World of White Hat Hackers

Sanchit Nanda
BE – Computer Engineering (2022)
Thapar Institute of Engineering and Technology, Patiala, Punjab – 147003, India.
sanchit17nanda@gmail.com

Abstract: This paper explores the world of white hat hackers and the problems that lie in their path. This paper also looks at ways in which the dignity of hacking can be prevented.

Keywords ---- Ethical hacking, white hackers, hacking, hackers, problems.

1. INTRODUCTION

Hacking often refers to the unauthorized intrusion into a network or computer; normally carried out by one or more "hackers." However, a hacker can be anyone. They can be an individual like you or me. They can work solo or be employed by an organization that has the motive to disrupt something or cause havoc—unnecessarily. Often, they look to alter security systems to achieve their goal, which differs from the actual purpose of the system [1].

A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them [2].

2. DISCUSSION

A. Knowing the difference

Traditionally, hackers were computer geeks who knew almost everything about computers (both hardware and software) and were widely respected for their wide array of knowledge. But over years, the reputation of hackers has been steadily going

down. Today, they are feared by most people and are looked upon as icons representing the underground community of our population [3].

A **black-hat hacker** is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons. The black-hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security systems, altering functions of websites and networks, or shutting down systems. They often do so to steal or gain access to passwords, financial information, and other personal data [4].

Grey hats exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies [4].

Usually, grey-hat hackers surf the net and hack into computer systems to notify the administrator or the owner that their system/network contains one or more vulnerabilities that must be fixed immediately. Grey hats may also extort the hacked, offering to correct the defect for a nominal fee [4].

White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white hat has permission to engage the targets and to compromise them within the prescribed rules of engagement [4].

White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization's information systems [4].

Unlike black-hat hackers, ethical hackers exploit security networks and look for backdoors when they are **legally permitted** to do so. White-hat hackers always disclose every vulnerability they find in the company's security system so that it can be fixed before they are being exploited by malicious actors [4].

Some Fortune 50 companies like Facebook, Microsoft, and Google also use white-hat hackers.[4]

Fig.1: Different types of Hackers

B. What it needs to be a White Hat Hacker?

White hat hacking involves a great deal of problem solving, as well as communication skills. A white hat hacker also requires a balance of intelligence and common sense, strong technical and organizational skills, impeccable judgement and the ability to remain cool under pressure. At the same time, a white hat needs to think like a black hat hacker, with all their nefarious goals and devious skills and behaviour. Some top-rate white hat hackers are former black hat hackers who got caught, and for various reasons decided to leave a life of crime behind and put their skills to work in a positive (and legal) way. There are no standard education criteria for a white hat hacker — every organization can impose its own requirements on that position — but a bachelor's or master's degree in information security, computer science or even mathematics provides a strong foundation. For those who aren't college bound, a military background, especially in intelligence, can help your resume get noticed by hiring managers. Military service is also a plus for employers who require or prefer those with security clearances [5].

C. Why be a White Hat Hacker?

White hat hackers have been stealing the tech spotlight, praised for protecting everything from valuable Instagram-influencer accounts to detecting cyber weaknesses at multi-million-dollar companies. And, they are being paid well for their efforts. Bugcrowd, a platform that crowd sources bug hunters for other companies, recently released a report on the economics of white hat hackers. According to Bugcrowd, the average yearly payout of the top 50 white hat hackers in 2018 was $145,000. White hat hackers tend to be young, digital natives who consider screens as essential as food and water [6].

D. Problems faced by White Hat Hackers

The word "hacker" does not bring the best of thoughts to most people's minds. The popular definition of a hacker is someone who intentionally breaks into systems or networks to illegally procure information or infuse chaos into a network for the express purpose of control. Hackers are not usually associated with doing good deeds; in fact, the term "hacker" is often synonymous with "criminal" to the public [7].

People often are not aware about the types of hackers and often consider a person related to the term hacking as a criminal.

3. COUNTERING THE PROBLEM

White hat hacking plays a significant role in securing the information systems that are crucial in our computer driven world. That is not to say that it does not present some ethical problems in itself but if it is used correctly, it has tremendous potential in helping to secure information. Much of its success will come down to the morals and ethics that are at the core of the individual hacker. The more ethical-minded the individual, the more trustworthy and beneficial that individual white hat hacker will prove to be. We have already seen a number of white hat hackers using their skills to help catch criminals 27 and prevent others with mal-intent from exploiting vulnerabilities. Corporations, government agencies, and the military have all made use

of white hat hackers to help protect, secure, safeguard not only our information but our businesses and our way of living. To catch a thief, you have to be able to think like one and that is exactly what a white hat hacker is all about. If you want security, you must be able to assess your weaknesses and address them accordingly. Security is about being protected and staying free from danger requiring that we think and plan ahead. Realizing and addressing threats and vulnerabilities before the enemy finds and exploits them can prove to be crucial in the struggle to secure information. If you fail to think ahead, your opponents will exploit your weaknesses at every opportunity. As we begin to realize the increased need for security and the potential benefit of utilizing white hat hackers, there will be an ongoing information security battle taking place between a newly trained group of white hat hackers and their opposing black hat counterparts in the years to come [8].

4. CONCLUSION

Technology has continued to grow at a high rate over the years and continues to do so; scholars are putting themselves in vulnerable positions by helping individuals to hack. The mind is a very powerful tool that has no control, the control will continue to grow proportionally with the desire to get knowledge of something that is impossible to achieve in its entity, but not forgotten in its entirety. Hackers will always find ways of getting into systems, whether they are doing it for good or bad.

5. REFERENCES

[1] https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/
[2] https://www.techopedia.com/definition/10349/white-hat-hacker
[3] A. Fadia, 2008, *"An Unofficial Guide to Ethical Hacking"*, Macmillan India Ltd, New Delhi, 586 p.
[4] https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/
[5] https://www.businessnewsdaily.com/10713-white-hat-hacker-career.html
[6] https://kwhs.wharton.upenn.edu/2019/01/world-white-hat-hacker/
[7] https://www.lifewire.com/hackers-good-or-bad-3481592
[8] https://digitalcommons.pace.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1012&context=honorscollege_theses