Assessing the tools and techniques used in Ethical Hacking

Pradeep Nagaraj
MSc.Computer Science, ***1140698***
nagarajp@lakehaedu.ca
Lakehead University, Thunder Bay

***Abstract*—While communication technologies have brought the world closer together, they have also created uneasiness among system owners around the world. Security is a major concern in today's world, and everything should be done safely and securely. Hacking, specifically cracking computer systems, is the primary cause of this insecurity. Hacking is a procedure in which an individual or group exploits a system's flaw for personal gain or enjoyment. Ethical hacking is the technique of breaking into a network with good intentions and in an ethical manner to protect the system from being hacked. For organizations and governments, ethical hacking, also known as penetration testing or intrusion testing, has become a major concern. Companies are concerned about being "hacked," while potential customers are concerned about keeping control of their personal information. This paper introduces a detailed analysis of ethical hacking, the need for Ethical hacking, and major tools used in ethical hacking. This paper also identifies the code of conduct for an Ethical Hacker and its need. I intend to complete the mentioned project within 2 months but to analyze from hackers perspective and implement or achieve the mentioned security issues or vulnerabilities in a organization system, it will take time to develop a secured system. The main motivation behind this topic is the wide usage of the Internet, which leads to security concerns and fear of losing personal information and the potential of being hacked.**

I. INTRODUCTION AND BACKGROUND

The internet has accelerated the digitalization of several activities such as banking, online purchases, online financial transactions, collaborative computing, e-mail, and new avenues for advertising, information distribution, and data gathering. With the rapid development of the internet and the increasing number of users, the risk of data security is increasing, and the problem of information security is becoming extremely important. Because most technical advancements have made all information available online, some people use it to gain knowledge, while others use it to disrupt or steal information from websites or databases without the owner's knowledge. HACKING is the terminology used for this dark side.

A. *Hacking*

Hacking is the process of identifying and exploiting weak links or gaps in computer systems or networks in order to obtain unauthorized access to data or modify the features of the target computer systems or networks. Hacking is the alteration of computer hardware, software, or networks to achieve goals that are not aligned with the interests of the users. It's also known as breaching someone's security and capturing personal or confidential information such as contact information, credit card numbers, internet banking credentials, and so on.

The methodology or the steps followed by the Hackers [1], as follows

- **Reconnaissance:** Reconnaissance is the process of gathering information about a target system. This is also referred to as "footprinting." The hacker gathers information on the company that will be hacked. The process requires locating vulnerabilities in the computer system, which entails determining which paths have been left open to attack. If the hacker can get access to the system, he or she will advance with the hacking process. The hacker has a lot of information at the end of

the reconnaissance phase, and he can use it to build a viable attack on the target system.

- **Scanning:** The hacker wants to know which system is up, what programs are being utilized, and what versions of the programs are being utilized before launching an assault by creating a blueprint of the target network. The actual IP addresses of the target network, as well as the services that are running on those systems, are all included in the blueprint. The information obtained during the reconnaissance phase is utilized to inspect the network in this phase, which includes the use of tools such as diallers and port scanners [1].
- **Gaining Access or Control:** The information obtained in the previous two phases is utilized to enter and take control of the target system over the network or physically in this phase. This is an actual hacking phase that gives the hacker entry to the hacker system. When it comes to system hacking, the first hacker will attempt to gain access to the system, often referred to as "Owning the System."
- **Maintaining Access:** Now that the hacker has gained access to the system, he begins uploading and downloading files. After acquiring access to the system in the previous stage, the hacker keeps it for future attacks and makes changes to it so that no other security personnel or hacker can acquire access to the compromised system. The attacked system is referred to as the "Zombie System" in this situation.
- **Clearing Tracks:** It is the technique of erasing any remaining log files or other sorts of evidence on the hacked system that could lead to the hacker's capture. The hacker's login will be saved in the login log whenever he or she downloads a file or install the software. Hackers typically hide their tracks by removing log files, audit files, and registry files containing failed log-in attempts and suspicious network behavior.

