mitp

Sebastian
Brabetz

2. Auflage

# Penetration Testing mit mimikatz

## Das Praxis-Handbuch

**Hacking-Angriffe verstehen und Pentests durchführen**

Sebastian Brabetz

# Penetration Testing mit mimikatz

## Das Praxis-Handbuch

### Hacking-Angriffe verstehen und Pentests durchführen

mitp

**Bibliografische Information der Deutschen Nationalbibliothek**
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-0162-7
2. Auflage 2021

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082



Lektorat: Janina Bahlmann
Sprachkorrektorat: Sibylle Feldmann
Covergestaltung: Christian Kalkert
Coverbild: © teerawit/stock.adobe.com
Satz: III-satz, Husby, www.drei-satz.de

# Inhaltsverzeichnis

# 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.

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.

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

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!

Kapitel 1

# Einleitung

## 1.1 Ziel und Inhalt des Buchs

mimikatz hat wahrscheinlich jeder schon einmal gehört, der sich intensiver mit IT-Sicherheit auseinandersetzt. Über die Jahre hat sich mimikatz als eines der bekanntesten »Hacking-Tools« etabliert – nicht zuletzt als es für den Crypto-Trojaner NotPetya zweckentfremdet wurde, der in der zweiten Jahreshälfte 2017 um die Welt ging und unzählige Computer verschlüsselte.

Auch bei allen, die sich tiefgehend mit IT-Security auseinandersetzen, um z. B. Penetration-Tester zu werden oder als Verteidiger ihre Unternehmen zu schützen, ist mimikatz schnell im Gespräch.

mimikatz ist vor allem für die Funktion bekannt, dem Arbeitsspeicher eines PCs, auf dem mimikatz läuft, Klartextpasswörter zu entlocken. Das ist nicht verwunderlich, da Klartextpasswörter die am einfachsten zu verstehenden und weiterverwendbaren Geheimnisse darstellen, die man einem Computer entlocken kann.

Klartextpasswörter lassen sich ohne großes Verständnis dafür, wie Computersysteme und deren Sicherheitskonzepte funktionieren, weiterverwenden und beliebig an anderen Stellen ausprobieren. Nicht selten werden Passwörter für verschiedene Accounts, Dienste und Webseiten wiederverwendet, weshalb Klartextpasswörter oft zur Kompromittierung weiterer Daten und Systeme führen.

Auch liegt es in der Natur moderner Computersysteme, mittels sogenannter *Single-Sign-on-Mechanismen* User automatisch und bequem in alle Dienste komplexer IT-Systemlandschaften einzuloggen. Diese Vertrauensstellungen zwischen Systemen führen dazu, dass man mit einem Passwort nicht nur das System, von dem man es erhalten hat, kontrolliert, sondern auch unzählige weitere Ressourcen, wie z. B. E-Mail-Konten, Webseiten und Kollaborationsplattformen wie SharePoint und viele andere, anzapfen und auslesen kann.

## 1.2 Mehr als nur Klartextpasswörter

All das ist sehr effektiv und in den falschen Händen schon ziemlich gefährlich – aber auch sehr hilfreich, wenn es von Verteidigern eingesetzt wird, um zielgerichtet Awareness zu schaffen und systematisch Sicherheitslücken aufzudecken. Aller-

dings kann mimikatz deutlich mehr, als nur dem Arbeitsspeicher eines Windows-PCs Klartextpasswörter zu entlocken.

mimikatz ist quasi ein maßgeschneidertes Tool, um die in Windows-Domänen eingesetzten Sicherheitsmechanismen und Protokolle wie z. B. NTLM und Kerberos gezielt auszunutzen und sich mit deren Hilfe durch Windows-Domänen zu hacken.

Wie Sie in späteren Kapiteln lesen werden, ist Kerberos keine Erfindung von Microsoft und findet auch abseits von Windows Anwendung. Nicht selten werden Linux- oder Mac-Systeme mithilfe von Kerberos in Windows-Domänen integriert. mimikatz kann also auch genutzt werden, um diese Geräte anzugreifen oder über sie den Rest einer Windows-Domäne anzugreifen.

Folglich stellt mimikatz ein umfangreiches Werkzeug dar, insbesondere zum Ausnutzen des Kerberos-Protokolls.

