Stephen Northcutt, Judy Novak

Network Intrusion Detection

Übersetzung und Überarbeitung aus dem Amerikanischen
von Marc Ruef

Hüthig

Inhaltsverzeichnis

Widmung **11**

Über die Autoren **12**

Vorwort zur deutschen Neuauflage **13**

Einführung **15**

Teil I TCP/IP **17**

1 IP-Konzepte 19
1.1 Das TCP/IP-Internet-Modell 20
1.2 Verpackung (Mehr als Papier und Plastik) 22
1.3 Adressen 27
1.4 Dienst-Ports 32
1.5 IP-Protokolle 33
1.6 Domain Name System 35
1.7 Routing: Wie kommt man von hier nach da? / 36
1.8 Zusammenfassung 37

2 Einführung in TCPdump und TCP 39
2.1 TCPdump 40
2.2 Einführung in TCP 47
2.3 TCP auf Abwegen 55
2.4 Zusammenfassung **58**

3 Fragmentierung **61**
3.1 Theorie der Fragmentierung 61
3.2 Bösartige Fragmentierung 71
3.3 Zusammenfassung 74

4 ICMP 75
4.1 ICMP-Theorie 75
4.2 Mapping-Techniken 78
4.3 Gewöhnliche ICMP-Aktivität 83

4.4 Bösartige ICMP-Aktivität . . . 87
4.5 Blockieren oder nicht blockieren . . . 94
4.6 Zusammenfassung . . . 97

5 Reiz und Reaktion . . . 99
5.1 Das Erwartete . . . 99
5.2 Eine Tour durch die Protokolle . . . 107
5.3 Ungewöhnliche Reize . . . 112
5.4 Zusammenfassung . . . 121

6 **DNS** . . . 123
6.1 Zurück zu den Grundlagen: DNS-Theorie . . . 123
6.2 DNS zur Informationsgewinnung . . . 135
6.3 Bösartige DNS-Antworten . . . 140
6.4 Zusammenfassung . . . 142

Teil II Traffic Analysis . . . 143

7 Pakete zerlegen mittels TCPdump . . . 145
7.1 Wieso Paket-Analyse lernen? . . . 147
7.2 Sidestep DNS-Abfragen . . . 149
7.3 Einführung in das Zerlegen von Paketen mittels TCPdump . . . 151
7.4 Wo hört IP auf und wo beginnt das eingebettete Protokoll? . . . 153
7.5 Andere Längen-Felder . . . 154
7.6 Die Snaplen vergrößern . . . 156
7.7 Das gesamte Paket zerlegen . . . 158
7.8 Freeware-Tools für die Paket-Zerlegung . . . 161
7.9 Zusammenfassung . . . 164

8 Felder des IP-Headers analysieren . . . 165
8.1 Insertion- und Ausweich-Angriffe . . . 165
8.2 Felder des IP-Headers . . . 169
8.3 Die More Fragments(-MF)-Flagge . . . 173
8.4 Zusammenfassung . . . 181

9 Felder des Headers des eingebetteten Protokolls analysieren . . . 183
9.1 TCP . . . 183
9.2 UDP . . . 200

9.3 ICMP 202
9.4 Zusammenfassung 204

10 Echte Analyse 205
10.1 Sie sind gehackt worden 205
10.2 NetBus-Scan 208
10.3 Wie langsam können Sie gehen? 214
10.4 RingZero-Wurm 217
10.5 Zusammenfassung 220

11 Mysteriöser Verkehr 223
11.1 Die Ereignisse 223
11.2 Der Verkehr 224
11.3 DDoS oder Scan 225
11.4 Fingerprinting benachbarter Hosts 229
11.5 Zusammenfassung 236

Teil IM Filter/Regeln für die Netzwerk-Überwachung 237

12 TCPdump-Filter schreiben 239
12.1 Der Vorgang des Schreibens eines TCPdump-Filters 240
12.2 Bit-Maskierung 242
12.3 TCPdump IP-Filter 245
12.4 TCPdump-UDP-Filter 247
12.5 TCPdump TCP-Filter 248
12.6 Zusammenfassung 252

