BRAIN-MEDIA.DE

PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold

# WLAN Security kompakt


Security.Edition

## Praxiseinstieg in das Penetration Testing von drahtlosen Netzwerken

**Holger Reibold**

# WLAN Security kompakt

# Inhaltsverzeichnis

Herausgeber: Dr. Holger Reibold

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Coverbild: streichholz / photocase.de

Korrektur: Theresa Tting

ISBN: 978-3-95444-221-8

# Vorwort

Drahtlose Netzwerke findet man heute überall. Man muss nur sein Smartphone zücken, einen WLAN-Scan durchführen und schon findet man – je nach Standort – mehrere bis Dutzende Access Points. WLANs kommen in privaten Wohnungen genauso wie in Büros und industriellen Produktionsstätten zum Einsatz.

Die drahtlose Technik macht das Leben unglaublich einfach und bietet uns viel Mobilität, doch sie birgt auch nicht unerhebliche Risiken. Da potenzielle Angreifer nicht mehr direkten Zugang zu einem Netzwerk besitzen müssen, sondern sich mit gebührendem Abstand an ein drahtloses Netzwerk herantasten können, sind Angriffe vergleichsweise einfach durchzuführen.

Die Häufigkeit von Hacker-Angriffen hat in den vergangenen Jahren deutlich zugenommen, aber Netzwerkbetrieber sind oft ratlos, wenn es um die Sicherung drahtloser Netzwerke geht. Der erste Schritt, ein WLAN gegen Angriffe von außen (und innen) zu schützen, ist das Aufdecken von möglichen Schwachstellen. Hier kommt Penetration Testing ins Spiel.

In diesem Einstieg zeige ich Ihnen, wie Sie die Sicherheit Ihres WLANs auf Herz und Nieren überprüfen. Ich zeige Ihnen auch, wie Hacker vorgehen und wie Sie das gewonnene Wissen dazu nutzen, Ihre Umgebung sicherer zu machen.

Ich wünsche Ihnen beim Einstieg in das WLAN Penetration Testing viel Erfolg!

Herzlichst,

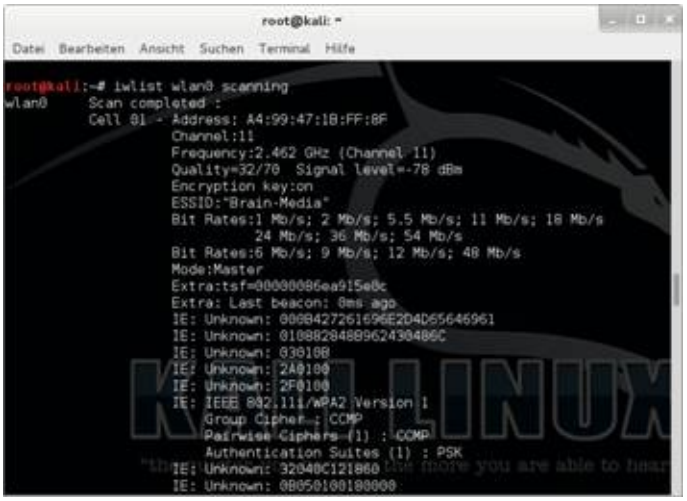
Holger Reibold

(August 2015)

# 1 WLAN-Sicherheit – der Einstieg

Drahtlose Netzwerke gehören heute zu jeder modernen IT-Infrastruktur und sind aus unserem Alltag kaum mehr wegzudenken. Man findet sie nicht nur im privaten und öffentlichen Raum, sondern immer häufiger auch in Unternehmen. Wenngleich gerade dort, wo immer möglich, man auf kabelgebundene Verbindungen setzen sollte, um die Zahl der Angriffspunkte zu minimieren. Das Problem für Unternehmen und Administratoren, die für die Sicherheit einer Umgebung zuständig sind, ist der Umstand, dass Angreifer keinen physikalischen Zugang zu einem Netzwerk besitzen müssen, sondern in Wardriver-Manier sich um die Ecke verstecken und dort ihr Unwesen treiben können.

Im Folgenden zeige ich Ihnen, wie Sie (mit Kali Linux und anderen Tools) einfach und ohne großen Staub aufzuwirbeln, ein drahtloses Netzwerk auf Schwachstellen überprüfen und diese ausnutzen können. Wir gehen davon aus, dass Sie bereits über einen WLAN Access Point verfügen, den Sie als Angriffsziel verwenden wollen und dürfen. Zu Testzwecken ist es allerdings ratsam, einen eigenen Test-Access Point anzulegen und diesen dann zu attackieren.




**Das Prüfen auf verfügbare WLANs im Umfeld.**

Als das Standardwerkzeug für Penetration Testing jeglicher Art hat sich Kali Linux etabliert. So ist es nicht weiter verwunderlich, dass Kali Linux auch in Sachen WLAN bestens ausgestattet ist. In der Regel kann das Linux-Betriebssystem den WLAN-Adapter Ihres Notebooks zuverlässig identifizieren und konfigurieren. Das können Sie leicht prüfen, indem Sie in der rechten oberen Ecke auf das Balkendiagrammsymbol klicken. Mit einem Klick rufen Sie den Dialog auf, der Ihnen die in Ihrer Nähe verfügbaren drahtlosen Netzwerke aufführt.

Um weitere Details wie die MAC-Adresse, ESSID, Verschlüsselung, Kanal etc. abzurufen, greifen Sie zur Konsole. Mit folgendem Befehl können Sie jede Menge Details zu den verfügbaren WLANs in Ihrer Umgebung abrufen:

```
iwlist wlan0 scanning
```

Da Access Points die gleiche SSID besitzen können, müssen Sie die MAC-Adresse, die im Address-Feld ausgegeben wird, verifizieren. Da Sie als Admini-strator Zugang zur Access Point-Konfiguration haben, können Sie das leicht tun.

Führen Sie als Nächstes die beiden folgenden Befehle aus, um den Status des Access Points zu prüfen. Wir verwenden im Folgenden den Access Point *Brain-Media*. Sie können die Bezeichnung entsprechend anpassen:

```
iwconfig wlan0 essid “Brain-Media“
iwconfig wlan0
```

Da wir nun wissen, dass das Management-Interface des WLAN-Access Points die IP-Adresse 192.168.2.1 besitzt, weisen wir dem Notebook die IP-Adresse des gleichen Subnetzes zu:

```
ifconfig wlan0 192.168.2.20 netmask 255.255.255.0 up
```

Prüfen Sie die Konfiguration anhand der Ausgabe des folgenden Befehls:

```
ifconfig wlan0
```

Nun haben Sie den WLAN-Adapter des Penetration-Notebooks dem Subnetz des Access Points zugeordnet und können als Nächstes mit Ping prüfen, ob der Access Point erreichbar ist:

```
ping 192.168.2.1
```

Ergänzend können Sie mit dem Befehl *arp -a* prüfen, ob das Signal auch tatsächlich von dem Accesss Point stammt. Im Protokoll des Access Points können Sie dann prüfen, dass eine Verbindung vom Notebook zum Access Point hergestellt wurde.

## 1.1 Unsicherheiten in WLANs

Um zu verstehen, wie WLANs angreifbar sind, muss man sich ein wenig mit der Art befassen, wie WLAN-Kommunikation funktioniert. In drahtlosen Netzwerken erfolgt die Kommunikation über sogenannte Frames. Dabei gibt es drei zentrale Frame-Typen:

- **Management Frames**: Diese sind für die Verwaltung der Kommunika-tion zuständig, also die Authentifizierung, Request und Responses etc.
- **Control Frames**: Diese Frames steuern die Kommunikation und sorgen für einen sauberen Datenaustausch zwischen Access Points und WLAN-Clients.
- **Data Frames**: In diesen Frames sind die eigentlichen Daten, also die Nutzlast

enthalten, die über die drahtlose Verbindung übermittelt werden.

Mit Werkzeugen wie Wireshark, ein Sniffer, der ebenfalls in Kali Linux enthalten ist, kann man diese Frames sichtbar machen. Dazu müssen Sie zunächst den sogenannten Promiscuous Mode auf dem Penetration-Notebook aktivieren. In diesem Modus liest der WLAN-Adapter den gesamten ankommenden Datenverkehr an die in diesen Modus geschaltete Netzwerkschnittstelle mit und gibt die Daten zur Verarbeitung an das Betriebssystem weiter. Wir bevorzugen einen weiteren Modus: den Monitormodus. Bei diesem Modus werden im Unterschied zum Promiscuous Mode alle empfangenen Frames weitergeleitet, nicht nur die des Netzwerks, mit dem der Client aktuell verbunden ist. Sie können den aktuellen Modus einfach mit folgendem Befehl abrufen:

```
iwconfig
```

Um das Notebook nun in den Monitormodus zu versetzen, greifen wir zu einem weiteren Tool, das in Kali Linux integriert ist: Airmon-ng. Mit diesem Kommando können Sie auch prüfen, welche WLAN-Adapter in Ihrem Notebook verfügbar sind. Doch der Reihe nach. Prüfen Sie zunächst, ob der WLAN-Adapter korrekt installiert und vom System erkannt wird:

```
ifconfig
```

Dann führen Sie folgenden Befehl aus:

```
ifconfig wlan0 up
```

Um den Adapter in den Monitormodus zu versetzen, führen Sie folgenden Befehl aus:

```
airmon-ng
```

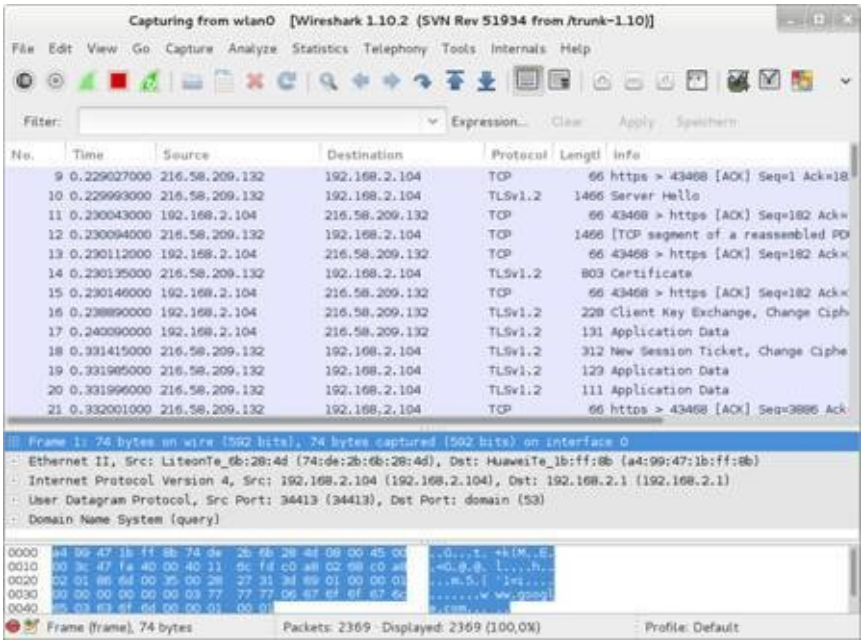
Dann folgenden Befehl:

```
airmon-ng start wlan1
```

Sie können mehrere Monitormodi auf einem identischen Netzwerkadapter ausführen. Damit haben wir zwei Schnittstellen angelegt, von denen einer sich im Monitormodus befindet. Starten Sie als Nächstes mit dem Menübefehl *Anwendungen > Kali Linux > Sniffing & Spoofing > Netzwerksniffer > Wireshark* den beliebten Open Source-Sniffer.

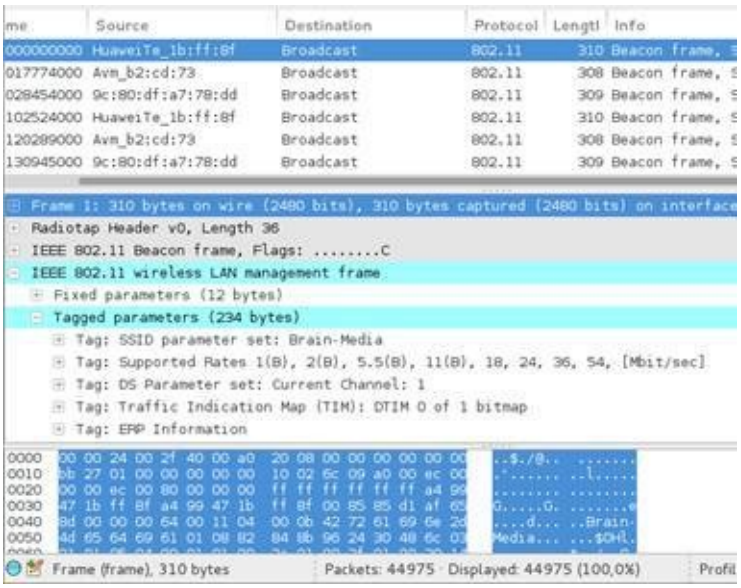

**Die Wireshark-Sniffer in Aktion.**

Um mit den Sniffer Daten aufzeichnen zu können, müssen Sie zunächst die Aufzeichnungsschnittstellen konfigurieren. Dazu führen Sie den Menübefehl *Capture* > *Interfaces* aus. Im Dialog *Capture Interface* wählen Sie die Schnittstelle aus, über die der drahtlose Traffic läuft. Klicken Sie anschließend auf *Start*. Anschließend sollten Sie im Hauptfenster von Wireshark die Aufzeichnung der ersten Datenpakete verfolgen können.




**Der erste drahtlose Traffic wurde mit Wireshark aufgezeichnet.**

Das Hauptfenster von Wireshark erlaubt Ihnen das Sortieren der Nachrichten nach Quell- und Zieladresse sowie nach Protokollen. Dazu klicken Sie einfach auf den entsprechenden Kopf. Über den Filter können Sie die Ansicht auf die Informationen beschränken, die gerade für Sie von Interesse sind. Um die Ansicht auf den WLAN-Traffic zu beschränken, geben Sie einfach *wlan* in das Eingabefeld *Filter* ein. Die Ansicht wird automatisch in der sogenannten Paketliste eingeschränkt.




**Die Details einer Aufzeichnung. In der Mitte die Paketdetails, darunter die Rohdatenansicht.**

Wenn Sie sich für bestimmte Details des WLAN-Traffics interessieren, öffnen Sie in den Paketdetails den Eintrag *Wireless LAN management frame*. In der darunterliegenden sogenannten Rohdatenansicht können Sie nun die eigentlichen Inhalte einsehen. Über Filter kommen Sie wie bereits erwähnt recht schnell ans Ziel. Sie können einfach eine Zeichenfolge wie *password* verwenden und landen schon bei dem Frame, der für die Passwortübermittlung zuständig ist.

Anhand zweier simpler Beispiele möchte ich Ihnen zeigen, wie einfach und effektiv die Verwendung von Wireshark und den Kali Linux-Tools beim Aufdecken von Schwachstellen und der Traffic-Analyse ist.

Bei der Suche nach Schwachstellen und Verwundbarkeiten interessiert uns insbesondere der Traffic, der nicht verschlüsselt ist, weil man diesen am ehesten interessante Informationen entlocken kann.

Dazu müssen Sie zunächst herausfinden, auf welchem Kanal der Access Point läuft. Das ist einfach:

airodump-ng —bssid <mac> mon0 where <mac>

Dieser Befehl gibt Ihnen schnell den Kanal aus. Als Nächstes können Sie den Traffic auf diesem Kanal beschränken:

wlan.bssid == <mac>

Wichtig ist, dass Sie dabei die korrekte MAC-Adresse des Access Points angeben. Das Besondere an Wireshark sind die vielfältigen Filtermöglichkeiten, die das Programm bietet. Durch die Kombination von Filteroptionen können Sie die Ansicht gezielt einschränken.

Wenn Sie sich nur für den Traffic interessieren, der an Ihren Access Point gerichtet ist,

ergänzen Sie obige Suchoption wie folgt:

(wlan.bssid == <mac>) && (wlan.fc.type_subtype == 0x20)

Nun können Sie mit einem Browser das Web-Interface des Access Points öffnen. In Wireshark werden dann nur die unverschlüsselten Daten angezeigt.

Für das Aufdecken von Schwachstellen in drahtlosen Netzwerken sind alle Informationen über das Zielsystem relevant, die Sie sammeln können. WLANs operieren üblicherweise auf zwei Frequenzbereichen:

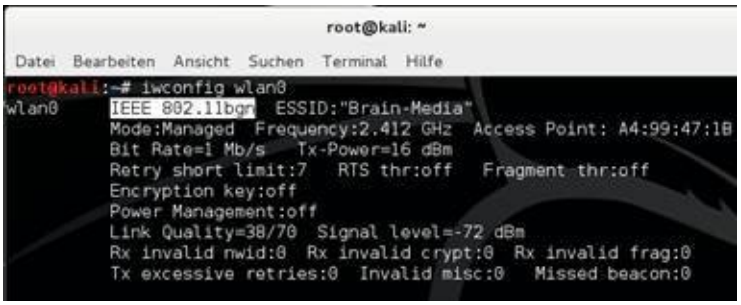
- 2,4 GHz
- 5.0 GHz

Nicht jeder WLAN-Adapter unterstützt all diese Frequenzbereiche. Aktuell dürften nach wie vor 2,4 GHz Access Points die Landschaft bestimmen.

Aber ein weiterer interessanter Punkt in diesem Zusammenhang ist der Umstand, dass jedes Frequenzband mehrere Kanäle verwendet. Das ist für das Sniffen von WLAN-Verbindungen wichtig, denn wir können nicht alle Kanäle gleichzeitig sniffen, also den Traffic aufzeichnen.

Sendet der für uns interessante Access Point auf Kanal 1, so muss man auch die WLAN-Konfiguration des Penetration-Notebooks entsprechend konfigurieren. Um die Adapterkonfiguration zu optimieren, rufen Sie zunächst seine Eigenschaften ab:

iwconfig wlan0




**Die Details des Access Points.**

Obiger Ausgabe können Sie entnehmen, dass der Access Point den Standard IEEE 802.11bgn auf dem Frequenzband 2,4 GHz nutzt. Sie können Ihren WLAN-Adapter nun so konfigurieren, dass dieser einen bestimmten Kanal verwendet:

iwconfig wlan0 channel x

Dabei ersetzen Sie das kleine x durch einen Wert, beispielsweise 10 oder 11. Schon ist die Verwendung auf diesen Kanal beschränkt.

Doch leider endet die Komplexität der WLAN-Technologie nicht an dieser Stelle. Vielmehr verwendet jedes Land bzw. jeder Kontinent sein eigenes Spektrum. Das erschwert die Suchen nach Schwachstellen unter Umständen zusätzlich. Sie können in der Protokolldatei */var/log/messages* in der Regel erkennen, welche Länderkonfiguration zum Einsatz kommt. Dazu suchen Sie in der Protokolldatei den WLAN-Eintrag und prüfen diesen. Um die deutsche Ländereinstellung zu setzen, verwenden Sie folgenden Befehl:

```
iw reg set DE
```

Damit sind Sie mit den wichtigsten WLAN-Funktionalitäten vertraut, die Kali Linux zu bieten hat.

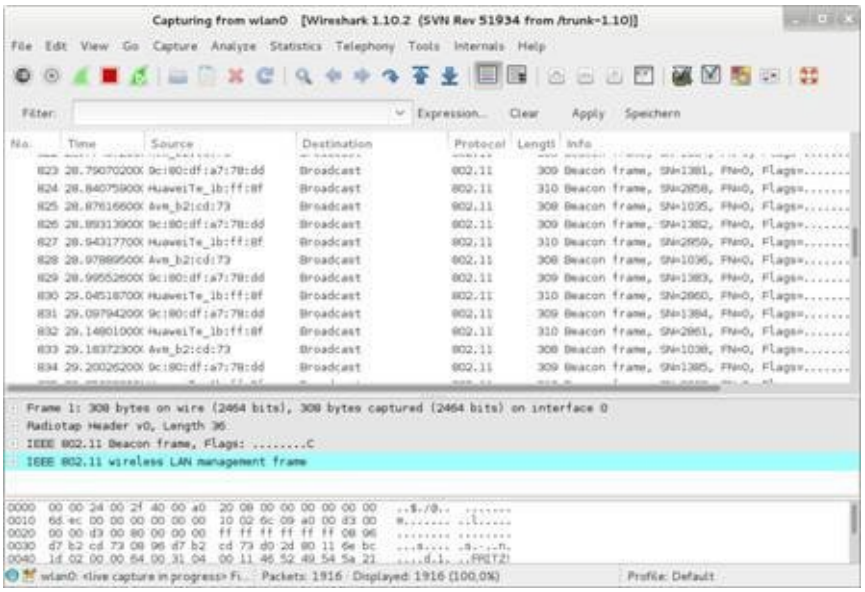
## 1.2 WLAN-Authentifizierung umgehen

WLANs verwenden üblicherweise eine Authentifizierung, über die sich WLAN-Clients Zugang zu einem Netzwerk verschaffen. Doch diese Mechanismen sind oftmals nicht mehr als ein Semi-Schutz und nicht selten leicht zu umgehen.

### 1.2.1 Versteckte WLANs aufspüren

In der Standardkonfiguration senden alle Access Points Ihre SSID im sogenannten Beacon Frame. Der Beacon Frame ist einer der Management-Frames von IEEE 802.11-basierten WLANs. Er enthält alle wichtigen Informationen über das Netzwerk. Die Beacon Frames werden kontinuierlich versendet, um die Existenz eines WLANs anzuzeigen.

Nur Clients, die die SSID kennen, können sich mit einem solchen Netzwerk verbinden. Leider bietet diese Technik weit weniger Schutz, als die meisten Anwender und Administratoren vermuten. Auch versteckte SSIDs bieten nur einen bedingten Schutz.




**Die Aufzeichnung der Beacon Frames in Wireshark.**

Wenn Sie mit Wireshark den drahtlosen Traffic aufzeichnen, so können Sie die SSID den Aufzeichnungen als Rohtext entnehmen. Wie Sie obiger Abbildung entnehmen können, kann Wireshark die WLAN-Pakete und insbesondere die Beacon Frames sehr schön aufzeichnen und für Sie sichtbar machen.