## 1.3 Zielgruppe des Buchs und Voraussetzungen zum Verständnis

Jeder, der sich mit IT-Sicherheit befasst, sollte wissen, wie einfach es ist, selbst den aktuellsten Windows-Versionen Passwörter zu entlocken. Für IT-Sicherheitsverantwortliche in Umgebungen mit Windows-Domänen sollte ein Verständnis von mimikatz und den damit möglichen Angriffen daher zum Pflichtprogramm gehören.

Mit diesem Buch möchte ich Ihnen einen leicht verständlichen Einstieg in die Funktionalität von mimikatz und Windows-Domänen-Eskalation geben. Natürlich können Sie die Funktionsweise von mimikatz auch im Internet recherchieren. Doch ich möchte Ihnen mit diesem Buch die komplexen Hintergründe des Programms zusammenhängend und verständlich näherbringen. Dabei setze ich nur grundlegende Kenntnisse im Bereich der IT-Security voraus, sodass sich dieses Buch sowohl an Einsteiger als auch an langjährige Profis richtet.

Nach einer kleinen Historie zu mimikatz werde ich Ihnen zuerst aufzeigen, wie Sie sich eine kleine Testumgebung zum Nachspielen der Angriffe leicht aufbauen können.

Danach werde ich gezielt auf einige Grundlagen der Windows-Security-Architektur und auf das Kerberos-Protokoll eingehen, um die notwendigen Grundlagen für das Verständnis von mimikatz zu festigen.

Im Hauptteil des Buchs werde ich dann gängige Angriffstechniken, die durch mimikatz ermöglicht werden, im Labor Schritt für Schritt erläutern, sodass Sie diese bei Bedarf gern parallel durchspielen können.

Als kleines Highlight wird sich eines der Kapitel auch einer recht modernen Angriffstechnik – dem sogenannten Kerberoasting – widmen, die zwar nun auch schon seit ein paar Jahren bekannt, aber trotzdem noch nicht annährend jeder Firma in Deutschland ein Begriff ist.

Um die vorgestellten Angriffe und Techniken in diesem Buch nachzuvollziehen und zu üben, benötigen Sie keinen Zugriff auf eine lebendige Firmenumgebung. Heutzutage ist es recht einfach möglich, mit kostenlosen Virtualisierungslösungen und kostenlosen Microsoft-Testinstallationen komplexe Windows-Domänen nachzustellen. Sie können problemlos alle Techniken in einer sicheren, abgeschotteten Testumgebung erproben, ohne Gefahr zu laufen, die eigene Firma zu beeinträchtigen. Des Weiteren können Sie problemlos, auch ohne Zugriff auf eine Firmenumgebung, wertvolles Know-how aufbauen und für den produktiven Einsatz erproben.

Zusammenfassend, ist dieses Buch für jeden interessant, der noch kein mimikatz-Veteran ist und Interesse an IT-Security hat oder seinen Marktwert steigern möchte.

## 1.4 Rechtliches

Wahrscheinlich kommt kein Buch, das sich um IT-Security dreht, ohne einen entsprechenden Warnhinweis aus: Das unbedarfte und unkontrollierte Anwenden von Werkzeugen wie mimikatz kann (gegebenenfalls versehentlich) zu Straftaten führen. Es verstößt gegen deutsches Gesetz, IT-Systeme ohne Erlaubnis der Eigentümer auf Schwachstellen hin zu überprüfen oder gar Schwachstellen in diesen Systemen auszunutzen. Selbst mit Erlaubnis und Einverständniserklärung der Eigentümer kann es durchaus nicht rechtens sein, IT-Systeme zu auditieren. Nehmen wir einmal das Beispiel eines Mailservers in der eigenen Firma. Auf diesem Mailserver liegen gegebenenfalls vertrauliche oder private E-Mails, die dem deutschen Postgeheimnis entsprechend zu behandeln sind.

Auch Shared-Hosting-Umgebungen, wie sie z. B. bei jeglichen Cloud-Providern vorliegen, stellen ein Problem dar: Entdecken oder nutzen Sie gar eine Schwachstelle in der unterliegenden Infrastruktur des Cloud-Providers, können Sie gegebenenfalls an Daten anderer Nutzer dieser Infrastruktur gelangen. Dies gilt es unbedingt zu vermeiden und bedarf ganz klarer vertraglicher Regelungen mit dem jeweiligen Provider.

