

Inhaltsverzeichnis

| | | |
|-------|---|----|
| | Geleitwort von HD Moore. | 13 |
| | Vorwort. | 17 |
| | Einführung. | 21 |
| I | Grundlagen des Penetrationstests | 27 |
| I.1 | Die PTES-Phasen. | 27 |
| I.1.1 | Vorbereitungsphase. | 27 |
| I.1.2 | Informationsbeschaffung. | 28 |
| I.1.3 | Threat Modeling. | 28 |
| I.1.4 | Schwachstellenanalyse. | 29 |
| I.1.5 | Rechnerübernahme. | 29 |
| I.1.6 | Nach der Übernahme. | 29 |
| I.1.7 | Berichterstattung. | 30 |
| I.2 | Arten des Penetrationstests. | 31 |
| I.2.1 | Offene Penetrationstests. | 31 |
| I.2.2 | Verdeckte Penetrationstests. | 32 |
| I.3 | Schwachstellenscanner. | 32 |
| I.4 | Auf den Punkt gebracht. | 33 |
| 2 | Metasploit-Grundkenntnisse | 35 |
| 2.1 | Terminologie. | 35 |
| 2.1.1 | Exploit. | 35 |
| 2.1.2 | Payload. | 35 |
| 2.1.3 | Shellcode. | 36 |
| 2.1.4 | Module. | 36 |
| 2.1.5 | Listener. | 36 |
| 2.2 | Metasploit-Schnittstellen. | 36 |
| 2.2.1 | MSFconsole. | 37 |
| 2.2.2 | MSFconsole starten. | 37 |
| 2.2.3 | MSFcli. | 38 |
| 2.2.4 | Einsatzbeispiel. | 38 |

| | | |
|----------|--|-----------|
| 2.2.5 | Armitage | 40 |
| 2.2.6 | Armitage starten | 41 |
| 2.3 | Metasploit-Hilfsprogramme | 41 |
| 2.3.1 | MSFPayload | 41 |
| 2.3.2 | MSFencode | 42 |
| 2.3.3 | Nasm Shell | 42 |
| 2.4 | Metasploit Express und Metasploit Pro | 43 |
| 2.5 | Fazit | 43 |
| 3 | Die Informationsbeschaffung | 45 |
| 3.1 | Passive Informationsbeschaffung | 46 |
| 3.1.1 | whois-Recherche | 46 |
| 3.1.2 | Netcraft | 47 |
| 3.1.3 | NSlookup | 48 |
| 3.2 | Aktive Informationsbeschaffung | 49 |
| 3.2.1 | Portscans mit nmap | 49 |
| 3.2.2 | Verwendung von Datenbanken in Metasploit | 51 |
| 3.2.3 | nmap-Scanergebnisse in Metasploit importieren | 52 |
| 3.2.4 | Erweitertes Scannen mit nmap: TCP Idle Scan | 53 |
| 3.2.5 | nmap in MSFconsole verwenden | 55 |
| 3.2.6 | Portscans mit Metasploit | 57 |
| 3.3 | Gezieltes Scannen | 58 |
| 3.3.1 | Server Message Block-Scans | 58 |
| 3.3.2 | Fahndung nach mangelhaft konfigurierten Microsoft-SQL-Servern | 60 |
| 3.3.3 | Scannen nach SSH-Servern | 61 |
| 3.3.4 | Scannen nach FTP-Servern | 62 |
| 3.3.5 | SNMP-Abtastung | 63 |
| 3.4 | Benutzerdefinierte Scanner | 64 |
| 3.5 | Ausblick | 67 |
| 4 | Der Schwachstellenscan | 69 |
| 4.1 | Ein einfacher Schwachstellenscan | 69 |
| 4.2 | Scannen mit NeXpose | 71 |
| 4.2.1 | Konfiguration | 71 |
| 4.2.2 | Der Standort-Assistent | 72 |
| 4.2.3 | Der Assistent für manuelles Scannen | 74 |
| 4.2.4 | Der Bericht-Assistent | 74 |
| 4.2.5 | Berichte in Metasploit importieren | 76 |

