

Stichwortverzeichnis

A

Access Control. *Siehe auch*
Zugangskontrolle
Access Control List (ACL)
132, 152, 162, 184
Empfehlungen 199
Ping Sweeps 49
Retesting 207
Achtsamkeit 201
Acknowledgment 127
Address Spoofing. *Siehe*
Spoofing
Advanced Persistent Threat
(APT) 2, 91, 156
AV-Bypass 136
Cyberwarfare 131
Destroy Attack als Vorwand
117
Drei-Schichten-Architektur
93
in Multilevel-Attacke 153
Logs 200
Projektplanung 147
Spoofing 96
subversive Angriffe 125
Aktives Monitoring 165
Analyse
Eavesdropping 98
Angriffe
Client-seitige 192
physische 119, 220, 229
Angriffsvektor 36, 73
Definition 74
Reporting 172
subversive Angriffe 131
Web-Zugang 94
Wireshark 94
Anonymous (Gruppe) 54
Antivirus-(AV-)Software 51
Clients 192
Desktop-Rechner 191
Destroy Attacks 116, 122
DoS-Attacken 107
Empfehlungen 196
subversive Angriffe 126

umgehen 135
und Malware 134
Application Programming
Interface (API)
Wireshark 62
ARP-Cache 132, 161
ARP-Poisoning 97
Attack Surface Reduction
(ASR) 191
Aufklärung. *Siehe* Reconnaissance 1
Authentifizierung, Autorisierung, Abrechnung (AAA)
187, 190, 199

B

Backout-Plan 150
Backups 35, 87, 115,
142–143, 164
Prävention 166
Speicherinfrastruktur 193
Basic Network Scan 61
Basic Networking 30
Benutzernamen
Social Engineering 75
Best Practice 165
Network Hardening
188
Blackbox Security Testing
31
Blackhat 226
Black Hat 54–55
Bombe
logische 120
Bring Your Own Device
(BYOD) 82
Buffer 107
Buffer Overflow 45, 96, 107
Tiny Packet Attack 112
Bugs 50
Burp Proxy 92
Burp Suite 92
Business Continuity Planning
(BCP) 193
Bypass 130, 136

C

Carnegie Mellon University
(CMU) 233
CERT 233
Certification Authority (CA)
92
Certified Ethical Hacker
(CEH) 4
Certified Ethical Hacker
(CEH) Certification 28
Change Control 143, 150
Retesting 207
Risikominderung 181
Risk Register 209
Change Management
Retesting 204
Change Ticket 143
Cisco 233
Cisco Discovery Protokoll
(CDP) 132
Click Baiting 120
Clickjacking 133
Client-seitige Angriffe 80, 192
Cloud Security 34, 195
Cloud-Ressourcen 80
Communitys 226
Pentesting 228
Compliance 52
Empfehlungen 190
CompTIA PenTest+ 3, 28
Conclusion 176
Confidentiality, Integrity und
Availability (CIA) 29, 84
Core 188, 189
Cross Site Scripting 34
Crowdsourcing 26
Cybercrime 1
Cyberkriegführung 36
Cyberkriminalität 34
Statistiken 216
subversive Angriffe 130
Cybersecurity *Siehe* Security
Cyberterrorismus 36
Cyberwarfare
subversive Angriffe 130

D

Dark Reading 236
 Daten
 klassifizieren 179
 Datenpakete
 manipulierte Größe 112
 Datenschicht 93
 Defcon 226
 Defense in Depth 29
 Bewertung 162
 Definition 47
 Infiltration 152
 Mythen 220
 physische Angriffe 229
 physische Security 124
 Restesting 208
 Vektoren 75
 Dekodieren 84
 Demilitarized Zone (DMZ)
 32, 38, 81
 Empfehlungen 190, 196
 Denial of Service (DoS) 101
 Bewertung 163
 Definition 105
 Spoofing 96
 Denial-of-Service-Angriff 39
 Destroy Attack 115, 163
 Bewertung 164
 NTP-Masterserver 211
 Prävention 166
 Dienste
 nicht benötigte 186, 187,
 195
 Disaster Recovery (DR) 193
 Cloud Security 195
 Distributed Denial of Service
 (DDoS) 55, 102, 106
 Smurf Attack 110
 Internet of Things (IoT) 74
 Dokumentation
 Change Management 149
 Projektplanung 143
 Retesting 211
 Domain Name System (DNS)
 33
 Drahtlose Netzwerke 82
 Drei-Schichten-Architektur 92
 Dual-Factor Authentication 47
 Dumpster Diving 56, 80
 Dynamic Host Configuration
 Protocol (DHCP) 158

