Ethical Hacking: White Hat Hackers

Vikram Kumawat, Priyanshi Pal, Pradeep Jha

Department of CSE, Arya College of Engineering Research Centre, Jaipur, Rajasthan, India

Corresponding author: Vikram Kumawat, Email: vikramkumawat.arya@gmail.com

Nowadays the demand for Computers and Smart phones has increased so much that people cannot complete their work except these two things. Whether we do our own business or work in a company or bank, computers are used everywhere. To run a company or to run a business, it is necessary to use a computer because with its help we do a lot of work and calculations in a few minutes. Similarly, to how minor and large obstacles must be overcome in order to complete any assignment, many problems must be overcome when dealing with computers. For decades, hacking has been a huge part of the computing world. It is a large field that encompasses a wide range of issues. If we first determine when this hacking occurred, we will learn that it was first utilized in 1960 by MIT, and that at the same time, the term ”hacker” was coined and later became well-known.

Keywords: Hacker, Hacking, Ethical Hacking, White hat hacker, Problems for white hat hackers.

2021. In Prashant Singh Rana, Deepak Bhatia & Himanshu Arora (eds.), *SCRS Proceedings of International Conference of Undergraduate Students*, 13–17. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-01-1-2

1 Introduction

The Hacking is done by a person using a computer. This person is known as a hacker, and he has extensive computer and computer knowledge, making him adept at stealing data from other people's computers. When you hear the word "hacking," you know it's a bad thing to do because it's illegal and can get you in trouble. However, hacking is not always wrong because not all hackers are the same; some are excellent hackers and others are malicious. Let's learn more about good and evil hackers, as well as what they do [1-2].

If we consider the technical aspects of hacking, the most important task is to identify potential entry points into any computer network or computer system and then to penetrate it. Typically, hacking entails gaining illegal access to a computer system or network. Its goal is either to cause harm to the system or to steal the system's sensitive data. The term "Ethical Hacker" refers to a computer professional who performs the hacking himself. Ethical hackers are those who utilize their skills to learn more about how systems work, how they're designed, and sometimes to test the system's security [3].

White hat hackers are the polar opposite of black hat hackers, in that they examine the security of a computer with authorization and exclusively for the purpose of learning or assisting a firm. What level of security does their system have, and can that security be easily breached? They are also known as ethical hackers [4].

2 Need of Ethical Hacking

Today max of the data is transmitted through the internet. No network is completely secure [5-7]. Everyone has some or the other drawback, it just goes unnoticed by the hackers sometimes. Since the data is precious, it is necessary for any company/organization to detect the shortcomings in the network in time, but how will the network flaws be detected, will we wait for any untoward incident? Here come the ethical hackers in other words the cyber security experts.

The basic purpose of ethical hacking is to find and fix the flaws in the network. For this, white hat hackers do penetration testing. Penetration testing (abbreviated pen testing) is a simulated cyber attack that is performed to find potential threats and vulnerable parts of a network through which a black hat hacker can gain access to the network and harm the company [8].

3 Hacking Attacks

Nowadays, we do all of our major transactions on the internet. While greater global connection makes our lives simpler, the risk of our personal information being taken by a hacker or cybercriminal has also grown. Hackers now have a plethora of options for stealing and misusing personal information.

4 Phases of Ethical Hacking

Reconnaissance:

Hackers act like detectives while doing reconnaissance, acquiring data and information to better understand their targets. They want to know more about the organization than the people who operate and care after it, so they look at email records and open-source data. They concentrate on the security aspect of the invention, research the flaws, and exploit any flaws to their advantage.

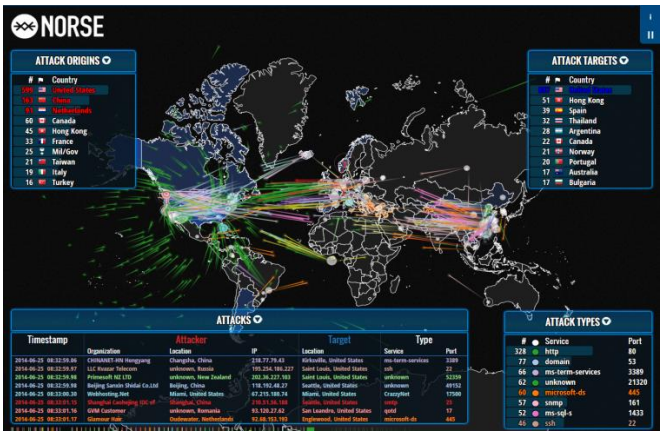

Fig. 1. Overview of Hacking Attacks

Scanning and Enumeration:

Enumeration is the process performed by an attacker user group operating name network resource. port or services about the jism attacker system. Enumeration is used by the taker tab when the user wants to find out what is the system my username, how many user groups open ports are there, what is the name of the computer, how many services are running. If you feel that we have already integrated all this information in footprint scanning, then why doing enumeration is the difference between scanning or enumeration.

