WLAN-Sniffer

aus Wikipedia, der freien Enzyklopädie

Ein **WLAN-Sniffer** ist ein Programm, das zum Auffinden und Abhören von Wireless LANs dient.

Inhaltsverzeichnis

Funktionsweise

Es gibt zwei Arten von WLAN-Sniffern: Aktive und Passive.

Aktive WLAN-Sniffer

Zu dieser Kategorie gehört der recht verbreitete Netstumbler, der vor allem auf Windowssystemen genutzt wird. Aktive WLAN-Sniffer senden sogenannte Probe-Request-Pakete an den Access-Point, welcher daraufhin mit einem Probe-Response-Paket antwortet. Es findet also eine explizite Abfrage statt. Umgangssprachlich kann man das vielleicht folgendermaßen erklären: Der Sniffer ruft auf jedem Kanal "Hallo, ist da jemand?" und jeder Access-Point, der diesen "hören" kann (im aktuellen WLAN-Kanal) antwortet "Ja, hier ist Netz 'soundso'".

Passive WLAN-Sniffer

Der bekannteste Sniffer dieser Kategorie ist der unter (u.a.) GNU/Linux weit verbreitete Sniffer Kismet. Zum Auffinden und Abhören wird die WLAN-Karte in einen Monitormodus (nicht zu verwechseln mit dem Promiscuous Mode, der eine Schicht höher arbeitet) geschaltet. Sie sendet nun keine Daten mehr, sondern reicht die empfangenen Pakete direkt und roh an den WLAN-Sniffer weiter. Damit kann der Benutzer des Sniffers erkennen, ob sich ein WLAN in Reichweite befindet und

welche Parameter das Netz hat. Empfangen werden entweder die Nutzdaten (der normale Netzverkehr) des WLANs oder, wenn beispielsweise nachts der AP der einzige Knoten im WLAN-Netz ist, die sogenannten Beacons. Sobald ausreichend "Pakete" (bis zu 10 Mio. - bei neueren Angriffen wie dem von KoreK genügen jedoch häufig schon 10% oder weniger davon) gesammelt wurden, kann mit dem Erraten des WEP Schlüssels begonnen werden. Passivscanner haben ein paar Vorteile gegenüber Aktivscannern:

- Passivscanner können nicht ausgemacht werden, da keinerlei Emissionen vom Scanner ausgehen. Wardriving mit passivem Scanner ist demzufolge nicht in Logfiles (außer dem des Scanners) nachweisbar.
- Passivscanner können natürlich Aktivscanner erkennen. So ist es beispielsweise möglich Intrusion Detection Systeme wie Snort an passive Scanner wie Kismet zu koppeln, um Angriffe auf WLAN-Netzwerke zu bemerken.
- Passivscanner erkennen auch "exotische" WLAN-Netze, die nicht auf normale Probe-Requests antworten, abgewandelte Protokolle verwenden (Straßenbahnen in manchen Städten), oder deren ESSID verborgen ist, kurz gesagt, bei denen kein "Handshake" wie oben beschrieben zustande kommt.

WLAN-Sniffer werden auch von WarDrivern und WarWalkern eingesetzt. Diese Programme sind sehr einfach zu benutzen und somit auch für ein Skriptkiddie geeignet. Das unerlaubte, absichtliche Abhören oder Protokollieren von Funkverbindungen ist natürlich verboten. Ungewolltes Abhören scheint nach dem Telekommunikationsgesetz erlaubt zu sein, jedoch ist eine Speicherung, Weitergabe oder Verwendung der derart erlangten Daten ebenfalls nicht zulässig.

WLAN-Sniffer

POSIX

- dstumbler (http://dachb0den.com/projects/dstumbler.html) – BSD
- bsd-airtools (http://dachb0den.com/projects/bsd-airtools.html) – BSD, Toolkit (passiv, WEP-Cracker, WLAN-Bibliothek, ...)
- wifiscanner (http://wifiscanner.sourceforge.net/) – Linux, *BSD, Mac OS X (GPL)
- Kismet (http://kismetwireless.net/) – Linux, *BSD, Mac OS X (GPL)
- KisMAC (http://kismac.binaervarianz.de/) – Mac OS X
- MacStumbler (http://www.macstumbler.com/) – Mac OS X

Windows

- NetStumbler (http://www.netstumbler.com/) – Windows
- Airopeek (http://www.airopeek.de/) – Windows (kommerziell)
- Sniff'em (http://www.sniff-em.com/) – Windows (kommerziell)

Andere verwendete Programme

- Airsnort (http://airsnort.shmoo.com/) – Programm zum Brechen der WEP-Verschlüsselung

- fakeAP (http://www.blackalchemy.to/project/fakeap/) – simuliert viele falsche WLANs (zum Ärgern von WarDrivern)

Siehe auch

- Sniffer
- Wired Equivalent Privacy (WEP),
- Wi-Fi Protected Access (WPA)

Von "http://de.wikipedia.org/wiki/WLAN-Sniffer"

Kategorie: WLAN