**Das Unsichtbarmachen eines WLANs.**

Alle mir bekannten WLAN-Router bieten die Möglichkeit, den WLAN Access Point unsichtbar zu machen. Das verspricht einen gewissen Schutz, weil sie nicht auf den ersten Blick erkennbar sind und sich sozusagen hinter den sichtbaren dralosen Netzwerken verstecken.

Versetzen Sie dazu Ihren Access Point in den Unsichtbar-Modus. Bei einem Speedport-Router erfolgt diese Einstellung in den WLAN-Grundeinstellungen. Wenn Sie nun den Traffic mit Wireshark analysieren, stellen Sie fest, dass die SSID im Beacon Frame verschwunden ist.

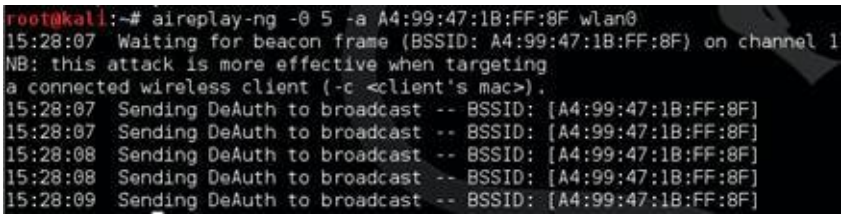
Um nun doch an eine versteckte SSID zu gelangen, umgehen wir mit einem kleinen Trick das Beacon Frame und nutzen eine passive Technik für die Legitimierung des Clients am Access Point. Suchen Sie in Ihren Aufzeichnungen nach einem *Probe Response*-Eintrag und öffnen Sie dort die SSID-Parameter.

Wenn Sie nun einen entsprechenden Paketeintrag unter die Lupe nehmen und dessen SSID-Informationen öffnen, werden Sie feststellen, dass Sie dort die ID wieder finden. Somit ist es recht einfach, versteckte WLANs aufzuspüren, die auf den ersten Blick nicht sichtbar sind.

Alternativ können Sie auch mit Aireplay-ng ein Deauthentifizierungspaket an alle potenziellen Access Points senden:

```
aireplay-ng -0 5 -a <mac>  —ignore-negative wlan0
```

Dabei ersetzen Sie <*mac*> durch die MAC-Adresse des Routers. Die Option *-0* führt die Deauthentifizierungsattacke aus, der Wert 5 bestimmt die Anzahl der Deauthentifizierungspakete. Mit der Option *-a* zeigen Sie an, dass die folgende Adresse die des Access Points ist.




**Der Einsatz von Aireplay-ng.**

Dieser Befehl führt dazu, dass alle legitimierten Client-Verbindungen unterbrochen und wieder aufgebaut werden. Zeichnen Sie diese Aktionen mit Wireshark auf. Uns interessieren als Nächstes die Deauthentifizierungs-Pakete. Begrenzen Sie die Ansicht in der Wireshark auf diese Pakete.

Wenn Sie sich nun wieder mit Wireshark die Probe Respones anschauen, wird dort in den SSID-Knoten die aufgedeckte Access Point-Bezeichnung aufgeführt.

### 1.2.2 MAC-Filter aushebeln

Die Verwendung von MAC-Filtern ist eine eher antiquierte Authentifizierungsmöglichkeit, aber in vielen Unternehmen nach wie vor anzutreffen. Sie hat ihre Wurzeln in der kabelgebundenen Netzwerktechnik. Mit dem Aufkommen der WLAN-Technik hat sie sich in die drahtlose Kommunikation gerettet, ist dort aber aufgrund des mangelhaften Schutzes nahezu unbrauchbar.

Die Authentifizierung der Clients am Access Point erfolgt auf der Grundlage der Client-MAC-Adresse. Auf Seiten des drahtlosen Zugangspunktes wird eine Liste der zulässigen MAC-Adressen verwaltet.


**Die Verwaltung der Zugänge auf Basis der MAC-Adresse.**

Alle handelsüblichen WLAN-Router bieten die Möglichkeit, eigene Zugangslisten

anzulegen. Das kann automatisch mit einer bestehenden Zugangskennung oder manuell erfolgen. Nachdem Sie die MAC-Filterung aktiviert haben, können sich nur noch die Clients beim Access Point anmelden, die im Router hinterlegt sind. Verbindungen aller anderen Clients werden abgelehnt. Misslingt die Anmeldung, so gibt der Router eine Fehlermeldung zurück, die Sie wieder in Wireshark mitschneiden können.

Aber Sie können mit Hilfe eines kleinen Tools herausfinden, welche MAC-Adressen eine Verbindung zu dem Router herstellen können. Dazu greifen Sie zu Airodump-ng. Um konkret herauszufinden, welche MAC-Adressen auf Kanal 10 bei der angegebenen BSSID von dem Router akzeptiert werden, führen Sie folgenden Befehl aus:

```
airodump-ng-c 10 -a —bssid <mac> wlan0
```

Der Access Point gibt eine Liste der gültigen MAC-Adresse aus. Damit wissen Sie, welche sich Zugang zu dem Netzwerk verschaffen können.

Alles, was Sie jetzt noch tun müssen, ist die MAC des eigenen Penetration-Systems zu ändern. Auch hierfür stellt Ihnen Kali Linux wieder das geeignete Werkzeug zur Verfügung: macchanger. Fahren Sie zunächst den WLAN-Adapter herunter:

```
ifconfig wlan0 down
```

Dann ändern Sie mit macchanger die Belegung:

```
macchanger -m 11:22:33:44:55:66 wlan0
```

Das Tool gibt die permanente, die aktuelle und die neue MAC-Adresse aus. Anhand der Ausgabe können Sie direkt erkennen, dass der Client nun die gewünschte MAC-Adresse besitzt. Nun machen Sie die Probe auf’s Exempel: Voilà, Sie sind drin!

### 1.2.3 Schlüsselauthentifizierung umgehen

Die mit Abstand häufigste Art der Authentifizierung eines WLAN-Clients an einem Access Point ist die Verwendung eines WEP- oder eines WPA-Schlüssels. Dabei sendet der Client zunächst eine Authentifizierungsanfrage an den Zugangspunkt, der mit einer Challenge antwortet. Der Client sendet dann die Antwort zurück und der Access Point gibt ein *OK* oder eine Fehlermeldung zurück.

Das Problem für den Netzwerkadministrator ist dabei, dass ein potenzieller Angreifer in aller Ruhe den Authentifizierungsablauf zwischen WLAN-Client und Access Point abhören und auswerten kann.

Das Grundprinzip der schlüsselbasierten Authentifizierung können Sie am besten nachvollziehen, wenn Sie versuchen, eine WEP-basierte Sicherung zu knacken. Die WEP-Nachfolger WPA und WPA2 sind deutlich schwieriger zu knacken, aber das Grundprinzip ist ähnlich.


**Zu Testzwecken aktivieren Sie die WEP-Verschlüsselung.**

Um einen WEP-basierten Schutz zu knacken, aktivieren Sie auf Seiten des Access Points die WEP-Unterstützung und legen die dafür notwendige Passwortphrase an. Stellen Sie als Nächstes eine Verbindung zwischen dem Client und Access Point her.

Mit Wireshark zeichnen Sie nur die Verbindung zwischen beiden auf. Außerdem protokollieren wir den gesamten Authentifizierungsaustausch. Hierfür greifen wir wieder zu Airodump-ng. Führen Sie dazu folgenden Befehl aus:

airodump-ng wlan0 -c 10 —bssid <mac> -w keystream

Die Option -*w* sorgt dafür, dass die Aufzeichnung in einer Datei mit dem Präfix *keystream* gesichert wird. Eine typische Bezeichnng lautet wie folgt:

keystream-01-02-1234-A1-B2-34.xor

Um die Schlüsselauthentifizierung zu faken, greifen wir wieder zu Aireplay-ng. Führen Sie folgenden Befehl aus:

aireplay-ng -1 0 -e “WLAN” -y keystream-01-02-1234-A1-B2-34.xor -a <mac> -h AA:AA:AA:AA:AA:AA wlan0

Das Tool Aireplay-ng verwendet den Keystream und versucht sich an der Authentifizierung an dem Access Point mit der SSID *WLAN*. Starten Sie nun Wireshark und begrenzen Sie die Ansicht auf die MAC-Adresse:

wlan.addr == AA:AA:AA:AA:AA:AA

Anhand der Info *Authentifícation* können Sie im gefilterten Traffic entnehmen, dass es sich bei dem ersten Eintrag um den Authentifizierungs-Request von Aireplay-ng handelt.

Das zweite Paket enthält die Antwort des Access Points mit dem Challenge Text an den Client. Das dritte Paket enthält schließlich die verschlüsselte Anwort des Clients.

Das Aireplay-ng-Tool verwendet die Keystream-Aufzeichnung für die Entschlüsselung. Im Idealfall gelingt die Authentifizierung und der Access Point gibt eine Erfolgsmeldung aus. Nachdem die Authentifizierung erfolgreich abgeschlossen ist, stellt das Tool die

gefakte Verbindung her.

Abschließend können Sie dann in der Protokolldatei des WLAN-Routers das Zustandekommen einer Verbindung mit der MAC-Adresse *AA:AA:AA:AA:AA:AA* finden. Das ist unser WLAN-Client mit der Kali Linux-Installation. Der entsprechende Rechnereintrag in der Protokolldatei lautet einfach *Kali*.

## 1.3 Verschlüsselungslücken ausnutzen

Jeder wie auch immer geartete Sicherheitsmechanismus kann noch so sorgsam entworfen sein: Er wird spätestens bei der Implementierung Lücken und Schwachstellen aufweisen. WEP wurde Anfang 2000 zur Sicherung von drahtlosen Verbindungen eingeführt. Doch schnell war klar, dass dieser Schutz nicht ausreichte und so wurden WPA und WPA2 entwickelt.

Die fundamentale Schwäche von WEP ist die Verwendung von RC4. Mit den Tools der Aircrack-ng-Suite (Airmon-ng, Aireplay-ng, Airodump-ng und Aircrack-ng) ist es heute einfach, diesen Schutz zu knacken. Dazu gehen Sie in der Praxis wie folgt vor:

- Aktivieren Sie zunächst auf dem Access Point die WEP-Verwendung. Dort haben Sie die Möglichkeit, die Passphrase mit einem 64- oder 128 Bit-Schlüssel zu verschlüsseln. Nach dem Sichern steht die WEP-gesicherte Verbindung zur Verfügung.


**Die WEP-Konfiguration auf einem Access Point.**

- Dann führen Sie folgende Kommandos aus, um das Knacken der WEP-Schlüssel mit Ihrem Penetrationsystem vorzubereiten:

```
ifconfig wlan0 up
airmon-ng start wlan0
```

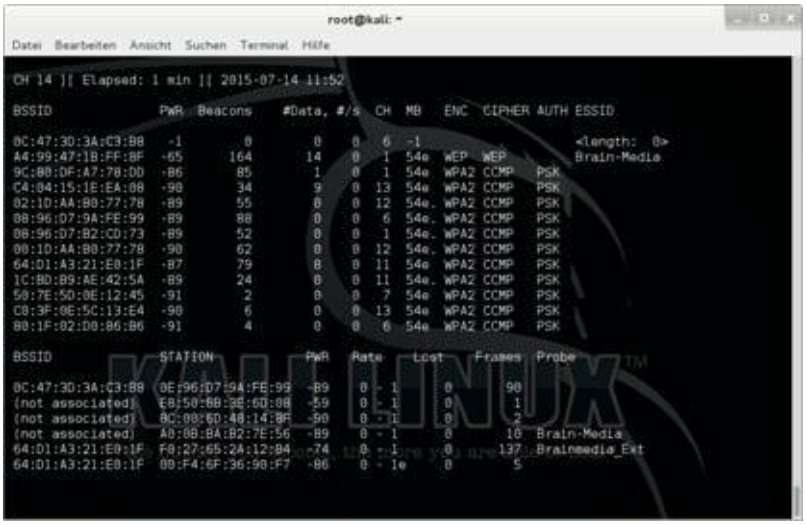
  Mit dem *iwconfig*-Befehl können Sie verifizieren, dass sich die Schnittstelle im Monitormodus befindet.

- Der nächste Schritt dient dem Ermitteln der drathlosen Netzwerke in Ihrer Nähe:

```
airodump-ng mon0
```

- 

- Auf der Konsole werden die erkannten drahtlosen Netzwerke ausgegeben. Dazu jede Menge Details wie die MAC-Adresse, die verwendeten Kanäle und nicht minder wichtig: das Verschlüsselungsverfahren. Wie Sie nachstehender Abbildung entnehmen können, wird dort das Netzwerk *Brain-Media* mit WEP gesichert.




**Airodump-ng hat jede Menge drahtlose Netzwerke im Umfeld ermittelt.**

- Da wir uns nur für den Traffic des WLANs *Brain-Media* interessieren, schränken wir die Darstellung ein:

```
airodump-ng -–bssid A4:99:47:1B:FF:8F —channel 11 —write Brain-Media mon0
```

Bei der Eingabe des Befehls müssen Sie darauf achten, dass Ihnen keine Tippfehler unterlaufen, denn sonst erhalten Sie eine Fehlermeldung.


**Die Beschränkung der Darstellung.**

- Die oben verwendete —*write*-Option schreibt den Traffic in eine CAP-Datei, die die SSID der Access Points als Dateiname verwendet. In diesem Beispiel wird die Datei *Brain-Media-01.cap* erzeugt. Airodump-ng erzeugt außerdem eine CSV-Datei, in der

die Aufzeichnungen festgehalten werden. Das können Sie einfach mit dem Kommando *ls* abrufen.


**Die Aufzeichnungen.**

- Für das Knacken der WEP-Sicherung benötigen wir in der Aufzeichnung möglichst viele Datenpakete. Mit der MAC-Adresse und der Station-Nummer, die Sie einfach mit dem Befehl *airodump-ng mon0* abrufen, injizieren wir als Nächstes einen ARP-Request in das Netzwerk. Dazu führen Sie folgenden Befehl aus:

  airodump-ng -3 -b A4:99:47:1B:FF:8F -h 11:22:33:44:55:66

- Kurz darauf sollten die ARP-Pakete auf der Konsole ausgegeben werden. Etwaige Fehlermeldungen können sie mit der Option *—ignore-negative-one* ausblenden.
- Es folgt das eigentliche Cracken. Dazu starten Sie Aircrack-ng mit der Option *Brain-Media-01.cap* in einem neuen Fenster. Damit beginnt Air-crack-ng automatisch mit dem Knacken der Sicherung und greift dabei auf die Auszeichungsdatei zurück. Zum besseren Verständnis: Aireplay-ng führt die Attacke aus, Aircrack-ng knackt die Sicherung.
- Stehen Aircrack-ng genügend Aufzeichnungen zur Analyse zur Verfügung, so gibt das Tool im Idealfall nach ca. 5 bis 10 Minunten eine Erfolgsmeldung aus:

  KEY FOUND!

  Der Wert wird in eckigen Klammern angezeigt.

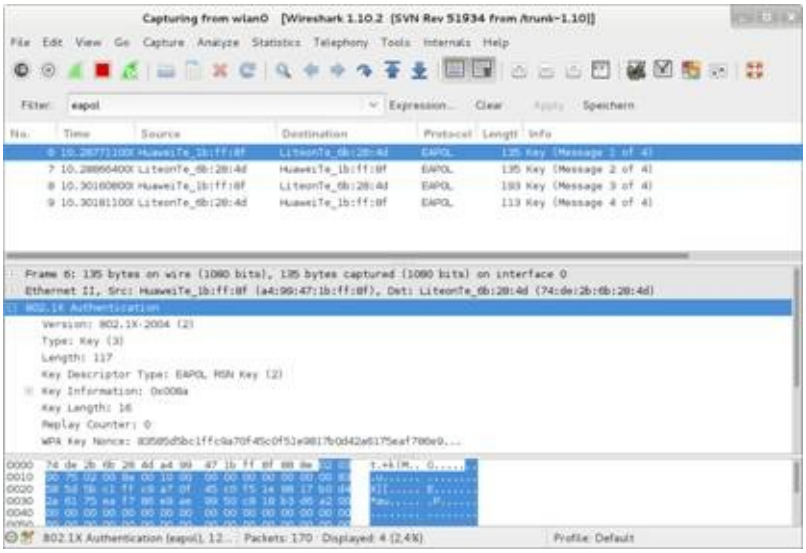
## 1.4 WPA-Sicherung aushebeln

Während WEP-gesicherte Verbindungen ohnehin nicht als sonderlich sicher gel-ten, ist die Sicherheit von WPA- und WPA2-Verbindungen deutlich höher. Doch auch sie sind anfällig, insbesondere gegen Wörterbuchangriffe (dictionary attack). Mit Tools wie Aircrack-ng können Sie versuchen, WPA-/WPA2-Passphrasen zu knacken. Beginnen wir mit dem Knacken einer WPA-PSK-gesicherten Verbindung. Der Aufwand für das Cracken einer solchen Sicherung ist höher, aber dennoch nicht unmöglich. Aktivieren Sie zu Testzwecken daher aus dem WLAN-Access Point die Verwendung von WPA-PSK.

Mit Airodump-ng zeichnen wir wieder den Datenverkehr auf und sichern ihn in einer Datei:

airodump-ng —bssid A4:99:47:1B:FF:8F —channel 11 —write Brain-Media mon0

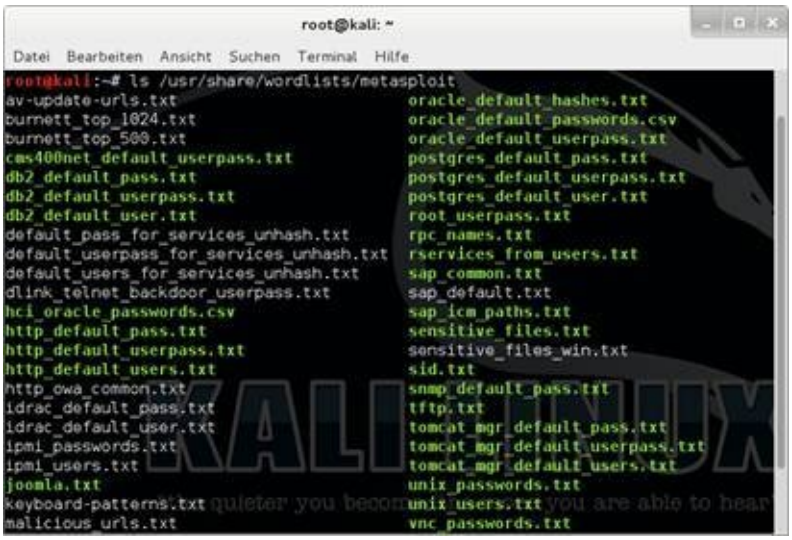
Nun stellen Sie mit einem Client eine Verbindung zu dem Access Point her und zeichnen den WPA-Handshake auf. Auch bei dieser Attacke können Sie eine Deauthentifizierungs-Nachricht an den Access Point senden, damit die Client-Verbindungen unterbrochen und wieder aufgenommen werden.




**Der WPA-Handshake in Wireshark.**

Sowie ein WPA-Handshake erfolgt, zeigt Kali Linux das in der rechten oberen Ecke an. Nun halten wir Airodump-ng an und öffnen die Aufzeichnung mit Wire-shark. Im Sniffer können Sie dann den Vierweg-Handshake unter die Lupe nehmen. Beschränken Sie die Ansicht mit *EAPOL* auf das Handshake-Protokoll. In der Spalte *Info* werden dann die vier Nachrichten aufgeführt (*Message 1 of 4* etc.).

Der nächste Schritt dient dem eigentlichen Knacken des WPA-PSK-Schlüssels. Dazu bedienen wir uns eines weiteren Tools: Metasploit. Für eine Wörterbuchattacke benötigen wir nun ein Verzeichnis mit gängigen Wörtern. Kali Linux verfügt im Metasploit-Ordner über umfangreiche Passwortlisten. Sie liegen im Verzeichnis */usr/share/wordlists/metasploit*.

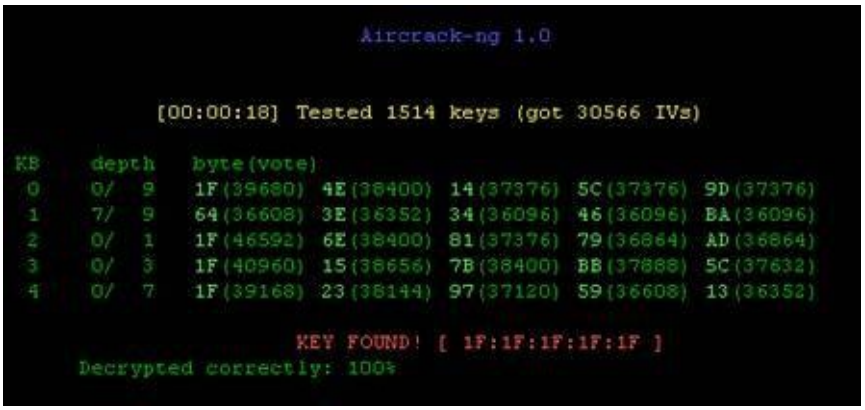



**Bei der Wörterbuchattacke greifen Sie auf Metasploit-Wörterlisten zurück.**

Als Nächstes rufen wir Aircrack-ng mit der Aufzeichnungsdatei und einem Link zur Wörterbuchliste *liste.txt* auf:

```
aircrack-ng Brain-Media-01.cap -w /usr/share/wordlists/liste.txt
```

Aircrack-ng testet nun verschiedenste Passwortkombinationen. Im Idealfall gelingt das Cracken und das Tool gibt eine Erfolgsmeldung aus: *KEY FOUND!*




**Hurra, Aircrack konnte den Schlüssel knacken!**

Gelingt das Knacken nicht, gibt Aircrack-ng entsprechend eine Fehlermeldung aus. In Kali Linux ist mit CowPatty ein weiterer Spezialist für Wörterlistenattacken integriert. Auch dieses Tool analysiert Aufzeichnungsdateien und verwendet Wörterlisten für das Knacken eines WPA-PSK-Schlüssels. Der Auruf erfolgt auf der Konsole mit *cowpatty -optionen*.

