36clicks, 123RF

Kismet, Aircrack-NG und Karmetasploit

Funkloch

Dass drahtlose Netzwerke nicht der Gipfel der Netzwerksicherheit sind, dürfte mittlerweile bekannt sein. Hier erfahren Sie im Detail, welche Techniken Angreifer verwenden und was sie damit anstellen. Kurt Seifried

Gibt es eigentlich noch jemanden, der zu Hause kein drahtloses Netzwerk nutzt? Jeder kauft sich doch heute einen Laptop und für 50 Euro einen Accesspoint, wenn der nicht ohnehin schon im Paket des Providers enthalten ist. Doch wer diesen Artikel gelesen hat, wird vielleicht gerne wieder zum Kabel wechseln.

Eines der gegenwärtig besten Tools, um drahtlose Netze zu finden, ist Kismet. Viele Linux-Distributionen bringen allerdings nur eine alte Version mit, laden Sie also am besten die neueste von der Homepage herunter [1] und installiere sie von Hand. Vor »make install« müssen Sie zuerst noch das Skript »config« ausführen. Weil Kismet Administrator-Rechte erfordert, starten Sie es als Root oder mit »sudo«.

Kismet besteht aus drei Komponenten: der Drone, dem Server und dem Client. Die Drone schneidet den Netzwerkverkehr mit und sendet ihn an den Server, der auf dem gleichen oder einem anderen Rechner laufen kann. Der Server sammelt die Daten und der Client präsentiert sie dem Anwender in einem textbasierten Interface. Diese Architektur erlaubt es, mit mehreren Dronen Daten mitzuschneiden und sie an zentraler Stelle zu sammeln.

Mit GPS

Um Kismet zu starten, geben Sie einfach »kismet_client« ein. Sie haben dann die Option, den Server ebenfalls zu starten. Der Server schreibt mehrere Dateien: GPS-Daten, um Netzwerke einem Ort zuzuordnen, Netzwerk-Metadaten (wie Channels und Konfiguration) und schließlich den Mitschnitt in Form einer Pcap-Datei.

Wenn Kismet mit nur einer Datenquelle arbeitet, muss es immer wieder die Kanäle wechseln, um alle elf Möglichkeiten abzudecken. So findet es zwar alle Netze, aber die Mitschnitte sind fragmentiert

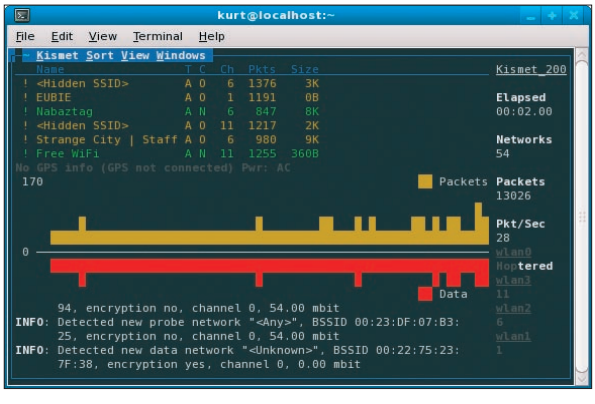

Abbildung 1: Der Kismet-Client mit vier Capture-Quellen.

und enthalten mal einen Ausschnitt des Traffic von einem Kanal und dann wieder von einem anderen.

Die Lösung ist, mehrere WLAN-Geräte zu besorgen (zum Beispiel mit USB) und entsprechende Capture-Interfaces in Kismet anzulegen. Mit vier WLAN-Karten decken Sie schon eine Menge ab, denn damit können Sie die drei Hauptkanäle 1, 3 und 11 (siehe Abbildung 1) permanent mitschneiden und mit der vierten Karte die restlichen Kanäle durchscannen (siehe Abbildung 2). Die Konfiguration dafür zeigt Listing 1.

Bei einem Test in einem Café eines dicht besiedelten Viertels ließen sich so innerhalb weniger Minuten über 40 drahtlose Netze finden. Bei einem weiteren Versuch waren es sogar über 70 WLANs. Im Durchschnitt war etwa die Hälfte der Netze unverschlüsselt. Viele waren kostenpflichtige WLANs, in einigen gab es nur einen Client, vermutlich in den typischen Heimnetzen. Bei den Bezahlnetzen ließen sich sehr leicht die MAC-Adressen der Benutzer mitschneiden, was so interessant ist, weil viele Filter auf der Basis von MAC-Adressen arbeiten, die sich leicht fälschen lassen.

Verschlüsselt

Dass WEP sich leicht knacken lässt, dürfte mittlerweile bekannt sein, dennoch findet man immer wieder auch mal ein WEP-Netz. Die meisten Linux-Distributionen enthalten das Programm Aircrack-NG [2], das Angriffe auf mit WEP oder WPA gesicherte Distributionen erlaubt. Um es zu benutzen, starten Sie »airoscript«, das ein textbasiertes User-Interface bietet. Beschränken Sie solche Angriffe aber auf das eigene WLAN, andernfalls begehen Sie eine Straftat. Wer faul ist, kann mit der Option »auto« alles Weitere dem Aircrack-Tool überlassen.

