INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	**:**	**Koo Wai Kit (TP081761)**
INTAKE CODE	**:**	**APUMF2406CYS**
MODULE TITLE	**:**	**Cyber Security**
MODULE LECTURER	**:**	**Dr Seyedmostafa Safavi**
PROJECT TITLE		**An Overview of White Hat and Black Hat Hackers**
DATE ASSIGNED	**:**	**25TH JUNE 2024**
DATE COMPLETED	**:**	**29TH JUNE 2024**

Table of Contents

1. Introduction

In the rapidly evolving digital landscape of information security, it is becoming increasingly important to protect sensitive data and maintaining the integrity of digital infrastructure. Within this domain, white hat hackers and black hat hackers play distinct roles in shaping the cybersecurity framework and practices in modern organizations. According to Kaspersky (n.d.), a hacker's type is primarily determined by their motivation and whether their actions are legal or illegal. Hackers are typically classified into three primary categories: White Hat Hackers, Black Hat Hackers, and Grey Hat Hackers (Townsend, n.d.). In this paper, we will delve into the world of white hat and black hat hackers, discussing them through sections on the literature review, findings and outcomes, methodology and techniques, and concluding with future works and recommendations.

Consider a scenario where a hacker infiltrates a system — is their objective to safeguard it or exploit it? This fundamental distinction is what differentiate white hat and black hat hackers (Kaspersky, n.d.). Black hat hackers are individuals who exploit security vulnerabilities for personal gain or political interest (Townsend, n.d.). They are known for illegal activities like getting unauthorized access to systems, data theft and manipulation, and compromising security. They deploy a range of techniques from malware distribution to exploiting vulnerabilities, posing significant cybersecurity threats. In contrast, white hat hackers, also known as ethical hackers, use their skills to identify and address security flaws, employed either by organizations or governments. Townsend (n.d.) also mentions that they play a critical role in enhancing cybersecurity by conducting penetration testing and ensuring systems are resilient against malicious attacks, ultimately protecting businesses and institutions from potential harms.

Kaspersky (n.d.) states that the primary distinction between black hat hackers and white hat hackers lies in their motivations and methods. Black hat hackers illegally breach systems with malicious intent, often for personal gain or to cause harm, while white hat hackers collaborate with organizations to identify and address vulnerabilities, aiming to enhance system security and prevent unauthorized access by malicious actors.

2. Literature Review

Next, we will examine an existing literature on white hat and black hat hacking, which is "A Comparative Analysis of Black Hat and White Hat Hacking" by Raviraj Yogesh Mehendale, which explores the behaviours, motivations, and impacts of both types of hacking within the cybersecurity landscape.

2.1 Black Hat Hacking

According to Mehendale (2023), black hat hacking involves methodologies aimed at exploiting vulnerabilities in software, networks, and systems for personal gain or malicious intent. These hackers typically operate without authorization, as they breaches security protocols to access sensitive information or disrupt operations. They will utilize anonymization techniques to evade detection and legal repercussions, which complicates the efforts to trace their activities. The motivations driving black hat hackers include financial gain, political or ideological agendas, personal vendettas and excitement. Actions with financial motivation consist of data theft, ransomware attacks, and the illegal sale of stolen data on the dark web. Some hackers leverage cyberattacks to advance political causes or express dissent, targeting businesses or government entities. Additionally, personal grievances or the pursuit of adrenaline-driven challenges also fuel their malicious actions. The impacts of black hat hacking are significant, leading to significant financial losses to organizations from data breaches, ransom payments, and legal expenses incurred in aftermath. Moreover, reputational damage can erode trust among clients and business partners, affecting long-term viability. In addition, individuals may suffer privacy violations and financial harm through identity theft. The most severe impact would be the disruption of critical infrastructure, which will impair societal functions and public trust in digital systems.

