
PASSWORD CRACKING
WITH KALI LINUX
DANIEL W. DIETERLE
@Cyberarms

PASSWORD CRACKING WITH KALI LINUX

Cover Image by Pete Linforth

Version 1

DEDICATION

To my family and friends for their unending support and encouragement. You all mean the world to me! Yes, I know, I said I wasn't ever going to write another book. But you know me well - I say that every time, and your support without judgement is why we are best friends!

"Every secret creates a potential failure point." — Bruce Schneier

"My primary goal of hacking was the intellectual curiosity, the seduction of adventure" - Kevin Mitnick

"Someone cracked my password, now I need to rename my puppy" - Unknown

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive that enemy; not on the chance of the enemy not attacking, but rather on the fact that we have made our position unassailable."

- Sun Tzu, The Art of War

"Behold, I send you forth as sheep in the midst of wolves: be ye therefore wise as serpents, and harmless as doves" - Matthew 10:16 (KJV)

ABOUT THE AUTHOR

Daniel W. Dieterle

Daniel W. Dieterle has worked in the IT field for over 20 years. During this time, he worked for a computer support company where he provided system and network support for hundreds of companies across Upstate New York and throughout Northern Pennsylvania. He also worked in a Fortune 500 Corporate Data Center, an Ivy League School's Computer Support Department and served as an Executive at an Electrical Engineering company and on the Board of Directors for a Non-Profit corporation.

For over the last 11 years Daniel has been completely focused on security as a Computer Security Researcher and Author. His articles have been published in international security magazines, and referenced by both technical entities and the media. His Kali Linux based books are used worldwide as a teaching & training resource for universities, technical training centers, government and private sector organizations. Daniel has assisted with creating and reviewing numerous security training classes, technical books and articles for publishing companies. He also enjoys helping out those new to the field.

E-mail: cyberarms@live.com
Website: cyberarms.wordpress.com, DanTheIoTMan.com
Twitter: @cyberarms

THANK YOU

Iron sharpens Iron and no one is an island unto themselves. Any successful project is always a team effort, and so much more in this case. I wanted to take a moment and give a special thanks to my friends, colleagues, and peers who helped with this book. So many offered invaluable wisdom, counsel and advice - sharing news, experiences, techniques and tools from the trenches. Your assistance, time, insight and input were so greatly appreciated - Thank you!

A Special Thanks To:

D. Cole – This book would not exist without you. Your constant support, knowledge, feedback, focus adjustments, encouragement, food pics, and your friendship is so very appreciated!

Bill Marcy – My book writing career would not exist without you. Your wisdom, insight, incredible knowledge and of course the occasional kick in the pants are invaluable to me. Thank you so much my friend!

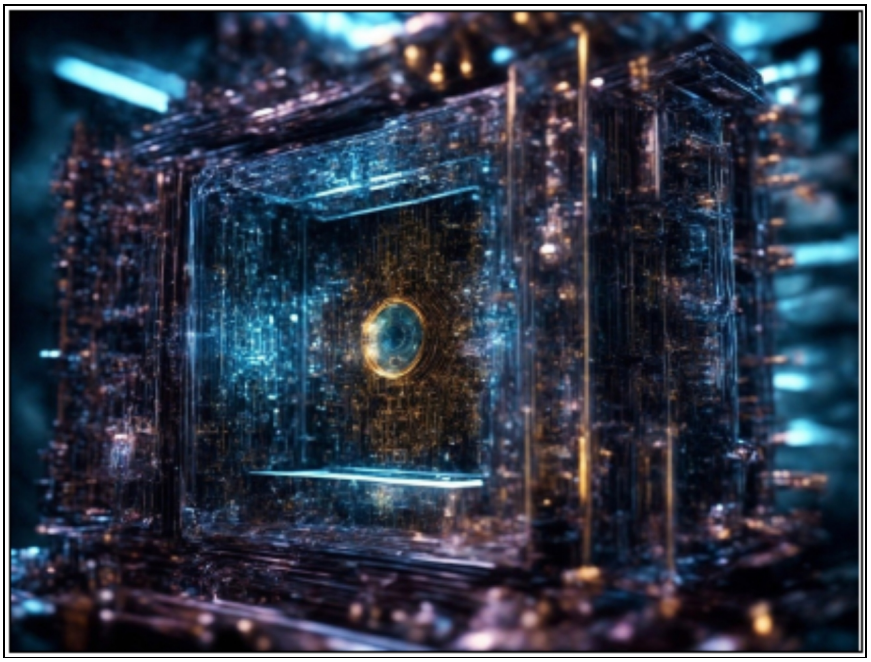
Alex – What would I do without you? I so appreciate your constant support and encouragement. Thank you for the long talks and your deep insight. For making the hard days easier with your unique viewpoints and wisdom. Thank you for all.

