

# Inhaltsverzeichnis

	<b>Vorwort</b> .....	9
<b>1</b>	<b>Einleitung</b> .....	13
1.1	Ziel und Inhalt des Buchs. ....	13
1.2	Mehr als nur Klartextpasswörter .....	13
1.3	Zielgruppe des Buchs und Voraussetzungen zum Verständnis ....	14
1.4	Rechtliches .....	15
1.5	Begrifflichkeiten und Glossar .....	16
<b>2</b>	<b>Hintergrundinformationen zu mimikatz</b> .....	17
2.1	Die erste Version von mimikatz .....	18
2.2	Wie es zu der Open-Source-Veröffentlichung von mimikatz kam ..	19
2.3	mimikatz 2.0: kiwi ... und eine neue Befehlsstruktur. ....	21
2.4	mimikatz und Metasploit .....	21
2.5	Neue Features: das Changelog im Blick behalten .....	22
2.6	Verwendung von mimikatz in vergangenen Hacks .....	22
<b>3</b>	<b>Eigene Lab-Umgebung aufbauen</b> .....	27
3.1	Ein Labor muss nicht teuer sein. ....	27
3.2	Die Hardware .....	28
3.2.1	Kompakt und stromsparend: der HP-MicroServer .....	28
3.2.2	Über den Tellerrand: Netzwerk-Sniffing .....	33
3.3	Die Software: Hypervisor .....	33
3.3.1	VMware vSphere Hypervisor (ehemals ESXi) .....	34
3.4	Die Software: Gastbetriebssysteme .....	35
3.4.1	Aktuellste Windows-Server-2016-Testversion für 180 Tage .....	35
3.5	Die Windows-Domäne aufsetzen .....	43
3.5.1	Der Domain Controller .....	43
3.5.2	Der erste Member-Server: ein Fileserver .....	56
3.5.3	Aller guten Dinge sind drei! – Ein Admin-Sprunghost. ....	59
3.6	Domänenberechtigungen .....	60
3.6.1	Anlegen von Benutzern und Gruppen .....	60
3.6.2	Berechtigung der Gruppe ServerAdmins .....	65
3.6.3	Anlage und Berechtigung der Fileshares .....	65

3.6.4	Anlegen eines Kerberos SPN . . . . .	69
3.7	Zusammenfassung . . . . .	71
4	<b>Grundlagen Windows LSA</b> . . . . .	73
4.1	Die Credential-Architektur bei einem Domänenmitgliedssystem. . . . .	74
4.1.1	Lokale Authentifizierung gegen die lokale SAM-Datenbank . . . . .	75
4.1.2	Domänenauthentifizierung gegen einen Domain Controller . . . . .	76
5	<b>Grundlagen Kerberos</b> . . . . .	79
5.1	Historie von Kerberos . . . . .	79
5.2	Grundlegende Funktionsweise von Kerberos in Windows-Domänen . . . . .	80
5.2.1	Die Clientauthentifizierung . . . . .	81
5.3	Zusammenfassung . . . . .	88
6	<b>Erste Schritte mit mimikatz</b> . . . . .	89
6.1	Vorbereiten von Windows für den ersten mimikatz-Start . . . . .	89
6.1.1	Virenschanner: das Katz-und-Maus-Spiel . . . . .	89
6.1.2	Deaktivieren des Windows Defender in der Laborumgebung . . . . .	91
6.1.3	Herunterladen von mimikatz . . . . .	92
6.1.4	Erste Start- und Gehversuche . . . . .	94
6.1.5	Berechtigungen: Debug-Privilegien . . . . .	96
6.2	Zusammenfassung . . . . .	100
7	<b>Angriffe mit mimikatz</b> . . . . .	101
7.1	Ausgangssituation . . . . .	101
7.2	Klartextpasswörter . . . . .	102
7.3	Pass-the-Hash (PtH) . . . . .	104
7.3.1	Anwendung von PtH im Labor . . . . .	105
7.3.2	Besonders große Gefahr: Local User Password Reuse . . . . .	109
7.3.3	Zusammenfassung Pass-the-Hash . . . . .	111
7.4	Overpass-the-Hash (OtH)/Pass-the-Key (PtK) . . . . .	112
7.4.1	Normale Funktionsweise der Kerberos-Ticket-Ausstellung . . . . .	112
7.4.2	Overpass-the-Hash (OtH). . . . .	114
7.4.3	Pass-the-Key (PtK). . . . .	120

