**Universiteti i Prishtinës**

**“Hasan Prishtina”**



**Projekti 2**

**Lënda:** “Siguria në Internet”

**Tema:** Veglat për sulme “Wireless”

(Eng. “Wireless Attack Tools”)

**“Aircrack-ng”**

*Prof. Asoc. Blerim Rexha Punoi:*

*Msc. Arbnor Halili Ndriçim Halili*

*Prishtinë, 2021*

Table of Contents

[1. Hyrja – Aircrack-ng 3](#_Toc66184480)

[1.1. Instalimi i “Aircrack-ng” 3](#_Toc66184481)

[1.2. Përdorimi i “Aircrack-ng” 3](#_Toc66184482)

[1.3. Komandat e “aircrack-ng” 4](#_Toc66184483)

[2. “Airmon-ng” dhe “Airodump-ng” 4](#_Toc66184484)

[3. Gjetja e fjalëkalimit të një rrjeti 5](#_Toc66184485)

[3.1. “Rockyou.txt” 6](#_Toc66184486)

[3.2. Gjetja e fjalëkalimit me anë të “dictionary attack” 7](#_Toc66184487)

[4. Më shumë rreth “Aircrack-ng” 8](#_Toc66184488)

[4.1. Tabela e komandave për “Airdump-ng” 8](#_Toc66184489)

[4.2. Tabela e modeve për “Aireplay-ng” 9](#_Toc66184490)

# Hyrja – Aircrack-ng

“Aircrack-ng” është një vegël në Linux që përdoret për analizimin dhe sulmin e rrjeteve pa kabëll (ang. “Wireless”). Kjo vegël është në fakt një bashkësi e gjerë veglsh të ndryshme që përdoren me “Command line”.

“Aircrack-ng” është një bashkësi veglash që bën analiza të rrjeteve pa kabëll për pika të dobëta. Mund të përdoret për monitorimin e sigurisë së “Wi-Fi”, kapjen e paketave të të dhënave dhe eksportimin e tyre në fajlla për analiza të mëtejshme. Testuestit e depërtimit të rrjetave (Ang. “Penetration testers” ,ndryshe “Pen testers”) mund ta përdorin për sulme dhe thyerje të rrjetave që përdorin protokollet e sigurisë: “WPA” dhe “WEP”.

## Instalimi i “Aircrack-ng”

Për instalim nevojitet të kemi privilegjin e adminit, kështu që duhet të përdorim komandën “sudo”, por pasi jam qasu si “root”, kjo nuk është e nevojshme.

Si fillim, metoda më e thjeshtë është përdorimi i komandës “Apt-get”

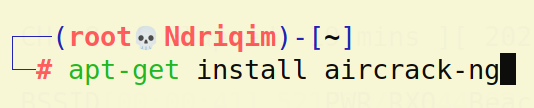


Figure 1 Instalimi i "aircrack-ng"

Pas instalimit mund të përdoret komanda “—help” për më shumë detaje.

Gjitashtu, për instalim mund të përdoret linku: “[Aircrack-ng (aircrack-ng.org)](https://www.aircrack-ng.org/)”. Në këtë ndodhet gjithçka që nevojitet për të përdorur veglën, si dhe ndihmesa, wiki, forume etj... për të ndihmuar çdokënd që përdor këtë vegël.

## Përdorimi i “Aircrack-ng”

Nëse përdorim komandën “--help”, atëherë na shfaqet një lloj shablloni për përdorim.