My Infosec Family – There are many of you that I don't see as friends, but as family. You know who you are - Thank you all so much for sharing your time, knowledge and friendship with me.

Book Reviewers – Thank you to Bill Marcy, D. Cole and Sudo Zues for reviewing chapters and providing exceptional feedback.

CONTENTS

CHAPTER 1
A Journey into Attacking Password Security



In an age where our lives are intricately woven into the digital fabric, safeguarding personal information is of paramount importance. As security-conscious individuals navigating the vast expanse of cyberspace, understanding the significance of cybersecurity and the crucial role ethical hacking plays in fortifying virtual boundaries becomes essential. This book takes readers on a journey into the realm of authentication hacking, with a specific focus on the art and science of password cracking, unveiling the layers of security that shield our digital identities.

Password cracking, often considered the proverbial skeleton key of cybersecurity, is an intriguing area of study that delves into deciphering and exploiting weak links in digital defenses. This exploration leads us into the arsenal of password cracking tools—sophisticated instruments wielded by Pentesters and Red Teams to assess and strengthen digital fortifications, and by attackers seeking unauthorized access. Navigating this technological landscape, we will unravel the complexities of these tools, demystifying their functionality and shedding light on their applications in the realm of cybersecurity.

As we delve into the intricacies of password cracking, it becomes apparent that it is both an art and a science. The process involves understanding encryption algorithms, exploiting vulnerabilities, and employing various techniques to unveil passwords hidden behind layers of security. This book aims to provide readers with a comprehensive understanding of these methodologies, empowering them with knowledge that can be used to bolster defenses or assess vulnerabilities.

Windows, as one of the predominant operating systems shaping the corporate digital world, becomes a focal point in our learning adventure. We will begin our journey with a look into the intricacies of Windows password security, and the technology it uses to create passwords. Understanding the basics of how Windows safeguards its users' credentials is not only valuable knowledge for aspiring Ethical Hackers and Pentesters but is also pivotal for anyone in the realm of security seeking to fortify their own digital presence in an interconnected world. We will then dive deep into the tools, tactics and techniques of breaking this security and cracking passwords, opening up the keys to the digital kingdom, and cracking the digital fortress.

PRE-REQUISITES AND SCOPE

This book is geared towards computer security professionals that want to increase their skills at cracking passwords. It is also written for the cybersecurity student who wants to learn more about password security. The book assumes that the reader is already familiar with basic Windows and Linux security topics, and is comfortable with using Kali Linux. Though the introduction section on Windows Kerberos theory is rather challenging, it is a very complex topic, the rest of the book is written so if someone isn't that familiar with the topic, they can, "learn by doing". This book is part of my, "Security Testing with Kali Linux" series. I highly suggest the reader be familiar with the topics in both my Basic and Advanced Security Testing with Kali Linux books before tackling this one.

LAB SETUP

For the lab setup I used Kali Linux 2023, Windows 11, Windows Server 2022, and Metasploitable2 in VMWare. The systems were setup so all could communicate together. The Windows Server was setup as a Domain Controller and then modified with SecFrame's "Bad Blood" to add thousands of unsecure Active Directory Objects. For those who have read my other books, this is the exact same lab setup.

As Bad Blood creates random users and objects every time you run it, you will never have the exact same Active Directory environment as the one I use in this book. But the concepts and techniques are solid, you should be able to run the commands on any current Windows Server lab target system with similar results – as long as you have permission to do so.

