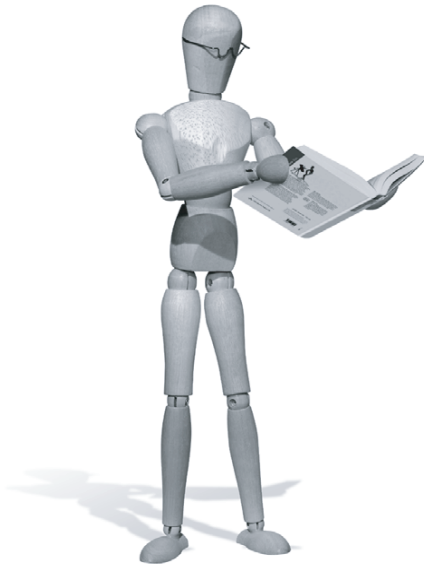


Ralf Spenneberg

Intrusion Detection und Prevention mit Snort 2 & Co.

Einbrüche auf Linux-Servern erkennen und verhindern



 ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Inhaltsverzeichnis

Vorwort zur zweiten Auflage	25
Einleitung	27
Teil I Einführung in die Intrusion Detection	33
1 Was ist eine Intrusion, was ist Intrusion Detection?	35
1.1 Was ist eine Intrusion?	35
1.2 Was macht die Intrusion Detection?	38
1.2.1 Angriffs-/Einbruchserkennung	38
1.2.2 Missbrauchserkennung	39
1.2.3 Anomalie-Erkennung	39
1.3 Was macht die Intrusion Prevention?	39
2 Benötige ich ein IDS oder ein IPS und eine Firewall?	41
2.1 Einordnung der IDS und IPS in eine Sicherheitsstrategie	41
2.2 Welchen Schutz bietet eine Firewall?	41
2.2.1 Was ist eine Firewall?	41
2.3 Welchen Schutz bietet darüber hinaus ein IDS?	46
2.3.1 Host Intrusion Detection System	47
2.3.2 Network-Intrusion-Detection-System	50
2.4 Welchen Schutz bietet darüber hinaus ein IPS?	53
2.4.1 Host Intrusion Prevention System	53
2.4.2 Network Intrusion Prevention System	53
2.4.3 Vor- und Nachteile eines IPS	54
3 Was kann/soll ein IDS leisten?	55
3.1 Anforderungen an ein Intrusion-Detection-System	55
3.2 Anforderungen an ein Intrusion Prevention System	57
3.3 Gebotene Leistung (Wirklichkeit)	57
3.4 Aufwand und Kosten	60
3.5 Kommerzielle und freie IDS	64

3.5.1	NetRanger/Cisco Secure IDS	65
3.5.2	RealSecure	65
3.5.3	Netscreen	66
3.5.4	Snort	67
3.5.5	Network Flight Recorder NID	68
3.5.6	Dragon	68
3.5.7	Prelude	69
3.5.8	Samhain	70
3.5.9	Entercept.	70
3.5.10	NFR HID.	71
3.5.11	LIDS	71
3.5.12	Tripwire.	72
4	Rechtliche Fragestellungen beim Einsatz eines IDS	73
4.1	Welche Gesetze sind anwendbar?	73
4.1.1	Datenschutz und IDS	73
4.1.2	Verwertbarkeit vor Gericht	75
4.1.3	Allgemeiner Hinweis	76
5	Vorbereitung auf den Ernstfall.	77
5.1	Notfallteam: Computer Emergency Response Team	77
5.2	Notfallplan	79
5.3	Entwicklung der Sicherheitsrichtlinie	80
5.3.1	E-Mail-Sicherheitsrichtlinie	81
5.3.2	Acceptable Use	82
6	IDS im Einsatz.	85
6.1	Prävention.	85
6.2	Einbruch	87
6.3	Erkennung.	87
6.4	Reaktion	88
6.5	Analyse.	89
6.6	Recovery.	90
6.7	Konsequenzen.	91

