



tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

€ 10,90 Österreich € 12,00 Benelux € 12,55 Schweiz SFR 21,80

IT-**Un**Sicherheit

Hacker-Tools für sichere PCs & Netze einsetzen

140 Seiten Praxis

- Schwachstellen im WLAN
- Netzwerk-Überwachung
- Sniffing mit Ethereal
- Fehlersuche im LAN
- Rootkit-Detection
- Illegale Sniffer finden
- Patch-Management
- LDAP richtig einsetzen
- Netzwerk-Check für VoIP



Die CD enthält keine Jugend freigegebenen Inhalte.

Boot-CD mit Betriebssystem:

- Daten retten mit der Live-CD
- Perfekte Netzwerk-Einbindung
- Leistungsfähige Admin-Tools für Linux & Windows
- Software zu den Workshops: Ethereal, Snort, Aircrack, Nessus uvm.



Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
 Chef vom Dienst / Textchef: Kerstin Möller
 Grafik: stroemung, Michael Oliver Rupp, Yvonne Reitinger, Bernd Maier-Leppla
 Titelgestaltung: Twentyfirst Communications

Redaktion tecCHANNEL:

Lyonel-Feininger-Straße 26, 80807 München,
 Tel.: 0 89/3 60 86-897, Fax: -878
 Homepage: www.tecChannel.de,
 E-Mail: redtechannel@idginteractive.de

Autoren dieser Ausgabe: Jürgen Donauer, Mike Hartmann, Moritz Jäger, Stefan Rubner, Ralf Spenneberg, Roland Stooss, Thomas Wölfer
 Schlussredaktion: Claudia Feige

Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IDG Interactive GmbH. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, vor allem durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags nicht zulässig.

Anzeigen:

Anzeigenleitung: Dirk Limburg,
 Tel.: 0 89/3 60 86-871
 Leitung Anzeigendisposition: Rudolf Schuster,
 Tel.: 0 89/3 60 86-135, Fax: -99135
 Digitale Anzeigenannahme: Manfred Aumaier,
 Tel.: 0 89/3 60 86-602, Andreas Mallin,
 Tel.: 0 89/3 60 86-603, ISDN: 0 89/20 80 70
 und 0 89/3 60 86-493

Vertrieb / Produktion:

Vertrieb: Josef Kreitmayr (leitend), Katrin Elser
 Vertriebsmarketing: Peter Prieuwasser (leitend),
 Stefanie Kusseler

Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb, Breslauer Straße 5, 85386 Eching, Tel.: 0 89/3 19 06-0, Fax: -113, E-Mail: mzv@mzv.de, Website: www.mzv.de

Produktionsleitung: Heinz Zimmermann

Druck: Schoder Druck, Gutenbergstraße 12, 86368 Gersthofen

Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in tecCHANNEL-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Interactive GmbH ist die IDG Communications Verlag AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA

Verlag: IDG Interactive GmbH, Lyonel-Feininger-Straße 26, 80807 München, Tel.: 0 89/3 60 86-0, Fax: -118, Website: www.idg-verlag.de

Handelsregisternummer: HR 127140

Umsatzidentifikationsnummer: DE 203 066

Geschäftsführer: York von Heimburg

Group Publisher: Stephan Scherzer

Verlagsleitung: Frank Klinkenberg

Vorstand: York von Heimburg, Keith Arnot, Pat Kenealy

Mitglieder der Konzerngeschäftsführung:

Karin Giffhorn, Stephan Scherzer, Josef Lohner

Aufsichtsratsvorsitzender:

Patrick J. McGovern

Dieses tecCHANNEL-Compact wurde mit der Adobe Creative Suite CS produziert. tecCHANNEL-Compact erscheint im Verlag der PC-WELT. Zu unserer Verlagsgruppe gehören folgende Zeitschriften:

COMPUTERWOCHE
Macwelt

ComputerPartner
GameStar

PCWELT
CIO

DigitalWorld
gamepro

Leser- und Abo-Service:

Dialog-Service-Center GmbH, Konrad-Zuse-Straße 16, 74172 Neckarsulm, Telefon: 0 18 05/9 99-802, Fax: 0 71 32/9 59-166, E-Mail: tecchannel@d-s-center.de

Inhalt

	Editorial	4
	Impressum	5
1.	Installation	11
1.1	WHAX installieren	11
1.1.1	Partitionierung	12
1.1.2	Installation	13
1.1.3	Fazit	15
1.2	Die Windows-Tools auf CD	16
	WinPcap 3.0	16
	AirSnare 0.8	16
	Ethereal 0.10.12	17
	WinSnort 2.3.3 Build 14	18
	IDS Policy Manager 1.7.0	19
	RAT 4.2.6	20
	RTP Monitor 1.0	20
1.3	Tools auf der WHAX-CD	22
1.3.1	rdesktop	22
1.3.2	LDAP-Browser	23
1.3.3	Die GUI für SSH-Verbindungen – KSSH	24
1.3.4	NTFS-Partitionen mit Schreibzugriff mittels Captive mounten	25
1.3.5	Multifunktions-Netzwerk-Tool NetWag	26
1.3.6	Sicherheitscheck mit fuzzer.py	28
1.3.7	Der Sniffer Etherape	28
1.3.8	Xtraceroute und traceroute	29
1.3.9	Default Passwords	30
1.3.10	Fazit	31
2.	Diagnose	32
2.1	Netzwerküberwachung mit Snort	32
2.1.1	Einrichtung von Snort unter WHAX	32
	CD-Inhalt	34
2.1.2	Windows-Sensor	36
2.1.3	Ausgabe der Ergebnisse	36
2.1.4	IDS Policy Manager	38
2.1.5	Policy erstellen	40

