mitp

Sebastian
Brabetz

2. Auflage

Penetration Testing mit mimikatz

Das Praxis-Handbuch

Hacking-Angriffe verstehen und Pentests durchführen

Inhaltsverzeichnis

	Vorwort	9
1	**Einleitung**	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
2	**Hintergrundinformationen zu mimikatz**	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
3	**Eigene Lab-Umgebung aufbauen**	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

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

3.6.4 Anlegen eines Kerberos SPN 69
3.7 Zusammenfassung 71

4 Grundlagen Windows LSA 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 Grundlagen Kerberos 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 Erste Schritte mit mimikatz 89
6.1 Vorbereiten von Windows für den ersten mimikatz-Start 89
6.1.1 Virenscanner: 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 Angriffe mit mimikatz 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

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

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 mimikatz im Alltag 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

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

9 mimikatz erkennen 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

10 Schlusswort 223
10.1 keko: ein neues Tool von Benjamin Delpy 223
10.2 Weiterführende Informationen zur Active Directory Security 224

11 Glossar 225

Stichwortverzeichnis 231

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Vorwort

Ich hatte die Chance, über das Aufbauen, Administrieren und Betreuen von Firewalls in einer größeren Firma in das Feld der IT-Security hineinzurutschen.

Beim täglichen Bearbeiten der Firewall-Regelwerke und dem Abschotten von Internet und DMZs gegenüber dem internen Netzwerk konnte ich ein gutes Gespür dafür entwickeln, was es bedeutet, Zugriffe möglichst einzugrenzen, aber auch dafür, Risiken in Form von freizugebenden Kommunikationskanälen gegen strikte IT-Security-Theorien abzuwägen.

Was mir das Administrieren von Firewalls allerdings nie vermitteln konnte, war eine verständliche Erklärung dafür, was Hacker wirklich tun und wie Angriffe auf IT-Systeme in der Realität aussehen.

Nach ein paar Jahren als Firewall-Administrator hatte ich die Chance, zwei Metasploit-Workshops eines sehr talentierten Trainers beizuwohnen. Metasploit ermöglichte mir, trotz fehlenden tiefgehenden Programmierhintergrunds zu verstehen, wie sich Softwareschwachstellen mittels Exploits ausnutzen lassen.

Seit diesen Metasploit-Workshops weiß ich es mehr zu schätzen, welche wichtige Aufgabe Firewalls erfüllen, indem sie nur die notwendigsten Dienste exponieren und Zugriffe auf das Nötigste beschränken können. Jedoch wurde mir auf der anderen Seite plötzlich auch bewusst, wie nutzlos Firewalls allein sind, wenn die Dienste, die man schlussendlich durch sie hindurch verfügbar machen will – und muss –, verwundbar sind.

Noch zwei weitere für meine Reise in die IT-Security wesentliche Erkenntnisse konnte ich aus diesen Metasploit-Workshops mitnehmen:

- zum einen die Existenz des *Penetration Testing with Backtrack Linux*, kurz PWB (mittlerweile *Penetration Testing with Kali Linux*, PWK), und der dazugehörigen OSCP-Zertifizierung, die ich einige Jahre später auf Basis dieser beiden Workshops selbst absolviert habe, und
- zum anderen die Existenz des Nessus-Schwachstellenscanners, den ich seitdem regelmäßig nutze, vertreibe und mit dessen Hilfe ich zum Thema Schwachstellenmanagement berate.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Neben dem Wissen über Netzwerkkommunikation und deren Reglementierung hatte ich nun also auch ein gewisses Verständnis von Softwareschwachstellen, deren Ausnutzung sowie das systematische Auffinden und Vermeiden derselben.

Ein wichtiger Angriffsvektor, der mir weiterhin noch wenig geläufig war, stellten Konfigurationsschwachstellen dar, die für sich allein genommen teilweise noch nicht mal unbedingt schlimm sein müssen. In Verbindung mit weiteren Zuständen in komplexen Firmennetzwerken können sie es aber ermöglichen, IT-Systeme und ganze IT-Landschaften zu kompromittieren.

Genau an dieser Stelle setzt aus meiner Sicht mimikatz als mächtiges Werkzeug an: mimikatz nutzt auf einer tiefen Ebene Möglichkeiten und Funktionen von Windows und den in Windows verwendeten Authentifizierungsprotokollen aus. Die richtigen (oder auch falschen) Personen können sich so trotz Firewalls, Virenscannern und Schwachstellenmanagement durch moderne Windows-Domänen bewegen wie Neo durch die Matrix.

Letzterer Vergleich ist sicherlich albern und ein Klischee, jedoch ist es dieser einfache Vergleich, mit dem ich diese Art von Schwachstellen und Angriffsvektoren für mich am besten greifbar machen und einordnen kann.

Sie halten nun bereits die zweite Auflage dieses Buchs in den Händen!

Seit der Veröffentlichung der ersten Auflage habe ich viel Neues über die Hintergründe von mimikatz gelernt. Dies habe ich im zweiten Kapitel in Form der Geschichte rund um die Open-Source-Veröffentlichung von mimikatz sowie die Verwendung von mimikatz in berühmten öffentlich gewordenen Hacks eingebracht.

In meinem Beruf werde ich neben dem offensiven Audit von IT-Systemen (Red Teaming) auch nahezu in gleichem Maße mit der Verteidigung von IT-Infrastrukturen (Blue Teaming) konfrontiert. Daher habe ich mich dazu entschlossen, diese zweite Auflage um ein komplett neues Kapitel zur Erkennung von Angriffen mit mimikatz und damit zur Verteidigung von IT-Systemen gegen mimikatz zu ergänzen. Dieses Kapitel wird Ihnen einen Einblick darin geben, wie Sie Spuren von mimikatz mittels Yara-Regeln entdecken sowie mithilfe von PowerShell die Anwendung von mimikatz rückblickend in Windows-Eventlogs aufdecken können. Abschließend gibt das neue Kapitel einen Ausblick dazu, wie das systematisch in großen Umgebungen angegangen werden kann.

Sehr wichtig ist es mir, dass ich keinerlei Anerkennung für die in diesem Buch vorgestellten Programme und Angriffstechniken erlangen möchte. Alles, was in diesem Buch vorgestellt wird, wurde von sehr talentierten Menschen entwickelt und kostenlos dem Rest der Welt zur Verfügung gestellt, um transparent zu machen, welche Schwächen sich in Computersystemen verbergen.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

An dieser Stelle einzelne Namen zu nennen, wird wahrscheinlich der Tatsache nicht gerecht, dass auch diese Personen auf der Arbeit anderer Personen vor ihnen aufgebaut haben. Insofern spare ich mir hier das explizite Nennen von Namen und verweise auf die Stellen im Buch, an denen ich auf die Menschen oder Namen eingehe, die unmittelbar für die vorgestellten Programme oder Techniken eine Erwähnung verdienen.

