WEP verschlüsseltes WLan

Auf mit der veralteten Verschlüsselungstechnik WEP für drahtlose Netzwerke existieren einige gut funktionierende Angriffe. Voraussetzung für einen schnellen Erfolg ist jedoch ausreichender Datenverkehr im angegriffenen Netzwerk - wenn ein WEP-gesichertes Netz keine Teilnehmer hat, ist die Wahrscheinlichkeit gering, den Schlüssel schnell zu berechnen, da man nicht genügend Datenpakete mitschneiden kann. Die meisten Angriffe nutzen die Schwachstelle des mit 24 Bit sehr kurzen Initialisierungsvektor IV bei der RC4-Verschlüsselung aus. Diese Angriffsmethode wird häufig als Related-Key-Attack bezeichnet.

Disclaimer: Um rechtliche Probleme zu vermeiden sei auf die rechtlichen Rahmenbedingungen verwiesen. Um nicht in Konflikt mit dem Hacker-Paragrafen zu kommen, teste die folgenden Schritte ausschließlich an deinem eigenen WLAN, um dessen Sicherheitsstatus zu überprüfen. Sprich gegebenenfalls **vorher** mit deinen Eltern!

Grundsätzliches Vorgehen

Grundsätzlich verläuft der Angriff in 4 Schritten

1. Vorbereiten der Werkzeuge
2. Informationsbeschaffung
3. Informationssammlung
4. Informationsauswertung

Vorbereiten der Werkzeuge

Wir starten Kali-Linux, sorgen für ein deutsches Tastaturlayout und bereiten die WLan-Karte vor. Damit der Angriff durchgeführt werden kann, muss man die Wlan Karte in den Monitoring Modus versetzen, das ist nicht mit jeder Karte möglich. Außerdem können sich Device-Namen und ähnliches je nach Hardware unterscheiden. Die vorliegende Anleitung ist also nicht "idiotensicher", sondern lediglich ein Leitfaden, wie man prinzipiell vorgeht.

Die weiteren Befehle müssen als Benutzer `root` ausgeführt werden.

Mit dem Befehl `airmon-ng` kann man sich zunächst die Wlan Umgebung anzeigen lassen, mit `airmon-ng start wlan0` erhält man für gewöhnlich eine Meldung, dass die Wlan Schnittstelle derzeit von anderen Prozessen verwendet wird. Mit `airmon-ng check kill` können diese Prozesse beendet werden. Nun ist Kali-Linux meist offline, da die Prozesse, welche den Netzzugang für den Laptop zur Verfügung gestellt haben beendet wurden, außer man verfügt zusätzlich über eine kabelgebundene Verbindung.

Die erneute Eingabe von `airmon-ng` zeigt die veränderte Umgebung an, mit `airmon-ng start`

`wlan0mon` kann man das Interface in den Monitoring-Modus versetzen.

Informationsbeschaffung

Der Befehl

```
airodump-ng wlan0mon
```

zeigt die WLan Umgebung unseres Laptops an.

Hier identifizieren wir das Netzwerk, das wir angreifen möchten und notieren BSSID, SSID, CHANNEL. Wenn erkennbar kann man optional die MAC Adresse eines oder mehrerer mit dem WLan verbundener Clients notieren.

Informationssammlung

Jetzt können wir gezielt Informationen zu unserem Zielnetzwerk sammeln - im ersten Schritt haben wir ja Infos zu allen Netzwerken und Geräten in unserer Umgebung gesehen, nun konzentrieren wir uns also auf unser Ziel.

Mit dem Befehl

```
airodump-ng {MON-DEVICE} -c {CHANNEL} --bssid {BSSID} -w wepstream
```

sammelt man Pakete uns speichert diese in Dateien, die alle mit `wepstream` beginnen. Der Kanal und die BSSID müssen entsprechende der Infos angepasst werden, die man im Schritt Informationsbeschaffung ermittelt hat. Während der Sammlung werden einige Statistikdaten angezeigt, besonders wichtig ist die Spalte `#Data`, welche die Zahl der gesammelten Datenpakete anzeigt. Hier benötigt man eine große Zahl an Paketen, damit im nächsten Schritt die Bestimmung des Schlüssels aus den Initialisierungsvektoren gelingen kann. Wenn im angegriffenen WLan wenig Datenverkehr herrscht, kann das mitunter lange dauern und durch weitere Tricks wie ARP-Replay- oder Deauthentication-Attacken auf verbundene Clients beschleunigt werden.[1)]

Wenn man genügend Datenpakete gesammelt hat, beendet man die Sammlung mit STRG-C

Informationsauswertung

Die gesammelten Pakete befinden sich in der Datei wepstream*.cap. Mit dem Befehl

```
aircrack-ng wepstream-01.cap
```

werden die Pakete ausgewertet und wenn möglich der Key berechnet.

WLan Schnittstelle in Kali zurücksetzen

Um anschließend wieder mit Kali weiterzuarbeiten und dabei auch die WLan-Schnittstelle wieder nutzen zu können, muss man den Monitor-Modus beenden und die nötigen Dienste neu starten:

```
airmon-ng stop wlan0mon
service networking restart
service NetworkManager restart
```

Anschließend kann man sich unter Verwendung des zuvor "gehackten" WEP-Passworts mit dem Wlan verbinden.

Übersichtsvideo

[1)]

Anmerkung für die Lehrperson: Sorgen Sie für einen Client im Wlan, der Traffic erzeugt