



mitp



Jayson E.
Street

Kent
Nabors

Brian
Baskin

Forbieten Network

Anatomie eines Hacks

Index

Numerisch

- 2600 Club 414
- 3DNF hacken 231
 - Domäneninformation 238
 - Google Apps 236
 - Informationsbeschaffung aus Blogs 237
 - Personal 233
 - Twitter zur Informationsbeschaffung 239

A

- Advanced Dork 209
- Angriffsmethode
 - Recherchen 315
- Anwendungsprotokoll 356
- Authentifizierung
 - Anatomie eines Hacks 267
 - Best Practices
 - RSA-Token 271
 - Smart Card 272
 - Stärke des Passworts 270
 - Exploit-Techniken 268
 - mit einer Komponente 270
 - Sicherheit 267
 - weitere Informationen 273

B

- Becript Trusted Client 313
- Befehlszeilschnittstelle
 - von Metasploit 346
- Betriebssystem
 - für Scans 244
- Bildschirm Sperre
 - automatische 325
- Bit Bucket 407
- Black Hat 395
- Block All Drive-by Download Exploits (BLADE), Tool 290
- Blog 380
 - Informationsbeschaffung 237
 - persönliches 380
 - von Firmen 381

- Bluebugging 262
- Bluejacking 262
- Bluesnarfung 262
- Bluesniffing 261
 - Bluetooth
 - Sicherheit 260
- Bouncer 341
- Bristow, Sydney 416
- Browser 293
 - Passwörter speichern 293
- Browser aufräumen
 - Anatomie eines Hacks 363
 - Best Practices 366
 - Exploit-Techniken 364
 - Privatsphäre beim Surfen 365
 - weitere Informationen 367
- Browser-Sicherheit
 - Anatomie eines Hacks 293
 - Best Practices
 - mobile Passwort-Safes 300
 - Passwörter einprägen 295
 - Passwort-Safes 296
 - zufällig generierte Passwörter 298
 - Exploit-Techniken
 - Passwortspeicher 294
 - weitere Informationen 302
- BruCON 375
- Brute Force
 - Passwort knacken 322
- Bürgerwehr
 - online 411

C

- cache: Operator 204, 208
- Cantenna 253
- Capture The Flag 415
- Chaos Communication Congress (CCC) 377, 416
- Chrome, Browser 365
- CitySec-Meeting 378
- Client-Steuerung
 - gesicherte 313
- Colbert, Stephen 372

Cold-Boot-Attacke 310
 Common Access Card (CAC) 272
 Cracken
 von Passwörtern 328
 CyberBob 417
 Cyberkrieg 385

D

Datenschutz
 Richtlinien 312
 Debitkarte 335
 Deep Web
 Suche 211
 DEFCON 377, 382, 412, 424
 Domäneninformation 238

E

Easter Egg 407, 410
 Echelon 421
 EDGAR (Electronic Data-Gathering, Analysis,
 and Retrieval), Datenbank 212
 Electronic Frontier Foundation (EFF) 342
 E-Mail
 sichere 327
 Ereignisprotokoll 356
 Erkundung
 als Verteidigungsmechanismus 219
 Definition 191
 Erweiterte Suchoperatoren 203
 Ethereal, Traffic-Analysierer 283
 Event-Log 356
 Anwendungsprotokoll 356
 Sicherheitsprotokoll 356
 Systemprotokoll 356
 ExcaliburCon 377
 Exfiltration 311
 Exfiltrationscontainer 310
 Exploit
 Definition 191
 Exploit-Techniken 244
 ext: Operator 204, 206

F

Facebook 197
 Anatomie eines Hacks 197
 Falken, Bob 413
 Finanzdaten
 Sicherheit 338
 Finanzverbrechen
 Schutzvorkehrungen 338
 Firma
 Blog 381

Freedom of Information Act (FOIA) 213
 Full Disk Encryption (FDE) 310
 Funknetzverschlüsselung
 hacken 247
 Funknetzwerk
 der Polizei 248
 Sicherheit 250

G

Gehackte Funknetzverschlüsselung 247
 Geldautomat 336
 Transaktionen 338
 Geldkurier 336
 Gerät
 verborgenes 408
 Gesicherte Client-Steuerung 313
 gh0stRAT 422
 GOBBLES Security 370, 371
 Google Apps 236
 Google Cache 206
 Google Chrome 365
 Google Hacking Database (GHDB) 202
 Google-Hacking
 Anatomie eines Hacks 202
 Best Practices 210
 Exploit-Techniken
 Advanced Dork 209
 Archivierte Webseiten 206
 Erweiterte Suchoperatoren 203
 Lokalisierung von Schwachstellen 202
 Weitere Informationen 210
 Graphics Processing Unit (GPU)
 zum Passwort cracken 323
 Grey Hat 395

