**Universiteti i Prishtinës “Hasan Prishtina”**

**Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike**



Lënda: Siguria në Internet

Tema : Airolib-ng

Mentorë:                                                                                 Studentet:

Prof. Dr. Blerim Rexha                                                           Gresa Salihu     180718100004

Msc. Arbnor Halili                                                                Leonita Nika     180714100107

                                                                                                Mihrije Kadriu  180714100014

                                                               Prishtinë, 2021

**Permbajtja**

[**1.Hyrje** 3](#_Toc61290915)

[**1.1 Cka është airolib-ng?** 3](#_Toc61290916)

[**1.2 Cka është aircrack-ng?** 3](#_Toc61290917)

[**1.3 Si ta instalojmë Aircrack-ng?** 3](#_Toc61290918)

[**1.4 Pse e perdorim veglën Airolib-ng?** 4](#_Toc61290919)

[**2. Funksionaliteti i veglës Airolib-ng** 5](#_Toc61290920)

[**3. Testimet** 5](#_Toc61290921)

[**3.1 Testimi i komandës airolib-ng :** 10](#_Toc61290923)

[**3.3 Testimi i komandës –import :** 11](#_Toc61290925)

[**3.4 Testimi i komandave gedit dhe cat** 12](#_Toc61290926)

[**3.5 Testimi i komandes –batch** 13](#_Toc61290927)

[**3.6 Testimi i komandës --verify** 13](#_Toc61290928)

[**3.7 Testimi i komandës –stats** 14](#_Toc61290929)

[**3.8 Testimi i komandës --clean** 15](#_Toc61290930)

[**3.9 Testimi i komandës aircrack-ng – r <DB>** 16](#_Toc61290931)

[**4.Konkludimi** 17](#_Toc61290932)

[**5.Shtojca e figurave** 17](#_Toc61290933)

[**6.Referencat** 18](#_Toc61290934)

# **1.Hyrje**

## **1.1 Cka është airolib-ng?**

**Airolib-ng** është një vegël e Kali Linux e cila shërben për të ruajtur dhe menaxhuar listat e essid dhe fjalëkalimeve.Airolib-ng bënë pjesë në veglën e famshme të Kali Linux e cila është aircrack-ng.

## **1.2 Cka është aircrack-ng?**

**Aircrack-ng** është një tërësi mjetesh për të vlerësuar sigurinë e rrjetit WiFi.

Aircrack-ng përqendrohet në fusha të ndryshme të sigurisë WiFi:

* Monitorimi:

Mbledhja dhe eksportimi i të dhënave në skedarët e tekstit për përpunim të mëtejshëm nga mjetet e palëve të treta.

* Sulmi:

Rishikoni sulmet, çaktivizimin, pikat e rreme të qasjes dhe të tjerët përmes injeksionit të paketave.

* Testimi:

Kontrollimi i kartave WiFi dhe aftësive të driver-it (kapja dhe injeksioni).

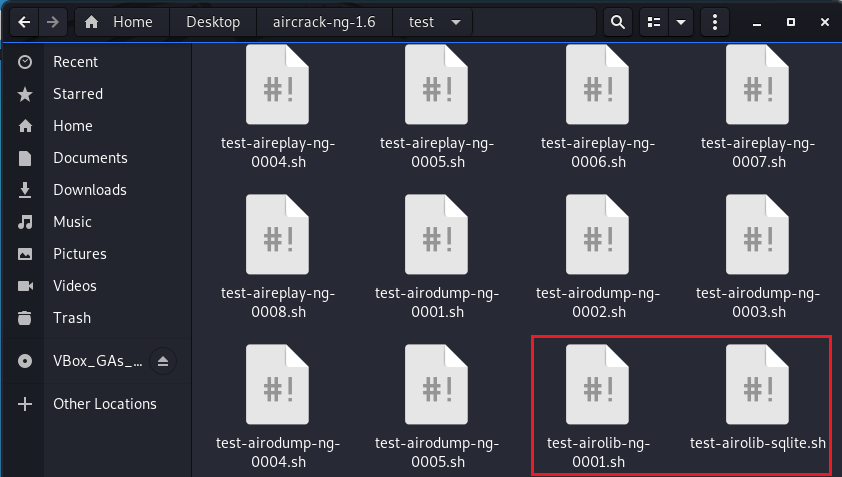
* Cracking:

WEP dhe WPA (WPA 1 dhe 2).