13 Einführung in Snort und Snort-Regeln 255
13.1 Überblick : der Betrieb von Snort 256
13.2 Snort-Regeln 258
13.3 Zusammenfassung 265

14 Snort-Regeln - Teil II 267
14.1 Format der Snort-Optionen 267
14.2 Regel-Optionen 268
14.3 Alles zusammenführen 286
14.4 Zusammenfassung 288

Teil IV Intrusion Infrastructure 289

15 Mitnick-Angriff 291
15.1 Die Ausnutzung von TCP **291**
15.2 Die Entdeckung des Mitnick-Angriffs **303**
15.3 Netzwerkbasierte Intrusion-Detection-Systeme **304**
15.4 Hostbasierte Intrusion-Detection-Systeme **306**
15.5 Prävention des Mitnick-Angriffs **308**
15.6 Zusammenfassung **308**

16 Architektur-Aspekte **311**
16.1 Interessante Vorkommnisse - Events of Interest **312**
16.2 Grenzen der Beobachtung **314**
16.3 Das Paradigma der niedrig hängenden Früchte **316**
16.4 Menschliche Faktoren schränken Entdeckungen ein **317**
16.5 Schweregrad **320**
16.6 Gegenmaßnahmen **323**
16.7 Berechnung des Schweregrades **324**
16.8 Sensor-Platzierung **327**
16.9 Außerhalb der Firewall **328**
16.10 Push/Pull **331**
16.11 Die Konsole des Analysten **332**
16.12 Host- oder netzwerkbasierte Intrusion Detection **337**
16.13 Zusammenfassung **338**

17 Organisatorische Überlegungen **341**
17.1 Betriebliches Sicherheitsmodell **341**
17.2 Bestimmung der Risiken 346
17.3 Risiko 347
17.4 Bestimmung der Gefahren **354**
17.5 Risikomanagement hängt vom Geld ab **358**
17.6 Wie risikoreich ist ein Risiko? **359**
17.7 Zusammenfassung **360**

18 Automatisierte und manuelle Reaktionen **363**
18.1 Automatisierte Reaktionen 364
18.2 Honeypot **371**
18.3 Manuelle Reaktionen 374
18.4 Zusammenfassung **383**

19 Business Case für Intrusion Detection ... 385
19.1 Teil eins: Management-Entscheidung ... 387
19.2 Teil zwei: Bedrohungen und Verwundbarkeiten ... 394
19.3 Teil drei: Kompromisse und empfohlene Lösung ... 399
19.4 Wiederholen der Aufgabenübersicht ... 405
19.5 Zusammenfassung ... 405

20 **Richtungen für die Zukunft** ... 407
20.1 Zunahme der Gefahren ... 407
20.2 Sich gegen Übergriffe verteidigen ... 411
20.3 Verteidigung im Detail ... 416
20.4 Neue Techniken ... 420
20.5 Zusammenfassung ... 424

Teil V Anhänge ... 425

A Angriffe und Scans, die Angriffe vorbereiten ... 427
A.i False Positives ... 427
A.2 IMAP-Exploits ... 436
A.3 Scans, um Angriffe durchzuführen ... 439
A.4 Einfacher Angriff, Portmap ... 443
A.5 Zusammenfassung ... 451

B Denial of Service ... 453
B.i Brute-Force Denial-of-Service Traces ... 453
B.2 Elegant Kills ... 458
B.3 nmap ... 461
B.4 Distributed Denial of Service-Angriffe ... 462
B.5 Zusammenfassung ... 465

C Erkennung von Informationsgewinnungsversuchen ... 467
C.i Netzwerk- und Host-Mapping ... 467
C.2 NetBIOS-spezifische Traces ... 478
C.3 Stealth-Angriffe ... 481
C.4 Messen der Antwortzeiten ... 485
C.5 Viren als Informationssammler ... 488
C.6 Zusammenfassung ... **492**