Mit diesem Buch möchte ich das Wissen, das ich mir über einen langen Zeitraum hart erarbeiten musste, anderen Personen leichter zugänglich machen, als es für mich zugänglich war.

Ich habe dabei auch keinerlei Angst, dass das Senken der Einstiegshürde in spannende IT-Security-Themen zu weniger Arbeit für mich oder andere IT-Security-Professionals führen wird. Denn trotz stetiger Weiterentwicklung der Technik scheint eines derzeit auf der ganzen Welt nicht wirklich zu funktionieren: gänzlich sichere IT-Systeme und Programme zu entwickeln und aufzubauen.

Es herrscht ein Mangel an versiertem IT-Security-Personal, und gleichzeitig werden Computer in immer mehr Bereichen des täglichen Lebens verankert: smarte Autos und Häuser, vernetzte Krankenhäuser, Personal-Fitness-Geräte und noch so vieles mehr.

Insofern ist dieses Buch für mich schon ein voller Erfolg, wenn nur eine einzige Person dadurch einen besseren Einblick in die Sicherheit von Windows-Domänen erlangt oder einfach nur Spaß an IT-Security hat.

Mein Beitrag für die IT-Security-Community ist mit diesem Buch also primär das Absenken der Einstiegshürde in einen spannenden Bereich der IT-Security: Active Directory Security.

Abschließen möchte ich das Vorwort mit einem Dank an die Personen, die mir das Schreiben dieses Buchs ermöglicht haben:

Uli

der mitp-Verlag

Sabine Janatschek

Janina Bahlmann

Andrej Schwab

Martin Pizalla

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Ich hoffe, Ihnen gefällt diese zweite, abgerundete Auflage des Buchs und Sie werden genauso viel Spaß mit der Materie haben wie ich! Obgleich ich dieser Tage meine Zeit für die Leidenschaft rund um IT-Security mit einem neuen Bewohner dieser Erde teilen darf:

Willkommen Tamara!

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Kapitel 6

Erste Schritte mit mimikatz

Bevor es mit mimikatz ans Eingemachte geht, sollten Sie die grundlegende Funktionalität, die Syntax und die Menüstruktur von mimikatz verstehen.

6.1 Vorbereiten von Windows für den ersten mimikatz-Start

Zunächst einmal müssen Sie sich, bevor Sie mimikatz überhaupt herunterladen und starten können, mit den wahrscheinlich unter Windows präsenten Virenscannern befassen.

6.1.1 Virenscanner: das Katz-und-Maus-Spiel

mimikatz ist bekannt wie ein bunter Hund! Jegliche Antivirenprogrammhersteller (kurz AV-Hersteller) wissen von der Existenz von mimikatz und haben teils bessere und teils schlechtere Erkennungspatterns für ihre Produkte erstellt, um mimikatz in den nackten unveränderten Versionen von GitHub zu erkennen.

In einem Pentest sind Sie natürlich mit Virenscannern konfrontiert. Sie müssen für die Verwendung von mimikatz auf einem Zielsystem in der anzugreifenden Domäne generell bereits Administrator sein, um die meisten Funktionalitäten von mimikatz nutzen zu können.

Als Administrator wäre es Ihnen z. B. möglich, den Virenscanner zu deinstallieren oder zu deaktivieren. Auch könnten Sie natürlich mit ein wenig Aufwand klassische AV-Produkte austricksen, indem Sie gezielt die Dinge im Code von mimikatz ändern, die die AV-Scanner mit ihren limitierten Patterns alarmieren.

In der Vergangenheit reichten hierzu bereits einfache Techniken des Umbenennens von Strings im Quellcode (aus `mimikatz` wurde `mimidogz`). Teilweise wurden auch kompliziertere Techniken wie das Verschleiern oder Packen der Binärdateien eingesetzt – bis hin zum gänzlichen Neuimplementieren von mimikatz in anderen, neuen Programmiersprachen wie z. B. Go, die nicht von allen Virenscannern gut analysiert werden können.

Eines haben alle vorgenannten Techniken aber gemeinsam: Sobald sie für einen gewissen Zeitraum bekannt waren, haben sich Hersteller von klassischen AV-Produkten überlegt, wie sie diese Techniken identifizieren und abfangen können.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Genau hier liegt aber auch der Schwachpunkt von klassischen AV-Herstellern. Sie laufen immer nur einzelnen Techniken hinterher und schaffen neue limitierte Erkennungsmerkmale. Dadurch machen sie ihre Produkte immer invasiver und leistungshungriger, um einen vermeintlichen Schutz und damit gefühlte Sicherheit zu schaffen.

Verstehen Sie das bitte nicht falsch, ein Pentest wird deutlich spannender und aufwendiger, wenn auf allen Systemen, die man vorfindet, AV-Produkte installiert sind. Der Windows Defender ist z. B. im Bereich PowerShell-Erkennung sehr mächtig geworden, während sich etwa Kaspersky sehr tief im System einnistet und schwer abzutöten ist. Allerdings hat bisher jede Pentest-Geschichte, die ich zu diesem Thema gehört habe, damit geendet, dass es mit irgendeiner neuen Technik schlussendlich dennoch möglich war, den AV-Scanner auszutricksen oder zu deaktivieren. In anderen Fällen haben die Pentester einfach so lange gesucht, bis sie irgendwo ein auf der Domäne befindliches System vorgefunden haben, auf dem kein AV-Scanner installiert werden durfte oder versehentlich vergessen wurde.

Ein Lichtblick in Bezug auf die IT-Sicherheit sind neuere *Next-Gen-Antivirenprodukte*, die nicht mehr auf Basis von Bitmustern alarmieren, sondern mitunter leichtgewichtig im Betriebssystem bestimmte Funktionsaufrufe überwachen. Sie achten gezielt auf eine Aneinanderreihung von Events im Betriebssystem und können so Prozesse beenden sowie Systeme abkapseln, noch bevor Schadsoftware oder mimikatz ihren Dienst verrichten können. Aber auch diese Produkte erreichen wieder ein zusätzliches Level an Komplexität, und sobald der Angreifer von ihrer Existenz weiß, kann er sich Mittel und Wege überlegen, sie zu umgehen oder entsprechend geschützte Systeme nicht weiter anzufassen.