2.1.6	Einschränkungen	41
2.1.7	Ausblick	42
2.2	Illegale WLAN-Zugangspunkte aufspüren	43
2.2.1	Netstumbler	44
2.2.2	Scripts und GPS	45
2.2.3	Ministumbler	46
2.2.4	Airsnare	46
2.2.5	AirMail und AirHorn	48
2.2.6	Fazit	49
2.3	Sniffing mit Ethereal	50
2.3.1	Sniffing-Grundlagen	50
2.3.2	Sniffing-Tools	51
2.3.3	Erste Schritte mit Ethereal	52
2.3.4	Erstes Capture	53
2.3.5	Filtern nach Kriterien	56
2.3.6	E-Mail überwacht	57
2.3.7	Sniffing im Netzwerk	58
2.3.8	Sniffing im geschwitzen LAN	59
2.3.9	Sniffing im WLAN	60
2.3.10	Lokale Angriffe von Sniffern	61
2.3.11	Entdecken von Sniffern	61
2.3.12	Fazit	62
2.4	Rootkit-Detection	63
2.4.1	Überprüfen der offenen Ports	63
2.4.2	Grafisches Frontend zu nmap	64
2.4.3	Der Portscanner amap	65
2.4.4	Das Programm netstat	66
2.4.5	Rootkit-Hunter chkrootkit	67
2.4.6	Fazit	68
2.5	Webanalyse	69
2.5.1	Der Linkchecker KLinkStatus	69
2.5.2	Das Tool list-urls	70
2.5.3	Kommandozeilen-Tool LinkChecker	71
2.5.4	Fazit	75
2.6	VoIP-Analyse mit Bordmitteln	77
2.6.1	Delay/Jitter	77
2.6.2	Paketverlust	78
2.6.3	Messungen	78
2.6.4	RTP-Messungen	80
2.6.5	Ausblick	83

3.	Sicherheits-Check	84
3.1	Passwort-Sicherheit	84
3.1.1	Password-Dictionaries optimieren	84
3.2	Vulnerability-Scanner Nessus	90
3.2.1	Nessus – vorbereitende Schritte	90
3.2.2	Nessus – Client GUI	91
3.2.3	Fazit	95
3.3	Sicherheitsrisiko WEP	96
3.3.1	Angriffsziel Initialisierungsvektor	97
3.3.2	Chopper – das Ende von WEP	97
3.3.3	Airodump – der Paketsammler	98
3.3.4	Aireplay – mehr Pakete, mehr IVs	99
3.3.5	Aircrack – knackt jeden WEP-Key	100
3.3.6	Alternative WPA?	101
3.3.7	Fazit	101
4.	Erste Hilfe	103
4.1	Datensicherung von Windows-Rechnern	103
4.1.1	Sicherung mittels SCP (Secure Copy)	104
4.1.2	Sicherung auf einen Samba- oder Windows-Server	105
4.1.3	Grafisches Mouneten mit Smb4K	106
4.1.4	Manuelles Mouneten auf Commandline	107
4.1.5	Fazit	108
4.2	K3b: Linux brennt!	109
4.2.1	Erste Schritte	110
4.2.2	Der Brennvorgang	111
4.2.3	Fazit	113
4.3	Viren scannen mit Linux	115
4.3.1	Das Antivirenpaket – clamav	115
4.3.2	eEYE-Scanner	118
4.3.3	Fazit	119
4.4	LAN-Analyse mit Bordmitteln	120
4.4.1	ping	120
4.4.2	route und tracert/traceroute	121
4.4.3	pathping und mtr	123
4.4.4	arp und ipconfig/ifconfig	124
4.4.5	netdiag und netstat	125
4.4.6	nslookup und nbtstat	126
4.4.7	Netzwerkanalyse mit Windows XP	126

5.4	Professionelle Datenrettung	163
5.4.1	Ausfallursachen	163
5.4.2	Defekte bei Festplatten	164
5.4.3	Mechanikschäden bei Festplatten	165
5.4.4	Headcrash bei Festplatten	166
5.4.5	Headcrash durch Überhitzung	166
5.4.6	Kühlung verhindert Headcrash	166
5.4.7	Kosten durch verlorene Daten	167
5.4.8	Richtiges Verhalten bei Defekt	169
5.4.9	Wichtige Informationen bei Notfall	169
5.4.10	Rettbare Medien und Dateisysteme	170
5.4.11	Grenzen der Datenrettung	170
5.4.12	Datenfeind Hitze	171
5.4.13	Datenrettungslabore	171
5.4.14	Datenrettungslabor: Lager und Speicher	172
5.4.15	Phase I: Analyse	172
5.4.16	Phase II: physikalische Rettung	173
5.4.17	Phase III: Pattern-Analyser	173
5.4.18	Phase IV: logische Rettung	174
5.4.19	Datenretter im Überblick	175
5.4.20	Kosten: Analyse und Rettung	180
5.4.21	Fazit	181
5.5	Das Linux-Verzeichnis	182
5.5.1	Einsatzgebiete von LDAP	182
5.5.2	OpenLDAP-Installation	183
5.5.3	Erste Einstellungen	183
5.5.4	Das Verzeichnis füllen	185
5.5.5	LDAP-Daten abfragen	187
5.5.6	LDAP-Zugriff mit Evolution	188
5.5.7	LDAP-Fähigkeiten erweitern	189
5.5.8	Den Zugriff regeln	191
	Glossar	192
	Index	197
	tecCHANNEL-Leserumfrage – Mitmachen und gewinnen!	200