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

© 2015 Brain-Media.de

Herausgeber: Dr. Holger Reibold

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Coverbild: streichholz / photocase.de

Korrektur: Theresa Tting

Inhaltsverzeichnis

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,

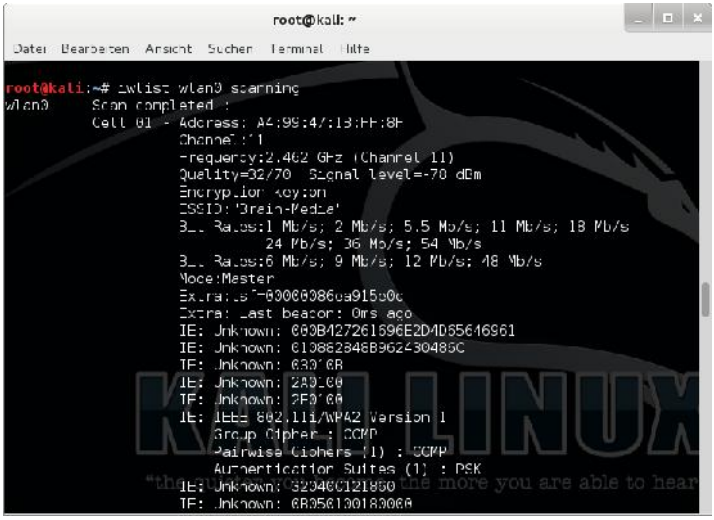
Holger Reibold

(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 Administrator 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 Kommunikation 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
```

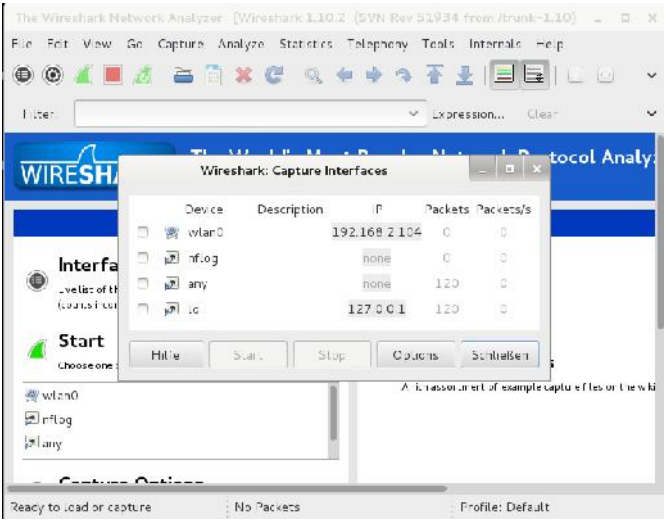
Um den Adapter in den Monitormodus zu versetzen, führen Sie folgenden Befehl aus:

