LINUX

SO EINFACH BRECHEN

PC DIREKT zeigt Ihnen, wie leicht Hacker in scheinbar sichere

München, Hauptbahnhof, Herbst 2001. Ein junger Mann sitzt auf der Wartebank eines Bahnsteigs, in seinem Schoß liegt ein Notebook eines großen US-Markenherstellers. Gespannt blickt er auf das LC-Display, hin und wieder huschen seine Finger über die Tastatur. Sie werden sich jetzt denken: „Und? Was ist daran schon Besonderes?“ Auf den ersten Blick – und in Zeiten der New Economy – nichts; wenn dieser Mann nicht gerade versuchen würde, sich per Funk in das Netzwerk eines großen, ortsansässigen Unternehmens zu hacken.

Wie einfach das ist, zeigt ein Feldversuch. Alleine bei ein paar oberirdischen Fahrten mit der S-Bahn durch verschiedene Münchner Stadtteile entdecken wir 20 verschiedene Wireless-LANs. Das Hacken wird in den meisten Fällen nicht schwer gemacht: Über 60 Prozent der gefundenen WLANs sind nicht einmal verschlüsselt – ganz gleich, ob es sich um kleine, private Netze oder große, kommerzielle Unternehmensnetzwerke handelt. Da in allen Netzwerken das Protokoll TCP/IP (Internet) zum Einsatz kommt, existieren zahlreiche Werkzeuge, um gängige Verbindungstypen bis aufs Letzte auszuspionieren: Mitlesen lassen sich E-Mails, News, private Unterhaltungen ebenso wie Kennwörter für sensible Maschinen, wie beispielsweise Datenbanken. Aber auch die durch den Standard „WEP“ geschützten Netzwerke sind keineswegs sicher: Zwar suggeriert „Wired Equivalent Privacy“, dass die Daten abhörsicher durch den Äther übertragen werden; allerdings ist diese Seifenblase der Illusion seit knapp einem halben Jahr geplatzt. Wie ein Team von Wissenschaftlern herausfand, lässt sich die WEP-Verschlüsselung durchaus angreifen – und sogar mit äußerst geringen finanziellen Mitteln knacken.

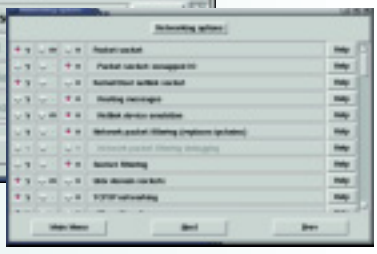
Fortsetzung auf Seite 126 ▶

1 So konfigurieren Sie den Linux-Kernel

Für den Hack eines WLAN benötigen Sie einen aktuellen Linux-Kernel (Version 2.4.x), den Sie unter http://www.de.kernel.org im Internet finden. Diesen packen Sie im Verzeichnis /usr/src/linux aus und starten seine Konfiguration mit dem Befehl „make xconfig“.

2 So konfigurieren Sie PCMCIA und Netlink

Leider ist der im Kernel 2.4.x enthaltene PCMCIA-Code für unsere Zwecke unbrauchbar. Aus diesem Grund kommentieren Sie im Menü „General Setup“ und Untermenü „PCMCIA/Cardbus support“ die Verwendung dieses Codes einfach aus.

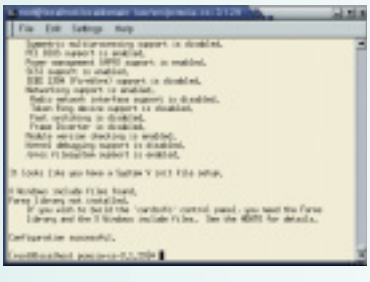


Die Datenpakete eines Netzwerks durchlaufen bei Linux eigentlich nur den geschützten Kernel-Bereich. Damit Sie diese Pakete erfolgreich erschnüffeln können, müssen Sie daher im Menü „Networking options“ die Unterstützung für den „Kernel/User Netlink socket“ aktivieren.

3 So übersetzen Sie den Linux-Kernel

Eine Anleitung zur Übersetzung des Linux-Kernels finden Sie im Verzeichnis /usr/src/linux in der Datei README und im Internet unter http://www.linux.org/docs/ldp/howto/Kernel-HOWTO.html. Hier die Grundschritte: Nach der Konfiguration geben Sie die Befehle „make bzImage“, „make modules“ und „make modules_install“ ein.