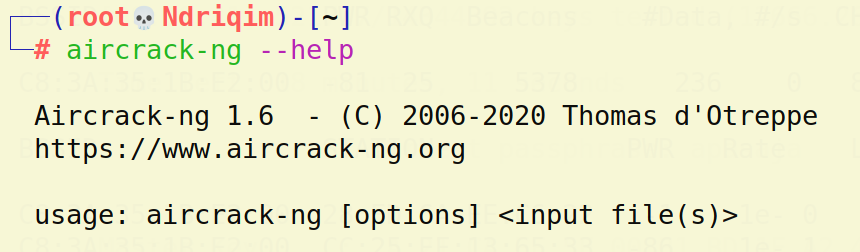


Figure 2 Ndihma për "Aircrack-ng"

* [options] janë opsionet që duam të përdorim (këto opsione janë paraqitur në tabelën më poshtë)
* <input file(s)> janë fajllat që duam të përdorim, këto fajlla mund të jenë të llojllojshme si .cap, (fajlla që përmbajnë “raw data” të paketave) tekst fajlla për dalje ose edhe për “wordlists” etj.

## Komandat e “aircrack-ng”

|  |  |
| --- | --- |
| -a <amode> | Modi i sulmit (1/për WEP dhe 2/WPA-PSK) |
| -e <essid> | Zgjedhja e paisjes me anë të emrit |
| -b <bssid> | Zgjedhja e paisjes me anë të MAC adresës |
| -p <nbcpu> | Numri i procesorëve që do të përdoret (default: të gjithë procesorët) |
| -q | Ndiz modin e “heshtur” (nuk regjistrohet dalja) |
| -C <macs> | Bashkoji “Access Points” në një të “Access point” virtual |
| -l <file> | Shkruaj çelësin në fajll. (Mbishkruan fajllin e dhënë) |

Table 1 Komandat më të përdorura të "Aircrack-ng"

# “Airmon-ng” dhe “Airodump-ng”

“Airmon-ng” dhe “Airodump-ng” janë nëbashkësi e bashkësisë së veglave të “Aircrack-ng”.

“Airmon-ng” Përdoret për t’i bërë ndërfaqet (ang. “Interfaces”) e “Wireless” në modin e monitorimit të rrjetit

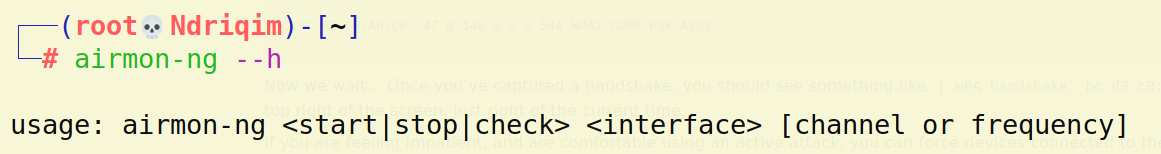


Figure 3 Përdorimi i "Airmon-ng"

Përdorimi i kësaj vegle është i thjeshtë, ku prej të cilit mund të krijojmë një ndërfaqe të “Wireless” për monitorim.

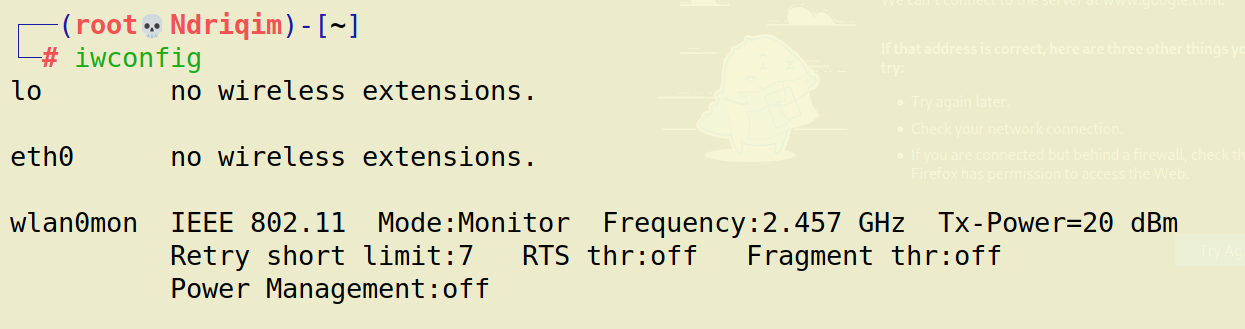


Figure 4 Shohim ne "iwconfig" që kemi wlan0mon në modin e monitorimit

Pas kësaj ne përdorim veglën “Airodump-ng” për të parë rrjetin:

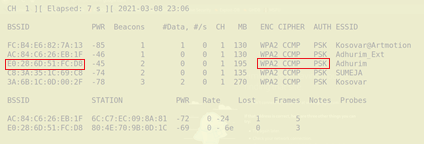


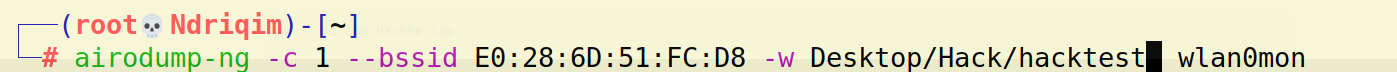
Figure 5 "Tabela" e pikave të qasjes ("Access Points")

Me këtë tabelë ne shohim të gjitha pikat e qasjes së rrjetave të ndryshme që duam t’ju qasemi. Për vazhdim zgjedhim rrjetin “Adhurim” pasi është rrjeti nën pronën time, që të mos bëjmë ndonjë keqpërdorim të veglave.

# Gjetja e fjalëkalimit të një rrjeti

Pas zgjedhjes së rrjetit që duam të sulmojmë ne duhet ta monitorojmë atë për “4 way handshakes”, këto janë “duarshtrëngime” ose më saktë, komunikime në mes një paisjeje klient me pikën e qasjes kur autentifikohet në rrjet. Shkurt, ne duam të gjejmë një paketë që e dërgon klienti te pika e qasjes për autentifikim në rrjet, me anë të kësaj pakete edhe ne mund të marrim qasje në rrjet.

Këtë e bëjmë me komandën:



Ku me opsionin “-c” zgjedhim kanalin ku transmeton pika e qasjes që po suljmojmë dhe “--bssid” është MAC adresa e kësaj pike. “-w” tregon se ku duam ta ruajmë paketën që do të marrim, si dhe “wlan0mon” tregon se cilën ndërfaqje do të përdorim për monitorim.

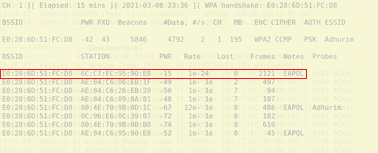
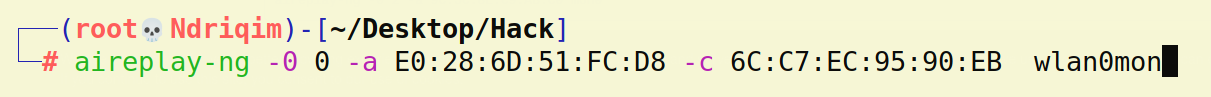


Figure 6 Monitorimi i paketave që shkojnë te pika e qasjes

Gjatë monitorimit ne duhet të presim një paketë e formës “EAPoL” (Ang. “Extensible Authentication Protocol over LAN”), që do të thotë se njëri prej klientëve po bën kërkesë për autentifikim në rrjet. Kjo është paktë që na nevojitet se pse përmban informatat e mjaftueshme për të gjetur fjalëkalimin e rrjetit.

Gjitashshtu, si shtojcë, ne mund të përdorim komandën



Vegla “Aireplay-ng” shpesh përdoret për deautentifikimin e një klienti -c “6C:C7:EC:95:90:EB” nga pika e qasjes -a “E0:28:6D:51:FC:D8” me anë të ndërfaqjes “wlan0mon”, (këtu (-0 0) “-0” ndryshe është edhe “-deauth”).