| | | |
|-------|---|-----|
| 4.2.6 | NeXpose in MSFconsole nutzen | 77 |
| 4.3 | Scannen mit Nessus | 79 |
| 4.3.1 | Nessus-Konfiguration | 80 |
| 4.3.2 | Erstellen einer Scanrichtlinie für Nessus | 80 |
| 4.3.3 | Ausführen eines Scans mit Nessus. | 83 |
| 4.3.4 | Nessus-Berichte | 83 |
| 4.3.5 | Ergebnisse in Metasploit importieren. | 84 |
| 4.3.6 | Scannen mit Nessus aus Metasploit heraus. | 85 |
| 4.4 | Spezielle Schwachstellenscanner | 88 |
| 4.4.1 | SMB-Logins überprüfen | 88 |
| 4.4.2 | Scannen nach ungeschützten VNC-Servern | 89 |
| 4.4.3 | Scannen nach ungeschützten X11-Servern. | 92 |
| 4.5 | Scanergebnisse für das Autopwning nutzen. | 93 |
| 5 | Das Vergnügen der Übernahme | 95 |
| 5.1 | Übernahme eines Rechners | 95 |
| 5.1.1 | msf > show exploits | 96 |
| 5.1.2 | msf > show auxiliary. | 96 |
| 5.1.3 | msf > show options | 96 |
| 5.1.4 | msf > show payloads | 98 |
| 5.1.5 | msf > show targets | 100 |
| 5.1.6 | info | 101 |
| 5.1.7 | set und unset. | 101 |
| 5.1.8 | setg und unsetg | 102 |
| 5.1.9 | save | 102 |
| 5.2 | Einen Rechner übernehmen. | 103 |
| 5.3 | Übernahme eines Ubuntu-Rechners | 108 |
| 5.4 | Durchprobieren offener Ports per Payload | 111 |
| 5.5 | Ressourcendateien. | 113 |
| 5.6 | Fazit | 115 |
| 6 | Meterpreter | 117 |
| 6.1 | Kompromittierung einer virtuellen Windows-XP-Maschine | 117 |
| 6.1.1 | Mit nmap nach Ports scannen. | 117 |
| 6.1.2 | MS SQL angreifen | 118 |
| 6.1.3 | MS-SQL-Passwörter durchprobieren | 120 |
| 6.1.4 | Die xp_cmdshell | 121 |
| 6.1.5 | Elementare Meterpreter-Kommandos | 123 |
| 6.1.6 | Tastatureingaben mitschneiden | 124 |

| | | |
|-------|---|-----|
| 6.2 | Benutzernamen und Passwörter ausgeben | 126 |
| 6.2.1 | Hashwerte der Passwörter extrahieren | 126 |
| 6.2.2 | Hashwerte von Passwörtern anzeigen | 127 |
| 6.3 | Übergabe von Hashwerten | 128 |
| 6.4 | Rechteausweitung | 129 |
| 6.5 | Imitation von Kerberos-Token | 132 |
| 6.6 | Verwendung von ps | 132 |
| 6.7 | Pivoting – mehrschichtige Angriffe | 134 |
| 6.8 | Verwendung von Meterpreter-Scripts | 138 |
| 6.8.1 | Einen Prozess verlagern | 139 |
| 6.8.2 | Antivirus-Software beenden | 139 |
| 6.8.3 | Systempasswort-Hashes abrufen | 140 |
| 6.8.4 | Sämtlichen Datenverkehr der Zielmaschine aufzeichnen | 140 |
| 6.8.5 | Im System schürfen | 140 |
| 6.8.6 | Das Persistence-Script | 141 |
| 6.9 | Module nach der Übernahme einsetzen | 142 |
| 6.10 | Die Kommandozeile zu Meterpreter ausbauen | 143 |
| 6.11 | Windows-Programmierschnittstellen mit der Railgun-Erweiterung manipulieren | 144 |
| 6.12 | Fazit | 145 |
| 7 | Die Entdeckung vermeiden | 147 |
| 7.1 | Mit MSFpayload eigenständige Programme erstellen | 148 |
| 7.2 | Antivirus-Erkennung umgehen | 149 |
| 7.2.1 | Mit MSFencode verschlüsseln | 150 |
| 7.2.2 | Mehrfachverschlüsselung | 152 |
| 7.3 | Benutzerdefinierte Programmvorlagen | 154 |
| 7.4 | Eine Payload heimlich starten | 155 |
| 7.5 | Packprogramme | 156 |
| 7.6 | Eine abschließende Bemerkung zur Umgehung von Antivirus-Software | 158 |
| 8 | Übernahme durch clientseitige Angriffe | 159 |
| 8.1 | Browser-Exploits | 160 |
| 8.1.1 | So funktionieren Browser-Exploits | 161 |
| 8.1.2 | Ein Blick auf NOPs | 162 |
| 8.2 | NOP-Shellcode entschlüsseln | 163 |
| 8.3 | Der Aurora-Exploit | 166 |
| 8.4 | Dateiformat-Exploits | 171 |