WPA2 bietet noch einmal ein deutliches Plus an Sicherheit, weil hier die Passphrase und die SSID verschlüsselt und über 4096 Mal miteinander kombiniert werden. Der Schutz dieses Verfahrens ist erheblich und nicht so einfach zu umgehen. Aber auch hier scheitern Hacker nicht zwangsläufig.

Aber wir können einen Weg einschlagen, um die WPA2-Entschlüsselung zu ermöglichen und zu beschleunigen. Das Zauberwort heißt Pairwise Master Key, kurz PMK, ein vorkalkulierter Schlüssel.

Um den PMK für eine gegebene SSID vorzuberechnen, verwenden wir eine Wortliste und das Programm genpmk. Das führen Sie wie folgt aus:

genpmk –f <wortliste>–d PMK-Brain-Media –s “Brain-Media”

Wir erzeugen als Nächstes ein WPA-PSK-Netzwerk mit der Passphrase *geheim* und zeichnen den Traffic auf. Mit CowPatty können Sie nun versuchen, die Phrase zu entschlüsseln. Sie werden staunen: Das dauert meist nicht einmal 10 Minuten. Wenn Sie den gleichen Vorgang ohne einen vorberechneten Wert mit Aircrack-ng durchführen, kann das auch mal eine halbe Stunde dauern. Sie erkennen damit den Nutzen der Vorberechnung.

## 1.5 WEP- und WPA-Pakete entschlüsseln

Wenn Sie nun den WEP- oder WPA-Schlüssel geknackt haben, stellt sich die nächste Frage: Was machen wir überhaupt damit? Die Beantwortung ist simpel: Wir können den aufgezeichneten oder mitgeschnitten Traffic entschlüsseln, konkret also die WEP- und WPA-Datenpakete öffnen.

Und so gehen Sie in der Praxis vor:

- Ziel ist das Entschlüsseln der oben erstellten Aufzeichnungsdatei *Brain-Media-01.cap*. Hier greifen wir wieder zu einem Werkzeug der Aircrack-ng-Suite: Airdecap-ng. Führen Sie folgenden Befehl aus, um die CAP-Datei zu entschlüsseln:

  airdecap-ng -w schluessel Brain-Media-01.cap

  Der Schlüssel ist bei einer WEP-Verschlüsselung mit 128 Bit sechsundzwanzig Zeichen lang.

  Auf der Konsole können Sie die Entschlüsselung verfolgen. Die entschlüsselten Daten werden anschließend im gleichen Verzeichnis wie die Ausgangsdatei gespeichert. Allerdings besitzt sie den Zusatz *dec*:

  Brain-Media-01-dec.cap

  Mit dem Kommando *tshark* können Sie einen Blick auf die 10 ersten Zeilen werfen.

- Das Entschlüsseln von WPA-verschlüsselten Aufzeichnungen erfolgt nach folgendem Schema:

  airdecap-ng –p schluessel Brain-Media-02.cap –e “Brain-Media”

## 1.6 Verbindung testen

Nachdem Sie den Schlüssel eines WEP- oder WPA-gesicherten WLANs geknackt haben, können Sie natürlich eine Verbindung zu diesem aufnehmen. Das ist dann sozusagen der

„ultimative“ Beweis, dass Sie das WLAN geknackt haben. Je nach Netzwerk können Sie sich dann mehr oder minder frei darin bewegen.

Um die Verbindung zu einem WEP-Netzwerk herzustellen, verwenden Sie den Befehl *iwconfig*:

```
iwconfig wlan0 essid „Brain-Media“ key schluessel
```

Das Herstellen einer Verbindung zu einem WPA-gesicherten WLAN ist ein bisschen komplizierter. Erzeugen Sie eine Konfigurationsdatei *wpa-supp.conf*, die Sie in das Verzeichnis */etc/wpa_suppliant* kopieren. Die sollte wie folgt aussehen:

```
network={
    ssid=“Netzwerkname”
    scan_ssid=1
    proto=RSN
    key_mgmt=WPA-PSK
    pairwise=CCMP
    group=TKIP
    psk=“meinschluessel”
}
```

Die Verbindung können Sie dann wie folgt aufbauen:

```
wpa_supplicant -i wlan0 -D wext -c /etc/wpa_supplicant/wpa_supplicant.conf
```

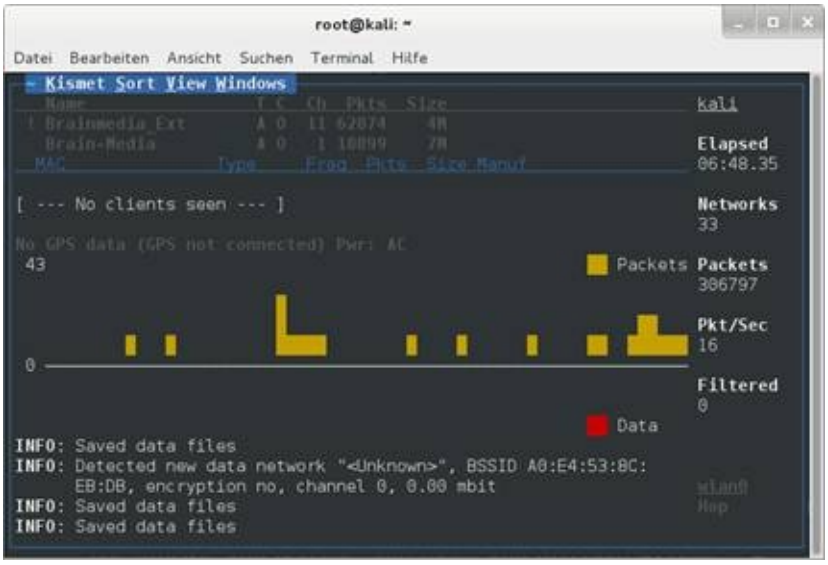
Deutlich einfacher ist der Aufbau einer Verbindung natürlich mit Kali Linux-eigenen Werkzeugen.

# 2 WLANs mit Kismet ermitteln

In Kapitel 1 haben Sie im Schnelldurchlauf die Vorgehensweisen zum Ermitteln und Hacken von drahtlosen Netzwerken kennengelernt. Um zu verstehen, wie Hacker üblicherweise vorgehen und wie man möglichen Attacken begegnet, sollte man deren Herangehensweise kennen.

Das A&O für einen erfolgversprechenden Angriff auf ein drahtloses Netzwerk sind möglichst viele Informationen über das potentielle Ziel. Je besser man über ein WLAN, genauer einen Access Point, informiert ist, umso besser ist man vorbereitet.

In Kapitel 1 haben Sie verschiedene Möglichkeiten kennengelernt, wie Sie Daten über WLAN ermitteln. In diesem Kapitel möchte ich einen weiteren Spezialisten vorstellen, mit dem Sie noch tiefer in verfügbare WLANs vordringen können: Kismet.




**Kismet in Aktion.**

## 2.1 Erste Schritte

Kismet (*http://www.kismetwireless.net*) ist ein multifunktionaler Spezialist für das Erkennen von IEEE 802.11-basierten drahtlosen Netzwerken. Das Programm kann auch als Sniffer und Intrusion Detection System (IDS) eingesetzt werden. Der Spezialist arbeitet mit allen WLAN-Adaptern zusammen, die den Monitormodus unterstützen und kann 802.11b-, 802.11a-, 802.11g- und 802.11n-Traffic sniffen, also aufzeichnen. Über die Plug-in-Architektur können auch prinzipiell Nicht-802.11-Protokolle dekodiert werden.

Kismet identifiziert die drahtlosen Netzwerke durch das passive Sammeln und Erkennen von Paketen. Auch versteckte WLANs, bei denen der Versand des Beacon Frames unterbunden ist, kann der Detektor zuverlässig ermitteln.

Kismet ist Bestandteil einer Kali Linux-Installation, aber Sie können das Programm auch

unter Mac OS X und Windows einsetzen. Der Start unter Kali Linux erfolgt mit folgendem Befehl:

```
kismet
```

Wenn Sie Kismet unter einer anderen Linux-Distribution einsetzen, sollten Sie beachten, dass das Programm für die meisten Aktionen Root-Berechtigungen benötigt.

Nach dem Start des Programms erfolgt die Abfrage, ob Sie die Verbindung zum Kismet-Server herstellen wollen. Das bestätigen Sie mit *Yes*. Als Nächstes legen Sie das Interface fest, über das die Aufzeichnung läuft. Geben Sie dazu einfach die gewünschte Interface-Bezeichnung ein, beispielsweise *wlan0*.

Die Liste der verfügbaren WLAN-Interfaces erhalten Sie mit folgendem Befehl:

```
iwconfig
```

Kismet erkennt dann automatisch den Typ und die unterstützten Channel. Falls nicht, müssen Sie das gegebenenfalls in der Kismet-Konfiguration manuell nachholen.

Sollte der Typ nicht erkannt werden, können Sie den verwendeten Chipsatz bei einer PCI- oder PCMCIA-Karte identifizieren:

```
lspci | grep -i net
```

Bei einem USB-Adapter lautet der Befehl entsprechend *lsusb*.

Mit diesen Informationen können Sie dann auch gegebenenfalls den korrekten Treiber installieren. Die entsprechenden Informationen finden Sie in der Datei */usr/share/doc/kismet* im Abschnitt *Capture Sources*.

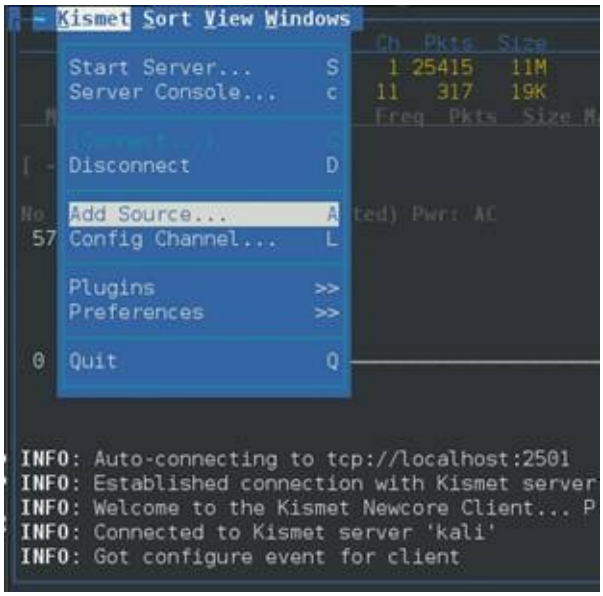
Kismet legt außerdem umfangreiche Protokolldateien an, denen Sie weitere Informationen entnehmen. Kismet schreibt seine Konfiguration in die Konfigurationsdatei */etc/kismet/kismet.conf*.

Das Interface, das Sie zum Sammeln der Daten verwenden, wird in der Konfiguration durch folgenden Eintrag konfiguriert, der den Source-Typ, das Interface und eine erklärende Bezeichnung enthält:

```
source=none,none,notiz
```

In der Regel genügt es allerdings, wenn Sie Kismet dem WLAN-Adapter mitteilen.

Sie können in Kismet auch jederzeit eine neue Schnittstelle anlegen. Dazu verwenden Sie den Menübefehl *Kismet > Add Source*.




**Das Anlegen eines neuen Adapters.**

Alle Pakete in Kismet stammen von einer sogenannten Capture-Quelle. Dabei handelt es sich üblicherweise um die Netzwerkkarte eines lokalen Systems. Allerdings kann es sich dabei auch um Aufzeichnungen handeln, die Sie mit einem anderen Werkzeug erstellt haben. Airodump-ng erzeugt beispielsweise bei Verwendung der —*write*-Option ebenfalls eine Datei im Kismet-Format.

Da Kismet in der Regel den korrekten Treiber identifiziert und die unterstützten Kanäle für die Aufzeichnung verwendet, dürfte das für die meisten Anforderungen genügen. Unabhängig davon stellt Ihnen Kismet vielfältige Schalter für die Steuerung des Programms zur Verfügung.

Da Kismet Pakete der IEEE 802.11-Schicht aufzeichnet, muss der Netzwerkmodus so angepasst werden, dass eine „normale“ Verwendung der Schnittstelle nicht mehr möglich ist. Sollten Sie mit dem Notebook parallel weitere Dienste nutzen wollen, müssten Sie gegebenfalls einen weiteren WLAN-Adapter einrichten.

Wenn Sie über die Kismet-Benutzerschnittstelle mit dem Befehl *Add Source* eine Schnittstelle angelegt haben, finden Sie den entsprechenden Eintrag in der Kismet-Konfigurationsdatei *kismet.conf* mit der Option *ncsource=*. Ein entsprechender Eintrag sieht wie folgt aus:

```
ncsource=wlan0:option1=wert1,option2=wert2
```

Wenn Sie eine bereits existierende PCAP-Datei analysieren wollen, so geben Sie einfach den Pfad in der Konfigurationsdatei an:

```
ncsource=/home/pfad/aufzeichnung.pcap
```

Sie können mit Kismet auch eine Airpcap-Device eines Windows-Systems aufzeichnen:

```
ncsource=airpcap
```

Sie können auch die Daten einer Remote-Installation verwenden. Auch hierfür verwenden Sie die Option *ncscouce*. Ein Beispiel:

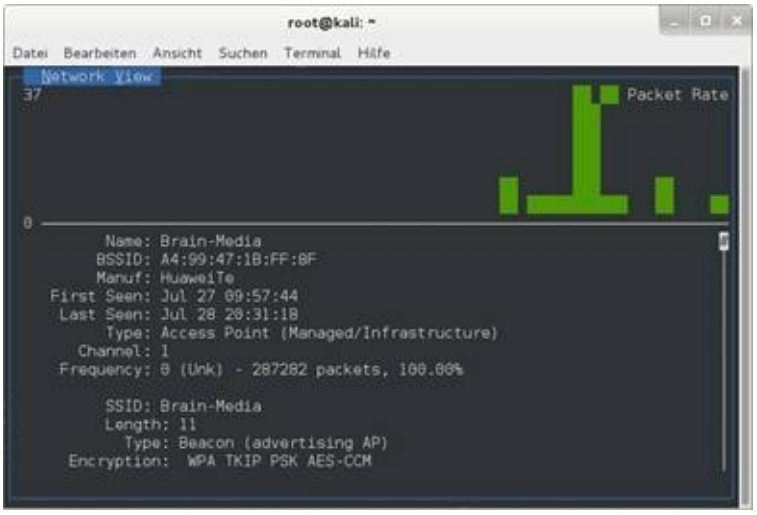
```
ncsource=drone:host=192.168.2.100.2,port=2502
```

Dabei wird der Server gestartet und die Oberfläche im Terminal geladen. Im Startfenster den Cursor in das kleine Begrüßungsfenster schieben und die Leertaste drücken. Weitere Aufrufe sind unter *Nützliche Kommandozeilenparameter* aufgeführt.

Kismet verwendet eine ein wenig antiquiert wirkende Benutzerschnittstelle, die an „alte“ DOS-Zeiten erinnern. Die gefundenen Netzwerke stellt das Programm in einer Tabelle mit einigen wichtigen Informationen dar:

- **Name**: SSID des Netzwerks
- **T**: Typ des Netzwerks
- **W**: Informationen zu WEP
- **Ch**: Verwendeter Kanal
- **Pkts**: Anzahl gesammelter Pakete
- **Size**: Paketgröße

Mit Hilfe der *Pfeil hoch*- und *Pfeil runter*-Tasten bewegen Sie sich in der Netzwerkliste.




**Die Details zu einem drahtlosen Netzwerk.**

Details zu einem Netzwerk rufen Sie ab, indem Sie einen Eintrag markieren und dann die Enter-Taste betätigen. Durch Betätigen der ESC-Taste greifen Sie auf das Kismet-Menü zu.

Wenn Sie die Details abrufen, werden diese in einem Unterfenster angezeigt. Den Details können Sie entnehmen, welche Verschlüsselungstechnik zum Einsatz kommt und welchen

Kanal der Access Point verwendet. Den Details können Sie auch die aktuellen Client-Verbindungen entnehmen.

Über die GUI können Sie außerdem die Sortierungen ändern. Dazu verwenden Sie das Menü *Sort*. Das stellt Ihnen verschiedene Sortierungmöglichkeiten zur Verfügung, beispielsweise folgende:

- Typ
- Kanal
- Verschlüsselung
- BSSID
- SSID
- Signal
- Packet

Das *View*-Menü erlaubt Ihnen das Ein- und Ausblenden verschiedener Informationen. Sie können beispielsweise den Status- und die Quellinformationen ausblenden.

## 2.2 Anpassungsmöglichkeiten

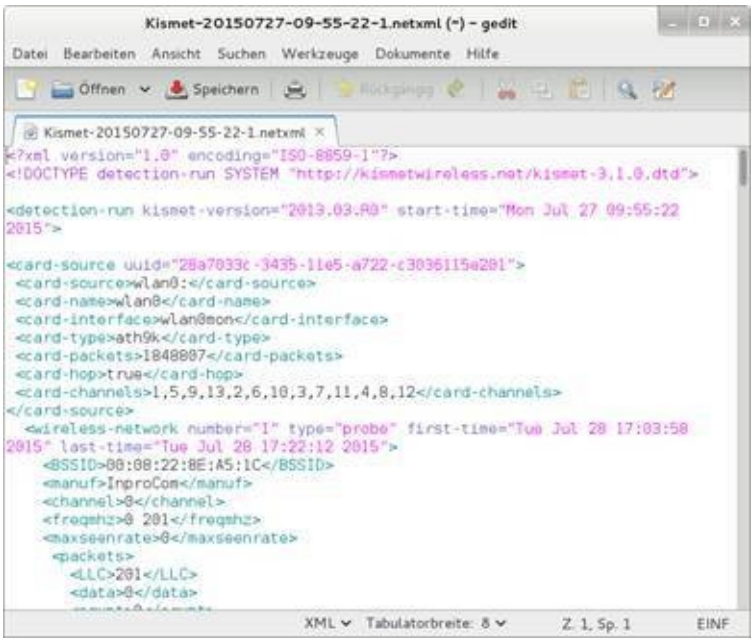
Das Kismet-Menü bietet Ihnen verschiedene Anpassungsmöglichkeiten, hier insbesondere das Untermenü *Preferences*, aber Kismet ist auch über Plug-ins funktional erweiterbar.

Unter *Preferences* können Sie beispielsweise mit dem Untermenü *Startup & Shutdown* festlegen, ob Kismet automatisch beim nächsten Systemstart ausgeführt werden soll. Sie können auch die Farbgestaltung – soweit man das als solche bezeichnen kann – und die Tonausgabe anpassen. Wenn Sie die Verwendung von GPS-Daten in der Kismet-Konfiguration eingerichtet haben, können Sie auch die Verwendung dieser Daten ändern.

Kismet protokolliert standardmäßig die PCAP-Datei, das GPS-Signal (sofern es verwendet wird), Warnungen und Netzwerkinformationen in XML- und Textformat. Für das Logging verwendet das Tool insbesondere den PPI-Header, dem man beispielsweise mit Wireshark verschiedene technische Informationen entnehmen kann. Das Protokollformat wird über die Kismet-Konfigurationsdatei mit folgenden Einträgen bestimmt:

```
pcapdumpformat=ppi
pcapdumpformat=80211
```

Die Protokolldatei besitzt ein XML-Format und die Dateierweiterung *netxml*. Das Lesen und Verstehen der XML-basierten Daten ist nicht unbedingt einfach. Doch hier gibt es mit dem Kismet Log Viewer ein interessantes Werkzeug, das die XML-Daten lesbar aufbereitet. Sie finden den Viewer unter folgender URL:




**Die Kismet-Protokolldatei in Texteditor.**

Kismet stellt Ihnen auch einfache Filterfunktionen zur Verfügfung, mit denen Sie Rechner oder ganze Netzwerke auf Basis von BSSID, Quell- oder Ziel-MAC-Adresse von der Verfolgung ausschließen können.

Sie können mit der Filterung gezielt Systeme von der Analyse aus- bzw. einschließen. Leider ist die Filterkonfiguration ein wenig umständlich vorzunehmen, da sie in der Kismet-Konfigurationsdatei hinterlegt wird. Damit Kismet nur die Pakete des Netzwerks mit der BSSID *AA:BB:CC:DD:EE:FF* vornimmt, verwenden Sie folgenden Eintrag:

```
filter_tracker=BSSID(AA:BB:CC:DD:EE:FF)
```

Sie können den Filter auch umkehren. Dazu verwenden Sie das Ausrufungszeichen als Operator. Um die Pakete dieser MAC-Adresse auszuschließen, verwenden Sie diese Konfiguration:

```
filter_tracker=BSSID(!AA:BB:CC:DD:EE:FF)
```

Sie können auch mehrere MAC-Adressen in einem Filter verwenden:

```
filter_tracker=BSSID(!AA:BB:CC:DD:EE:FF,!00:11:22:33:44:55)
```

MAC-Adressen können auch ähnlich wie Netmask-Bereiche angegebenen werden. Auf diesem Weg können Sie nur Netzwerke eines Herstellers verarbeiten:

```
filter_tracker=BSSID(AA:BB:CC:00:00:00/FF:FF:FF:00:00:00)
```

Auch die Quellenangabe kann für die Filterung herangezogen werden. Um lediglich die Pakete, die von der MAC-Adresse 11:22:33:44:55:66 stammen, darzustellen, verwenden Sie folgenden Eintrag in der Kismet-Konfigurationsdatei:

```
filter_tracker=SOURCE(11:22:33:44:55:66)
```

Anstelle der Quelle können Sie mit *DEST* auch die Zieladresse angeben.

Kismet kann in seiner Ausgabe auch GPS-Daten verwenden. Die entsprechenden Daten werden dann in der tabellarischen Übersicht der Kismet-Startseite ausgegeben und in visualisierter Form dargestellt. Kismet greift dabei auf das Tool GPSMAP zurück, das die NETXML- und GPSXMLX-Dateien einliest, die Daten auswertet, Karten aus unterschiedlichen Quellen bezieht und daraus aus eine Darstellung der Scan-Ergebnisse generiert.

Der Darstellung können Sie die ungefähre Position und den Sendebereich entnehmen.

