Inhalt

Geleitwort 17

Vorwort 19

Kapitel 1: Die Testorganisation 21

1.1 Der Auftrag 22
1.1.1 Testtypen 22
1.1.2 Methodik 26
1.1.3 Audit 31
1.2 Die Dokumentation 35
1.3 Der Vertrag 39
1.3.1 Vereinbarungen 39
1.3.2 Vertragsanhang 44
1.4 Der Arbeitsplatz 45

Kapitel 2: Die Arbeitsumgebung 47

2.1 Testprogramme 48
2.1.1 Passwort-Programme 55
Wortlisten 57
Passworte bruteforce erraten 61
Passworte offline knacken 61
Sniffer und Passwortknacker 67
Sniffer und Man in the Middle 68
2.1.2 WLAN-Tools 74
aircrack-ng 74
2.1.3 Informationsverwaltung 83

2.2 Exploit-Frameworks ... 87
2.2.1 Metasploit Framework ... 89
Programme ... 93
Module ... 105
Plugins ... 111
2.2.2 Social Engineering Toolkit ... 112
Installation ... 113
Konfiguration ... 114
Angriffe ... 115
Backdoors ... 119
2.2.3 Web Application Attack and Audit Framework ... 121
Profile ... 126
Angriffe ... 130
Shell-Sitzung ... 132
2.3 Tools für IPv6 ... 133
2.3.1 THC IPv6 Attack Toolkit ... 134
dos-new-ip6 ... 134
detect-new-ip6 ... 135
alive6 ... 135
redir6 ... 136
Fake_router6 ... 137
parasite6 ... 138
2.4 Backtrack ... 139
2.4.1 Installation ... 141
2.4.2 Grafische Oberfläche ... 152
2.4.3 Verschlüsselung ... 155
2.4.4 Konfiguration ... 160
2.4.5 Aktualisierung ... 169

Kapitel 3: Informationsgewinnung ... 171

3.1 Veröffentlichte Informationen sammeln ... 171
3.1.1 Basisinformationen ... 172
3.1.2 Detailinformationen ... 177
3.1.3 Domaininformationen ... 180
3.1.4 Infizierte Systeme suchen ... 184
3.1.5 Suchmaschinen ... 187
3.1.6 Testhindernisse suchen ... 197

3.1.7 Internetpräsenz untersuchen ... 201
3.2 Unveröffentlichte Informationen sammeln ... 208
3.2.1 Gesprächsführung ... 210
3.2.2 Rollen ... 214
3.2.3 Gesprächspartner einschätzen ... 216
3.2.4 Beeinflussung ... 224
3.2.5 Wahrnehmungsänderung ... 226

Kapitel 4: Dienste abtasten ... 229

4.1 Netzwerkverbindungen ... 229
4.1.1 Transport-Protokolle ... 231
4.1.2 TCP-Flags ... 235
4.1.3 Portscanner ... 236
Nmap ... 236
Unicornscan ... 241
Scanner-Hilfsmodule ... 243
4.1.4 IP-Adresse verbergen ... 244
4.2 Offene Ports untersuchen ... 246
4.2.1 FTP, Port 21 ... 247
Versionserkennung ... 247
Anonymer Zugang ... 247
Bruteforce-Angriff ... 248
Zugangsdaten mitlesen ... 249
Konfigurationsdateien ... 249
4.2.2 SSH, Port 22 ... 249
Versionserkennung ... 250
Bruteforce-Angriff ... 250
Zugangsdaten mitlesen ... 251
Konfigurationsdateien ... 253
4.2.3 Telnet, Port 23 ... 253
Bruteforce-Angriff ... 254
Zugangsdaten mitlesen ... 254
Konfigurationsdateien ... 254
4.2.4 SMTP, Port 25 ... 254
Versionserkennung ... 255
Benutzernamen raten ... 255
Bruteforce-Angriff auf Zugangsdaten ... 256