| | | |
|--------|--|-----|
| 8.5 | Übertragen der Payload | 172 |
| 8.6 | Fazit | 173 |
| 9 | Metasploit-Zusatzmodule | 175 |
| 9.1 | Verwendung von Zusatzmodulen | 178 |
| 9.2 | Die Struktur eines Zusatzmoduls | 182 |
| 9.3 | Ausblick | 187 |
| 10 | Das Social-Engineer Toolkit | 189 |
| 10.1 | Social-Engineer Toolkit konfigurieren | 190 |
| 10.2 | Spear-Phishing | 191 |
| 10.3 | Webangriffsvektoren | 197 |
| 10.3.1 | Java-Applet | 197 |
| 10.3.2 | Clientseitige Web-Exploits | 202 |
| 10.3.3 | Benutzernamen und Passwörter erbeuten | 204 |
| 10.3.4 | Tabnabbing | 207 |
| 10.3.5 | Man-Left-in-the-Middle | 207 |
| 10.3.6 | Web-Jacking | 207 |
| 10.3.7 | Ein mehrgleisiger Angriff | 209 |
| 10.4 | Erstellen infektiöser Datenträger | 214 |
| 10.5 | Angriff per Teensy USB HID | 214 |
| 10.6 | Weitere SET-Funktionalitäten | 218 |
| 10.7 | Ausblick | 219 |
| 11 | Fast-Track | 221 |
| 11.1 | Microsoft SQL-Injektion | 222 |
| 11.1.1 | SQL Injector – Angriff per Abfragestring | 222 |
| 11.1.2 | SQL Injector – POST Parameter | 224 |
| 11.1.3 | Manuelle Injektion | 225 |
| 11.1.4 | MSSQL Bruter | 226 |
| 11.1.5 | SQLPwnage | 230 |
| 11.2 | Binär-zu-Hex-Generator | 233 |
| 11.3 | Clientseitiger Massenangriff | 234 |
| 11.4 | Einige Bemerkungen zur Automatisierung | 236 |
| 12 | Karmetasploit | 237 |
| 12.1 | Konfiguration | 237 |
| 12.2 | Angriff starten | 239 |
| 12.3 | Zugangsdaten erbeuten | 242 |
| 12.4 | Eine Shell erhalten | 242 |
| 12.5 | Fazit | 246 |

