Fardin Ahosan Shawon

by Iftekhar Efat

Submission date: 13-Mar-2022 12:27AM (UTC-0500)
Submission ID: 1782964741
File name: ASH1825019M.pdf (382.73K)
Word count: 3400
Character count: 17054

White hat And Black hat Hackers

Fardin Ahosan Shawon
ASH1825019M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security:White hat and Black hat heacker**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

Massive growth of the Internet has brought in many good things such as e-commerce, easy access to extensive sources of learning material, collaborative computing, e-mail, and new avenues for enlightenment and information distribution to name a few. Today, since almost all the work is done over the internet, crucial data is sent over the web and other information is placed over the internet. So ensuring data security over the internet is very important and should be taken care of at utmost priority. As with most technological advances, there is also a dark side attached to it, i.e. hacking. Hacking is an activity in which a person (namely hackers) exploits the weaknesses and vulnerabilities in a system for self profit or gratification. With the growing movement of the world from offline to online culture like shopping, banking, sharing information access to sensitive information through the web applications has increased. Thus the need of protecting the systems from hacking arises to promote the persons who will punch back the illegal attacks on the computer systems and will ensure data security. As every coin has two faces, this coin also has one another face which generally acts as a life saver for the victims of hacking.

1 Introduction

Who are hackers? What do they do? Are they evil people? The majority of pieces published by the media about hackers is negative. “The black-hat sense proved irresistible to members of the media and other non-techies, no doubt in part because ‘hack’ sounds malicious—not to mention that ‘hack’ rhymes with ‘attack’.” Another reason that hackers are portrayed as the bad guys is not because there are more evil hackers, but because danger sells.Hacking is the technique in which the persons ,what’s in a name? Call them hackers, crackers, intruders, or attackers, they are

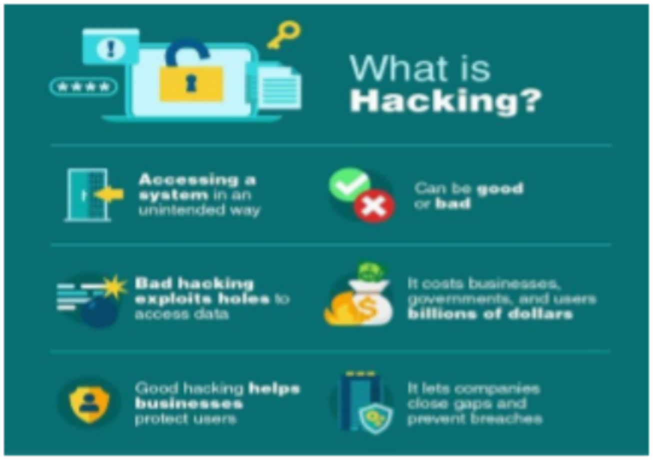
What is Hacking?
Accessing a system in an unintended way
Can be good or bad
Bad hacking exploits holes to access data
It costs businesses, governments, and users billions of dollars
Good hacking helps businesses protect users
It lets companies close gaps and prevent breaches

Figure 1: Defination of hacking

all interlopers who are trying to break into your networks and systems. Some do it for fun, some do it for profit,or some simply do it to disrupt your operations and perhaps gain some recognition. Though they all have one thing in common; they are trying to uncover a weakness in your system in order to exploit it Even though sometimes hackers break laws and cause harm, they are necessary in society and do not deserve to be labeled as “villains” or “criminals.” in fact, hackers are good and necessary. In this paper, I will first provide background information about hackers. Then, I will introduce different types of hackers and provide research that proves how each type is beneficial to society. Next, I will discuss the reason that some people believe hackers are evil. Finally, I will weigh the pros and cons of hacker’s actions and come to a conclusion.[4]

2 Background Information

What aspects of life does the internet and technology impact? People utilize the internet for school, work, and entertainment purposes. In addition, people depend on technology for research, agriculture, factories, and more. In today's world, we are encompassed by internet and technology everywhere we go. According to Pew Research Center, conductor of social science research, as of September 2016, only 13 percent of Americans were not considered internet users (Anderson Perrin). That means in the less than thirty years that the internet has been accessible to the public, that from 1991 to today, it has become of use to nearly 90 percent of the American population. The internet is seemingly unstoppable. People who use the internet and whose lives incorporate technology need to know about hackers because they could be effected.