```
airmon-ng
```

Dann folgenden Befehl:

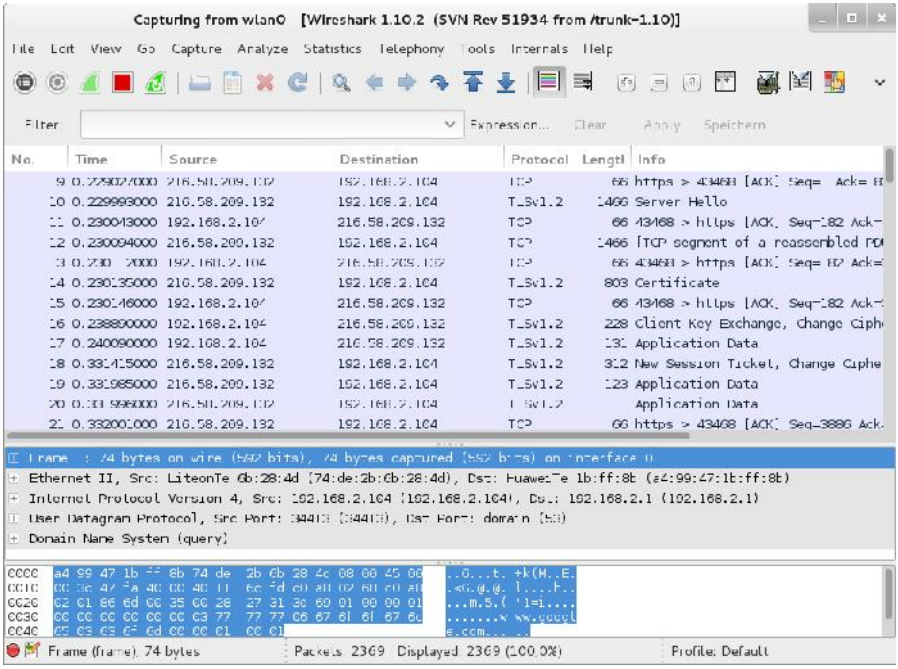
```
airmon-ng start wlan1
```

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.



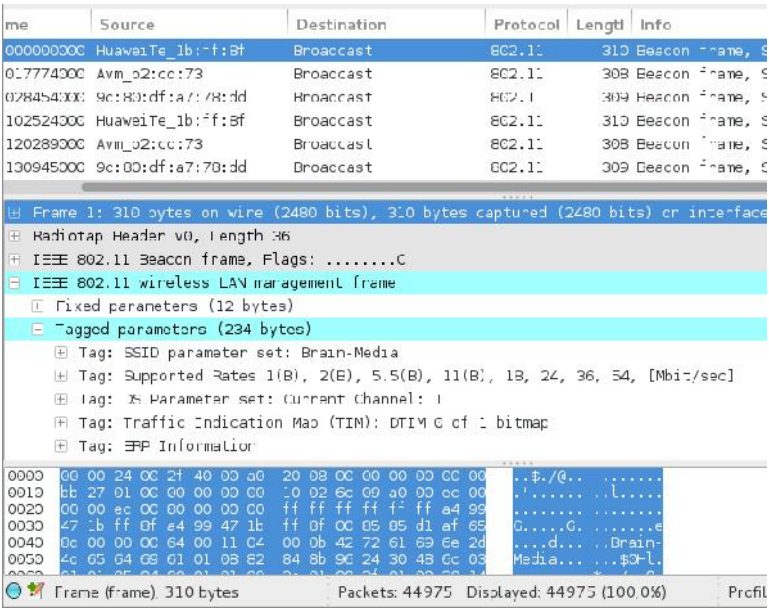
Die Wireshark-Sniffer in Aktion.

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.

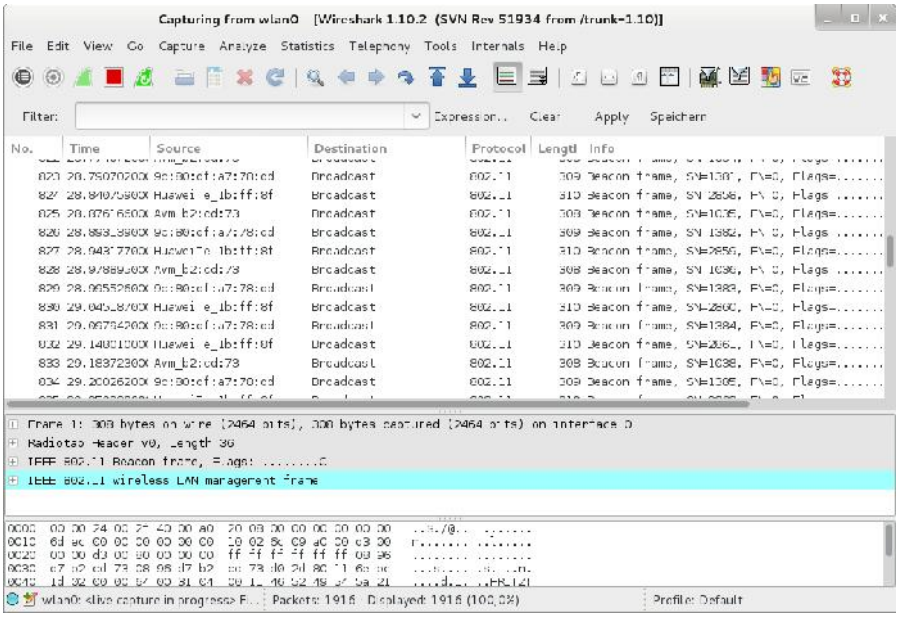
1.2 WLAN-Authentifizierung umgehen

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.

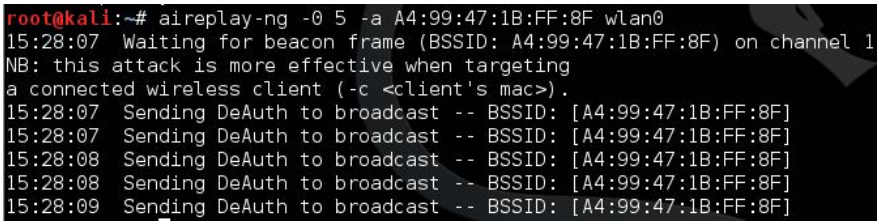
Wenn Sie nun einen entsprechenden Paketeintrag unter die Lupe nehmen und dessen SSID-Informationen öffnen, werden Sie feststellen, dass Sie dort die ID wieder

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.

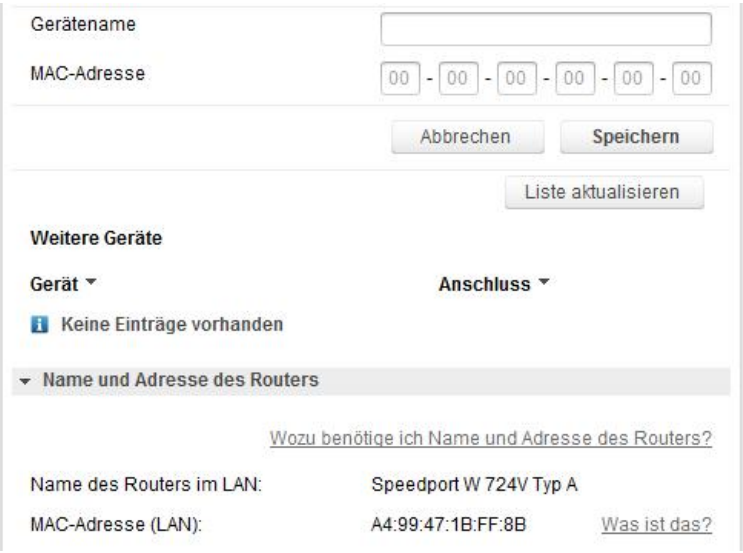
