

Inhaltsverzeichnis

Inhalt	Seite
Voraussetzungen	8
Lernziel.....	9
Kursbeschreibung	10 - 13
Wichtiger Hinweis	14
Rauminstallation.....	15
Inhalte der Kurs-CD-ROM	16
<i>Abschnitt 1:</i>	
Grundlagen	17 - 58
Einführung.....	19
Gründe für Netzwerkangriffe	20
Arten von Angreifern (Hackern)	21
Häufige Arten von Sicherheitslücken	23
Häufige Methoden bei Netzwerkangriffen.....	24
Arten von Sicherheitsbedrohungen	25
Windows-Sicherheitsfeatures aus Sicht des Angreifers	26
Kernel Mode & User Mode	27
Sicherheitsprinzipale	29
SAM und Active Directory (AD)	34
SYSKEY	35
„Ausführen als...“	37
Gruppenrichtlinien	38
Patches & Service Packs	40
Windows-Firewall	41
Windows-Defender	42
Schutz der Datenübertragung mit IPSec.....	43
Datenschutz mit NTFS und Encrypting File System (EFS)	44
Festplattenverschlüsselung mit „Bitlocker“	46
User Account Control (UAC)	47
Rechtliche Grundlagen.....	48
Strafbare Handlungen	49
Straftatbestände nach StGB und UWG	51
Strafanzeige und Strafantrag.....	54
Beweismittel.....	56
Zusammenfassung.....	57
Lernzielkontrolle	58
<i>Abschnitt 2:</i>	
Planen von Angriffen	59 - 170
Einführung.....	61
Google-Hacking – Opfersuche leicht gemacht.....	62
Terminal Services-Anmeldemasken.....	62
Suche nach VNC-Servern	63
Suche nach Kennwörtern	63
Der absolute „Overkill“ – Nessus-Reports!	64
Google-Hacking leicht gemacht.....	65
SiteDigger	65
Firmenwebsite und Stellenausschreibungen	66
Zurück in die Vergangenheit – „archive.org“	67
Suchmaschinen, Usenet & Newsgroups	68
Copernic Agent	70
Bingooo.....	71

1st Email Adress Spider	72
eMail-Searcher	73
Praktische Übung.....	74
Footprinting – dem Opfer auf der Spur	75
Informationsgewinnung im Internet.....	78
HTTrack Web Site Copier	79
Webbasierte Zugänge zu Netzwerkdiensten	80
Google-Earth & Co.	82
GeoWhere Footprinting Tool.....	83
eMailTrackerPro	84
Read Notify.....	85
DNS-Abfragen & WHOIS	86
Ermittlung des Inhabers bestimmter IP-Adressen	88
SamSpade.....	89
Abfragen an DNS-Server	90
Routenverfolgung mit Traceroute	92
Grafische Traceroute-Tools	94
Praktische Übung.....	96
Scanning – die Suche nach der offenen „Tür“	97
Rechner orten – am Anfang steht die Suche	99
Firewalk	100
Portscan-Tools.....	101
Portscan-„Light“ mit telnet	113
Praktische Übung.....	115
Portscans erkennen	116
Enumeration – Windows & Unix ausspähen.....	117
Ausspähen von Webservern	118
Ausspähen weiterer Netzwerkdienste.....	124
Ausspähen von FTP-Servern.....	125
Ausspähen von SMTP-Servern.....	126
Ausspähen von NetBIOS-Name Services	127
Ausspähen von Arbeitsgruppen und Domänen	128
Verhindern der NetBIOS-Name Service-Ausspähung	131
Ausspähen des Administrator-Kontos.....	132
Ausspähen von NetBIOS-Sitzungen	134
Netzwerkfreigaben ausspähen.....	139
Praktische Übung.....	143
Schutz gegen den Missbrauch der IPC\$-Freigabe	144
„RestrictAnonymous=1“ – umgehen	145
Active Directory ausspähen	150
Ausspähen von Active Directory verhindern	153
Praktische Übung.....	155
Unix ausspähen	156
Verhindern der RPC-Ausspähung unter Unix	158
Benutzer unter UNIX/Linux abfragen	159
Abfragemöglichkeit über rwho nd rusers verhindern	159
Suche nach passenden Exploits	161
MetaSploit-Framework – Exploits für alle	164
Angriffsplan erstellen.....	166
Botnets	167
Open Proxys.....	168
Zusammenfassung.....	169
Lernzielkontrolle	170

Abschnitt 3:

Angriffstechniken	171 - 277
Einführung.....	173
Konventionelle Angriffstechnik	174
Social Engineering	175
Electronic Social Engineering	177

