Ethical Hacking : A Review on Tools, Techniques and Approaches

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

***Abstract*—Security is a major concern in today's world, and everything should be done safely and securely. While communication technologies have brought the world closer together, they have also created uneasiness among system owners around the world. 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. Penetration testing, colloquially known as ethical hacking, is a process of testing and inspecting an information technology environment for probable weak links and vulnerabilities, intending to resolve a system's security flaws. This paper summarises what hacking is, who hackers are, what ethical hacking is, and the process behind ethical hacking and penetration testing.**

***Index Terms*—Hacking, Ethical Hacking, Penetration testing, Vulnerability analysis, Network security, Pen-testing tools ;**

I. Introduction

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, 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.

- **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. This stage is 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 [1]. 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 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.

B. Ethical Hacking - Penetration testing

Despite the fact that internet security is improving, hackers continue to find ways to breach systems. 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. 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 [2]. Ethical hackers utilize the same methods 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. There is, however, a narrow line of distinction between these two terms [3]. Penetration testing is a term that refers to the process of detecting vulnerabilities, dangers, and target environments in order to secure and take control of a system. Ethical hacking, on the other hand, is a broad concept that encompasses all hacking techniques as well as other computer attack strategies. So, in addition to identifying security flaws and vulnerabilities and verifying the target system's security, it goes beyond hacking the system but with authorization to protect the security for future purposes.

Penetration testing, also known as intrusion testing or red teaming, is a process of evaluating computer and network security flaws and vulnerabilities [4]. Penetration testing is used to determine whether a system's security is effective or ineffective. The main objective of penetration testing is to find security holes in a controlled environment so that they may be fixed before hackers exploit the system. 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. We can quickly uncover the most crucial as well as the least significant vulnerabilities by doing penetration tests. 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. Pen-testing is divided into three main types, namely, white box testing, grey box testing, and black-box testing. The type of penetration testing is based on the hacker's level of knowledge against its target and the situation of an organization that wants to test it, whether the scope is to simulate an attack by an insider or an external source [4].

- **White-Box Testing:** White-Box is known as Open box testing. It relies on a thorough understanding of the intended and targeted system, as well as all of its software and firmware components. White box testing is based on the attacker's ability to have a comprehensive understanding of how an organization functions. Because the system has already been fully understood, white-box testing takes less time. As a result, it's ideal for testing algorithms. It also assures that all logical statements are validated, as well as syntax checking for any potential design flaws.
- **Grey-Box Testing:** Grey box is also known as translucent testing. It is based on having limited information about the system from a secondary source. In other words, having only a partial understanding of a system. Because the internal programming is only partially known, it takes longer than white-box testing. It is not, however, appropriate for testing algorithms. In reality, it is non-intrusive and unbiased, with the lowest likelihood of tester-developer conflict.
- **Black-Box Testing:** Black box also known as Closed box testing. It is based upon the fact that testers are unfamiliar with the internal/external system, as well as the software and firmware structure. As a result, such a test is conducted from the perspective of the user rather than the designer. Even if the application used is unknown, a pen-tester can be an expert because testers rely on system inconsistencies. Due to the lack of prior knowledge of the tested system, this testing form takes the longest to complete. However, because many program routes are left untested, it is ineffective for testing algorithms or large parts of code.

This study used the ”methodology approach” of classifying and analyzing penetration testers' tools, strategies, and techniques to detect hackers and possible weak links and vulnerabilities, intending to resolve a system's security flaws and to gain a better understanding of the ethical hacking and penetration testing domains. Defending and assaulting a targeted organization is a constant competition between hackers and ethical hackers. The primary goal of this work is to emphasize the importance of ethical hacking as well as the necessity of performing and conducting penetration testing to safeguard the data. This aids in assessing a company's security and immunity to dangers, hazards, and attacks that have already been identified. This is possible by assessing and mitigating risks. This keeps anyone from becoming a victim of a cyber-attack. As a result, the aim is to enhance the use of pen testing to detect and address any exploitable vulnerabilities or security gaps before hacking attempts.

II. Literature Review

To ensure a much more accurate and successful pen testing process, numerous solutions were presented using various tools and techniques. Rather than just training developing teams, different protective precautions and actions are already being taken into account in order to protect a given system from any cyber-attack based on ethical hacking techniques.