7.5	Pass-the-Ticket (PtT) .....	123
7.5.1	Stehlen und Weiterleiten des User Ticket Granting Tickets (TGT) .....	124
7.5.2	Stehlen und Weiterleiten des Service Tickets .....	127
7.6	Dumpen von Kerberos-Geheimnissen auf Domain Controllern: dcsync .....	129
7.7	Kerberos Golden Tickets .....	134
7.7.1	Definition und Voraussetzung eines Golden Tickets .....	135
7.7.2	Erstellung und Anwendung des Golden Tickets mit mimikatz im Labor .....	137
7.7.3	Abhängigkeiten bei der Erstellung von Golden Tickets .....	142
7.7.4	Abhilfe bei kompromittiertem krbtgt-Account .....	143
7.8	Kerberos Silver Tickets .....	144
7.8.1	Rotation der Computer\$-Account-Passwörter .....	145
7.8.2	Kerberos Service Principal Names .....	146
7.8.3	Erstellung und Anwendung des Silver Tickets mit mimikatz im Labor .....	147
7.8.4	Warum Silver Tickets verwenden? .....	150
7.9	Kerberoasting .....	151
7.9.1	Definition von Kerberoasting .....	151
7.9.2	Ablauf der Kerberos-Authentifizierungsschritte, die Kerberoasting ermöglichen .....	153
7.9.3	Technischer Ablauf des Kerberoasting .....	155
7.9.4	Zusammenfassung Kerberoasting .....	163
7.10	Domain Cached Credentials (DCC) .....	163
7.11	Zusammenfassung der Angriffe .....	166
8	<b>mimikatz im Alltag</b> .....	169
8.1	Invoke-Mimikatz .....	169
8.1.1	Aktuelle Versionen von Invoke-Mimikatz .....	170
8.1.2	Betrachten von Invoke-Mimikatz .....	171
8.1.3	Ausführen von Invoke-Mimikatz .....	174
8.1.4	PowerShell-Logging von Invoke-Mimikatz .....	179
8.2	Aufruf von Invoke-Mimikatz mittels PowerLine (AppLocker-Evasion) .....	179
8.2.1	Vorbereiten der PowerLine.exe .....	180
8.3	Unzählige weitere Möglichkeiten zur Ausführung von mimikatz .....	184

<b>9</b>	<b>mimikatz erkennen</b> .....	185
9.1	mimikatz-Ausführung mittels Yara in Memory Dumps erkennen .....	186
9.1.1	Anfertigen eines Memory Dump .....	186
9.1.2	Untersuchen des Memory Dump mit Yara unter Python ...	189
9.2	mimikatz-Ausführung in Windows-Logs erkennen – Sysmon .....	193
9.2.1	Installation von Sysmon .....	194
9.2.2	Erkennen der Ausführung von mimikatz in Sysmon-Logs .....	197
9.2.3	Erkennen der Ausführung von mimikatz mit Windows-Standard-Logs .....	200
9.3	mimikatz-Ausführung in PowerShell mit PowerShell-Logging erkennen .....	203
9.3.1	Aktivieren des erweiterten PowerShell-Loggings .....	204
9.3.2	Ausführen und Detektieren von Invoke-Mimikatz in PowerShell .....	207
9.4	Weiterführende Ideen: zentrales Logging .....	209
9.4.1	Unterschiedliche Logging- und SIEM-Lösungen .....	210
9.5	Zusammenfassung .....	220
<b>10</b>	<b>Schlusswort</b> .....	223
10.1	keko: ein neues Tool von Benjamin Delpy .....	223
10.2	Weiterführende Informationen zur Active Directory Security .....	224
<b>11</b>	<b>Glossar</b> .....	225
	<b>Stichwortverzeichnis</b> .....	231