Tani, afër fundit, ne e “pastrojmë” fajllin “hacktest.cap” me anë të komandës

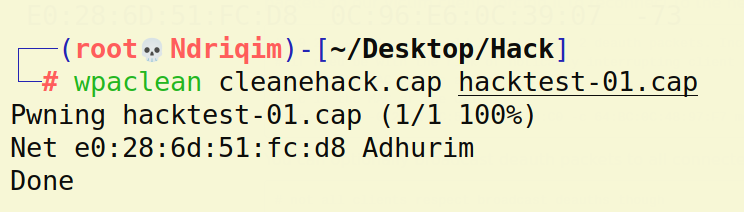


Figure 7 Pastrimi i "hacktest-01.cap"

## “Rockyou.txt”

Para se të fillojmë gjetjen e fjalëkalimit, neve na nevojitet një “wordlist”, dmth nja listë fjalëkalimesh të mundshme që testohen për të gjetur fjalëkalimin që ka pika e qasjes. Kjo njihet edhe si “Dictionary attack”

Si “wordlist” kam përdorur fajllin “rockyou.txt”, ky fajll përmban mbi 14 milionë fjalëkalime të mundshme. Fatkeqësisht, fjalëkalimi i rrjetit tim nuk gjendet në këtë fajll, por për shkaqe testimi e kam vendosur në fund, për të parë rastin më të keq.

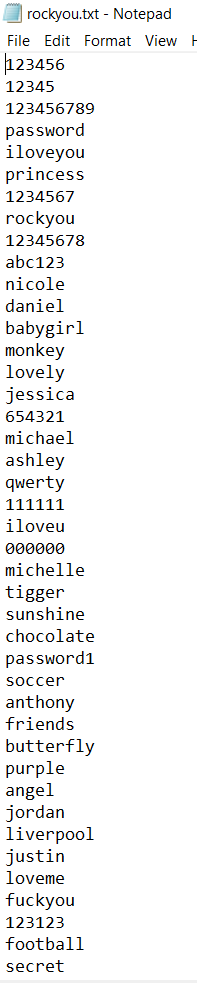


Figure 8 Fajlli "Rockyou.txt", në "Windows"

## Gjetja e fjalëkalimit me anë të “dictionary attack”

Tani si fund, përdorim komandën:

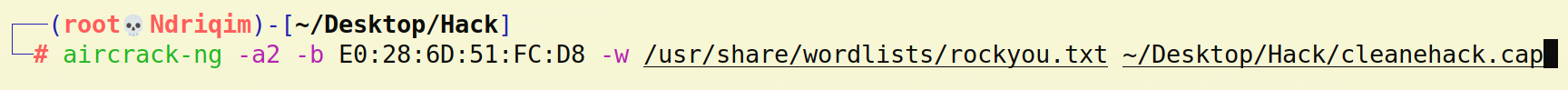


Figure 9 Komanda për gjetjen e fjalëkalimit

Këtu kemi “-a2“ për llojin e sigurisë që është “WPA2-PSK”, ku mund të shihet nga [fig.5](#figura_5) ose [fig\_6](#figura_6), dhe “-b” për MAC adresën e cilës pikë qasjeje po sulmojmë. Pas “-w” kemi se cilin “wordlist” do të përdorim dhe në fund kemi fajllin ku është ruajtur paketa me “EAPoL”.