The definition of a hacker is not inherently negative. Generally speaking, the media and public view hackers as criminals who break the law to access confidential information and embezzle money . Computer people, "techies" have a very different view of hackers. Keren Elazari, cyber security analyst and senior researcher at the Tel Aviv University, thinks highly of hackers. Elazari states that "they (hackers) push the Internet to become stronger and healthier, wielding their power to create a better world (Elazari)."A hacker could be someone who alters computer hardware and software for benevolent or malevolent purposes. A general definition of the term "hacking" is:

> The practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as "hackers" ("Cyber Laws").

One of the main problems surrounding hackers is that more often than not, people place all hackers together into a single group and make assumptions about hackers based off of one or two stories that they hear. Movies and TV shows have a tendency to portray hackers in a negative light. Often times hackers are made out to be the villains and provoke fear amongst the audience. An example of a TV show that perpetuates the stereotype of hackers is "Cyber Chase." It is a kids cartoon where three children have to battle against an evil computer genius. The kids TV show pains a poor picture of hackers that influences people from a young age (IMBD). However, similarly to any group of people, each and every hacker has a different motive and end goal. Therefore, they cannot all be put into the same category. It is important that people be weary of evil hackers, but people need to know about the other kinds of hackers. . . the heroes behind computer screens.

The first hackers in the 1950's were a group of students at MIT who tapped into software for fun and as a prank. . . not to do any harm (Boswell).

Hackers soon discover that toy whistles produce the right frequency for them to "phreak" Ma Bell's telephone system, allowing them to place long-distance calls for free. Among those who make names for themselves as "phone phreaks" are Steve Wozniak and Steve Jobs, the future founders of Apple (McCormick).

It was not for years after the first hacking incident that hackers came to be known as threats and feared by masses of people. The Jargon File, a glossary for programmers from 1975, contains several definitions for the word 'hacker.' "The first reads, 'A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.' The following six definitions are equally approving views about hackers. The final definition is '[deprecated] A malicious meddler who tries to discover sensitive information by poking around' ." The fact that the first six of seven definitions are positive, and that only the last definition defines hackers to be bad people shows that the majority of people did always view hackers in a negative light like we do today.

Eventually, harmless pranking hacks evolved to be much more. One example of a harmless prankster that unintentionally turned into something more is Christopher Poole. In 2003, when he was only 15 years old, Poole created a website called 4chan.org. Upon creation, the website was popular for its cat memes and innocent jokes. As time progressed, 4chan.org became a popular forum where anonymous hackers communicated and shared coding tips which turned into systemized cyber war. Some people consider 4chan.org to be the awakening of Anonymous, a group of activist hackers (Sicilano Dewey)

Figure 2: White hat and black hat hackers represented as the devil and an an angel.

[5]

3 Survey On Ic3 Report

I have discovered a report from a government website which is about "Internet Crime Current Report". The Internet Crime complaint center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NWC3).According to the current 2019 report by IC3 and as depicted in the graph above (figure1), till 2019 the number of complaints of hacking has increased at an exponential rate. Moreover, it has affected mostly the people who are generally of age over 60 years. The above graph depicts the total counts of victims of hacking. As we can see, a large number of people of every age group are rapidly and increasingly becoming the victims of hacking. This shows how essential and vulnerable the data security is in this era of the cyber world. [1]

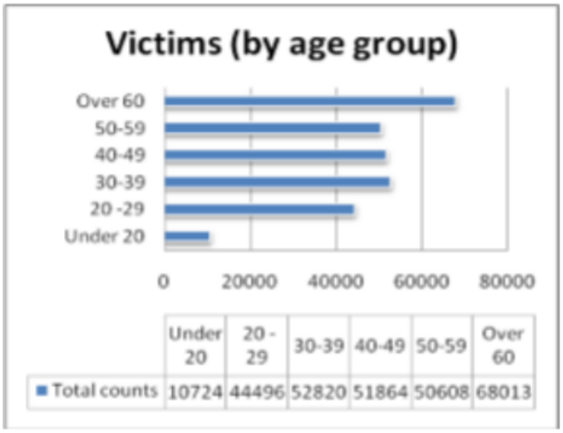

Figure 3: Total victims of Hacking

4 Hacking Typology

4.1 Black Hats

Black hat hackers are who the government and majority of the general public consider the bad guys. Black hat hackers are the traditional "cyber criminals." The reasons and influences behind these hackers vary immensely. Some motives include financial gain, revenge, accessing confidential information, creating chaos, and shutting down servers. One example of a hacker with the end goal of major financial gain is Kevin Poulsen, also known as Dark Dante. Kevin Poulsen is known for hacking into a radio station's telephone lines to make himself the 102nd caller. He won a Porsche and other high priced items as a prize. Years later when he was finally caught, he was sentenced to over four years in prison (Siciliano).[2]