Teil II	Verfügbare Open-Source-Intrusion-Detection-Systeme	93
7	Intrusion Detection selfmade	95
7.1	Ausnutzen der Protokollfunktionen allgemeiner Dienste	95
7.1.1	Konfiguration des DNS-Nameservers Bind 9	96
7.1.2	Definition eines dDoS-Schwellwertes mit iptables	97
7.2	Einfache lokale IDS	99
7.3	Einfache netzwerkbasierte IDS	101
7.3.1	Tcpdump	102
7.4	ngrep	108
8	Hostbasierte Intrusion-Detection-Systeme	111
8.1	Automatische Protokollanalyse	112
8.1.1	Logsurfer	112
8.1.2	Fwlogwatch	121
8.1.3	Logwatch	130
8.1.4	Logcheck (auch LogSentry)	134
8.2	Tiger	135
8.2.1	Einführung	135
8.2.2	Geschichte	136
8.2.3	Tiger-Installation	136
8.2.4	Audit-Werkzeug	137
8.2.5	Tiger als IDS	143
8.2.6	Tiger-Erweiterungen	144
8.3	Tripwire	147
8.3.1	Einführung	147
8.3.2	Geschichte	148
8.3.3	Lizenz	149
8.3.4	Aufbau	149
8.3.5	Installation	150
8.3.6	Vor der ersten Verwendung	151
8.3.7	Erzeugung der Datenbank	157
8.3.8	Überprüfung der Datenbank	159
8.3.9	Aktualisierung der Datenbank	165
8.3.10	Aktualisierung der Richtlinien	166
8.3.11	Weitere Administration	168
8.3.12	Anpassung der Konfiguration und der Richtlinien	173

8.3.13	Optimierung der Regeln	183
8.3.14	Zusammenfassung	187
8.4	Samhain und Beltane	187
8.4.1	Einführung	187
8.4.2	Stand-alone-Installation und -Konfiguration	188
8.4.3	Samhain als Client/Server	212
8.4.4	Zentrale Überwachung mit Beltane	218
8.5	SNARE	226
8.5.1	SNARE-Installation.	227
8.5.2	SNARE-Konfiguration	227
8.5.3	SNARE im Einsatz	232
9	Netzwerkbasierte Intrusion-Detection-Systeme	235
9.1	Aufgaben eines NIDS	235
9.1.1	Einfache Paketanalyse	236
9.1.2	Defragmentierung	237
9.1.3	TCP-Streamreassemblierung	238
9.1.4	Dekodierung des Applikationsprotokolls	238
9.1.5	Anomalie-Erkennung	239
9.1.6	Critical Path	239
9.2	Snort	239
9.2.1	Einführung	239
9.2.2	Geschichte	240
9.2.3	Lizenz	240
9.2.4	Funktionen von Snort.	240
9.2.5	Installation.	244
9.2.6	libpcap-Bibliothek mit Ringpuffer	246
9.2.7	Erste Anwendung	247
9.2.8	Erzeugung der Regeln	261
9.2.9	Fortgeschrittene Regeln	292
9.2.10	Fortgeschrittene Protokollierung	326
9.2.11	Snort-Wireless	371
9.2.12	Konfigurationswerkzeuge für Snort	375
9.3	ARPPwatch	376