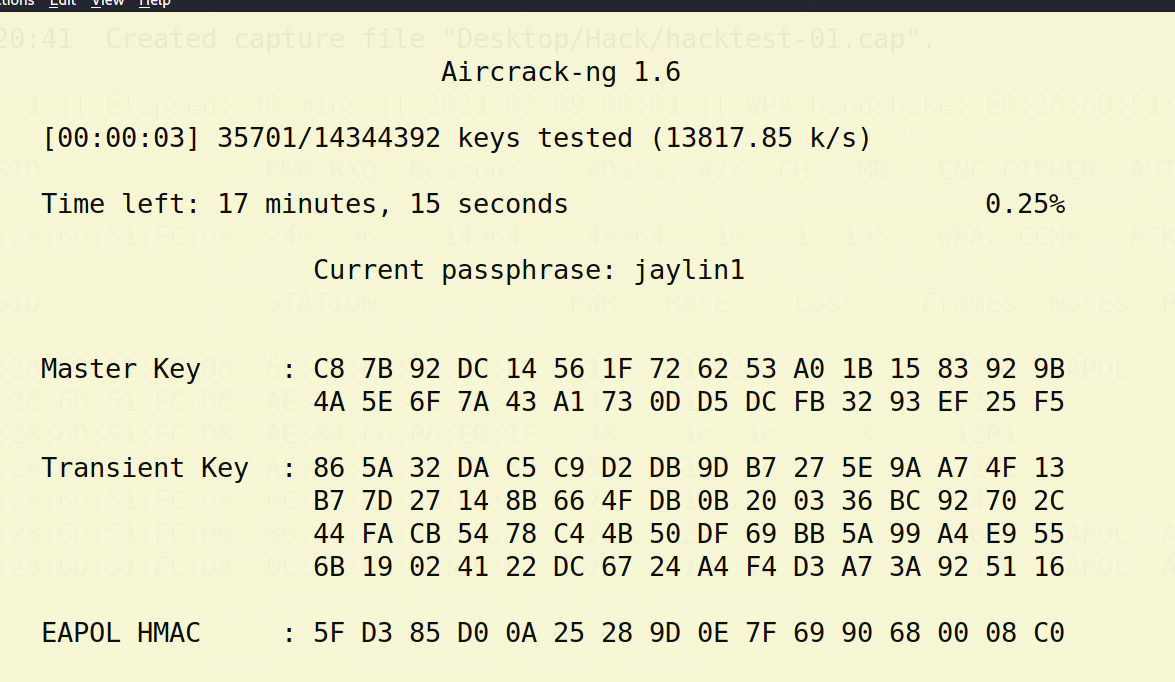


Figure 10 "Dictionary attack" në rrjet

Fatkeqësisht, ose më mirë fatmirësisht, fjalëkalimi im nuk ishtë në “wordlist”-in “rockyou” dhe në fund është dhënë dalja

