**Term Project Draft - Black Hat Hacking and White Hat Hacking (Ethical Hacking)**

Jaycee Welcome

Saint Leo University

COM-203-CA01: Computer Systems

Professor Weicht

March 23rd, 2025

**Introduction**

**Impact on Cyber Security**

The act of Hacking is gaining unauthorized access to a computer system or network with the intention of stealing or manipulating data Kaspersky (2022). Hacking has impacted the world of Cybersecurity greatly. Black hat hacking is the practice of attaining unauthorized access to a computer system or network to proceed with illegal activities such as data theft, system disruption, etc. White hat hacking (ethical hacking) is when hacking skills are used to address vulnerabilities in systems to help improve their cybersecurity to avoid hackers.

Firstly, I’ll talk about how black hat hacking can impact Cybersecurity. Black Hat hacking has caused Cybersecurity professionals major mental stress. For example, The Solar Winds hack, which was a major hack that affected many organizations and the US government. These hackers gained access to networks and systems and the data of SolarWinds customers which included more than 30,000 public and private organizations. They inserted a malicious code in (SUNBURST) which created backdoors to access sensitive data, create new accounts, impersonate users, etc. Oladimehi, Kerner (2023).

Secondly, White Hat hacking has also impacted Cybersecurity but in a more positive way than Black Hat hacking. It has prevented the increase of Cyberattacks. These hackers conduct tests such as penetration tests and simulated attacks. For example, there was a white hat hacker in 2021 who discovered a vulnerability in the platform “Poly Network” which allowed the hacker to gain access to $600 million in cryptocurrency. Instead of stealing these funds, they promised to return it and eventually handed over the money along with a key which enabled the company to recover stolen assets. However, many people would argue that this hacker wasn’t a white hat hacker because of the many times the platform had to plead with them to get their money back, but they did return the money and told the platform that this was somewhat of a lesson for the platform to ensure that they are digitally protected to avoid other hackers in the future Browne (2021).

**The Purpose of this Paper**

The purpose of this paper is to inform people about the different types of hacking and how it impacts technology usage, which impacts the whole world essentially now that that technology is incredibly popular and is used by approximately 67.9% of the world as of February 2025 . DataReportal. (n.d.-a).

## ****Brief History of Ethical Hacking****

## ****History****

## The term “ethical hacking” was first used in 1995 by IBM Vice President John Patrick, even though the concept has existed for much longer.

## In the 1960s, the term “hacking” was used by engineering students to find ways to run machines to their best ability according to The Redteam. During the 1990s when the internet started to be used worldwide, the number of hackers increased. As the internet became widespread, so did personal computers. Personal data were stored in these computers and as this was common knowledge, hackers would try to gain access into the computer systems to gain this private information. This led to all hackers being seen as criminals. RedTeam Hacker Academy. (2025)

**The Role of White Hat Hackers**

We have already discussed what the definition of a white hat hacker is. The objectives of a white hat hacker are to identify and report vulnerabilities in computer systems and to improve security.

**Rules they must follow**

Being a white hat hacker, it is important that the hacking taking place is done legally, they have to have explicit permission of the target company first. This includes written authorization and agreeing on terms and conditions. Being an ethical hacker, comes with drawbacks, such as coming across sensitive data, for example, personal information, trade secrets etc. They must follow laws and regulations such as the Computer Fraud and Abuse Act (CFAA) in America or the General Data Protection Regulation (GDPR) in Europe. These hackers have to make detailed reports on their findings to the targeted organization that they’re working for, noting any vulnerabilities found, the impact, and recommended steps needed to improve their networks and systems. Also, because ethical hackers have the information of the targeted audience, as they need this information to access the systems and networks, they may need to sign non-disclosure agreements (NDAs) before conducting assessments, to protect the company’s data. Going against this agreement can lead to legal consequences HackerOne. (n.d.).

**Becoming a White Hat Hacker**

White Hat Hackers have to go through a lengthy process of learning the different skills and gaining certifications to prove their level of expertise. These hackers start by learning the basics of computing (computer systems and computer programming). They also have to learn to use the different operating systems, such as Windows, Linux and macOS, network concepts and programming languages. (Python, Java or C++).

## ****The Role of Black Hat Hackers****

Opposite to the White Hat Hacker, the Black Hat Hacker’s objective is for financial gain, data destruction, hacktivism (the use of hacking for a political, social or ideological purpose) etc.

**Techniques used**

Hackers use a range of techniques to get into computer systems. To name a few, they use malware, ransomware, phishing attacks, and social engineering to exploit software vulnerabilities Sangfor Technologies. (n.d.). The three most common techniques seen in 2024 and predicted for 2025 are social engineering, password attacks, and ransomware.

**Social Engineering**

Hackers use this technique as they create attacks that manipulate people into sharing their private personal information, manipulating them into downloading software that shouldn’t be downloaded, or even manipulating the user to send the hacker money (Ibm 2025).