2.2 White Hat Hacking

In comparison, white hat hacking, also known as ethical hacking or penetration testing, involves legally and ethically identifying and addressing vulnerabilities in software, networks, and computer systems (Mehendale, 2023). Ethical hacking focuses on enhancing cybersecurity through authorized access and permission from system owners. Motivated by a commitment to improving cybersecurity practices, ethical hackers employ methodologies such as vulnerability assessment, penetration testing, security auditing, code review, and social engineering testing. They use tools like network scanners and penetration testing frameworks to proactively identify and mitigate security weaknesses before they can be exploited by malicious actors. Ethical

hackers are driven by a combination of professional responsibility, intellectual curiosity, and a desire to protect digital environments from threats. Besides, they play a crucial role in not only identifying vulnerabilities but also in promoting cybersecurity awareness and best practices within organizations and communities. By collaborating and sharing knowledge within cybersecurity communities, white hat hackers contribute to the continuous improvement of security measures and secure digital infrastructures. Their efforts help organizations establish robust defence mechanisms and mitigate risks associated with cyber threats, ultimately fostering a safer and more resilient digital ecosystem.

In summary, the comparative study highlights how black hat hacking undermines cybersecurity with malicious intent, while white hat hacking strengthens defences ethically, as discussed within the literature. Understanding these distinctions is vital for advancing effective cybersecurity measures.

3. Findings and Outcomes

In this section, we will explore the specific findings and outcomes from our investigation into white-hat and black-hat hackers. This section will include the contrasting motivations, similarities, and impacts of white hat and black hat hackers on society and organizations. A real life case of both types of hacking will also be included.

To start off, it is essential to understand what is hacking and a hacker. According to HackerOne (n.d.), Hacking involves exploiting weaknesses in computer systems, networks, or software to gain unauthorized access, alter, or disrupt their normal operations. Hackers are individuals or groups with advanced technical abilities (HackerOne, n.d.). There is a wide range of hacker types, each with distinct motivations, ethical considerations, and objectives. In this paper, we will focus on the two primary types of hackers: white-hat hackers and black-hat hackers.

Black hat hackers, also known as threat actors, engage in hacking activities with malicious intent, including data theft, impersonation, causing disruption to system, or causing harm. They exploit vulnerabilities without authorization and typically harbour criminal intentions (HackerOne, n.d.). White hat hackers, also known as ethical hackers, are cybersecurity experts who leverage their hacking proficiency to detect and address vulnerabilities in computer systems, networks, or software. They possess legal authorization to conduct security assessments and adhere to ethical standards aimed at enhancing organizational security(HackerOne, n.d.). Their main differences can be compared in Table 1 below.

3.1 Similarities and Differences

Table 1: Differences between white hat hackers and black hat hackers (Karan, 2023)

White Hat Hackers	Black Hat Hackers
Have altruistic intentions	Have selfish motives
Focus on strengthening security	Focus on identifying and exploiting security weaknesses
Aims to protect individuals and organizations from cyber threats	Aims to cause harm by stealing data or damaging systems
Legal, because it involves authorized activities aimed at improving cybersecurity with the consent of system owners	Illegal, because it involves unauthorized access to systems for malicious purposes
Hired by organizations, businesses, and government agencies	Engage in hacking activities without permission from system owners
Educate users about cybersecurity risks and promote preventive measures to enhance awareness	Exploit users' lack of awareness about cyber threats to manipulate or defraud them

Despite their fundamental differences, black hat and white hat hackers share several similarities (Mehendale, 2023). Both possess deep knowledge of coding, networks, and cybersecurity tools, enabling them to effectively navigate and assess digital systems. They use similar techniques to identify vulnerabilities; black hat hackers exploit these for malicious purposes, while white hat hackers aim to fix them. Additionally, both groups stay updated on cybersecurity trends and emerging threats. Ultimately, both impact vulnerable systems, where black hat hackers compromise or damage information, while white hat hackers strengthen security protocols and reduce vulnerabilities.

3.2 Impacts on the Cybersecurity Landscape

Additionally, the influence of both black hat and white hat hackers on the cybersecurity landscape is extensive and complex. The actions of black hat and white hat hackers significantly shape the cybersecurity landscape, despite in opposing ways. According to Mehendale (2023), black hat hackers increase the risk of cyberattacks by introducing new threats and vulnerabilities, leading to constant advancements and adaptability in cybersecurity practices. In contrast, white hat hackers play a crucial role in identifying and fixing these

vulnerabilities before they can be exploited, thereby enhancing overall cybersecurity (Mehendale, 2023). Their proactive efforts help strengthen digital defences and make the internet safer. In addition, organizations must invest in robust vulnerability management processes to promptly identify and address security weaknesses, involving continuous monitoring, evaluation, and swift mitigation (Mehendale, 2023). Collaboration between white hat hackers, security experts, and organizations is essential for building a robust and secure digital environment, fostering innovation, and ensuring coordinated defence against cyber threats.