WEP(Wired Equivalent Privacy qëllimin kryesor ka mbrojtjen e përdoruesëve të WLAN nga përgjimet, si dhe të ndalojë hyrjet e paautorizuara në Wifi) dhe WPA(Wi-Fi Protected Access qellimin kryesor e ka te siguroje rrjetet kompjuterike wireless [[1](#_Referencat)] .

## **1.3 Si ta instalojmë Aircrack-ng?**

Supozojmë se kemi në dispozicion një sistem linux dhe kemi të instaluar package manager-in qe njihet me emrin pip. Procesi supozon që jemi perdorues me privilegje, në të kundërten përdorim komandën **sudo** [[2](#_Referencat)].

Airolib-ng është paraprakisht e instaluar brenda veglës Aircrack-n

sudo apt-get install aircrack-ng

Figure 1 Airolib-ng brenda veglës Aircrack-ng

Ndërsa për ta përdorur veglën Aircrack-ng përmes Sistemit Operativ Windows ne duhet të instalojm manualisht softuerin pasi që kjo vegël nuk është e instaluar paraprakisht .

Hapat që duhet të ndjekim për të instaluar veglën Aircrack-ng në Sistemin Operativ Windows :

-Shkarkoni në kompjuterin tuaj versionin më të fundit të kompletit Aircrack-ng për Windows.

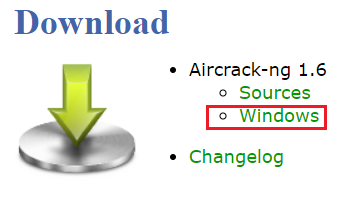


Figure 2 Instalimi i Aircrack-ng përmes Windows

- Kjo do të krijojë një direktori të quajtur "aircrack-ng-1.6-win". Ky emër i direktoriumit do të ndryshojë bazuar në versionin e saktë që kemi shkarkuar. Ky direktori kryesor përmban tre nëndirektori - "bin", "src" dhe "test” [[3](#_Referencat)] .

## **1.4 Pse e perdorim veglën Airolib-ng?**

**Airolib-ng** është një vegël e Kali Linux e cila shërben për të ruajtur dhe menaxhuar listat e ESSID (Extended Service Set Identification, që në thelb nënkupton emrin identifikues të rrjetit pa tel) dhe listat e fjalekalimeve , gjithashtu ajo shërben për të llogaritur çelësat kryesorë të tyre në çift (PMK) dhe t'i përdorë ato në WPA / WPA2 cracking. Sistemi i menaxhimit të bazës së të dhënave i përdorur nga ky program është SQLite3 si mekanizëm ruajtjeje i cili është i disponueshëm në shumicën e platformave. Baza e të dhënave SQLite3 u zgjodh duke marrë parasysh disponueshmërinë e platformës plus menaxhimin, kujtesën dhe madhësinë e diskut [[1](#_Referencat)].

WPA/WPA2 cracking përfshin llogaritjen e çelësit kryesor çift, nga i cili rrjedh çelësi kalimtar privat (PTK). Duke përdorur PTK-në, ne mund të llogarisim kodin e identitetit të mesazhit kornizë (MIC) për një paketë të caktuar dhe potencialisht do të gjejmë që MIC të jetë identike me paketën, kështu që PTK do ishte e saktë, prandaj edhe PMK do te ishte e saktë [[4](#_Referencat)].

Llogaritja e PMK është shumë e ngadaltë pasi që përdor algoritmin pbkdf2(Password-Based Key Derivation Function). Megjithatë, PMK-ja është gjithmonë e njëjtë për një kombinim të dhënë ESSID dhe fjalëkalimi. Kjo na lejon të para-llogarisim PMK-në për kombinimet e dhëna dhe të shpejtojmë cracking(thyerjen) e wpa / wpa2 handshake. Testet kanë treguar se përdorimi i kësaj teknike në aircrack-ng mund të kontrollojë më shumë se 50 000 fjalëkalime në sekondë duke përdorur tabelat e para-llogaritura PMK gje e cila e bene Airolib-ng nje nder mjetet me te perdorura te Aircrack-ng [[2]](#_Referencat)

Llogaritja e PMK-së ende kërkohet, megjithatë ne mund të: llogarisim ate me perpara për përdorim të mëvonshëm ose të përbashkët.

# **2. Funksionaliteti i veglës Airolib-ng**

Përdorimi: **airolib-ng <database> <operation> [options]**

-***database*** është emri i fajllit të bazës së të dhënave .

*-****operation*** specifikon veprimin që dëshironi të ndërmerret në bazën e të dhënave.