Dieser Befehl führt dazu, dass alle legitimierten Client-Verbindungen unterbrochen und wieder aufgebaut werden. Zeichnen Sie diese Aktionen mit Wireshark auf. Uns interessieren als Nächstes die Deauthentifizierungs-Pakete. Begrenzen Sie die Ansicht in der Wireshark auf diese Pakete.

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!

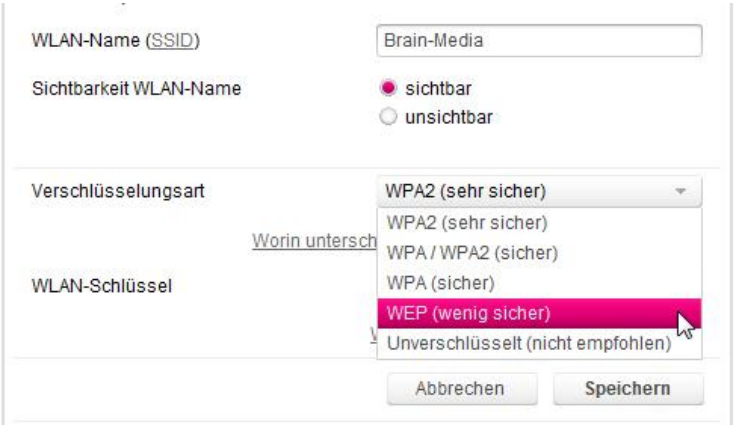
1.2.3 Schlüsselauthentifizierung umgehen

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.

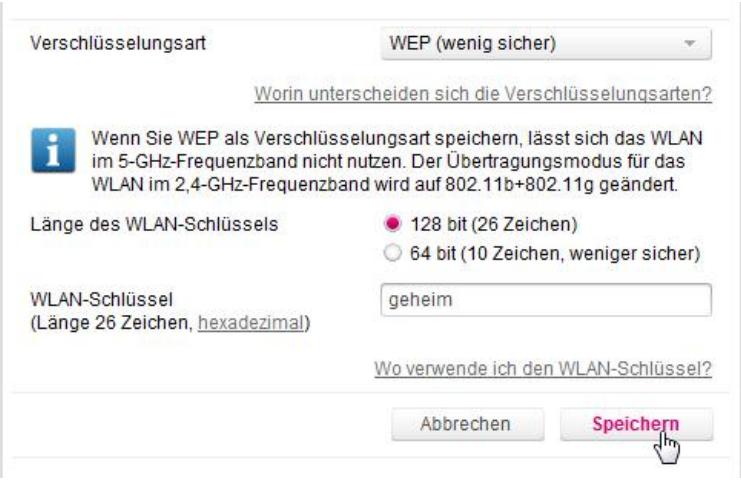
Abschließend können Sie dann in der Protokolldatei des WLAN-Routers das Zustandekommen einer Verbindung mit der MAC-Adresse *AA:AA:AA:AA:AA:AA* finden. Das ist unser WLAN-Client mit der Kali Linux-Installation. Der entsprechende Rechnereintrag in der Protokolldatei lautet einfach *Kali*.

