IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, January 2023

A Review Paper on Ethical Hacking

Sayed Suhel Mohd Salim
Anjuman-I-Islam's College of Hotel & Tourism Management Studies & Research, Mumbai

Abstract: *An ethical hacker is a network expert and computer who breaches security systems on their owner's behalf in an attempt to find vulnerabilities that a malevolent hacker could exploit. The Internet's rapid expansion has brought about a number of positive developments, including e-commerce, e-mail, collaborative computing, and new avenues for information delivery and advertising. Businesses and governments are becoming very concerned about ethical hacking, sometimes referred to as penetration testing, intrusion testing, or red teaming. Potential customers are worried about maintaining control over personal information, and organizations are worried about the likelihood of being "hacked". Hackers are categorized based on their expertise and area of work. The ethical hackers are known as white hat hackers. Hacking techniques are used by ethical hackers to guarantee security. To shield the system from the harm that hackers can cause, ethical hacking is required. The primary goal of the ethical hacking study is to evaluate security and provide the target system owner with a report. This essay offers a concise overview of ethical hacking in all of its facets*

Keywords: Cybercrimes, Clearing Tracks, Computer Security, Ethical Hacking, Scanning and Enumeration

I. INTRODUCTION

Ethical hacking is a relatively new field, but it has quickly become an essential part of cybersecurity. As the world becomes increasingly digitized, so too does the threat landscape. Malicious actors are constantly developing new and innovative ways to exploit security vulnerabilities and gain access to sensitive data. Ethical hackers play a vital role in helping organizations to identify and fix these vulnerabilities before they can be exploited.

Ethical hacking is not just about finding and exploiting vulnerabilities. It is also about understanding the underlying principles of cybersecurity and how to design and implement secure systems and networks. Ethical hackers must also be able to think like an attacker in order to identify the most likely attack vectors.

Technology related to ethical hacking is expanding throughout many spheres of life, especially the computer sector. The right technology should be used to interact with the necessary to protect the common's dominant data. The newest and most cutting-edge computer technology is ethical hacking, which emerged as a result of hackers' intelligence. Every company, no matter how big or little, uses this as the first line of defense to safeguard its data. These days, it can be challenging to discern the genuine intents of the public and even more so to understand the motivations of individual ethical hackers who penetrate weak networks or systems.

Technology is always evolving, and people are discovering resources that support it. When these gadgets end up in the wrong hands, they could spark a heated debate that violates of our constitutional right to seclusion, dignity & freewill.

With the surge of cybercrime, ethical hacking is becoming a potent policy in the battle against online threats. Generally speaking, ethical hackers who are permitted to break into supposedly "secure" computer systems do so with the intention of discovering vulnerabilities so that they can take better preservation measures. The senior staff, and occasionally just two or three board members, are the only ones aware of the attack. Occasionally, the local IT security officers or managers in a company are informed that such an assault is to take place, usually called a "penetration test," and they may even look over the shoulder of the hacker. Nevertheless, this is not always the case. Many ethical hackers work as consultants, while others are paid employees that carry out prearranged hacking tasks on a regular basis.Since there are several specializations within the broad field of ethical hacking, it is not practical to classify all "hackers" into a single, all-inclusive category. A few famous ethical hackers, sometimes referred to as white-hat hackers or sneakers, assist businesses safeguard their systems by hacking without malice in their hearts. A 'black-hat' hacker, on the other hand, is someone who uses their skills to commit cybercrimes, usually with the intention of making money. The 'grey-hat' hackers have been detected and are alerting the company while they look for affected systems.

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, January 2023

The objective of this research paper is to provide a comprehensive overview of ethical hacking, including its definition, principles, benefits, challenges, types, tools and techniques, and ethical considerations.