10	Hybrid-Intrusion-Detection-Systeme	379
10.1	Prelude-Einführung	379
10.2	Prelude-Installation	384
10.3	Prelude-Konfiguration	386
10.4	Einbindung externer Sensoren	408
10.4.1	Snort	408
10.4.2	Samhain	412
10.4.3	Libsafe	412
10.4.4	Systrace	414
10.4.5	Honeyd	416
10.4.6	Nessus	416
10.5	Fortgeschrittene Prelude-Konfiguration.	416
10.5.1	LML-Regeln	416
10.5.2	Relaying, Replikation und Hochverfügbarkeit	417
Teil III	Verfügbare Open-Source-Intrusion-Prevention-Systeme.	419
11	Linux-Intrusion-Detection-System – LIDS.	421
11.1	Einführung	421
11.2	Geschichte	422
11.3	Lizenz	423
11.4	Installation	423
11.4.1	Kernel 2.4	423
11.4.2	Kernel 2.6	426
11.5	LIDS-Hintergründe	427
11.6	Konfiguration	430
11.6.1	Kommandozeilenwerkzeuge	430
11.6.2	LIDS 1.x.x Konfigurationsdateien	433
11.6.3	LIDS 2.x.x Konfigurationsdateien	436
11.6.4	Regelsyntax und Beispiele	438
11.6.5	Grundregeln für jeden Rechner.	442
11.7	Welche Rechner sollen mit LIDS geschützt werden?	444
11.7.1	Webserver	444
11.7.2	DNS-Server	445

11.7.3	Proxy-Server.	445
11.7.4	Firewall/Snort-Sensor	446
11.8	LIDS-Protokollierung durch LIDS.	447
11.9	LIDS und Netfilter	448
11.10	Wurmbekämpfung mit LIDS	449
11.11	LIDS Learning-Mode/ACL-Discovery	450
11.12	LIDS Trusted Path Execution.	451
11.13	LIDS Trusted Domain Enforcement	452
11.13.1	TDE-Richtlinie	452
11.13.2	TDE-Sandbox	452
11.14	LIDS-Zusammenfassung.	452
12	Systrace	455
12.1	Einführung	455
12.2	Installation von Systrace	456
12.3	Systrace Anwendung	458
12.4	Systrace-Beispiel	461
13	Snort-Inline	465
13.1	Einführung	465
13.2	Installation von Snort-Inline	466
13.3	Anpassung der Snort-Regeln	468
13.3.1	Paketmodifikation	468
13.3.2	TCP-Zustandsüberwachung	469
13.3.3	Automatische Anpassung der Regeln.	470
13.4	Clamav	470
13.5	Einbindung als IPS mit iptables.	472
Teil IV	Einsatz in einem Unternehmensnetzwerk.	475
14	Tripwire im Unternehmensnetzwerk	477
14.1	Zentrale Erzeugung der Konfigurationsdateien	477
14.1.1	twcfg.txt	478
14.1.2	twpol.txt	478

14.2	Zentrale Verwaltung der Schlüssel	485
14.3	Distribution der Dateien mit rsync	486
14.4	Erzeugung und Überprüfung der Datenbanken mit ssh	490
14.5	Zentrale Auswertung	492
14.6	Zusammenfassung.	494
15	Aufbau eines Netzes aus Snort-Sensoren.	495
15.1	Auswahl der Sensor-Standorte	495
15.2	Installation der Sensoren	496
15.2.1	Hardware.	497
15.2.2	Software-Installation	499
15.2.3	Konfiguration der Sensoren.	501
15.2.4	Start von Snort und Barnyard	510
15.3	Installation der Managementkonsole	510
15.3.1	Analysis Console for Intrusion Detection (ACID).	510
15.3.2	Zentrale Sammlung der Daten in Datenbanken	519
15.4	Snort-Center	526
15.4.1	Installation von Snort-Center	527
15.4.2	Konfiguration von Snort-Center	528
15.4.3	Installation des Snort-Center Agents	530
15.4.4	ACID-Plug-In.	533
15.5	Korrelation und Analyse der Daten	535
15.5.1	Verwaltung der Meldungen	537
15.5.2	Suchfunktionen	538
15.5.3	Paketbetrachter	541
15.5.4	Erzeugung von Grafiken	542
15.5.5	Fazit	544
15.6	Snort-Analyse mit Sguil	544
15.6.1	Sguil-Installation.	544
15.6.2	Sguil-Start	553
15.6.3	Sguil-Anwendung	554
15.6.4	Fazit	558
16	Zentrale Protokollserver	559
16.1	Einrichtung der zentralen Protokollierung unter Linux	560

