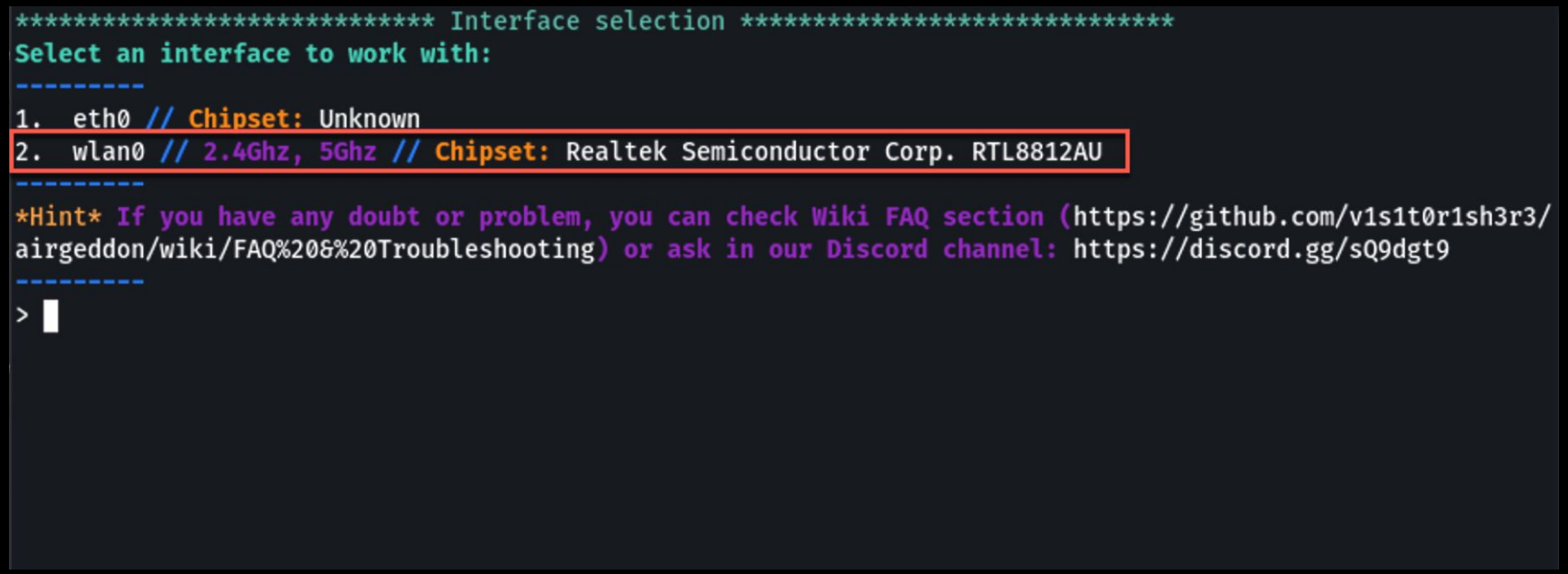
1. Slachtoffer maakt connectie met eigen WIFI  internet toegang
2. Crimineel maakt eigen WIFI punt met zelfde naam (SSID).
3. Crimineel verstoord connectie tussen slachtoffer en eigen WIFI
4. WIFI punt crimineel laat slachtoffer een verbinding maken



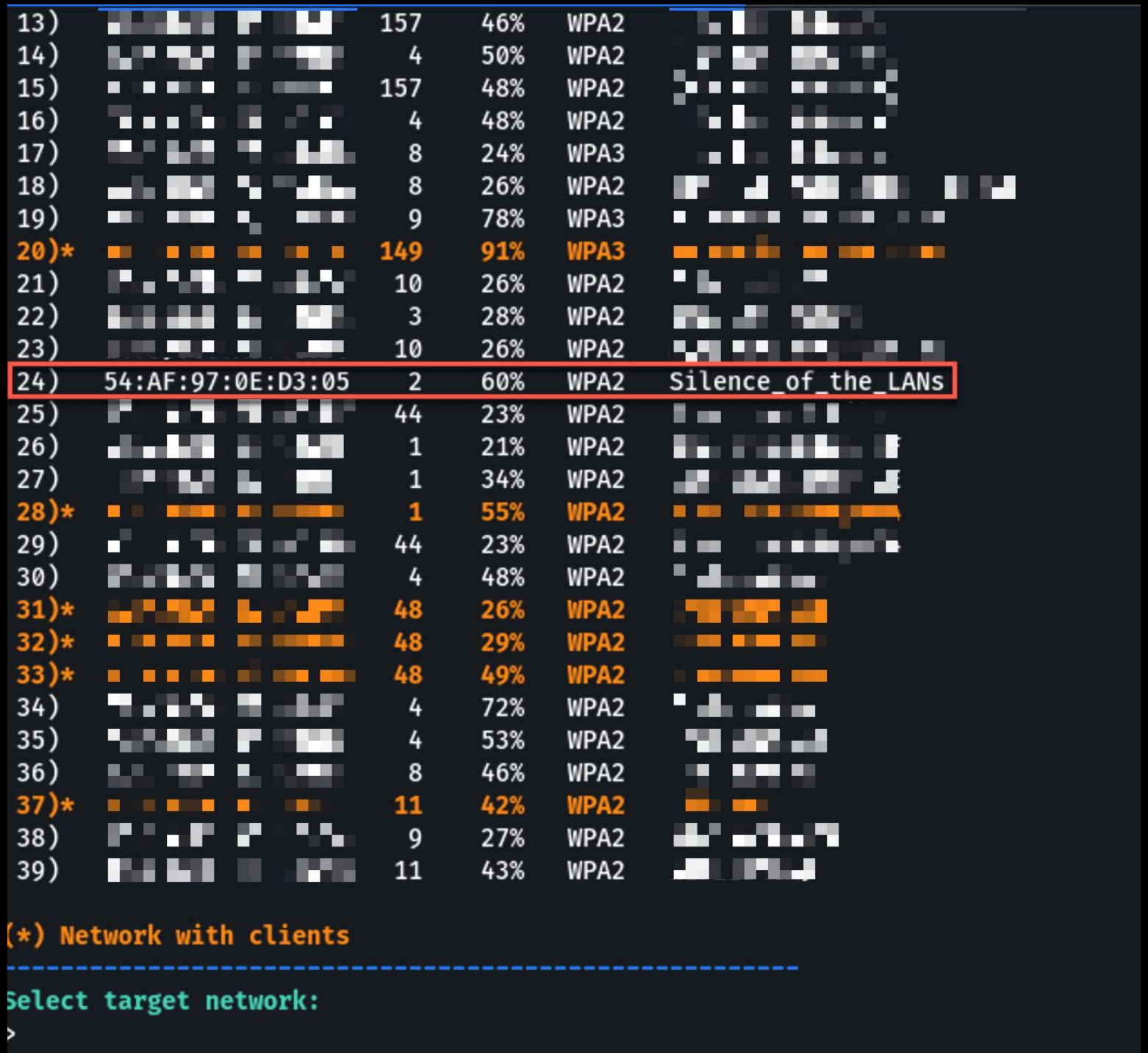
Welcome to airgeddon script v9.21

Developed by v1s1t0r




********** Interface selection **********
Select an interface to work with:
---
1. eth0 // Chipset: Unknown
2. wlan0 // 2.4Ghz, 5Ghz // Chipset: Realtek Semiconductor Corp. RTL8812AU
---
*Hint* If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting) or ask in our Discord channel: https://discord.gg/sQ9dgt9
---
>

```
***************************** Evil Twin attacks menu *****************************
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) ----------------
5.  Evil Twin attack just AP
---------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
------------- (without sniffing, captive portal) -------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
---------
*Hint* In order to use the Evil Twin just AP and sniffing attacks, you must have another one interface in
