**Lënda: “Sigurimi i informacionit”**

**Profesori i lëndës:** Prof. Dr. Blerim Rexha

**Niveli:** Master, “Inxhinieri kompjuterike”

**Studenti:** Albulenë Mushica

Wifi Honey Package

Qëllimi

Përshkrimi dhe demonstrimi i Wifi Honey Package duke përdorë Kali Linux.

Përmbajta

[Hyrja 2](#_Toc59573791)

[Kali Linux 2](#_Toc59573792)

[Përshkrimi i skriptës Wifi Honey 2](#_Toc59573793)

[Demonstrimi ne Kali Linux 2](#_Toc59573794)

[Konkludimi 6](#_Toc59573795)

[Bibliografia 7](#_Toc59573796)

# Hyrja

Në këtë dokument do te shpjegohet përdorimi dhe funksioni i skriptës Wifi Honey, si dhe përdorimi i komandave në Kali Linux.

# Kali Linux

Kali Linux është distribuim i Linux-it me bazë Debian i cili ka për synim advanced penetration testing dhe security auditing. Kali Linux për herë të parë u lancua në 13 mars të vitit 2013, si një rindërtim nga lartë-poshtë i BackTrack Linux, duke iu përshtatur standardve të zhvillimit të Debian-it.

Kali Linux përmbanë disa qindra tools (ang. mjete) të cilat kanë për qëllim apo detyra kryesore hulumtimin e sigurisë në nivele të ndryshme. Një nga ato është edhe Wifi Honey, e që sa i përket paisjeve wireless, Kali Linux është i ndërtuar në atë formë që ti përkrahë një rreth sa më të gjerë të tyre.

Disa nga tasqet më të përdorura që përfshihen në Kali Linux:

* Mbledhja e informacionit: mbledhja e të dhënave në lidhje me rrjetin dhe strukturën e targetit, identifikimi i kompjuterëve, sistemeve operative dhe shërbimet që i përdorin.
* Analizimi i dobësive: testimi i shpejtë i sistemeve, për të parë nëse kanë konfigurime të pasigurta.
* Analizimi i Ueb Aplikacioneve: identifikimi i konfigurimeve të gabuara dhe dobësitë e sigurisë.
* Vlerësimi i bazës së të dhënave: prej SQL injections deri te sulmi i kredencialeve, janë ndër sulmet më të zakonshme.
* Sulmet e fjalëkalimeve: përdoren mjete online dhe offline për sulme ndaj sistemeve të enkriptimit.
* Sulmet e wireless-it: meqë rrjetet wireless janë më të përahapurat, kjo i bën ato një target të zakonshëm. Kali Linux ka zgjedhje të shumta për këtë lloj sulmi.

