Author by XEL # xel.white@gmail.com

Az aircrack-ng használata

0x0 Tartalom

0x1 Bevezető

Az aircrack-ng egy wireless auditing tool, mellyel a wireless hálózatok (IEEE 802.11 a/b/g/n) biztonsága tesztelhető, de akár fel is törhető. Ez az egyik legprofesszionálisabb programcsomag mely a dinamikus fejlesztése mellett több platformon is elérhető. Ebben a leírásban az aircrack-ng alapvető használatát prezentálom. A későbbiek folyamán élesben is megmutatom hogyan használható vezetéknélküli hálózatok kulcsainak visszafejtésére, de ez a leírás csupán a program használatára és annak alapvető funkcióira koncetrál.
Fontos megjegyezni, hogy a program fő funkciói csak az általa támogatott vezetéknélküli hálózati eszközök használata esetén lehetséges.

0x2 Telepítés

Az aircrack-ng honlapja az alábbi linken található: http://www.aircrack-ng.org
Az általa támogatott wireless hálózati eszközök itt megtekinthetők: http://www.aircrack-ng.org/doku.php?id=compatibility_drivers

Multiplatformos programról beszélünk, ami azt jelenti, hogy több rendszeren is elérhető. Futtatható Microsoft Windows és Linux operációs rendszereken is egyaránt. Azt azonban ki kell emelnem, hogy Linux alatt sokkal több hálózati kártya használható injectációra mint Windowson.

Mi is az az injectáció? Injectációnak nevezzük amikor egy hálózati forgalomba csomagokat szúrunk be, forgatunk vissza.

Telepítés Microsoft Windows operációs rendszerre

Ahhoz, hogy az aircrack-ng programot használni tudjuk Windows rendszerünkön, még telepítésre sincs szükség, csupán meg kell látogatnunk az aircrack-ng oldalát, letöltenünk a legfrissebb stabil verziót Windows alá, majd a letöltött .zip állományt ki kell csomagolnunk. Ha ezt megtettük akkor az aircrack-ng/bin mappában találhatók a futtatható fájlok, mellyek használatra készek.

Telepítés Linux operációs rendszerre

Linux alá többféle képpen telepíthetjük a programot. Ha olyan disztribúciót használunk, melynek a repositoryjában megtalálható az aircrack-ng (Debian, Ubuntu de valószínűleg többen is) akkor tökéletesen megfelel a csomagkezelővel való telepítés. Hangsúlyozom, a most következő parancsokat csak Debian alapú operációs rendszeren lehet elvégezni, vagy olyanban, amiben az **apt** csomagkezelő telepítve van. Az installáláshoz Debian / Ubuntu rendszeren a következő parancsot kell kiadnunk terminálba, root (rendszergazda) jogosúltságokkal:

apt-get update && apt-get install aircrack-ng iw -y

Ha megtalálható a repositoryban és van internet kapcsolatunk, akkor valószínűleg feltepelíti és használhatjuk is. Azonban ha eltérő disztribuciót használunk, vagy megváltozik a neve a repositoryban, más néven kell telepítenünk. Ekkor próbáljunk rákeresni a megfelelő csomagkezelővel. Debian / Ubuntuban például a következő képpen:

apt-cache search aircrack

vagy

aptitude search aircrack

Ha kényelmesebb, telepítésre és keresésre is használhatjuk a disztribució által kínált csomagkezelő software grafikus változatát.

Másik megoldás a telepítésre ha forrásból fordítjuk. Ezt a megoldást azonban csak gyakorlottabb felhasználóknak ajánlom. Látogassunk el az aircrack-ng oldalára és töltsük le a program forrását. Csomagoljuk ki a **tar xvzf <filenev>** (kacsacsőr nélkül) paranccsal majd lépjünk be az aircrack-ng könyvtárba **cd** -vel. Ezután használjuk root privilégiummal a **make && make install** paranacsot. Ez lefordítja nekünk a a forrást binárissá és feltelepíti nekünk. Ez a megoldás eléggé rendszerfüggő, különböző függőségi problémák adódhatnak. Ezek megoldásához nem tudok leírást készíteni, mert ahány rendszer annyi probléma fordulhat elő. Ami viszont biztos, a libcurl4-dev és az iw csomag szükséges hozzá. Ezek beszerzését vagy a repositoryból kell megoldanunk, vagy saját magunknak kell letölteni és lefordítani. Ha mindent jól csináltunk, ezek után már használható a program.