-***options*** mund të kërkohen në varësi të operacionit të specifikuar

Disa nga komandat e Airolib-ng :

**-- stats** : Informacioni dalës në lidhje me bazën e të dhënave.

**-- sql <sql>:** Për ekzekutim të deklaratës së specifikuar SQL.

**-- clean [all]:** Pastroni bazën e të dhënave të vjetra . 'all’ do gjithashtu zvogëloni madhësinë e fajllit nëse është e mundur dhe kryeni një kontroll të integritetit.

**-- batch**: Filloni të përpunon të gjitha kombinimet e ESSID dhe fjalëkalimet.

**-- verify [all]:** Verifikoni një grup PMK të zgjedhura rastësisht. Nëse jepet 'all’, të gjitha PMK-të e pavlefshme do të fshihen.

**-- import [eseid | passwd] <file >**: Importoni një tekst fajll si një listë e ESSID ose fjalëkalimeve.

-**- import cowpatty**<file >: Importo një cowpatty fajll. CoWPAtty është një mjet i komandës që është i instaluar paraprakisht në Kali Linux dhe shërben për automatizim të sulmit të fjalorit për WPA-PSK.

-- **export cowpatty**<essid> <file> : Eksporto në një cowpatty fajll[.[3]](#_Referencat)

# **3. Testimet**

Si fillim për të kryer testimet e komandave të veglës Airolib-ng në makinën Virual Box , ne duhet që të konektojmë një wifi adapter me sistemin operativ kali linux.

Wifi adapteri që e kemi perdorur gjatë testimeve :



Figure 3 Wifi Adapter

Për konektimin e wifi adapterit me Sistemin Operativ Kali Linux duhet të kalojmë në disa hapa :

1. Hapi1 për konektimin e Wifi Adapter

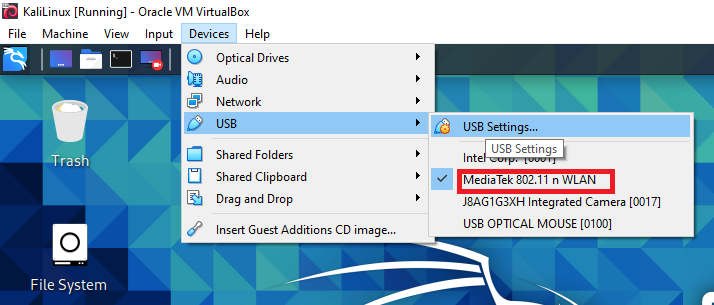


Figure 4 Hapi 1 për konektimin e Wifi Adapter

1. Hapi2 për konektimin e Wifi Adapter

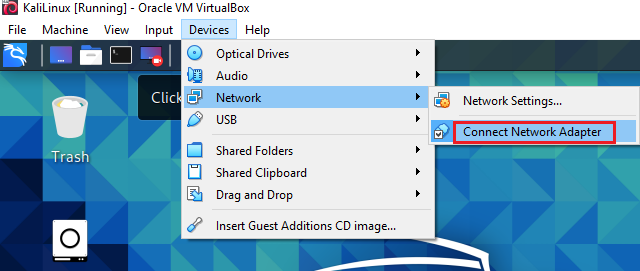


Figure 5 Hapi 2 për konektimin e Wifi Adapter

## **3.1 Ekzekutimi i komandave**

Komanda airmon-ng na jep të gjitha network interface card (NIC) . Dhe përmes komandës

airmon-ng start wlan0

mundësohet startimi i monitor mode qe i mundëson një pajisje me network interface controller për të monitoruar të gjithë trafikun e marrë nga wireless network .

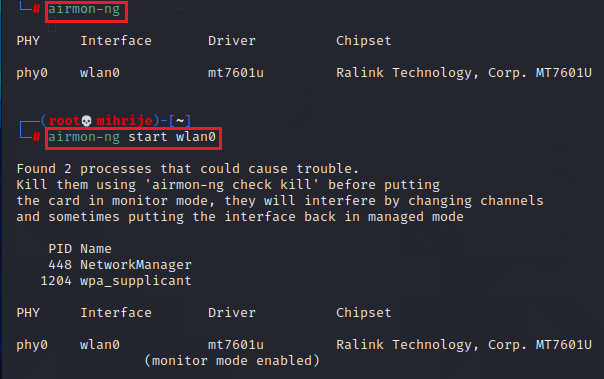


Figure 6 Testimi i komandës airmon-ng

Ndërsa përmes ekzekutimit të komandës

airodump-ng wlan0

Shfaqen të gjitha wireless që gjenden në rrethinën tonë.  
Qëllimi kryesor i komandës airdump-ng është ta zë handshake dhe përmes kësaj ta sulmojmë   
 përmes dictionary attack.