5 Gaining Access

Web apps used by a legal company are targeted utilizing standard approaches once possible ways have been searched for. These are some of them:

- SQL injections - if a web application's text fields are incorrectly coded, unauthorized code can be run within the application.
- Cross-site scripting - websites occasionally allow other sources to work. If one of these external sources is compromised, the website is as well.
- Hackers can identify backdoors, which allow a service to be accessed without requiring user authentication.
- Session mismatches - when a user is using an application and the application is processing it, a hacker can take the user's identity.

6 Maintaining Access

Once access has been acquired, an ethical hacker must figure out how to keep it. This generally entails injecting a virus or other flaw into the system that can repeatedly perform the same access technique. This is the stage at which the actual scope of the vulnerability is revealed. If a hacker is unable to

sustain access, the vulnerability's scope is reduced. Otherwise, the magnitude of the vulnerability is huge if a big amount of information can be taken, especially without being discovered for a long period.

7 Problems Faced by White Hat Hackers

White hat hackers use the same technique that black hat hackers use. They also hack the system, but they can only hack the system which allows them to hack that system or website to test the security of the system. They focus on security and security of the IT system. And that is why white hat hacking is not considered a legal crime [9].

Phishing: Phishing is a type of email scam in which you are requested to provide personal information. It looks like real. Hackers try to trick you through phishing emails to make you believe that they are asking for bank account information or other data for your benefit.

Mail ware: It is software that is created to steal the information or data of a system. This malware is capable of stealing sensitive data, erasing it, altering the system's operation, and monitoring the person running the system. This program can be installed in your system by several ways. An outdated operating system or pirated OS, clicking on unintentional links, or installing fake software can result in mail ware installs.

Mobile Apps: The Google Play Store and the Apple Store do not have all secure apps. One, these apps ask you for permission to access all the data of the mobile, so that the hacker can steal all your information and on the other hand, having access to the message / media file, it can also make your confidential information public.

Unsecured Network: Hackers can easily steal personal information of customers using public Wi-Fi. Credit card numbers, passwords, chat messages, email IDs, PAN numbers, and Aadhaar numbers are among the data that hackers are attempting to acquire. This is called identity theft in common language. To keep your information safe, do not do activities like shopping or net banking from these places.

8 Conclusion

In a way, ethical hackers also do the same thing as hackers (cyber criminals), but their aim is to make a computer system more secure than before, instead of harming it. Because of our increasing reliance on the Internet, ethical hackers have become a serious issue in the IT security business. It's a demanding job that, on occasion, necessitates working 24 hours a day. Hacking has become a lucrative business for criminals in this era where data has become serious. The need for data security and curbing malicious hacking and its destructive effects has led to the rise of ethical hackers.

They test systems for the possibility of being hacked and take precautions as well as implement measures that ensure that the data is sealed. This includes all devices that store information and use the network. There are also different types of hackers, depending on their intentions and the way they operate. Hacking ethically is a positive habit that improves security. All businesses should consider implementing this on their firms if they want to protect their operations and data.

References

[1] Trabelsi, Zouheir; McCoey, Margaret (2016). Ethical Hacking in Information Security Curricula. International Journal of Information and Communication Technology Education, 12(1):1-10.

[2] Wang, Yien; Yang, Jianhua (2017). [IEEE 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) - Taipei, Taiwan (2017.3.27-2017.3.29)] 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) - Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool. , (), 110–113. doi:10.1109/WAINA.2017.39.

[3] Prabhat Kumar Sahu, Biswamohan Acharya (2020). A Review Paper on Ethical Hacking. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(12):163-168.

[4] Baha Abu-Shaqra (2016). Technoethical Inquiry into Ethical Hacking at a Canadian University. International Journal of Technoethics (IJT), 7(1):1-15.

[5] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon (2021). Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption. IEEE 2021 6th International Conference on Communication and Electronics Systems (ICCES), 1153-1157.

[6] Himanshu Arora, Mr. Manish Kumar and Mr. Sanjay Tiwari (2020). Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm. International Journal of Advanced Science and Technology, 29 (8):6167-6177.

[7] Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain (2020). A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm. Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, 83-90.

[8] S. Patil, A. Jangra, M. Bhale, A. Raina and P. Kulkarni (2017). Ethical hacking: The need for cyber security. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 1602-1606.

[9] L. Wilbanks (2008). When Black Hats Are Really White. in IT Professional, 10(5):64-64.