2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON) | 978-1-6654-9602-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/COM-IT-CON54601.2022.9850601

Ethical Hacking: A Technique to Enhance Information Security

Tathagat Yash
Computer Science and Engineering
Manav Rachna International Institute of Research and Studies
Faridabad, India
tathagatyash28@gmail.com

Dinki
Computer Science and Engineering
Manav Rachna International Institute of Research and Studies
Faridabad, India
dinki444bansal@gmail.com

Suresh Kumar
Computer Science and Engineering
Manav Rachna International Institute of Research and Studies
Faridabad, India
suresh.fet@mriu.edu.in

Kamlesh Sharma
Computer Science and Engineering
Manav Rachna International Institute of Research and Studies
Faridabad, India
kamlesh.fet@mriu.edu.in

***Abstract*—In today's world, security has become the paramount truth. Every organization faces several challenges in securing their information, like master card info from online-looking websites and other crucial information. Every organization fears black hat hackers because they perform hacking to an intrusive extent to hack the data and information for their benefit. Hacking is an act of finding possible entry points or finding vulnerable flaws in a particular system or a network device so that a hacker can get into the system through that vulnerabilities or entry points. So, this research paper discusses 'Ethical Hacking' as a legal process by which one can secure data and protect it from malicious hackers by applying tools and techniques. Ethical hacking is also known as penetration testing, which uses its powers to hack data and information, steal passwords, credit card info, scan their e-mail id and other personal information for a good purpose in the world**

Keywords—Hackers, Hacking, White Hat, Malicious Hacker

I. INTRODUCTION

With the growth of the internet and many networks connected to it, computer security has become a concern for all businesses and governments. They all can take the benefits from the internet for advertising, electronic commerce, ability to identify, obtain and make use of databases or information effectively. Still, they all have a fear of being hacked [2]. The term hacking is the process of finding all the system's weaknesses that can be created or exploited by the hackers. So, hacking is usually done to foot-in unauthorized access to a particular device. The intention behind hacking would be different, like some hackers want to hack a specific system or network to steal some sensitive information.

In contrast, another hacker may usually want to hack the system to destroy or harm a particular system [10-12]. The term ethical hacking is used to hack for a legal or good purpose. The person who performs ethical hacking is called an ethical hacker. So, the job responsibilities or functions of ethical hackers are to perform penetration testing, find vulnerabilities in their own companies, and protect their company's data [16,17]. Ethical hackers do not perform hacking to harm a particular organization. They all are worried about maintaining control of their personal information like credit card pin codes and other important information. Hacking is double-edged, and as it is the process of finding the weak line in the computer network that can be identified and exploited by an attacker, to foot in unauthorized access of data and information into the computer system or networks to perform some changes in the files and folders [4,7]. On the contrary ethical hacking is very effective, as it helps to recover the lost data and information, especially when you've lost your password.

Today's world is associated with malicious web attacks and other networks [5]. Black hat hackers are also called criminals who break the network with vicious attacks. They may destroy the data and information, steal the passwords, scan their e-mail, freeze the device, and take up crucial data. There are so many scripts available online that black hat hackers can use them [1,17]. There is no control that can prevent all security threats, and there is no single bullet. Many security architectures have complex prevention, incorporating a mixture of detection and administrative controls. So, the need to ensure the improvement of cybersecurity programs is now prominent.

Now, ensuring the cybersecurity program is essential, and it is seen that a progressive method to do this is through conducting a penetration test [13,15]. The penetration test plays a significant role by engaging a team of professionals to attack an organization as a criminal hacker would. These professionals are known as Ethical Hackers. The major aim of this penetration test is to assess the control's effectiveness and tell someone information that has been discovered [3,18]. The penetration test is a simulated attack against your computer system to check the weakness in a software system. The penetration test is a process of testing the security weaknesses of any application, system, or network [4-8]. In this, hackers try to find out how secure our network, application, or system are and the chances or possibilities of our application being hacked [9]. Ethical hacking is entirely legal because they first take permission from the organization's owner and then perform their hacking skills to break the data. Hacking is a principle where an individual or a group of individuals try to break into a computer system with some security flaws.

Those with trust issues don't believe that good thing can happen to them; having trust issues means that a person isn't comfortable with another person [11,14]. The primary purpose of ethical hacking is to test and ensure that an organization's network is safe. So many people can always trust white hat hackers because they are trustworthy hackers. White hat hackers firstly take permission from the owner of the organization. But many people have trust issues because of the black hat hackers. As there are so many scripts available online that can be used by the attacker or black hat hacker [18,19]. But it is seen that with the growth of the internet, everybody depends on it and ethical hacking has become a major requirement for most people. There is a connection at a certain level of trust between the ethical hacker and the owner of the organization. The organization engages them to conduct the trust based on trust. While hiring a certified professional, the organization confirms its commitment to security [6].

