A REVIEW PAPER ON ETHICAL HACKING

Mrs. Shallu Dogra
Assistant Professor, Dept of CSE
HIET GROUP OF INSTITUTIONS, Shahpur, HP, India

Nitin Singh, Ayush, Sahil
Student of CSE
HIET GROUP OF INSTITUTIONS, Shahpur, HP, India

ABSTRACT

Ethical Hacking is a proactive approach to cybersecurity that involves authorizing and systematically testing information systems to find vulnerabilities before they can be exploited by criminals. Ethical hackers are network and computer experts who attack security systems on behalf of their owners, looking for vulnerabilities that can be exploited by malicious hackers. The explosive growth of the Internet has given rise to many good things, including electronic commerce, email, collaborative computing, and new areas of advertising and information distribution. Ethical hacking, also known as penetration testing, or red teaming, has become a major concern for businesses and governments. Organizations are concerned about the possibility of being "hacked" and potential customers are concerned about having their personal information under control. Hackers are classified according to their work and knowledge. White hat hackers are ethical hackers. Ethical hackers use hacking techniques to ensure security. Ethical hacking is necessary to protect systems from damage.

KEYWORDS: Cybersecurity, Ethical Hacking, It's Impact, Vulnerability Assessment, Security Tool, Cyberthreats

1. INTRODUCTION

Computer technology is constantly evolving. They also have their uncertainties. With the rapid development of the Internet, a lot of information is spread over the Internet, so information security is very important. The Internet has led to the expansion of digital privacy risks and the digitalization of many environments, such as banking, online commerce, online payments, and sending and receiving various types of information over the Internet. Today, many organizations, institutions, banks, and websites are targeted by hackers due to various types of attacks. These people have computer skills and try to access other people's security systems to access their own information, but this is not always the case. We have honest hackers in this field to prevent the threat of hacking by programmers who are beloved by computer experts but are restricted or very specialized due to the combination of rules and multiple organizational changes. Ethical hacking is the deliberate and authorized investigation of computer systems, networks, and applications to identify vulnerabilities before they can be exploited by malicious attackers. Unlike black hat hackers who engage in criminal activities for personal gain or to disrupt businesses, honest hackers operate within the law and with the permission of the system owner. The main purpose of a breach is to expose weaknesses in security measures, allowing organizations to strengthen their defenses and improve their overall security.

2. ETHICAL HACKING

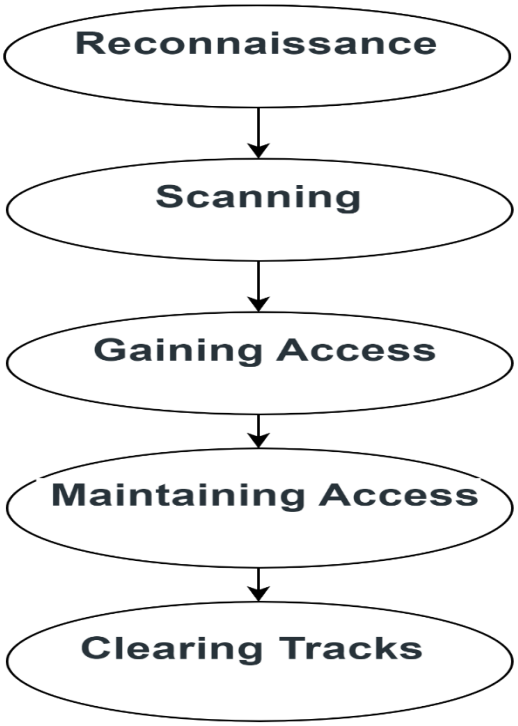
Ethical hacking is the process of finding flaws in systems or organizational structures that hackers can use to exploit an individual or organization. They use this technique to aid in cyberattacks and security breaches by legitimately entering systems and finding vulnerabilities. Honest hackers follow the process and allow the bad hackers to enter and test the organization's policies and networks. Criminal justice is the deliberate act of gaining unauthorized access to computer systems, operations, or data using the tactics and malicious behavior of hacker .This practice helps identify vulnerabilities that can be fixed before malicious actors have a chance to exploit them. With the approval of the IT asset organization or owner, honest hacking accusations are the result of malicious activity.

2.1 ETHICAL HACKER

An ethical programmer, also known as a white hat programmer or penetration analyst, would be a cybersecurity professional who uses their skills and knowledge to help organizations improve by identifying and resolving vulnerabilities. Unlike rogue employees who abuse security measures to harm or harm people, honest employees do so with permission, in accordance with the law and ethics. Honest hackers would be cybersecurity professionals who use their skills to help protect organizations' systems, systems, and data from malicious attacks. Unlike black hat employees who take advantage of adverse situations to harm or harm people, white hat employees follow the rules and ethics with the approval of the framework owner.

2.2 PHASES OF ETHICAL HACKING

Therefore, each stage is important to the entire process of hacking as part of the organization's efforts to strengthen its security posture**.**



- **RECONNAISSANCE**

Reconnaissance is often referred to as the preparatory phase, where hackers gather important information about the target before launching an attack. This phase is done before exploiting the system. The first step in scouting is dumpster diving. Hackers scan the data dump to uncover important information, such as old passwords and the names of key employees (like the head of cyber). Hackers then perform a process called foot printing, which helps them understand the security target. They focus on specific IP addresses, identify system vulnerabilities, and create network plans to better understand and access systems. The footprint provides important Information such as domain names, TCP and UDP services, system names, passwords, etc. Employees are now happy with things like fraud, etc.