Gefälschte E-Mails versenden ... 257
Konfigurationsdateien ... 258
4.2.5 DNS, Port 53 ... 259
Versionserkennung ... 259
IP-Adressen abfragen ... 260
Domain-Informationen abfragen ... 261
Konfigurationsdateien ... 265
4.2.6 TFTP, Port 69 ... 266
4.2.7 Finger, Port 79 ... 266
Befehlsausführung ... 266
Abfragen über mehrere Systeme hinweg ... 267
4.2.8 HTTP, Ports 80, 8080, 443 ... 267
Versionserkennung ... 268
Funktionsprüfung ... 269
Schutzmaßnahmen suchen ... 271
Verzeichnisse suchen ... 272
Content-Management-Systeme prüfen ... 273
Informationsgewinnung ... 275
Zugangsgeschützte Bereiche angreifen ... 276
Datenverkehr untersuchen ... 279
Java-Applets analysieren ... 283
Web-Backdoor einschleusen ... 285
Schwachstellen auf statischen Webseiten suchen ... 290
Schwachstellen in Webanwendungen suchen ... 291
Schwachstellen ausnutzen ... 293
Web-Datenbanken angreifen ... 297
Konfigurationsdateien ... 309
4.2.9 RPC (Remote Procedure Call), Port 111 ... 310
4.2.10 NTP, Port 123 ... 310
4.2.11 NetBIOS/NetBEUI/CIFS (Samba), Ports 135 bis 139, 445 ... 312
Versionserkennung ... 312
Informationsgewinnung ... 313
Bruteforce-Angriff ... 314
Windows-Verbindungsdaten mitlesen ... 315
Samba-Verkehr umleiten ... 319
Code-Ausführung ... 321
Konfigurationsdateien ... 323
4.2.12 SNMP, Port 161 ... 323
Bruteforce-Angriff ... 323
Zugangsdaten mitlesen ... 325

Informationen auslesen ... 325
Systemwerte ändern ... 326
Konfigurationsdateien ... 327
4.2.13 LDAP, Port 389 ... 327
4.2.14 VPN, Port 500 ... 329
IPSec-VPN ... 330
SSL-VPN ... 336
4.2.15 MS-SQL Server, Port 1433 und 1434 ... 337
Versionserkennung ... 337
Bruteforce-Angriff ... 338
4.2.16 Citrix-ICA-Server, Port 1494, 80, 443 ... 340
Citrix-Mainframes suchen ... 341
Informationsgewinnung ... 341
Bruteforce-Angriff ... 342
Klassisches Hacken ... 342
4.2.17 Oracle, Port 1521 ... 351
Bruteforce-Angriff ... 352
Zugangsdaten mitlesen ... 353
Backtrack-Tools ... 354
4.2.18 NFS, Port 2049 ... 354
Freigaben anzeigen ... 354
NFS-Freigabe einbinden ... 355
NFS-Dateirechte umgehen ... 355
Zugriff auf NFS-Shares ... 356
Konfigurationsdateien ... 357
4.2.19 MySQL, Port 3306 ... 358
Versionserkennung ... 358
Brutefoce-Angriff ... 359
Zugangsdaten mitlesen ... 359
SQL-Abfragen ... 360
Abfragen automatisieren ... 365
Konfigurationsdateien ... 367
4.2.20 RDP, Port 3389 ... 368
4.2.21 Sybase, Port 5000 ... 369
4.2.22 SIP, Port 5060 ... 369
Fingerprinting ... 371
Telefongeräte suchen ... 375
Gespräche mitschneiden ... 375
Bruteforce-Angriff ... 376
Authentisierungsdaten mitlesen ... 377

Telefonsystem abstürzen lassen ... 378
Konfigurationsdateien ... 379
4.2.23 PostgreSQL, Port 5432 ... 379
Versionserkennung ... 380
Bruteforce-Angriff ... 380
Datenbankserver abfragen ... 380
Dateien auslesen ... 381
4.2.24 VNC, Port 5900 ... 382
VNC-Server mit Authentifizierung ... 382
VNC-Server ohne Authentifizierung ... 383
Konfigurationsdateien ... 383
4.2.25 X11, Port 6000 ... 383
Offene X11-Systeme suchen ... 384
Bildschirm abfangen ... 385
Tastatureingaben abfangen ... 385
Konfigurationsdateien ... 386
4.2.26 JetDirect, Port 9100 ... 386
4.2.27 Unbekannter Port und Dienst ... 387
Bannerabfrage ... 387
Prüfung auf HTTP ... 388
Kommunikation über SSL ... 388
Identifizierte Dienste ... 390

Kapitel 5: Systeme angreifen und kontrollieren ... 393

5.1 Schwachstellen ausnutzen ... 393
5.1.1 Exploit suchen ... 394
Exploit-DB ... 395
OSVDB ... 397
CVE ... 400
Packet Storm ... 402
Metasploit Framework ... 404
5.2 Direkter Systemzugriff ... 405
5.2.1 Klartextpasswörter suchen ... 406
5.2.2 Windows-System booten ... 406
5.2.3 Linux-System booten ... 409
5.2.4 Universelle Boot-CD ... 410
5.3 Systemkontrolle ... 412