16.2	Modular Syslog	563
16.2.1	Installation von msyslogd	564
16.2.2	Konfiguration von msyslogd	565
16.3	Zeitsynchronisation	572
16.3.1	Erste Synchronisation	573
16.3.2	Konfiguration und Einsatz	573
16.3.3	Sicherheit von ntpd	574
17	Datenschutz-Aspekte in einem Unternehmensnetzwerk	577
17.1	IDS im Unternehmen	577
17.2	Benutzerordnungen	579
Teil V	Incident Response – Reaktion und Wiederherstellung	583
18	Reaktion auf den Einbruch.	585
18.1	Do not Panic!	585
18.2	Meldung des Einbruchs	586
18.2.1	Adressenlisten und URLs	589
18.3	Aufsuchen professioneller Hilfe	592
18.4	Neuinstallation oder Reparatur.	593
19	Lessons Learned	595
19.1	Anpassen der Maßnahmen.	595
19.2	Weiterbildung	597
Teil VI	Fortgeschrittene Analyse.	601
20	Analyse des Rechners nach einem Einbruch.	603
20.1	Forensische Analyse eines Rechners.	604
20.2	Dokumentation der Analyse	605
20.3	Analyse flüchtiger Daten	607
20.3.1	Zeitsynchronisation	608
20.3.2	Kernel-Mitteilungen, Module und Arbeitsspeicher	608
20.3.3	Prozessanalyse	609
20.3.4	Analyse der Netzwerkkonfiguration.	609

- 20.3.5 Offene Dateien 611
- 20.3.6 Analyse des Kernels auf ein kernelbasiertes Rootkit 611
- 20.4 Analyse der Dateisysteme 616
 - 20.4.1 Sicherung der Dateisysteme 616
 - 20.4.2 Analyse einzelner Dateien 619
 - 20.4.3 Analyse der Dateisysteme mit RPM 620
 - 20.4.4 Analyse der Dateisysteme mit ChkRootKit 622
- 20.5 Analyse des Rechners mit The Coroner's Toolkit 628
 - 20.5.1 Installation und Konfiguration von TCT 629
 - 20.5.2 Leichenfledderei: grave-robber 630
 - 20.5.3 Erzeugen eines Logbuches: mactime 633
 - 20.5.4 Auferwecken der Toten: unrm und lazarus 636
 - 20.5.5 TCTs kleine Helfer: ils und icat 638
- 20.6 Sleuthkit und Autopsy 642
 - 20.6.1 Hash-Datenbanken 653
- 20.7 Analyse mit Foremost 654
- 20.8 Analyse modifizierter Dateien und Befehle 655
- 20.9 Fazit 658
- 21 Analyse von Netzwerkdaten 659**
 - 21.1 Analyse der Paket-Header: SYN/FIN, ACK, und FIN Scan 659
 - 21.1.1 SYN/FIN Scan 660
 - 21.1.2 ACK Scan 662
 - 21.1.3 FIN Scan 663
 - 21.2 Analyse des Paketinhaltes 664
 - 21.2.1 Beispiel: verdächtige ICMP-Pakete 664
 - 21.2.2 Fragmentiertes Paket 667
 - 21.3 Auffinden der Nadel im Heuhaufen 670
 - 21.3.1 Ethereal 670
 - 21.3.2 TCPshow 671
 - 21.3.3 TCPflow 672
 - 21.3.4 TCPtrace 673
 - 21.3.5 Traffic-Vis 674
 - 21.4 TCP-Streamreassemblierungsangriff 675