## 

Figure 7 Testimi i komandës airodump-ng wlan0

Për të marrë VPN handshake ky duhet të monitoroj një interface të caktuar( e monitoron kush do të lidhet në të ) .  
Monitorimin e bëjmë përmes kësaj komande:

airodump-ng -c 1 - - bssid 3E:A4:B7:13:89:94 –w ~/Desktop/wlan0

Në këtë komandë 1 paraqet kanalin e networkut të targetuar ndërsa 3E:A4:B7:13:89:94 paraqet BSSID e networkut.   
Ky fillon të kapë paketat që ndodhen në networkun e targetuar.

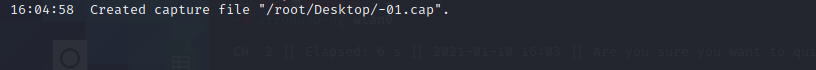
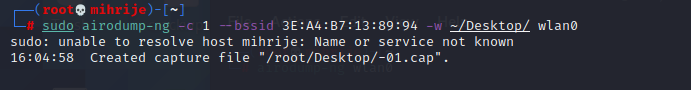


Figure 8 Testimi i komandës airodump-ng në networkun e targetuar

Përmes kësaj komande bëhet e mundur që të kapet një handshake në network dhe rezultati do të ruhet në fajllin e krijuar -01.cap .

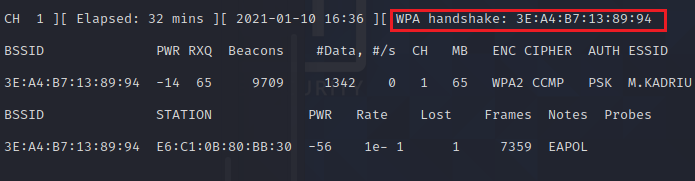


Figure 9 WPA handshake

Nga kjo figurë shihet se është gjetur një WPA handshake në networkun 3E:A4:B7:13:89:94 .Ky handshake do të na ndihmoj për gjetjen e fjalëkalimit.

* Komanda që mundëson gjetjen e fjalëkalimit :

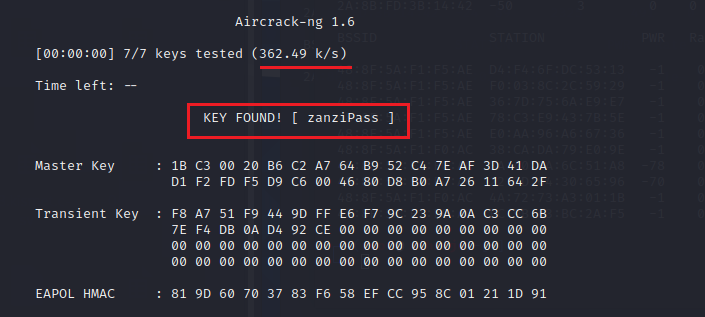
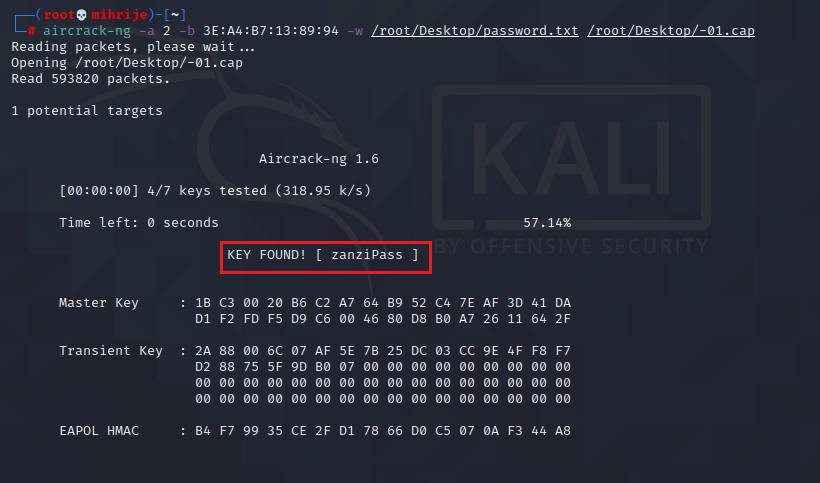