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:

1. 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.

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

   ```
   ifconfig wlan0 up
   ```

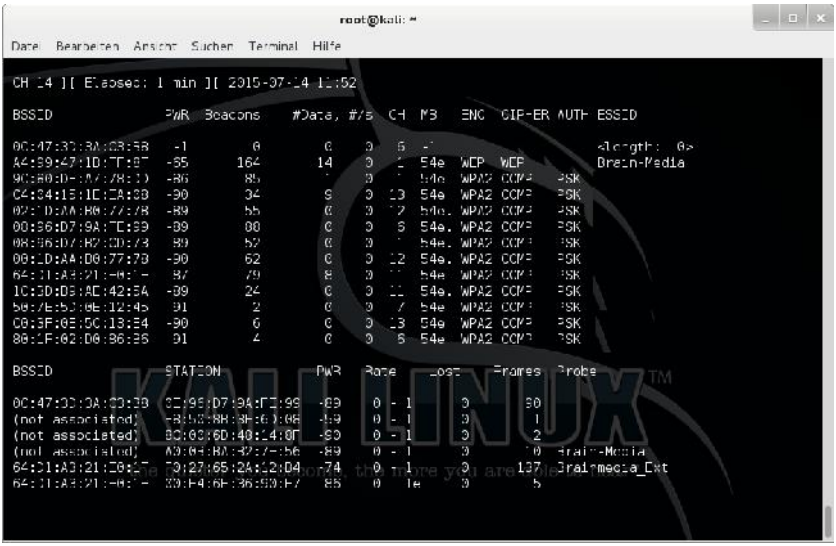
   ```
   airmon-ng start wlan0
   ```

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

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

   ```
   airodump-ng mon0
   ```

4. 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.

5. 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.

6. 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
   ```