Neuere Ansätze beim Cracken von WPA/WPA2-PSK benutzen die Parallel-Rechenfähigkeiten von Nvidia-Grafikkarten für eine Brute-Force-Attacke. So kann das Pyrit-Tool [3] auf vier parallel rechnenden Geforce 295 GTX knapp 90 000 Schlüssel in der Sekunde erzeugen.

Umgekehrt

Ein weiteres potenzielles Problem mit WLAN-Sicherheit dreht den Spieß um. Angreifer brechen nicht in ein bestehendes Netz ein, sondern gaukeln einem Client ein legitimes WLAN vor. Sie greifen dann die Authentifizierungs-Informationen ab und leiten sie an den echten Accesspoint weiter.

Die weitergeleiteten Daten können sie nach Lust und Laune verändern. Ein Tool, das einen so genannten Rogue Accesspoint aufbaut, heißt Karmetasploit [4] und ist Teil des Metasploit-Framework, über das der ADMIN-Artikel [5] mehr Details verrät.

Wenn Metasploit und Aircrack-NG installiert sind, fehlt noch ein DHCP-Server für die WLAN-Netzwerkschnittstelle. Ist er installiert, übernimmt »airbase-ng« den Part des Accesspoint. Die Servermodule von Metasploit können dann Man-in-the-Middle-Attacken starten und mit »autopwn« Malware in Webseiten einschleusen. Mit der gleichen Technik simulieren Cracker auch kostenpflichtige Accesspoints und präsentieren dem arglosen Anwender im Webbrowser Zugangsseiten, über die sie Kreditkarten-Informationen abgreifen.

Klartext

Selbst wer vorsichtig ist, kann sich nicht auf WLAN-Sicherheit verlassen. So verwenden die meisten Bezahl-WLANs keine Verschlüsselung, weil es zu aufwendig wäre, jedem Kunden einen Key zukommen zu lassen. Einen von allen gemeinsam genutzen Schlüssel könnte ein Angreifer ohnehin wieder in seinen Besitz bringen und damit alles mitlesen. Auch wenn WLAN-Anbieter während des Bezahlens die Verbindung mit SSL verschlüsseln, können Hacker danach wieder Ihren ganzen Netzwerkverkehr sniffen und mitlesen.

Listing 1: Vier Quellen

```
01 channellist=hoplist:2,3,4,5,7,8,9,10
02 ncsource=wlan0:hop=false,channel=1
03 ncsource=wlan1:hop=false,channel=6
04 ncsource=wlan2:hop=false,channel=11
05 ncsource=wlan3:hop=true,channellist=hoplist
```

Beste Lösung: VPN

Das beste Mittel gegen jede Art von Abhören sind sichere Tunnel, wie Sie ein Artikel im letzten ADMIN-Heft beschreibt [6], zum Beispiel mit VPN. Wer keinen eigenen Server hat, um einen VPN-Endpunkt zu betreiben, kann bei einem Dienstleister wie Ipredator oder Swiss-VPN einen VPN-Dienst einkaufen. Hier ist allerdings wieder Vertrauen in die Zuverlässigkeit und Kompetenz des Dienstleisters gefragt. *(ofr)* ■

Infos

[1] Kismet: [http://www.kismetwireless.net]
[2] Aircrack-NG: [http://www.aircrack-ng.org/]
[3] Pyrit: [http://code.google.com/p/pyrit/]
[4] Karmetasploit: [http://trac.metasploit.com/wiki/Karmetasploit]
[5] Kurt Seifried, „Security Auditing mit Metasploit“: ADMIN 01/2009, [http://www.admin-magazin.de/content/security-auditing-mit-metasploit]
[6] Kurt Seifried, „Tunnel-Techniken“: ADMIN 05/2010, S. 94

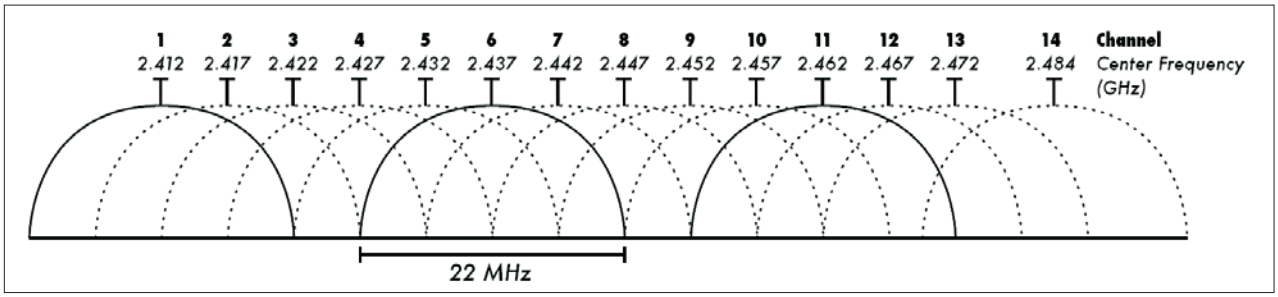

Abbildung 2: Frequenzdiagramm des WLAN-Spektrums: Nur die Hauptkanäle 1, 6 und 11 sind überschneidungsfrei. (Quelle: Wikipedia)