E

Eavesdropping 97
 EC-Council 4
 Elite-Hacker 54
 Ransomware 121
 Empfehlungen 172, 177, 183
 Endpoints 80, 82
 Erlaubnis 26, 142
 Erpressung. *Siehe* Ransom-
 ware
 Erwartungen 139, 141
 Ethernet
 Paketgröße 112
 Ethical Hacker 1, 25
 Genehmigungsverfahren
 142
 Grenze zu Cybercrime 35
 Exclusions 49
 Executive Summary 172
 Exfiltration 2
 Bewertung 163
 Exploit 152, 156
 Bewertung 163
 Penetration und 73
 Exposed Code 116
 Externe Netzwerke 190
 Externe Security Analysts 28,
 140

F

Falsch positive Ergebnisse
 178
 Fehlinterpretationen 178
 File Transfer Protocol (FTP)
 nicht benötigter Dienst 195
 Secure FTP 64
 Wireshark 64
 Firefox 185
 Firewall 32, 45, 196
 Netzwerksegmentierung 188
 Regeln 200
 Fixes
 Retesting 203
 Footprint
 reduzieren 186
 Windows-Rechner 191
 Forescout 97
 Fragmentation Attack 110
 Tiny Packet Attack 112
 Fragrouter 110
 Frühere Testergebnisse 144

G

Ganzheitliches Sicherheits-
 konzept 29
 Ganzheitliches Sicherheits-
 verständnis 171
 Geldautomaten 99
 Genehmigungsverfahren 142
 Geräte
 vernetzte 82
 Gesundheitswesen 164
 Global Information Assurance
 Certification (GIAC)
 4, 232
 Certification Penetration
 Tester (GPEN) 4, 232
 Grey Hat 25, 54–55

H

Hacker 53
 denken wie ein 225
 Elite- 54
 Ethical. *Siehe* Ethical Hacker
 Kevin Mitnick 225
 Reconnaissance 30
 Hackerone.com 27
 Hacktivist 54
 Handshake 129
 Hardening 164, *Siehe*
 Network Hardening
 Heuristisches Scannen
 51
 Honeypot 161, 180, 186, 191
 Hop. *Siehe* Network Hops
 Hosts
 Scan 58
 SYN Stealth Scan 129
 Hotfixes 123
 HTTP
 Port 80 38

I

IANA 68, 189, 195
 Identifiziertes Risiko 43
 Identitätsdiebstahl 91
 Incident Handling 2
 Incident Response 47
 Retesting 204
 Incident Response Team
 (IRT) 47, 158
 Infiltration 1, 152–153
 Bewertung 162

Infrastruktur 193
 Interne Netzwerke 189
 Internet Control Message Protocol (ICMP) 49
 Smurf Attack 111
 Internet of Things (IoT) 29, 219
 Internet Protocol (IP) 31
 Internet Protocol Security (IPsec) 86
 Internet Service Provider (ISP) 81
 Internet Storm Center 231
 Intrusion Detection Software (IDS) 51, 158, 166
 Intrusion Prevention Software (IPS) 51, 166
 IP Fragmentation Attack 110
 IP-Adresse
 IANA 189
 Infiltration 155
 Netzwerksegmente 188
 öffentlicher IP-Adressraum 104
 Spoofing 95–96
 vertrauenswürdige 152
 ISC2 CISSP 28

K

Kali
 DoS 102
 Frag Attacks 110
 Offensive Security 237
 Router Hopping 187
 subversive Angriffe 126
 Kali Linux 2
 im Toolkit 64
 Passwortknacken 83
 SET 75
 Karten-Skimmer 99
 Key Logger 99
 Kick-off-Meeting 139
 Kiwi 201
 Klassifizieren von Daten 179
 Klonen von Webseiten 76
 Konferenzen 226
 Kosten 216
 Kryptografie 84