II. Literature Review

Gurpreet K. Juneja [5] addressed the idea of ethical hacking from several perspectives. It also proposed the security lifecycle of an ethical hacker & the phases of hacking.

Ajinkya A Farsole [7] proposed the idea of ethical hacking & its affairs with the corporate & reporting back to the owners with the vulnerabilities they found security.

Bhawana Sahare [6] describes ethical hacking, the types of ethical hacking, the impact of hacking on businesses and governments, and the different types of hacking with their phases.

Danish Jamil [9] explores the ethics behind ethical hacking and gives so many solutions to the problems that will raise issues in the future.

Aman Gupta [10] describes the types, working of the malicious hackers, various attacks performed by the hackers, and some information about the Linux operating system.

Thomas Georg [3] proposed the issues of implied trust in ethical hacking and highlights the importance of professionalism and ethical behavior.

Namosha Veerasamy [1] proposed the idea of a combined blue and red team methodology for security auditing and penetration testing tasks.

C. M. Rakshitha [2] explores the information security controls and the procedures and techniques to shield data frameworks from unauthorized access to modify data.

Pike, Ronald E [13] describes the mechanisms beyond the classroom-based curriculum to minimize the risk of students committing criminal acts using ethical hacking skills.

Neeraj Rathore [14] explores several hacking activities that came under cybercrime. It also highlights the role of ethical hackers and illustrates the approach to minimize cybercrime.

Hartley, Regina D [15] analyze the use of an ethical hacking pedagogical approach to improve information security instruction. And describes the ethical and legal consequences of teaching students to hack.

Azhar Ushmani [16] describes the phases of hacking, the impact of hacking on businesses, and the purpose of ethical hacking.

K.Bala Chowdappa [12] discusses the overview of hacking, how ethical hacking disturbs security, and how malicious and ethical hackers are different. They discussed the hacking categories with different types of methods of penetration testing.

OMOYIOLA Bayo Olushola [17] analyze the acceptability and legality of ethical hacking and why it is not a criminal activity.

Miguel Hernandez [18] analysis the characteristics that make up a mobile device, the different risks to which they are exposed, and vulnerabilities.

Abhineet Anand [10] describes who hackers are, what ethical hacking is, the code of conduct of ethical hackers, and the need for them.

C.C.Palmer [19] proposed testing the security of a system by trying to break into it is not new and describes the different ways to attack computer security.

Amruta G. Kashikar [7] describes the role of ethical hacking and it encloses the epigrammatic disclosure about the hacking.

III. Methodology

As we know that ethical hacking is just like how normal hackers work but this is considered legal because you have the permission of the owner of the organizations. So, another analogy for ethical hacking is basically how you will rob a bank. For example, a person is trying to attack the bank then he might take different steps which are as follows:

Fig. 1. Ethical hacking phases

A. *Information Gathering*

It includes different timings for the bank, how the different cameras are working inside the bank, how the different types of people are working inside the bank, how the security is being maintained, how the people of the security are interchanging being each other, and all other crucial data and information. In this, hackers use different types of tools, for example, network mapping tool as it is a very helpful tool for doing an internal hack, it helps in finding the topology of networks. It includes all the information about the target and finding vulnerabilities in the different

systems. It means study about the organization. In this, the hacker tries to see what's the IP addresses. Hackers usually collect information about the host, people involved in this, or networking. It takes a lot of time. In the end, the hacker should have a bunch of information about the target.
It is basically of two types:

Active: directly interacting with the target.

Passive: indirectly interacting with the target.

B. Scanning

In the scanning phase, the hacker scans every component of the system or the website to find the vulnerabilities. It includes what kind of ports, what kind of services does the bank is using. These services could be related to that like cash, registries coming into the bank to refill the atm, etc. It also includes what type of software banks are using, what type of guns security guards are using. This phase includes the usage of tools like sweepers, port scanners, and vulnerability scanners to scan the data. Port scanners are used for network mapping. It obtains target IP addresses, user accounts, etc.

Three processes are involved in scanning tools:

- Port scanning: This is used to find the vulnerabilities in the system. In this, hackers have to locate the host and the used topologies of the target organization.
- Network scanning: In the network scanning, hackers identify the active host which is present on a network.
- Vulnerability scanning: This type of scanner is installed on the target network to determine the safety threats.