| | | |
|-----------|--|------------|
| 13 | Eigene Module erstellen | 247 |
| 13.1 | Microsoft-SQL-Befehle ausführen | 248 |
| 13.2 | Analyse eines Metasploit-Moduls | 249 |
| 13.3 | Ein neues Modul erstellen | 251 |
| 13.3.1 | PowerShell | 251 |
| 13.3.2 | Shell-Exploit starten | 253 |
| 13.3.3 | powershell_upload_exec erstellen | 254 |
| 13.3.4 | Konvertierung von Hex nach Binär | 255 |
| 13.3.5 | Zähler | 257 |
| 13.3.6 | Exploit starten | 259 |
| 13.4 | Vorteile wiederverwendbaren Codes | 259 |
| 14 | Erstellen eigener Exploits | 261 |
| 14.1 | Die Kunst des Fuzzings | 262 |
| 14.2 | Manipulieren der strukturierten Ausnahmebehandlung | 266 |
| 14.3 | SEH-Beschränkungen umgehen | 269 |
| 14.4 | Eine Rücksprungadresse finden | 271 |
| 14.5 | Ungültige Zeichen und entfernte Codeausführung | 276 |
| 14.6 | Fazit | 280 |
| 15 | Exploits an Metasploit anpassen | 281 |
| 15.1 | Grundlagen der Assembler-Sprache | 281 |
| 15.1.1 | EIP- und ESP-Register | 281 |
| 15.1.2 | Der JMP-Befehl | 282 |
| 15.1.3 | NOPs und NOP-Rutschen | 282 |
| 15.1.4 | Portierung eines Pufferüberlaufs | 282 |
| 15.1.5 | Grundgerüst eines Exploits | 284 |
| 15.1.6 | Definition des Exploits | 285 |
| 15.1.7 | Test des Exploit-Gerüsts | 286 |
| 15.1.8 | Metasploit-Funktionalitäten einbauen | 287 |
| 15.1.9 | Zufälligkeit hinzufügen | 289 |
| 15.1.10 | Die NOP-Rutsche entfernen | 290 |
| 15.1.11 | Den Pseudo-Shellcode entfernen | 291 |
| 15.1.12 | Das fertige Modul | 291 |
| 15.2 | SEH überschreiben | 293 |
| 15.3 | Fazit | 301 |
| 16 | Meterpreter-Scripting | 303 |
| 16.1 | Grundlagen des Meterpreter-Scriptings | 303 |
| 16.2 | Meterpreter-API | 310 |

| | | |
|--------|---|------------|
| 16.2.1 | Ausgabe..... | 310 |
| 16.2.2 | Einfache API-Aufrufe..... | 311 |
| 16.2.3 | Meterpreter-Mixins..... | 311 |
| 16.3 | Grundregeln beim Schreiben von Meterpreter-Scripts..... | 313 |
| 16.4 | Benutzerdefinierte Meterpreter-Scripts..... | 314 |
| 16.5 | Fazit..... | 321 |
| 17 | Ein simulierter Penetrationstest..... | 323 |
| 17.1 | Vorbereitungsphase..... | 323 |
| 17.2 | Informationsbeschaffung..... | 324 |
| 17.3 | Threat Modeling..... | 324 |
| 17.4 | Übernahme..... | 327 |
| 17.5 | MSFconsole anpassen..... | 327 |
| 17.6 | Nach der Übernahme..... | 329 |
| 17.6.1 | Scannen des Metasploitable-Systems..... | 330 |
| 17.6.2 | Angreifbare Dienste auffinden..... | 331 |
| 17.7 | Apache Tomcat angreifen..... | 333 |
| 17.8 | Unbekannte Dienste angreifen..... | 335 |
| 17.9 | Spuren verwischen..... | 337 |
| 17.10 | Fazit..... | 339 |
| A | Konfiguration der Zielsysteme..... | 341 |
| A.1 | Installation und Einrichtung..... | 341 |
| A.2 | Start der virtuellen Linux-Maschine..... | 342 |
| A.3 | Einrichten eines angreifbaren Windows-XP-Systems..... | 343 |
| A.3.1 | Webserverkonfiguration unter Windows XP..... | 343 |
| A.3.2 | SQL-Server aufsetzen..... | 344 |
| A.3.3 | Eine angreifbare Webanwendung erstellen..... | 346 |
| A.3.4 | Back Track aktualisieren..... | 349 |
| B | Referenz..... | 351 |
| B.1 | MSFconsole-Befehle..... | 351 |
| B.2 | Meterpreter-Befehle..... | 353 |
| B.3 | MSFpayload-Befehle..... | 355 |
| B.4 | MSFencode-Befehle..... | 355 |
| B.5 | MSFcli-Befehle..... | 356 |
| B.6 | MSF, Ninja, Fu..... | 356 |
| B.7 | MSFvenom..... | 357 |
| B.8 | Meterpreter-Befehle nach der Übernahme..... | 357 |
| | Stichwortverzeichnis..... | 361 |