Schlussendlich zielen alle präventiven Schutzsysteme wie klassische AV-Scanner oder verhaltensbasierte Produkte wie Next-Gen darauf ab, die erste Infektion zu verhindern oder davor zu warnen. Schafft es ein Angreifer erst einmal über vorgesehene Zugriffe in die Zielumgebung – z. B. über vom Benutzer ausgeführte speziell für einen einzelnen Einsatz programmierte *Custom-Malware* oder *legitim geklaute Zugangsdaten* oder meinetwegen über einen brandneuen nicht bekannten *Zero-Day-Exploit* –, wird ein gut geschulter Angreifer früher oder später in der Lage sein, die komplette Umgebung zu übernehmen.

In diesem Buch werde ich das Thema AV-Evasion nicht weiter beleuchten. Wenn Sie Interesse haben, solche Techniken zu erlernen und zu üben, können Sie danach in der Suchmaschine Ihrer Wahl suchen und werden eine Vielzahl an Treffern erhalten. Erwarten Sie hierbei nicht eine einfache 1-Klick-Lösung, die alle Virenscanner nachhaltig und für immer austrickst. Vielmehr basiert die Lösung zum Umgehen von Virenscannern immer darauf, dass man versucht, gezielt den einen eingesetzten AV-Scanner über seine individuellen Schwächen auszutricksen. Hierzu wird der AV-Scanner in einem Labor installiert und nach dem Updaten von der Außenwelt abgeschnitten, sodass er den Hersteller nicht über Funde informieren kann.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Spannende Blogartikel und Anleitungen zu diesem Thema finden Sie regelmäßig bei der amerikanischen Pentesting-Firma *Black Hills Information Security* in englischer Sprache:

`https://www.blackhillsinfosec.com/blog/`

Halten Sie auch bei YouTube nach den jährlichen Videos mit dem Titel *Sacred Cash-Cow Tipping* Ausschau, die ebenfalls von dieser Pentesting-Firma erstellt werden, um die AV-Industrie ein wenig in Bewegung zu halten.

6.1.2 Deaktivieren des Windows Defender in der Laborumgebung

Wenn Sie Ihr eigenes Labor abweichend von dem im Buch vorgestellten Labor verwenden, deaktivieren Sie gegebenenfalls einfach die verwendete AV-Lösung, sofern überhaupt eine installiert wurde.

Sofern Sie, wie in diesem Buch demonstriert, Windows Server 2016 installiert haben, kommt dieser von Haus aus mit dem Windows Defender, den Sie über die Systemeinstellungen deaktivieren können.

Loggen Sie sich dazu als Administrator an dem Sprunghost ein und entfernen Sie alle Haken des Windows Defender.

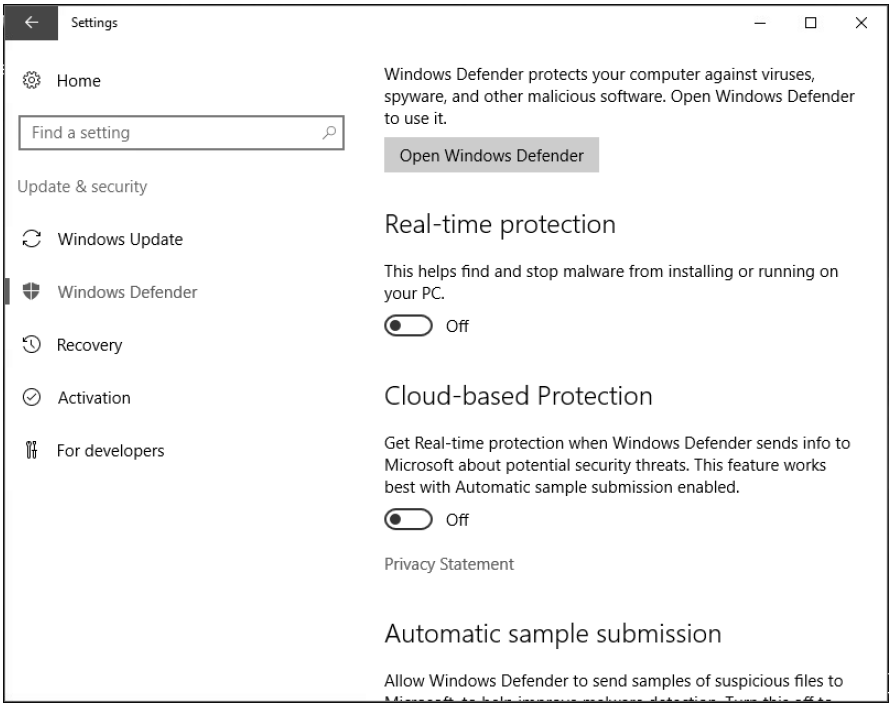

Abb. 6.1: Deaktivieren des Windows Defender

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Deaktivieren Sie den Windows Defender vorerst wirklich nur auf dem Sprunghost und lassen Sie ihn auf dem Fileserver und dem Domain Controller weiterlaufen. Stellen Sie dort auch gern sicher, dass er mit allen aktuellen Updates versorgt ist. Dies wird Ihnen demonstrieren, dass ein schwaches Kettenglied oftmals ausreicht und es nahezu fahrlässig ist, sich nur auf das Vorhandensein eines Virenscanners zu verlassen.

6.1.3 Herunterladen von mimikatz

Stellen Sie bitte sicher, dass Sie mimikatz stets aus dem offiziellen GitHub-Repository von Benjamin Delpy beziehen:

`https://github.com/gentilkiwi/mimikatz`

Das Herunterladen und Kompilieren des Quellcodes werde ich hier nicht weiter thematisieren, stattdessen werde ich der Einfachheit halber die vorkompilierten Binaries aus dem Repository verwenden, die unter folgender Adresse zu finden sind:

`https://github.com/gentilkiwi/mimikatz/releases`

Spätestens dann, wenn Sie sich mit dem Thema AV-Evasion näher befassen wollen, sollten Sie sich aber auch noch mal die Zeit nehmen und sich anschauen, wie Sie den Quellcode selbst kompilieren können. In Abbildung 6.2 sehen Sie die zum Zeitpunkt der Drucklegung des Buchs aktuellste Version von mimikatz 2.2.0.

