

Christoph Busch / Stephen D. Wolthusen

Netzwerksicherheit

Inhaltsverzeichnis

1 Einführung	1
1.1 Historischer Hintergrund	1
1.2 Der Morris-Worm	11
2 Risikoanalysen und Sicherheitspolitiken	19
2.1 Methodik für Risikoanalysen	19
2.2 Baumbasierte Verfahren für Risikoanalysen	23
2.3 Die Sicherheitspolitik	28
2.4 Rechtliche Aspekte	38
3 Grundlagen des Internet Protocol	55
3.1 Das OSI-Referenzmodell	55
3.2 Ethernet	58
3.3 Address Resolution Protocol	64
3.4 Reverse Address Resolution Protocol	66
3.5 Internet Protocol	66
3.6 ICMP	76
3.7 UDP	83
3.8 TCP	84
3.9 Routing-Verfahren	91
4 Firewall-Architekturen	93
4.1 Paketfilter	94
4.2 Proxying-Systeme	106
4.3 Zustandsbasierte Paketfilter	112
4.4 Hybride Architekturen	121
4.5 Firewall-Topologien	122
4.6 Screening Router	123
4.7 Dual-Homed Host	124
4.8 Bastion Hosts	126
4.9 ScreenedHost	126
4.10 Screened Subnet	127
5 Angriffsmechanismen	131
5.1 Modus Operandi	131
5.2 Angriffe auf Authentisierungsmechanismen	134
5.3 Angriffe mittels Datenmaterial	135
5.4 Kompromittierung von legitimen Verbindungen	145

5.5	Denial of Service	148
5.6	Wiedereinspielungs-Angriffe	159
5.7	Einfügen von Daten in Verbindungen	159
5.8	Veränderung von Daten in Verbindungen	160
5.9	Angriffe auf Befehlskanäle	160
5.10	Systemprofile	161
6	Anwendungsprotokolle	165
6.1	Domain Name Service	165
6.2	Simple Mail Transfer Protocol	172
6.3	Telnet	177
6.4	File Transfer Protocol	179
6.5	Hypertext Transfer Protocol	185
6.6	Simple Object Access Protocol	188
6.7	Network Time Protocol	194
6.8	RealAudio	195
7	Revisionsmechanismen	201
7.1	BSDSyslog	201
7.2	SNMPv1	210
7.3	SNMPv2	216
7.4	SNMPv3	220
7.5	Windows NT Event Log	222
7.6	Tripwire	224
7.7	Protokollierungs-Architekturen	224
8	Handhabung von Vorfällen	227
8.1	Handhabung laufender Angriffe	227
8.2	Anomalien	232
8.3	Aktive Verteidigung	233
8.4	Sammlung forensischer Daten	233
8.5	Fernwartungs Werkzeuge	240
8.6	RootKits	242
8.7	BSD Security Levels	244
8.8	Analyse der Penetrationstiefe	245
8.9	Wiederherstellung des Regelbetriebes	246
9	Zuverlässigkeit und Skalierbarkeit	247
9.1	Redundanz von Netzwerk-Komponenten	247
9.2	Mechanismen für den Lastausgleich	255
9.3	Verteilung von Regelwerken	267
9.4	Vertrauenswürdigkeit	267
10	IP Version 6	287
10.1	Grundlagen	287
10.2	Adressierung	297
10.3	ICMP Version 6	299
10.4	Kapselung von IPv6 in Ethernet	300

10.5	IPSec	300
10.6	Neighbor Discovery	313
10.7	Mobile IPv6	317
10.8	Erweiterungen im Domain Name System	319
11	VPNundNAT	321
11.1	Network Address Translation	321
11.2	Virtual Private Networks	333
11.3	Schlüsselaustausch in IPSEC	334
11.4	GRE	346
11.5	L2TP	348
11.6	PPTP	350
12	Intrusion Detection Systems	353
12.1	Motivation und Einordnung	353
12.2	Ein generisches IDS-Modell	355
12.3	Taxonomische Merkmale	357
12.4	Analytische Verfahren	359
12.5	Implementierungen	375
A	Protokollmitschnitte	379
A.1	Protokollmitschnitt TCP Verbindungsaufbau	379
A.2	Protokollmitschnitt TCP Session Hijacking	379
A.3	Protokollmitschnitt TCP-Verbindungsaufbau A	383
A.4	Protokollmitschnitt TCP-Verbindungsaufbau B	384
A.5	Protokollmitschnitt TCP-Verbindungsaufbau C	385
	Literaturverzeichnis	391
	Index	417