In [6], Rushing et al. described a software project that revolves around network pen testing as well as team-based efforts to solve problems. It was accomplished by utilizing existing network analysis technologies and tools. As a result, the Collaborative Penetration-testing and Analysis Toolkit (CPAT) was introduced as a means for security analysts to ensure a collaborative foundation for conducting pen testing, particularly to aid in the (data) reconnaissance phase. CPAT was introduced as a tool to help network security analysts do pen testing by providing collaborative workspaces as well as reactive data management. Tetskyi et al. [7] demonstrated their technique for pen testing web applications based on the use of Neural Network-Based. Their online service design employs a neural network to generate a decision-assist tool. Despite its ease of implementation and adaptability, the biggest disadvantage of their solution is the large number of requirements to meet the needs of the authorities. Aside from that, the advantage stems from its ease of implementation in comparison to other algorithms, as well as its versatility. Trivedi et al. proposed a Comprehensive Online Tool [WR-3] that discovers security issues in networks [8]. A solution of this type is a given application that can be used to analyze any network security problem. This enables network managers to safeguard their networks in a much more convenient manner. The authors also stated that their offered IDS solution prevents any cross-scripting vulnerabilities while analyzing any requested service (s) for any potential security faults.

Visoottiviseth et al. presented ”Penetration Testing Tool for Internet of Things Devices” shortly PENTOS in [9]. PENTOS assisted customers in identifying any vulnerabilities and risks associated with the IoT device. PENTOS was created by merging numerous technologies, including Kali Linux and Linux APIs for penetration testing. But the authors stated they couldn't finish the research work based on the ZigBee pen-testing module because it necessitates the use of specialized but expensive ZigBee sniffing hardware. Zhou et al. mentioned the ASCFETA (Analysis System for Computer Forensic Education, Training, and Awareness) system in [10]. ASCFETA plays a critical role in the security policy of the organization. The primary goal of this system is to ensure system analysis, which assists any organization in developing the best ASCFETA plan possible. This provides developers and managers with the ability to recognize and address any deficiencies in the computer forensic field.

Shah et al. [11] introduced the ”Net-Nirikshak 1.0” model developed at IDRBT to aid the Vulnerability Assessment and Penetration Testing (VAPT). This tool is completely automated and interactive, requiring no high technical skills or knowledge. As a result, Bank personnel will find it simple to administer the examination themselves. This program can detect and exploit SQL injection vulnerabilities as well as indicate the severity level of each found vulnerability. Goel et al. presented a novel approach to improving vulnerability assessment and penetration testing (VAPT) accuracy in [12]. This methodology tries to improve the accuracy of vulnerability

assessment and pen-testing. In fact, the authors explained VAPT techniques and tools, as well as their limitations, before implementing their own model and developing a software called "VEnsemble 1.0". Such software runs on a variety of VAPT tools and can detect various vulnerability kinds by combining several open-source VAPT tools.

Furthermore, Ning et al. [13] established a pen testing attack model that can effectively represent the relationships between different attack types in sequential order of executed assault. This model also incorporates the situation of the target under assault as well as the attack execution. The results show that this model can successfully teach pen assault and unify its implementation. As a result, it has the potential to be useful in intrusion detection areas. Sandhya et al., on the other hand, relied on Wireshark as a packet sniffer methodology to execute information gathering pen testing in [14]. This technique was used by them to determine if a website was secure or not. According to the authors, the findings indicate that an evaluated website has a flaw in its own security mechanism. Almubairik et al. developed a Threat Model-Driven Approach for Automated Pen Testing in [15]. An algorithm of this type was successfully built to assess the resistance of tested systems to malicious attacks. Instead of utilizing mathematical notations, the method was built for human reading. In addition, the method can also be used in business to implement security measures to mitigate the effects of sensitive data exposure. As a result, business continuity is ensured by assisting security specialists in avoiding the oversight of any threat.

In [16], Abbasi et al. identified experienced hackers based on their specialties using a scalable and generalised framework that analyses the hacker's forum content. Their framework is a social media analytical approach that may be used for many types of User Generated Content (UGC), encompassing both structural and content elements. As a result, any interaction between users and hacking communities, including hackers' Web forums, can be extracted. Gamification is a novel methodology being used by numerous researchers to assess the effectiveness of a given security solution and its performance in a simulated attack scenario. Bailey et al. [17] developed a new technique based on an ethical hacking game, secured by an authorisation infrastructure that observes user action pre/post adaption, in contrast to prior methods. Live studies have demonstrated the capacity to handle the harmful behaviour of genuine and intelligent users while also gathering user responses to new adaptations.

III. Conclusion

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. In this paper, we reviewed, the significance of pen testing, as well as the reliance on trusted ethical hackers to perform simulated attacks, which is emphasized and carefully explored. Through regular auditing, intrusion detection, and excellent system administration, one may secure sensitive data and protect important information from intruders. This enables an assessment of the level of security against known and common threats and assaults. A basic overview of pen testing was provided, as well as the numerous available techniques, technologies, approaches, and tools. An overview of various pen-testing techniques, technologies, approaches, and tools that are now accessible.