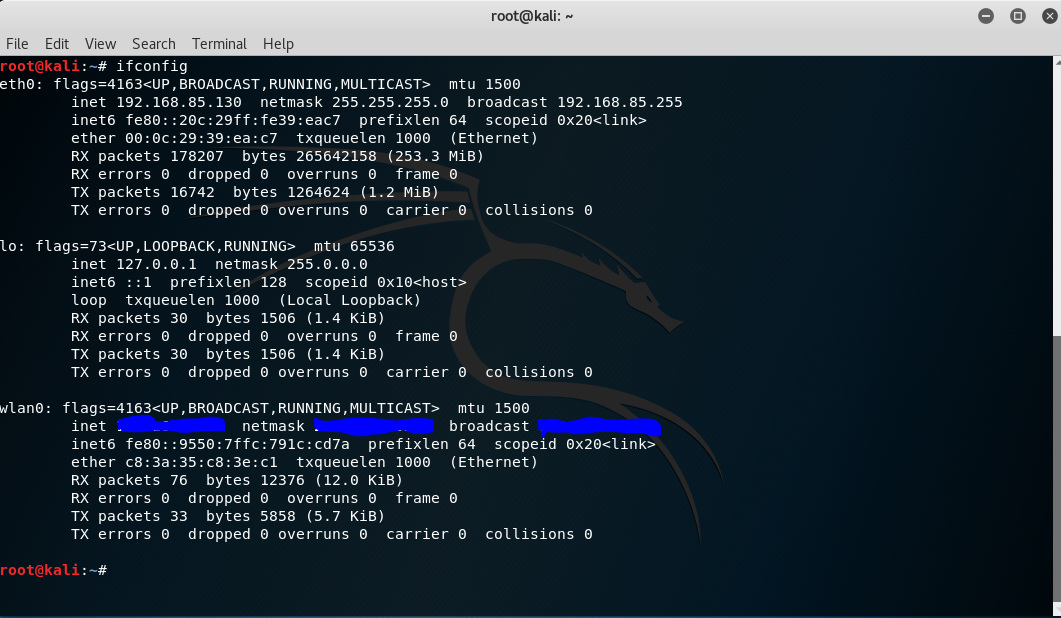
# Përshkrimi i skriptës Wifi Honey

Skripta e wifi honey krijon pesë ndërfaqe në modin e monitorimit, katër prej tyre përdoren si access points APs (të cilat janë paisje harduerike që lejojnë paisjet e tjera Wi-Fi të lidhen në rrjet), kurse e pesta përdoret për airodump-ng.

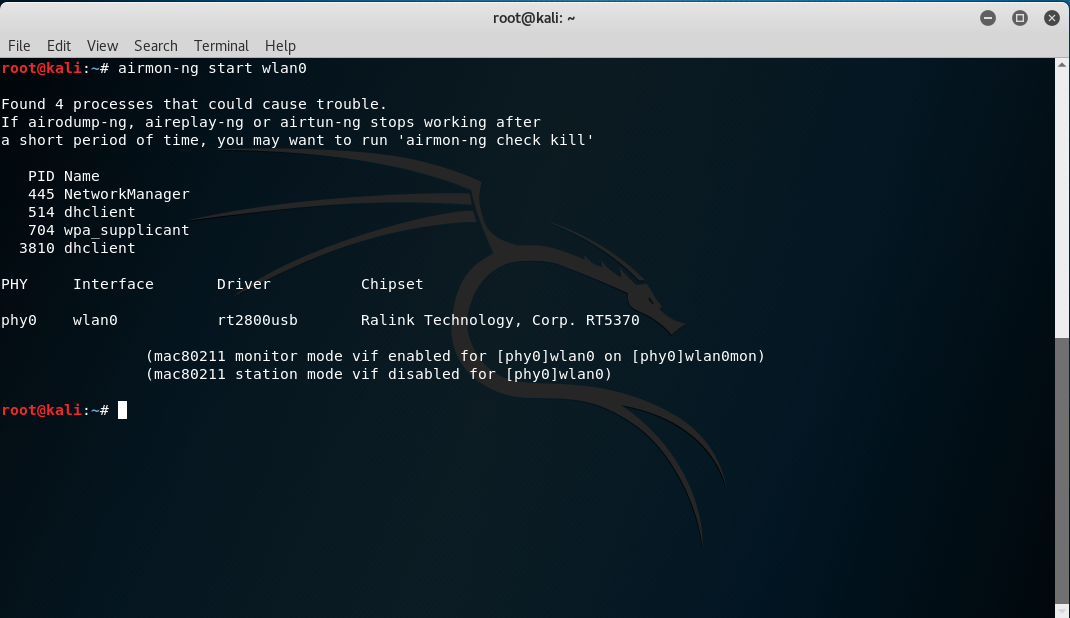
# Demonstrimi ne Kali Linux

Për ekzekutimin dhe përdorimin e skriptës Wifi Honey në Kali Linux, duhen përdorë komanda e këtij sistemi operativ.

Meqenëse kjo skriptë ka për qëllim të sulmojë ndërfaqet e rrjetit, fillimisht përdorim komandën **“ifconfig”** mund të përdoret për të caktuar ndonjë adresë, konfigurimin apo shfaqje të informacionit të rrjetit dhe duhet të përdoret në fillimin e sistemit për të përcaktuar adresën e rrjetit të secilës ndërfaqe të pranishme në një makinë.