II. ETHICALHACKING

Ethical Hacker

A white hat ethical hackers is the hacker who exploits for some great cause (such asprotecting some organization). The good people are basically ethical hackers. They have legal permission tointerferewiththeprogramofothers. Theethicalhackersearchports,websites&locatebugs that can be targeted by a cracker. Once the weaknesses for any device are known, the attacks canbedoneeasily.Tobesafeinthisinternetworld,userneedstolearnhowahacker(cracker) can get into his network. Ethical hacking is learning the conception of hacking & applying them to secure any systems, organization for any great cause. Fig.1 describes the levels for ethical hacking consisting of five blocks.

Reconnaissance
Scanning & Enumeration
Gaining Access
Maintaining Access
Clearing Tracks

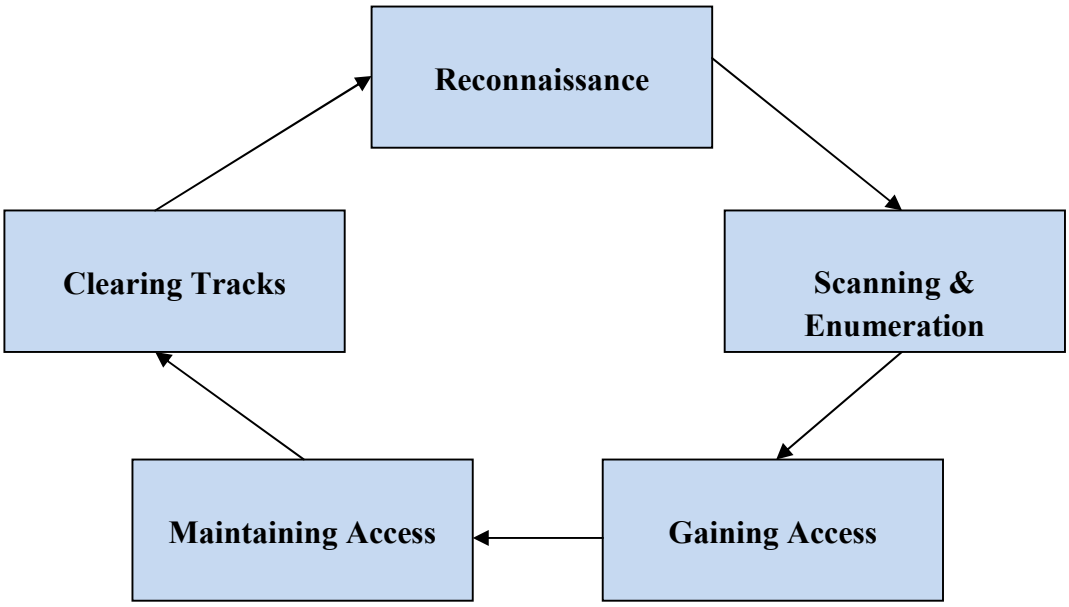

Figure 1 Ethical Hacking Steps

Reconnaissance: It is the set of procedures & technique used to gather information's about the target systems secretly. In this, the ethical hacker seeks to gather as more information as possible about the target systems, following the 7 steps mentioned below.

Identification of active machines
Preliminary information collection
Identification of every ports services
Network mapping
Identification of open ports & access points
OS fingerprinting

Scanning & Enumeration: The 2nd step of the penetration testing & ethical hacking is the enumeration and scanning. Scanning is the common technique that pen tester uses to find the open door. Scanning isworn to determine the weaknesses of the service that operate on the port. They need to figure outthe operating systems included, live host, firewalls, services, intrusion detection, perimeter equipment,routing &general networkstopology

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, January 2023

(physicalnetworklayout) thatare partsofthe targets organization during this phase. Enumeration is the main priority network attack. Enumeration is a producer by actively connecting to it to collect information about the target machine.

Gaining Access: Once the observation is finished & every weakness are tested, the hackers then attempts with the help of some tools & techniques to gain access. This essentially focuses on the retrieval of the password. Either bypass techniques (like using konboot) or password cracking the techniques that can be used for this by hacker.