Damit Sie die GPS-Funktion nutzen können, die standardmäßig in der Kismet-Konfiguration aktiviert ist, benötigen Sie einen GPS-Empfänger. Kostengünstige USB-Geräte können im Fachhandel oder über bekannte Online-Shops bezogen werden. Auch Bluetooth-GPS-Geräte können für die Verwendung der GPS-Daten verwendet werden.

## 2.3 Kismet mit Plug-ins erweitern

Eine weitere Besonderheit von Kismet: Sie können das Programm um Plug-ins erweitern und somit beispielsweise die Prototkollfunktionen, die Ausgabe von IDS-Warnungen, das Hinzufügen von neuen Capture-Quellen und von weiteren grafischen Komponenten hinzufügen. Da Plug-ins Zugriff auf die Kismet-Sourcen- und Konfigurationsdateien benötigen, sollten Sie im Falle von Kismet-Versionsänderungen neu kompiliert werden.

Wie wir oben gesehen haben, basiert Kismet auf einer Client-Server-Architektur. Prinzipiell können die Erweiterungen auf Seiten des Clients oder des Servers ausgeführt werden.

Plug-ins für den Kismet-Server werden standardmäßig im Verzeichnis */usr/local/lib/kismet/* abgelegt, die des Users in *~/.kismet/plugins*. Die Server-Plug-ins werden nur dann geladen, wenn in der Kismet-Konfigurationsdatei *kismet.conf* folgende Einstellungen vorgenommen ist:

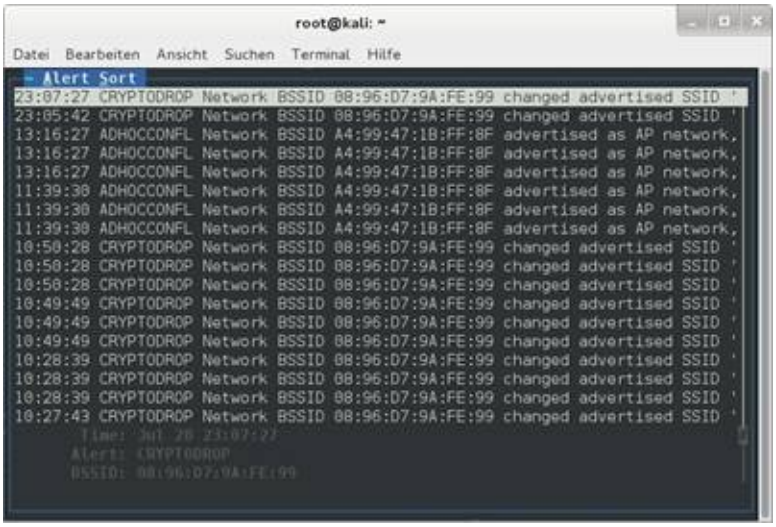
```
allowplugins=true
```

Die Client-Plug-ins holt sich Kismet aus dem systemweiten Plug-in-Verzeichnis */usr/local/lib/kismet_client* oder aus dem Benutzerverzeichnis *~/.kismet/cli-ent_plugins*. Nachdem Sie das Plug-in in den betreffenden Ordner kopiert haben, können Sie dieses nach einem Neustart von Kismet über das Plug-in-Untermenü aktivieren und einrichten. Eine Übersicht der aktuell verfügbaren Erweiterungen finden Sie unter folgender URL:

```
https://www.kismetwireless.net/links.shtml
```

## 2.4 Kismet als IDS

Kismet leistet Ihnen nicht nur hervorragende Dienste beim Scannen von WLANs und dem Ermitteln relevanter Informationen, sondern stellt Ihnen auch einfache Intrusion Detection System-Funktionen zur Verfügung. Kismet kann als zustandsorientiertes und zustandsloses IDS für Layer 2 und 3-WLAN-Attacken verwendet werden. Die Warnungen können dabei auf Fingerprints und auf Trends basieren. Da Kismet einen leistungsfähigen Exportmechanismus besitzt, können diese Daten auch in Snort & Co. verwendet werden.




**Die von Kismet verwalteten Warnungen.**

Die IDS-Funktionen konfigurieren Sie im Abschnitt *alert=* der Kismet-Konfigurationsdatei. Dort stehen Ihnen zwei Zeitparameter zur Verfügung: *throttle* und burst. Mit der Option *trottle* bestimmen Sie, wie viele Warnungen pro Zeiteinheit zulässig sind, die Option *burst* bestimmt, wie viele Warnungen in einer Reihe ausgegeben werden können. Ein Beispiel:

```
alert=NETSTUMBLER,5/min,1/sec
```

Diese Konfiguration erlaubt eine Warnung pro Sekunde bei maximal fünf pro Minute.

Dabei sind verschiedenste Warnungen möglich. In voranstehendem Beispiel wird die NetStumbler-Ausgabe für das Erzeugen einer Warnung verwendet. Kismet kann fast 20 weitere Quellen verwenden. In voranstehendem Beispiel taucht der Eintrag *CRYPTODROP* auf. Dabei kann es sich um eine Spoofing-Attacke handeln.

Mit Kismet können Sie sogar ein verteiltes IDS aufbauen. Dazu verwandeln Sie eine Kismet-Installation in einen Agent. In der Kismet-Terminologie wird eine solche Installation auch als Drohne, der sammelnde Server als Drohnen-Server bezeichnet.

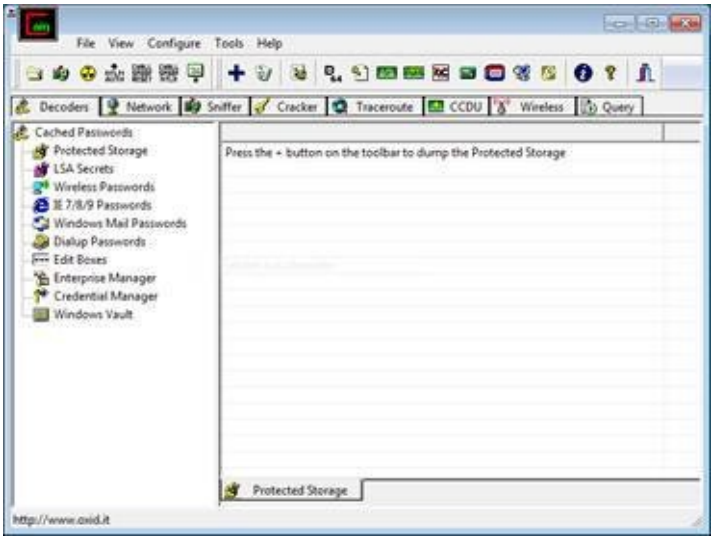
Die Daten der einzelnen Kismet-Installationen werden an den zentralen Server übermittel. Dazu muss in der Kismet-Konfiguration der Server hinterlegt werden. Einen Drohnen-Server richten Sie mit der Konfigurationsdatei *kismet_drone.conf* ein, die Sie im gleichen

Verzeichnis wie die Kismet-Konfigurationsdatei finden. Hier weisen Sie dem Server eine Bezeichnung zu und hinterlegen die Clients, von denen die Daten gesammelt werden.

Kismet bietet in der Summe eine Fülle von nützlichen Funktionen für das Ermitteln von drahtlosen Netzwerken. Aber der Einsatz im Unternehmen macht nicht nur zur WLAN-Ermittlung Sinn, sondern die IDS-Funktionen sollten für eine Abwehr gegen mögliche Attacken genutzt werden.

## 2.5 Alternative Werkzeuge

Kismet und die in Kali Linux integrierten Werkzeuge sind ein guter Ausgangspunkt, doch nicht immer ist Linux als Betriebssystem die erste Wahl. Da in den meisten Unternehmen Windows-Rechner dominieren, stellt sich die Frage, ob es auch für diese Plattform geeignete Werkzeuge gibt? Die gute Nachricht: Ja, es gibt sie. Sogar sehr interessante, mit denen man auch verschiedene Angriffsszenarien simulieren kann. In diesem Abschnitt lernen Sie drei weitere Hilfsmittel für Windows kennen, die Ihnen beim Scannen von WLAN und dem Identifizieren von weiteren Schwachstellen eine wertvolle Hilfe sind.




**Der Klassiker für MitM-Attacken: Cain & Abel.**

### 2.5.1 Cain & Abel – typisches Einsatzszenario

Eines der Werkzeuge, das Sie kennen sollten, ist Cain & Abel (*http://www.oxid.it/cain.html*). Eigentlich dient es dazu, Passwörter wiederherzustellen und Netzwerk-Traffic zu sniffen, aber es kann auch zur Prüfung der WLAN-Sicherheit verwendet werden.

Um tiefer in ein Netzwerk, seine Struktur und seine Anwendungen eindringen zu können, müssen Sie Daten abfangen, mit denen Sie irgendwie weiterkommen. Dabei sind ARP-Spoofing-Methoden sehr hilfreich, und hierbei insbesondere die sogenannten Man-in-the-Middle-Angriffe, kurz MitM, die auch als Janusangriffe (in Anspielung auf den doppelgesichtigen Janus der römischen Mythologie) genannt werden.

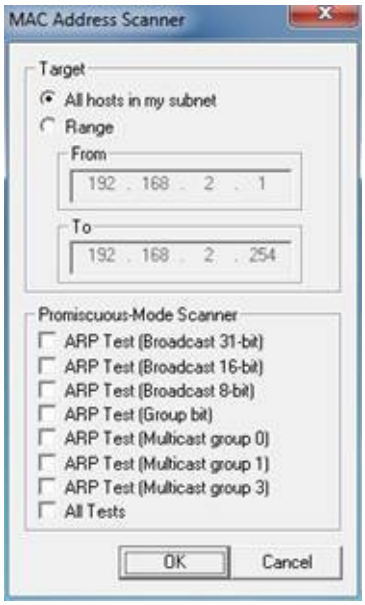
ARP-Spoofing ist eine spezielle Man-in-the-Middle-Attacke. Dabei befindet sich der

potenzielle Angreifer entweder physikalisch oder logisch zwischen den beiden Kommunikationspartnern. Er hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Die Janusköpfigkeit des Angreifers besteht darin, dass er den Kommunikationspartnern vortäuscht, dsa jeweilige Gegenüber zu sein.

Als eines der besten Werkzeuge dieser Art gilt das Windows-Programm Cain & Abel (*http://www.oxid.it/cain.html*). Die Anwendungsbereiche sind sehr vielfältig. Sie können damit beispielsweise Passwörter abgreifen und knacken, WLAN-Traffic mitschneiden und vieles mehr. Beim ARP-Spoofing werden gefälschte ARP-Pakete an das Ziel übermittelt. Dabei wird beim Zielrechner die ARP-Tabelle überschrieben, wodurch der gesamte Netzwerkverkehr des Zielrechners auf den Penetration-Rechner umgeleitet wird. Das Besondere an Cain & Abel: Es ist ein Multifunktionswerkzeug, welches nicht nur das einfache Auslesen aller Passwörter, sondern eben auch das Sniffing, die Durchführung von Brute Force-Attacken und noch vieles mehr erlaubt.

Nach der Installation müssen Sie zunächst die Netzwerkkonfiguration anpassen. Dazu klicken Sie in der Symbolleiste auf das zweite Symbol von links (*Start/Stop Sniffer*). Wählen Sie den Netzwerkadapter aus, den Sie für die Aufzeichnung verwenden wollen. Dann aktualisieren wir im Hauptfenster die Hostliste. Öffnen Sie die Registerkarte *Sniffer* und dort das Unterregister *Hosts*.

Anschließend bestimmen Sie den Adressbereich, der für Sie von Interesse ist. Dazu klicken Sie auf das Pluszeichen, bestimmen den Bereich oder wählen alle Hosts des Subnetzes, in dem Sie sich befinden. Mit einem Klick auf *OK* wird die Liste aktualisiert. Das Tool durchkämmt das Netzwerk und stellt Ihnen die gefundenen Hosts in einer Tabelle zur Auswahl.

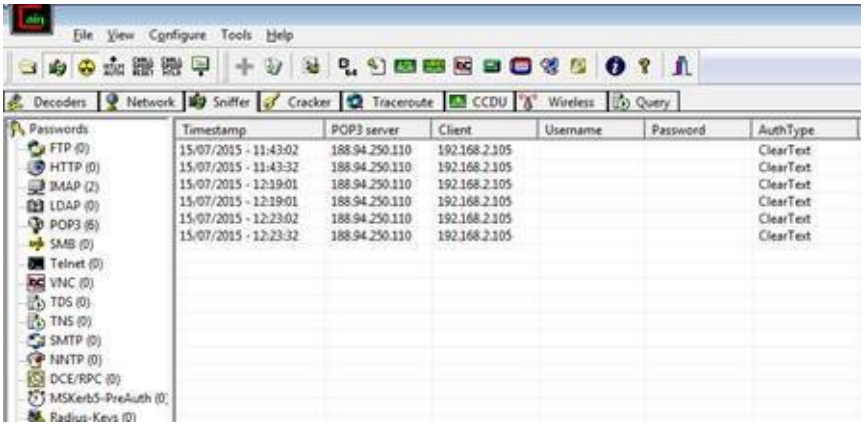



**Die Konfiguration des Adressbereichs.**

Wählen Sie das Ziel aus. Dazu wechseln Sie zur Registerkarte *ARP*. Markieren Sie in der

linken Spalte zunächst den Haupteintrag *ARP*. Es öffnet sich rechts ein zweigeteilter Bereich. Mit einem Klick erscheint in der Symbolleiste das blaue Pluszeichen. Cain & Abel präsentiert Ihnen den Dialog *ARP Poison Route*. Dort wählen Sie links beispielsweise Ihren DSL-Router und rechts einen Zielrechner. Mit Cain & Abel können Sie sich dann zwischen diese beiden Komunikationspartner einhängen.

Um den eigentlichen Angriff zu starten, klicken Sie den Radioaktiv-Button (*Start/Stop ARP*). Wenn Sie parallel dazu den Traffic mit Wireshark aufgezeichnet haben, können Sie diesen mitlesen.




**Die Registerkarte *Passwords* verrät Ihnen nun, welche Passwörter zwischen den beiden Systemen ausgetauscht wurden.**

Wenn Sie nun die Registerkarte *Passwords* öffnen, können Sie dort Informationen (Benutzername/Passwort) abrufen, die zwischen den beiden Rechnern übermittelt wurden, zwischen die Sie sich mit Cain & Abel gesetzt haben. Wenn das Passwort dann auch noch im Klartext übermittelt wird, haben Sie den Zugang zum jeweiligen Dienst.

Bei der Ausführung von Cain & Abel ist zu beachten, dass es sich dabei um ein Windows-Programm handelt und daher nicht direkt auf einem Kali Linux-System, wohl aber auf einer VM ausgeführt werden kann. Für den Betrieb von Cain & Abel müssen Sie außerdem die windowseigene Firewall oder die eines Drittanbieters deaktivieren.

Wenn Sie einen genaueren Blick auf die Benutzerschnittstelle von Cain & Abel werfen, stellen Sie fest, dass es dort auch eine Registerkarte *Wireless* gibt. Bevor Sie diese Funktion verwenden können, müssen Sie einen zweiten WLAN-Adapter samt AirPCAP-Treiberinstallation besitzen.

Cain & Abel kann aktiv und passiv nach WLAN Access Points suchen. Für das aktive Scannen verwendet das Programm den WinPCAP-Paketreiber für die Steuerung des WLAN-Adapters. Access Points und Ad-hoc-Netzwerke werden mit Hilfe des Windows DDK ermittelt.

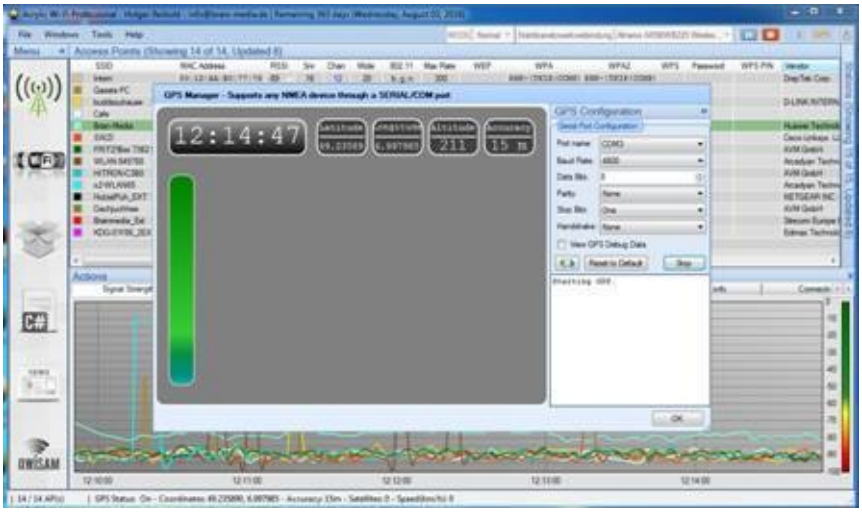
Für das passive Scannen greift Cain & Abel auf den AirPCAP-Treiber zurück, der Access Points (obere Liste) und Clients (untere Liste) ermittelt.

Mit einem Klick auf die *Analyze*-Schaltfläche macht sich das Programm an die Analyse der WLAN-Sicherung. Das Ergebnis präsentiert Ihnen Cain & Abel im Dialog *Wireless*

*Encrypted Networks*. Dort stehen Ihnen auch drei Angriffsfunktionen zur Verfügung, mit denen Sie versuchen können, WEP- oder WPA-Schlüssel zu knacken.

### 2.5.2 Komfortabels WLAN-Scannen: Acrylic WiFi

Wenn Sie bereit sind, ein paar Euros zu investieren, sollten Sie sich einmal Acrylic WiFi Pro (*https://www.acrylicwifi.com/de*) anschauen, das auch in einer freien Version verfügbar ist. Mit Acrylic WiFi können Sie die WLAN-Netze in Ihrer Reichweite erkennen und scannen, Sicherheitsinformationen einlesen und generische WLAN-Passwörter erstellen.




**Acrylic WiFi Pro in Aktion.**

Die Benutzerschnittstelle zeigt Informationen zu WLAN-Netzen und WIFI-Empfängern an, die aktuell erreichbar sind. Anhand von Grafiken zur Signalstärke der Zugriffspunkte erkennen Sie direkt, wer wie stark sendet. Mit der Inventarfunktion können Sie Namen für bekannte WLAN-Empfangsgeräte anlegen und verwalten.

Das Programm bietet Ihnen jede Menge Sicherheitsinformationen zu WEP, WPA oder WPA2 und erlaubt sogar das Attackieren solcher Schutzmaßnahmen. Acrylic WiFi zeigt auch detaillierte Informationen zu verborgenen WLAN-Netzen an. Auch die Anzeige der Pakete ist möglich, denn das Programm funktioniert wie ein WLAN-Sniffer. Alternativ kann über einen Treiber auch eine Wireshark-Installation integriert werden. Die Pro-Variante kann auch den Monitormodus aktivieren und so detaillierte Paketinformationen liefern. Auch die Integration eines GPS-Empfängers ist möglich.

### 2.5.3 NetStumbler

Im bisherigen Verlauf dieses Einstiegs haben Sie einige Werkzeuge für das Ermitteln von Access Points und deren Eigenschaften kennengelernt. Eine weitere Anwendung sollten Sie insbesondere dann kennenlernen, wenn Sie vorzugsweise mit Windows arbeiten.

Als Schweizer Taschenmesser für die drahtlose Netzwerkanalyse gilt NetStumbler

(*http://www.netstumbler.com*). Auch wenn man bei der Programmbezeichnung damit rechnen könnte, dass man mit dem Tool eher durch ein Netzwerk stolpert, als, dass man es systematisch erkundet, ist doch eher das Gegenteil der Fall: Mit NetStumbler können Sie nahezu jeden Bereich einer drahtlosen Infrastruktur ermitteln. Das Programm ist für den privaten Einsatz kostenfrei. Der Entwickler bittet professionelle Anwender um 50 Dollar. NetStumbler unterstützt alle gängigen WLAN-Adapter und kann in der Regel sehr zuverlässig Access Points, das Rauschen und die Signalstärken ermitteln.

# 3 WLAN-Infrastruktur testen

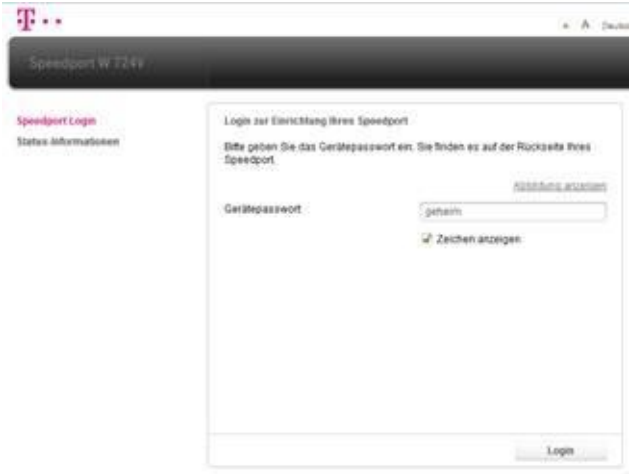
Der Begriff WLAN-Infrastruktur fasst all die Komponenten und Dienste zusammen, die WLAN-spezifische Dienste bereitstellen. Jede Komponente und jeder Dienst stellt dabei einen potenziellen Angriffspunkt dar. Dabei kann es sich um Access Points, aber auch Standard-Accounts handeln. In diesem Kapitel schauen wir uns die verschiedenen Möglichkeiten an, wie man Komponenten und Dienste einer typischen WLAN-Infrastruktur attackieren kann.

## 3.1 Access Point attackieren

Die drahtlosen Access Points sind die wichtigsten Elemente einer WLAN-Infrastruktur. Obwohl Sie eine exponierte Rolle übernehmen, sind sie erstaunlicherweise sehr oft nahezu ungeschützt. Oftmals verwenden Access Points den Standardbenutzernamen und das Standardpasswort, das ihnen bei der Auslieferung zugewiesen wurde. Dann ist ein „Angriff“ ein Kinderspiel. Und selbst wenn das Passwort geändert wurde, ist es dennoch recht einfach, durch raten oder eine Wörterbuch-Attacke Zugang zu dem Access Point zu erlangen.

Mit Acrylic Wi-Fi Professional, Airodum-ng oder Cain & Abel können Sie einfach nach Access Points in Ihrer Umgebung fahnden und diese mit den verbundenen Clients ermitteln.