5.3.1 Systemzugang ... 412
Backdoor einschleusen ... 414
Gegenstelle einrichten ... 422
Persistente Backdoor ... 423
Backdoor schützen ... 423
5.3.2 Informationsgewinnung ... 429
Systeminformationen ... 430
Windows-Registry ... 432
Virtualisierung prüfen ... 437
5.3.3 Netzwerkprüfung ... 438
Netzwerke auslesen ... 438
DNS-Auflösung manipulieren ... 438
Datenverkehr mitlesen ... 439
Zielsystem als Gateway ... 441
5.3.4 Datenabfluß ... 443
Daten vom Zielsystem laden ... 443
Tastatureingaben abfangen ... 444
5.3.5 Rechteausweitung ... 444
Benutzerrechte übernehmen ... 444
Passworthashes auslesen ... 446
Passworthashes knacken ... 447
5.3.6 Zugangsausweitung ... 448
Windows-Fernverbindungen ... 448
Telnet-Server ... 450
5.3.7 Spurenbeseitigung ... 450
Zeitstempel manipulieren ... 450
Systemlogs leeren ... 452

Kapitel 6: Angriffe auf gehärtete Umgebungen ... 455

6.1 Drahtlose Verbindungen ... 455
6.1.1 WLAN-Zugangsdaten ... 457
Unverschlüsseltes WLAN ... 457
WEP-Verschlüsselung ... 459
WPA/WPA2-Verschlüsselung ... 460
WPA Enterprise ... 461
WPS-Verschlüsselung ... 464
Denial of Service ... 466

Mobile WLAN-Clients ... 467
6.1.2 WLAN-Datenverkehr mitlesen ... 470
Zugangspunkt fälschen ... 470
Datenverkehr umleiten ... 473
6.1.3 DECT-Telefonate ... 475
6.2 Firewalls ... 480
6.2.1 Architektur ... 480
6.2.2 Schwächen ausnutzen ... 483
RATTE-Server ... 484
RATTE-Client ... 486
RATTE verteilen ... 488
RATTE ausführen ... 490
6.3 Netzwerkgeräte ... 494
6.3.1 Router ... 494
6.3.2 Netzwerkkontroll-Systeme ... 495
6.4 Kiosk- und Terminalsysteme ... 498
6.5 Online-Banking ... 499
6.5.1 Sitzungsdaten abfangen ... 501
6.5.2 Signaturstick angreifen ... 505
Browser ... 506
Update ... 506
Verbindung ... 507
6.5.3 Eigener Signaturstick ... 508
6.6 Client-Systeme ... 509
6.6.1 Eigener Exploit-Stick ... 509
6.6.2 USB-Angriffsgerät ... 515
6.6.3 Präparierte Webseite ... 520
SET konfigurieren ... 521
Payload auswählen ... 522
6.7 Anwendungen und Systeme ... 526
6.7.1 Office-Dokumente ... 526
Dokument bauen ... 527
Dokument verteilen ... 533
6.7.2 Browser ... 533
Ungezielte Browser-Exploits ... 533
Gezielte Browser-Exploits ... 535
Präparierte Webseiten ... 537
Phishing ... 542
Kombinierter Angriff ... 546
6.7.3 Truecrypt-Festplattenverschlüsselung ... 548

6.7.4 E-Mails
6.7.5 IBM i5
6.7.6 Domänen-Controller
6.8 SAP ERP ... 567
6.8.1 SAP-Server ... 569
SAP-Server identifizieren ... 569
Passwort-Angriffe ... 572
Rootshell ... 583
Schwachstellenprüfung ... 587
ABAP-Programme manipulieren ... 604
Backdoor einschleusen ... 606
6.8.2 SAP-Clients ... 608

6.7.4 E-Mails ... 553
6.7.5 IBM i5 ... 556
6.7.6 Domänen-Controller ... 559
6.8 SAP ERP ... 567
6.8.1 SAP-Server ... 569
SAP-Server identifizieren ... 569
Passwort-Angriffe ... 572
Rootshell ... 583
Schwachstellenprüfung ... 587
ABAP-Programme manipulieren ... 604
Backdoor einschleusen ... 606
6.8.2 SAP-Clients ... 608