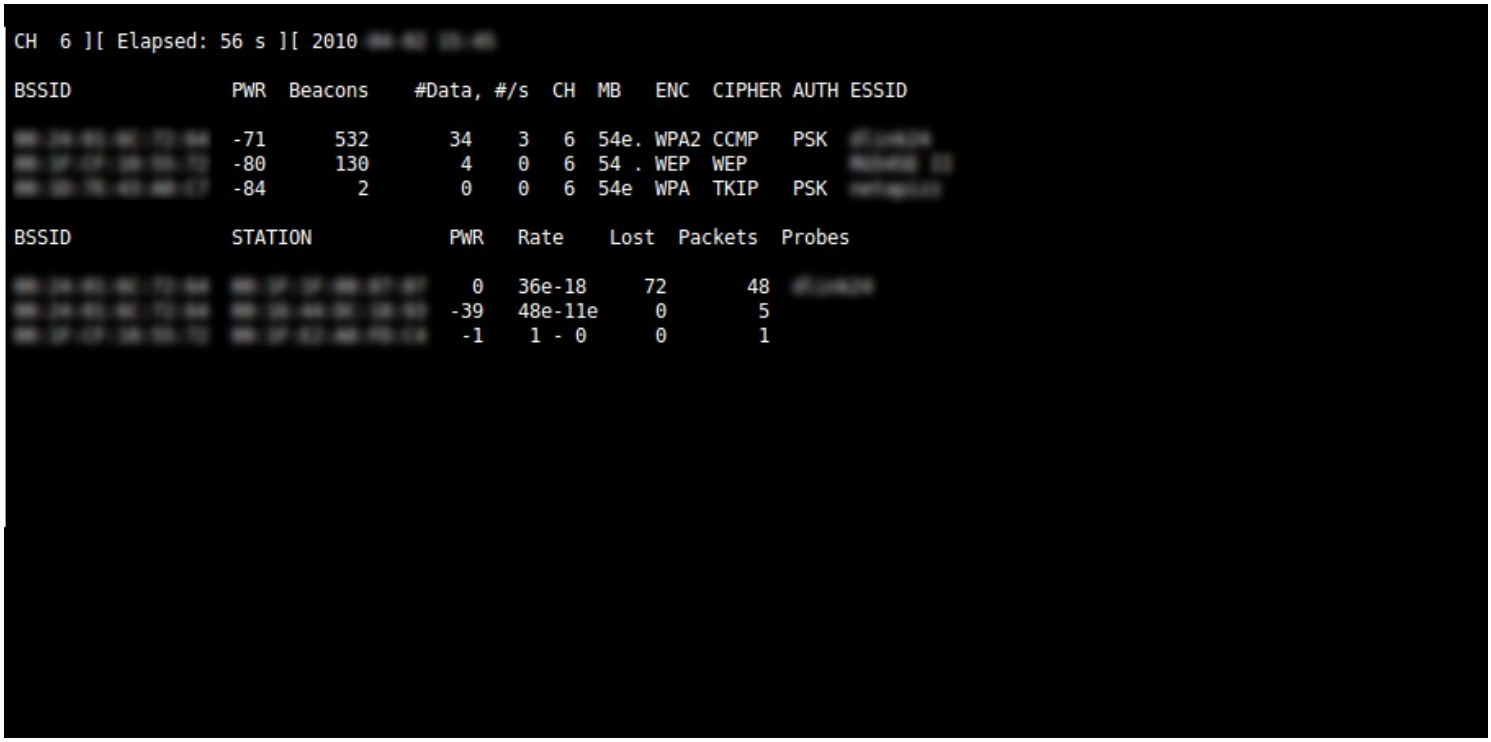
0x3 Airmon-ng

Az airmon-ng program segítségével monitor módba tehetjük a hálózati interfészünket, így lehetőségünk nyilik a hálózat monitorozására, scannelésére. A program használata a következő: **airmon-ng start <hálózati interfész>**
Például: **airmon-ng start wlan0**
Két lehetőség van. Vagy a wlan0 interfész kerül monitor módba, vagy egy új, virtuális interfész jön létre, ami bridged szerepet tölt be és a későbbiek során használhatunk. Például: **mon0**

```
Interface       Chipset         Driver

wlan0           RTL8187         rtl8187 - [phy0]
wlan1           Ralink 2573 USB rt73usb - [phy10]
                                (monitor mode enabled on mon0)
```