Lassen Sie sich hiervon aber nicht abschrecken. Sicherheitsaudits sind auch in diesen Umgebungen sehr nützlich und wichtig. Gute Cloud-Provider lassen Sicherheitsaudits unter abgesteckten Bedingungen zu.

Auch könnte der Internet-Service-Provider, über dessen Infrastruktur ein einfacher Portscan durchgeführt werden soll, Portscans verbieten. Viele Internet-Service-Provider haben hierzu Klauseln in den Verträgen. Gerade bei privaten Anschlüssen wird das Portscanning gern pauschal verboten. Ich selbst habe zwar noch keine

Fälle erlebt, bei denen Internet-Provider aufgrund des Verstoßes gegen dieses Verbot Anschlüsse gekündigt oder Kunden abgemahnt hätten, aber Sie gehen auf Nummer sicher, wenn Sie sich auch hier explizit eine Freigabe einholen.

Zu guter Letzt sollten Sie bedenken, dass es ein Kündigungsgrund sein kann, wenn Sie unbedarft mit mimikatz bei Ihrem Arbeitgeber experimentieren, selbst wenn Sie dabei nichts zerstören und nur gute Beweggründe haben.

### Die Einverständniserklärung

Zu jedem Penetrationstest und jedem Schwachstellenaudit gehört also immer eine schriftlich und vertraglich festgehaltene Einverständniserklärung des Eigentümers der Infrastruktur und aller beteiligten Provider. Vorlagen hierfür bekommen Sie beim Beauftragen von Schwachstellenscans und Penetrationstests bei professionellen Anbietern oder sicherlich auch frei verfügbar im Internet. Lassen Sie eine solche Vorlage aber vorsichtshalber durch Anwälte prüfen, bevor Sie größere Audits unternehmen.

**IANAL – I am not a Lawyer**

Dieses Buch stellt keine fundierte Rechtsberatung dar.

Ich möchte an dieser Stelle lediglich darauf hinweisen, dass die rechtlichen Rahmenbedingungen der IT-Security sehr ernst genommen werden müssen.

Im Zweifelsfall arbeiten Sie beim Lesen und Nachvollziehen dieses Buchs komplett auf virtuellen Maschinen auf Ihrem privaten Computer oder besuchen entsprechend vorbereitete Workshops oder Weiterbildungen, die abgeschottete Demo-Umgebungen bereitstellen.

## 1.5 Begrifflichkeiten und Glossar

Zu guter Letzt möchte ich darauf hinweisen, dass es bei tiefgehenden Themen wie mimikatz und IT-Security immer mal wieder vorkommen kann, dass Ihnen einzelne Begriffe oder Hintergründe unklar sind. Ich habe daher versucht, entsprechende Begriffe direkt im Text durch **Fettschrift** kenntlich zu machen und sie im Glossar am Ende des Buchs zu beschreiben.

Sollte Ihnen trotzdem beim Lesen noch etwas unklar sein, scheuen Sie sich nicht davor, den Begriff einfach in die Suchmaschine Ihrer Wahl einzugeben. Ich versichere Ihnen, dass Sie zu allen Inhalten in diesem Buch eine Vielzahl von Webseiten finden werden, die Ihnen die Hintergründe weiterführend erläutern.

Kapitel 2

# Hintergrundinformationen zu mimikatz

mimikatz ist eines der bekanntesten IT-Security-Werkzeuge auf der ganzen Welt. Doch wie kam es zur Entstehung von mimikatz?

