White Hat Hacking and Password Cracking

A project by Nate Otting, Joshua Mata, and Everett Getchell

**Foreword: Why we chose this subject as our project**

Most often we see hackers in movies as morally questionable, but it is good to know that not all hackers are fighting to take our information, but instead to find ways to protect them.

To explore white hat hacking and its essential role in protecting digital systems with ethical hacking practices and professional hacking techniques.

White hat hackers can provide insight into what a company or body needs to do when it comes to hardening systems or networks

**Objective of the project**

To define, explain, and give credit to white hat hackers, for making cyber security more effective and efficient, and to display how password cracking can be performed more easily than one may think and to provide insights on how to harden passwords and log ins, as well as other alternatives.

**Project Management Timeline**

**A screenshot of a computer

Description automatically generated**

**QR code Linking to our GitHub Repository:**

A qr code on a white background

Description automatically generated

<https://github.com/egetche/CompSystemsSecProject>

**Section I: What exactly is a White Hat in terms of computer security?**

In computer security, "white hat” refers to an ethical hacker or cybersecurity professional who uses their skills and techniques to identify and fix security vulnerabilities in different systems, networks, and applications. White hats usually operate within legal and ethical boundaries, with the primary goal of improving security and preventing unauthorized access or malicious activities and exploits. White hat hackers go through a lot of training to get certifications to increase their expertise in cybersecurity like the CompTIA Security+ certificate. They also increase their skills in programming languages, scripting languages, network analysis, cryptography, and reverse engineering.

**Section II: What sets them apart from other types of hackers?**

When it comes to computer security, there are three major “sides” of hacking. There are people who use hacking tools and other software for malicious intent or for personal gain, and these are known colloquially as “Black Hat” hackers. On the other hand, there are those who use such tools for the benefit of either individuals or companies. These hackers only use their skills and tools to test security systems and to locate vulnerabilities within an environment. These are known as “White Hat” hackers, and they are people who utilize their methods ethically and by the law. In between the two are the “Grey Hat” hackers, who are morally ambiguous and are not the focus of this presentation.

**Section III: The importance of White Hats in today’s online ecosystem**

Every corporate entity and every enterprise body uses an online-based system in some form. Companies that are responsible for the maintenance and protection of the data of countless users like banks, accounting firms, state firms and insurance companies are all big targets for threat actors who would benefit from the theft of user data. This is where White Hat hackers come into play- they are hired by a company to test their security systems, and to infiltrate (within preset confines) different layers of the company’s infrastructure, and to detect these vulnerabilities. They then inform the security officers of the company what the best course of action to take would be.

**Section IV: Famous White Hat Hackers**

Kevin Mitnick: First accused of being unethically hacking and tried as a black hat before receiving support from the public before being released becoming a white hat and helping law firms dubbed by many as the #1 top ethical hacker for his exploits with older technology and social engineering, a part of the Ghost Global Team which does Pen testing, Red Team Engagements, Mobile App Pen test, and social engineering testing.

Charlie Miller: The man with a PhD who won the “Super Bowl of Hacking” event four separate occasions, who was the first to exploit the iPhone, which he did the same for the android on its release and managed to exploit the iPhone via SMS message and has been hacking into automotive cars

Tsutomu Shimomura: a Security Consultant works with the National Security agency and worked heavily with the FBI to capture Kevin Mitnick, who was still deemed a criminal at the time.

Greg Hoglund: Contributed great amounts of research to vulnerabilities and rootkits, which is a set of software tools that enables unauthorized users to gain control of a computer system without detection, also created one of the first network vulnerability scanners

HD Moore: Discovered many security risks and vulnerabilities, one of which being Metasploit framework, an open-source pen testing platform.

**Section V: Timeline**

Stage 1: Planning

In this stage, it was a bit difficult for what we wanted to do as we initially wanted to see if it was possible to have a dummy account set up with our school’s security administrator, but that was deemed not possible for security purposes, which is to be expected. From there, we moved on to the idea of deploying a virtual machine or using a Raspberry Pi that is purposely vulnerable to see how from a security perspective one would consider hardening the system.

**Stage 2: Resources**

In this stage, we are gathering information on how we would go about our idea in practice. We expect to reach our set objective through the use of Kali Linux and Ubuntu Linux machines, as well as the use of SSH remote access, and a specific software known as Hashcat. In addition, we started to add information to our documents of importance with the different important white hats, and their achievements as well as important dates that white hats pushed for an achievement. It seems that using an Ubuntu machine was not feasible, as the password encryption method used by modern versions of Ubuntu could not be cracked by Hashcat. As a result, we had to transition to the use of a Windows machine.