0x4 Airodump-ng



Az airodump-ng az aircrack-ng csomag része. Az airodump-ng segítségével scannelhetjük a wifi hálózatokat a már monitor módba léptetett hálózati intefészünkkel. A program segítségével a hálózatokról az alábbi információkat kaphatjuk: **BSSID, PWR, Beacons, Data, CH, MB, ENC, ESSID** és még sok másról. Az airodump-ng felső részén ezeket látjuk, nézzük is sorba mi – mit jelent:

- **BSSID:** A wifi router (Access Point / AP) MAC címe
- **PWR (Power):** Jelerősség dBm -ben (-50 dBm a legerősebb)
- **Beacons:** Az AP által küldött ébrenléti csomagok, ezek alapján hírdeti magát
- **Data:** A wireless router által küldött adat csomagok számát jelöli
- **CH (Channel):** Az AP csatorna száma
- **#/s:** Az AP által küldött csomagok száma másodpercenként
- **MB:** Access Point által támogatott maximális adatátviteli sebesség
- **ENC:** A titkosítás típusát határozza meg (WEP / WPA / WPA2)
- **Cipher:** A titkosítás algoritmusát határozza meg (TKIP / CCMP / Mixed)
- **ESSID:** A vezetéknélküli hálózat neve

Az airodump-ng alján az Access Pointhoz csatlakozott kliensekről láthatunk információkat:

- **BSSID:** Az AP MAC címe
- **STATION:** Az AP-hez csatlakozott kliens MAC címe
- **PWR:** Jelerősség dBm-ben
- **Rate:** A kliens és az AP közötti kapcsolat sávszélességét mutatja meg
- **Lost:** Az elveszett csomagok száma
- **Packets:** Az eddig küldött csomagok száma
- **Probes:** A kliens által keresett, vagy hozzá csatlakozott ESSID -t mutatja meg

Az airodump-ng az alábbi paranccsal indítható a legegyszerűbben, mindenféle szükségtelen paraméter nélkül:
airodump-ng mon0

A parancs értelmezése a következő:
Az **airodump-ng** a futtatandó programot jelenti, míg a **mon0** a monitorozásra használni kívánt hálózati csatolót definiálja.

Érdemes egy-két paramétert megjegyeznünk, amire szükségünk lesz a továbbiakban:

--bssid <AP mac címe>: Lehetőségünk van csak egy adott MAC című AP forgalmát figyelni, monitorozni

-c <csatorna szám> : Egy adott csatornára való szűkítés megvalósításának lehetőségére nyílik módunk

-w <fájlnév> : Azokat a csomagokat melyeket az airodump elfogott az éterben, lehetőségünk van egy fájlba menteni. Erre a fájlra lesz szükségünk ahhoz, hogy a kulcsot a csomagok alapján visszafejtsük.

Például: **airodump-ng --bssid 00:FA:A3:27:84:5B -c 6 -w capture**

0x5 Aireplay-ng

Az aireplay-ng segítségével csomagokat injectálhatunk vagy forgathatunk vissza a hálózatba, erre viszont olyan hálózati interfészre és driverre van szükségünk, amely támogatja ezt. Az aireplay-ng több csomaginjectációs lehetőséget biztosít.