Maintaining Access: Once the intruder has got access to the targeted systems, he can take advantage of both the systems&itsresources&usethe systemsasacatapult padfortesting &harming other system, orcanretainthelowprofile&continuetoexploitthesystemswithoutthegenuineuserknowing every acts. Those 2 acts will demolish the organization that leads to a calamity. Rootkits gain entrance at the operating systems level, while the Trojan horses gain entrance at the program levels.AttackersthatcanusetheTrojanhorsestomigrateonthesystem userpasswords, names & credit card information's. Organizations that can use tools for honeypots or intrusion detection todetect the intruders.Nonetheless,thehindmostisnotcommendunlessthecompany has the necessary security personnel to take advantage of the defense principle.

Clearing Tracks: For several purposes such as avoiding detection & further penalizing for intrusion, an offender will destroy confirmation of his activities and existence. Eliminating evidence that is oftenreferredtothe'clearingtracks'is therequirementforeveryintruderwhoneedstoremain anonymousandpreventdetectback.Usuallythisstepsbeginsbydeletetheadulterateloginsor all other possible errors messages generated from the attack process on the victim system. For e.g., a buffer overflow attack usually leaves a message that needs to be cleared in the systems logs.Nextattentionisfocusedonmaking changesinordernottologintopotentiallogins. The 1st thing a systems administrator does to trace the system's uncommon activity is to review all the systems log file, it is necessary for trespasser to use the tool to change the system logs so that the administrator cannot track them. Making the system look like it did before they obtain access & set up backdoor for their own use is important for attackers. Any files that have been modified must be swap back to their actual feature's so there is no doubt into the mind of administrators that the systems have been trespasser.

TOOLS USED IN ETHICALHACKING

Tools for Reconnaissance:
Google, Whois Lookup and NSLookup.
Tools forScanning:
Ping, Tracert, Nmap, Zenmap, Nikto WebsiteVulnerability Scanner, Netcraft.
Tools for GainingAccess:
John the Ripper, Wireshark, KonBoot, pwdump7, Aircrack, Fluxion, Cain andAbel.
Tools that are used for the Maintaining Access: Metasploit Penetration Testing Software, Beast, Cain & Abel.
Tools for ClearingTracks:
Metasploit Penetration Testing Software, OS Forensics.

TYPES OF CYBERHACKER

White-hat:

Awhite-hathacker,alsoknownastheethicalhackers,iscelebritywhohasnon-mischievous intent every time they breaks into security systems. Most white-hat hacker is safety specialist, often working with a company to track & enhance security weaknesses legally.

Black-hat:

The ' black-hat ' hackers, sometimes referred to as a ' cracker, ' is celebrity who hack with malicious intent & without permission. The hackers typically want to prove her or his hacking skills & will perform a variety of cybercrimes, such as credit card fraud, identity theft and piracy.Ablackhathackerisapersonwithdetailedcomputerknowledg eaimedatinfringingor bypassing internet security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, January 2023

Grey-hat:
As the color suggests, somewhere between white-hat & black-hat hackers is a ' grey-hat ' hacker, as he or she possesses both characteristics. For example, in search of compromised systems,somegrey-hathackerswillroamintheInternet;likethewhite-hathackers,thetargeted companywillbeawareofanyvulnerability&willpatchthem,butlikethegrey-hathacker,the black-hat hacker will hack without permission.

Blue-hat:
Independent specialist companies for computer security are employed to check a program forvulnerabilitiesbeforeitisreleased,findingweaklinksthatcanberemoved.Bluehatisalso affiliatedwithMicrosoft'sannualsecurityconventionwhereMicrosoftengineers& hackersare able to communicate freely. Blue hat hackers are someone outside of the consultancy firm of computer security who tests a system before it is launched, looking for exploits to be closed. TheBlueHatHackerisalsoreferringtoMicrosoft'ssecurityexecutivetoexecutearbitrarycode in Windows. The word was also connected with Microsoft's annual security convention, the unofficial names associated with Microsoft employee badges from the blue color.