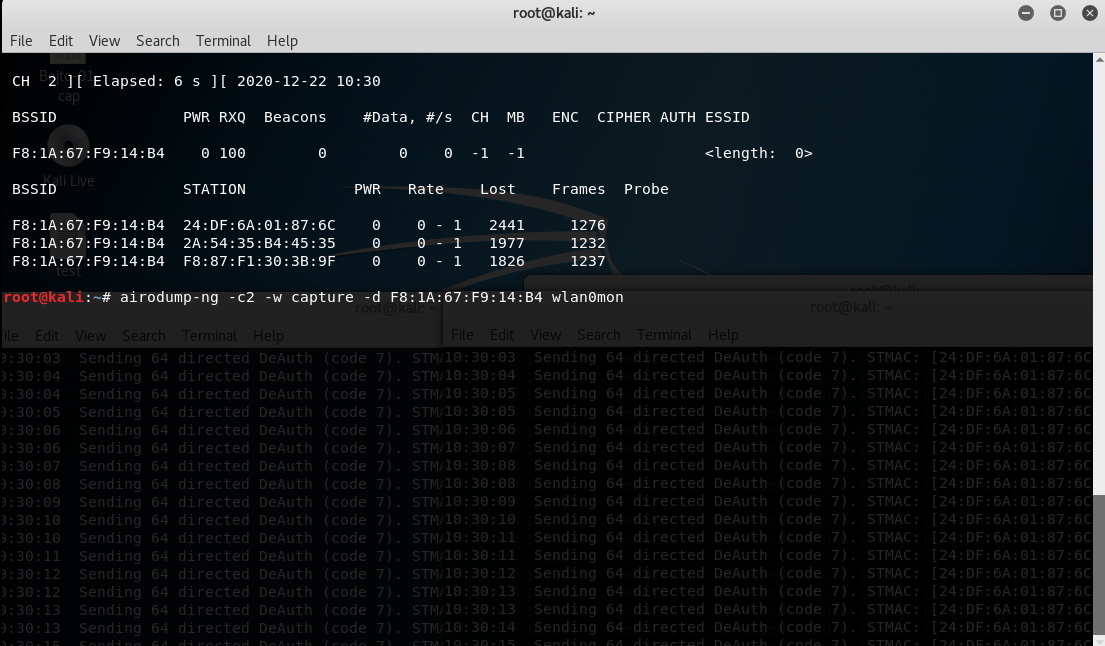


Pas, ifconfig ku shohim ndërfaqen wlan0 vjen komanda **“airmon-ng start wlan0”,** e cila ndërron modin e ndërfaqes nga Managed Mode në Monitoring Mode, në mënyrë që të mund të skanojmë për të gjitha paisjet lokale që tentojnë të lidhen në router-at lokalë.