Sometimes, black hat hackers are difficult for the government to track down and apprehend. These evil hackers can be very intelligent and hide their trail expertly. One way that the government can catch them is by looking through their engagement

Figure 4: This is a photo of the Guy Fawkes mask that the hacking group, Anonymous, uses to represent themselves.

on computer forums, a place where hackers sometimes share code and collaborate together. Websites like Reddit and 4chan sometimes provide clues to taking down the hackers for the government (Iyer). When someone is trying to alter software or hardware they often ask one another for help or advice. Because they can be difficult to catch, the government hires their own hackers to help track down hackers with ill intent (Peterson).Hackers like Kevin Poulsen are those who give all hackers the reputation they have. Our society views black hats as evil because they are portrayed in a negative light in the media.

”I think that like Robin Hood, they are in the business of redistribution, but what they are after isn't your money. It's not your documents. It's your attention. They grab the spotlight for causes they support, forcing us to take note, acting as a global magnifying glass for issues that we are not as aware of but perhaps we should be (Elazari).”

If you do a simple google search on hackers, black hats come up in the majority of the search results. Many people think that the negative effects that black hats yield far outweigh the positive effects that they have on society. The negative side of black hats is that they steal, lie, and are motivated by self-interest (Iyer). The positive side of black hats is that they use their hacking skills to cause chaos in order to draw attention to issues that would go otherwise unnoticed (Elazari). Even though hackers are viewed as villains there are positive aspects to every kind of hacker.[6] Black hat hackers are also known as crackers.

4.2 White Hats

White hat hackers are “the good guys” in the world of hacking. White hats are often hired to do “penetration testing.” White hat hackers are also known as ethical hackers. An example of one of the first white hats was Dr. Cliff Stoll, who in 1986 ran an investigation that led to the capture of black hat hacker Markus Hess. Although Dr. Stoll wasn’t a hacker, his activities of hunting for a malicious hacker place him as a white hat. This is when a hacker is hired by a company to hack into their own system and find flaws in their software. The white hats try to penetrate into the system just like a black hat hacker would. Once they get through the security, the white hat hackers report back to the company that they are hired by and work to create a more secure network and close the gaps. White hat hackers are different from grey and black hats because they never hack into a system without permission and never exploit information without permission. Everything that a white hat hacker does is legal and ethical.

Figure 5: Heacker is everywhere.

Companies like Facebook sometimes pay people when they find and report a security breach in their software. In situations like these, people who are not hired specifically to do “penetration testing” are still compensated and given an incentive to do the right thing and report the breach in security. The government also relies on white hat hackers. Recently, the Australian government started a competition called the “Cyber Security Challenge Australia.” This is the fifth year of the competition. The reason that the Australian Government holds the competition is to find the new wave of technological geniuses in order help the government maintain tight security and to prevent future security breaches.

An example of a famous white hat hacker is Kevin “Condor” Mitnick. Condor is a special case because he actually started out as a black hat hacker. At one point in time, the US Federal Communications Commissions named him “the most wanted computer criminal in U.S. history." Mitnick earned this title because he hacked into private information and a string of other internet crimes. Once he was caught in 1995, he served five years in jail. There was a gigantic controversy surrounding Mitnick because he was jailed for a long period of time before his trials even took place. Once he was released back into the real world, he made a complete 180-degree turn and changed from one of the evilest hackers to one of the most highly regarded white hat hackers in history. Mitnick also spoke out about his situation. "I had a deal with the government for about, for seven years after I was released from custody. So it expired around Jan. 21, 2007. Mitnick is saying that the government required that he not tell his side of the story for a certain amount of time.

This shows how corrupt the government was because they took away one of Mitnick's fundamental rights (freedom of speech) as an American. This is also proof that we need hackers because someone has to be there to contradict the government if they are in the wrong. Despite the unusual circumstance, Condor became a security consultant and works for some of the largest companies and did not revert to his black hat ways. Condor's situation also shows how the government sometimes reacts in unfair ways toward hackers.

White hat hackers are viewed as the "knights in shining armor" because they protect businesses from being hacked and help the government protect confidential information. In addition, white hat hackers do everything "correctly" and abide by the law.[3]

5 BENEFITS OF ETHICAL HACKING

The benefits range from simply preventing malicious hacking to preventing national security breaches . The benefits include:

- It helps us to fight against cyber terrorism and to fight against national security breaches.
- It helps us to take preventive action against hackers.
- It helps to build a system which prevents any kinds of penetration by hackers.
- Ethical hacking offers security to banking and financial establishments.
- It helps to identify and close the open holes in a computer system or network

6 Conclusion

People fear what they do not understand. The average American uses their device in the most simplistic way. They do not attempt to understand how their phone does what it does. They simply use what is already there. Hackers go leaps and bounds beyond this. They know the ins and outs of technology. We fear hackers because they can do what we cannot. Is this fair? No, it is not. Every hacker fights for their own cause and believes that their efforts are ethical and proper.