C. Gaining access

It includes how you are going to enter into the bank and how you will perform different types of activities with the bank. This is the real part of the hacking procedure. You have seen that these are the vulnerabilities or exploitations present in the system. Then the hacker will use these exploitations to gain access. In this, the hacker uses all the information discovered in the above two phases to enter the bank. So, the hacker needs to gain access if they behave like a robbery. This phase is also known as 'Owning the system'. Finally, the hacker gains access to the target by using different tools and techniques. When the system is accessed, the hacker must reach a certain level to modify data.

D.Maintaining access

Maintaining access is another phase of the ethical hacking methodology. Hackers have to maintain access to the system for the attacks that they are not able to remove you from the system. This step involves maintaining access to the target until the hacker completed the tasks. In this, hackers have so many accounts. He starts to look for and change the password according to him to maintain access to the network.

E. Clearing tracks:

Once the hacker has completed all the processes, if a hacker is going inside the bank with the secret method then he will clear all the cookies and cache, uninstalling all applications that he or she can be used. All the folders that are created, applications installed will delete in this phase.

Tools used by Ethical Hackers:

There are so many tools that are used with ethical hacking. Some of the important tools are as follows:

1. *NMAP*: NMAP stands for Network Mapper. It is an open-source tool that is used widely for network discovery.
2. *Metasploit*: It is one of the most powerful exploiting tools. This tool is available from a company which is known as rapid 7. It is also used with the graphic user interface. It can perform basic penetration testing.
3. *Burp suite*: It is mainly used for tracking your request and responses between the servers and clients.
4. *Linux:* Linux® is an open-source operating system (OS). An operating system is software that directly manages a system's hardware and resources, like CPU, memory, and storage.

IV. Case Study:The Holiday Hacker

Here is a story of one organization. Hacker waits to hack on holiday. When 'Time Hop' introduced information of 21 million in 2018, it published a timeline. In that timeline, the corporation of the organization found out that the hacker waits for the 4th of July to execute an attack.
How did the breach start?
Time Hop says the hacker gets admission, after which the attacker creates an account within the system. then he checked again and again and after collecting some essential information he logs out and waits for some more time. Then on 4th July 2018: the cyberattack begin hacker logs in at 2:04 pm. On 5th July: it manages the aftermath of the cyberattack
6:09 am – He logs in and lists Cloud Computing Environment users, and logs out.
12:10 pm – Time Hop engineers start the research.
12:30 pm – Time Hop engineers log carefully and finish that has been attacked.
An incident is declared.
As a result, the attacks take only 22 hours and changed into further days for the attacker to get admission to the network.

Notable Hacking Groups: Legion of doom, Anonymous, Lizard Squads, Masters of Doom

V. Types of Attacks

There are three forms of attacks an attacker can use that are as follows:

A. Physical: In a physical attack, hackers use different kinds of bombs or instruments to destroy the data. It also includes breaking into the piece of equipment and collects some crucial information through garbage cans.
B. Syntactic: In a Syntactic attack, hackers use different types of viruses, malware, trojan horse to disrupt a system.
C. Semantic: In a Semantic attack, firstly hacker approaches a target, then causes an error to the system.

These three are classified into some specific hacking tricks. A few of them are discussed below:

- *Waterhole attacks*: In this, the attacker targets someone at the place.
  For example, a person is in a coffee shop. Then he or she may normally use the Wi-Fi which is available in that coffee shop. An attacker may monitor your schedule then he creates a fake Wi-Fi access point in the shop and modifies all interested websites. When you join with that fake access, the attacker will be able to modify your personal information.

- *Clickjacking:* This is also known as user-interface redressing. In this, you may click on something that you can see as a link or button but there is a virtual, so it may results error to that system.
  For example, a user uses a website and then clicks on a button to close the window. But he or she didn't know that attacker invisibly monitoring your schedule and he placed a button that will raise issues, delete the firewall rules, and trigger the download of a trojan horse.

- *Cookie Theft:* It occurs when an attacker steals a cookie and uses that cookie for a session. It is also considered a form of session hijacking.
  For example, a user login into Facebook, the website sends them a cookie. If he or she is browsing the net in a public place then the attacker will be able to read messages and so on.

VI. Mitigation Of Vulnerabilities

Mitigation usually refers to reduce the risks of cyberattacks. As we have a lot of businesses online, hackers trapping up their businesses and then they sell to other people, their servers, their products, and everything that can be possible. So, it is become even more important to protect these businesses and people from attackers who can cause potential harm. Then, you can take a chance with mitigation. At least, Mitigation will help you to reduce the risks of a company data breach.