4 So erstellen Sie PCMCIA-Kernel-Module



Ein PCMCIA-Paket finden Sie im Web unter http://sourceforge.net/projects/pcmcia-cs. Die Konfiguration: Entpacken Sie das Paket ins Verzeichnis /usr/src/pcmcia-cs-3.1.29. Dort führen Sie diese Befehle aus: „make config“, „make all“, „make install“. Bei der Konfiguration können Sie die Standardvorgaben verwenden.

D-Link

DWL-650

Avitos
(018 05) 60 60 65
www.avitos.de

299 DM

Eine Wireless-LAN-Steckkarte für Notebooks bietet D-Link mit dem Modell DWL-650 an. Die Karte arbeitet nach dem Standard 802.11b mit 11 MBit/s. Mit DWL-1000AP bietet D-Link einen passenden Wireless-LAN-Access-Point an, zu dessen Highlights die Zugriffsbeschränkung auf Basis der MAC-Adresse von WLAN-Karten zählt.

SMC

2632W

Axmax
(089) 907 78 80
www.axmax.de

359 DM

Wenn Sie eine Wireless-LAN-Steckkarte für Ihr Notebook suchen, liegen Sie beim Modell 2632W von SMC genau richtig. Die Karte basiert auf dem Prism-II-Chipsatz von Intersil und arbeitet nach dem schnellen Standard 802.11b mit 11 MBit/s. Einen passenden Wireless-LAN-Access-Point liefert der Hersteller mit dem Modell 2652W für rund 899 Mark aus.

Linksys

WPC11

Drabo-COM
(07 00) 37 22 62 66
www.drabo-com.de

359 DM

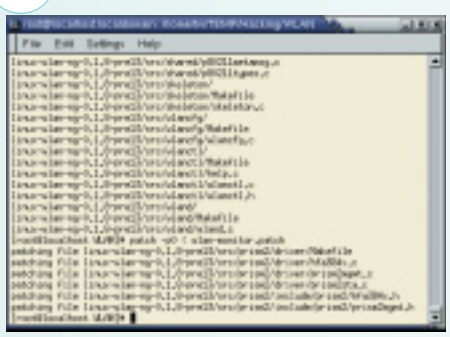
Ein breites Spektrum von WLAN-Produkten stellt der Hersteller Linksys vor. Mit dem Modell WPC11 erhalten Sie eine nach dem Standard 802.11b arbeitende 11-MBit/s-Steckkarte für den Einsatz im Notebook. Alternativ bietet Linksys mit dem WDT11 einen Adapter für die Karte zum Einbau in den PCI-Steckplatz an.

HACKER IN IHR FUNKNETZ EIN

Netze eindringen. Mit wenigen Schritten schützen Sie sich vor diesen Attacken.

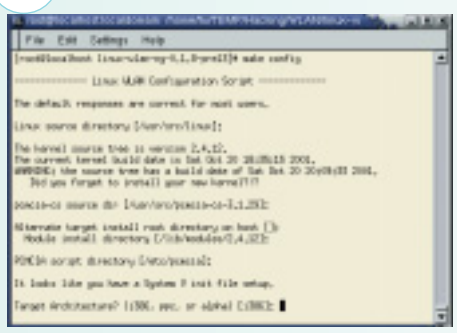
Das Protokoll führten Jörg Jokubeit und Hans Klumbies

5 So bereiten Sie das WLAN-Paket auf den Hack vor



Für den Wireless-LAN-Hack benötigen Sie das von Absolute Value Systems entwickelte Treiberpaket „linux-wlan-ng", das Sie auf unserer Heft-CD finden. Packen Sie dieses Paket mit dem Befehl „tar zxvf linux-wlan-ng-0.1.8-pre13.tar.gz" aus. Diese Treiber enthalten allerdings nicht die von uns benötigten Lauschfunktionen. Diese erhalten Sie, indem Sie einen speziellen Patch (ebenfalls auf der Heft-CD) ausführen. Das Kommando lautet: „patch -p0 < wlan-monitor.patch". Achtung: Der Patch arbeitet nur mit der Version 0.1.8-pre13 zusammen!