H

Hacker-Honeyrot 321
 Hackerkultur
 Dan Kaminsky 391
 Johnny Long 394
 Hash-Algorithmus 322, 416
 HijackThis (HJT) 292
 Honeyrot Project 414
 Honeyrot 413
 von Hackern 321

I

iDefense Labs 316
 inanchor: Operator 204
 Inferenz 196
 Informationssicherheit
 Blogs von Firmen 381
 persönliche Blogs 380

- Podcasts 379
- Profis 372
- Terminplanung 379
- InfraGard 420
- InPrivate-Browsen 365
- Instant Messaging 199
- Internet Archive
 - Wayback Machine 208
- Internet Storm Center (ISC) 315
- intext: Operator 204
- intitle: Operator 204
- Intrusion Detection System (IDS) 257, 259, 317
- Intrusion Prevention System (IPS) 259, 317
- inurl: Operator 204
- IP-Spoofing 340

K

- Kaminsky, Dan 370, 391
- KeePass 296
- Kennkarte
 - gefälschte 276
- Kismet, Wireless-Scanner 245
- Kreditkartenbetrug
 - Anatomie eines Hacks 334
 - Best Practices 337
 - Verbraucherschutz 337
 - Exploit-Techniken 335
 - Geldkurier 336
 - Skimming 335
 - weitere Informationen 338

L

- LastPass 298
- link: Operator 204
- Linksys-Netzwerk 420
- Lockpicking 423
- Log-Analyse
 - Anatomie eines Hacks 225
 - Best Practices
 - Log-Visualisierung 229
 - Nagios 229
 - Snort-Regeln 227
 - Exploit-Techniken 226
 - Visualisierung 229
 - Weitere Informationen 231
- Long, Johnny 394
- Löschung
 - des Browserverlaufs 355

M

- Malware
 - ruhende 287
 - Entfernen von 290

- Maryland Department of Assessments and Taxation (MDAT) 214
- MD5 416
- MediaDefender, Inc. 329
- Message-Digest Algorithm 5 (MD 5) 416
- Metasploit
 - Anatomie eines Hacks 345
 - Befehlszeilenschnittstelle 346
 - Best Practices 348
 - Exploit-Techniken 346
 - Web-Interface 347
 - weitere Informationen 349
- MicroSD 408
- Microsoft Outlook 328
 - Unterbinden der PST-Nutzung 330
- Mobiler Passwort-Safe 300
- Money Mule 337
- Moss, Jeff 382
- Mozilla Firefox 366
- MyKeePass 300

N

- n3td3v 371
- Nagios 229
- National Archives and Records Administration (NARA) 313
- NetStumbler, Tool 245
- Nmap 257
- Norton Security Suite 296

O

- Obfuskation siehe Verschleierung
- Odysseus 409
- Offenlegung
 - verantwortungsbewusste 318
- Onion Routing (OR), Netzwerk 342
- Online-Bürgerwehr 411
- Open Security Foundation 308
- Ophcrack, Tool 323
- Out-of-Band-Kommunikation
 - Anatomie eines Hacks 302
 - Best Practices 304
 - Exploit-Techniken 303
 - weitere Informationen 305

P

- Passwort
 - Angriff mit Brute Force 309
 - Best Practices
 - Stärke 270
 - Blanking 320
 - Erinnerung 320