L

Lab-Umgebung 37, 151, 227
 Legal Penetration Sites 234
 Lauschangriff 97, 152

Legal Penetration Sites 233
 Lessons learned 165
 Localhost 59
 Metasploit 87
 SET 79
 Lockvogel 161, 180, 186, 191
 Logische Bombe 120
 Logs
 APTs 200
 Retesting 207

M

MAC-Adresse 130, 132
 Malware 45, 82, 119
 Destroy Attacks 116
 DoS 102, 107
 Empfehlungen 196
 in Toolkits 58
 Phishing 133
 subversive Angriffe 125, 127
 und AV-Software 134
 Man in the Middle (MITM) 91, 96
 Attack 64
 Burp Suite 94
 Management- und Monitoring-Tool 122
 Mapping 159
 Maximum Transmission Unit Size (MTU) 112
 Message Integrity 85
 Metasploit 37, 86
 Default-Scan 88
 Passwortknacken 83
 SSL 85
 Methoden
 Reporting 172
 Microsoft Security Compliance Toolkit 191
 Middleware 93
 Mobile Device Management (MDM) 34
 Mobile Systeme 194
 Mobile Technologien 34
 Monitoring
 aktives 165
 Multifactor Authentication (MFA) 200
 Multilevel-Attacke 153
 Mythen 215

N

Nachrichtenintegrität 85
 Namensauflösung 187
 Need-to-know-Basis 48
 Empfehlungen 186, 202
 Reporting 179
 Nessus 2, 38, 46
 Destroy Attacks 116
 Empfehlungen 185
 im Toolkit 58
 Netzwerk-Map 159
 Report 117
 Scans 116
 SMB 198
 SSL 85
 Tenable 235
 Nessus-Web-Client 59
 Network Access Control (NAC) 97
 Network Hardening 187
 Hardening Guide 188
 Toolkits 191
 Network Hops 130–131
 Hop-by-Hop-Strategie 152
 Network Time Protocol (NTP) 211
 Netzwerk Access Control (NAC) 118
 Netzwerke
 drahtlose 82
 externe 190
 interne 189
 Segmente 80
 Segmentierung 188, 199
 Netzwerk-Map 68, 159
 Nicht benötigte Dienste 195
 Nmap 3, 68
 für Infiltration 155
 in anderen Tools 88
 Kali Linux 67
 Metasploit Default-Scan 88
 Netzwerk-Map 159
 NTP 211
 offene Ports 50
 Skripte 126
 Spoofing 133
 subversive Angriffe 126
 Website 235
 N-Schichten-Architektur 93

O

- Offene Ports 50, 82
 - Datenbank- 156
 - DHCP 158
 - Retesting 208
 - subversive Angriffe 127
- Offensive Security 66, 237
- Offensive Security Certified Professional (OSCP) 4
- Öffentlicher IP-Adressraum 104
- One-time-Passwort (OTP) 200
- Open Systems Interconnect (OSI) 30
 - ARP-Poisoning 97
- Open Web Application Security Project (OWASP) 126, 234
- Outsourcing-Dienste 195
- Overwhelm and Disrupt Attack 102, 104, 162–163
- Prävention 165

P

- Packet Capture
 - Verschlüsselung 85
- Passcode 194
- Passive Reconnaissance 56
- Password Capture Hack 64
- Passwörter 45
 - Dual-Factor Authentication 47
 - Empfehlungen 200
 - knacken 82
 - Mobilgeräte 194
 - OTP 200
 - Preisgabe 55
 - Projektplanung 147
 - Social Engineering 75
 - subversive Angriffe 132
 - Wireshark 63, 147
- Passwortrichtlinie 45
- Patch Audit 116
- Patch Window/Cycle 117
- Patches 50, 123
 - DNS-Server 175
 - Patch-Programm 196
 - Retesting 203
- Penetration 152, 155
 - Bewertung 162
- Penetration Assessments 46