In the 1960s, programmers at MIT invented the term "hacker" to characterize someone who could understand and manipulate technology [2]. Hackers have moved beyond only manipulating technology to manipulating people, such as through phishing and a wider range of social engineering techniques. Although hackers continue to exploit technology, their position and nature have also progressed. Hackers are currently classified into three major categories [3] based on their intentions: black-hat, white-hat, and gray-hat.

- **Black hat:** The black-hat hacker is the most well-known form of a hacker; they violate computer security for personal benefit. A "Cracker," a more advanced form of the black-hat hacker, is a computer hardware and software expert who breaks into someone's security with evil intent or bad intentions of stealing or damaging their important or secret information, compromising the security of large organizations, or shutting down or modifying the features of websites and networks. However, they are extremely difficult to locate because they are true experts in both the skills and understanding domains.
- **White Hat:** A white-hat hacker is a computer security expert who breaks into and finds security vulnerabilities in an organization's or company's protected networks or computer systems, then fixes them to improve security. With some certificates (CEC - Certified Ethical Hackers), White-Hat is characterized as the nice guys or "ethical hackers". White Hat Hackers utilize their talents and knowledge to protect an organization before malicious or bad hackers discover it and cause harm to it. White-hat or ethical hackers are hired by companies to secure their systems and prevent them from other hackers. Even though their methods are similar to those used by black-hat hackers, they have permission from the company or organization that hired them. Following the completion of the engagement, the ethical hacker will produce a report of findings, which will typically include recommendations for how to secure the systems.
- **Grey hat:** A grey-hat hacker is a hybrid of black-hat hackers who work with malicious intent to exploit computer systems and white-hat hackers who strive to keep systems secure. A grey hat hacker is a computer hacker or security expert who occasionally breaks the

law but, unlike black hat hackers, has no bad intentions. Grey hat hackers are those who are sponsored to hack. Because they can quickly switch from black-hat to white-hat hacking and vice versa, grey-hat hackers are among the most dangerous types of hackers.

Even though internet security is improving, hackers continue to find ways to breach systems. Emerging technologies, such as social media, cloud computing, smartphone technology, and vital infrastructure, have become increasingly dangerous. If a company is hacked, sensitive data such as business process documentation and trade secrets, as well as employee and customer contact information, might be stolen. Hackers can potentially harm data by removing or modifying it, as well as causing hardware damage. If someone else's data is stolen or an organization is unable to fulfil contracts due to hacking concerns, the consequences of hacking might include legal liability. Hackers can make use of exploits, or faults in computer systems, to obtain access to information they shouldn't have. Damage to digital data or even physical equipment can occur as a result of hacking. In order to harm their targets, some hackers may purposefully destroy data. In some circumstances, valuable data may be accidentally corrupted or lost due to hacker intrusion or the tools used by hackers. If hackers aren't paid, data may be encrypted and held for ransom, rendering it unusable. Hackers may also utilize computers that control other devices to harm hardware or physical equipment in rare situations. A defender must understand an attacker's thought process and approach, as well as the tools available to them. A hacker attack can cause a lot of damage to a company. When an organization survives an attack, it must make significant modifications to its defenses and implement a new philosophy, generally with new personnel. Some companies outsource their security. As a result, many new independent businesses might benefit from focusing on hacking avoidance. Because of their limited staffing and financial resources, small and medium businesses may benefit from outsourcing [4] [5]. To protect systems from hackers necessitates the promotion of Ethical Hackers, who will fight back against illegal attacks on our computer systems. Ethical hacking is the process of examining security flaws and identifying prospective security vulnerabilities for an organization in charge of the information technology environment under attack [6].

II. RESEARCH QUESTIONS

Ethical hackers use many tools and techniques to find vulnerabilities in the system. Ethical hackers utilize the same methods as hackers to evaluate a security system as their less ethical counterparts, but instead of exploiting flaws, they report them. Ethical hacking and penetration testing are often used interchangeably since they are so closely related.