Die oben genannten Tools verraten Ihnen, wer der Hersteller ist und gegebenenfalls weitere Details, wie die exakte Produktbeschreibung.  Welches die Benutzernamen und das Standardpasswort eines Access Points eines bestimmten Herstellers sind, können Sie einfach dem jeweiligen Produkthandbuch entnehmen, die üblicherweise bei allen Herstellern über deren Website verfügbar sind. Bei TP-Link-Geräten lautet der Administratorbenutzernamen meist *admin*, dass Passwort ist leer. Bei Netgear lautet der Admin-Benutzer üblicherweise *admin* und das Passwort *password*. Ein Telekom Speedport-Router besitzt keinen Benutzer, das Passwort lautet unter Umständen *0000*. Bei AVM-Geräten ist es ähnlich. Mit den Zugangsdaten *admin/admin* bzw. *admin/password* liegen Sie oft richtig.




**Ein Standard-Login-Dialog wie der des Speedport bietet oft nur einen unzureichenden Schutz des Access Points.**

Wenn Sie nun wissen, welche Clients auf einen Access Point zugreifen, so ist das ein einfachster Ansatz für die Attacke: Sie verwenden die gängigen Zugangsdaten oder versuchen es mit der Rechnerbezeichnung der zugreifenden WLAN-Clients. Sollten Sie an einen Access Point geraten, der weiterhin die Zugangsdaten der Erstauslieferung verwendet, haben Angreifer den Zugangspunkt nach wenigen Klicks unter ihrer Kontrolle.

Passwörter sind vermutlich das Sicherheitsrisiko Nr. 1. Selbst dann, wenn Sie das Passwort eines Access Points nicht kennen, ist es weitaus einfacher, sich zu diesem Zugang zu verschaffen. Hierfür gibt es zwei Ansätze: Sie können eine Brute Force- oder eine Wörterbuch-Attacke für das Knacken des Passwortes verwenden. Insbesondere Wörterbuchattacken erzielen meist das gewünschte Ergebnis.

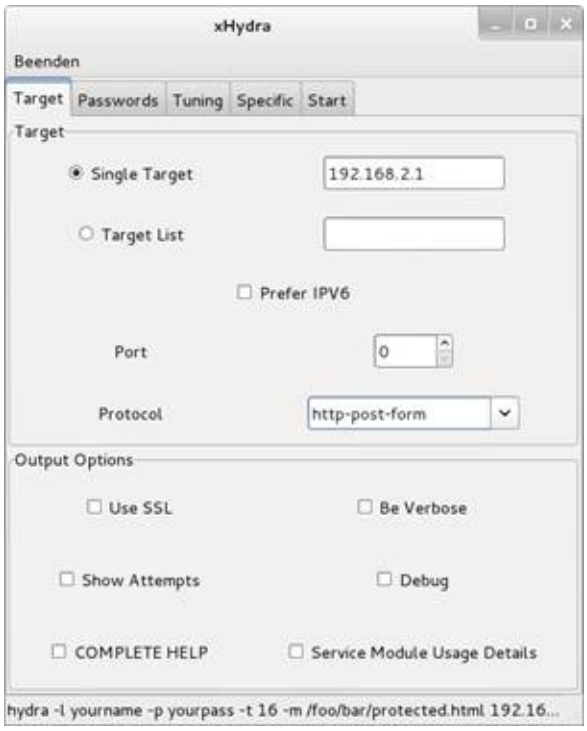
Doch wie gehen Sie dabei vor? Die Antwort auf diese Frage ist schnell beantwortet: Greifen Sie zu einem entsprechenden Spezialisten. Wenn Sie mit Kali Linux arbeiten, ist dort mit Hyrda bzw. der grafischen Variante xHydra ein Tool inte-griert, mit dem Sie insbesondere Wörterbuchattacken ausführen können.

Ich persönlich ziehe die GUI-Variante vor, weil Sie einfacher zu verwenden und weniger fehleranfällig ist. Sie starten xHydra auf der Konsole mit folgender Eingabe:

```
xhydra
```

Hydra ist ein parallel arbeitender Login-Cracker, der alle relevanten Protokolle und Dienste unterstützt, die für einen Penetrationtester in der Regel von Bedeutung sind. Sie werden nicht schlecht staunen:

Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1, v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC und XMPP




**Der Startbildschirm von xHydra.**

Für HTTP, POP3, IMAP und SMTP stehen spezifische Login-Funktionen wie die Verwendung von reinem Text oder von MD5-Digests zur Verfügung. Das Ziel von Hydra und xHydra: Dem Penetrationstester steht ein Tool für den Machbarkeitsnachweis (Proof of concept) zur Verfügung, mit dem er prüfen kann, ob Hacker sich über einen Login-Dialog Zugang zu einem System verschaffen können.

Die Verwendung von xHydra ist wirklich einfach. Nach dem Start geben Sie zunächst auf der Registerkarte *Target* die IP-Adresse des bzw. der Ziele an. Ziele können Sie in einer Zielliste anlegen. Wichtig für den Zugriff auf den Access Point und dessen webbasierte Schnittstelle ist die korrekte Wahl des Protokolls. Hier verwenden Sie *http-post-form*. Wenn Sie andere Dienste wie einen FTP- oder Telnet-Server knacken wollen, verwenden Sie entsprechend die Protokolle *ftp* bzw. *telnet*.


**Die Passworteinstellungen.**

Als Nächstes wenden Sie sich den Passworteinstellungen zu, die Sie auf der Registerkarte *Passwords* vornehmen. Als Benutzername tragen Sie den vermeintlich verwendeten Benutzer ein. Mit *admin* liegen Sie meist richtig.

Da Sie das Passwort vermutlich nicht kennen, verwenden Sie unter *Password* die Option *Password List*. Dabei sollte es sich um eine Textdatei handeln, in der die möglichen Passwörter hinterlegt sind.

Nun können Sie diese Liste selbst anlegen. Aber es geht auch einfacher: Verwenden Sie doch bestehende Passwortlisten. Doch wo holt man diese her? Hierfür gibt es verschiedene Quellen. Am effektivsten dürfte die Verwendung von sogenannten Rainbow Tables sein. Diese „Regenbogentabellen“ besitzen eine spezielle Datenstruktur, die eine schnelle, probabilistische Suche nach einem Element des Urbilds (meist ein Passwort) eines gegebenen Hash-Werts erlauben. Unter folgender URL stehen verschiedene solcher Dateien zum Download bereit:

http://project-rainbowcrack.com/table.htm

Sie umfassen mehrere Milliarden Einträge (ja, Sie lesen richtig) und dürften daher in der Regel auch einen geeigneten Passworteintrag beinhalten. Beachten Sie, dass die Datenmenge entsprechend der Vielzahl an Einträgen groß ist. Das Standardpaket umfasst bereits 29 GB. Leider sind diese Daten gebührenpflichtig.

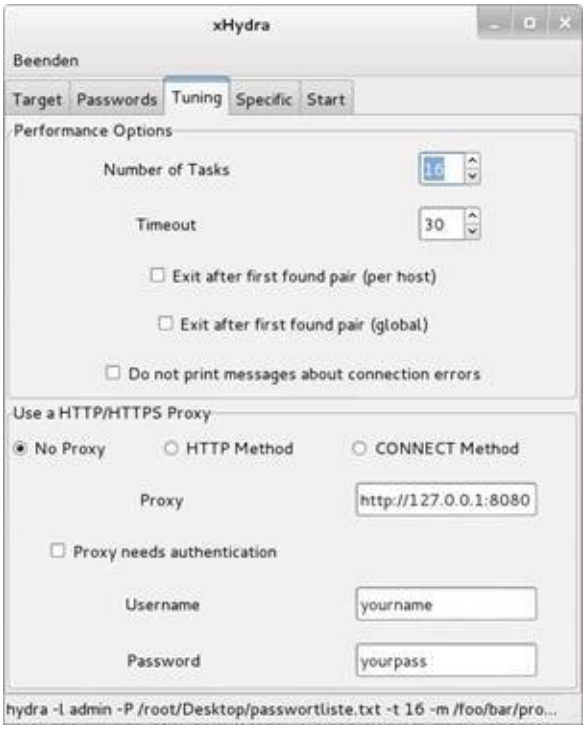
Alternativ finden Sie unter der nachfolgend aufgeführten Adresse kostenlose Tabellen für unterschiedliche Anwendungszwecke:

https://www.freerainbowtables.com/de/tables2/

Auch hier müssen Sie mit beachtlichen Datenmengen hantieren. Zum besseren Verständnis: Kommt ein Passwort zum Einsatz, das gerade einmal 7 Zeichen lang ist, so würde man für eine entsprechende Liste, die alle Möglichkeiten aufführt ca. 417 TB Speicherplatz benötigen. Bei Rainbow Tables sind es ca. 80 GB. Der Datenbestand der Website *Free Rainbox Tables* umfasst nicht minder beeindruckende 9.741 GB.

Auf der Registerkarte *Passwords* können Sie außerdem die Optionen *Try login as password* und *Try empty password* aktivieren, damit auch der Benutzername und eine leere Eingabe als Passwort verwendet werden.

xHydra hat weitere Anpassungs- und Konfigurationsmöglichkeiten zu bieten. Auf der Registerkarte *Tuning* können Sie beispielswiese die Anzahl an Tasks bestimmen. Die ist standardmäßig auf den Wert 16 gesetzt. Auch die Verwendung eines Proxy Servers ist vorgesehen.




**Das Tuning von xHydra.**

Auf der Register *Specific* können Sie verschiedene dienstspezifische Anpassungen vornehmen. Sie können dort beispielsweise ein bestimmtes Verzeichnis eines Web-Dienstes ansteuern, SMB-spezifische Einstellungen vornehmen und die SNMP-Version bestimmen.

Wichtig bei einem Angriff auf einen WLAN-Router: Sie müssen auf der Registerkarte *Specific* in dem Eingabefeld *http/https url* den Pfad zum Login-Formular angeben. Sofern er sich nicht aus dem Zugriff oder dem Handbuch des Routers ergibt, können Sie den Pfad beispielsweise mit einem Web Application Security Scanner wie der Burp Suite ermitteln.

Um die Wörterbuch-Attacke zu starten, wechseln Sie zur Registerkarte *Start* und klicken dort auf die Schaltfäche *Start*. Im Anzeigebereich können Sie die Aktionen verfolgen, die xHydra am Zielsystem durchführt. Gelingt die Wörterbuchattacke, so können Sie das der

Ausgabe entnehmen. Die lautet dann beispielsweise wie folgt:

[80][www] host:192.168.2.1 login: admin password: geheim

[Status]  Attack finished

… weitere Statusinformationen …

<finished>

Alle Versuche, sich Zugriff zu dem Router zu verschaffen, beginnen mit *[ATTEMPT]*. Das Schöne an xHydra ist der Umstand, dass die GUI die zugehörigen Hydra-Befehle in der Statuszeile anzeigt. Was mit (x)Hydra klappt, funktioniert übrigens auch wunderbar mit Cain & Abel. Mehr zu Cain & Abel und dessen unzähligen Möglichkeiten erfahren Sie in *Cain & Abel kompakt* (ISBN 978-3-95444-226-3).

## 3.2 Der böse Zwilling

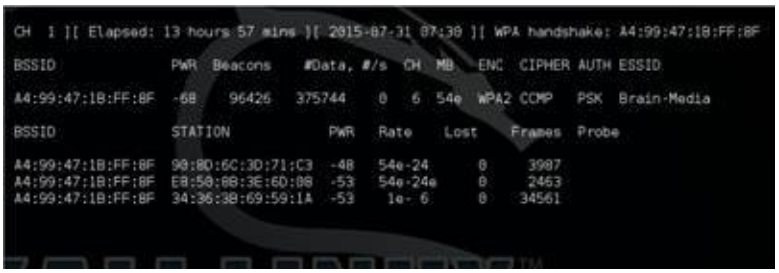
Besonders einfach für Angreifer ist es, Daten aufzuzeichnen, wenn die über ein öffentlich zugängliches WLAN laufen oder wenn der Schlüssel bekannt ist. Ein potentieller Angreifer kann einfach den Netzwerknamen eines bestehenden Netzwerks nachahmen und somit einen Hotspot mit dem gleichen Namen einrichten. Man spricht in diesem Zusammenhang auch von einem Evil Twin Access Point.

Befindet sich das potenzielle Opfer nun näher an dem gefakten Access Point, so verbindet er sich automatisch mit diesem. Das Opfer erkennt keinen Unterschied zwischen beiden, da die Daten in der Regel direkt weitergereicht werden. Für den Angreifer, der sich bereits zwischen das Ziel und das Netzwerk gesetzt hat, kann nun eine Man-in-the-middle-Attacke durchführen und dabei beispielsweise Passwörter, E-Mails und den sonstigen Datentransfer mitlesen.

Der Einsatz eines Evil Twin Access Points ist immer dann möglich, wenn Sie mit dem Penetration Testing-System eine Verbindung zu dem WLAN herstellen können. Ob das drahtlose Netzwerk nicht oder per WEP bzw. WPA/WPA2 geschützt ist, spielt dabei keine Rolle.

Für das Aufsetzen eines Evil Twin Access Points benötigen Sie eine Kali Linux-Installation mit zwei WLAN-Adaptern, von denen ein Adapter eine Internet-Verbindung aufbauen kann. Auch ein WLAN-Adapter und ein LAN-Anschluss genügen. Wie setzt man nun einen Evil Twin Access Point in der Praxis auf? Das ist einfach, denn die meisten Tools und Kommandos haben Sie in diesem Einstieg bereits kennengelernt. Und so gehen Hacker vor, um einen Evil Twin Access Point einzurichten:

- Zunächst verwenden Sie Airodump-ng, um die BSSID und ESSID des Access Points herauszufinden, den Sie emulieren wollen. Begrenzen Sie die Ansicht am besten auf diesen einen Access Point.
- Dann stellen Sie eine Client-Verbindung her, um zu testen, dass es sich bei diesem Ausgangszugangspunkt um den gewünschten Access Point handelt. Anhand der Ausgabe können Sie das Zustandekommen verfolgen.

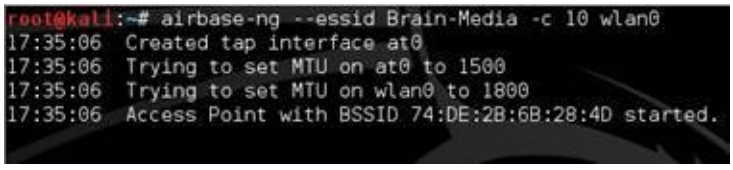



**Die Ansicht wurde auf einen Access Point und dessen Verbindungen begrenzt.**

- Mit den gewonnen Informationen erzeugen wir nun einen neuen Access Point mit der gleichen ESSID, aber mit einer anderen BSSID und einer anderen MAC-Adresse. Dazu verwenden wir den Befehl *airbase-ng*. In der Ausgabe können Fehlermeldungen auftreten. Die können Sie in der Regel einfach ignorieren. Um einen weiteren Access Point mit der Bezeichnung *Brain-Media* anzulegen, verwenden Sie folgenden Befehl:

  airbase-ng —essid Brain-Media -c wlan0

  Der Konsolenausgabe können Sie entnehmen, dass ein neuer Access Point eingerichtet wurde.




**Ein Evil Twin wurde angelegt.**

- Prüfen Sie nun mit *airodump-ng*, ob auch tatsächlich ein zweiter Access Point angelegt wurde.


**Es existieren zwei Access Points mit der identischen ESSID.**

- Als Nächstes senden wir einen Deauthentifizierung-Frame an den Client, damit die Verbindung mit dem Ausgangs-Access Point unterbrochen wird und eine neue Verbindung aufgebaut werden muss:

  aireplay-ng -0 5 -a <mac> —ignore-negative wlan0

1.

- Kann der gefakte Access Point näher dem zu attackierenden System positioniert

werden, stellt der WLAN-Client eine Verbindung zu dem Evil Twin Access Point her.

- Wir können außerdem die BSSID und die Mac-Adresse des Access Points vortäuschen:

  airbase-ng –a <router mac> —essid Brain-Media –c 11 wlan0

- Wenn Sie nun mit Airodump-ng einen Blick auf die aktuelle WLAN-Umgebung werfen, ist kaum zu erkennen, dass es sich um zwei unterschiedliche Access Points handelt.

1.

## 3.3 Rogue Access Point

In diesem Zusammenhang muss auch der sogenannte Rogue Access Point erwähnt werden. Dieser Begriff bezeichnet die WLAN-Geräte, die unerlaubt versuchen, als Access Point, Teilnehmer in einem WLAN zu werden.

Rogue AP werden beispielsweise von Mitarbeitern einer Firma ohne Kenntnis und/oder Erlaubnis der Systemadministratoren an das Netzwerk angeschlossen – oder eben von Hackern. Sie stellen ungesicherte WLAN-Zugänge zur Verfügung und öffnen potentiellen Angreifern Tür und Tor, da der Angreifer sozusagen durch die Hintertüre die Sicherheitsmaßnahmen umgehen kann. Selbst Firewalls und Intrusion Prevention System können hier wenig ausrichten.

Meist sind die Rogue Access Points ungesichert und verwenden keinerlei Verschlüsselung. Umso einfacher ist es, einen solchen Zugangspunkt anzulegen. Wenn Sie physikalischen Zugang zu einem solchen Netzwerk haben, so ist es recht einfach, denn Sie stöpseln einfach einen Access Point in die bestehende Netzwerkinfrastruktur. Alternativ setzen Sie einen softwarebasierten Access Point auf und erzeugen eine Bridge zum Ethernet-Netzwerk. Das ist praktisch mit jedem Notebook möglich, das Zugang zu einem Netzwerk besitzt. Und so gehen wir dazu vor:

- Zunächst verwandeln wir unser Notebook in einen Access Point mit der Bezeichnung *Rogue*:

  airbase-ng —essid Rogue -c 10 wlan0

- Mit Airodump-ng können Sie schnell prüfen, ob der neue Access Point verfügbar ist:

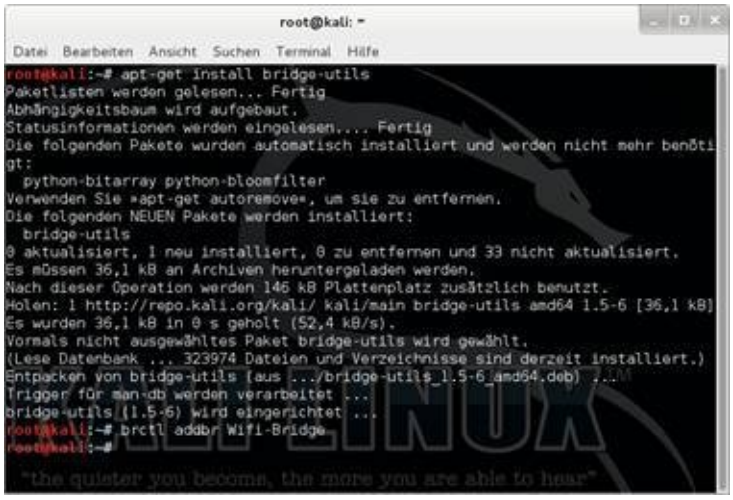
  airodump-ng wlan0

- Vorausgesetzt, Ihr Notebook besitzt auch einen Ethernet-Anschluss, mit dem der Anschluss an dem Firmennetzwerk hergestellt wird, kann der WLAN-Adapter für das Aufsezten des Rogue-Knoten verwendet werden. Damit der Access Point auch auf das lokale Netzwerk zugreifen kann, müssen Sie sozusagen die Brücke zwischen beiden schlagen. Wir bezeichnen Sie als Wifi-Bridge. Dazu installieren Sie zunächst die Bridge Utilities und richten die Bridge ein:

apt-get install bridge-utils

brctl addbr Wifi-Bridge

Die zugehörige Ausgabe zeigt nachstehende Abbildung.




**Das Anlegen der Bridge.**

- Dann fügen wir den Ethernet- und das virtuelle Interface, das von Airbase-ng angelegt wurde, der Bridge-Konfiguration hinzu:

  brctl addif Wifi-Bridge eth0

  brctl addif Wifi-Bridge ath0

- Der nächste Schritt dient dem Aktivieren der Schnittstellen:

  ifconfig eth0 0.0.0.0 up

  ifconfig ath0 0.0.0.0 up

- Als Nächstes aktivieren wir das IP-Forwarding im Kernel, damit die Pakete auch zwischen den beiden Schnittstellen weitergereicht werden:

  echo 1 > /proc/sys/net/ipv4/ip_forward

- Fertig! Mit dieser Konfiguration hat nun jeder Client, der über den Rogue Access Point auf das Netzwerk zugreift, vollen Zugriff auf das Netzwerk.

## 3.4 WLAN-Client attackieren

Die meisten Penetration-Tester haben bei der Analyse eines WLANs die wichtigste Infrastrukturkomponente im Blick. Es ist durchaus nachvollziehbar, dass der Fokus auf dem Access Points liegt, aber auch die WLAN-Clients sind potenzielle An-griffspunkte. Auch hier sind verschiedene Angriffsszenarien denkbar, angefangen von Honeypots über Caffe Latte- bis hin zu Hirte-Attacken.

Wenn WLAN-Clients eingeschaltet werden, suchen Sie normalerweise nach Netzwerken, mit denen sie sich zuvor bereits erfolgreich verbunden haben. Diese Netzwerke werden in einer Liste der bevorzugten Netzwerke verwaltet. Außerdem zeigt ein WLAN-Client üblicherweise alle weiteren gefundenen Access Points in seiner Nähe an. Hier gibt es kaum Unterschiede zwischen den unterschiedlichen Client-Typen.

Für potentielle Angreifer gibt es nun verschiedene Angriffspunkte. Er kann beispielsweise in aller Ruhe den Traffic analysieren und einen eigenen Access Point mit der gleichen ESSID einrichten. Unter Umständen gelingt es so, die Client-Verbindung auf das eigene System umzulenken. In öffentlichen Netzwerken kann er sehr einfach einen solchen Evil Twin Access Point einrichten und verwenden. Außerdem kann der Angreifer das Verhalten des potenziellen Opfers studieren und so gegebenenfalls weitere Angriffspunkte ausmachen.

