

Inhaltsverzeichnis

	Vorwort	9
1	Einleitung	13
1.1	Ziel und Inhalt des Buches	13
1.2	Mehr als nur Klartextpasswörter	14
1.3	Zielgruppe des Buches und Voraussetzungen zum Verständnis	14
1.4	Rechtliches	16
1.5	Begrifflichkeiten und Glossar	17
2	mimikatz Hintergrundinformationen	19
2.1	Die erste Version von mimikatz	21
2.2	mimikatz 2.0: kiwi ... und eine neue Befehlsstruktur	22
2.3	mimikatz und Metasploit	22
2.4	Neue Features: Das Changelog im Blick behalten	24
3	Eigene Lab-Umgebung Aufbauen	25
3.1	Ein Labor muss nicht teuer sein	26
3.2	Hardware	26
3.2.1	Kompakt und stromsparend: Der HP-Microserver ..	27
3.2.2	Über den Tellerrand: Netzwerk-Sniffing	32
3.3	Die Software: Hypervisor	33
3.3.1	VMware vSphere Hypervisor (ehm. ESXi)	33
3.4	Die Software: Gastbetriebssysteme	35
3.4.1	Aktuellste Windows-Server-2016-Testversion für 180 Tage	35
3.5	Die Windows-Domäne aufsetzen	45
3.5.1	Der Domain Controller	45
3.5.2	Der erste Member-Server: ein Fileserver	60
3.5.3	Aller guten Dinge sind drei! Ein Admin- Sprunghost	65

3.6	Domänenberechtigungen	66
3.6.1	Anlegen von Benutzern und Gruppen.	66
3.6.2	Berechtigung der Gruppe ServerAdmins	71
3.6.3	Anlegen und Berechtigen der Fileshares.	72
3.6.4	Anlegen eines Kerberos SPNs	76
3.7	Zusammenfassung.	78
4	Grundlagen Windows LSA.	81
4.1	Die Credential-Architektur bei einem Domänen Mitgliedssystem	82
4.1.1	Lokale Authentifizierung gegen die lokale SAM- Datenbank	84
4.1.2	Domänen-Authentifizierung gegen einen Domänencontroller	85
5	Grundlagen Kerberos	89
5.1	Historie von Kerberos	89
5.2	Grundlegende Funktionsweise von Kerberos in Windows- Domänen.	90
5.2.1	Die Clientauthentifizierung	91
5.3	Zusammenfassung.	99
6	Erste Schritte mit mimikatz.	101
6.1	Vorbereiten von Windows für den ersten mimikatz-Start. . .	101
6.1.1	Virens Scanner: das Katz-und-Maus-Spiel	101
6.1.2	Deaktivieren des Windows Defenders in der Laborumgebung	104
6.1.3	Herunterladen von mimikatz	105
6.1.4	Erste Start- und Gehversuche	107
6.1.5	Berechtigungen: Debug-Privilegien	109
6.2	Zusammenfassung.	114
7	Angriffe mit mimikatz	115
7.1	Ausgangssituation	115
7.2	Klartextpasswörter	116

7.3	Pass-the-Hash (PtH)	119
7.3.1	Anwendung von PtH im Labor	120
7.3.2	Besonders große Gefahr: Local User Password Reuse	126
7.3.3	Zusammenfassung Pass-the-Hash.	128
7.4	Overpass-the-Hash (OtH) / Pass-the-Key (PtK)	129
7.4.1	Normale Funktionsweise der Kerberos- Ticketausstellung.	130
7.4.2	Overpass-the-Hash (OtH)	132
7.4.3	Pass-the-Key (PtK)	138
7.5	Pass-the-Ticket (PtT)	141
7.5.1	Stehlen und Weiterleiten des User Ticket Granting Tickets (TGT)	142
7.5.2	Stehlen und Weiterleiten des Service Tickets	146
7.6	Dumpen von Kerberos-Geheimnissen auf Domänencontrollern: dcsync.	148
7.7	Kerberos Golden Tickets	154
7.7.1	Definition und Voraussetzung eines Golden Tickets	155
7.7.2	Erstellung und Anwendung des Golden Tickets mit mimikatz im Labor.	158
7.7.3	Abhängigkeiten bei der Erstellung von Golden Tickets	163
7.7.4	Abhilfe bei kompromittiertem krbtgt-Account	164
7.8	Kerberos Silver Tickets	166
7.8.1	Rotation der Computer\$-Account-Passwörter	167
7.8.2	Kerberos Service Principal Names	167
7.8.3	Erstellung und Anwendung des Silver Tickets mit mimikatz im Labor	169
7.8.4	Warum Silver Tickets verwenden?	172
7.9	Kerberoasting	173
7.9.1	Definition von Kerberoasting	174
7.9.2	Ablauf der Kerberos-Authentifizierungsschritte, die Kerberoasting ermöglichen	176

79.3	Technischer Ablauf des Kerberoasting	178
79.4	Zusammenfassung Kerberoasting	188
710	Domain Cached Credentials (DCC).	188
711	Angriffszusammenfassung	191
8	mimikatz im Alltag.	195
8.1	Invoke-Mimikatz.	196
8.1.1	Aktuelle Versionen von Invoke-Mimikatz	197
8.1.2	Betrachten von Invoke-Mimikatz	198
8.1.3	Ausführen von Invoke-Mimikatz	201
8.1.4	PowerShell Logging von Invoke-Mimikatz	207
8.2	Aufruf von Invoke-Mimikatz mittels PowerLine (AppLocker-Evasion)	208
8.2.1	Vorbereiten der PowerLine.exe.	209
8.3	Unzählige weitere Möglichkeiten zur Ausführung von mimikatz	214
9	Schlusswort.	215
9.1	keko: ein neues Tool von Benjamin Delpy	215
9.2	Weiterführende Informationen zur Active Directory Security	216
10	Glossar.	219
	Stichwortverzeichnis	227