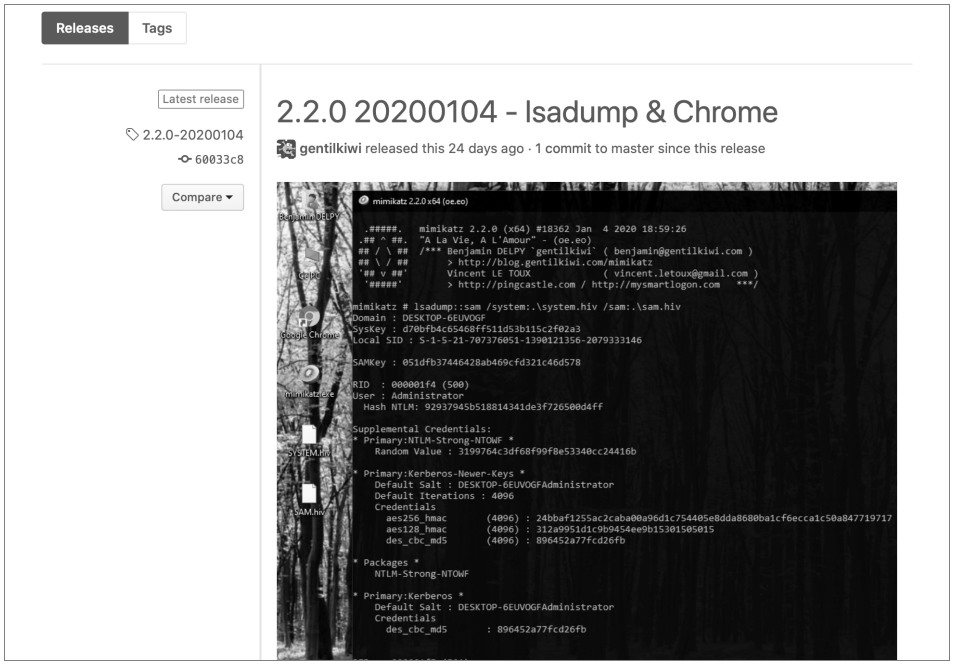

Abb. 6.2: Derzeit aktuelles Release von mimikatz 2.2.0

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Wechselnde Versionsnummern

Während des Schreibens dieses Buchs und auch zwischen den Auflagen werden regelmäßig neue mimikatz-Versionen durch Benjamin Delpy auf GitHub veröffentlicht.

Für den Funktionsumfang in den jeweiligen Demonstrationen hat sich dadurch bis zur Drucklegung dieses Buchs keine Änderung ergeben.

Wundern Sie sich also nicht, wenn auf den Screenshots immer die gleiche Version referenziert ist und nicht die neueste Version, die Sie auf GitHub vorfinden – das ist zu erwarten und ändert nichts an den gezeigten Angriffen!

Nachdem Sie den Virenscanner als Administrator deaktiviert haben, loggen Sie sich bitte mit dem niedrig privilegierten Domänenbenutzer ein, den Sie im Zuge der Laborinstallation angelegt haben, und laden `mimkatz_trunk.zip` für diesen Benutzer herunter.

Sollten Sie beim Downloaden von mimikatz mit dem Internet Explorer Probleme mit der *Internet Explorer hardened Configuration* bekommen, können Sie diese über den Server-Manager deaktivieren:

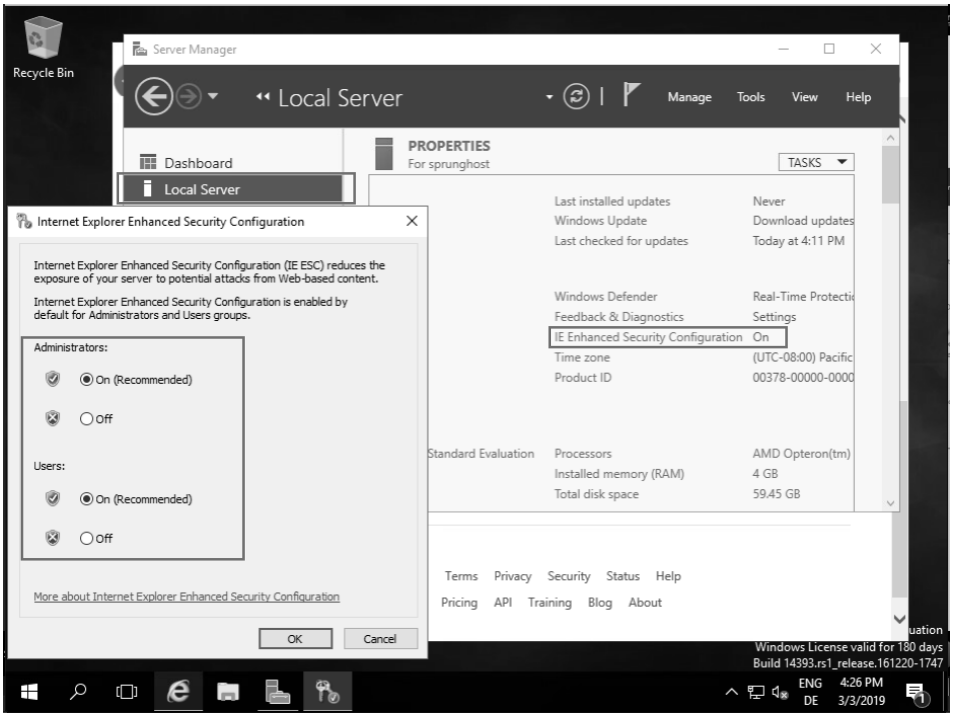

Abb. 6.3: Deaktivieren der IE Enhanced Security Configuration

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Vergessen Sie nicht, gegebenenfalls den Internet Explorer neu zu starten, nachdem Sie die Deaktivierung durchgeführt haben. Spätestens dann sollte der Download mittels IE funktionieren.

6.1.4 Erste Start- und Gehversuche

Nach dem Herunterladen und Entpacken können Sie die 64-Bit-Version von mimikatz aus dem Ordner `x64` starten.