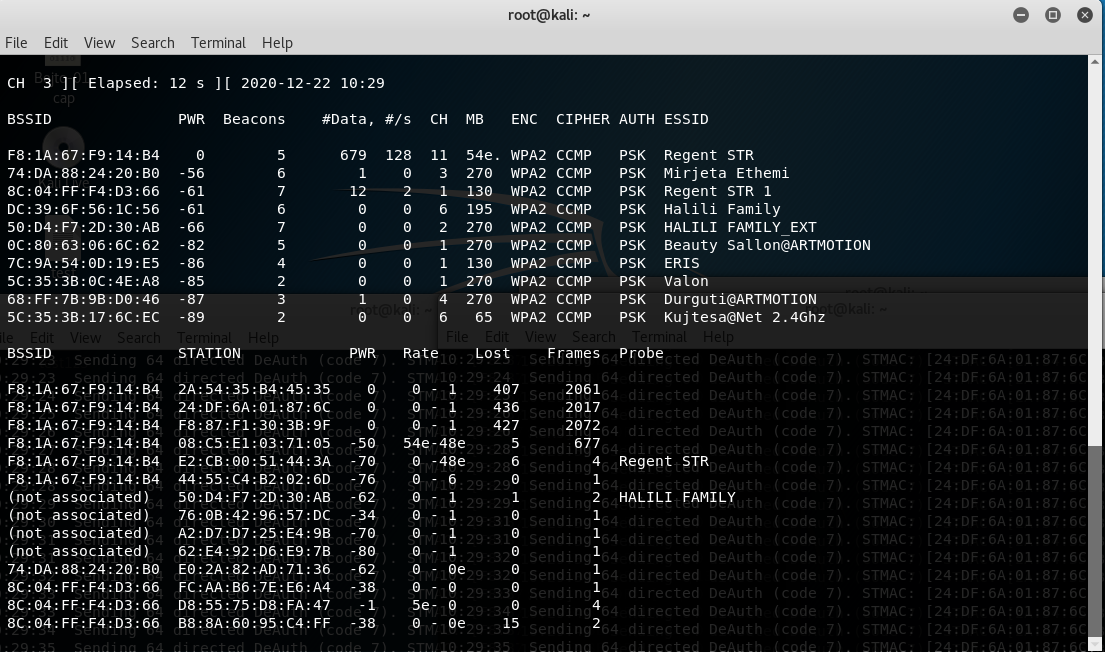


Meqë tani jemi në Monitoring Mode, fillojmë me skanimin e rrjetit duke përdorë komandën

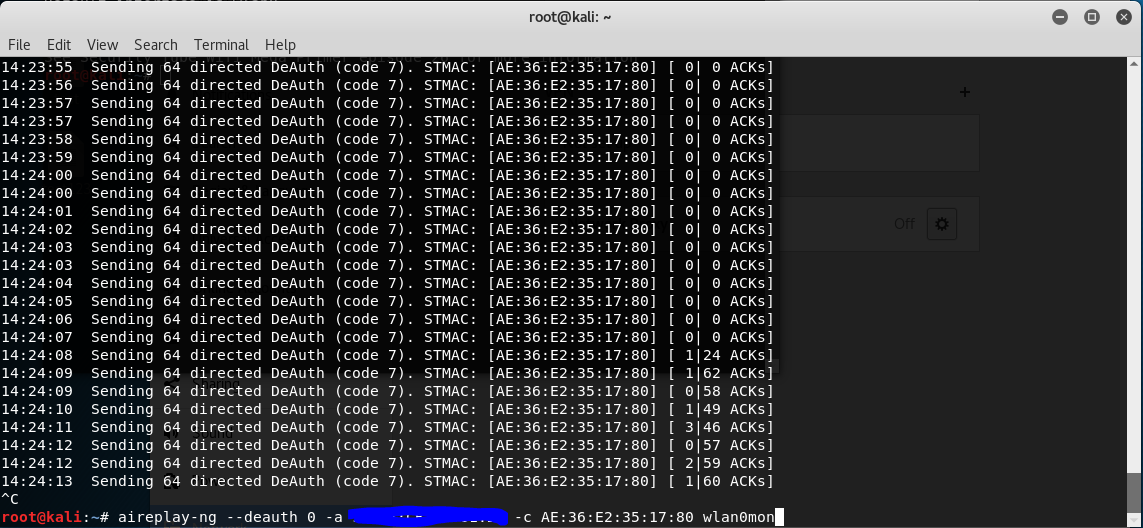
**“airodump-ng wlan0mon”.** Airodump-ng përdoret për të kapur paketat në ndërfaqen e monitorimit, ky proces ndryshe njihet si Channel Hopping, për shkak të ndryshimit të kanaleve, dhe sepse provon ti gjejë paisjet që përpiqen të lidhen në të gjitha APs, pa marrë parasysh në cilin kanal janë. Më poshtë mund ti shohim të listuara të gjitha ESSID e skanuara me të dhënat tjera si BSSID, CH që do ti përdorim në hapat e ardhshëm.



