By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/mason-honor-code/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site.

Introduction

For as long as the internet has been out, there has been security protocols introduced to make it a safe place for people to do their daily tasks. No person wants to worry about their card getting stolen or their information getting leaked to the public. Everyone must be cautious of who they talk to online because they can be hacked. Now there are 3 different types of hackers we will be going over. I know when you first think of a “hacker”, there is an immediate negative connotation that comes with it. I’ll tell you not all hackers are bad hackers and there is a such thing known as good hackers or ethical hackers. I will go over black hat hackers, grey hat hackers, and white hat hackers.

White Hat Hackers

Ethical hacking is an information security branch and called as “Penetration testing” or “White Hat hacking”. They are waged professionals. To overcome the risk of being hacked by hackers, we have ethical hacker in this field, which are specialized in computer security that violates and find loopholes in protected networks or computer systems of some organizations or companies and corrects them to improve security working under set of rules and regulations by various organizations. These are the people who try to protect data while on the internet with various attacks from hackers and keep it safe with the owner. Ethical hackers use the same approaches as black hat hackers, but their intention is to use their knowledge productively. Information obtained from ethical hacking is used to maintain the security of the system and to prevent system from further potential attacks.

Grey Hat Hackers

A Gray Hat Hacker is a security expert who frequently breaches the law but has no malicious intent such as the black hat hackers. The word Gray Hat is obtained from Black Hat and White Hat because white hat hackers or ethical hacker discover weaknesses and loopholes in the networks and computer system or and do not tell anyone until it is fixed, while others hackers apart from the black hat illegally hack the computer system or the network to discover loopholes and leak the information to the third parties and the gray hat hacker does not illegally hack and does not tell anyone how to do it.

Black Hat Hackers

Black hat hackers are criminals who bypass security protocols and break into computer networks. Their primary goal is to make money, but sometimes, they’re involved in corporate espionage or activism. Not only do they look to steal data, but they often seek to modify or destroy it, depending on their motivations. People belonging to this category can be any age, gender, or ethnicity.

Annotated Bibliography

(1) Shlyakhtunov, M. A. (2021). White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies. *International Journal of Advanced Computer Science and Applications*, *12*(8). https://www.proquest.com/docview/2655113348/C842B6C43597414CPQ/1?accountid=14541
This reference is relevant to my research because it talks about the ideas of whute hat hackers, gray hat hackers, and black hat hackers. It goes into depth with the reasoning for black hat hackers such as them ranging from amateurs to experienced criminals. White hat hackers being professional cybersecurity experts hired by many companies. They'll perform penetration testing and seeing vulneralbilities in companies. Gray hat hackers are in the middle of the two. What they are doing is illegal though it is not in a malicous intent.

(2) Antil, Y. (2022, January 13). Ethical Hacking and Hacking Attacks. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *06*(01). https://www.proquest.com/docview/2634513488/C842B6C43597414CPQ/3?accountid=14541
This refernce helps understanding the different types of hacker a bit more in depth. It goes into the advantages and disadvantages of ethical hacking. Ethical hacking is an information security branch and also called "penetration testing" or "white hat hacking". There is also unethical hacking which affects the development of system and networks in a negative way. It is carried out without the target's knowledge and are called cybercriminals. Process of ethical hacking goes from reconnaissance, scanning, gaining control, maintaining access, to log clearing.

(3) *White hat, gray hat, black hat*. (2005, October 3). Proquest. https://www.proquest.com/docview/218870905/C842B6C43597414CPQ/10?accountid=14541
This article is really tallking about how the government benefits and does not benefit from the different type of hackers. Hiring white hat hackers is good for your network or and company. Paying them to see if it is vulnerable or not. However, you are not ever supposed to hire a black hat hacker. They are liable to do something illegal.