3.3 Practical Example

To illustrate the practical implications of both white hat and black hat hacking, we will examine real-life cases of each type. For instance, cybersecurity researchers Tommy Mysk and Talal Haj Bakry demonstrated a critical Tesla vulnerability by using a $169 Flipper Zero device and a Wi-Fi development board to steal a Tesla Model 3 (Fearn, 2024). They created a fake “Tesla Guest” Wi-Fi network to trick users into entering their login credentials, including two-factor authentication codes. With these details, they accessed the Tesla account, added a digital key, and remotely controlled the vehicle without triggering alerts. Despite Tesla’s manual stating that a physical key card is needed to add or remove keys, this is only enforced for removing keys. Tesla dismissed the issue as “intended behaviour,” highlighting the need for stronger security measures and alerts for adding new keys.

Next, to illustrate the malicious impact of black hat hacking, consider the case where a suspected hacker was arrested in Kuala Lumpur for attempting to sell government agency data on the dark web, offering it for US$200 (RM927) per set and expecting payment in cryptocurrency (Camoens, 2024). The arrest followed a raid by Bukit Aman's Commercial Crime Investigation Department on December 25, with the suspect identified and apprehended by the Cryptocurrency Crime Investigation Unit. The case, classified under Section 4(1) of the Computer Crimes Act 1997, involved personal and sensitive government information.

3.4 Summary

In conclusion, the exploration of white hat and black hat hackers reveals contrasting motivations, methodologies, and impacts on cybersecurity. White hat hackers contribute to digital safety by proactively identifying and mitigating vulnerabilities, while black hat hackers pose threats by exploiting these weaknesses for malicious purposes. The real-life cases

discussed underscore the critical need for robust cybersecurity measures, and proactive defence strategies to safeguard digital assets and privacy in an increasingly interconnected world. Understanding these dynamics is essential for organizations and individuals alike to navigate and mitigate the evolving landscape of cyber threats effectively.

4. Methodology and Techniques (10%)

In this section, we delve into the methodology and techniques crucial to understanding both white hat and black hat hackers. This discussion encompasses five essential phases of hacking. A brief discussion on hacking techniques and tools will also be included in each phase.

A white hat hacker employs the steps and mindset of a black hat hacker to gain authorized access and evaluate the organization's security measures and network (EC-Council, 2024). Therefore, both types of hacker follow the same five-step hacking process to infiltrate networks or systems. We will refer to this five-step process as ethical hacking phases.

4.1 Phase 1: Reconnaissance

The initial phase in ethical hacking methodology is reconnaissance, also known as footprinting or information gathering (EC-Council, 2024). The aim is to gather comprehensive data about the target. Prior to initiating an attack, an attacker gathers crucial information such as passwords and employee details. Attackers use tools like HTTPTrack to download websites and search engines such as Maltego to collect data on individuals through job profiles and news. This phase identifies vulnerabilities and potential attack routes, focusing on TCP/UDP services and specific IP addresses.

4.2 Phase 2: Scanning

The second phase is scanning, where attackers seek various methods to gather information about the target, such as user accounts, credentials, and IP addresses (EC-Council, 2024). Tools like port scanners, network mappers, and vulnerability scanners are utilized to identify vulnerabilities and exploit weaknesses in the target's systems. Vulnerability scanning targets specific weaknesses using automated tools like Netsparker and Nmap, while port scanning listens for open TCP and UDP ports to gain access to systems. Network scanning detects active devices on networks, which aids the identification and fortification of vulnerabilities within organizational networks.

4.3 Phase 3: Gaining Access

In the third phase of hacking, known as gaining access, attackers employ various tools and methods to breach a system, application, or network without authorization (EC-Council, 2024). This phase aims to download malware, steal sensitive data, or secure unauthorized access, potentially demanding ransom. Tools like Metasploit are commonly used for gaining access, while social engineering is a common tactic to exploit vulnerabilities. Ethical hackers focus on securing entry points, fortifying systems with passwords, and safeguarding network infrastructure through measures like firewalls. They also simulate social engineering attacks to identify susceptible employees that are vulnerable to cyber-attacks.