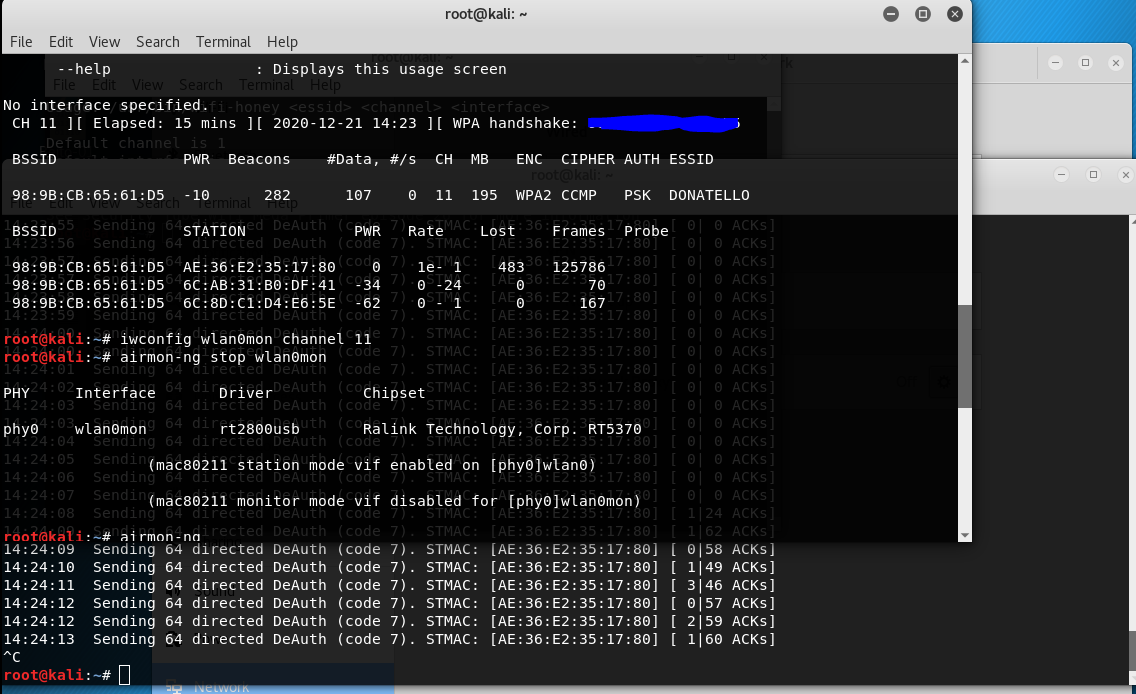
Tani pasi shohim BSSID që po transmetohet për secilën paisje duke zbuluar AP e tyre dhe për secilën kemi stacionet/klientët, ne zgjedhim kanalin që na intereson duke defiltruar gjithëcka tjetër dhe këtë e arrijmë përmes komandës **“airodump-ng -c2 -w capture -d F8:1A:67:14:B4 wlan0mon”.** Ku -c është tagu i kanalit, -w është tagu për të shkruar paketën e kapur në një fajll të quajtur “capture”, pastaj specifikohet BSSID dhe në fund ndërfaqja.