- **--deauth** => Kliens és AP közötti kapcsolat megszakítása
- **--fakeauth** => Hamis authentikációt hoz létre az AP-vel
- **--interactive** => Egy .cap fájl alapján képes a fájlban lévő csomagokat visszaforgatni a hálózatba
- **--arpreplay** => Az AP és kliens közötti kapcsolatból próbál ARP kérést elkapni és azt a küldő MAC címével visszaforgatni. Mivel az ARP csomagok is titkosítottak egy jelszóval védett hálózaton, ezért a csomag méretéből következtet arra, hogy ARP csomagról van szó vagy sem. Az ARP csomag mérete ~28 byte.
- **--chopchop** => chopchop technikával olyan csomagot hoz létre, amit a hálózatba visszaforgatva az AP válaszol és elegendő csomagot tudunk elkapni a WEP kulcs visszafejtéséhez
- **--fragment** => fregmentációs technikával olyan csomagot hoz létre, amit a hálózatba visszaforgatva az AP válaszol és elegendő csomagot tudunk elkapni a WEP kulcs visszafejtéséhez
- **--caffe-latte** => Kliens felé történő kérés az IVkért.
- **--cfrag** =>
- **--test** => injectáció tesztet hajt végre

Az aireplay szükséges paraméterei:

- Támadási mód => Pl.: --arpreplay
- -b vagy -a (támadási módtól függ) => BSSID
- -h => A támadó kliens hálózati interfészének MAC címe (A miénk, pl.: mon0)
- hálózati interfész => Pl.: mon0

Egy példa Fake Authentikációra:

aireplay-ng -1 <az authentikáció ismétlésének gyakorisága mp-ben> -a <bssid> -h <mon0 MAC címe> <interfész>

aireplay-ng -1 10 -a 00:A4:34:D3:AC:33 -h 00:4F:AD:45:11:25 mon0

Egy példa ARP Replay támadási módra:

aireplay-ng -3 -b <bssid> -h <mon0 MAC címe> <interfész>

aireplay-ng -3 -b 00:A4:34:D3:AC:33 -h 00:4F:AD:45:11:25 mon0

```
Read 4862 packets...

        Size: 234, FromDS: 1, ToDS: 0 (WEP)

              BSSID  =
          Dest. MAC  =
         Source MAC  =

        0x0000:  0842 0000 3333 0000 000c 001f cf10 5572  .B..33........Ur
        0x0010:  001f e2a8 fdc4 902f e7d6 0500 4a07 b9b2  ......./....J...
        0x0020:  7156 b64c ab9c bedd 9c41 f860 695a c648  qV.L.....A.`iZ.H
        0x0030:  1c2e e044 4510 c09a 3f43 c55c 8307 2e07  ...DE...?C.\....
        0x0040:  bebd 7950 c5be c71e f37e d076 cece cef3  ..yP.....~.v....
        0x0050:  1aa6 0283 48a3 5dbc 9ff2 8283 f3df f514  ....H.].........
        0x0060:  1f46 b1c0 0b63 266a 90f0 6877 43a0 91f7  .F...c&j..hwC...
        0x0070:  d080 cc12 43aa 9336 5ffe 2f3c 721d 670e  ....C..6_./<r.g.
        0x0080:  500c b2b0 98bd 2082 aa4b d622 fdfe 34db  P..... ..K."..4.
        0x0090:  1f29 e6b7 7028 5dba 6109 cea4 27e8 9b88  .)..p(].a...'...
        0x00a0:  1f3c 2a82 0b17 97e9 144b 0ffe 03ae e2ce  .<*......K......
        0x00b0:  f2e6 0d45 5086 0d02 a9d6 8b11 8c6d 283e  ...EP........m(>
        0x00c0:  0401 0266 bc4c 19d0 961c 028e e58d 13a3  ...f.L..........
        0x00d0:  afb9 3423 b10d 90b5 d81f b2b7 56e1 47b4  ..4#........V.G.
        --- CUT ---
```

0x6 Aircrack-ng

Az aircrack-ng feladata a jelszó visszafejtése egy fájlból, melyet az **airodump-ng -w** paraméterével mentettünk. Két fajta töréshez használható:

- WEP
- WPA / WPA2

A WEP töréséhez több megoldás létezik. Ha statisztikai úton próbáljuk visszafejteni a kulcsot, akkor x mennyiségű elkapott DATA csomagra van szükségünk. Egy 64 bites WEP kulcshoz ~ 10000 DATA csomag szükséges, míg egy 128 biteshez 20000 – 40000 csomag. Ez változó.
Lehetőségünk van szótárfájl alapú töréshez is WEP kulcs esetében. Ilyenkor meg kell adni a szótárfájl elérési útvonalát. Ezt az aircrack-ng -w paraméterével tudjuk beállítani. WEP kulcs visszafejtéséhez ajánlatos a statisztikai támadást haszálni, mert nagyon gyors és ha megvan az elegendő DATA csomag mennyiség, akkor 100% a pontosság. Egy WEP kulcs manapság 2 perc alatt feltörhető!