Anscheinend war es ein Experiment:

> *»mimikatz is a tool I've made to learn C and make some experiments with Windows security.«*

So schreibt es jedenfalls Benjamin Delpy, der Programmierer von mimikatz, auf der GitHub-Projektseite:

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

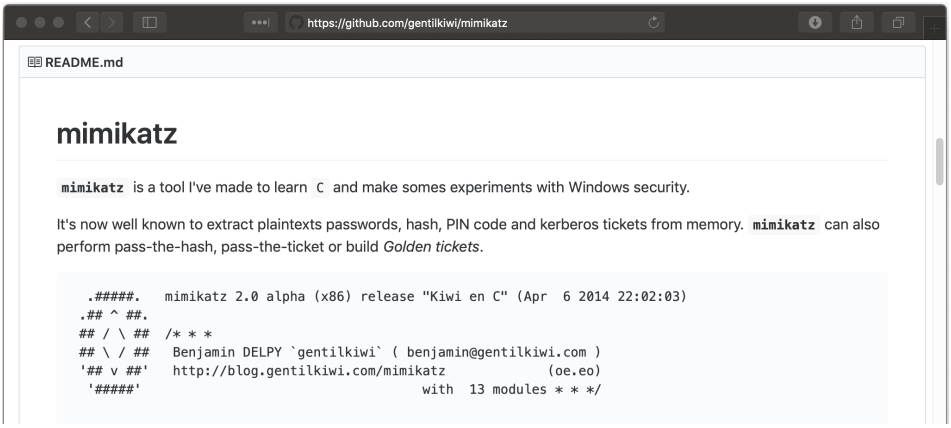


**Abb. 2.1:** mimikatz-Projektseite auf GitHub

Benjamin Delpy ist dem einen oder anderen Leser möglicherweise besser bekannt unter dem Nickname »gentilkiwi«. »Kiwi« meint übrigens sowohl die Frucht als auch den Vogel:

> *»Its symbol/icon is a kiwi, sometimes the animal, but mostly the fruit!«*

An dieser Stelle möchte ich Benjamin Delpy in Form seines Twitter-Profils eine Seite dieses Buchs widmen. Es ist nicht selbstverständlich, dass Menschen ihre Zeit

investieren, um Werkzeuge zu bauen, die sie der Welt kostenlos zur Verfügung stellen. Mit seiner Arbeit trägt Benjamin Delpy dazu bei, die Welt ein Stück weit sicherer zu machen, und er ermöglicht Menschen wie z. B. Pentestern oder Administratoren, auf Basis seines Programms ihren Lebensunterhalt zu verdienen.

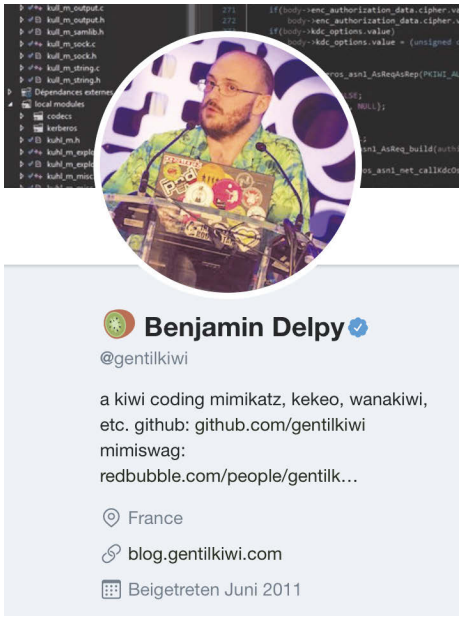


**Abb. 2.2:** Benjamin Delpys Twitter-Profil

Mit kostenloser Software wie mimikatz, **Kali Linux** sowie **Metasploit** und unzähligen weiteren Tools kann sich jeder, der das Geld für ein günstiges Notebook und genug Zeit investiert, wertvolles Know-how aneignen und damit Geld verdienen. Gleichzeitig steigert er auf diese Weise seinen eigenen Marktwert und somit sein Gehalt.

## 2.1 Die erste Version von mimikatz

mimikatz wird ständig weiterentwickelt! So ist der Funktionsumfang, während ich dieses Buch schreibe, deutlich größer als in den ersten Monaten und Jahren nach Veröffentlichung der ersten Version. In IT-Security-Kreisen wurde mimikatz zuerst als das Programm bekannt, das dem Arbeitsspeicher von Windows-Systemen Klartextpasswörter entlocken konnte.

Benjamin Delpy selbst schreibt in einer seiner öffentlich verfügbaren Präsentationen, dass mimikatz im Mai 2011 das erste Klartextpasswort aus dem WDigest-Credential-Provider von Windows extrahierte.