- **SCANNING**

Hackers are looking for a quick way to access your network and gather information. There are three scanning methods: pre-attack, port scanning/sniffing, and data extraction. Each level presents a unique vulnerability that hackers can use to exploit weaknesses in the system. During the pre-attack, hackers will search your network for information based on the information obtained during the search. During the port scanning or sniffing phase, information is collected by tools such as dialers, port scanners, vulnerability scanners, and other devices. Finally, during data extraction, the attacker collects detailed information about the port, active computer, and operating system to prepare for the attack.

- **GAINING ACCESS**

This is where honest hackers do real hacking. Using all the data collected and analyzed in the first two stages, the attackers create a comprehensive attack on the system or network they are trying to access. They use all the quirks to control the impact. During this time, the hacker can access all available information, cause physical damage, infect the system with viruses and other malware, or control the system for their own benefit.

- **MAINTAINING ACCESS**

Hackers have a specific role or strategy when accessing an organization's systems. Simply gaining access to a system is not enough malicious operators often use Trojans, backdoors, or rootkits to control this access. This stage can also be an opportunity for further attacks to further damage the organization.

- **CLEARING TRACKS**

This is the final step in the criminal justice process. Once this stage is complete, the integrity manager has access to the system or network. He could do a lot of damage but he didn't want to leave evidence behind. It is important to hide his activities to avoid detection when entering and leaving the network or server. Current security measures should not detect intruders.

3. TOOLS IN ETHICAL HACKING

- **NETWORK HACKING TOOL**

Using hacking tools, you can perform network mapping and inventory, DNS analysis, host analysis, packet sniffing, and even attack simulations to test your network's defenses. Understand the nature of interaction patterns and data flows in large and small networks.

- **WIRELESS HACKING TOOL**

These hacking tools actually work like a radar and can detect invisible signals, allowing users to use tricks to measure the security of a WiFi network, thereby revealing weaknesses such as bad access or bad content.

- **VULNEARABILITY HACKING TOOL**

A vulnerability hacking tool is a software that detects, investigates, and exploits weaknesses in a system, app lication, or network. It helps security professinals and ethical hackers detect vulnerabilities in systems to imp rove security and prevent threats.

- **PASSWORD HACKING TOOL**

Honest hackers use this tool to show how easy it is to crack weak passwords, which helps emphasize the imp ortance of strong and complex passwords.
These hacking tools can crack passwords using a variety of techniquesincluding brute-force attacks, dictionary attacks, and rainbow table attacks.

COMPARING DIFFERENT ETHICAL HACKING TOOLS

TOOL CATEGORY	PURPOSE	STRENGHTS	EXAMPLE	USE CASES
NETWORK TOOL	Network analysis and discovery	Comprehensive visibility, service detection	Superscan, Fping	Specialized for wireless environments
PASSWORD TOOL	Password recovery and cracking	Supports various algorithms, high speed	Hydra, Medusa	Testing password strength
VULNEARABILITY TOOL	Detect security vulnearability	Automated scanning, detailed reporting	Nikto, Nexpose	Security assessments, compliance checks

WIRELESS TOOL	Destroy wireless network	Specialized for wireless environments	Bully, kismet	Auditing Wi-Fi security, securing configurations

IMPACT ON BUSINESSES

Ethical hacking has positive impact on Businesses. Here are some benefits:

Securely Improving Security: By the process of identifying vulnerabilities beforehand of malicious hackers, ethical hacking strengthens a company's overall security posture.

Risk Management: Ethical hackers help in the risk exposure of a business and align resources toward the most important vulnerabilities.

Compliance to Regulation: Many industries are very strict when it comes to compliance. Ethical hacking works to ensure that those companies address this requirement, thereby avoiding fines.

Building Trust: It demonstrates seriousness over security, so it boosts trust among customers and gives them an added incentive to stay.

Cost Savings: Organizations save cost from extortionate rates associated with data breach, attorney fees, remediation, and damaged reputations, which could be saved by the organization through vulnerability preventions.

Effective Incident Response: The practice of ethical hacking enhances an organization's incident response by simulating real-world attacks in order to test the effectiveness of their response policies.

Security culture training and awareness: Education in ethical hacking often brings increased employee awareness about the best security practices and creates a security-aware culture within the organization.

4. CONCLUSION

As long as developers continue to work on the current system, security problems will continue. As long as there is money to find to create temporary and secure solutions to these bad solutions, and the indisputable results of acc ess groups are accepted as evidence that computer systems security is not sufficient security. In any of these areas, a failure can impact the company's connectivity, loss of revenue, reputational damage, o r worse. Every new technology has its advantages and disadvantages. While ethical hackers can help customers beco me more aware of their security needs, it is up to the customer to manage their protection**.**

References:

1. "Is Ethical Hacking Ethical?," Int. J. Eng. Sci. Technol., 2011.
2. S.-P. Oriyano, "Introduction to Ethical Hacking," in CEHTMv9, 2017.
3. Chowdappa Bala K., Lakshmi Subba S. P.N.V.S. Kumar Pavan, International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, "Ethical Hacking Techniques with penetration testing
4. https://searchsecurity.techtarget.com
5. S. Tulasi Prasad, "Ethical Hacking and Types of Hackers," Int. J. Emerg. Technol. Comput. Sci. Electron., 2014.
6. Certified Ethical Hacker - CEH Certification | EC-Council." *EC-Council*. N.p., 2018. Web. 14 Dec. 2018.
7. Marsh, Devin. "Are Ethical Hackers The Best Solution For Combating The Growing World Of Cyber-Crime?." *Jewlscholar.mtsu.edu*. N.p., 2017. Web