addition to the wifi network interface will become the AP, which will provide internet access to other cli
ents on the network. This doesn't need to be wifi, can be ethernet
---------
>
```

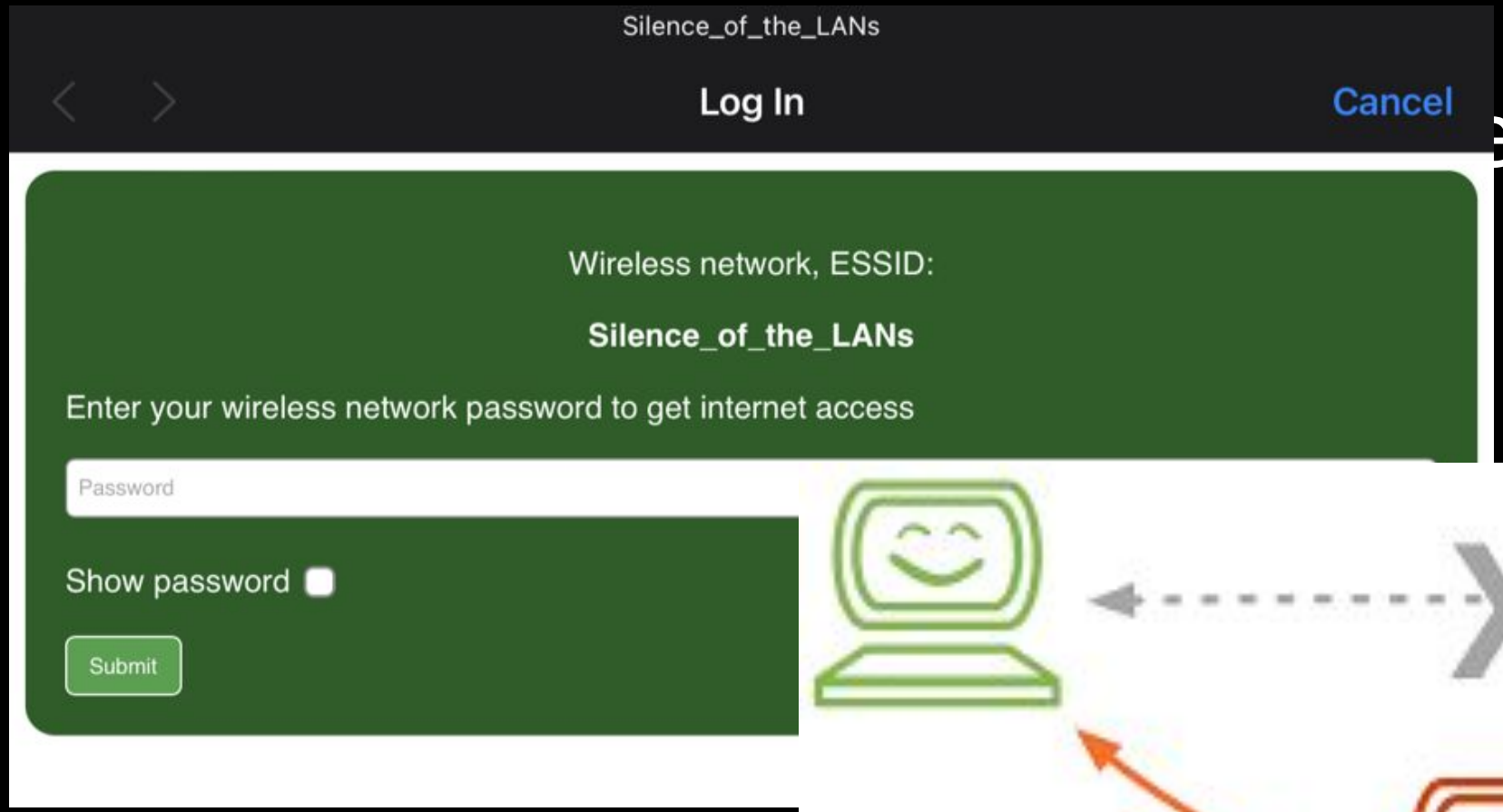

13) 157 46% WPA2
14) 4 50% WPA2
15) 157 48% WPA2
16) 4 48% WPA2
17) 8 24% WPA3
18) 8 26% WPA2
19) 9 78% WPA3
20)* 149 91% WPA3
21) 10 26% WPA2
22) 3 28% WPA2
23) 10 26% WPA2
24) 54:AF:97:0E:D3:05 2 60% WPA2 Silence_of_the_LANs
25) 44 23% WPA2
26) 1 21% WPA2
27) 1 34% WPA2
28)* 1 55% WPA2
29) 44 23% WPA2
30) 4 48% WPA2
31)* 48 26% WPA2
32)* 48 29% WPA2
33)* 48 49% WPA2
34) 4 72% WPA2
35) 4 53% WPA2
36) 8 46% WPA2
37)* 11 42% WPA2
38) 9 27% WPA2
39) 11 43% WPA2
(*) Network with clients
Select target network:
>

```
************************** Evil Twin attacks menu **************************
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
----------------- (without sniffing, just AP) -----------------
5.  Evil Twin attack just AP
---------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
-------------- (without sniffing, captive portal) --------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
---------
*Hint* If you use the attack without sniffing, just the AP, you can use any external sniffer script