**Abb. 2.3:** Die Anfänge von mimikatz aus einer Präsentation von Benjamin Delpy (`http://blog.gentilkiwi.com/downloads/mimikatz-asfws.pdf`)

Danach folgten in kurzer Zeit viele weitere mächtige Funktionen – nicht zuletzt komplexe Kerberos-Integrationen. mimikatz befindet sich bis heute in der Entwicklung; sehr wahrscheinlich wird es auch zukünftig noch durch weitere spannende Funktionen ergänzt und damit neue Angriffe auf Windows-Systeme ermöglichen.

Wenn Sie an dieser Stelle noch nichts mit Begriffen wie Credential-Provider, WDigest oder Kerberos anfangen können oder nur eine grobe Vorstellung davon haben, was sie bedeuten könnten, seien Sie nicht abgeschreckt. Dieses Buch wird zur richtigen Zeit jeweils auf die notwendigen Hintergründe eingehen und es Ihnen ermöglichen, die vorgestellten Funktionen und Angriffe nachzuvollziehen.

## 2.2 Wie es zu der Open-Source-Veröffentlichung von mimikatz kam

Ich selbst bin erst kürzlich auf die Geschichte rund um die Open-Source-Veröffentlichung von mimikatz gestoßen, als ich das im November 2019 erschienene Buch *Sandworm* von Andy Greenberg gelesen habe.

In dem Buch geht Greenberg unter anderem auf die Geschichte rund um die Open-Source-Veröffentlichung von mimikatz durch Benjamin Delpy ein.

Ein Auszug dieser Geschichte wurde bereits 2017 in einem Artikel auf der Wired-Webseite veröffentlicht:

`https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/`

Im Jahr 2012 hat der damals 25 Jahre alte Benjamin Delpy einen Vortrag über mimikatz auf der Security-Konferenz »Positive Hack Days« gehalten. Man findet im Internet weiterhin die Ankündigung für diesen Talk:

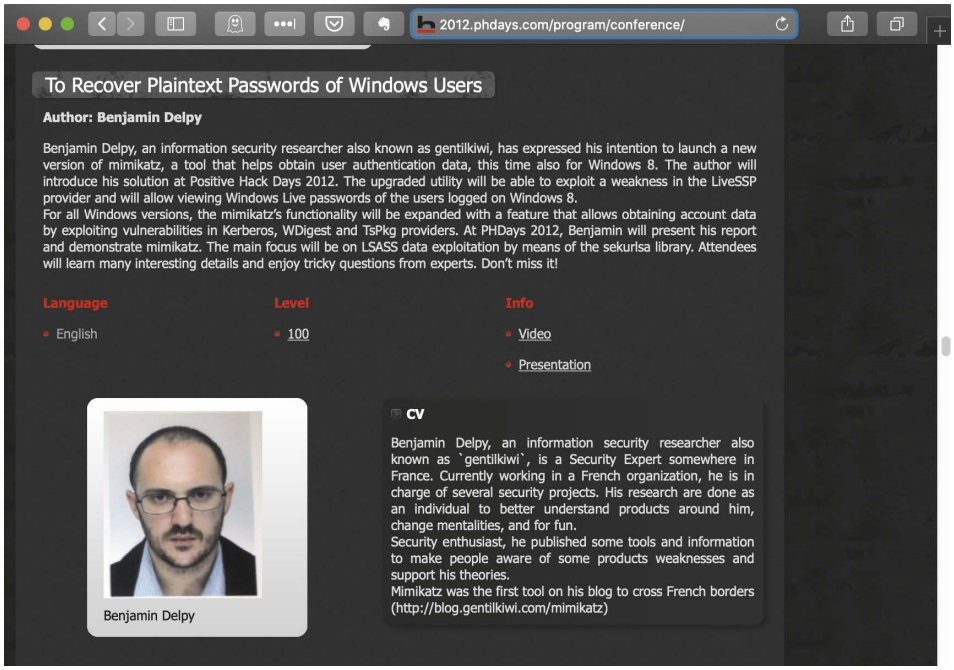


**Abb. 2.4:** Ankündigung des Vortrags für die Positive Hack Days

Benjamin Delpy reiste zwei Tage vor der Konferenz in Russland an und übernachtete im President Hotel in Moskau. Allerdings funktionierte das Internet in seinem Zimmer nicht, und Delpy begab sich zur Rezeption.