Teil VII	Honeypot	679
22	Einsatz eines Honeypots	681
22.1	Was ist ein Honeypot? Sinn und Unsinn	681
22.2	Honeypot-Varianten	684
22.3	Honeypots und das Gesetz	686
23	Tiny Honeypot und Honeyd	689
23.1	Tiny Honeypot	689
23.2	Honeyd	693
24	Aufbau und Konfiguration eines »echten« Honeypots	699
24.1	Auswahl und Installation des Betriebssystems	699
24.2	Verwendung von UserModeLinux oder VMware als virtueller Rechner	700
24.2.1	Installation und Konfiguration von VMware	701
24.2.2	Installation und Konfiguration von UserModeLinux	706
24.3	Konfiguration der Netzwerkdienste	709
24.4	Zugang zum Honeypot und Schutz weiterer Systeme vor dem Honeypot	710
24.4.1	Routing des Honeypots	711
24.4.2	NAT (Network Address Translation) des Honeypots	713
24.4.3	Weiter gehende Firewall-Konfiguration	715
24.5	Überwachung des Honeypots von außen	717
24.6	Fazit	720
Anhang	723
A	Netzwerkgrundlagen	725
A.1	TCP/IP	725
A.2	IP	725
A.2.1	Version	727
A.2.2	Header-Länge	727
A.2.3	Type of Service	727
A.2.4	Gesamtpaketlänge	727
A.2.5	Identifikationsnummer	727
A.2.6	Flaggen	728

A.2.7	Fragment-Offset	728
A.2.8	Time To Live (TTL)	729
A.2.9	Protokoll	729
A.2.10	Prüfsumme	729
A.2.11	Quell-IP-Adresse	730
A.2.12	Ziel-IP-Adresse	730
A.2.13	IP-Optionen	730
A.3	UDP	732
A.4	TCP	734
A.4.1	Auf- und Abbau einer TCP-Verbindung	735
A.4.2	TCP-Header	736
A.4.3	Fortgeschrittene Eigenschaften von TCP	742
A.5	Explicit Congestion Notification	744
A.6	ICMP	746
A.6.1	Destination Unreachable	748
A.6.2	Source Quench	749
A.6.3	Time Exceeded	749
A.6.4	Redirect	750
A.6.5	Parameter Problem	750
A.6.6	Echo-Request und Reply	750
A.6.7	Address Mask Request und Reply	751
A.6.8	Timestamp Request und Reply	751
A.6.9	Router Solicitation und Advertisement	752
A.7	ARP	752
B	Typische Netzwerkangriffe	755
B.1	Firewalking	755
B.2	SYN-Flood	756
B.3	Spoofing	757
B.3.1	IP-Spoofing	757
B.3.2	ARP-Spoofing	758
B.3.3	DNS-Spoofing	759
B.4	Mitnick-Angriff	761
B.5	Session Hijacking	762
B.6	Gespoofter Portscan	763

C	Rootkits	765
	C.1 Normale Rootkits	765
	C.2 Kernelbasierte modulare Rootkits	767
	C.3 Kernel-Intrusion-System (KIS)	770
D	Kryptografie	773
	D.1 Geschichte	773
	D.2 Anwendungen	774
	D.3 Funktionsweise	775
	D.3.1 Schlüsselbasierte Verfahren	775
	D.4 Symmetrische Kryptografie	776
	D.5 Asymmetrische Kryptografie	776
	D.6 Diffie-Hellmann-Schlüsselaustausch	778
	D.7 Hash-Algorithmen	779
	D.8 Verfahren und ihre sinnvollen Schlüssellängen	780
	D.8.1 Symmetrische Verfahren	780
	D.8.2 Asymmetrische Verfahren	783
	D.8.3 Hash-Algorithmen	784
	D.9 Fazit	785
E	The Forensic Challenge	787
	E.1 The Forensic Challenge	787
	E.1.1 Introduction	787
	E.1.2 The Challenge	788
	E.1.3 The Rules	791
F	Lizenzen	795
	F.1 GNU GPL	795
G	URLs	803
	G.1 Umfragen	803
	G.2 Eingesetzte Werkzeuge	803
	G.3 CERTs	804
	G.4 Datenbanken für Sicherheitslücken	804
	G.5 Konferenzen	805
	G.6 Linux-Distributionen	805

H Die CD-ROM zum Buch	807
H.1 Rescue-Modus	807
H.2 Honeynet-Daten	808
I Glossar	809
J Literaturhinweise	817
Stichwortverzeichnis	819
Über den Autor	831