Phishing-Versuche erkennen – geht das?	178
Professionelles Phishing.....	179
Pharming.....	180
Schutz gegen Phishing und Pharming	
Daten ausspähen mit Keyloggern.....	182
Anti-Keylogger.....	184
Print Monitor Spy-Tool.....	185
Schutz gegen physikalische Angriffe	186
Angriffe mit vorgefertigten Tools	187
Definition „Sicherheitstools“	187
Sniffer-Tools.....	188
Einführung in Sniffer-Tools	189
WireShark (ehemals Ethereal).....	190
Tcpdump und Windump.....	191
BUTTSniffer	192
Dsniff.....	193
Praktische Übung.....	194
Sniffer aufspüren mit PromiScan	195
Praktische Übung.....	196
Portumleitungstools.....	197
Portumleitung mit FPipe	198
Praktische Übung.....	201
Windows-Verwaltungstools	202
Einführung in Windows-Verwaltungstools	203
Web Hacking-Tools	206
N-Stealth Security Scanner	208
Weitere Web Hacking-Tools	209
Praktische Übung.....	210
Brute Force-Tools	211
Brute Force-Tools – Passwörter cracken	212
Passwörter – und sichere Passwörter	213
Angriffe auf Passwörter in Windows-Netzwerken.....	215
Verbesserungen mit NTLMv2	218
Methoden für den Angriff auf Kennwörter.....	220
Kontosperrungsschwelle mittels Passprop	224
Nach Kennwörtern „sniffen“	225
Passwort-Crack.....	229
Cain and Abel	232
Brutus AET2.....	233
John-the-Ripper	234
LOphtCrack.....	235
NTCrack.....	237
mns PasswordRecovery	238
Advanced Office Password Recovery	239
Praktische Übung.....	240
Weitere Passwort-Cracker	241
Remote Access-Tools	242
Remote Access-Tools und Backdoors	243
VNC	244
SubSeven	245
NetBus Pro & BackOrifice.....	246
OptixPro	248
Praktische Übung.....	249
WinDHCP.....	250
Weitere Backdoor-Tools	251
Multifunktionstools.....	252
Netcat (NC)	253
Cryptcat.....	254
Praktische Übung.....	255
DoS – Denial of Service-Attacken	256
Ansätze von DoS-Attacken.....	257

Abwehrmaßnahmen.....	258
SYNFlooder.....	259
DDoSPing.....	260
Kombinierte Revisionstools.....	261
GFI LanGuard Network Security Scanner.....	263
Praktische Übung.....	266
Retina Network Security Scanner.....	267
STAT Scanner.....	268
ISS-Internet Security Scanner.....	270
Nessus.....	271
Praktische Übung.....	273
Tripwire.....	274
Demo.....	275
Zusammenfassung.....	276
Lernzielkontrolle.....	277
 <i>Abschnitt 4:</i>	
WLAN-Hacking.....	279 - 293
Einführung.....	281
Wireless LAN-Hacking.....	282
NetStumbler.....	283
AiroPeek.....	284
AeroSol.....	285
AirSnort und AirCrack.....	286
coWPAtty und WPA Cracker.....	287
Praktische Übung.....	288
WLAN-Hack ganz ohne Tools?.....	289
Tipps für das Betreiben von sicheren WLANs.....	290
Zusammenfassung.....	292
Lernzielkontrolle.....	293
 <i>Abschnitt 5:</i>	
Daten vernichten und wiederherstellen.....	295 - 304
Einführung.....	297
Daten vernichten und wiederherstellen.....	298
Daten sicher löschen.....	299
Gelöschte Daten wieder herstellen.....	301
Ontrack EasyRecovery.....	205
Praktische Übung.....	302
Zusammenfassung.....	303
Lernzielkontrolle.....	304
 <i>Abschnitt 6:</i>	
Toolkits für Administratoren.....	305 - 333
Einführung.....	307
Live Response-Toolkit für Windows.....	308
Verwendung des Live Response-Toolkit für Windows.....	309
cmd.exe.....	310
Fport.....	311
Netstat.....	312
Nbtstat.....	313
ARP.....	314
kill.....	315
dir.....	316
Auditpol.....	318
psloggedon.....	319
NTLast.....	320
dumpel (Dump Event Log).....	321
Regdmp.....	322

SFind.....	323
Md5sum	324
Praktische Übung.....	325
Anpassung des Live Response-Toolkit für Windows	326
Praktische Übung.....	329
Live Response-Toolkit für Unix/Linux	330
Kommerzielle, forensische Imaging-Toolkits.....	331
Zusammenfassung.....	332
Lernzielkontrolle	333
 <i>Abschnitt 7:</i>	
Firewalls und Honeypods	335 - 348
Einführung.....	337
Firewallsysteme	338
Einsatzkonzepte für Firewalls	339
Bastion Host.....	340
Dreifach vernetzter Firewall	341
Back-to-Back-Firewall	342
GFI DownloadSecurity for ISA Server	343
Honeypod-Technologie	344
KeyFocus KFSensor.....	345
Praktische Übung.....	346
Zusammenfassung.....	347
Lernzielkontrolle	348
 <i>Abschnitt 8:</i>	
Penetrationstests.....	349 - 358
Einführung.....	351
Zweck eines Penetrationstests	352
Phasen eines Penetrationstests	353
Phase 1: Vorbereitung	353
Phase 2: Informationsbeschaffung und –auswertung	354
Phase 3: Bewertung der Informationen / Risikoanalyse.....	354
Phase 4: Aktive Eindringversuche	355
Phase 5: Abschlussanalyse	355
Praktische Übung.....	356
Zusammenfassung.....	357
Lernzielkontrolle	358
 <i>Abschnitt 9:</i>	
BSI-Grundschutzhandbuch.....	359 - 366
Einführung.....	361
BSI-Grundschutzhandbuch	362
BSI-Grundschutzprüfung	363
Praktische Übung.....	364
Zusammenfassung.....	365
Lernzielkontrolle	366
Anhang A: Portnummern (Auszug)	367
Anhang B: ASCII-Tabelle	375
Anhang C: Wichtige Weblinks	379
Anhang D: Top-25-Schwachstellen	383
Anhang E: Antworten zur Lernzielkontrolle	387