An der Rezeption wurde er dazu aufgefordert, in der Lobby zu warten, bis ein Techniker das Problem in seinem Zimmer behoben haben würde. Als Delpy zu seinem Zimmer zurückkehrte, fand er dort einen Mann im schwarzen Anzug an seinem eingeschalteten Notebook vor, das sich im Windows-Log-in-Bildschirm befand.

Es ist davon auszugehen, dass dieser Vorfall direkt mit seiner Präsentation für die anstehende Konferenz zusammenhing, da Delpy direkt nach seinem Vortrag er-

neut von einem weiteren Mann in schwarzem Anzug angesprochen und nachdrücklich dazu aufgefordert wurde, einen USB-Stick mit seiner Präsentation und dem Code von mimikatz auszuhändigen.

Zu diesem Zeitpunkt war mimikatz noch als Closed Source Binary durch Delpy veröffentlicht. Nach diesem Vorfall allerdings entschloss er sich noch in Russland dazu, den Sourcecode von mimikatz auf GitHub zu veröffentlichen, um solchen Vorfällen in Zukunft vorzubeugen und allen Ländern und Interessenten auf der Welt die gleiche Ausgangslage zu verschaffen.

## 2.3 mimikatz 2.0: kiwi ... und eine neue Befehlsstruktur

Im April 2014 wurde Version 2.0 von mimikatz mit dem Codenamen kiwi – wer hätte es gedacht? – eingeführt. Mit dieser zweiten Version hat sich die Befehlssyntax von mimikatz grundlegend geändert. Wenn Sie im Internet recherchieren oder ältere Bücher lesen, stolpern Sie somit gegebenenfalls über Kommandos, die so nicht mehr funktionieren und jetzt leicht abgewandelt eingegeben werden müssen.

Diese Befehlsänderungen sind nicht allzu komplex, und sobald man die neue Menüstruktur und die neue Syntax von mimikatz einmal verinnerlicht hat, findet man alle Funktionen sehr einfach und schnell wieder – trotzdem möchte ich bereits an dieser Stelle darauf hinweisen, um Verwirrung vorzubeugen.

Dieses Buch wird sich ausschließlich mit dem aktuellen Versionszweig 2.x von mimikatz und dessen Syntax befassen.

## 2.4 mimikatz und Metasploit

Es soll nicht unerwähnt bleiben, dass es schon seit Langem mimikatz-Module für die Metasploit-Payload-Meterpreter gibt. So erlaubt Ihnen Meterpreter, auf bereits übernommenen Windows-Systemen eine recht alte Version von mimikatz im 1.x-Versionszweig auf ein Zielsystem nachzuladen. Verwenden Sie dazu den Befehl

`load mimikatz`.

Der Meterpreter-Befehl

`load kiwi`

hingegen lädt zurzeit eine leicht veraltete, aber aus dem 2.x-Zweig stammende Version von mimikatz nach.

Warum gibt es dann überhaupt noch die Möglichkeit, alte Versionen aus dem 1.x-Versionszweig nachzuladen?

mimikatz 2.x ist nicht kompatibel mit alten Betriebssystemversionen wie Windows 2000 oder XP. Wenn Sie diesen alten Betriebssystemen z. B. bei einem Pentest be-

gegnen, ist es hilfreich, auf alte mimikatz-Versionen zurückgreifen zu können – und das ist durchaus häufig noch der Fall.