Figure 10 Gjetja e fjalëkalimit

Në rastin kur kemi shumë fjalëkalime në bazën e të dhënave:

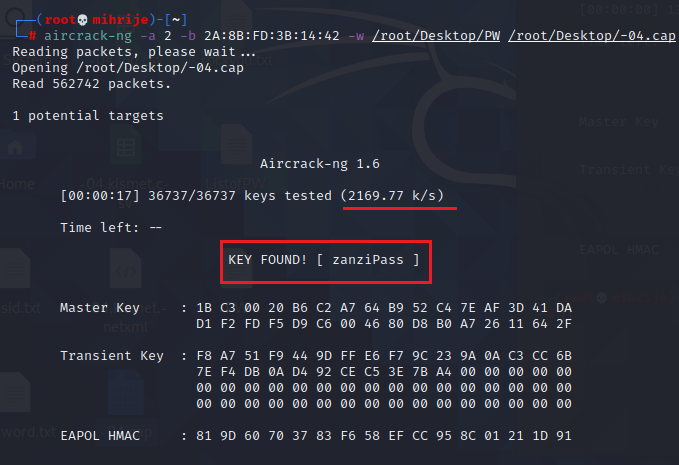


Figure 11 Gjetja e fjalëkalimit ne testimin 2

## **3.1 Testimi i komandës airolib-ng :**

Kjo komandë do të kthej si përgjigje opsionin help të veglës airolib-ng :

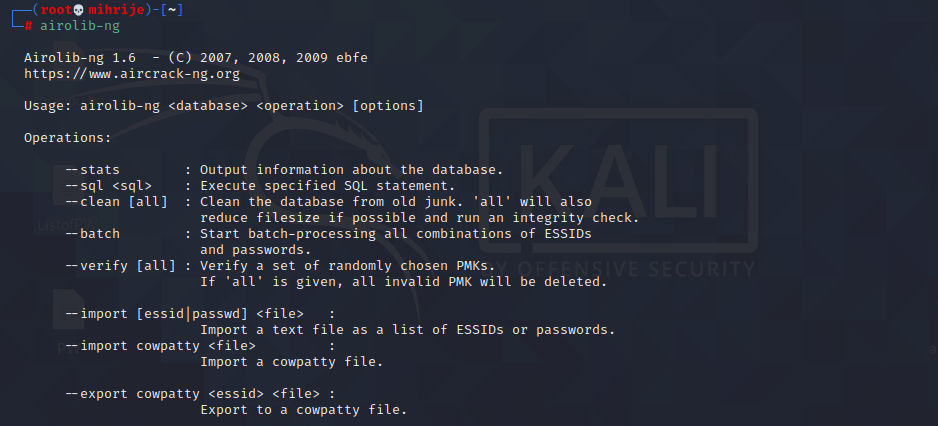


Figure 12 Testimi i komandës airolib-ng

## **3.3 Testimi i komandës –import :**

airolib-ng crackwpa –-import essid essid.txt

* crackwpa është emri i databazës që do të krijohet
* --import operacioni që do të kryhet
* essid paraqet listën e essid-ve
* essid.txt fajll që përmban essid-të

Sistemi do të kthej këtë përgjigje:

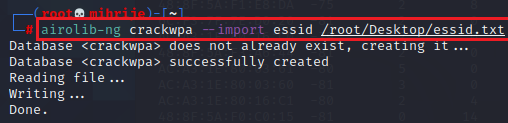


Figure 14 Testimi i komandës --import

Që nënkupton se databaza nuk ekziston paraprakisht por krijohet në momentin kur ekzekutohet kjo komandë,njëkohësisht mundësohet edhe leximi i fajllit te essid.txt si dhe importimi i këtyre të dhënave në databazën e sapo krijuar .[[1]](#_Referencat)

Databaza e krijuar:

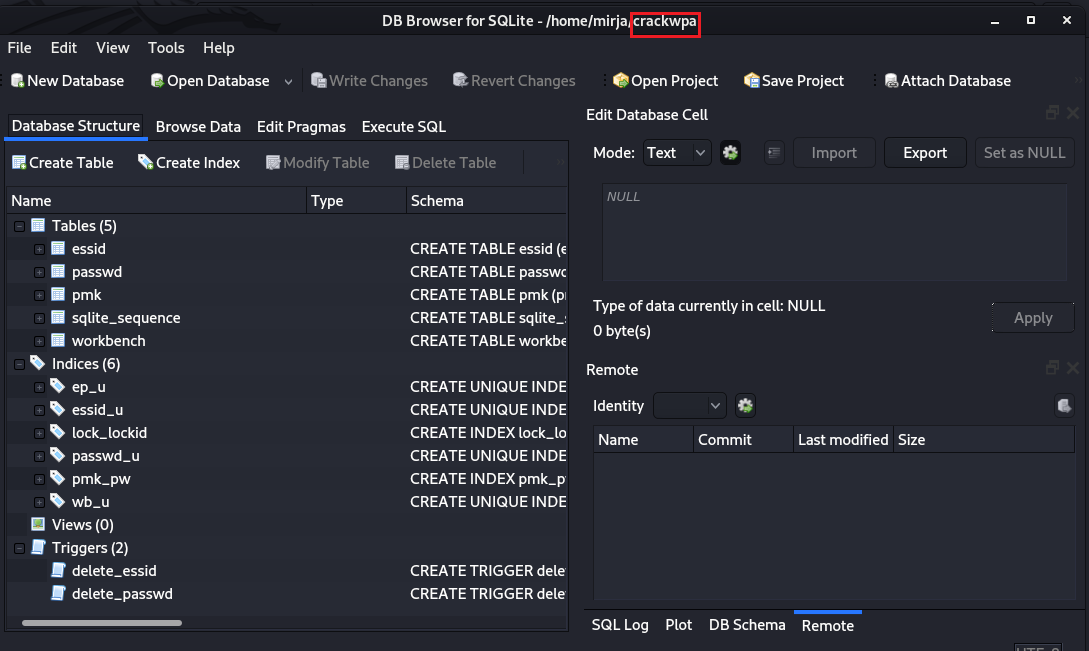


Figure 15 Krijimi i databazës crackwpa

Hapja / krijimi i një baze të të dhënave nuk funksionon kur airolib-ng është në direktorium që përmbajnë karaktere speciale si 'ç', 'é', 'è', 'à',’ë’.  
Zgjidhja për këtë problem është që të zhvendosim airolib-ng dhe bazën e të dhënave në një direktorium tjetër pa këto karaktere speciale.

airolib-ng crackwpa –-import passwd password.txt

* crackwpa është emri i databazës
* --import operacioni që do të kryhet
* passwd paraqet listën e fjalëkalimeve
* password.txt fajll që permban fjalëkalimet

Sistemi do të kthej këtë përgjigje:

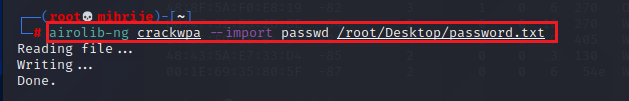


Figure 16 Testimi i komandes --import passwd

Që nënkupton se ekzekutimi i kesaj komande do të mundësoj leximin e fajllit password.txt si dhe importimin e të gjitha fjalëkalimeve në bazën e të dhënave crackwpa .[[4](#_Referencat)]

## **3.4 Testimi i komandave gedit dhe cat**

gedit essid.txt

* gedit është komandë e linux që shërben për krijimin dhe editimin e fajllave
* essid.txt fajll që në këtë rast editohet përmes komandës gedit

dhe

cat essid.txt

* cat është komandë e linux që shërben për leximin e fajllit dhe në dalje jep përmbajtjen e tij
* essid.txt fajll që në këtë rast lexohet përmes komandës cat [[2]](#_Referencat)

Sistemi do të kthej këtë përgjigje:



Figure 17 Testimi i komandave gedit dhe cat

## **3.5 Testimi i komandes –batch**

airolib-ng crackwpa --batch

* crackwpa është emri i databazës
* --batch operacioni që do të kryhet (përpunon të gjitha kombinimet e ESSID dhe fjalëkalimeve)

Sistemi do të kthej këtë përgjigje:

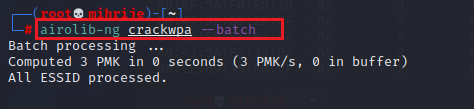


Figure 18 Testimi i komandës --batch

## **3.6 Testimi i komandës --verify**

Airolib-ng crackwpa --verify

* crackwpa është emri i databazës
* --verify operacioni që do të kryhet(verifikon një grup PMK të zgjedhur)

Sistemi do të kthej këtë përgjigje:

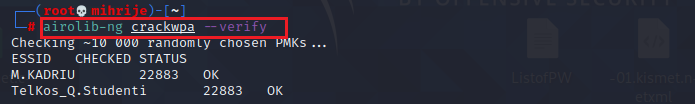


Figure 19 Testimi i komandës --verify

Nëse duam të verifikojmë të gjitha PMK-të atëherë duhet ta ekzekutojm komandën :