Schauen wir uns an, wie man einen WLAN-Client derart in die Irre führt. Zunächst führen Sie *airodump-ng wlan0* aus und prüfen die Ausgabe. Der Ausgabe können Sie schnell entnehmen, dass der Client nicht mit einem Access Point verbunden ist (*Not associated*) und die verfügbaren SSIDs prüft.

Starten Sie als Nächstes Wireshark und zeichnen Sie den WLAN-Traffic über die drahtlose Schnittstelle auf. Mit Hilfe der Filterfunktion beschränken Sie die Ansicht auf alle Probe Response-Pakete.

Dann erzeugen Sie einen Fake Access Point für das Netzwerk *Brain-Media*:

```
airbase-ng –c 3 –e  “Brain-Media” wlan0
```

Der Airbase-ng-Ausgabe können Sie innerhalb von Sekunden entnehmen, dass sich ein Client erfolgreich verbunden hat.

Dann greifen wir zu einem weiteren Router und erzeugen dort ebenfalls einen Access Point mit der identischen Bezeichnung. Auf diesem Router verwenden wir einen anderen Kanal, beispielsweise Kanal 3. Stellen Sie dann die Verbindung zu diesem Access Point her. Mit Airodump-ng können Sie das einfach verifizieren.

Starten Sie dann den Fake Access Point mit Hilfe von Airbase-ng. Der WLAN-Client sollte immer noch mit dem „richtigen“ Access Point verbunden sein. Die Verbindung unterbrechen Sie durch das Senden einer Deauthentifizierungsnachricht mit Aireplay-ng (Option *—deauth*). Der Client versucht automatisch die Verbindung wieder aufzunehmen. Mit Hilfe von Airodump-ng können Sie einfach verfolgen, dass er sich mit dem Fake Access Point verbindet.

Ihnen stehen weitere Angriffsvarianten zur Verfügung. Mit Airbase-ng können Sie bei Verwendung von WEP auch Caffe-Latte- und Hirte-Attacken nutzen (siehe Kapitel 4.5). In Kapitel 1 haben Sie bereits einen anderen Weg zum Knacken von WEP-Verbindungen kennengelernt.

Oben haben Sie die Möglichkeit kennengelernt, wie Sie einen WPA/WPA2 PSK-Schutz mit Aircrack-ng aushebeln können. Die Grundidee dahinter: Man zeichnet den Vier-Wege-WPA-Handshake auf und führt dann eine Wörterbuchattacke aus. Die spannende Frage ist nun, ob man einen WPA-Schutz auch ohne einen Access Point knacken kann. Sie ahnen es

schon: Ja, auch das ist möglich – und zwar einfacher, als Sie vermuten. Und so gehen Sie vor:

- Zunächst richten wir einen WPA-PSK-Zugang mit der ESSID *Brain-Media* ein. Die Option *-z 2* erzeugt den Access Point, der TKIP verwendet:

  ```
  airbase-ng –c 3 –e  “Brain-Media” –W 1 -z 2 wlan0
  ```

- Dann starten wir Airodump-ng, um die Daten aufzuzeichnen:

  ```
  airodump-ng -c 3 —bssid <MAC-Adresse> —write AP-los-Aufzeichnung wlan0
  ```

- Wenn der WLAN-Client nun eine Verbindung zu dem Access Point her-stellt, beginnt der Handshake-Vorgang, bricht aber bei Schritt 2 ab. Doch das ist nicht weiter tragisch, denn die für den Hacker relevanten Daten sind aufgezeichnet.
- Nun müssen Sie nur noch die Aufzeichnuntg mit Hilfe von Aircrack-ng knacken.

## 3.5 Man-in-the-middle-Attacke

Die sogenannten Man-in-the-middle-Attacken, kurz MITM-Attacken, bieten gerade bei Angriffen auf WLANs das höchste Potenzial. Dabei sind die verschieden-sten Einsatzszenarien denkbar.

Ein simples Szenario: Ein potenzieller Angreifer verfügt über eine LAN-Anbindung an das Internet und erzeugt einen Fake Acess Point mit seinem WLAN-Adapter. Dieser Access Point besitzt die gleiche SSID, wie der Hotspot des Opfers.

Das Opfer kann sich nun versehentlich mit dem Fake Access Point verbinden oder durch eine Deauthentifizierungsattacke, verbunden mit einer höheren Sendeleistung des Access Points, zur Verbindungsaufnahme gezwungen werden. Das Fatale dabei: Der Angreifer kann nun den Traffic des Benutzers über die eigene Bridge forwarden. Das Opfer hat kaum eine Möglichkeit, diese Attacke als solche zu erkennen.

Und so simulieren Sie eine solche Attacke:

- Zunächst richten Sie einen Access Point für die Attacke ein. Den Bezeichnen wir hier exemplarisch als *mitm*. Zur Einrichtung greifen Sie zu Airbase-ng:

  ```
  airbase-ng —essid mitm –c 11 wlan0
  ```

  Der Ausgabe können Sie entnehmen, dass eine neuer Access Point erzeugt wurde. Die Schnittstelle kann wie eine drahtgebundene angesprochen werden. Auch der Abruf über weitere Details mit *ifconfig* ist möglich. Probieren Sie es einfach aus: *ifconfig wlan0*.
- Als Nächstes erzeugen wir eine Bridge von dem Notebook, das über die Ethernet-Schnittstelle *eth0* und den WLAN-Adapter *wlan0* verfügt:

  ```
  brctl addbr mitm-bridge
  brctl addif mitm-bridge eth0
  ```

```
brctl addif mitm-bridge wlan0
ifconfig eth0 0.0.0.0 up
ifconfig at0 0.0.0.0 up
```

- Dann weisen wir der Bridge eine IP-Adresse zu und prüfen die Konnektivität mit dem Gateway. Wir verwenden dabei nicht DHCP, sondern führen folgenden Befehl aus:

```
ifconfig mitm-bridge 192.168.1.100 up
```

  Mit Hilfe von Ping können Sie die Verbindung prüfen.

- Mit dem nächsten Schritt aktivieren wir das IP-Forwarding i m Kernel, damit das Routing und das Paket-Forwarding zuverlässig funktionieren:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Dann stellen wir mit einem WLAN-Client eine Verbindung zum Access Point *mitm* her. Der Client erhält automatisch eine IP-Adresse von dem DHCP-Server zugewiesen, der auf Seiten des kabelgebundenen Netzwerks ausgeführt wird. In diesem Beispiel erhält er die IP-Adresse *192.168.1.200*. Auch das können Sie wieder einfach mit *ipconfig* und Ping verifizieren.
- Verifizieren Sie zusätzlich mit Airbase-ng, dass der Client eine Verbindung hergestellt hat:

```
airbase-ng —essid mitm –c 11 wlan0
```

- Das Interessante an dieser Konfiguration ist der Umstand, dass Sie die volle Kontrolle über den Traffic haben, der über die WLAN-LAN-Bridge läuft. Das können Sie leicht mit Wireshark verifizieren, indem Sie die Aufzeichnung auf die verwendete Schnittstelle *wlan0* beschränken.

In Ihren Aufzeichnungen können Sie nun nach den gewünschten Informationen suchen.

## 3.6 Angriffspunkte WLAN und RADIUS

Lange Zeit galten die Verwendung von WPA und RADIUS in Unternehnen als ultimativer Schutz vor möglichen Angreifern. Heute weis man es besser: Auch diese Schutzfunktionen können ausgehebelt werden. In Sachen RADIUS ist die freie Implementierung FreeRADIUS der Quasi-Standard. Daher zeige ich Ihnen anhand dieser Implemtierung, wie potenzielle Angreifer einen solchen Schutz umgehen können.

Die Inbetriebnahme einer FreeRADIUS-Installation ist nicht gerade trivial. Sie sollten

dennoch auch hier zunächst eine Testumgebung aufsetzen, anhand der Sie die folgenden Schritte nachvollziehen können.

Joshua Wright hat ein Patch für FreeRADIUS geschrieben, dass die Durchführung von Attacken gegen einen RADIUS-Server deutlich vereinfacht: FreeRADIUS-WPE (Wireless Pwnage Edition). Da das Patch nicht in Kali integriert ist, müssen Sie es zunächst von der Website des Entwicklers herunterladen. Die URL lautet wie folgt:

https://github.com/brad-anton/freeradius-wpe/

Nach dem Download installieren Sie das Skript:

dpkg –i freeradius-server-wpe_2.1.12-1_i386.deb

Als Nächstes richten wir einen Access Point mit FreeRADIUS-WPE ein. Dazu verbinden Sie einen LAN-Port des Notebooks mit dem RADIUS-System. In diesem Beispiel verwenden wir *eth0*. Führen Sie als Nächstes einen Reload der DHCP-Konfiguration durch:

# dhcpclient eth0

Prüfen Sie außerdem mit Ping die Verfügbarkeit des Access Points.

Als Nächstes konfigurieren Sie den Access Point für das Zusammenspiel mit dem RADIUS-Server. Öffnen Sie dazu die Einstellungen *WPA/WPA2-Enterprise*, aktivieren Sie WPA2 und verwenden Sie als Verschlüsselungsmethode AES.

Im Abschnitt *EAP (802.1x)* bzw. einer entsprechenden Bezeichnung tragen Sie unter *Radius Server* die IP-Adresse des Kali Linux-Systems ein. Der Standard-RADIUS-Port lautet 1812. Geben Sie als Passwort *test* an.

Dann installieren Sie das Skript:

sudo dpkg —install freeradius-server-wpe_2.1.12-1_i386.deb

sudo ldconfig

Sie müssen außerdem folgenden Befehl ausführen:

cd /usr/local/etc/raddb/certs/

./bootstrap

Überprüfen Sie dann die RADIUS-Version:

radiusd -v

Dann öffnen Sie die Konfigurationsdatei *eap.conf*. Dort finden Sie den Eintrag *default_eap_type*. Den konfigurieren Sie wie folgt:

```
default_eap_type = peap
```

Als Nächstes editieren Sie *clients.conf*. In dieser Datei sind die Clients hinterlegt, die eine Verbindung zum RADIUS-Server aufbauen dürfen. Die sieht wie folgt aus:

```
# clients.conf
    client 192.168.0.0/16 {
    # Geheimnis zwischen dem Authentifierer (Access Point)
    # und dem Authentifizierungsserver (RADIUS).
    secret          = test
    shortname       = test
    }
```

Starten Sie dann den RADIUS-Server: *radiusd -s -X*. Der Server gibt anschließend einige Statusmeldungen an. Insbesondere an den Listening-Meldungen können Sie erkennen, dass der Server vollfunktionstüchtig und aktiv ist.

Wie wir oben gesehen haben, ist auch WPA2 gegen Wörterbuchattacken anfällig. Solche Probleme kann man bei einer WLAN-Anmeldung mit individuellen Zugangsdaten (Username/Passwort-Kombination) oder per Zertifikat elegant umschiffen – eine Technik, die WPA2 praktischerweise unterstützt. Die Funktion nennt sich dann, wie bereits erwähnt, meist WPA2-Enterprise, WPA2-1x oder WPA2-802.1x. Sie erledigt sichere Authentifizierung beispielsweise gegen einen RADIUS-Server.

Dabei kommt ein weiteres Protokoll zum Einsatz, dass ebenfalls angreifbar ist:
PEAP (Protected Extensible Authentication Protocol). PEAP ist Teil von EAP (Extensible Authentication-Protokoll).

PEAP nutzt seinerseits TLS (Transport Layer Security) zur Erstellung eines verschlüsselten Kanals zwischen einem sich authentifizierenden PEAP-Client, z. B. ein WLAN-Client, und einem PEAP-Authentifikator, z. B. einem RADIUS-Server. PEAP ist in zwei Version verfügbar: v1 und v2. Beide sind insbesondere unter Windows verfügbar. Das macht speziell Windows-Clients für eine PEAP-Attacke anfällig.

PEAP bietet mehrere Angriffsflächen, eine beispielsweise dann, wenn die Zertifikatvalidierung auf Seiten des Clients ausgeschaltet ist. Ist der RADIUS-Server gestartet und FreeRADIUS-WPE installiert, so überwachen Sie die Protokolldatei, die durch das Skript erzeugt wird:

```
/usr/local/var/log/radius/# tail -f freeradius-server-wpe.log
```

In den Eigenschaften der WLAN-Verbindung des Windows-Clients müssen Sie den PEAP-Dienst deaktivieren. Konfigurieren Sie den Client außerdem so, dass er den Benutzernamen und das Passwort nicht automatisch zur Anmeldung verwendet. Dort aktivieren Sie die Benutzerauthentifizierung.

Sowie der Client versucht, eine Verbindung zum Access Point herzustellen, wird er zur

Eingabe des Benutzernamens und des Passwortes aufgefordert. Sowie das geschieht, erscheint eine MSCHAP-v2 Challenge Response in der Protokolldatei.

Nun müssen Sie nur noch das Tool *asleaf* bemühen, um das Passwort zu knacken. Auch dieses Tool ist in Kali Linux integriert.

## 4.7 WPS-Attacke

Eine letzte Möglichkeit, einen WLAN-Client zu attackieren, möchte ich Ihnen noch vorstellen: die WPS-Attacke. WPS (Wireless Protected Setup) wurde 2006 eingeführt und soll Nutzern das unproblematische Verbinden von WLAN-Clients an einen WLAN Access Point erlauben. Alle mir bekannten Router und Smartphone unterstützen diese Technik.

Die Idee dahinter: Auf Seiten des Zugangsgerätes ist Hardware-seitig ein Wert hinterlegt, der für die Authentifizierung mit einem Client verwendet wird. Betätigt man den WPS-Button und aktiviert man auf Seiten des Clients ebenfalls die WPS-Funktion, so tauschen sich die beiden aus. Ein Zugang kann nur dann eingerichtet werden, wenn der Button auf Seiten des Access Points betätigt wird. Der Vorteil gegenüber WPA-gesicherten Verbindungen: Nur wer Zugang zum Access Point besitzt und den WPS-Button betätigen kann, kann sich auch Zugriff auf das WLAN verschaffen.

Ende 2011 wurde bekannt, dass der WPS-Mechanismus auch für Brute Force-Attacken anfällig ist. Konkret ist der Traffic für den WPS-Datenaustausch fälschbar und die WPS-PIN ist nur acht Zeichen lang, wobei Zahlen zwischen 0 und 9 verwendet werden. Der WPS-Mechanismus weist zwei weitere Schwachstellen auf, die dafür sorgen, dass am Ende nur ca. 11.000 mögliche Werte zulässig sind. Dieser Wert ist ein Klacks für Cracker.

Und so simulieren Sie eine WPS-Attacke:

- Zunächst öffnen Sie die Access Point-Einstellungen und stellen sicher, dass die WPS-Unterstützung aktiviert ist.
- Dann starten Sie Airmon-ng:

  ```
  airmon-ng start wlan0
  ```

- Dann richten wir ein Monitoring-Interface *mon0* ein und bezeichnen es als *wpsa*:

  ```
  wpsa —ignore-fcs -i mon0
  ```

  Die Option *—ignore fcs* sorgt für das erwartete Format. Die Ausgabe führt alle Geräte mit WPS-Unterstützung auf. Der Ausgabe können Sie auch die WPS-Version und den Status entnehmen. Lautet der Status *unlocked*, steht einer Attacke nichts im Weg.
- Als Nächstes kommt ein Spezialist zum Einsatz: reaver. Führen Sie mit diesem Tool folgenden Befehl aus:

  ```
  reaver -i wlan0 -b <mac> -vv
  ```

Glückwunsch! Auch dieser Schutzmechanismus ist erfolgreich ausgehebelt.

# 4 Die Tools der Aircrack-ng-Suite

Die Aircrack-Suite ist das Herzstück für das Penetration Testing von drahtlosen Infrastrukturen. In der Suite sind ein Dutzend Tools zu einem Paket geschnürrt, das seines Gleichen sucht. Im bisherigen Verlauf dieses Buches haben Sie bereits mehrfach mit Arodump-ng & Co. Bekanntschaft gemacht. In diesem Kapitel werfen wir einen genaueren Blick auf die verschiedenen Tools. In der Aircrack-ng-Suite sind die folgenden Tools gebündelt:

- **Airmon-ng**: Versetzt den WLAN-Adapter in den Monitormodus.
- **Airodump-ng**: Sammelt Informationen zu den Access Points und zeigt die empfangenen WLANs und Handshakes an.
- **Aireplay-ng**: Dient verschiedenen Angriffstypen, beispielsweise der Deauthentifzierung und der ARP-Injektion.
- **Aircrack-ng**: Dient dem Knacken einer WPA-gesicherten Verbindung.
- **Airbase-ng**: Kann Access Points faken sowie Caffe Latte- und Hirte-Angriffe durchführen.
- **Airdriver-ng**: Dient der Installation von drahtlosen Treibern, Patches etc.
- **Airolib-ng**: Dieses Tool speichert und verwaltet ESSID und Passwort-Listen.
- **Airserv-ng**: Mit diesem Tool können Sie WLAN-Adapter über das TCP-/IP Netzwerk verwenden.
- **Airtun-ng**: Stellt ein virtuelles Tunnel-Interface bereit.
- **Buddy-ng**: Loopback-Server für Easside-ng.
- **Packetforge**: Erzeugt verschlüsselte Pakete für Injektionen.
- **Airdecap-ng**: Kann WEP/WPA/WPA2-Dateien entschlüsseln.

## 4.1 Airmon-ng

Aus Kapitel 1 kennen Sie das Tool Airmon-ng. Wie man anhand seiner Bezeichnung bereits erkennen kann, kann man damit einen WLAN-Adapter vom sogenannten Managed- in den Monitormodus schalten. Im Monitormodus erhalten Sie weit mehr Informationen und können so gezielter beim Penetration Testing vorgehen. Die Verwendung ist einfach. Der typische Befehlsaufbau sieht wie folgt aus:

```
airmon-ng <start|stop> <schnittstelle> [kanal]
```

Mit den beiden Optionen *start* und *stop* starten bzw. halten Sie die Schnittstelle an. Mit *schnittstelle* bestimmen Sie, auf welchen Adapter der Befehl angewendet wird. Typische Beispiele sind *wlan0* und *ath1*. Optional können Sie auch den Kanal bestimmen.

Einge Beispiele erläutern die Verwendung des Befehls. Um den Monitoringmodus für die Schnittstelle *wlan0* zu aktivieren, verwenden Sie folgende Eingabe:

```
airmon-ng start wlan0
```

Um Kanal 10 zu starten, lautet das Kommandoo wie folgt:

```
airmon-ng start wlan0 10
```

Sie halten den Monitormodus mit folgendem Kommando an:

```
airmon-ng stop wlan0
```

Den Interface-Status fragen Sie wie folgt ab:

```
airmon-ng
```

Wie setzt man dieses Tool nun über die Aufgaben hinweg ein, die Sie im bisherigen Verlauf dieses Buchs kennengelernt haben? Um eine Schnittstelle in den Monitormodus zu schalten, rufen Sie nach dem Systemstart zunächst den Status Ihrer Umgebung ab:

```
iwconfig
```