6 So erstellen Sie die WLAN-Kernel-Module



Wenn Sie den Patch erfolgreich ausgeführt haben, können Sie die Linux-WLAN-NG-Kernel-Module jetzt konfigurieren und installieren. Dazu wechseln Sie zunächst ins Verzeichnis linux-wlan-ng-0.1.8-pre13 und führen dort den Befehl „make config" aus. Im Regelfall erkennt das Programm alle notwendigen Pfade wie „/usr/src/linux" und „/usr/src/pcmcia-cs-3.1.29" vollautomatisch, sodass Sie alle Fragen mit der Eingabetaste bestätigen können. Anschließend führen Sie die Übersetzung der Kernel-Module mit „make all" aus. Abschließend installieren Sie die Module mit „make install".

7 So booten Sie Ihren Hacker-Kernel

Um Ihren neuen Hacker-Kernel erfolgreich zu starten, kopieren Sie zunächst den Kernel mit dem Befehl „cp /usr/src/linux/arch/i386/boot/bzImage /boot/wlan-hack". Anschließend passen Sie die Datei „/etc/lilo.conf" so an, dass ein eigener Eintrag für den Hacker-Kernel existiert. In unserem Beispiel sehen Sie drei Einträge: „linux" startet den regulären Linux-Kernel, „w2k" startet die Windows-2000-Partition und „wlan_crack" startet unseren eben konfigurierten Hacker-Kernel. Wichtig: Nachdem Sie Änderungen an „/etc/lilo.conf" durchgeführt haben, müssen Sie den Befehl „lilo -v" ausführen! Weitere Informationen zum Thema Kernel-Installation finden Sie in der Linux-Dokumentation.

Wer Funknetze abhört, kann mit bis zu zwei Jahren Gefängnis bestraft werden

1. Ist das Belauschen ungesicherter Funknetzwerke strafbar?
Ja. Das Abhören von Funknetzen, unabhängig davon, ob sie geschützt sind oder nicht, ist mit bis zu zwei Jahren Gefängnis oder Geldstrafe strafbar (§ 95, 86 Telekommunikationsgesetz).

2. Wie verhält es sich bei Funknetzwerken, die gegen Eindringen gesichert sind?
Neben der Strafbarkeit wegen Abhörens eines Funknetzwerks kommt hier auch eine Strafbarkeit wegen Ausspähens von Daten (§ 202a Strafgesetzbuch) in Betracht, was den Strafrahmen auf bis zu drei Jahre erhöht.

3. Was für eine Strafe steht auf das Speichern oder Beschädigen der Funknetz-Inhalte?
Der Täter kann in diesem Fall wegen Datenveränderung (§ 303a Strafgesetzbuch) verfolgt werden, was mit bis zu 2 Jahren Gefängnis oder Geldstrafe geahndet wird. Erheblich schärfere Strafen (5 Jahre) stehen auf Computersabotage (§ 303b StGB). Diese liegt unter anderem vor, wenn die Computeranlagen eines Betriebs durch die Störung des Funknetzwerks dauerhaft, jedenfalls aber längerfristig gestört oder beschädigt werden.

Der Münchner Rechtsanwalt Christian Czirnich beschäftigt sich seit 1994 mit den Themengebieten Computer-, Online-, Multimedia- und Urheberrecht und gilt als Experte auf diesen Bereichen.

Die Verschlüsselung im WEP basiert im Grunde auf zwei Werten: einem so genannten „Initialization Vector“ (IV) und einem Kennwort (KEY), das der Administrator bei der Einrichtung des Wireless LAN festlegt. Um sich erfolgreich ins WLAN einklicken zu können, muss jedem Client der KEY bekannt sein. Die Schwachstelle von WEP liegt in der Verknüpfung zwischen IV und KEY. Nimmt der IV einen bestimmten Wert an (Byte1: 03-07 oder 03-13, Byte2: 255, Byte3: egal), lässt sich auf mathematischem Weg der Wert eines Bytes des KEY bestimmen. Wenn einem Angreifer alle Werte des KEY bekannt sind, kann er einfach in das Wireless LAN eindringen. Dort kann er beliebige Daten ausspähen oder Ressourcen wie Server oder Internet-Verbindungen „gratis“ mitnutzen.