The most common social engineering used by hackers is called “Phishing”, which is the practice of sending emails or other messages to reveal a person’s information (passwords and credit card numbers) Copado Team (2024).

**Password Attacks**

Another technique hackers use is password attacks. They employ various attacks including brute force, dictionary attacks, and password spraying. For example, using the example of password spraying, the hackers would use sets of common passwords and then use tools to try these passwords on people’s accounts on a popular online website Schrader (2024).

**Ransomware**

Ransomware is a type of malicious software hackers use to prevent you from accessing any systems on your computer. An example of this is “WannaCry”, which was a computer worm that which disabled people from accessing their accounts, giving all access to the hackers. With this advantage, they held people’s information for ransom, ranging from $300-$600 in Bitcoin. This malicious software targeted outdated versions of Microsoft Windows. This worm infected 200,000 computers in 150 countries which caused them all financial loss RSS. (n.d.).

## ****Debate****

## **When discussing hacking, there is Grey Hat Hacking, which is in between both White Hat Hacking and Black Hat Hacking. The ultimate debate that is seen today, is the argument on whether Grey Hat Hackers are ethical or unethical. It is known that White Hat Hacking is good and Black Hat Hacking is bad, but what about in between “Grey Hat Hacking”? I will be discussing the ethics of this type of hacker.**

## ****Grey Hat Hackers****

## **Grey Hat Hackers are in the middle. They are known to not ask for authorization but on the flip side, they don’t have the bad intentions that black hat hackers are driven by. Some common practices of these hackers are security testing, public disclosure, and dual intentions. Therefore, it depends on the circumstance and how they act to label them as ethical or unethical, it’s different for them all as opposed to white hat hackers (all good) and black hat hackers (all bad).** Jayaraman, N. (2023).

## ****Debate Against Hacking****

## **As there are many blurred lines, as seen with grey hat hackers it causes debate as they carry out illegal actions but still somewhat help organizations which leads people to question whether or not they should still be punished for breaking the rules. In addition, if companies put their trust in someone because they have good hacking skills, it can potentially backfire into the hacker hacking of the company’s system.**

## ****Debate For Hacking****

## **On the other hand, hacking can be used for good, which can bring great benefits to the companies/organizations/people being hacked. Seen with white hat hacking, there are many advantages, as stated before, they show vulnerabilities in a computer system, and they also provide detailed advice on what the company should improve according to their system protection. They carry out these hacks legally and follow protocols to be ethical. Therefore, many people argue that hacking should be accepted however, only if it’s used for good, and therefore should follow protocols to make sure there’s no fraudulent activity.**

## ****Conclusion****

## In conclusion, the term “hacking” covers a wide range of sub-topics. I’ve touched on the sub-topics: white hat hacking and black hat hacking, however, there are other sub-topics such as red hat hacking, blue hat hacking, and green hat hackers, which I haven’t discussed in this essay. Even though black hat hacking is unethical, it’s unlikely that the action of this will stop completely which is why I think that white hat hackers are extremely important and should be implemented in every organization which has an online presence or uses the technology in any way to store personal information. Therefore, ethical hacking plays a key role in online environments and creates a safe space for online users and people in everyday life.

## References:

## Kaspersky (2022). *What is hacking? And how do you prevent it* <https://usa.kaspersky.com/resource-center/definitions/what-is-hacking>

Oladimehi, Kerner (2023). SolarWinds hack <https://shorturl.at/kBPxc>

Browne (2021) *Hacker behind $600 million crypto heist* [https://shorturl.at/2GoEr](https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html)

DataReportal. (n.d.-a). *Digital around the world* <https://datareportal.com/global-digital-overview>

RedTeam Hacker Academy. (2025). *History of ethical hacking - evolution and impact*.<https://redteamacademy.com/history-of-ethical-hacking/>

HackerOne. (n.d.). *White Hat hackers: Techniques, tools, and how to become one*. <https://www.hackerone.com/knowledge-center/white-hat-hacker>

Sangfor Technologies (n.d.) *What is Black Hat Hacking? Sangfor*<https://www.sangfor.com/glossary/cybersecurity/what-is-black-hat-hacking>

IBM (2025). *What is* *Social Engineering* <https://shorturl.at/fXlge>

Copado Team (2024) *social engineering attacks* [https://shorturl.at/oSLFM](https://www.copado.com/resources/blog/12-types-of-social-engineering-attacks-to-look-out-for#:~:text=Phishing,numbers%2C%20or%20other%20personal%20information)

Schrader (2024). *A comprehensive look into password attacks and how to stop them*.<https://blog.netwrix.com/password-attack#:~:text=An%20example%20is%20a%20password,on%20a%20popular%20online%20system>.

RSS. (n.d.). *17 ransomware examples & how they occurred:*<https://www.upguard.com/blog/ransomware-examples>

Jayaraman, N. (2023). *What is Grey Hat hacking- a complete guide*. <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/unveiling-grey-hat-hacking-exploring-ethical-dilemmas-practices-and-implications/>