4.4 Phase 4: Maintaining Access

The fourth phase is maintaining access. Once a hacker gains entry into a system, their objective is to sustain that access covertly (EC-Council, 2024). They may employ tactics like launching DDoS attacks, using the compromised system as a base for further attacks, or extracting sensitive data like databases. Tools like backdoors and Trojans enable them to exploit vulnerabilities and steal credentials. Ethical hackers can counteract this by conducting comprehensive scans of organizational infrastructure to detect and eliminate malicious activities, thereby preventing ongoing exploitation of systems.

4.5 Phase 5: Clearing Track

The fifth and final phase is clearing track. According to EC-Council (2024), hackers aim to cover their footsteps to avoid detection. This involves eliminating any traces or evidence that could lead back to their unauthorized access. Actions may include altering or deleting logs, corrupting registry values, uninstalling software, or restoring altered files to their original state. This process ensures that the hacker maintains undetected access within the system, evading investigation from incident response teams or forensic investigators.

4.6 Summary

In conclusion, understanding the methodology and techniques used by both white hat and black hat hackers provides critical insights into cybersecurity defences. By following a systematic approach that mirrors malicious intent, ethical hackers can effectively assess and fortify organizational security measures. Each phase, from reconnaissance to clearing tracks,

plays a vital role in identifying vulnerabilities, securing systems, and mitigating potential threats.

5. Conclusion / Future Works and Recommendations

To summarize, this report has explored the critical distinctions between white hat and black hat hackers within the evolving landscape of cybersecurity. White hat hackers, driven by ethical standards and legal authorization, play a pivotal role in safeguarding organizations through proactive vulnerability assessments and security enhancements. In contrast, black hat hackers pose significant threats by exploiting vulnerabilities for personal gain or malicious intent, highlighting the need for robust cybersecurity measures. By dissecting the five phases of hacking, we underscored the importance of understanding and mitigating potential risks across digital infrastructures.

Additionally, there are some key recommendations that can be provided. Firstly, Mehendale (2024) states that organizations must be aware of the importance of strong security measures, ongoing threat monitoring, and collaboration with ethical hackers to address vulnerabilities. In addition, establishing and upholding ethical frameworks in cybersecurity practices is essential, alongside investing in employee awareness and training to counter prevalent threats like social engineering.

Future research should focus on tracking evolving threats, exploring ethical hacking dilemmas, advocating for adaptable legislative frameworks, and conducting thorough impact assessments to enhance cybersecurity strategies (Mehendale, 2024).

6. References

Camoens, A. (2024). Police arrest black-hat hacker. The Star. https://www.thestar.com.my/news/nation/2024/01/05/police-arrest-black-hat-hacker

EC-Council (2024). What is Ethical Hacking? And Complete Guide to Ethical Hacker in Cybersecurity. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-ethical-hacking/

Fearn, N. (2024). 'White hat hackers' carjacked a Tesla using cheap, legal hardware — exposing major security flaws in the vehicle. Live Science. https://www.livescience.com/technology/electric-vehicles/white-hat-hackers-

carjacked-a-tesla-using-cheap-legal-hardware-exposing-major-security-flaws-in-the-vehicle

HackerOne (n.d.). What Is Hacking? Black Hat, White Hat, Blue Hat, and More. https://www.hackerone.com/knowledge-center/what-hacking-black-hat-white-hat-blue-hat-and-more

Karan, R. (2023). White Hat vs Black Hat Hackers: What's the Difference?. Shiksha. https://www.shiksha.com/online-courses/articles/difference-between-white-hat-vs-black-hat-hackers/

Kaspersky (n.d.). Black hat, White hat, and Gray hat hackers – Definition and Explanation. https://www.kaspersky.com/resource-center/definitions/hacker-hat-types

Mehendale, R. Y. (2023). A comparative analysis of black hat and white hat hacking. Episteme: An Online Interdisciplinary, Multidisciplinary & Multi-Cultural Journal, 12(2). https://episteme.net.in/content/73/8297/attachments/1-AComparativeAnalysisofBlackHatandWhiteHatHacking.pdf

Townsend, C. (n.d.). What is the Difference Between a White Hat Hacker and Black Hat Hacker?. United States Cybersecurity Magazine. https://www.uscybersecurity.net/white-hat-hacker-black-hat-hacker/