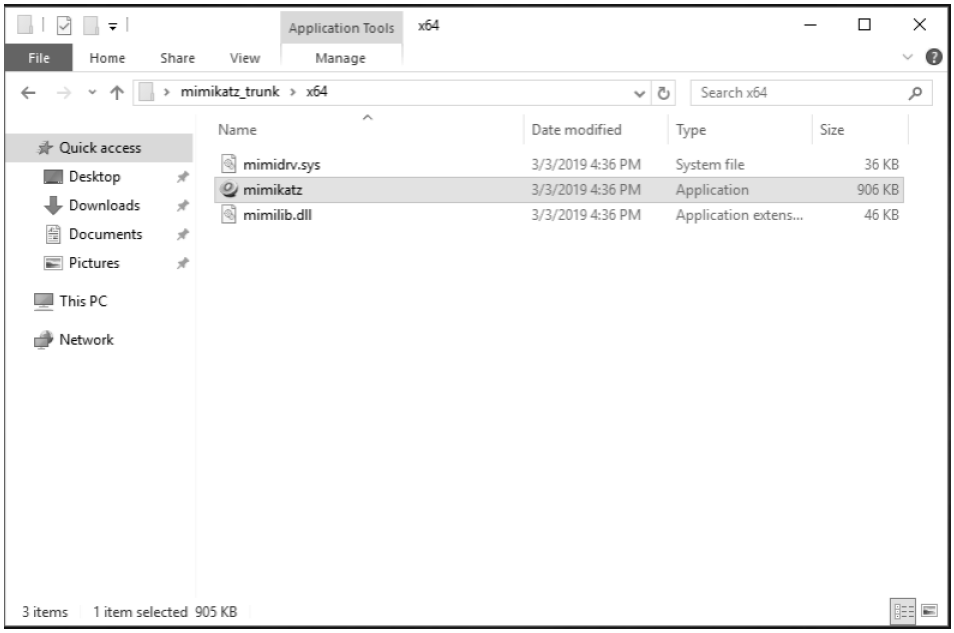

Abb. 6.4: mimikatz-X64-Version

Natürlich starten Sie auf einem 64-Bit-Betriebssystem eine 64-Bit-Version von mimikatz und auf einem 32-Bit-Betriebssystem die 32-Bit-Version. Sie können zwar auch die 32-Bit-Version von mimikatz auf einem 64-Bit-Windows starten, allerdings wird mimikatz aufgrund der WOW64-Abstrahierung dann nahezu nutzlos sein.

Nach dem Start werden Sie mit einem Banner und Versionsinformationen begrüßt.

Zur Syntax von mimikatz müssen Sie wissen, dass mimikatz nach Modulen strukturiert ist, die abgegrenzt mit zwei Doppelpunkten Unterbefehle ermöglichen.

Um zu sehen, welche Module es gibt, können Sie einfach `::` (zwei Doppelpunkte) ohne jegliches Modul oder irgendeinen Befehlsnamen eingeben, wie in Abbildung 6.5 zu sehen ist. Daraufhin präsentiert mimikatz zuerst eine Fehler-

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

meldung, die sagt, dass das eingegebene Modul nicht gefunden werden konnte. Dies können Sie getrost ignorieren. Wichtiger ist die darauffolgende Liste an verfügbaren Modulen.

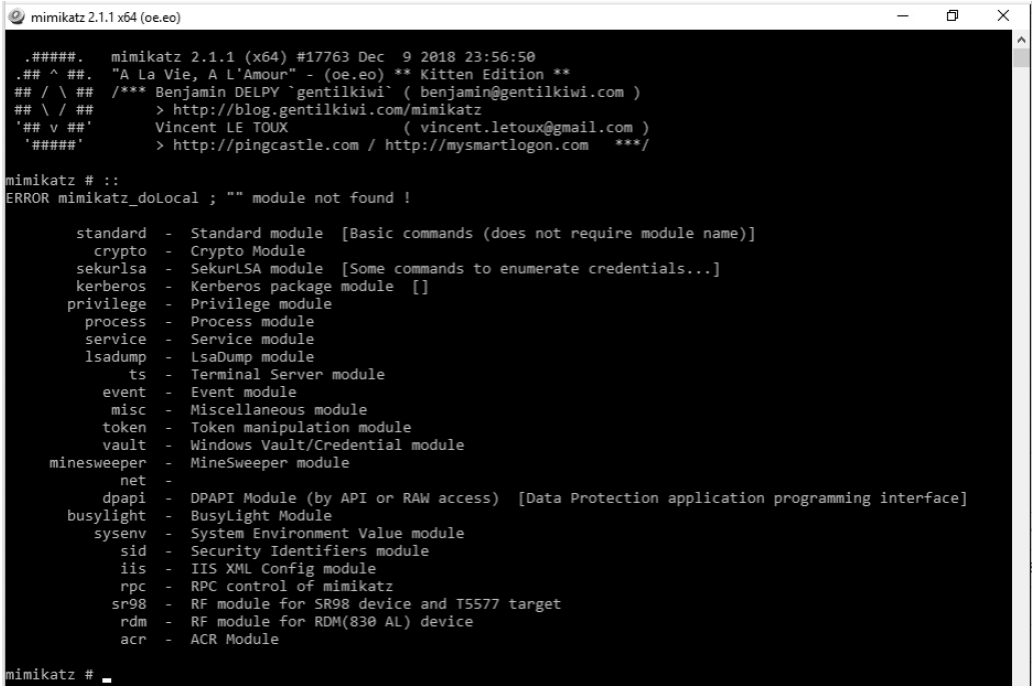

Abb. 6.5: Erster Start von mimikatz und Anzeigen der Befehle

Spätestens jetzt werden Sie den einen oder anderen Begriff aus den beiden Grundlagenkapiteln 4 und 5 wiederfinden, z. B.:

- `sekurlsa` – was eine absichtlich falsche Schreibweise von `secure` LSA darstellt – das Modul rund um die LSA
- `kerberos` – das Modul rund um die Interaktion mit Kerberos

Schauen Sie sich nun erst einmal das Modul `standard` an und prüfen Sie, welche Funktionen sich hinter diesem Modul verstecken, indem Sie `standard::` eingeben.

Erneut startet die Ausgabe mit einer Fehlermeldung, die Ihnen sagt, dass der Befehl »null« nicht gefunden wurde, gefolgt von einer Übersicht aller Befehle, die sich hinter dem `standard`-Modul befinden.

Zu guter Letzt sehen Sie den beispielhaften Aufruf der beiden Befehle `standard::answer` und `standard::version`, wie in Abbildung 6.6 gezeigt.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