- mit Brute Force knacken 322
- mit SSD knacken 324
- mobiler Safe 300
- per Zufallsgenerator 298
- Speicher 294
- Stärke 311
- starkes und einmaliges 324
- Passwort-Safe 296
 - mobiler 300
- Passwortsicherheit
 - Anatomic eines Hacks 319
 - Best Practices
 - automatische Bildschirmsperre 325
 - starke und einmalige Passwörter 324
 - Exploit-Techniken
 - Passwort mit GPU knacken 323
 - Passwortangriff mit Brute Force 322
 - Passwort-Blanking 320
 - Passwort-Erinnerung 320
 - Rainbow Tables 323
 - weitere Informationen 327
- Payment Card Industry Data Security Standard (PCI DSS) 337
- Perl-Skript 421
- Personal Storage Table (PST) 328, 329
- Perverted Justice 411, 412
- PH-Neutral 375
- Physische Sicherheit
 - Anatomic eines Hacks 274
 - Best Practices
 - BIOS-Sicherheit 274
 - Sicherheitskennkarten 279
 - Exploit-Techniken
 - BIOS-Sicherheit 273
 - gefälschte Kennkarten 276
 - weitere Informationen 281
- Physische Überwachung
 - Anatomic eines Hacks 218
 - Best Practices
 - Speicheranforderungen 223
 - Verfolgung der Überwachung 222
 - Verschlüsseltes Backup 224
 - Exploit-Techniken 219
 - Überwachung öffentlicher Webcams 220
 - Webcam-Hacking 220
 - Weitere Informationen 224
- Podcast 379
- Polizei
 - Funknetzwerk 248
- Pretty Good Privacy (PGP) 308
- Privatsphäre beim Surfen 365
- Prominente Hacker
 - Dan Kaminsky 370, 391
 - Jayson Street 375

- Jeff Moss 382
- Johnny Long 394
- Marcus J. Ranum 400
- n3td3v 371
- Stephen Colbert 372
- Tony Watson 371
- psad, Tool 230

R

- Radio-Frequency Identification (RFID) 277
- Rainbow Tables 323
- Ranum, Marcus J. 400
- Recherche
 - über Angriffsmethoden 315
 - Anatomic eines Hacks 315
 - Best Practices 317
 - Intrusion Prevention Systems 317
 - Exploit-Techniken 315
 - Firmen für Exploit-Erfassung 316
 - SANS Internet Storm Center 315
 - weitere Informationen 319
- Reconnaissance
 - Definition siehe Erkundung
- Recording Industry Association of America (RIAA) 371
- Responsible Disclosure siehe Offenlegung
 - verantwortungsbewusste
- RSA-Token 271
- Ruhende Malware
 - Anatomic eines Hacks 287
 - Best Practices
 - Applikationen zur Entfernung von Malware 290
 - präemptiver Schutz 289
 - Exploit-Techniken 288
 - Weitere Informationen 292

S

- SANS Internet Storm Center 315
- Scan
 - durch Betriebssystem 244
- Scanning-Tools
 - Anatomic eines Hacks 255
 - Best Practices
 - Intrusion Detection System 259
 - Intrusion Prevention System 259
 - Exploit-Techniken 256
 - Nmap 257
 - SuperScan 256
 - weitere Informationen 260
- Schlüssel des zuletzt eingeloggten Nutzers 357
- sfportscan 229
- ShmooCon 376

- SHODAN, Suchmaschine 221
 - Sichere E-Mail
 - Anatomie eines Hacks 327
 - Best Practices
 - Richtlinien zur E-Mail-Aufbewahrung 330
 - Unterbinder der PST-Nutzung 330
 - Exploit-Techniken
 - Cracken von Passwörtern 328
 - umgeleitete E-Mails 329
 - weitere Informationen 331
 - Sicherheit
 - Finanzdaten 338
 - Sicherheit bei Bluetooth
 - Anatomie eines Hacks 260
 - Best Practices 263
 - Exploit-Techniken 261
 - weitere Informationen 264
 - Sicherheitskennkarte 279
 - Sicherheitskonferenz
 - Auflistung 372
 - BruCON 375
 - Chaos Communication Congress (CCC) 377
 - DEFCON 377
 - ExcaliburCon 377
 - PH-Neutral 375
 - ShmooCon 376
 - SYSCAN 376
 - UCon 378
 - XCon 376
 - Sicherheitsprotokoll 356
 - Signal Intelligence (SIGINT) 421
 - Simple Network Management Protocol (SNMP) 345
 - site: Operator 204
 - Skimmer 335
 - Skimming 335
 - Skriptsprache 422
 - Smart Card 272
 - Sneakers – Die Lautlosen (Film) 411
 - Snort 227, 317
 - Social Networking
 - Anatomie eines Hacks 193
 - Angestellte ausbeuten 194
 - Best Practices 199
 - Den Hintergrund der Mitarbeiter prüfen 199
 - Schulungen 200
 - Das Unternehmen ausbeuten 195
 - Exploit-Techniken 194
 - Facebook ausbeuten 197
 - Twitter ausbeuten 198
 - Weitere Informationen 201
 - Solid State Drive (SSD)
 - zur Unterstützung beim Passwort knacken 324
 - spear phishing 236
 - Speichermedium
 - verschlüsseltes 307
 - Spot the Fed 412
 - Street, Jayson 375
 - SubSeven 288
 - Suche im versteckten Web
 - Anatomie eines Hacks 211
 - Best Practices 217
 - Exploit-Techniken 212
 - Datenbanken der Finanzämter 214
 - Gelistetes Material verstehen 216
 - Partnerschaften 216
 - Pressemittelungen 215
 - United States Securities and Exchange Commission 212
 - Weitere Informationen 218
 - SuperScan 256
 - SYSCAN 376
 - System for Electronic Document Analysis and Retrieval (SEDAR) 214
 - Systemprotokoll 356
- T**
- T.J. Maxx-Exploit 248
 - The Onion Router (Tor) 342
 - Tiger Team 411
 - TippingPoint 316
 - Tor, Netzwerk 342
 - Traffic
 - Netzwerk zur Umleitung 341
 - Verschleierung 339
 - Traffic-Sniffing 281
 - Anatomie eines Hacks 281
 - Best Practices
 - Entwicklung von Firewall- und IDS-Regeln 285
 - Erkennen von unpassendem Traffic 285
 - Schützen von Netzwerk-Ports 284
 - Exploit-Techniken
 - Platzierung des Sniffers 282
 - Traffic-Review 283
 - weitere Informationen 287
 - Trammell, Dustin D. 21
 - Trojanisches Pferd 409
 - TrueCrypt 309, 312
 - Twitter
 - Anatomie eines Hacks 198
 - Instant Messaging 198
 - zur Informationsbeschaffung 239

