

# Inhalt

Widmung.....	11	
Danksagungen .....	11	
Vorwort .....	13	
W13 m4n F0rb1dd3n Network – Anatomie eines Hacks l13st.....	17	
Über die Autoren .....	19	
<b>Teil 1: F0rb1dd3n</b> .....	23	<b>3</b>
Pr010g .....	25	
Ein neuer Auftrag .....	25	
ON3.....	41	
Problem gelöst .....	41	
Die Akquisition .....	50	
TWO .....	55	
Ein ganz normaler Tag .....	55	
Die Installation.....	62	
THR33 .....	65	
Im Land .....	65	
FOUR.....	79	
In Real Life.....	79	
F1V3.....	91	
Statuscheck.....	91	
Log Review.....	99	
S1X .....	107	
Das Meeting .....	107	

Erste Spuren.....	111
Die Entdeckung.....	115
S3V3N.....	123
Code-Review.....	123
EIGHT.....	137
Schlachtpläne.....	137
Datensammlung.....	144
N1N3.....	155
Datenanalyse.....	155
Schrumpfendes Team.....	156
Gefährliche Verbindungen.....	158
Lose Enden.....	165
Verzichtbares Kapital.....	168
T3N.....	175
Partei ergreifen.....	175
3P1L0G.....	187
Prozessende.....	187

4

## Teil 2: Security Threats Are Real (STAR) 2.0 189

Kapitel 1 Erkundung.....	191
Social Networking.....	193
Exploit-Techniken.....	194
Best Practices.....	199
Zusammenfassung.....	200
Weitere Informationen.....	201
Google-Hacking.....	202
Exploit-Techniken.....	203
Best Practices.....	210
Zusammenfassung.....	210
Weitere Informationen.....	210
Suche im versteckten Web.....	211
Exploit-Techniken.....	212
Best Practices.....	217
Zusammenfassung.....	217
Weitere Informationen.....	218
Physische Überwachung.....	218

Exploit-Techniken .....	219
Best Practices .....	222
Zusammenfassung .....	224
Weitere Informationen .....	224
Log-Analyse .....	225
Exploit-Techniken .....	226
Best Practices .....	226
Zusammenfassung .....	230
Weitere Informationen .....	231
Do It Yourself: 3DNF hacken .....	231
Das Personal als Ziel .....	233
Google Apps .....	236
Informationsbeschaffung aus Blogs .....	237
Domäneninformationen .....	238
Twitter für Informationsbeschaffung .....	239
Quellen .....	241
<b>Kapitel 2 Scan .....</b>	<b>243</b>
Wardriving .....	243
Exploit-Techniken .....	244
Best Practices .....	250
Zusammenfassung .....	251
Weitere Informationen .....	252
Wireless-Scanning über Distanz .....	252
Exploit-Techniken .....	253
Best Practices .....	254
Zusammenfassung .....	255
Weitere Informationen .....	255
Scanning-Tools .....	255
Exploit-Techniken .....	256
Best Practices .....	258
Zusammenfassung .....	259
Weitere Informationen .....	260
Sicherheit bei Bluetooth .....	260
Exploit-Techniken .....	261
Best Practices .....	263
Zusammenfassung .....	263
Weitere Informationen .....	264
Quellen .....	265

<b>Kapitel 3 Ausspähen</b> .....	267
Sicherheit der Authentifizierung .....	267
Exploit-Techniken .....	268
Best Practices .....	269
Zusammenfassung .....	272
Weitere Informationen .....	273
Physische Sicherheit .....	273
Exploit-Techniken .....	273
Best Practices .....	277
BIOS-Sicherheit .....	277
Sicherheitskennkarten .....	279
Zusammenfassung .....	280
Weitere Informationen .....	281
Sniffing von Netzwerk-Traffic .....	281
Exploit-Techniken .....	282
Best Practices .....	284
Zusammenfassung .....	286
Weitere Informationen .....	287
Ruhende Malware .....	287
Exploit-Techniken .....	288
Best Practices .....	289
Zusammenfassung .....	292
Weitere Informationen .....	292
Die Sicherheit von Browsern .....	293
Exploit-Techniken .....	293
Best Practices .....	295
Zusammenfassung .....	301
Weitere Informationen .....	302
Out-of-Band-Kommunikation .....	302
Exploit-Techniken .....	303
Best Practices .....	304
Zusammenfassung .....	304
Weitere Informationen .....	305
Quellen .....	305
<b>Kapitel 4 Exploit</b> .....	307
Verschlüsselte Speichermedien .....	307
Exploit-Techniken .....	309
Best Practices .....	311

Zusammenfassung .....	314
Weitere Informationen .....	314
Recherche der Angriffsmethoden .....	315
Exploit-Techniken .....	315
Best Practices .....	317
Zusammenfassung .....	318
Weitere Informationen .....	319
Passwortsicherheit .....	319
Exploit-Techniken .....	320
Best Practices .....	324
Zusammenfassung .....	326
Weitere Informationen .....	327
Sichere E-Mail .....	327
Exploit-Techniken .....	328
Best Practices .....	329
Zusammenfassung .....	330
Weitere Informationen .....	331
»Null Share«-Exploit unter Windows .....	331
Exploit-Techniken .....	332
Best Practices .....	333
Zusammenfassung .....	333
Weitere Informationen .....	334
Kreditkartenbetrug .....	334
Exploit-Techniken .....	335
Best Practices .....	337
Zusammenfassung .....	338
Weitere Informationen .....	338
Verschleierung von Traffic .....	339
Exploit-Techniken .....	340
Best Practices .....	344
Zusammenfassung .....	344
Weitere Informationen .....	344
Metasploit .....	345
Exploit-Techniken .....	346
Best Practices .....	348
Zusammenfassung .....	349
Weitere Informationen .....	349
Quellen .....	350

<b>Kapitel 5 Spuren verwischen</b>	355
Spuren von Windows-Logins entfernen	355
Exploit-Techniken	356
Best Practices	358
Zusammenfassung	362
Weitere Informationen	363
Aufräumen des Browsers	363
Exploit-Techniken	364
Best Practices	366
Zusammenfassung	367
Weitere Informationen	367
Quellen	368
<b>Kapitel 6 Kultur der Hacker</b>	369
Prominente Hacker	369
Dan Kaminsky	370
Tony Watson	371
GOBBLES Security	371
n3td3v	371
Stephen Colbert	372
Fixpunkte des Hacker-Kompasses: Von BruCON zu DEFCON und von Beijing nach Brasilien	375
Treffen der Sicherheitsbranche	378
Weitere Informationen	379
Podcasts	379
Blogs	380
Interview mit einem Hacker	382
Jeff Moss (Dark Tangent)	382
Dan Kaminsky	391
Johnny Long	394
Marcus Ranum	400
Zusammenfassung	404
Quellen	405
<b>Kapitel 7 Bit Bucket</b>	407
Verborgene Geräte	408
Odysseus	409
Volksbank	410
Das Tiger Team	410

Online-Bürgerwehr.....	411
Spot the Fed.....	412
Bob Falken.....	413
Honeypots.....	413
2600 Clubs.....	414
Capture The Flag.....	415
MD5-Hash.....	415
Sydney Bristow.....	416
CyberBob.....	417
Linksys.....	420
InfraGard.....	420
Echelon.....	421
Perl-Skripte.....	421
gh0stRAT.....	422
Lockpicking.....	423
Quellen.....	424
<b>Index.....</b>	<b>427</b>