Die notwendigen Einbruchswerkzeuge sind kostenlos erhältlich: In unserem Feldversuch verwenden wir RedHat Linux 7.1, den neuesten Kernel 2.4.13 sowie die Zusatzpakete PCMCIA-CS und WLAN-NG für die Unterstützung von PCMCIA und den entsprechenden Wireless-Netzwerk-Karten. Prinzipiell funktioniert jede Wireless-LAN-Karte auf Basis des von der Firma Intersil entwickelten PRISM2-Chipsatzes.

Außerdem benötigen wir zum Hacken eines Wireless LANs das speziell dafür entwickelte Programm „AIRSNORT“ und einen speziellen Patch für WLAN-NG, mit dessen Hilfe sich Wireless-LAN-Verbindungen überhaupt erst belauschen lassen.

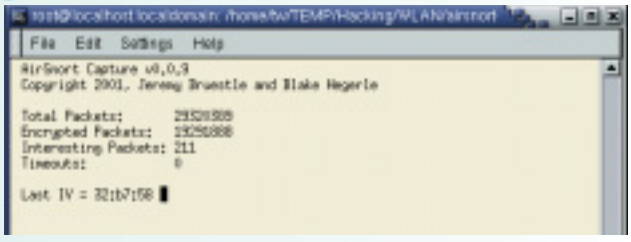
Im Gegensatz zu Windows eignet sich Linux hervorragend zum Hacken von Netzwerkverbindungen: Im Regelfall liegen die Treiber für alle Komponenten im Quellcode vor und lassen sich so leicht modifizieren. Bei Windows lässt sich ein vorhandener Treiber nicht einfach modifizieren, sondern müsste komplett neu entwickelt werden – keine spaßige Aufgabe!

Fazit: Der finanzielle Aufwand zum Knacken eines durch WEP geschützten WLANs ist äußerst gering: Sie benötigen lediglich eine Wireless-LAN-Karte zum Preis von 250 bis 400 Mark für das Notebook, das Betriebssystem Linux, die passende Software und entsprechende Treiber.

8 So konfigurieren Sie das Hack-Tool

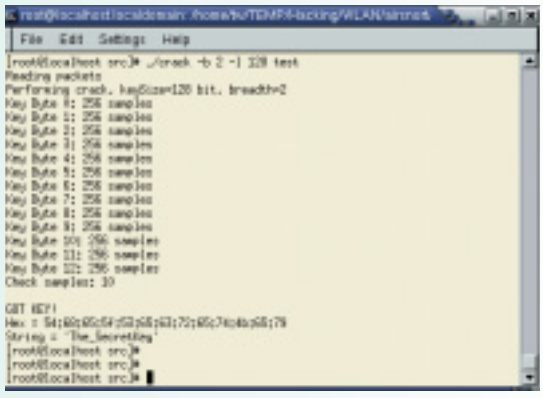
Zunächst entpacken Sie das Tool mit dem Befehl „tar xzvof airsnort-0.1.0.tar.gz“ und wechseln in das neu entstandene Verzeichnis „airsnort-0.1.0“. Dort wechseln Sie mit dem Befehl „cd src“ in das Verzeichnis mit dem C-Quellcode des Tools und übersetzen alle notwendigen Hacktools mit dem Kommando „make“.

9 So belauschen Sie das WLAN



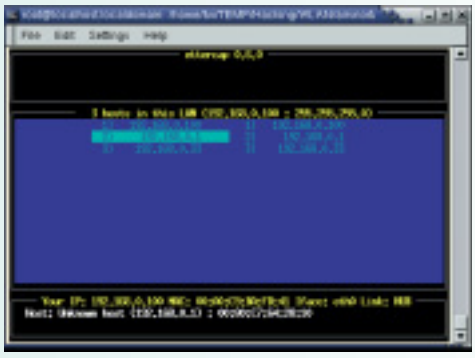
Zunächst bearbeiten Sie die Datei „dopromisc.sh“ im Unterverzeichnis „scripts“ Ihres Hacktools und legen dort den gewünschten Kanal fest. In den meisten Fällen wird Kanal „7“ verwendet. Den eigentlichen Mitschnitt der verschlüsselten Pakete starten Sie mit dem Befehl „./capture -c DATAFILE“ im Verzeichnis „src“.

