

Inhaltsverzeichnis

1	Einleitung	11
1.1	Ziel und Inhalt des Buches	11
1.2	Rechtliches	14
1.3	Die Einverständniserklärung	15
1.4	Begrifflichkeiten und Glossar	15
2	Metasploit-Framework: Hintergrund, Historie	17
2.1	Die Geschichte des Metasploit-Frameworks	17
2.2	Die Editionen von Metasploit	18
2.3	Die Wahl der Open-Source-Framework-Edition	19
3	Kali-Linux-Umgebung aufsetzen	21
3.1	Die richtige Plattform	21
3.2	Hintergründe zu Kali Linux	22
3.2.1	Offensive Security	22
3.2.2	Kali-Versionen – Rollierende Releases	23
3.3	Muss es unbedingt Kali Linux sein?	23
3.4	Fluch und Segen zugleich	24
3.5	Nativ oder als VM?	25
3.5.1	Kali als native Installation – volle Performance	25
3.5.2	Kali als VM – immer dabei	26
3.5.3	32 Bit oder 64 Bit?	27
3.6	Erste Schritte nach der Installation	27
3.6.1	Kali-Passwort setzen	27
3.6.2	Zurechtfinden	28
3.6.3	Aktualisieren des Systems	34
3.7	Ein erstes Zielsystem: Metasploitable2	37
4	Pentesting-Grundlagen	39
4.1	Begriffsdefinition	39
4.2	Der Scope	40
4.3	Schwarz, Weiß, Grau	41
4.4	Häufigkeit und Zeitpunkt	41
4.5	Verschiedene Arten von Pentests	42

4.5.1	Infrastruktur-Pentests	42
4.5.2	Windows-Domain-/Active-Directory-Pentest	42
4.5.3	Webapplication-Pentests	42
4.5.4	Application-Pentests	43
4.5.5	Wireless-, Physical-Pentests ... and so much more	43
4.5.6	All-In!	44
4.6	Pentesting-Phasen	44
4.6.1	Phase 1: Reconnaissance/Information Gathering	44
4.6.2	Phase 2: Exploitation	45
4.6.3	Phase 3: Privilege Escalation & Post Exploitation	46
4.6.4	Phase 4: Go back to 1 / Pivot and Escalate	46
4.7	Unterschied zwischen Schwachstellenscans, Pentests und Schwachstellenmanagement	46
4.7.1	Penetrationstest	46
4.7.2	Schwachstellenscan	47
4.7.3	Schwachstellenmanagement	47
4.7.4	Der Mix macht's!	48
5	Schwachstellen und Exploits	49
5.1	Softwareschwachstellen/Schwachstellen im Quelltext	49
5.2	Konfigurationsschwachstellen	50
5.3	Standard-, keine und unsichere Passwörter	51
5.3.1	Standard-Passwörter	52
5.3.2	Keine Passwörter	52
5.3.3	Unsichere Passwörter	52
5.3.4	Eine Lösung für das Passwort-Problem?	53
5.4	Exploits	54
5.4.1	Remote Buffer Overflow in SLmail 5.5	54
5.4.2	Der passende Exploit	56
5.4.3	Verschiedene Kategorien von Exploits	60
6	Nmap-Exkurs	63
6.1	Wie funktionieren Portscanner?	63
6.1.1	Ein wenig TCP/IP-Theorie	64
6.1.2	Wie erhebt ein Portscanner offene Ports?	66
6.2	Keine Angst vor der Nmap-Hilfe	71
6.3	Erste Gehversuche mit Nmap	72
6.3.1	Spezifizieren der zu scannenden Ports	73
6.3.2	Offene Ports vs. lauschende Dienste	76