U

- UCon 378
- Umleitung von Traffic
 - Netzwerk 341
- United States Postal Service (USPS) 208
- United States Securities and Exchange Commission 212

V

- Verborgenes Gerät 408
- Verbraucherschutz 337
- Verfolgung der Überwachung 222
- Verschleierung von Traffic
 - Anatomie eines Hacks 339
 - Best Practices 344
 - Exploit-Techniken
 - IP-Spoofing 340
 - Tor-Netzwerk 341
 - Umleitung von Traffic 341
 - weitere Informationen 344
- Verschlüsseltes Backup 224
- Verschlüsseltes Speichermedium 307
 - Anatomie eines Hacks 307
 - Best Practices 311
 - Exploit-Techniken 309
 - Cold-Boot-Angriffe 310
 - Exfiltrationscontainer 310
 - Passwortangriff mit Brute Force 309
 - weitere Informationen 314
- Virtual Private Network (VPN) 267, 313
- Visualisierungstechnik 229
- Volksbank 410
- Vulnerability Contribution Program (VCP) 316

W

- Wardriving-Angriff 243
 - Anatomie eines Hacks 243
 - Best Practices-Techniken
 - Kompatibilität der Hardware 251
 - Sicherheit der Funknetzwerke 250
 - Exploit-Techniken 244
 - Funknetzwerke der Polizei 248
 - gehackte Funknetzverschlüsselung 247
 - Kismet und NetStumbler 245
 - Scans durch das Betriebssystem 244
 - WiFiFoFum 246
 - weitere Informationen 252
- Watson, Tony 371

- Wayback Machine 208
- Webcam
 - Hacking 220
 - öffentliche überwachen 220
- Web-Interface
 - Metasploit 347
- White Hat 395
- Wi-Fi Protected Access (WPA) 248
- WiFiFoFum, Wi-Fi-Scanner 246
- Windows Null Share-Exploit
 - Anatomie eines Hacks 331
 - Best Practices 333
 - Exploit-Techniken 332
 - weitere Informationen 334
- Windows Task Scheduler 362
- Windows-Login
 - Best Practices 358
 - Spuren entfernen
 - Anatomie eines Hacks 355
 - Best Practices
 - Ereignisanzeige 358
 - Exploit-Techniken 356
 - Event-Logs 356
 - Schlüssel des zuletzt eingeloggten Nutzers 357
 - weitere Informationen 363
- Wired Equivalent Privacy (WEP) 247
- Wireless-Scanning über Distanz
 - Anatomie eines Hacks 252
 - Best Practices 254
 - Exploit-Techniken 253
 - Cantenna 253
 - Yagi-Gewehre 253
 - weitere Informationen 255
- Wireshark 283

X

- XCon 376

Y

- Yagi-Gewehr 253

Z

- Zero Day Initiative (ZDI) 316
- Zufallsgenerator
 - für Passwörter 298
- Zwei-Faktor-Authentifizierung siehe Smart Card