Penetration und Exploit 73

- APTs 91
- Penetrationstest 1
 - Erlaubnis 26
 - frühere Ergebnisse 144
 - Kosten 216
 - Mythen 215
 - Return on Investment 221
 - Rolle von 26
 - Toolkit 57
- PenTest+-Zertifikat 3
- Pentesting. *Siehe* Penetrationstest
- Pentests. *Siehe* Penetrationstest
 - Petya 121
- Pfad. *Siehe* Vektoren
- Phishing 76, 79
 - Sicherheitsbewusstsein 179
 - subversive Angriffe 133
 - Viren 120
- Physische Angriffe 119, 220, 229
- Ping Sweep 49
 - ICMP 49
 - Infiltration 155
 - Smurf Attacks 110
 - subversive Angriffe 132
 - Plan B 150, 225
- Port 80 (HTTP) 38
 - Empfehlungen 195
 - IANA 195
- Infrastruktur 193
 - offene 50
 - Port 80 161
 - Secure Shell (SSH) 68
 - Wireshark 63
- Port-Scanner 50
- portswigger.net 92
- Post-Pentesting 183
- Präsentationsschicht 93
- Prävention 164
- Pre-shared Keys 86
- Prioritäten
 - Risk Register 210
- Prioritäts-Flags 185
 - Retesting 205
- Projektumfang 141, 144
 - Empfehlungen 177
 - Reporting 174
- Protokolle
 - Infrastruktur 193

Q

- Quick PenTest Hosts Wizard 87

R

- RACI-Chart 140, 143–144
 - Report präsentieren 179
- Ransomware 121
- Rapid7 86
- Raspberry Pi 74
- Reconnaissance 1
 - Hacker 30
 - passive 56
 - Xmas Tree Attacks 113
- Report 171
 - Empfehlungen 183–184
 - Nessus 117
 - Retesting 208
 - Retesting-Plan 207
- Report out 178–179
- Retesting 141–142, 203
 - Change Control 207
 - Empfehlungen 184
 - Prävention 165
 - Prioritäten 175
 - Projektplanung 144
 - Reporting 177
 - Workflow 205
- Return on Investment 221
- Reverse Engineering 66
- Risiko 42
 - als Begriff 42
- Risk Register 43
 - aktualisieren 161
 - Beispiel 209
 - Empfehlungen 185
 - lebendes Dokument 44
 - Management 2
 - Patches 50
 - Projekt-Management 180
 - Projektplanung 145
 - Retesting 205, 209
 - Retesting-Plan 207
 - updaten 180
- Risk-Compliance-Programm 181
- Rollen 139
- Rootkit 106