The word “hacker” is a very broad term and generally carries negative connotations. However, as I discussed prior, the term “hacker” encompasses white hats and black hats, and other hacking groups that don’t fall into any category. Although they are similar terms, their meanings are drastically different. Similarly to any group of people, there are the good and the bad.

A black hat hacker who illegally wipes out the software of a company with evil intentions but saves thousands of employees retirement funds is obviously in the wrong. . . right? Ethical questions such as these cannot be viewed in black and white. For this same reason, we can not label hackers as “evil,” or even categorize them as “good guys” and “bad guys” because it is simply not possible. Hackers have an amazing power to represent groups of people that cannot stand up for themselves. In countries where the government takes control of a population, Hacktivists step up and fight for people who have no voice. Hackers are not inherently evil.

Every hacker group serves a purpose. White hat hackers prevent black hat hackers from causing too much chaos and help companies and groups of people secure information. . Even black hat hackers serve their purpose by attacking corporations who take advantage of people. None of this is to say that everything hackers do is just and positive. There are casualties and problems with hackers that are side effects of the forward progress that hackers attempt to make. Hackers super ability to represent groups of people and to keep the government in check outweighs the problems that are created in the process.

Acknowledgements

The authors of this paper would like to extend our sincerest thanks to our project advisor, Ifthekar Alam Efty, for his unwavering guidance and support throughout this entire process. He is not only inspired this project, but he kept our morale high throughout the entirety of its completion. We could not be more thankful for him or the time, energy, and effort he has dedicated to ensuring that this project was of the highest quality possible. Finally, we would like to thank the entire Institute and staff of Institute of Information Technology,NSTU for supporting us in this endeavor and pushing us to produce a work we are proud of.

References

[1] Amrinder Arora. Statistics hacking: Exploiting vulnerabilities in news websites. *International Journal of Computer Science and Network Security*, 7(3):342–347, 2007.

[2] Foram Gandhi, Drashti Pansaniya, and Swapna Naik. Ethical hacking: Types of hackers, cyber attacks and security. *International Research Journal of Innovations in Engineering and Technology*, 6(1):28, 2022.

[3] Amit Anand Jagnarine. The role of white hat hackers in information security. 2005.

[4] Jason Porterfield. *White and Black Hat Hackers*. The Rosen Publishing Group, Inc, 2016.

[5] Shivanshi Sinha, Dr Arora, et al. Ethical hacking: The story of a white hat hacker. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN*, pages 2347–5552, 2020.

[6] Georg Thomas, Greg Low, and Oliver Burmeister. "who was that masked man?": System penetrations—friend or foe? In *Cyber Weaponry*, pages 113–124. Springer, 2018.

Fardin Ahosan Shawon

ORIGINALITY REPORT

89%	89%	3%	35%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	sedonaengl.wordpress.com Internet Source	65%
2	www.ijircst.org Internet Source	9%
3	ijsrcseit.com Internet Source	4%
4	core.ac.uk Internet Source	3%
5	www.ijcstjournal.org Internet Source	2%
6	v1.overleaf.com Internet Source	2%
7	link.springer.com Internet Source	2%
8	global.oup.com Internet Source	1%
9	www.coursehero.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Fardin Ahosan Shawon

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Hyph. You may need to add a hyphen between these two words.

Article Error You may need to remove this article.

PAGE 3

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

PAGE 4

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Garbled Grammatical or spelling errors make the meaning of this sentence unclear. Proofread the sentence to correct the mistakes.

Compound These two words should be written as one compound word.

Possessive You may need to use an apostrophe to show possession.

Possessive You may need to use an apostrophe to show possession.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sentence Cap. Remember to capitalize the first word of each sentence.

Sentence Cap. Remember to capitalize the first word of each sentence.

Proper Noun If this word is a proper noun, you need to capitalize it.

PAGE 5

Prep. You may be using the wrong preposition.

Hyph. You may need to add a hyphen between these two words.

Dup. You have typed two **identical words** in a row. You may need to delete one of them.

PAGE 6

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Hyph. You may need to add a hyphen between these two words.

PAGE 7

Sentence Cap. Remember to capitalize the first word of each sentence.

Missing "," You may need to place a comma after this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Missing "," You may need to place a comma after this word.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 8

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 9

PAGE 10

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

PAGE 11

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 12