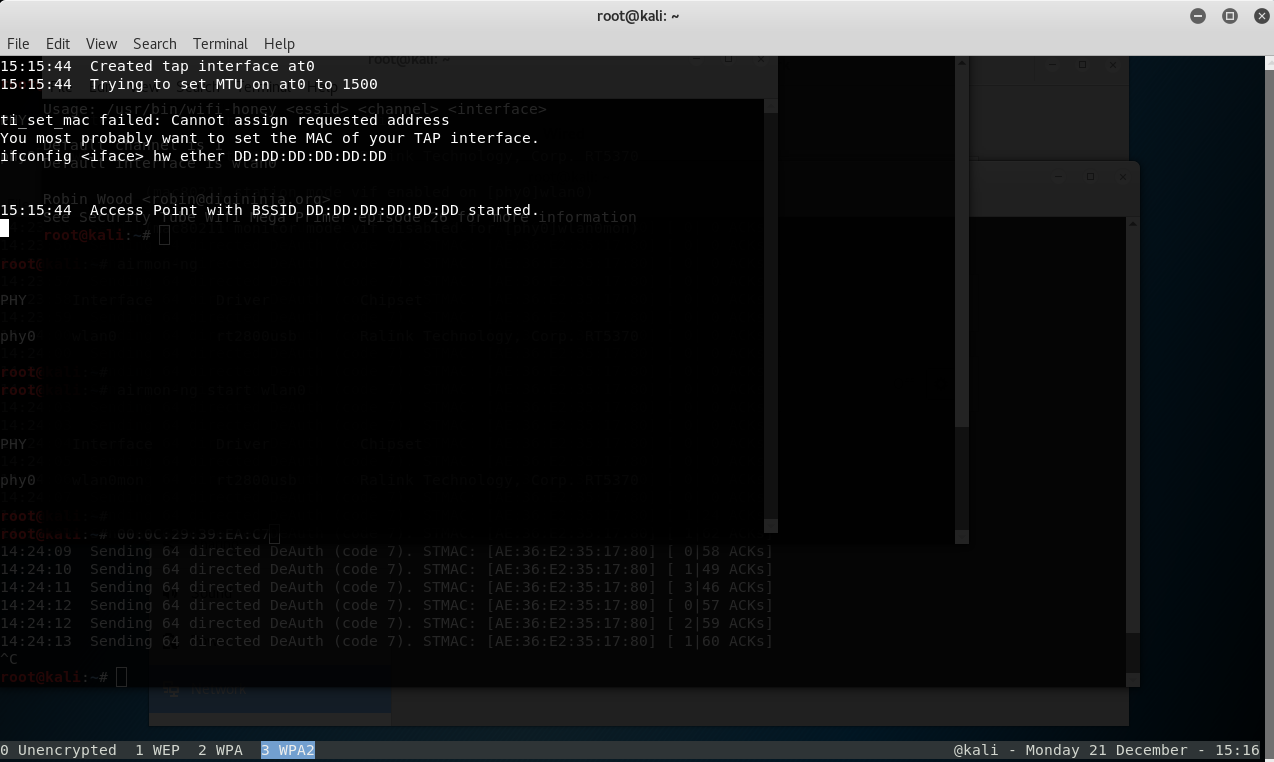
Qëllimi jonë është të largohet stacioni apo secila pasije tjetër e lidhur në këtë AP, në mënyrë që të ju duhet të lidhen prapë, kjo do të na mundësojë neve të kapim handshake (SYN-SYN-ACK, konfirmimi i identiteve në sisteme duke i lejuar atyre komunikimin) e rilidhjes. Për ta larguar klientin nga rrjetu, duhet së pari të deautentifikojmë, e kjo arrihet përmes komandës **“aireplay-ng –deauth 0 -a BSSID -c STATION wlan0mon”.**



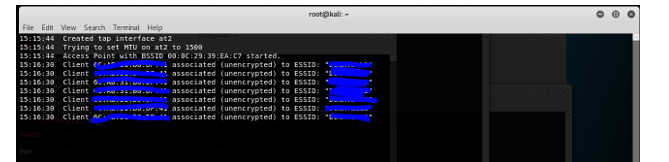
Pasi ti dërgojmë paketat e deautentifikimit te klienti, presim për të parë nëse ky proces ka sukese dhe kjo arrihet me paraqitjen e WPA handshake sic është paraqitë në figurën më poshtë.



Pasi të kapim handshake, japim komandën **“/usr/bin/wifihoney (emri i AP) kanali wlan0mon”** dhe shohim se Wifi Honey ka startuar dhe shihet se ka krijuar tre Aps.



Kurse ne foton më poshtë shohim se host-et që janë lidhë në AP e krijuar nga skripta Wifi Honey.



# Konkludimi

Kali Linux është një prej mjeteve më të sofistikuara të auditimit të sigurisë, sepse është shumë i fuqishëm dhe i përshtatshëm, Zgjedhja e mjeteve të Kali Linux, do të varet gjithëmonë prej qëllimit të detyrës apo synimeve e projektit aktual, ani pse ofron paketë komplete të mjeteve për secilen fazë të testimit. Sidoqofte, këto mjete jane të ndaluara të përdoren në rrjete, pa leje.

# Bibliografia

* Linux Security Blog

<https://linuxsecurityblog.com/2019/10/29/crack-wpa-handshake-using-aircrack-with-kali-linux/>

* Wifi Honey Package Description

<https://tools.kali.org/wireless-attacks/wifi-honey>

* Kali Linux Documentation

<https://www.kali.org/docs/>