- Router
 - Access Control List 184
- Router Hopping 81
- Routing Table 132
- S**
- SAMBA 197
- Sandbox. *Siehe* Lab-Umgebung
- SANS 4
- SANS GIAC Penetration
 - Testing Certification 28
- SANS Institute 231
- Schichten
 - N-Schichten-Architektur 92
- Schlüssel 84
- Schwachstellenanalyse 1, 102
- Scope 26
- Screen Scraping 56
- Screened Subnet. *Siehe* Demilitarized Zone
- Script Kiddies 54
 - DoS-Attracken 106
 - Infiltration 152
 - Ransomware 121
- Secure FTP 64
- Secure Shell (SSH) 68, 85
- Secure Sockets Layer (SSL) 62, 85
- Security
 - ganzheitliches Konzept 29
 - Mythen 215
 - Operationen 47
- Security Analysts 27, 42
 - externe 28, 140
 - Rollen und Verantwortlichkeiten 140
- Security Incident Handler 35
- Security Posture. *Siehe* Sicherheitslage
- Segmentierung 188, 199
- Server Message Block (SMB) 197
- Server-seitige Angriffe 80
- Service Packs 123
- Service Set Identifiers (SSIDs) 190
- Sicherheit
 - ganzheitliches Verständnis 171
- Sicherheitslage 38
- Sicherheitslücke
 - Definition 45
 - Risk-Register-Eintrag 210
- Sicherheitsrisiken
 - Energieversorgung 42
 - Finanzindustrie 42
 - Gesundheitswesen 42
 - Militär 42
 - produzierendes Gewerbe 42
 - staatliche Stellen 42
 - Transport und Verkehr 42
- Site Cloner 79
- Skimmer 99
- Skimming 56
- Skripte
 - Datenbank- 118
 - Destroy Attacks 118
 - Nmap 126
- Smurf Attack 110
- Sniffing 97
- Social Engineering 55, 56, 158
 - Empfehlungen 186, 201
 - Mythen 220
 - Sicherheitsbewusstsein 179
 - subversive Angriffe 133
 - Tools 64
 - Vektoren 75
 - Viren 120
- Social Engineering Toolkit (SET) 75
- Socket Access 159
- Software Engineering Institute 233
- Sophos 100
- Speicherinfrastruktur 193
- Spoofing 91, 95–96
 - ARP- 97
 - DoS 103, 111
 - subversive Angriffe 127, 133
- Spyware 120
- SQL Injection 181
- Standard Maximum Transmission Unit Size (MTU) 112
- Standardisierung 221
- Starke Verschlüsselung 198
- Stealth Operations. *Siehe* Subversive Angriffe
- Structured Query Language (SQL) 33
- Subversive Angriffe 125
 - Bewertung 162–164
 - Prävention 166
 - Sicherheitsbewusstsein 179
- Switch 132
- Symantec Endpoint Protection (SEP) 134
- SYN Stealth Scan 68, 127, 129
- Systemadministrator 175
- T**
- TCP/IP 31, 49
 - DoS 109
 - Fragmentation Attack 110
 - Funktionsweise 129
 - SYN Stealth Scan 129
- tcpdump 66
- Techie-Sprech 173
- Tenable 58, 235
- Test-PC 223, 227
- Time to Live (TTL) 111
- Tiny Packet Attack 112
- Toolkit
 - Aufbau 57
 - Identitätsdiebstahl 92
 - Network Hardening 191
 - Standardisierung 221
 - zusammenstellen 224
- Tools
 - Reporting 172
 - Schwachstellenanalyse 102
 - vertrauenswürdige 217
- traceroute/tracert 111
- Transmission Control Protocol (TCP) 31
 - SYN Stealth Scan 68
- Transport Layer Security (TLS) 62, 85
- Tripwire 158
- Trojaner 120
 - in Pentest-Tools 217
 - mobile Geräte 194
 - subversive Angriffe 127
- Trusted User 38, 158

U

Überschwemmen 101,
162–163
Prävention 165
Upgrades 43

V

Vektor. *Siehe* Angriffsvektor
Verantwortlichkeiten 139
Verdeckte Operationen. *Siehe*
Subversive Angriffe
Vernetzte Geräte 82
Verschlüsselung 84
Clients 192
Empfehlungen 198
Ransomware 121
starke 198
Vertrauen 229
Vertrauenswürdige IP-
Adressen 152
Viren 120
DoS 102
Virtual LANs 188
Netzwerksegmentierung 188
Virtualisierung 199, 223
Virtual Private Network
(VPN) 48, 86, 194
Malware 119

Vorfälle. *Siehe* Incident ...
Vulnerability. *Siehe* Sicherheits-
lücke
Vulnerability Scan
Risk-Register-Eintrag
210
Web- 92
Wireshark 62
Vulnerability-Scanner 50
Wireshark 62

W

WannaCry 121
Web-Architektur 92
Webseite
geklonte 75
Web-Vulnerability-Scans
92
Weiterbildung 223
White Hat 25, 54
WhoIs 154
Windows 10 ASR 191
WinPcap 62
Wire Packet Capture 31
Wireless Access Point
(WAP) 80
Alternativen 225
DoS 105
Projektplanung 144

Wireless-SSID 207
Wireshark 3
drahtlose Funktionen
147
Identitätsdiebstahl 94
im Toolkit 61
Lauschangriff 97
Spoofing 134
Tiny Packet Attack
112
Verschlüsselung 85
Website 236
Workflow
Retesting 205
World Wide Web 161
Würmer 120

X

Xmas Tree Attack 113

Z

Zenmap 69
Zero Day 120
Zertifizierungen 3, 28
Zombie 97
DoS 102–103, 106
Zugangskontrolle 194, 199
Zusammenfassung 176