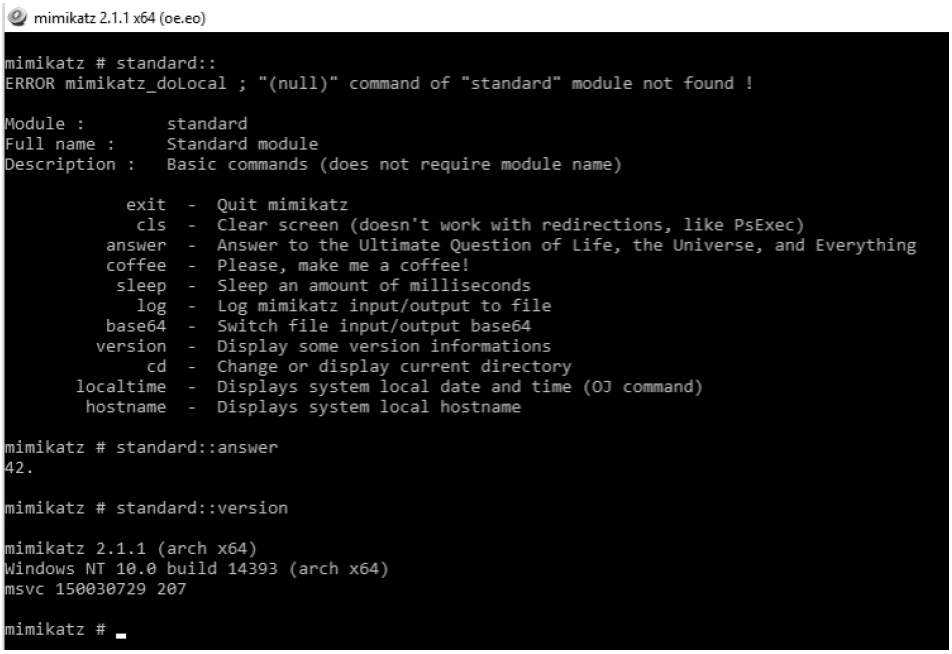

Abb. 6.6: Das Modul standard in mimikatz

6.1.5 Berechtigungen: Debug-Privilegien

Nachdem Sie sich nun die grundlegende Menüstruktur und Bedienung von mimikatz angeschaut haben, bleibt noch ein wichtiger letzter Aspekt, nämlich das Berechtigungsthema: mimikatz ist unter anderem dafür berühmt geworden, dass es Klartextpasswörter aus dem RAM extrahieren kann.

Geben Sie zum Testen den folgenden Befehl ein:

```
sekurlsa::logonPasswords
```

Sie werden von folgender Fehlermeldung begrüßt.

Abb. 6.7: Fehler beim Auslesen der Anmeldekennwörter

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Dies ist recht logisch, wenn man bedenkt, dass natürlich nicht jeder Benutzer einfach so das Recht hat, Passwörter aus dem RAM zu ziehen. Passwörter und andere sensitive Informationen werden von Windows im Speicherinhalt des `lsass.exe`-Prozesses verwaltet, der von Windows entsprechend geschützt wird.

Beenden Sie also mimikatz vorläufig und starten Sie es mit administrativen Rechten (Rechtsklick und RUN AS ADMINISTRATOR).

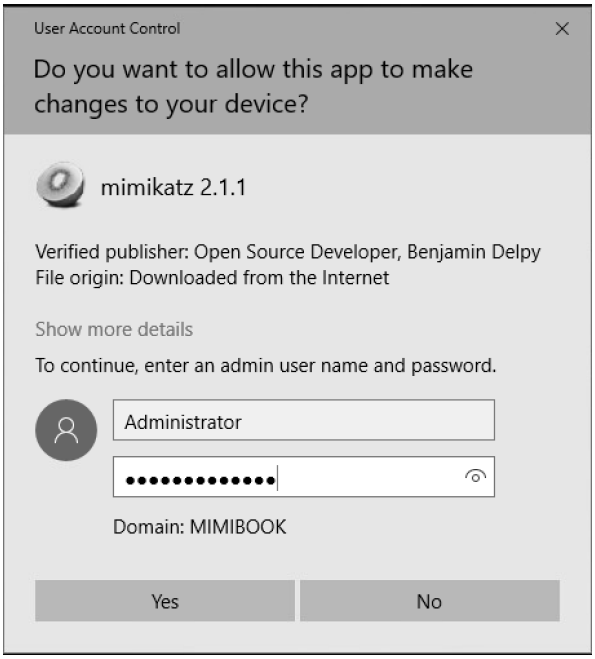

Abb. 6.8: Starten von mimikatz mit administrativen Rechten

Probieren Sie es jetzt noch einmal.

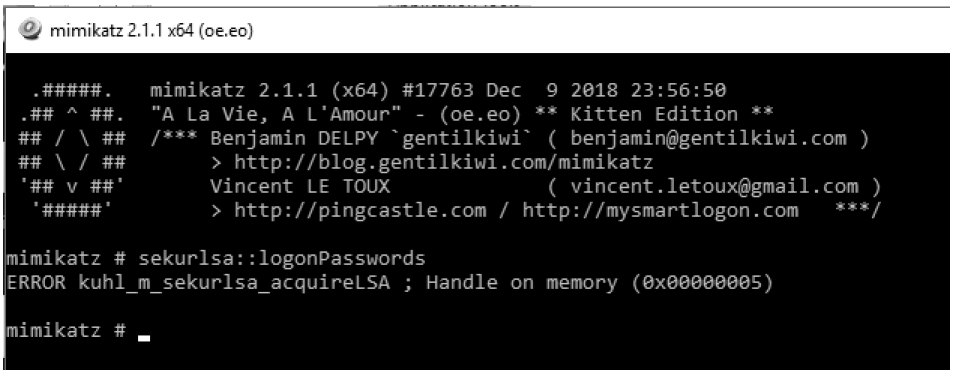

Abb. 6.9: Erneut Fehler beim Auslesen des Speichers

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Und wieder bekommen Sie den gleichen Fehler. Das liegt daran, dass der `lsass.exe`-Prozess im Kontext des SYSTEM-Benutzers läuft und selbst ein Administrator nicht auf dessen Arbeitsspeicherinhalt zugreifen darf (siehe Abbildung 6.10).

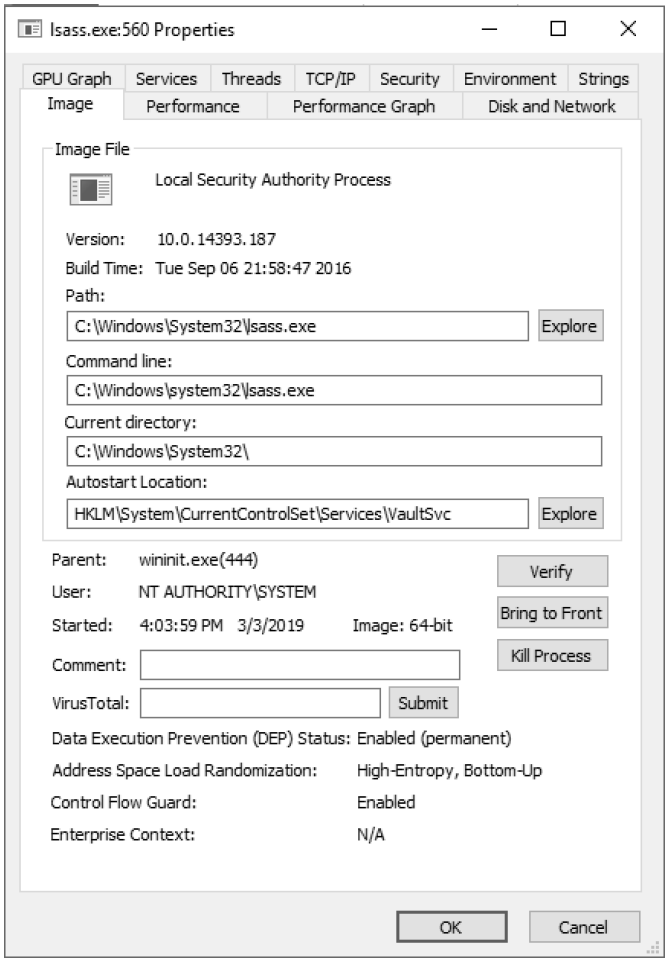

Abb. 6.10: lsass.exe-Prozesseigenschaften

Doch zum Glück gibt es auch hierfür eine Lösung. So darf sich der Administrator zum Debuggen an beliebige Prozesse andocken, auch an den LSA-Prozess. Einmal mit **Debug-Privilegien** angedockt, klappt dann auch das Extrahieren der Anmeldegeheimnisse mit mimikatz. Probieren Sie es einmal aus, indem Sie in Ihrem als Administrator gestarteten mimikatz den Befehl

```
privilege::debug
```


© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

eingeben, um sich Debug-Privilegien zu besorgen. Geben Sie dann erneut den Befehl

```
sekurlsa::logonPasswords
```

ein (siehe Abbildung 6.11).

Abb. 6.11: Erfolgreiche Ausgabe der Anmeldegeheimnisse

Nun kennen Sie den NTLM- und den SHA1-Hash sowie das Klartextpasswort `Buchadmin123!` des Domänenadministrator-Accounts, den ich genutzt habe, um mimikatz mit administrativen Rechten zu starten.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Dies ist natürlich sehr gestellt und erst der Anfang, aber es gibt Ihnen schon mal einen ersten Eindruck von der Macht von mimikatz und zeigt hoffentlich bereits eindrucksvoll, warum Sie einen sensitiven Account wie einen Domänenadministrator so selten wie möglich benutzen sollten. Denn sobald Sie ihn einsetzen, sind Ihre Passwörter und Passwort-Hashes potenziell an diesem System im Arbeitsspeicher gecacht.

6.2 Zusammenfassung

Sie haben in diesem Kapitel gesehen, wie sich mimikatz im Labor herunterladen und nach dem Deaktivieren des Windows Defender starten lässt. Über ein paar Basisbefehle konnten Sie außerdem die Syntax von mimikatz erproben. Zudem haben Sie gesehen, dass mimikatz seine volle Macht nur ausspielen kann, wenn Sie es mit administrativen Rechten starten, sodass es sich über Debug-Privilegien an den LSA-Prozess andocken kann.

Sie sind nun an dem Punkt angekommen, an dem alle Grundlagen und Voraussetzungen geklärt sind, und können im nächsten Kapitel mit den Angriffen starten.

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Stichwortverzeichnis

.kirbi-Datei 125

A

Access-Maske 203
    statisch 217
Active Directory 130
    dumpen 131
    Logs 150
Active Directory Security 46
Active-Directory-Datenbanken 52
AD *siehe* Active Directory
Administrative Center 60
Administrator
    lokal 109
AES Encryption Key 62
AES256 Encryption Key 120
Alarming 217
AMSI 177
Angriffsframework 209
AntiMalware Scan Interface 177
Application Blacklisting 180
Application Server 128
Arbeitsspeicherabbild 186
Artefakte 207, 216
Audit
    Zugriffslevel 201
Audit-Maske 200
Aufgabe 157, 162, 178, 184
Authentication Service 80, 81
AV-Evasion 90, 169, 174
AV-Scanner 89

B

Backdoor 135
BadRabbit 24
Banking-Trojaner 23
BareMetal-Hypervisor 34
Base64 209
Bash-Skript 192
Benjamin Delpy 17, 92
Benutzerberechtigungen 60
Benutzername
    Re-Validierung 143
Berechtigungsgruppen 63
Betriebssystemsprache 45
Binärdateien 89
Binaries 92
Binärmaske 203
Bitmuster 90
Blackhat 112, 177
BlueTeam 221
Bridged 38
Bruteforce 105, 151, 162, 163
Bundestag
    Hack 23

C

Carbanak 23
Changelog 22
CIFS Service Ticket 114, 128
Clientauthentifizierung 81
Clientbetriebssystem 59
Clientsystem
    Übernahme 152
Computer$-Account 144, 145
Computer$-Accounts
    Default-SPNs 146
copy-Befehl 184
Correlation Engine 218
Credential-Architektur 74
Credential-Provider 74
CredSSP.dll 77
Custom-Malware 90

D

Dashboard 217
Datenspeicherbrowser 186
dcpromo 48
dcsync 129, 131
Debug-Privilegien 96, 109
DES Encryption Key 62
DigitNotar 23
DLL 170
DNS 52
DNS-Server 47, 56
Docker 219

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

Domain Cached Credentials (DCC) 163
Übersicht 168
Domain Controller 35, 43
Benutzerverwaltung 46
LSA-Architektur 76
Domain-Member-System 101
Domänenadministrator-Account 58
Domänenberechtigungen 60
DSRS-Protokoll 131
Dumpen der Hashes 130

E

Einverständniserklärung 15
ELK 219
Empire 184, 209
ESXi *siehe* vSphere
Event-ID 202
Eventlog
kopieren 199
Eventlog Viewer 196
Exchange 80
Exchange Server 60

F

False Positives 209
Fileserver 56
Fileshares 80
berechtigen 65
Forensische Untersuchung 199
FQDN 119
FRITZ!Box 33
Funktionslevel 52

G

Gastbetriebssystem 35
Gen-Antivirenprodukte 90
Get-EventLog 199
GetSPN 155
Get-WinEvent 199
Global Catalog 52
Go 89
Golden Ticket 134
Abhängigkeiten 142
Lebenszeit 137
Voraussetzungen 136, 149
GPO 200
Graphical Identification and Authentication 74
Graylog 218
Open-Source-Version 218

H

Hardwarekonfiguration 34
Hardwareluxx 30, 31
Hash
ungesalzen 105
Hashcat 160
Hashdump 110
Haupteintrag 101
HELK 219
Homebrew 189, 192
Host-only 38
HP-MicroServer 28
Hypervisor 28, 33
BareMetal 34
vSphere 34

I

Incident-Response-Experte 143
Internet Explorer 93
Invoke-Kerberoast 160
Invoke-Mimikatz 169, 176, 209
detektieren 207
Protokolleinträge 179
ISE 157
ISO-Image 37