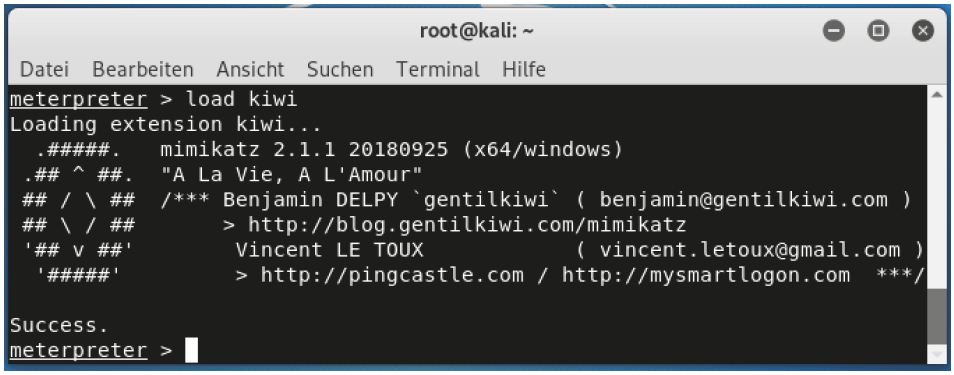


**Abb. 2.5:** Metasploit – Meterpreter – load kiwi

Beachten Sie bitte, dass dieser Abschnitt nur als kurze Referenz für den Umgang von mimikatz im Zusammenspiel mit Metasploit dient. Der Rest des Buchs dreht sich ausschließlich um eigenständige mimikatz-Versionen auf Windows-Systemen. Ein tiefgehendes Verständnis für Metasploit ist zwar immer von Nutzen, für dieses Buch aber nicht notwendig.

## 2.5 Neue Features: das Changelog im Blick behalten

Wie bereits beschrieben, wird mimikatz ständig weiterentwickelt. Daher ist es ratsam, regelmäßig die neuesten Releases von mimikatz unter

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

im Blick zu behalten.

Zum einen machen neue Windows-10-Versionen immer wieder Änderungen im Code notwendig, damit die Funktionalität von mimikatz erhalten bleibt. Zum anderen werden neben neuen grundlegenden Funktionalitäten – die neue Angriffe ermöglichen – auch regelmäßig kleinere Features ergänzt, die hilfreich im Alltag sein können.

## 2.6 Verwendung von mimikatz in vergangenen Hacks

Abschließen möchte ich dieses Kapitel mit einer kleinen Auflistung berühmter Hacks aus den Medien, bei denen nachweislich Teile des Codes von mimikatz zum Einsatz kamen:

### 2011 – DigitNotar

Im Jahr 2011 wurde die holländische Zertifizierungsstelle DigiNotar komplett kompromittiert, und die Schlüssel der Root-CA wurden entwendet.

Nachdem bekannt wurde, dass boshafte Zertifikate von DigiNotar im Umlauf waren und für schädliche Zwecke missbraucht wurden, übernahm die holländische Regierung die operative Leitung des Unternehmens und erklärte DigiNotar noch im selben Monat für bankrott.

Im Internet finden Sie einen umfangreichen Incident-Response-Report der Firma Fox-IT, die den Vorfall bearbeitet hat:

`http://cryptome.org/0005/diginotar-insec.pdf`

Der Bericht enthält zwar keine direkte Nennung von mimikatz, aber mit ein wenig Recherche können viele Anhaltspunkte zum Einsatz von mimikatz in diesem Hack gefunden werden.

### 2014 – Banking-Trojaner der Carbanak-Gruppe

Im Jahr 2014 wurde der Banking-Trojaner der Carbanak-Gruppe entdeckt. Die Firma Kaspersky veröffentlichte 2015 einen umfangreichen Report über die Gruppe und den Trojaner:

`https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf`

In diesem Report wird darauf hingewiesen, dass die Angreifer in den Zielnetzwerken unter anderem mimikatz benutzten, um sich weiter auszubreiten.

### 2017 – Russische Hacker im Deutschen Bundestag

2017 wurde bekannt, dass der Deutsche Bundestag durch russische Hacker infiltriert wurde. Die Zeitung *Die Zeit* hat hierzu einen sehr ausführlichen Artikel veröffentlicht:

`https://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland`

Ein Auszug aus diesem Artikel:

> *Eines der Programme, das sie verwenden, besteht nur aus ein paar Kommandozeilen. In der Hacker-Szene heißt es »mimikatz«, es lässt sich frei aus dem Internet herunterladen, Symbol: eine Kiwi.*
>
> *Mimikatz sucht gezielt nach Administratoren-Passwörtern. Und Mimikatz ist effektiv. Diesmal dauert es zwar nicht Stunden, sondern Tage, aber dann kontrollieren die Hacker fünf der sechs Administratoren-Accounts des Bundes-*