Eine entsprechende Ausgabe kann wie folgt aussehen:

```
lo        no wireless extensions.
eth0      no wireless extensions.
wifi0     no wireless extensions.
ath0      IEEE 802.11b  ESSID:""  Nickname:""
      Mode:Managed  Channel:0  Access Point: Not-Associated
      Bit Rate:0 kb/s   Tx-Power:0 dBm   Sensitivity=0/3
      Retry:off   RTS thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality:0  Signal level:0  Noise level:0
      Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
      Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Um einen Adapter in den Monitormodus zu versetzen, müssen Sie zunächst die

Schnittstelle anhalten:

airmon-ng stop ath0

Eine entsprechende Ausgabe sieht wie folgt aus:

Interface Chipset Driver

wifi0 Atheros madwifi-ng

ath0 Atheros madwifi-ng

Das können Sie mit *iwconfig* leicht verifizieren

lo no wireless extensions.

eth0 no wireless extensions.

wifi0 no wireless extensions.

Ist die gewünschte Schnittstelle angehalten, können Sie sie in den Monitormodus versetzen:

airmon-ng start wifi0

Die zugehörige Ausgabe des Systems sieht dann wie folgt aus:

Interface Chipset Driver

wifi0 Atheros madwifi-ng

ath0 Atheros madwifi-ng VAP

Mit *iwconfig* können Sie nun einfach prüfen, ob der Monitormodus aktiviert ist. Die entsprechende Ausgabe finden Sie unter *Mode*:

ath0 IEEE 802.11g ESSID:””

Mode:Monitor Frequency:2.452 GHz Access Point:

Damit ist der Monitormodus aktiviert. Sie können auch einen spezifischen Kanal starten:

airmon-ng start wifi0 9

Der Kanal lässt sich auch einfach bestimmen:

iwlist <interface > kanal

Neben der aktuellen Frequenz und dem Kanal werden auch noch die anderen Kanäle mit Kanalnummer und zugehöriger Frequenz ausgegeben. Zum Beenden des Monitormodus verwenden Sie die Option *stop*.

## 4.2 Airodump-ng

Mit Airdump-ng steht Ihnen ein leistungsfähiger Sniffer für die Aufzeichnung des drahtlosen Daten-Traffics zur Verfügung. In Verbindung mit einem GPS-Empfänger können Sie sogar zusätzlich die Koordinaten des Access Points speichern.

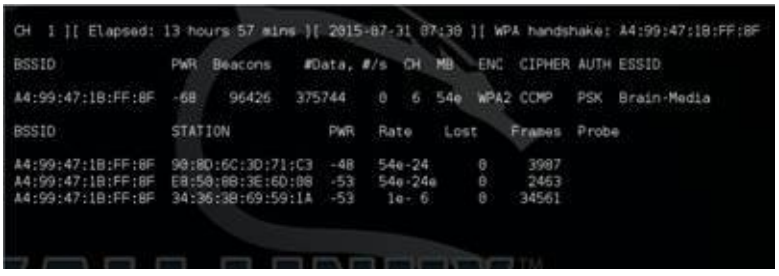
Die Aufzeichnung kann auf einzelne Kanäle begrenzt werden. Wenn Sie keinen Kanal angeben, wird auf allen Kanälen aufgezeichnet. Das Programm stoppen Sie mit der Tastenkombination *Strg + C.* Sie sollten außerdem darauf achten, dass Airodump-ng und Kismet nicht gleichzeitig ausgeführt werden.

Airodump-ng stellt Ihnen wie die anderen Tools dieser Suite ebenfalls verschiedenste Optionen und Parameter für die Ausführung zur Verfügung. Die Ausführung erfolgt nach diesem Schema:

airodump-ng <optione> <interface>[,<interface>,…]

Sie können dabei folgende Optionen verwenden:

- **—ivs**: Zeichnet nur IVS auf.
- **—gpsd**: Verwendet den GPS-Daemon für die Lokalisierung der A Cs.
- **—write <präfix>**: Bestimmt das Präfix der Aufzeichnungsdatei.
- **-w** : Entspricht der Option —*write*, die die Daten in eine Capture-Datei schreibt.
- **—beacons**: Speichert alle Beacon Frames in der Aufzeichnungsdatei.
- **—update <secs>**: Bestimmt das Update-Intervall in Sekunden.
- **—showack**: Gibt verschiedene statistische Informationen wie *ack*, *cts* und *rts* aus.
- **-h**: Versteckt bekannte Stationen vor —*showack.*
- **-f <millisek.>**: Intervall in Millisekunden zwischen zwei Kanalwechseln.
- **-r <datei>**: Liest die Pakete von der Datei.




**Airodump-ng zeigt eine Liste der entdeckten Access Points und eine weitere Liste der verbundenen Clients (*STATION*).**

Der ersten Zeile können Sie den aktuellen Kanal, die Scan-Zeit und das Datum entnehmen. Geht außerdem ein Client online, wird rechts der Handshake samt MAC-Adresse angezeigt. In der Tabelle finden Sie folgende Abkürzungen, wobei sich manche von alleine erklären, andere wieder nicht:

- **BSSID**: Zeigt die Netzwerke an. Wird beim Client die Info *not associated* angezeigt, sucht er gerade nach dem Acsess Point.
- **PWR**: Dieser Wert gibt die Stärke des Signals an. Er steigt, je mehr Sie sich dem Access Point nähern. Der Wert -1 deutet darauf hin, dass der Access Point zu weit entfernt ist.
- **RXQ**: Bewertet die Empfangsqualität in Prozent auf Grundlage der in den letzten 10 Sekunden empfangen Pakete.
- **Beacons**: Gibt die Anzahl der Beacon Frames an, die der Access Point ausgesendet hat.
- **# Data**: In dieser Spalte wird die Anzahl der gesammelten Pakete angezeigt.
- **#/s**: Gibt die Anzahl der Datenpakate in den vergangenen 10 Sekunden an.
- **CH**: Diese Spalte führt den Kanal auf, auf dem der AP sendet. Aufgrund von Interferenzen kann es schon mal vorkommen, dass Airodump-ng auch einzelne Pakete eines Nachbarkanals mitzählt.
- **MB**: Gibt die maximale Übertragungsgeschwindigkeit an, die der AP unterstützt. MB = 11 à 802.11b, MB = 22 à 802.11b+ und darüber ist 802.11g.
- **ENC**: Dieser Spalte entnehmen Sie die Verschlüsselung. Dabei steht *OPN* für keine Verschlüsselung, *WEP?* für WEP (oder höher).
- **CIPHER**: Zeigt die verwendete Verschlüsselungsmethode an, also beispeilsweise CCMP, WRAP, TKIP, WEP, WEP40 oder WEP104. Üblicherweise werden WPA TKIP und WPA2 CCMP verwendet.
- **AUTH**: Diese Spalte zeigt das Authentifizierungprotkoll an. Typische Einträge sind *MGT* (WPA/WPA2 die einen separaten Authentication-Server verwenden), *SKA* (Shared Key für WEP), *PSK* (Pre-Shared Key für WPA/WPA2) und *OPN* (Open für WEP).
- **ESSID**: Zeigt die SSID an, die Sie beispielsweise beim SSID-Hiding nicht sehen. In diesem Fall holt sich Airodump-ng die ID aus den Probe Responses und Association Requests.
- **STATION**: Zeigt die MAC-Adresse des Acess Points oder des Clients an.
- **Lost**: Hier erfahren Sie, wie viele Datenpakete in den letzten 10 Sekunden verworfen wurden.
- **Packets**: Führt die Anzahl der Pakete auf, die der Client verschickt.

- **Probes**: Hier erfahren Sie die ESSID, mit der sich der Client zu verbinden versucht.

## 4.3 Aireplay-ng

Mit diesem Tool können Sie verschiedene Attacken gegen einen Access Point fahren. Die primäre Funktion des Tools ist das Generieren von Traffic, um damit einen WEP- oder WPA-Schlüssel zu knacken. Dabei können Sie verschiedene Angriffsszenarien durchführen, beispielsweise eine Deauthentifizierung, um den WPA-Handshake aufzuzeichnen, um die Authentifizierung zu fälschen oder um eine ARP-Injektion zu initiieren. Die Verwendung:

```
aireplay-ng <optionen> <interface>
```

Bis auf die Deauthenfizierung und das Fälschen der Authentifizierung sollten Sie Aireplay-ng mit der Option *-b* verwenden, um den Traffic auf den für Sie relevanten Datenverkehr zu beschränken.

Ihnen stehen folgende Optionen zur Verfügung:

- **-0 <anzahl>, —deauth=<anzahl>**: Führt eine Deauthentifizierung durch.
- **-1 <delay>, —fakeauth=<delay>**: Fälscht die Authentifizierung am Access Point.
- **-2, —interactive**: Dient der interaktiven Frame-Auswahl.
- **-3, —arpreplay**: Standard ARP-Request Replay.
- **-4, —chopchop**: Entschlüsselt WEP-Pakete.
- **-5, —fragment**: Generiert einen gültigen Keystream.
- **-6**: Führt einen Caffe Latte-Angriff aus.
- **-7**: Führt einen Fragmentatierungsangriff durch
- **-9, —test**: Testet die Injektion und die Qualität.

Aireplay-ng protokolliert alle ARP-Anfragen und schickt diese Pakete wieder an den Access Point zurück. Das Programm schickt immer wieder die gleichen ARP-Anfragen und der Acess Point antwortet darauf mit einem neuen ARP-Request mit neuen IVs.

Wenn Sie genügend Datenpakete gesammelt haben, können Sie damit den Schlüssel berechnen. Hier ein Beispiel für die Verwendung:

```
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
```

Dabei gibt die Option *-3* den Wert für das ARP Request Replay an. *Mit* -b MAC-Adresse geben Sie die MAC-Addresse des Access Points an. Mit der Option *-h* bestimmen Sie die

MAC-Adresse der Quelle. Außerdem geben Sie den Netzwerkadapter an.

Um einen Angriff mit Aireplay-ng auszuführen, benötigen Sie entweder die MAC-Adresse eines verbundenen Clients oder eine Fake-MAC aus dem Fake Authentication-Angriff.

Besonders einfach können Sie die MAC-Adresse eines verbundenen Clients mit Airodump-ng herausfinden. Der Angriff wird dann wie folgt gestartet:

```
aireplay-ng -3 -b 00:14:6c:7e:40:80 -h 00:0F:B5:88:AC:82 ath0
```

Die Antwort des Systems sollte in etwa wie folgt aussehen:

```
Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies.
Read 11978 packets (got 7193 ARP requests), sent 3902 packets…
…
…
Read 39 packets (got 0 ARP requests), sent 0 packets…
```

Es kann einige Minuten dauern, bis ein ARP-Request angezeigt wird. Sollte keine Ausgabe erfolgen, war die Attacke erfolglos. Wichtig ist dabei, dass Sie den Daten-Traffic mit Airodump-ng aufzeichnen. Wichtig ist in diesem Zusammenhang die Tatsache, dass ein Fake Authentification-Angriff keine ARP-Pakete generiert und nicht bei WPA/WPA2 Access Points verwendet werden kann.

## 4.4 Aircrack-ng

Das Tool Aircrack-ng erlaubt es Ihnen, in ein WEP-/WPA-/WPA2-PSK-geschütztes WLAN einzudringen. Das Tool analysiert die gesendeten Datenpakete, die mit Airodump-ng aufgezeichnet wurde, und die zu jedem WEP-Paket gehörenden 24-Bit langen Initialisierungsvektoren (IVs).

Wurden ausreichend viele Pakete aufgezeichnet oder schwache IVs verwendet, kann Aircrack-ng auf den WEP-Schlüssel schließen. Dabei handelt es sich im Wesentlichen um einen statistisch-mathematischen Angriff, d. h., theoretisch ist es möglich, mit genügend vielen IVs auf den WEP-Schlüssel rückzuschließen.

Laut Angaben der Entwickler benötigt man ca. 50.000 Paketen für eine 50pro-zentige Chance, einen 128-Bit-Schlüssel zu errechnen. Beachten Sie allerdings, dass ein erfolgreiches Knacken nicht garantiert ist und von verschiedenen Faktoren beeinflusst wird. Aircrack-ng implementiert inzwischen sogar moderne Angriffe wie den KoreK-Angriff. Der kann WEP-Schlüssel oftmals innerhalb weniger Minuten knacken.

Aircrack-ng kann auch für das Knacken von WPA-verschlüsselte Netzwerke mit Hilfe von Wörterbuchangriffen verwendet werden. Dabei wird der beim Verbindungsaufbau stattfindende Four-Way-Handshake einer WPA-Verbindung mitgelesen und versucht, anschließend mit Hilfe einer Brute Force-Attacken zu entschlüsseln.

Die Ausführung:

aircrack-ng [optionen] <capture-datei(en)>

Die können mehrere Capture-Dateien auswählen, solange diese im *CAP*- oder *IVS*-Format vorliegen. Sie können auch Airodump-ng und Aircrack-ng parallel ausführen. Aircrack-ng aktualisiert automatisch, wenn neue IVs verfügbar sind.

Um eine Verschlüsselung erfolgreich zu knacken, benötigt man in der Regel mindestens 200.000 gesammelten IVs. Um einen 64-Bit Schlüssel zu attackieren, verwenden Sie folgenden Befehl:

aircrack-ng -n 64 capture-datei.cap

Einen WEP-geschützten Datenverkehr kann man meist innerhalb von wenigen Minuten entschüsseln. Von einem echten Schutz kann man daher kaum sprechen.

## 4.5 Airbase-ng

Auch Airbase-ng kennen Sie bereits. Mit diesem Tool können Sie einen eigenen Access Point erstellen. Die Ausführung ist wieder einfach:

airbase-ng <optionen> <interface>

Die Optionen im Überblick:

- **-a BSSID Definition**: Wenn Sie die BSSID mit dieser Option bestimmen, verwendet Airbase-ng die MAC-Adresss des aktuellen Adapters (*ath0*, *ath1* etc.).
- **-i iface**: Geben Sie eine Schnittstelle an, werden die Pakete ebenfalls aufgefangen und verarbeitet.
- **-w WEP Schlüssel**: Mit dieser Option bestimmen Sie den WEP-Schlüssel. Der Client kann kann zwischen Open System- oder Shared-Key Authentication entscheiden. Beide Authentifizierungsmethoden werden von Airbase-ng unterstützt. Um den Keystream zu erlangen, sollten Sie allerdings die Verwendung der Shared Key-Authentication erzwingen. Dazu verwenden Sie zusätzlich die Option *-s*.
- **-h MAC**: Diese Option bestimmt die Ursprungs-MAC-Adresse für eine Man-in-the-middle-Attacke. Dabei muss auch die Option *-M* angegeben werden.
- **-f allow/disallow**: Diese Option ist unspezifisch. Sie kann aber beispielsweise mit dem Filter-Optionen *-d* und *-D* verwendet werden. Verwenden Sie die Option *-f disallow*, werden all jene Clients abgelehnt, die mit *-d* und *-D* definiert wurden.
- **-W WEP Flag**: Diese Option bestimmt das WEP Beacon Flag.
- **-M MITM Attack**: Diese Option ist noch nicht implementiert. Sie soll in Zukunft

der Durchführung von Man-in-the-middle-Attacken zwischen beliebigen Clients und BSSIDs dienen.

- **-A Ad-Hoc Mode**: Wenn Sie diese Option verwenden, agiert das System als Ad-hoc-Client anstatt als Access Point.
- **-Y External Processing:** Diese Option erzeugt ein zweites Interface *atX*, das beispielsweise für Injektionen verwendet werden kann.
- **-s**: Erzwingt Shared Key Authentication.
- **-L**: Führt eine Caffe Latte-Attacke aus. Alternativ können Sie auch die Option —*caffe-latte* angeben.
- **-N**: Führt eine Hirte-Attacke aus.

Sie können außerdem verschiedene Filteroptionen verwenden:

- **—bssid <MAC>**: Bestimmt die BSSID, die Sie verwenden wollen.
- **—bssids <Datei>**: Liest eine Liste von BSSIDs aus der Datei (kurz -*B*).
- **—client <MAC>**: Gibt die MAC-Adresse des Clients an, der akzeptiert wird (kurz -*d*).
- **—clients <Datei>**: Liest eine Liste mit Client-MAC-Adressen aus der angegebenenen Datei (kurz -*D*).
- **—essid <ESSID>**: Gibt eine einzelne ESSID an (kurz -*e*).
- **—essids <Datei>**: Liest eine Liste von ESSIDs aus der angegebenen Datei (kurz -*E*).

Sie können Airbase-ng beispielsweis für das Aufzeichnen eines WPA/WPA2-Handshake verwenden. Beginnen wir mit dem WPA-Handshake. Um diesen aufzuzeichnen, verwenden Sie folgenden Befehl:

```
airbase-ng -c 10 -e Brain-Media -z 2 -W 1 wlan0
```

Dabei bestimmen *-c 10* den Kanal und *-e Brain-Media* die SSID. Die Option *-z 2* bestimmt das TKIP. *-W 1* bestimmt das WEP Flag, da manche Clients ohne diese Angabe irritiert sind. Schließlich spezifizieren Sie noch die drahtlose Schnittstelle.

Die Antwort sieht dann beispielsweise wie folgt aus:

```
12:00:10  Created tap interface at0
12:00:15  Client 00:0F:B5:AB:CB:9D associated (WPA1;TKIP) to ESSID: “Brain-Media”
```

Die zweite Zeile wird nur dann ausgegeben, wenn sich der Client mit dem Access Point

verbinden kann.

Parallel zu Airbase-ng starten Sie eine Aufzeichnung:

```
airodump-ng -c 10 -d 00:C0:C6:94:F4:87 -w cfrag wlan1
```

Dabei bestimmt *-c 10* wieder den Kanal. Die Option *-d 00:C0:C6:94:F4:87* filtert die Daten des gefakten Accesss Points. Mit *-w* spezifizieren Sie die Datei, in die die Aufzeichnung geschrieben wird. Auch hier geben Sie wieder den WLAN-Adapter an.

Sowie der Client eine Verbindung herstellt, können Sie das in der rechten oberen Ecke durch den Hinweis *WPA handshake: 00:C0:C6:94:F4:87* erkennen. Unterhalb wird folgende Ausgabe eingeblendet:

```
[CH 10][Elapsed: 5 mins][2015-07-25 12:00][WPA handshake: 00:C0:C6:94:F4:87]
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:C0:C6:94:F4:87  100  70     1602       14    0   9  54  WPA  TKIP   PSK  Brain-Media
BSSID              STATION            PWR   Rate  Lost  Packets  Probes
00:C0:C6:94:F4:87  00:0F:B5:AB:CB:9D   86   2- 1     0       75
```

Nun führen Sie den Befehl *aircrack-ng cfrag-01.cap* aus, um zu prüfen, ob es sich um einen gültigen WPA-Handshake handelt.

```
Opening cfrag-01.cap
Read 114392 packets.
#  BSSID              ESSID              Encryption
1  00:C0:C6:94:F4:87  Brain-Media        WPA (1 handshake)
```

Das Aufzeichnen eines WPA2-Handshakes verläuft nach dem gleichen Schema. Einziger Unterschied: Anstelle der Option *-z 2* verwenden Sie *-Z 4*. Also konkret:

```
airbase-ng -c 9 -e Brain-Media -Z 4 -W 1 wlan0
```

## 4.6 Airdriver-ng

Mit Airdriver-ng stellt Ihnen die Aircrack-ng-Suite eine Tool für die Treiberinstallationen zur Verfügung. Mit diesem Tool identifizieren Sie die angeschlossenen WLAN-Adapter und können dann notwendige Treiber und/oder Patches für den Monitormodus oder Injektionen installieren. Die Ausführung erfolgt nach diesem Schema:

```
airdriver-ng <befehl> [treibernummer | treibername]
```

Hier die wichtigsten Airdriver-ng-Kommandos:

- **installed**: Listet die drahtlosen Stacks und Treiber auf, die aktuell in-stalliert sind.

- **loaded**: Listet die Wireless Stacks und Treiber auf, die aktuell ausgeführt werden.
- **load**: Lädt den angegebenen Treiber in den Speichern.
- **unload**: Entfernt den Treiber aus dem Speicher. Die Treibernummer erfahren Sie mit dem Befehl *load*.
- **reload**: Lädt den angegebenen Treiber erneut.
- **install**: Installiert den angegebenen Treiber und lädt diesen in den Speicher.
- **remove**: Entfernt den Treiber permanent.
- **details**: Gibt Detailinformationen zum installierten Treiber aus.
- **detect**: Ermittelt die installierten WLAN-Adapter.

## 4.7 Airolib-ng

Airolib-ng speichert und verwaltet ESSIDs und deren Passwörter. Außerdem berechnet das Tool die sogenannten PMKs (Pairwise Master Keys) und verwendet diese zum Knacken von WPA-/WPA2-Schlüsseln. Das Tool verwendet eine SQLite3-Datenbank zur Speicherung der Daten.

Airolib-ng muss zum Cracken eines WPA-/WPA2-Schlüssels auch einen PMK kalkulieren, von dem sich wiederum der PTK (Pairwise Transient Key) ableiten lässt. Allerdings beansprucht die Berechnung des PMK viel Zeit, da Airolib-ng den pbkdf2-Algorithmus benutzt.

Und so führen Sie Airolib-ng aus:

```
Airolib-ng <datenbank> <operation> [option]
```

Dabei bestimmt *database* den Datenbankname, wobei optional auch ein Pfad angegeben werden kann. Mit *operation* bestimmen Sie die auszuführende Aktion, die Sie mit den Optionen steuern können.

Mögliche Operationen sind die folgenden:

- **-stats**: Dieser Befehl zeigt Informationen über die Datenbank an.
- **-sql {sql}**: Führt das eingegebene SQL-Statement aus.
- **-clean [all]**:  Befreit die Datenbank von „altem“ Müll.
- **-batch**: Startet den Batch-Prozess für alle Kombinationen von ESSIDs und Passwörtern.
- **-verify [all]**: Prüft einen Satz mit zufällig gewählten PMKs.
- **-export cowpatty {essid} {file}**: Exportiert die Daten in eine CowPatty-Datei.

- **-import cowpatty {file}**: Importiert eine CowPatty-Datei und erstellt die Datenbank, falls nicht vorhanden.
- **-import {essid|passwd} {file}**: Importiert eine Textdatei mit ESSID und Passwörtern. Dabei müssen pro Zeile eine ID und ein Passwort angegeben werden.

## 4.8 Airserv-ng

Mit Airserv-ng steht Ihnen ein weiterer interessanter Spezialist, genauer ein Server, zur Verfügung, mit dem die mehrfache Nutzung einer WLAN-Karte über eine TCP-Netzwerkverbindung möglich ist. Auf dem Server sind bereits WLAN-Treiber vorinstalliert. Damit entfällt die komplexe WLAN-Administration.

Ist der Server gestartet, hört er auf die vordefinierte IP-Adressee und Port-Nummer auf eventuelle Client-Verbindungen. Die WLAN-Anwendung kommuniziert dann über diese IP-Adresse und Port. Für die Aircrack-ng-Programme ist der betreffende Dienst nicht mehr über den Interface-Namen (z. B. *ath0*), sondern unter der Server-Adresse erreichbar.

Standardmäßig lautet der Befehl für die Aufzeichnung mit Airodump-ng wie folgt:

```
airodump-ng -c 6 -w normal ath0
```

Beim Einsatz von Airserv-ng:

```
airodump-ng -c 6 -w airserv-ng 192.168.1.100:666
```

Dabei ist *192.168.1.100* die IP-Adresse des Rechners, auf dem Airserv-ng läuft, und *666* der Port, auf den der Airserv-ng-Server lauscht.

Der Einsatz des Airserv-ng-Servers bringt verschiedene Vorteile. Die WLAN-Administration vereinfacht sich und auch die Wartungsarbeiten reduzieren sich enorm. Ein weiterer Vorteil: Remote-Sensoren sind leicht zu implementieren, da lediglich eine WLAN-Karte und Airserv-ng für den Betrieb des Remote-Sensors notwendig sind.

Die allgemeine Ausführung sieht wie folgt aus:

```
airserv-ng <optionen>
```

Dabei stehen Ihnen folgende Optionen zur Verfügung:

- **-p <port>**: Bestimmt den TCP-Port, auf den der Server hört. Der Standard ist 666.
- **-d <dev>**: Bestimmt das Interface, also beispielsweise *ath0* oder *wlan0*.
- **-c <kanal>**: Bestimmt den Kanal.
- **-v <level>**: Legt den Debug-Level fest.

## 4.9 Airtun-ng

Mit dem Programm Airtun-ng können Sie virtuelle Tunnel-Schnittstellen erzeugen. Es bietet zwei Grundfunktionen: Es erlaubt das Anzeigen von verschlüsseltem Traffic für Wirelss Intrusion Detection Systeme (WIDS) und das Injizieren von beliebigem Traffic in ein Netzwerk.

Um WIDS-Daten zu sammeln, benötigen Sie den Schlüssel und die BSSID des Netzwerks. Airtun-ng entschlüsselt den kompletten Traffic des angegebenen Netzwerks und reicht ihn an ein IDS-System weiter. Eine Traffic-Injektion kann komplett bidirektional erfolgen, wenn Sie den vollständigen Schlüssel besitzen.

Eine weitere Besonderheit von Airtun-ng: Sie können das Program als Repeater einsezten. Mit der Repeater-Funktion können Sie den vollständigen Traffic an ein anderes Gerät weiterreichen.

Die Anwendung des Programms:

```
airtun-ng <optionen> <interface>
```

Die verfügbaren Opionen:

- **-a <BSSID>**: Bestimmt die MAC-Adresse des Access Points.
- **-w <WEP-Schlüssel>**: WEP-Schlüssel, um die Pakete zu entschlüsseln. Beachten Sie, dass entweder die Option *-y* oder *-w* angegeben werden muss.
- **-y <Datei>**: Liest PRGA aus der angegebenen Datei.
- **-x <nbpps>**: Bestimmt die maximale Anzahl an Paketen pro Sekunde.
- **-i <Interface>**: Empfängt Pakete von diesem Interface.
- **-t <0/1>**: Sendet Pakete zum Access Poibt (1) oder zum Client (0).
- **-r <Datei>**: Liest die Frames aus einer PCAP-Datei.

Um den Adapter in den Repeater-Modus zu versetzen, verwenden Sie folgende Optionen:

- **-f**: Aktiviert die Repeater-Funktion. Alternativ verwenden Sie *—repeat*.
- **-d <MAC>**: Bestimmt die BSSID, die benutzt werden soll (*—bssid*).
- **-m <Maske>**: Netzmaske, um nach BSSIDs zu filtern (*—netmask*).

Um die WIDS-Funktionen von Airtun-ng zur verwenden, starten Sie den WLAN-Adapter zunächst im Monitormodus und führen dann folgenden Befehl aus:

```
airtun-ng -a 00:14:6C:7E:40:80 -w 1234567890 wlan0
```

Dabei bestimmt *-a 00:14:6C:7E:40:80* die MAC-Adresse des Access Points, dessen Traffic Sie verwenden wollen. Die Option *-w 1234567890* gibt den WLAN-Schlüssel an und *wlan0* das Interface, das Sie in den Monitormodus versetzt haben.

Die Antwort von Airtun-ng sollte wie folgt aussehen:

created tap interface at0

WEP encryption specified. Sending and receiving frames through wlan0.

FromDS bit set in all frames.

Wie Sie voranstehender Abbildung entnehmen können, hat Airtun-ng das Interface *ath0* angelegt. Das fahren Sie nun hoch:

ifconfig ath0 up

Der Repeater-Modus kann die eingehenden Nachrichten von einem WLAN-Adapter an einen beliebigen in Reichweite befindlichen Adapter weiterreichen. Diese Technik wird in lokalen Netzwerken dazu verwendet, die Verfügbarkeit eines WLANs räumlich auszudehnen.

Hacker können diese Fähgikeit auch dazu nutzen, den Traffic abzugreifen und dann auf weitere Rechner umzulenken. Dabei können sogar verschiedene Kanäle verwendet werden.

Das Repeating verlangt, dass beide WLAN-Adapter sich im Monitormodus befinden. Das eigentliche Repeating wird durch die Option *—repeat* realisiert:

airtun-ng -a 00:14:6C:7E:40:80  —repeat —bssid 00:14:6C:7E:40:80 -i ath0 wlan0

Dabei bestimmen *ath0* und *wlan0* die Ein- bzw. Ausgabeschnittstellen.

## 4.10 Buddy-ng

Hinter Buddy-ng verbirgt sich ein kleiner Server, der die verschlüsselten Datenpakete zurück an das System gibt, auf dem Easside-ng aufgeführt wird. Dazu muss zunächst der Buddy-Server gestartet werden. Dieser muss eine Verbindung zum Internet besitzen. Er muss außerdem von dem System, auf dem Easside-ng läuft, per TCP und vom Access Point per UDP erreichbar sein. Der Port 6969 darf nicht durch eine Firewall blockiert werden.

Um den Buddy-Server zu starten, führen Sie folgenden Befehl aus:

buddy-ng

Das Programm antwortet wie folgt:

buddy-ng

Waiting for connexion

## 4.11 Packetforge-ng

Mit Packetforge-ng stellen Sie verschlüsselte Pakete her, die Sie dann für das Injizieren verwenden können. Das Tool erlaubt das Erstellen von unterschiedlichen Pakettypen, beispielsweise von ARP-Requests, UDP-, ICMP- und spezifische Pakete. Meist verwendet man ARP-Requests für das Injizieren.

Um ein verschlüsseltes Paket zu generieren, benötigen Sie die PRGA-Datei (Pseudo Random Generation Algorithm), die Sie beispielsweise über einen Fragmentation-Angriff erhalten. Und so setzen Sie das Tool ein:

packetforge-ng <modus> <optionen>

Packetforge-ng unterstützt folgende Modi (wichtig ist, dass Sie den Doppelstrich verwenden):

- **—arp**: Fälscht ein ARP-Paket.
- **—udp**: Fälscht ein UDP-Paket.
- **—icmp**: Fläscht ein ICMP-Paket.
- **—null**: Erzeugt ein Null-Paket.
- **—custom**: Erzeugt ein benutzerdefiniertes Paket.

Dabei stehen Ihnen folgende Optionen zur Verfügung:

- **-a <bssid>**: Legt die MAC-Adresse des Access Points fest.
- **-c <dmac>**: Bestimmt die MAC-Adresse des Ziels.
- **-h <smac>**: Bestimmt die MAC-Adresse der Quelle.
- **-j**: Legt das FromDS-Bit fest.
- **-e**: Deaktiviert die WEP-Verschlüsselung
- **-k <ip[:port]>**: Bestimmt die IP-Adresse und den Port des Ziels.
- **-l <ip[:port]>**: Bestimmt die IP-Adresse und den Port der Quelle.
- **-t ttl**: Bestimmt den TTL-Wert.
- **-w <datei>**: Schreibt die Pakete in die PCAP-Datei.

Sie können außerdem zwei quellenspezifische Optionen verwenden:

- **-r <datei>**: Liest die Paket von der RAW-Datei.

- **-y <datei>**: Liest PRGA von der Datei.

Ein typisches Anwendungsbeispiel zeigt, wie man Packetforge-ng in der Praxis einsetzt. Wir generieren ein ARP-Request-Paket. Dazu muss zunächst eine XOR-Datei erzeugt werden. Das kann beispielsweise mit Aireplay-ng erfolgen. Liegt die XOR-Datei vor, führen Sie folgenden Befehl aus:

```
packetforge-ng -0 -a 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D -k 192.168.1.100 -l 192.168.1.1 -y fragment-0124-161129.xor -w arp-request
```

Die Option *-0* zeigt an, dass ein ARP-Request-Paket erzeugt wird. Die MAC-Adresse des Access Points bestimmt die Option *-a 00:14:6C:7E:40:80*.

Mit *-h 00:0F:B5:AB:CB:9D* geben Sie die MAC-Adresse der Quelle an. Die Ziel-IP-Adresse bestimmen Sie mit der Option *-k 192.168.1.100*. Die Quell-IP-Adresse bestimmen Sie mit *-l 192.168.1.1*. Dann bestimmen Sie die XOR-Datei und führen das Schreiben des ARP-Pakets mit *-w arp-packet* aus.

Das oben erstellte Paket können Sie mit folgendem Befehl entschlüsseln:

```
airdecap-ng -w <access point schlüssel> arp-request
```

Das Ergebnis des Befehls:

```
Total number of packets read          1
Total number of WEP data packets      1
Total number of WPA data packets      0
Number of plaintext data packets      0
Number of decrypted WEP  packets      1
Number of decrypted WPA  packets      0
```

Um das entschlüsselte Paket einzusehen, verwenden Sie folgenden Befehl:

```
tcpdump -n -vvv -e -s0 -r arp-request-dec
```

## 4.12 Airdecap-ng

Ein letztes Tool der Aircrack-Suite sollten Sie noch kennen: Airdecap-ng. Damit können Sie WEP-, WPA- und WPA2-verschlüsselte Pakete entschlüsseln. Außerdem können Sie damit die Wireless-Header von nicht verschlüsselten CAP-Dateien entfernen.

Die Ausführung:

```
airdecap-ng [optionen] <pcap-datei>
```

Dabei können Sie folgende Optionen verwenden:

- **-l**: Löscht die IEEE 802.11-Header nicht.
- **-b**: Bestimmt die MAC-Adresse des Routers.
- **-k**: WPA/WPA2-PMK in hexadezimaler Form.
- **-e**: Gibt die SSID an.
- **-p**: WPA-/WPA2-Schlüssel.
- **-w**: WEP-Schlüssel in hexadezimaler Form.

Was können Sie nun konkret mit diesem Tool anfangen? Einige Beispiele erläutern die Möglichkeiten. Um den Header von einer nicht verschlüsselten CAP-Datei zu entfernen, verwenden Sie folgenden Befehl:

```
airdecap-ng -b 00:09:5B:10:BC:5A beispiel.cap
```

Um eine WEP-verschlüsselte CAP-Datei zu entschlüsseln, verwenden Sie folgenden Befehl (wobei es wichtig ist, dass der WEP-Schüssel in hexadezimaler Form angegeben wird:

```
airdecap-ng -w 11A3E229084349BC25D97E2939 beispiel.cap
```

Um eine WPA- b zw. WPA2-verschlüsselte CAP-Datei zu entschlüsseln, verwenden Sie folgenden Befehl:

```
airdecap-ng -e ssid -p passphrase beispiel.cap
```

Damit das Entschlüsseln klappt, muss die CAP-Datei einen fehlerfreien Four-Way Handshake beinhalten.

# 5 Zusammenfassung – WLAN hacken und schützen

Der drahtlosen Technik haben wir es zu verdanken, dass wir sozusagen immer und überall online sein können. Und das mit den unterschiedlichsten Geräten. Sie können mit dem Notebook, mit dem Tablet und mit Ihrem Smartphone auf lokale und globale Netzwerk zugreifen. Und das über Gebäudegrenzen, Zäune und andere Hindernisse hinweg. Gerade diese Merkmale sind es, die es potentiellen Angreifern so einfach machen, ein WLAN zu attackieren. Drahtlose Netzwerke verwenden Radiowellen für die Verbindung der Computer, die auf Basis der Ebene 1 des OSI-Schichtenmodells implementiert sind.

Die meisten drahtlosen Geräte stellen ihren Anwendern nach dem Aktivieren des WLAN-Adapaters eine Liste der gefundenen WLANs zur Verfügung. Ist ein Netzwerk nicht geschützt, so hat man unmittelbar Zugang zu diesem. Bei passwortgeschützten WLANs benötigt man das Passwort.

## 5.1 Die Authentifizierung

Die Authentifizierung an einem WLAN erfolgt dabei mit drei verschiedenen Techniken: WEP, WPA und WPA2. Der älteste, aber heute immer noch anzutreffende Standard ist WEP (Wired Equivalent Privacy). Dieser Standard verschlüsselt die übertragenen Daten mit einem simplen Mechanismus, der selbst auf zwei Techniken setzt:

- **Open System Authentication** (OSA): Dieses Verfahren gewährt Zugang auf Grundlage einer Zugriffsrichtlinie.
- **Shared Key Authentication** (SKA): Dieses Verfahren sendet eine verschlüsselte Challenge-Nachricht an den Access Point und bittet um Zugang. Der Access Point verschlüsselt die Challenge mit seinem Schlüssel und antwortet. Stimmt die Verschlüsselung mit der Konfiguration des Access Points überein, gewährt dieser dem Client den Zugang.

Wie wir bereits im ersten Kapitel gesehen haben, weist WEP erhebliche Schwächen auf. Die Integrität der Pakete wird mittels Cyclic Redundancy Check (CRC32) geprüft. Dieser Check kann allerdings durch das Aufzeichnen zweier Pakete geknackt werden. Die Bits in dem verschlüsselten Datenstrom und der Prüfsumme können durch den Angreifer modifiziert werden, und werden dann von dem Authentifizierungsmechanismus akzeptiert. WEP verwendet den RC4-Verschlüsselungsalgorithmus. Wie wir oben gesehen haben, kann dieser Schutz recht einfach ausgehebelt werden und ist insbesondere für Wörterbuchattacken anfällig.

Der Nachfolger WPA bietet zwar gegenüber WEP einen deutlich besseren Schutz, aber auch er ist aufgrund von Implementierungsschwächen und für DoS-Attacken anfällig.

Im bisherigen Verlauf dieses Buchs haben Sie verschiedene Tools kennengelernt, die Sie beim Knacken von WLAN-Sicherungsmechanismen unterstützen. Um den WEP-Schutz

auszuheblen, benötigen Sie insbesondere die folgenden Werkzeuge:

- Aircrack-ng – Netzwerk-Sniffer und WEP-Cracker
  Download: htttp://www.aircrack-ng.org
- WEPCrack – Spezialist für das Knacken von WEP-Schlüsseln
  Download: http://wepcrack.sourceforge.net
- Kismet – WLAN-Detektor und Sniffer und IDS
  Download: http://www.kismetwireless.net
- WebDecrypt – Führt Wörterbuchattacken gegen WEP-Schlüssel durch
  Download: http://wepdecrypt.sourceforge.net

Für das Knacken von WPA-Schlüsseln, sollten Sie außerdem folgende Tools kennen:

- CowPatty – Führt Brute Force-Attacken aus
  Download: http://wirelessdefence.org/Contents/coWPAttyMain.htm
- Cain & Abel – Dekodierer, Sniffer und Cracker
  Download: http://www.oxid.it/cain.html

In diesem Handbuch haben Sie diese Tools – soweit erforderlich – kennengelernt. Sie haben auch gesehen, dass das Knacken von gängigen Schutzmechanismen kein Hexenwerk ist. Umso wichtiger ist es, dass Sie den Schutz und die Sicherheit Ihrer drahtlosen Umgebung erhöhen.

## 5.2 Schutz

Ein WLAN ist – ob man es will oder nicht – ein Segen für die Anwender, aber ein Fluch für die Sicherheit und für alle mit der Sicherheit beauftragten Personen. Wie aber optimiert man den Schutz für sein eigenes drahtloses Netzwerk? Den optimalen Schutz erzielen Sie, wenn Sie an allen Stellschrauben Ihrer WLAN-Infrastruktur die Sicherheit maximieren. So gehen Sie dabei vor:

- **Schritt 1 – Systemkonfigurationen härten**: Im ersten Schritt sollten Sie die Systemeinstellungen des Access Points und der WLAN-Clients optimieren. Dazu machen Sie zunächst den AC unsichtbar und aktivieren die Verwendung von WPA2.
- **Schritt 2 – Sicheres Passwort**: Verwenden Sie ein langes und kompliziertes Passwort. Es sollte mindestens 13 Zeichen lang sein und auch Sonderzeichen wie §, $ und ? enthalten. Implemtieren Sie außerdem eine Richtlinie, die festlegt, in welchen Intervallen die Passwörter geändert werden müssen.
- **Schritt 3 – WIDS/WIPS einrichten**: Richten Sie ein Wireless Intrusion Detection System bzw. ein Wireless Intrusion Prevention System ein. Damit steht Ihnen eine Lösung zur Verfügung, die mögliche Attacken erkennt und Ihnen

Reaktionsmöglichkeiten bietet.

- **Schritt 4 – Sicherheitschecks**: Führen Sie in regelmäßigen Abständen kontinuierliche Sicherheitschecks Ihrer WLAN-Umgebung durch. Diese Systeme liefern Ihnen auch entsprechende Empfehlungen zur Behebung potenzieller Schwachstellen.
- **Schritt 5 – Sichere Tunnel**: Überall dort, wo unternehmenskritische Daten zwischen einem Access Point einem WLAN-Client transferiert werden, sollten Sie zu einer VPN-Lösung greifen und so einen sicheren Datenkanal über eine unsichere Netzwerkverbindung legen. Entprechende VPN-Server und Clients gibt es zu Genüge. Mit OpenVPN steht Ihnen eine entsprechende Open Source-Lösung zur Verfügung. Auch für Smartphones, Tablets und Notebooks gibt es entsprechende Lösungen.

Bei Schritt 6 angelangt, beginnt das Spiel wieder von vorne – ein permanenter Kreislauf, mit dem Sie die Sicherheit Ihrer WLAN-Infrastruktur maximieren.

# Anhang – More Info

Mit Hilfe von Security Scannern können Sie in der Regel schnell und umkompliziert aktuelle Schwachstellen und Sicherheitslücken aufdecken. Parallel dazu sollten Sie regelmäßig die wichtigsten Schwachstellendatenbanken auf für Sie relevante Meldungen prüfen. Nachfolgend finden Sie eine Liste der interessantesten Informationsquellen:

- **CERT Vulnerability Notes Database** – https://www.kb.cert.org/vuls/
- **Datenbank für IT-Angriffsanalysen des Hasso-Plattner-Instituts** – https://www.hpi-vdb.de/vulndb/
- **Exploit Database** – https://www.exploit-db.com/
- **Google Hacking Database** (GHDB) – https://www.exploit-db.com/google-hacking-database/
- **National Vulnerability Database** – https://web.nvd.nist.gov/view/vuln/search/
- **SecurityFocus** - http://www.securityfocus.com/vulnerabilities/

Die Liste erhebt keinen Anspruch auf Vollständigkeit, sondern ist als Ausgangspunkt für Ihre weiteren Recherchen gedacht.

# Weitere Brain-Media.de-Bücher


**Dreambox 8000 kompakt**

Die Dreambox 8000 stellt ihre Vorgänger allesamt in den Schatten. Was Sie alles mit der Dreambox 8000 anfangen können, verrät Ihnen die Neuauflage unseres Dreambox-Klassikers. Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

**Umfang**: 450 Seiten plus CD
**ISBN**: 978-3-939316-90-9
**Preis**: 29,80 EUR


**X-Plane 10 kompakt**

Der Klassiker unter den Flugsimulatoren geht in die zehnte Runde. Viele neue Funktionen und verbessertes Handling warten auf die Anwender. Kein Wunder also, dass die Fangemeinde wächst und wächst. Unser Handbuch beschreibt alles, was Sie für das Fliegen mit X-Plane wissen sollten.

**Umfang**: 430 Seiten
**ISBN**: 978-3-939316-96-1
**Preis**: 24,80 EUR


**Audacity 2.0 kompakt**

Audacity ist zweifelsohne das beliebteste freie Audioprogramm. Vom anfänglichen Geheimtipp hat sich der Editor zum Standard für die Aufzeichnung und Bearbeitung von Audiodaten gemausert. Das Vorwort steuert der ehemalige Core-Entwickler Markus Meyer bei.

**Umfang**: 306 Seiten
**ISBN**: 978-3-95444-027-6

**Preis**: 24,80 EUR


**Evernote kompakt**

Bei der alltäglichen Informationsflut wird es immer schwieriger, Wichtiges von Unwichtigem zu trennen, Termine und Kontakte zu verwalten. Mit Evernote können Sie diese Flut bändigen und Ihren Alltag optimieren. “Evernote kompakt” vermittelt das notwendige Know-how für den Einsatz von Evernote auf Ihrem Desktop, Smartphone und online.

**Umfang**: 320 Seiten
**ISBN**: 978-3-95444-098-6
**Preis**: 22,80 EUR


**Fire TV kompakt**

Mit Fire TV hat Amazon eine tolle kleine Box für das Online-Entertainment auf den Markt gebracht, die für wenig Geld die gesamte Palette der Internet-basieren Unterhaltung abdeckt. In diesem Handbuch erfahren Sie, was Sie alles mit der kleinen Box anstellen können.

**Umfang**: 182 Seiten
**ISBN**: 978-3-95444-172-3
**Preis**: 16,80 EUR


**Magento SEO kompakt**

Magento ist die Standardumgebung für den Aufbau eines Online-Shops. Doch damit Sie mit Ihren Shop-Angebot auch im Internet wahrgenommen werden, müssen Sie ein wenig die Werbetrommel rühren und den Shop für Google & Co. optimieren. Mit wenigen Handgriffen machen Sie Ihren Online-Shop SEO-fest und maximieren Ihre Verkäufe.

**Umfang**: 100 Seiten
**ISBN**: 978-3-95444-098-6

**Preis**: 14,80 EUR


**Wireshark kompakt**

Wireshark ist der mit Abstand beliebteste Spezialist für die Netzwerk- und Protokollanalyse. In diesem Handbuch lernen Sie, wie Sie mit dem Tool typische Administratoraufgaben bewältigen. Das Buch beschränkt sich dabei auf die wesentlichen Aktionen, die im Admin-Alltag auf Sie warten, und verzichtet bewusst auf überflüssigen Ballast.

**Umfang**: 170 Seiten
**ISBN**: 978-3-95444-176-1
**Preis**: 16,80 EUR


**Scribus 1.5 kompakt**

Scribus ist längst ein ebenbürtiger Gegenspieler von InDesign & Co. In unserem Handbuch erfahren Sie alles, was Sie für den erfolgreichen Einstieg wissen müssen. 460 Seiten Praxis-Know-how. Dazu viele Tausend ClipArts und Schriften zum kostenlosen Download.

**Umfang**: 460 Seiten
**ISBN**: 978-3-95444-124-2
**Preis**: 27,80 EUR

# Weitere Titel in Vorbereitung

Wir bauen unser Programm kontinuierlich aus. Aktuell befinden sich folgende Titel in Vorbereitung:

· Android Forensik

· Android Security

· Alfresco 5.0 kompakt

· Cain & Abel kompakt

· VirtualBox 5.0 kompakt

· WordPress 4.x kompakt

· Smart Home kompakt

· Das papierlose Büro

· Galaxy Note 5 kompakt

## Plus+

Plus+ − unser neues Angebot für Sie … alle E-Books im Abo. Sie können 1 Jahr alle Brain-Media-Bücher als E-Book herunterladen und diese auf Ihrem PC, Tablet, iPad und Kindle verwenden − und das ohne irgendwelche Einschränkungen. Das Beste: Plus+ schließt auch alle jene Bücher ein, die in diesem Jahr noch erscheinen.

**Und das zum Sonderpreis von 29 Euro! Ein unschlagbares Angebot!**

Auf unserer Website steht ein detaillierter Überblick aller Titel im PDF-Format zum Download bereit (ca. 6,2 MB), der bereits zu Plus+ gehörende Titel aufführt und die in naher Zukunft hinzukommen.