J

John-The-Ripper 159

K

Kali Linux 18
Kaspersky 90
KDC 135
Kerberoasting 15, 70, 151, 167
Definition 151
Übersicht 167
Kerberos 14, 79, 80, 95
Angriffe erkennen 221
Authentifizierung 153
Rollen 81
Kerberos Encryption Key 113, 145
Kerberos Golden Ticket 134
Übersicht 167
Kerberos Service Principal Name 69
Kerberos Silver Ticket 144, 167
Übersicht 167
Kerberos SPN
anlegen 69
Kerberos.dll 78
Kerberos-Authentifizierung 81
Kerberos-Protokoll 79, 88
Key Distribution Center 79, 81

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

kiwi 21
Klartextpasswort 14, 77, 99, 102, 173
Kompromittierung 143
krbtgt 83, 134
krbtgt-Account 143, 144
  dumpen 133

L

Labor 27
  Ausstattung 28
  Netzwerkplan 71
LAPS 111
LDAP-Filter 156
Legacy-Systeme 152
Lightweight Directory Access Protocol 80
Linux 189
LM-Hash 105
Local Administrator Password Solution 111
Local User Password Reuse 109
Logging 210
Log-Management 185
Lokale Gruppe 65
LSA *siehe* Windows Local Security Authority
lsadump 131, 186, 191
lsass.exe 98, 195, 197

M

Machine$-Account 154
macOS 166, 189
Member-Server 35, 56
Memory Dump 186
  anfertigen 186
Memory-Snapshot 188
Menüstruktur 89
Metasploit 18, 21, 209
Metasploit-Meterpreter-Session 184
Meterpreter 21
Microsoft Advanced Threat Analytics 119
Microsoft LAPS 111
mimiception 132
mimikatz
  herunterladen 92
  Sitzungen 107
MIT 79
MS-Cache-2-Hash 164
Msv1_0.dll 78
Mutual Authentication 80

N

NegoExts.dll 78
Netlogon.dll 78
Netzwerkkonfiguration 38, 56
Netzwerklogs 210
Netzwerk-Sniffing 33
NotPetya 24
NTDS.DIT 131
ntds.dit 54
ntdsextract 130
NTLM 14, 78
  Authentifizierung 104
NTLM-Hash 104
NTLM-Passwort-Hash 76, 104
NTLMv2-Hash 164

O

Offline dumpen 130
Olympic Destroyer 24
OpenWRT 33
Outlook 80
Overpass-the-Hash (OtH) 114
  Auffälligkeit 119
  Übersicht 166

P

Pass-the-Hash (PtH) 104
  Übersicht 166
Pass-the-Key (PtK) 112, 120, 129, 166
  Übersicht 166
Pass-the-Service-Ticket 127
Pass-the-Ticket (PtT) 123
  Übersicht 166
  Varianten 124
Passwort cracken 162
Passwortänderungszeitraum 137
Passwort-Hashing-Algorithmus 62
Passwortmanagement 111
Passwort-Reset 143
Passwortrichtlinie 62
Pattern 89
pip3 189
Positive Hack Days 20
Post-Exploitation-Phase 101
Post-Exploitation-Techniken 152
PowerLine 179
PowerShell 198
  Aufrufe loggen 203
PowerShell Empire Framework 161
PowerShell Injection 186
PowerShell Remoting 172, 183
PowerShell v3 204
PowerShell v5 204
PowerShell Wrapper 180
PowerShell-Empire-Projekt 160
PowerShell-Logging
  erweitert 217

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

PowerShell-Skript 155
PowerSploit 170, 181
Präventive Schutzsysteme 90
pwer_pe_injcetion 191
Python 189
Python 2 189
Python 3 189

R

Rechte
  ausweiten 101
Registry 76
Registry Key 54
Remote Desktop Protocol (RDP) 38
Remote Session 106
Replay-Angriff 80
Report 217
Request for Comments 79
RFC 79
Rufus 34
Russinovich, Mark 193

S

SAM 75
SANS-Institut 156
Schannel.dll 78
Scope 135
Script Block Logging 205
Security Account Manager (SAM) 46
Security Onion 33
sekurlsa 95
Service Principal Name (SPN) 146
  frei erstellbarer 146
Service Principial Name
  Built-in 146
Service Session Key 84
Service Ticket 85, 124
  stehlen 127
Service-Account 70
Service-Account-Passwörter
  cracken 151
Session Key 83
Session Key Type 119, 123
SID 139
SIEM 185, 210
Silver Ticket 144
Single-Sign-on 80
Skripte
  Herkunft validieren 155
SMB/CIFS 84
Social Engineering 106
Sourcecode 21
SourceImage 198
Splunk 210
  anmelden 210
  Port 212
  SIEM 218
Splunk Universal Forwarder 213
Sprunghost 59, 74
SQL-Server 152
SSH 41
SSP-Layer 77
Switch 33
Syntax 89
Sysinternal 193
Sysmon 193
  Apps installieren 214
  installieren 194
Sysmon-Log 197
  automatisch auswerten 198
  filtern 199
Sysprep 40, 45
Systemrechte 109

T

TargetImage 198
Terminalserver 123
TGS Request 113
TGS *siehe* Ticket Granting Service
TGT *siehe* Ticket Granting Ticket
Threat Hunting 185, 219
Ticket Granting Service 80, 81
Ticket Granting Ticket 81, 113
  stehlen 124
Tim Medin 151
TLS-Authentifizierung 78
Token 208

U

Ubuntu 220
Upstream-DNS-Server 48
UTF8-Passwort 152

V

vCenter Converter 41
Verschleierung 111
Virenscanner 89, 92, 101
Virtuelle Maschine *siehe* VM
VM 27
  klonen 41
VMDK-Datei 56
vmkfstools 41
VM-Template
  erstellen 37
Volume Shadow Copy (VSS) 130

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161

vSphere 34, 186
Installation 34
Lizenzschlüssel 34

W

wce 186
WDigest 103
Wdigest.dll 77
WDigest-Credential-Provider 18
Whitelist 203
Wildcards 217
Windows 22, 189
Windows Defender 90, 91
deaktivieren 91
Windows Local Security Authority 73
Windows Security Eventlog 141
Windows Server 2016 35
Windows Server 2019 36
Windows-Domäne 43
Windows-Logs 193
Windows-Security-Architektur 74
Windows-Security-Eventlog
filtern 202
Windows-Security-Logging 193
Windows-Server-VM 27
Windows-Standard-Logs 200
Winlogbeat 220
WLAN-Access-Point 33
Wordlist 160
WOW64 94

X

XML 195

Y

Yara
stand-alone 192
Yara-File 186, 190
Yara-Regeln
anwenden 189
automatisieren 192

Z

Zentrales Logging 209
Zero-Day-Exploit 90

© des Titels »Penetration Testing mit mimikatz« (ISBN 9783747501610) 2021 by
mitp Verlags GmbH & Co. KG, Frechen. Nähere Informationen unter: http://www.mitp.de/0161