7. Kurz darauf sollten die ARP-Pakete auf der Konsole ausgegeben werden. Etwaige Fehlermeldungen können sie mit der Option *--ignore-negative-one* ausblenden.

8. Es folgt das eigentliche Cracken. Dazu starten Sie Aircrack-ng mit der Option *Brain-Media-01.cap* in einem neuen Fenster. Damit beginnt Aircrack-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.

9. 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.

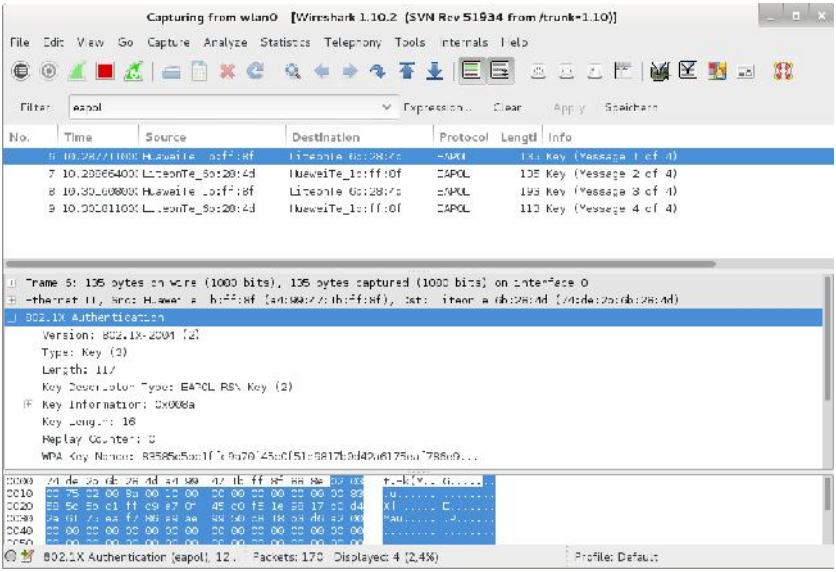
1.4 WPA-Sicherung aushebeln

Während WEP-gesicherte Verbindungen ohnehin nicht als sonderlich sicher gelten, 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
```

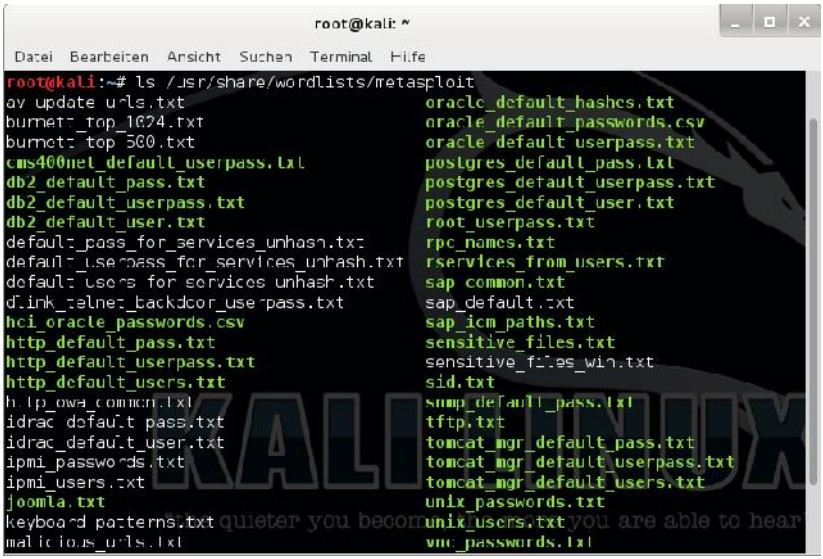
Nun stellen Sie mit einem Client eine Verbindung zu dem Access Point her und zeichnen den WPA-Handshake auf. Auch bei dieser Attacke können Sie eine Deauthentifizierungs-Nachricht an den Access Point senden, damit die Client-Verbindungen unterbrochen und wieder aufgenommen werden.



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 Wireshark. 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.*

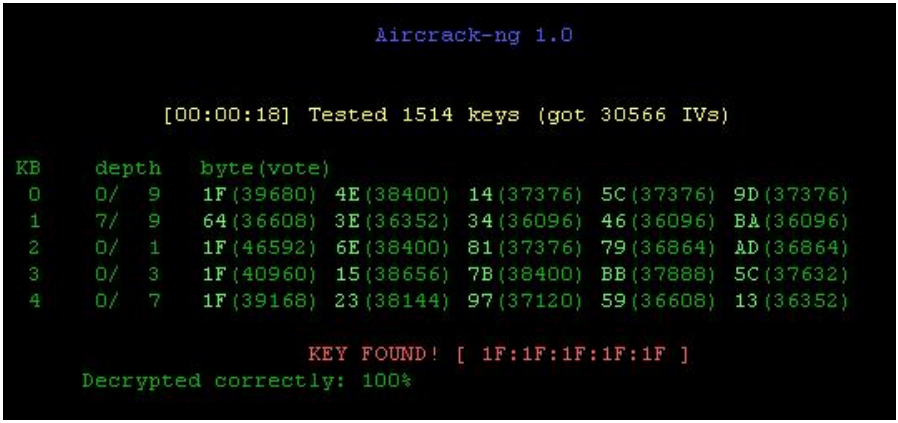


Bei der Wörterbuchattacke greifen Sie auf Metasploit-Wörterlisten zurück.

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:

1. 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.

2. 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.

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

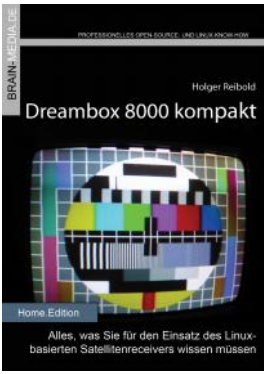
V

W

X

Z

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.