6.3.3	Nmap-Script-Scanning.	77
6.3.4	Schwachstellenscanning mit Nmap.	80
6.4	Intensität und Datenmengen von Portscans verstehen.	82
6.5	Die wichtigsten Nmap-Parameter.	84
7	Metasploit-Basics.	85
7.1	Der erste Start.	85
7.1.1	Die Datenbankanbindung.	85
7.1.2	Initialisierung der Datenbank.	86
7.2	Erste Gehversuche im Framework.	89
7.2.1	Tab Autocomplete und Befehlshilfen.	91
7.2.2	Modul-Workflow – Arbeitsschritte.	91
7.3	Metasploit-Module.	95
7.3.1	Die Modulfamilien.	97
7.4	Eine Ablaufkette am Beispiel von Metasploitable2.	105
7.4.1	Portscan mit Nmap.	105
7.4.2	Validierung mit Metasploit-Auxiliary-Modul.	106
7.4.3	Eindringen mittels Metasploit-Exploit und Payload.	107
7.4.4	Post-Exploitation.	114
7.4.5	Übungsaufgabe.	117
8	Metasploit in der Verteidigung.	119
8.1	Von der Heise-Meldung über das Patchen bis zur Validierung.	119
8.1.1	Transparenz und Awareness schaffen mit Metasploit.	122
8.1.2	Auffinden und Ausnutzen von Heartbleed mit Metasploit.	123
8.1.3	Schließen von Schwachstellen validieren.	127
8.2	Andere Einsatzmöglichkeiten in der Verteidigung.	128
9	Praxisbeispiele.	129
9.1	Vom Word-Dokument zum Domänen-Administrator.	130
9.1.1	Die Laborumgebung.	130
9.2	Initialvektor: Word-Makro.	134
9.2.1	Der soziale Aspekt – Social Engineering.	134
9.2.2	Research, Research, Research.	135
9.2.3	Erstellung der Word-Datei mit Metasploit.	136
9.2.4	Reverse Listener starten.	137
9.2.5	Übertragen und Ausführen der Word-Datei.	139
9.2.6	Local Privilege Escalation.	143
9.2.7	Situational Awareness.	151

9.3	Eskalation in der Windows-Domäne	156
9.3.1	Pivoting	156
9.3.2	Pass-The-Hash	164
9.3.3	Clientside-Exploitation	173
9.3.4	Letzte Hürde: Domänen-Administrator	176
9.4	Erkenntnisse für die Verteidigung	181
9.4.1	User-Awareness-Maßnahmen als erste Verteidigungslinie	182
9.4.2	Antiviren- und Endpoint-Security-Software	182
9.4.3	Office-Makros und Sicherheit allgemein	183
9.4.4	Keinerlei Ports aus dem LAN ins Internet öffnen	184
9.4.5	Berechtigungshygiene	186
9.4.6	Privilege Escalation mittels UAC unterbinden.	189
9.4.7	Auffinden von Schwachstellen durch aktive Schwachstellenscanner.	190
9.4.8	Alarmierung mittels Microsoft Defender for Identity (MDI). . .	190
9.4.9	Office-Angriffsfläche mit Windows Defender Exploit Guard verringern	191
9.5	Das IT-Security-Wettrüsten.	194
10	Anti-Virus-Evasion	195
10.1	Grundlagen der Anti-Virus-Evasion	196
10.1.1	Wann kann man von einem Virens Scanner erkannt werden?	196
10.1.2	Pattern-Matching	197
10.1.3	Wenn Virens Scanner selbst zur Schwachstelle werden.	198
10.1.4	Network-, Filetype-, Clientside- und Post-Exploitation.	200
10.2	Generierung von Stand-alone-Payloads mit Metasploit	201
10.2.1	msfvenom generiert Payloads	201
10.2.2	Standardtechniken: Packer und Encoder	206
10.3	AV-Evasion mit PowerShell	206
10.3.1	Gar nicht erst in Berührung mit dem Virens Scanner kommen: PowerShell	206
10.3.2	Invoke-Shellcode.ps1	207
10.3.3	Base64-All-The-Things by Hand	210
10.3.4	Klickbare Payload	212
10.3.5	Verteidigung: PowerShell sperren.	214
10.4	Katz-und-Maus-Spiel – Neue Techniken und Tricks nutzen	214

11	Nessus-Schwachstellenscanner	217
11.1	Schwachstellen scannen	218
11.2	Vergleich Schwachstellenscanner	219
11.2.1	Unterschied Schwachstellenscanner zu Virens Scanner	219
11.2.2	Funktionsweise von Schwachstellenscannern	220
11.3	Nessus-Versionen	225
11.4	Nessus-Anwendung in der Praxis	225
11.4.1	Installation und Start	226
11.4.2	Erstellen einer passenden Policy	232
11.4.3	Scan der bekannten Labor-Umgebung	248
11.4.4	Schwachstellen-Bewertungssysteme	255
11.4.5	Auswertung der Nessus-Scan-Ergebnisse	259
11.4.6	Effiziente Filtermöglichkeiten	265
11.5	Schwachstellenmanagement	274
11.5.1	Tenable.sc-SecurityCenter	274
12	Schlusswort	277
A	Glossar	279
	Stichwortverzeichnis	285