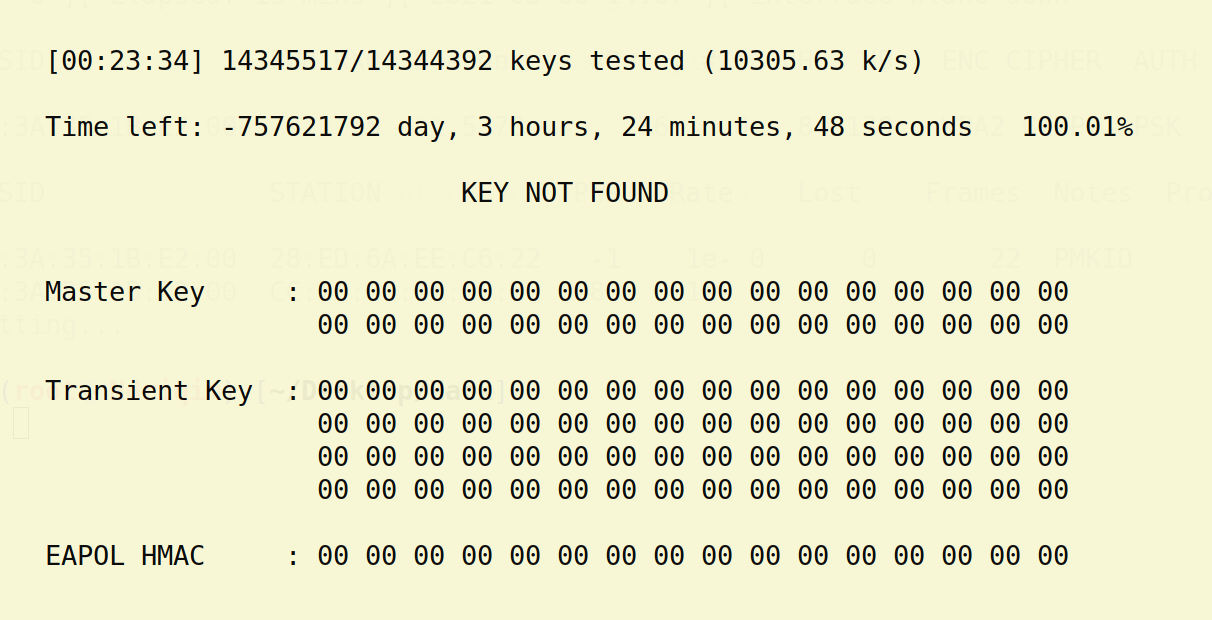


Figure 11 Nuk është gjetur çelësi (fjalëkalimi)

Sa për testim, kam vendosur fjalëkalimin e rrjetit në fund të “Rockyou” dhe në fund kam pasur daljen

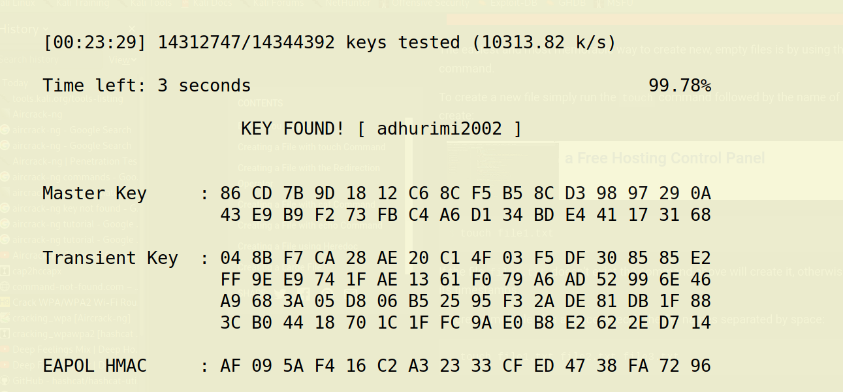


Figure 12 U gjetur çelësi

Në fund shohim se, në rastin më të keq, iu është nevojitur më pak se 24 minuta për të kryer të gjithë procedurën, kjo që është kohë jo e keqe, duke e marrë parasysh se jemi duke përdorur një makinë virtuale me 6 procesorë të rezervuar.

# Më shumë rreth “Aircrack-ng”

Deri tani kam folur rreth se si mund ta gjejmë fjalëkalimin e një rrjeti pa kabëll (“Wireless”), por gjatë rrugës pamë se si kemi përdorur mjete të ndryshme, si dhe sulme të ndryshme të mundshme.

* **“Airmon-ng” –** u përdor për të ndërruar përdorimin e një “Wi-Fi” ndërfaqjeje në modin e monitorimit. Kartela ose paisja për qasje në “Wireless” tani nuk mund të përdoret për qasje në internet, por për të skanuar rrjetet.
* **“Airodump-ng” -** u përdor, për të marrë informata rreth rrjetit që duam të sulmojmë. Duke monitoruar ne mund të shikojmë rrjetet që mund të lidhemi dhe më pas të marrim paketa që transmetohen prej klientëve te pika e qasjes. (Ang. “Packet sniffing”). Në këtë detyrë, paketat i kemi marrë nga pika jonë e qasjes, dhe i kemi ruajtur në kompjuterin tonë. Këtë paketë e kemi deshifruar me anë të “Aircrack-ng” por e njëjta mund të bëhet me vegla për thyerje të fjalëkalimeve, si p.sh. “Hashcat”. Në [tabelën 2](#Tabela_2) kemi paraqitur disa komanda që përdoren shpesh në “Airodump-ng”.
* **“Aireplay-ng” –** u përdor për të bërë deautentifikimin e një klienti, por kjo vegël ka përdorime më të gjera, si p.sh. mund të bëjmë deautentifikimin e të gjithë klientëve që iu janë qasur pikës në mënyrën pa kabëll (“Wireless”). Me një rresht:

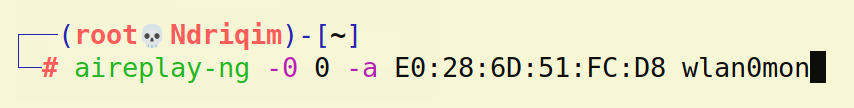


Figure 13 Deautentifikimi i çdo klienti nga pika e qasjes, këtu -0 tregon që po bëjmë deautentifikim, -a MAC adresa e pikës së qasjes dhe wlan0mon ndërfaqja e wireless

Siç shihet, kjo vegël është shumë e fuqishme për penguar njerëzit e tjerë. P.sh. ne mund të shkojmë në një kafene dhe të çrregullojmë çdo pikë qasjeje që të mos mund të përdoret nga askush. Kjo vegël ka edhe shumë përdorime të tjera, por që nuk mund t’i studijojmë të gjitha pasi ka shumë. Në [tabelën 3](#Tabela_3) kemi paraqitur modet e punës (sulmit) të “Aireplay-ng”.

## Tabela e komandave për “Airdump-ng”

|  |  |
| --- | --- |
| --ivs | Save only captured IVs |
| --gpsd | Use GPSd |
| --write <prefix> | Dump file prefix |
| -w | same as --write |
| --beacons | Record all beacons in dump file |
| --update <secs> | Display update delay in seconds |
| --showack | Prints ack/cts/rts statistics |
| -h | Hides known stations for --showack |
| -f <msecs> | Time in ms between hopping channels |
| --berlin <secs> | Time before removing the AP/client from the screen when no more packets are received (Default: 120 seconds) |
| -r <file> | Read packets from that file |
| -T | While reading packets from a file, simulate the arrival rate of them as if they were "live". |
| -x <msecs> | Active Scanning Simulation |
| --manufacturer | Display manufacturer from IEEE OUI list |
| --uptime | Display AP Uptime from Beacon Timestamp |
| --wps | Display WPS information (if any) |
| --output-format <formats> | Output format. Possible values: pcap, ivs, csv, gps, kismet, netxml, logcsv |
| --ignore-negative-one | Removes the message that says fixed channel <interface>: -1 |
| --write-interval<seconds> | Output file(s) write interval in seconds |
| --background <enable> | Override background detection. |
| -n <int> | Minimum AP packets recv'd before for displaying it |

Table 2 Komandat më të përdorura të "Airdump-ng" (Anglisht)

## Tabela e modeve për “Aireplay-ng”

|  |  |
| --- | --- |
| --deauth count | deauthenticate 1 or all stations (-0) |
| --fakeauth delay | fake authentication with AP (-1) |
| --interactive | interactive frame selection (-2) |
| --arpreplay | 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) |

Table 3 Modet e sulmit të "Aireplay-ng" (Anglisht)

# Përfundim

“Aircrack-ng” është një bashkësi veglash për sulme në rrjetat pa kabëll, pasi që ka shumë nënvegla, kjo e bën të gjithanshë, si dhe shumë të nevojshë për hakerët dhe testuesit e sigurisë. Pasi ka shumë vegla, në këtë detyrë jemi fokusuar më së shumti në gjetjen e fjalëkalimit të një rrjeti “Wireless”, sepse studimi i të gjithë veglës do të na merrte shumë kohë.

# Referencat

Vegla në tools.KaliLinux.org: [Aircrack-ng | Penetration Testing Tools (kali.org)](https://tools.kali.org/wireless-attacks/aircrack-ng)

Vegla në uebsaijtin zyrtar të “Aircrack-ng”: [Aircrack-ng (aircrack-ng.org)](https://www.aircrack-ng.org/)

Një tutorial që kam përdorur për gjetjen e fjalëkalimit të rrjetit: [Crack WPA/WPA2 Wi-Fi Routers with Aircrack-ng and Hashcat by Brannon Dorsey - (hakin9.org)](https://hakin9.org/crack-wpa-wpa2-wi-fi-routers-with-aircrack-ng-and-hashcat/)