10 So starten Sie den WLAN-Zugriff



Wenn Sie zwischen 80 und 100 „Interesting packets“ gesammelt haben, können Sie einen Hackversuch wagen. Brechen Sie mit „CTRL-C“ das Capture-Tool ab und rufen Sie folgenden Befehl auf: „./crack DATAFILE“. Wenn das Programm meldet „GOT KEY!“, gehört das Kennwort – und damit der Zugriff auf das WLAN – Ihnen.

11 So hören Sie den Datenverkehr ab



Anschließend konfigurieren Sie Ihr System einfach für den Zugriff aufs WLAN. Da Sie das Kennwort kennen, ist das kein Problem. Schnüffeln können Sie mit gängigen Programmen wie „Ettercap“ (Linux) oder „Ethereal“ (Windows und Linux), die es kostenfrei im Internet gibt.

So schützen Sie Ihr Funknetzwerk

Sicherheitslöcher im WLAN sind oft das Ergebnis falscher Konfiguration.

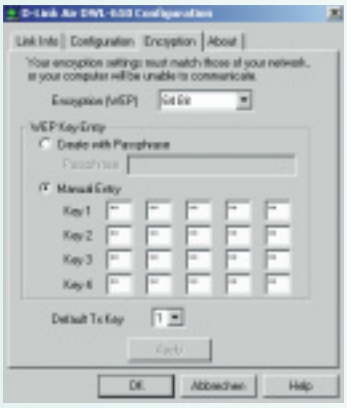
Das Protokoll führten Jörg Jokubeit und Hans Klumbies

Windows, Notebook und Wireless LAN liegen voll im Trend: Was ist cooler, als eine Präsentation, die zentral auf dem Abteilungsserver gespeichert ist, im Konferenzraum vorzutragen; ganz ohne Kabelgewirr und Konfigurationsaufwand. Oder E-Mails vom Server abrufen, während man die Kollegen im Nebenzimmer für ein kleines Schwätzchen besucht? Dieser Hauch von Luxus und Unabhängigkeit macht Wireless LANs immer beliebter. Hersteller wie Dell oder Compaq bieten mittlerweile für ihre Notebooks bereits Wireless-LAN-Komponenten als Quasistandard für Unternehmen an.

Allerdings birgt diese Dreiecks-Beziehung auch Gefahren: Den meisten Windows-Administratoren fehlt – im Gegensatz zu ihren Unix-Kollegen – leider immer noch der notwendige Bezug zum Thema Sicherheit. Das zeigte der Test unserer Rundreise durch München: 13 von 20 WLANs waren komplett unverschlüsselt und ungeschützt. Diese Schlamperei lässt sich nicht entschuldigen – auch nicht durch die Existenz von Werkzeugen wie „AIRSNORT“ und Aussagen wie „das kann man doch eh knacken“. Wer einen guten KEY wählt und diesen regelmäßig wechselt, erschwert dem Angreifer das Leben deutlich. Zusätzlich lassen sich weitere Sicherheitsmaßnahmen einsetzen, die unabhängig von WEP für eine Verschlüsselung sensibler Daten sorgen. Eine kleine Auswahl finden Sie rechts.

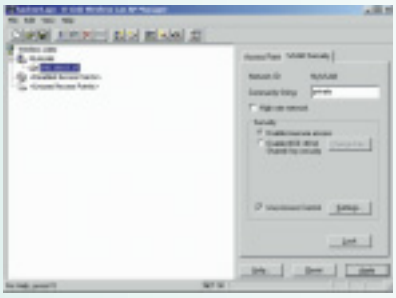
Fazit: Seien Sie ein Pessimist! Stellen Sie sich – trotz WEP – vor, dass alle Daten in Ihrem Wireless LAN von jedem beliebigen Hacker mitgelesen werden können. Untersuchen Sie sorgfältig, welche Dienste in Ihrem WLAN zum Einsatz kommen, und sehen Sie sich nach geeigneten Schutzmaßnahmen (IPSEC, SSH, SSL, etc.) um. Wenn kritische Daten im WLAN transportiert werden müssen, holen Sie sich auf *JEDEN* Fall professionelle Hilfe in Form eines Sicherheitsberaters.