The most important thing that you can do against cyberattacks is to fortify your network access. By using this, you can easily mitigate some chances of getting enraged. It helps you to limit your exposures to mobile apps, cloud computing, where other crucial information could be exposed to hundreds of other users. As soon as possible, install data scanners and security services to know about the status of your businesses that the company data breach is protected or not. Research and investigations are the most effective ways to mitigate cyberattacks. But most of the time, some companies don't know their shortcoming until anyone has already found and exploited them. It can be also costly to managing so many security devices for your organization. So, to overcome this problem, you can find some more manageable solutions to cyberattacks, while your information technology security teams will help you to find the correct solution to a problem instead of using some costly tools. They help you to protect your computer system or networks from unauthorized access or cyberattacks that are aimed at exploitation. So, before purchasing so many costly tools, you can take help from this team then after their suggestion, you can go for these tools. Mitigation of a vulnerability is only a temporary measure. You can also test the new software and obtain cooperation from system owners and business managers who are responsible for fixing security vulnerabilities and other bugs.

SAP also helps to analyze and neutralize cyberattacks when did they happen and before damage occurs. There are so many SAP terminologies such as GUI, transactional data, user profile, master data, Workflow, etc. There are so many varieties of management modules within systems, applications, and products, including project management, transportation management, customer management, and inventory management. The first steps for security control in the SAP environment become the most confusing. So, you will need a framework for SAP protection processes.

SAP Cybersecurity Framework gives you 3 step roadmaps towards the realization of each ERP security process. The first process is the minimum. The second step requires a medium level of the try and it provides you a basic level of security, and the third step includes all the high-level things.

VII. Conclusion

This paper highlight the issues of hacking and how it can be made successful for the organization to safeguards the password, login id, credit card info, and other crucial information. Ethical hacking shows positive behavior towards network security and that's why everybody depends on it. This paper illustrates the importance of the moral hacker. As many peoples think that malicious hacking is a computer crime but Ethical hacking is not a criminal activity. It is considered legal because the hacker takes permission from the owner of the organization to hack the network security. They automatically provide security to malicious attacks that can be created or exploited by the attacker to hack the system.

References

[1] Namosha Veerasamy, "High-Level Methodology for Carrying out Combined Red and Blue Teams", Computer and Electrical Engineering 2009. *ICCEE '09*. Second *International Conference on, vol. 1, page number- 416-420, 2009.*

[2] C. M. Rakshitha, "Scope and Limitations of Ethical Hacking and Information Security", Electronics and Sustainable Communication Systems 2020 International Conference on, page number 613-618, 2020.

[3] Thomas Georg,(2018).Issues of Implied trust in ethical hacking.ORBIT Journal,2(1) 10.29297/orbit.v2il.77,

International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 3 Issue 6 October 2019 available Online:www.ijtsrd.com e-ISSN:2456-6470

[4] Gurpreet K. Juneja," Ethical hacking: A technique to enhance information security" international journal of computer applications (3297: 2007), vol. 2, Issue 12, December

[5] Study of Ethical Hacking a paper by (Bhawana Sahare, Ankit Naik, Shashikala Khandey) http://www.ijecs.in/issue/v4 i4/68%20ijecs.pdf

[6] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala, "Ethical Hacking", International Journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010

[7] Deepak Kumar, Ankit Agarwal, Abhishek Bhardwaj, http://www.ijcstjournal.org/volume-2/issue-6/IJCST-V2I6P2.pdf

[8] J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? ", International Journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.

[9] Aman Gupta, IJECS Volume 6 Issue 4 April 2017 Page No. 21042-21050

[10] Bansal, A., & Arora, M. (2012). Ethical Hacking and Social Security. Radix International Journal of Research in Social Science, 1(11), 1-16.

[11] K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (3), 2014, 3389-3393

[12] Pike, Ronald E. (2013) "The "Ethics" of Teaching Ethical Hacking," Journal of International Technology and Information Management: Vol. 22: Iss. 4, Article 4.

[13] NK Rathore - Journal on Information Technology (JIT), 2016 - researchgate.net

[14] Hartley, Regina D. (2015) "Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack," Journal of International Technology and Information Management: Vol. 24: Iss. 4, Article 6.

[15] International Journal of Information Technology (IJIT) – Volume 4 Issue 6, Nov-Dec 2018 ISSN: 2454-5414 www.ijitjournal.org Page 1 Ethical Hacking Azhar Ushmani

[16] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 61-63 www.iosrjournals.org The Legality of Ethical Hacking OMOYIOLA Bayo Olushola

[17] International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16637-16647 © Research India Publications. http://www.ripublication.com 16637 Ethical Hacking on Mobile Devices: Considerations and practical uses. Miguel Hernandez

[18] Ethical Hacking by C. C. Palmar; IBM research division