Airolib-ng crackwpa –verify all

* crackwpa është emri i databazës
* --verify all operacioni që do të kryhet(verifikon të gjitha PMK-të)

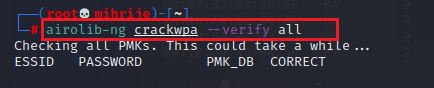


Figure 20 Testimi i komandës --verify all

## **3.7 Testimi i komandës –stats**

airolib-ng crackwpa –stats

* crackwpa është emri i databazës
* --stats është operacioni që do të kryhet(jep informacionin dalës në lidhje me bazën e të dhënave)

Sistemi do të kthej këtë përgjigje:

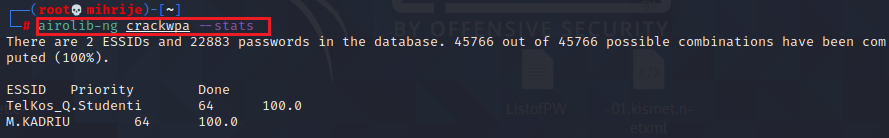


Figure 21 Testimi i komandës --stats

Që nënkupton se në databazën e krijuar me emrin crackwpa gjithsej janë 2 ESSIDs dhe 22883 fjalëkalime ku gjithsej kemi llogaritjen e 45766 nga 45766 kombinimeve të mundshme .

## **3.8 Testimi i komandës --clean**

airolib-ng crackwpa –clean

* crackwpa është emri i databazës
* --clean operacioni që do të kryhet (pastron bazën e të dhënave )

Sistemi do të kthej këtë përgjigje:

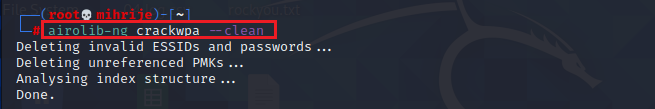


Figure 22 Testimi i komandës –clean

Nëse duam që të zvogëlojm madhësinë e fajllit dhe të kryejm një fshirje bazike ekzekutojmë komandën:

airolib-ng crackwpa –clean all

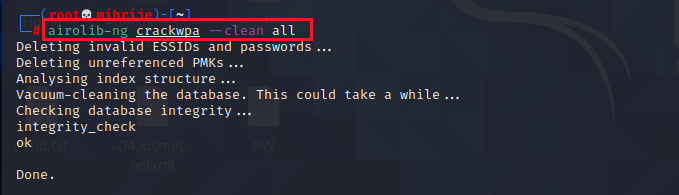


Figure 23 Testimi i komandës --clean all

* crackwpa është emri i databazës
* clean all operacioni që do të kryhet (pastron bazën e të dhënave duke

e zvogëluar madhesinë e fajllit)

## **3.9 Testimi i komandës aircrack-ng – r <DB>**

aircrack-ng –r crackwpa -01.cap

* -r path te databaza airolib-ng
* crackwpa është emri i databazës
* -01.cap përmban paketën e kapur të network-ut të targetuar

Në rastin kur kemi pak fjalëkalime:

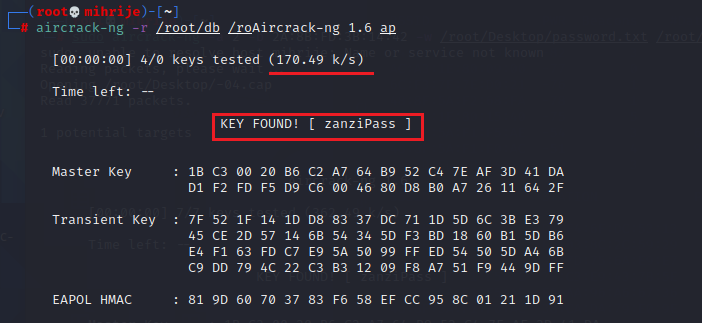


Figure 24 Testimi i komandës aircrack-ng -r <DB>

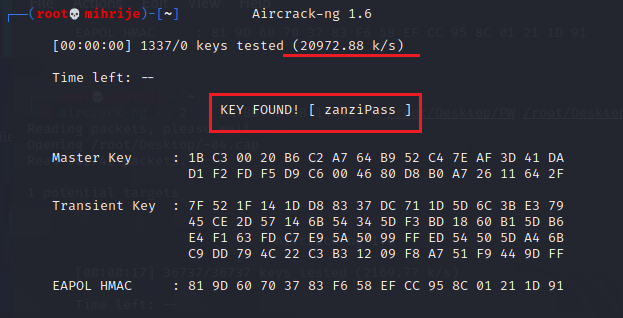


Figure 25 Gjetja e fjalëkalimit më shpejt përmes komandës aircrack-ng -r <DB>

Pra, përdorimi i kësaj komande ndikon dukshëm në shpejtesinë e gjetjes së fjalekalimit.