RQ: Who are Ethical Hacker's and what they do?

Ethical hacking also known as Penetration testing, intrusion testing is a process of evaluating computer and network security flaws and vulnerabilities. Ethical hacking is used to determine whether a system's security is effective or ineffective. The main objective of ethical hacking is to find security holes in a controlled environment so that they may be fixed before hackers exploit the system [5]. To find vulnerabilities, ethical hackers use their talents and conduct penetration testing. When making an assessment, special attention is given to data that is extremely sensitive. Penetration testing can be done from a business standpoint to protect the company from failure by preventing financial loss, or from an operational standpoint to discover risks and vulnerabilities. Penetration testing provides comprehensive information about real-world security threats that can be exploited and can quickly uncover the most crucial as well as the least significant vulnerabilities by doing penetration tests.

RQ: Why do we need Ethical Hackers?

Ethical hackers examine the security flaws and identifying prospective security vulnerabilities for an organization in charge of the information technology environment under attack. Every organization should be proactive rather than reactive to find the vulnerabilities in order to secure the system and protect from hackers. It is important to understand the types of Ethical Hacking and tools used.

RQ: How Ethical hackers approach towards finding intruders?

In assessing a system's security, an ethical hacker looks for answers to these basic questions: How

intruder can gain access to the target system? Are they any weak link in the security system? On the target systems, what can an intruder see? What could an intruder do with that data? Is anyone at the target paying attention to the intruder's efforts or successes? It is important to understand about weak links and Vulnerabilities in the system and more important to understand if the organization can track the activities of the intruder, if the owners of the target systems are unaware that someone is attempting to break-in, the intruders can and will try for weeks or months before succeeding.

RQ: Is Ethical Hacking "Ethical"?

On the other hand, there is a lot of debate over ethical hacking. Many people consider that hacking is unethical. However, with the rise of cyber-crime, it is clear that businesses and governments must ensure their cybersecurity is flawless. That takes us to the value of ethical hacking and its application in the digital world. Ethical hacking codes of ethics or conducts focus on the ethical hacker's duties, responsibilities, and limitations when performing his profession. The ethical hacker ensures that the client's system or network has been thoroughly examined for security flaws and vulnerabilities.

III. Research Methodology

Security is a major concern in today's world, and everything should be done safely and securely. HACKERS are one of the darker aspects of computer technology as it evolves. As the technology improves and security has been given utmost importance, the hacker still finds a way to compromise the system. An ethical hacker demonstrates the risks that an information technology environment faces, as well as the steps that can be done to mitigate or accept such dangers. In our paper, we focus on the importance of securing the system from hackers and the potential need for Ethical hackers, types of ethical hacking, and tools with the demonstration of few important tools used to find vulnerabilities and weak links in the system. The rise of cybercrime has made it clear that businesses and governments must ensure their cybersecurity is flawless. Many people consider that Ethical hacking is unethical, but the value of ethical hacking is growing in the digital world. We will outline the Ethical hacking codes of ethics or conducts focus on the ethical hacker's duties, responsibilities, and limitations.

Hackers always try to hack the users of the system rather than hacking the system. For example, usernames and passwords for authentication are weak due to insecure user behavior (choosing weak passwords, reusing passwords, and so on) this provides an easy way for a hacker to compromise the system. By the end of this research, we will be able to identify the need for ethical hacking, important tools, and methods used in penetration testing along with the guidelines or code of conduct that needs to be followed by ethical hackers. All ethical hackers have limitations and constraints which need to be followed as per the EC-Council code of conduct. The ethical hacker's offer some danger to the customer because a criminal hacker monitoring the ethical hacker's communications may be able to intercept the information. Another potential limitation for ethical hackers is that even after finding a potential weak link and re-mediating it, the advancement of technology provides a way for hackers to compromise the system. Every organization should perform penetration testing often, which will incur a cost based on the organization size and the amount of data to be tested.