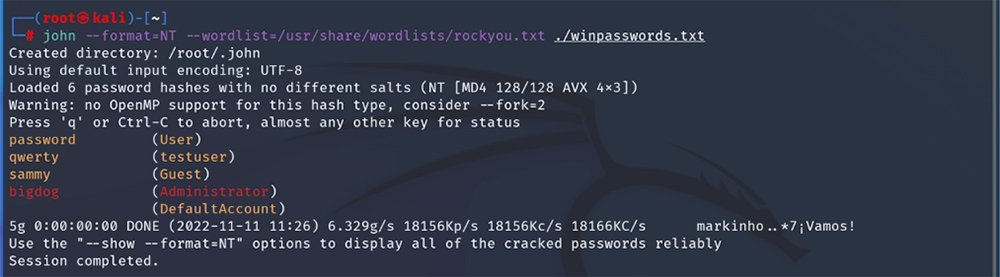
**Section V, Addendum I: Important Dates**

Begun in the Late 1960s- being first called “tiger teams” which were what white hats were originally called and were involved with “bug-bounties” which were monetary rewards for discovering or finding vulnerabilities. Hacking derived from the 1960s, used by engineering students to find more optimal ways to use machines. In 1995, Kevin Mitnick is pursued and captured by the FBI and Tsutomu Shimomura. Also in 1995, John Patrick coins the term “ethical hacking”, following this ethical hacking becomes a legitimate profession. In 1997, Nmap is first released it will evolve from there into a major tool for ethical hacking. In 2008 Ethereal is rewritten and remade into Wireshark version 1.0, becoming a new helpful tool for ethical hacking.

**Section VI: How we replicated what a White Hat would do**

Originally, we attempted to perform password cracking like a white hat would do to help get into a user’s locked account. We tried to use Hashcat but there were quite a few technological limitations. It was an authentic cyber security experience of trying something, it not working, and then not knowing why it will not work. After many attempts to figure out the problems as well as contacting the developers of Hashcat, we were told the best course of action is to move on, and to try using something else. That is the best and only course of action you can take sometimes. In our project, the intended purpose was to simulate helping someone who has lost access to their account regain access to their account through password recovery. As it turns out, Hashcat was not needed to recover their password. After being advised by a developer of Hashcat to use something else, we kept our priorities straight and got the job done using John the Ripper. Although using John the Ripper was easier than using Hashcat that was exactly what was needed to get the job done. What we did was we used Kali Linux with John the Ripper installed to use the rockyou.txt wordlist file that comes preinstalled with Kali to test against the passwords for another machine. The hashes of each password in rockyou.txt would be put against the machine that needed to be recovered until the correct hash was met, and the correct password was determined.



**Section VII: Conclusion of our report**

In conclusion, we did what we set out to do for this project in researching white hat hackers and giving them credit, though we need to give them a lot more credit after trying some of the things they do for ourselves. Ethical hacking like cracking passwords and penetration testing can be hard and sometimes it is not worth the time to try and find out what is wrong but find something else or some way else to be right. Using many different tools and techniques white hat hackers get the job done but we rarely ever see it or hear about it. They are heroes on the scale of police and firefighters, saving people’s online and internet lives. Lots of people’s information is on the internet now and the white hat hackers keep it a safer place for people to be.

**Section VIII: Works Cited**

*Leveraging white hat hackers for Enhanced Cyber Security: Navigating legal challenges*. Gowling WLG. (n.d.). <https://gowlingwlg.com/en/insights-resources/articles/2023/white-hat-hackers-enhanced-cyber-security/>

*History of ethical hacking 1960s to today: RedTeam Blogs*. RedTeam Hacker Academy. (2023, March 2). <https://redteamacademy.com/history-of-ethical-hacking/>

*What is ethical (white hat) hacking: CEH certification: Imperva*. Learning Center. (2023, December 20). <https://www.imperva.com/learn/application-security/ethical-hacking/>

*The history and future of Nmap: Nmap network scanning*. The History and Future of Nmap | Nmap Network Scanning. (n.d.). <https://nmap.org/book/history-future.html>

*1.4. A brief history of wireshark*. (n.d.). 1.4 A brief history of wireshark <https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html>

*Great rivalries in cybersecurity: Tsutomu Shimomura vs. Kevin Mitnick*. Online Masters Degree in Cybersecurity | Guide to Cybersecurity Graduate Programs. (2020, October 9). <https://www.cybersecurityeducationguides.org/tsutomu-shimomura-vs-kevin-mitnick/>

Kelly Jackson Higgins, E.-C. (2023, December 12). *HD moore unplugged*. Dark Reading. <https://www.darkreading.com/cyber-risk/hd-moore-unplugged>

*5 famous White Hat Hackers You should know. King University Online. (2020, February 27).* [*https://online.king.edu/news/5-famous-white-hat-hackers-you-should-know/*](https://online.king.edu/news/5-famous-white-hat-hackers-you-should-know/)

*U, C. (2021, December 1). The top 10 white hatters. Datatechvibe.* [*https://datatechvibe.com/interviews/the-top-10-white-hatters/*](https://datatechvibe.com/interviews/the-top-10-white-hatters/)

*Top 18 famous ethical hackers: The world has ever known. KnowledgeHut. (2024, January 17).* [*https://www.knowledgehut.com/blog/security/most-famous-ethical-hackers*](https://www.knowledgehut.com/blog/security/most-famous-ethical-hackers)

*Consulting, M. S. (n.d.). The global ghost team: Expert pentesting services: Mitnick Security. The Global Ghost Team | Expert Pentesting Services | Mitnick Security.* [*https://www.mitnicksecurity.com/global-ghost-team*](https://www.mitnicksecurity.com/global-ghost-team)

*1.4. A brief history of Wireshark. (n.d.).*[*https://www.wireshark.org/docs/wsug\_html\_chunked/ChIntroHistory.html*](https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html)

*The History and Future of NMAP | NMAP Network Scanning. (n.d.).*[*https://nmap.org/book/history-future.html*](https://nmap.org/book/history-future.html)