I cover creating a testing lab in my Basic Security Testing with Kali Linux book. I cover setting up Windows Server 2022 and BadBlood in my Advanced Security Testing with Kali Linux book. Just make sure that your systems are secured from outside access, are in a standalone and firewalled system, and do not have access to production systems as they will be vulnerable.

- VMWare Workstation Player - **https://www.vmware.com/products/workstation-player.html**
- Kali Virtual Machine Download - **https://www.kali.org/get-kali/#kali-virtual-machines**
- Metasploitable2 Download - **https://sourceforge.net/projects/metasploitable/**
- Windows 11 Eval VM Download - **https://developer.microsoft.com/en-**

us/windows/downloads/virtual-machines/

- ➢ Windows Server 2022 Eval Download - **https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022**
- ➢ Bad Blood Documentation - **https://secframe.com/docs/badblood/whatisbadblood/**

You can use a lab setup using whatever virtual environment that you wish. Though be sure to properly secure it as you will be using vulnerable virtual machines. If you are totally unfamiliar with setting up a testing lab, check out the Bonus Chapter at the end of this book!

ETHICAL HACKING ISSUES

In Ethical Hacking & Pentesting, a security tester basically acts like a hacker. They use tools and techniques that a hacker would most likely use to test a target network's security. The difference being they are hired by the company to test security and when done reveal to the leadership team how they got in and what they can do to plug the holes. The biggest issue I see in using these techniques is ethics and law. Some security testing techniques covered in this book are actually illegal to do in some areas. So, it is important that users check their Local, State and Federal laws before using the information in this book.

Also, you may have some users that try to use Kali Linux or other Ethical Hacking tools on a network that they do not have permission to do so. Or they will try to use a technique they learned, but may have not mastered on a production network. All of these are potential legal and ethical issues. Never run security tools against systems that you do not have express written permission to do so. In addition, it is always best to run tests that could modify data or possibly cause system instability on an offline, non-production replica of the network, and analyzing the results, before ever attempting to use them on live systems.

DISCLAIMER

Never try to gain access to a computer you do not own, or security test a network or computer when you do not have written permission to do so. Doing so could leave you facing legal prosecution and you could end up in jail.

The information in this book is for educational purposes only!

There are many issues and technologies that you would run into in a live environment that are not covered in this material. This book only demonstrates some of the most basic usage of the tools covered and should not be considered as an all-inclusive manual to Ethical hacking or Pentesting.

I did not create any of the tools or software programs covered in this book, nor am I a representative of Kali Linux, Offensive Security or Microsoft. Any errors, mistakes, or tutorial goofs in this book are solely mine and should not reflect on the tool creators. Every exercise in this book worked at the time of this writing. Tool usage, capabilities and links change over time, if the information presented here no longer works, please check the tool creator's website for the latest information. Thank you to the developers of Kali Linux for creating a spectacular product and thanks to the individual tool creators, you are all doing an amazing job and are helping secure systems worldwide!

WHAT WE WILL COVER IN OUR JOURNEY

In the first chapter, we will cover a basic introduction to the Windows foundational security authentication protocols Kerberos and NTLM. Both of these protocols create encrypted passkeys - tickets for Kerberos, and hashes for NTLM. For simplicity's sake, I will call both of these "password hashes" throughout the book. We will then cover some of the popular tools and techniques used to obtain these hashes.

We then take an extensive look at wordlists. Wordlists are the foundation to password cracking. Using a good wordlist will greatly increase your chances and speed of password cracking. We will cover how to find, create or generate effectual wordlists for password cracking. This includes using tools to create custom wordlists. Then we will dive into the actual cracking tools. How Wordlists are used by cracking programs to unlock access. In the

chapters ahead we will briefly cover John the Ripper and then take a deep dive, multiple chapters look at the pre-eminent password cracking tool, Hashcat.

First up, how do we obtain hashes for cracking? We will take a look at how the Kerberos and NTLM Authentication protocols work in Windows and then how to pull hashes from them. Strap in, buckle up, this is going to be a wild ride!