

Inhaltsverzeichnis

1 Ziel dieses Buches	1
2 „Wir sind sicher – Wir haben eine Firewall“	3
3 Allgemeines zu Web-Servern	7
4 Protokolle, Datenverkehr und Logfiles	11
4.1 HTTP-Header.....	11
4.2 Protokolldateien des Microsoft Internet Information Services	13
4.3 Protokolldateien des Apache-Servers.....	14
4.4 Wie funktioniert ein Web-Server.....	16
5 Zugriffsmethoden (Request Methods)	19
5.1 GET-Methode.....	19
5.2 HEAD-Methode.....	20
5.3 POST-Methode	20
5.4 PUT-Methode.....	21
5.5 DELETE-Methode	21
5.6 LINK-Methode.....	21
5.7 UNLINK-Methode	21
5.8 TRACE-Methode	21
5.9 OPTIONS-Methode.....	22
5.10 CONNECT-Methode	22
5.11 Weitere Methoden.....	22

6 Programmiersprachen im WWW	23
6.1 Perl.....	23
6.2 PHP	25
6.3 ASP.....	26
7 Hacker, Tools und Methoden	31
7.1 Abgrenzung: Hacker, Cracker, Angreifer	31
7.2 Typen und Klassifizierungen von Angriffsmethoden	34
7.3 Scanner, Sniffer, Passwortknacker und weitere Tools aus dem Internet... 35	
7.4 Trojaner.....	36
8 Penetrations-Test	39
8.1 Was vorher zu beachten wäre	39
8.2 Der Penetrations-Test-Konflikt.....	41
9 Informationsbeschaffung anhand eines Beispiels	45
9.1 Angriff auf die Webseiten von SCO	45
9.2 Informationsbeschaffung mittels Suchmaschinen am Beispiel Google 48	
9.2.1 Informationsbeschaffung Microsoft IIS 6.0.....	48
9.2.2 Google Suchanfragen nach verschiedenen Arten und Standardseiten von Web-Servern.....	50
9.3 ICMP-Echo-Anfragen	51
9.4 Informationen über Netzwerke sammeln.....	51
9.4.1 Dateistrukturen auf Ihrem Server auflisten nach Eingabe einer falschen URL	52
9.4.2 Informationen zu Applikationen sammeln.....	52
9.4.3 Informationen über angelegte Ordner, Dateien auf dem Web-Server	53
9.4.4 Stand der installierten Updates und Patches auf dem Server	55
9.4.5 "Out of Office"-Nachrichten per Email.....	55

10 Der Apache-Web-Server	59
10.1 Architektur des Apache-Web-Server.....	59
10.2 Multi-Thread und Multi-Prozess Web-Server.....	61
10.3 Serverlogging und Status beim Apache-Server	61
10.4 Architektur des Apache 2.0.....	62
10.5 Sicherheitsperspektiven.....	64
10.5.1 Installation des Apache unter einem anderen Benutzer	64
10.5.2 Dateisystem des Web-Server absichern.....	65
10.5.3 Server Limits konfigurieren	66
10.5.4 Verschlüsselung mit SSL	66
10.5.5 Zugriffsbeschränkungen per .htaccess	67
11 Internet Information Services (IIS) 6.0	75
11.1 Architektur des IIS 6.0	75
11.2 Integration in Windows.....	77
11.3 Zugriffsberechtigung und Dienste.....	78
11.4 Zugriffskontrolllisten – ACL.....	80
12 Angriffe auf IIS Web-Server	83
12.1 Bekannte Sicherheitsrisiken	83
12.1.1 Lockout-Funktion auf einem Web-Server	88
12.1.2 RPC-DCOM-Verwundbarkeiten	89
13 Angriffe auf Apache-Web-Server	91
13.1 Der PHP XML-RPC-Bug.....	91
13.2 Pufferüberlauf im Apache Tomcat Connector	92
13.3 Der Angriff auf die Software Foundation Web-Server	92

14 Maßnahmen zur Absicherung	97
14.1 Grundlegende Maßnahmen.....	98
14.1.1 Updates installierter Systeme und Programme	98
14.1.2 Entfernung aller unnötigen Script-Mappings und Beispieldateien	100
14.1.3 Zugriffsrechte für die Verzeichnisse festlegen	101
14.1.4 Den IIS-Dienst als separaten Dienst laufen lassen.....	102
14.1.5 Härten des Betriebssystems	103
14.1.6 Konzepte und Vorüberlegungen zur Absicherung	113
14.1.7 Tools und Programme zur Absicherung des Apache-Servers	113
14.1.8 Tools für den Internet Information Service.....	118
14.1.9 Tools für Apache (Windows/Unix).....	120
15 „Wenn es doch passiert ist“ – Was ist nach einem Einbruch zu tun?	125
15.1 Erste Schritte	126
15.2 Spurensicherung.....	127
15.3 Rechtliche Aspekte der Forensik.....	128
16 Fazit	131
Anhang	135
Anhang A	135
Anhang B – Apache Response Codes.....	137
Anhang C – IIS Response Codes	139
Anhang D – Beispielcode bindshell.c	143
Quellenverzeichnis	145
Sachwortverzeichnis	149