1 So legen Sie ein WLAN-Kennwort fest



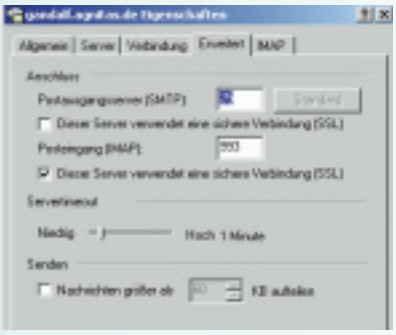
Über ein mitgeliefertes Tool legen Sie das Kennwort Ihres Wireless-LAN-Netzwerks fest. Am Beispiel des Konfigurationstools der D-Link DWL-650 sehen Sie, dass sich Kennwörter im Klartext oder als Hexcode-Zeichenfolge festlegen lassen.

2 So schützen Sie sich vor fremden Daten



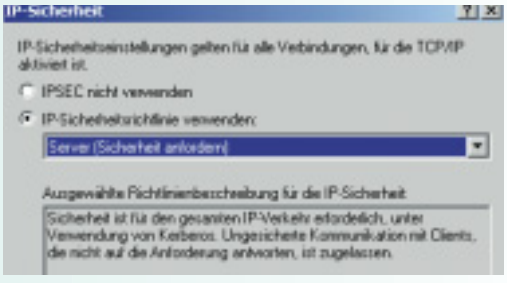
Der Access-Point DWL-1000AP von D-Link bietet einen Zugriffsschutz auf Basis der MAC-Adresse einer Wireless-LAN-Karte. Damit können Ihrem Wireless LAN zwar keine „fremden“ Datenpakete untergejubelt werden; mitlesen kann der Hacker allerdings immer noch. Wie Sie auch das verhindern, lesen Sie im Anschluss.

3 So stoppen Sie den Zutritt von Spionen



Viele Freemail-Dienste im Internet und alle kommerziellen Mailserver erlauben die Verschlüsselung von Benutzerkennwort und den übertragenen Maildaten. Aktivieren Sie diese Option im Menü „Konten/Eigenschaften/Erweitert“ (Outlook 2000), indem Sie das entsprechende Feld „Dieser Server verwendet eine sichere Verbindung (SSL)“ aktivieren.

4 So verschlüsseln Sie IP-Verbindungen



Wenn Sie wirklich kritische Informationen über Ihr Wireless LAN schicken, verwenden Sie *AUF JEDEN FALL* das Protokoll IPSEC. IPSEC ist in neueren Windows-Versionen, beispielsweise Windows 2000 Professionell, serienmäßig und kostenfrei vorhanden. Um die Einstellungen anzupassen, rufen Sie die erweiterten Eigenschaften des TCP/IP-Protokolls Ihrer Netzwerkkarte auf.

SSH
Secure Shell 3.0.1

SSH, Online-Shop
nur via Internet
www.ssh.com

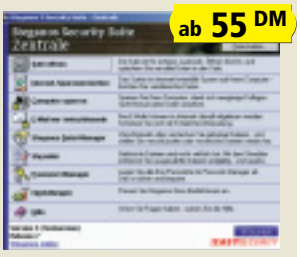
99 USD

Verzichten Sie besser auf die unverschlüsselte Datenübertragung à la Telnet und Co: Mit der Secure Shell von SSH erhalten Sie ein kommerzielles und sicheres Programm zur Kommunikation mit entfernten Servern. Das Programm arbeitet nach aktuellen Sicherheitsstandards wie AES.

Steganos
Security Suite 3

Steganos
(0800) 78 34 26 67
www.steganos.com

ab 55 DM



Mit der Steganos Security Suite 3 können Sie Daten auf sehr effektive Art und Weise verschlüsseln – Informationen lassen sich beispielsweise in Grafik- und Sounddateien verstecken. Die aktuelle Version 3 unterstützt neueste Verschlüsselungsverfahren, wie z.B. AES (128 Bit).

OpenBSD Org
OpenBSD 2.9

Lehmanns
(030) 61 79 110
www.lehmanns.de

79,95 DM

Ein Geheimtipp für Security-Profis ist OpenBSD. Das freie Betriebssystem eignet sich hervorragend zum Bau von sicherheitsrelevanten Serverlösungen; beispielsweise als Firewall oder Router mit VPN-Funktionalität (Virtual Private Network).
Im Internet ist OpenBSD unter www.openbsd.org frei verfügbar.