WEP kulcs törésére példa:

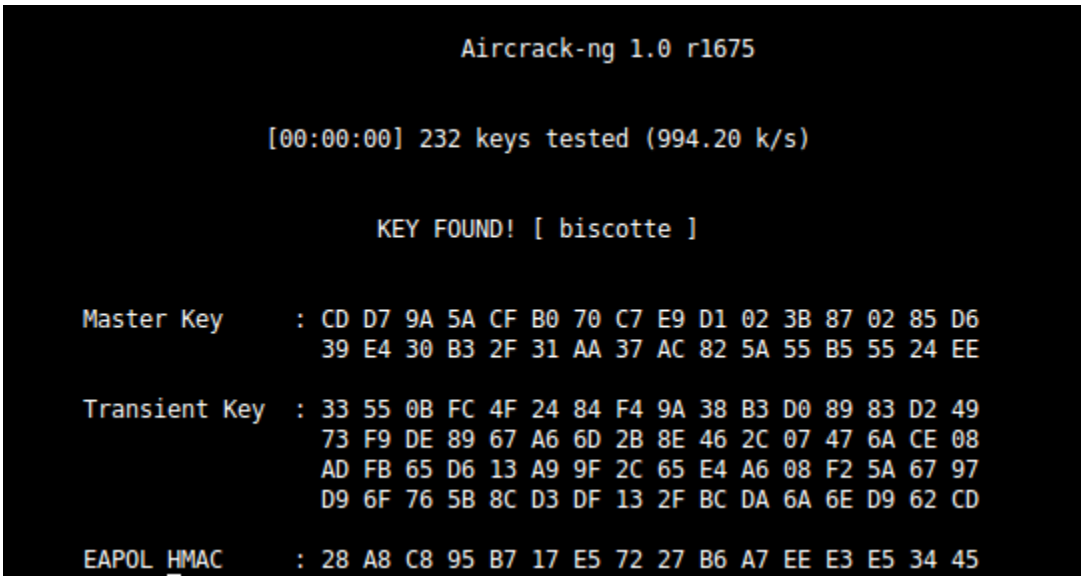
aircrack-ng -a 1 <az airodump-ng által rögzitett fájl elérési útvonala>

aircrack-ng -a 1 attack.cap

A WPA / WPA2 kulcs visszafejtéséhez csak a szótáralapú támadás lehetséges. Ez a következőképp működik:

aircrack-ng -a 2 <az airodump-ng által rögzitett fájl elérési útvonala> -w <szótárfájl elérési útvonala>

aircrack-ng -a 2 attack.cap dictionary.txt



0x7 A támadás menete

1. Az **airmon-ng start <interfész>** paranccsal a hálózati interfészünket monitor módba tesszük.
2. Az **airodump-ng <interfész>** paranccsal felfedezzük a hálózatokat és kiválasztjuk a megtámadni kívántat.
3. Leszűkítjük az airodump-ng találatát arra az AP -re amit megszeretnénk támadni és egy fájlba rögzítjük a csomagokat. Például: **airodump-ng --bssid 00:11:22:33:44:55 -c 7 -w essid mon0**
4. Egy új terminált nyitunk és az **aireplay-ng** programmal elvégezzük a megfelelő injectációt. Fontos, hogy az **airodump-ng** folyamatosan fusson, scanneljen és mentse a csomagokat a támadás végéig.
5. Miután elvégeztük a megfelelő injectációkat használjuk az **aircrack-ng** programot a kulcs meghatározásához.

0x8 Elérhetőség

Author: XEL
E-Mail: xel.white@gmail.com

Thank You!