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!