Elite Hacker:
These type of hackers that have prominence as the ' best in the business ' & areregardedas the innovators & experts. The invented language called ' Leets peak' was used by elite hackers to shield their pages from searching engines. A language meant that few letters were replaced in a words by the numerical similarity or other similar letters. The hacker is a common phase used to describe to a person who covertly gains access for the purpose of earning money to systems and networks. However, some practice the creative art of hacking because they get a certain amount of excitement from the test they are put into.

III. REVIEW OF LITERATURE

There is a growing body of literature on ethical hacking. Some of the key works in this area include:
"Hacking: The Art of Exploitation" by Jon Erickson
"The Hacker Playbook: Practical Guide to Penetration Testing" by Peter Kim
"Web Application Hacker's Handbook: Discovering and Exploiting Security Vulnerabilities" by Dafydd Stuttard and Marcus Pinto
"Ethical Hacking: A Hands-On Guide" by Michael Gregg
"CISM Review Manual" by Harold F. Tipton
These works provide a comprehensive overview of the different aspects of ethical hacking, including the tools and techniques used by ethical hackers, the ethical considerations that must be taken into account, and the different types of ethical hacking engagements.

Scope for Study:
The scope of this research paper is limited to the following:
Definition of ethical hacking
Principles of ethical hacking
Benefits of ethical hacking
Challenges of ethical hacking
Types of ethical hacking
Tools and techniques used by ethical hackers
Ethical considerations in ethical hacking

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, January 2023

IV. CONCLUSION

Ethical hacking is an essential part of any organization's cybersecurity strategy. By identifying and fixing security vulnerabilities before they can be exploited by malicious actors, ethical hackers can help organizations to protect their data and systems from attack.As long as builders stick to the current system architectures, which were created without certain security criteria, security issues will persist. As long as funds are available for ad hoc security solutions for these inadequate designs and as long as the fictitious findings of infiltration teams are accepted as proof of computer system security, proper security will not exist. Ensuring the security of a company requires regular monitoring, vigilant detection of intrusions, sound systems management practices, and computer security awareness. A single misstep in any of these locations could expose a business to cyber-terror, lost profits, embarrassment, or worse.Eachnewtechnologyhasitsadvantages &risks.Whiletheethicalhackersthatcanhelpcustomersbetterappreciatetheirsecurityneeds, keeping their guards in place is up to customers.

REFERENCES

[1]. "Is Ethical Hacking Ethical?," Int. J. Eng. Sci. Technol., 2011.
[2]. S.-P. Oriyano, "Introduction to Ethical Hacking," in CEHTMv9, 2017.
[3]. B. Sahare, A. Naik, and S. Khandey, "Study of Ethical Hacking," Int. J. Comput. Sci. Trends Technol., 2014.
[4]. S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security," in IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017, 2018, doi: 10.1109/ICPCSI.2017.8391982.
[5]. G. R. Lucas, "Cyber warfare," in The Ashgate Research Companion to Military Ethics, 2016.
[6]. P. Engebretson, "Reconnaissance," in The Basics of Hacking and Penetration Testing, 2011.
[7]. Ehacking, "Scanning and Enumeration- Second Step of Ethical Hacking,"ehacking,2011.
[8]. R. Baloch, Ethical Hacking and Penetration Testing Guide.2017.
[9]. No rton, "What is the Difference Between Black, White and Grey Hat Hackers?" Emerging Threats,2019
[10]. S. TulasiPrasad,"EthicalHackingandTypesofHackers,"Int.J.Emerg.Technol.Comput.Sci. Electron.,2014.
[11]. Boudreau, L. J. Van't Veer, and M. J. Bissell, "An 'elite hacker': Beast tumors exploit the normal microenvironment program to instruct their progression and biological diversity," Cell Adhesion and Migration. 2012, doi:10.4161/cam.20880.