Online tools, such as neural network-based web applications, can be used to create a decision-assist tool to assist testers. The Collaborative Penetration-testing and Analysis Toolkit assists network security analysts with pen testing by providing collaborative workspaces. Comprehensive [WR-3] for detecting network security flaws. PENTOS helps customers to discover any IoT device vulnerabilities and risks. For Vulnerability Assessment and Penetration Testing, the IDRBT tool is completely automated and interactive, requiring no high technical skills or knowledge, can detect and exploit SQL injection vulnerabilities as well as indicate severity level of each vulnerability, and the "VEnsemble 1.0" software can discover numerous vulnerability types by merging numerous open-source VAPT tools. Various information gathering techniques in pen-testing establish relationships between different attack types in sequential order of executed assault, as well as the use of the Wireshark tool as a packet sniffer methodology to execute information gathering

and determine if a website is secure or not. A Threat Model-Driven Approach to Automated Pen Testing was developed to measure the resistance of tested systems to malicious attacks. Social media and gaming platforms can be used to analyze hackers' behavior through hacker forum materials and handle the risky behavior of actual and clever users, as well as collect user responses to new adaptations, to understand and guess the psychology of hackers. In conclusion, penetration testers use their knowledge and network skills to find security weaknesses, inform customers and businesses, and secure the system.

IV. REFERENCES

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

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

3) Penetration Testing Vs. Ethical Hacking, "Tutorials point", https://www.tutorialspoint.com/penetration-testing/penetration-testing-vs-ethical-hacking.htm

4) C. Lakshmi, P. Basarkod, "BASICS OF ETHICAL HACKING", International Journal of Engineering Sciences Emerging Technologies, Jan 2015.ISSN: 22316604Volume 7, Issue 4, pp: 715-720.

5) 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.

6) D. Rushing, J. Guidry and I. Alkadi, "Collaborative penetration-testing and analysis toolkit (CPAT)," 2015 IEEE Aerospace Conference, 2015, pp. 1-9, doi: 10.1109/AERO.2015.7119262

7) A. Tetskyi, V. Kharchenko and D. Uzun, "Neural networks based choice of tools for penetration testing of web applications," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 402-405, doi: 10.1109/DESSERT.2018.8409167.

8) A. Trivedi, "A comprehensive online tool [WR-3] that detects security flaws in networks," 2010 3rd International Conference on Computer Science and Information Technology, 2010, pp. 316-320, doi: 10.1109/ICCSIT.2010.5564578.

9) V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart and S. Chotivatunyu, "PENTOS: Penetration testing tool for Internet of Thing devices," TENCON 2017 - 2017 IEEE Region 10 Conference, 2017, pp. 2279-2284, doi: 10.1109/TENCON.2017.8228241.

10) Y. Zhou and K. Jiang, "An Analysis System for Computer Forensic Education, Training, and Awareness," 2012 International Conference on Computing, Measurement, Control and Sensor Network, 2012, pp. 48-51, doi: 10.1109/CMCSN.2012.13.

11) S. Shah and B. M. Mehtre, "An automated approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014, pp. 707-712, doi: 10.1109/ICACCCT.2014.7019182.

12) J. N. Goel, M. H. Asghar, V. Kumar and S. K. Pandey, "Ensemble based approach to increase vulnerability assessment and penetration testing accuracy," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016, pp. 330-335, doi: 10.1109/ICICCS.2016.7542303.

13) Z. Ning, C. Xin-yuan, Z. Yong-fu and X. Si-yuan, "Design and Application of Penetration Attack Tree Model Oriented to

Attack Resistance Test," 2008 International Conference on Computer Science and Software Engineering, 2008, pp. 622-626, doi: 10.1109/CSSE.2008.1137.

14) S. Sandhya, S. Purkayastha, E. Joshua and A. Deep, "Assessment of website security by penetration testing using Wireshark," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp. 1-4, doi: 10.1109/ICACCS.2017.8014711.

15) N. A. Almubairik and G. Wills, "Automated penetration testing based on a threat model," 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, pp. 413-414, doi: 10.1109/ICITST.2016.7856742.

16) A. Abbasi, W. Li, V. Benjamin, S. Hu and H. Chen, "Descriptive Analytics: Examining Expert Hackers in Web Forums," 2014 IEEE Joint Intelligence and Security Informatics Conference, 2014, pp. 56-63, doi: 10.1109/JISIC.2014.18.

17) C. Bailey and R. Lemos, "Evaluating Self-Adaptive Authorisation Infrastructures Through Gamification", 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018, doi:10.1109/DSN.2018.00058.