IV. Schedule and Resources Required

Gantt Chart:

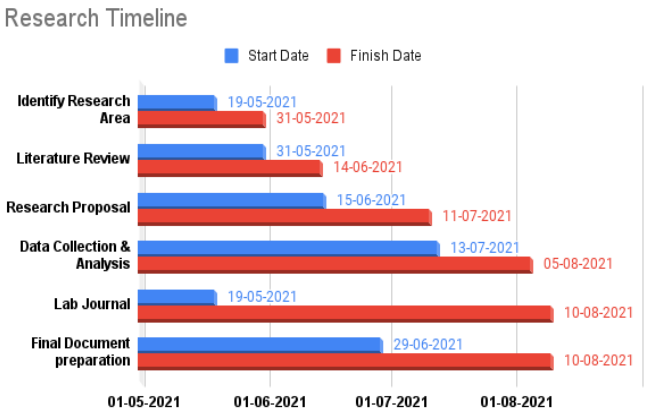

Fig. 1. Research Timeline

Resources Required: To perform penetration testing we use Kali linux. Kali Linux is a Linux distribution based on Debian that is mostly used for advanced penetration testing [8]. It can also be used as a tool for performing security audits. Kali Linux is a complete operating system with over 600 built-in penetration testing tools. The Kali Linux developers propose that the tools can be updated by updating the complete system rather than one software at a time.

V. Summary

The entire world is moving toward technological advancements and increasing digitization of real-world activities, which increases the danger of security. Hacking, specifically cracking computer systems, is the primary cause of this insecurity. As a result, the need to protect systems from hackers necessitates the promotion of Ethical Hackers, who will fight back against illegal attacks on our computer systems. In this paper, I have concentrated on the importance and limitations of ethical hacking or penetration testing, tools used for penetration testing, and guidelines or the code of conduct to be followed by ethical hackers.

Internet security is more proactive, such as Ethical Hackers who attempt to hack into a corporation or organization prior to an 'attack' in order to discover any weak links. Companies engage ethical hackers to hack their own firm and find any flaws where an ill-intentioned hacker could cause damage so that the company can improve its security and cover the risks. Ethical hacking, when done correctly, aids in the discovery of security flaws. Penetration testing is more useful in identifying security flaws in a system. It is important to prevent data loss, financial loss, and the proactive reduction of recognized dangers. They put their creativity and expertise to work to make a company's digital world a reliable and secure environment for both owners and customers. These 'Cyber Cops' are in charge of preventing cybercrime and ensuring the safety of the internet. Hacking is important in the computer system since it deals with both good and bad sides and it attracts lots of debate about ethical hacking. This demands the guidelines or EC-council code of conduct for ethical hackers to focus on the ethical hacker's duties, responsibilities, and limitations when performing his profession.

VI. References

1) GeeksforGeeks, Methodology followed by the Hackers, https://www.geeksforgeeks.org/methodology-followed-by-the-hackers

2) Hacker, "Search Security", https://searchsecurity.techtarget.com/definition/hacker

3) javaTpoint, Types of Hackers, https://www.javatpoint.com/types-of-hackers

4) Z. Cekerevac, L. Prigoda and Z. Dvorak, "Hacking, protection and the consequences of hacking", Communications - Scientific Letters of the University of Zilina, June 2018, DOI:10.26552/com.C.2018.2.83-87

5) Z. Cekerevac and J. Vasiljević, "INTERNET SAFETY OF SME REGARDING THE SECURITY OF ELECTRONIC MAIL", FBIM Transactions, Jan 2014, DOI:10.12709/fbim.02.02.01.05

6) J. Metso, "Penetration testing", Bachelor's thesis - Oulu University of Applied Sciences, Autumn 2019

7) S. Ashwini, K. Thippeswamy, "A Brief Information of Ethical Hacking", 3rd National Conference on Image Processing, Computing, Communication, Networking and Data Analytics (NCICCNDA 2018), April 28, 2018.

8) Wikipedia, "Kali Linux", https://en.wikipedia.org/wiki/Kali-Linux