# **4.** **Konkludimi**

Ne mësuam të instalojmë aircrack-ng në sistemet operative Linux dhe Windows si dhe të përdorim airolib-ng, mirëpo një paknaqësi që shfaqet nga ana e shfrytëzuesit është se për të punuar Aircrack-ng në Virtual Box duhet të perdorim WiFi adapter të jashtëm .

Në këtë dokument ne i kushtuam rëndësi të vecantë veglës Airolib-ng e cila ruan ESSID dhe listën me password-a në databazë gjë që e ndihmon veglën Aircrack-ng duke rritur shpejtesinë e auditimit te Wireless Security ose për të thyer fjalëkalimet e harruara.   
Ekzistojnë disa mjete të tjera të ngjashme në dispozicion për këtë qëllim por aircrack-ng me ndihmën e airolib-ng dhe mjeteve të tjera brenda paketës së tij është më i njohur për mbështetje të mirë, shkathtësi dhe saktësi në realizimin e qëllimit të tij.

# **5. Shtojca e figurave**

[Figure 1 Airolib-ng brenda veglës Aircrack-ng 3](#_Toc61296181)

[Figure 2 Instalimi i Aircrack-ng përmes Windows 4](#_Toc61296182)

[Figure 3 Wifi Adapter 5](#_Toc61296183)

[Figure 4 Hapi 1 për konektimin e Wifi Adapter 6](#_Toc61296184)

[Figure 5 Hapi 2 për konektimin e Wifi Adapter 6](#_Toc61296185)

[Figure 6 Testimi i komandës airmon-ng 7](#_Toc61296186)

[Figure 7 Testimi i komandës airodump-ng wlan0 8](#_Toc61296187)

[Figure 8 Testimi i komandës airodump-ng në networkun e targetuar 8](#_Toc61296188)

[Figure 9 WPA handshake 9](#_Toc61296189)

[Figure 10 Gjetja e fjalëkalimit 9](#_Toc61296190)

[Figure 11 Gjetja e fjalëkalimit ne testimin 2 10](#_Toc61296191)

[Figure 12 Testimi i komandës airolib-ng 10](#_Toc61296192)

[Figure 14 Testimi i komandës --import 11](#_Toc61296193)

[Figure 15 Krijimi i databazës crackwpa 11](#_Toc61296194)

[Figure 16 Testimi i komandes --import passwd 12](#_Toc61296195)

[Figure 17 Testimi i komandave gedit dhe cat 13](#_Toc61296196)

[Figure 18 Testimi i komandës --batch 13](#_Toc61296197)

[Figure 19 Testimi i komandës --verify 13](#_Toc61296198)

[Figure 20 Testimi i komandës --verify all 14](#_Toc61296199)

[Figure 21 Testimi i komandës --stats 14](#_Toc61296200)

[Figure 22 Testimi i komandës –clean 15](#_Toc61296201)

[Figure 23 Testimi i komandës --clean all 15](#_Toc61296202)

[Figure 24 Testimi i komandës aircrack-ng -r <DB> 16](#_Toc61296203)

[Figure 25 Gjetja e fjalëkalimit më shpejt përmes komandës aircrack-ng -r <DB> 16](#_Toc61296204)

# **6. Referencat**

[1] [https://www.aircrack-ng.org/doku.php?id=airolib-ng](https://meet.google.com/linkredirect?authuser=0&dest=https%3A%2F%2Fwww.aircrack-ng.org%2Fdoku.php%3Fid%3Dairolib-ng)

[2] http://www2.aircrack-ng.org/hiexpo/aircrack-ng\_book\_v1.pdf

[3] [https://tools.kali.org/wireless-attacks/airolib-ng](https://meet.google.com/linkredirect?authuser=0&dest=https%3A%2F%2Ftools.kali.org%2Fwireless-attacks%2Fairolib-ng)

[4] [https://www.youtube.com/watch?v=TsJG-6kBPeE](https://meet.google.com/linkredirect?authuser=0&dest=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DTsJG-6kBPeE)