---------
> 9

The interface wlan0 you have already selected is not supporting VIF (Virtual Interface). This attack needs
 it to virtually unfold itself to create the fake access point while also performing denial of service (Do
S). Do you want to continue? If yes, the denial of service will not work being an important part of the at
tack and making it probably ineffective [y/N]
>
```

```
********** Evil Twin deauth **********
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 54:AF:97:0E:D3:05
Selected channel: 2
Selected ESSID: Silence_of_the_LANs
Handshake file selected: None

Select an option from menu:
---------
0.  Return to Evil Twin attacks menu
---------
1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
---------
*Hint* If you can't deauth clients from an AP using an attack, choose another one :)
---------
>
```

```
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-54:AF:97:
0E:D3:05.cap]
>
The path is valid and you have write permissions. Script can continue...

Capture file generated successfully at [/root/handshake-54:AF:97:0E:D3:05.cap]
Press [Enter] key to continue...

BSSID set to 54:AF:97:0E:D3:05

Channel set to 2

ESSID set to Silence_of_the_LANs

If the password for the wifi network is achieved with the captive portal, you must decide where to save it
. Type the path to store the file or press [Enter] to accept the default proposal [/root/evil_twin_captive
_portal_password-Silence_of_the_LANs.txt]
>
```

```
******************** Evil Twin AP attack with captive portal ********************
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 54:AF:97:0E:D3:05
Selected channel: 2
Selected ESSID: Silence_of_the_LANs
Deauthentication chosen method: mdk4
Handshake file selected: /root/handshake-54:AF:97:0E:D3:05.cap

Choose the language in which network clients will see the captive portal:
---------
0.  Return to Evil Twin attacks menu
---------
1.  English
2.  Spanish
3.  French
4.  Catalan
5.  Portuguese
6.  Russian
7.  Greek
8.  Italian
9.  Polish
10. German
11. Turkish
12. Arabic
---------
*Hint* If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r3/
airgeddon/wiki/FAQ%20&%20Troubleshooting) or ask in our Discord channel: https://discord.gg/sQ9dgt9
---------
>
```


Silence_of_the_LANs
Log In
Cancel
Wireless network, ESSID:
Silence_of_the_LANs
Enter your wireless network password to get internet access
Password
Show password
Submit