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 16, May 2023

Ethical Hacking: A Solution for Most Dangerous Threat

Asmita A. Jagtap
Lecturer, Department of Information Technology
Bharati Vidyapeeth Institute of Technology, Navi Mumbai, India

Abstract: *: An ethical hacker is the network specialist and computer, who dive into some security systems seeking responsibility that could be exploited by a malicious hacker. The purpose of ethical hacking can be to deal with the breaches of cyber security with the knowledge of laws and also can be to build an effective cyber security wall against your organization. An ethical hacker can help the people who are suffered by the malicious hacking. Ethical hacker can analyse the vulnerabilities before the attacker may strike. It can help people to recovery the lost information and to perform penetration testing to strengthen computer and the network security. This paper describes about ethical hacking and aspects of ethical hacking.*

Keywords: Hacking, Hacker, Ethical Hacking, Security, Ethics

I. INTRODUCTION

"Security is a state of well-being of information and infrastructure in which the possibility of successful yet undetected theft, tempering and disruption of information and services are kept to low tolerable."

- Network security: Protecting a network and data, computer program, other computer system assets from unwanted intruders, and unauthorized user.
- Information Security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

There are following security services issues as given below

- Confidentiality
- Authentication
- Integrity
- No repudiation
- Access control
- Availability
- Authorization

1. Hacking

The word "Hacking" term refers to the hobby/profession of working with computers. It is describe the rapid development of new program or reverse engineering of existing software to make code better and efficient.

Hacking divided into two terms:

- Ethical Hacking
- Unethical Hacking

1.1 Ethical Hacking: The practice of breaking into computers without malicious intent, simply to find security hazards and report them to the people responsible. Ethical hacker refers to security professional who apply their hacking skills for defensive purpose and constructive purpose.

1.2 Unethical Hacking: Unethical Hacking is "cracking". Cracking activities is breaking the computer security without authorization or uses technology, or tools (usually weak links of a computer, phone system or network) for vandalism, credit card fraud, identity theft, piracy, or other types of illegal activity. So, cracker is refers to person who uses hacking skills or computer system knowledge inoffensive purpose.

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 16, May 2023

II. WHAT IS ETHICAL HACKING?

Ethical hacking technology spreads to diverse areas of life and in particular to every walks of the computer industry. They are required to protect dominant data of the common and should be communicated with the correct technology. Because of the smartness of hackers, ethical hacking arose as the latest and innovative computer technology. To protect their data, every small or large organization adopts this as the front layer of security. Understanding the general public's true intentions in these days is quite a difficult task,& it even more difficult to appreciate the motives of each ethical hacker entering vulnerable networks or systems. Technology is constantly increasing & people are finding resources that endorse them.

Ethical hacking becoming a powerful policy in fighting online threats with the rise of cybercrime. Generally speaking, ethical hackers that are allowed to shatter into ostensibly 'secure' computer system without malevolent intent, but with the goal of finding susceptibility in sequence to conduct about better preservation. Sometimes the local IT security officers or managers in a company are told that such an assault is to take place usually called a 'penetration test' and may even look over the shoulder of the hacker but frequently they are not, & knowledge of the attack is limited to the senior staff, sometimes just 2 or 3 members of the board. Some ethical hackers, also known as a white- hat sneaker or hacker is celebrity who hacks without spiteful intent and helps business secures their systems. However, the opposite is a 'black-hat' hacker who uses his or her abilities to perpetrate cybercrimes, usually to make the profit. Meanwhile, hackers identified the 'grey-hat' hacker are searching for compromised systems & informing the business.

III. ROLE OF ETHICAL HACKERS

Ethical Hacker is network and computer security professional who apply their knowledge and skills in defensive purpose. Roles of ethical are following:

- Evaluate the Weak links of network and computer system.
- Find out the malicious contents from the network traffic.
- Trace out the cyber culprits by using some tools and tracing tools etc.
- Shut down all the doors of network and operating system and information system for security pirates.
- Restricts the unauthorized access of network or system by installing advanced security or IDS system.

IV. TYPES OF HACKERS

White-hat:

A white-hat hacker, also known as the ethical hackers, is celebrity who has non-mischievous intent every time they break 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. A black hat hacker is a person with detailed computer knowledge aimed at infringing or bypassing internet security

Grey-hat:

As the colour 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, some grey-hat hackers will roam in the Internet; like thewhite-hat hackers, the targeted company will be aware of any vulnerability & will patch them, but like the grey-hat hacker, the black- hat hacker will hack without permission.

Blue-hat:

Independent specialist companies for computer security are employed to check a program for vulnerabilities before it is released, finding weak links that can be removed. Blue hat is also affiliated with Microsoft's annual security convention where Microsoft engineers & hackers are able to communicate freely. Blue hat hackers are someone outside of the

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 16, May 2023

consultancy firm of computer security who tests a system before it is launched, looking for exploits to be closed. The Blue Hat Hacker is also referring to Microsoft's security executive to execute arbitrary code in Windows. The word was also connected with Microsoft's annual security convention, the unofficial names associated with Microsoft employee badges from the blue colour.

Elite Hacker:

These types of hackers that have prominence as the ' best in the business ' & are regarded as 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.

V. PHASES OF HACKING

There are five phases of ethical hacking to ensure that all the bases of cyber security are covered while ethical hackers test an organization's network. These phases help in understanding the fundamentals of ethical hacking:

1. Reconnaissance: This is the first phase of ethical hacking and is often known as the preparatory phase. It is the set of procedures & technique used to gather information's about the target systems secretly. Within reconnaissance, the first phase is Dumpster Diving, where an ethical hacker hopes to find useful information such as old passwords, databases of employees, clients, archived financial information, etc. 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

2. Scanning & Enumeration: The 2nd step of the penetration testing & ethical hacking is the enumeration and scanning. Scanning is the process of getting quick access to the outer level of the security framework of any network or system. Scanning is worn to determine the weaknesses of the service that operate on the port. They need to figure out the operating systems included, live host, firewalls, services, intrusion detection, perimeter equipment, routing & general networks topology (physical network layout) that are parts of the targets organization during this phase. Enumeration is

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 16, May 2023

the main priority network attack. Enumeration is a producer by actively connecting to it to collect information about the target machine.

3. 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 bypasses techniques (like using konboot) or password cracking techniques that can be used for this by hacker. Once this happens, the hacker gains access and complete control over the network details and individual systems.

4. Maintaining Access: Once the intruder has got access to the targeted systems, he can take advantage of both the systems & its resources & use the systems as a catapult pad for testing & harming other system, or can retain the low profile & continue to exploit the systems without the genuine user knowing 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. Attackers that can use the Trojan horses to migrate on the system user passwords, names & credit card information's. Organizations that can use tools for honeypots or intrusion detection to detect the intruders. Nonetheless, the hindmost is not commended unless the company has the necessary security personnel to take advantage of the defence principle.

5. 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 often referred to the ' clearing tracks ' is the requirement for every intruder who needs to remain anonymous and prevent detect back. Usually this step begins by delete the adulterate logins or 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. Next attention is focused on making changes in order not to log in to potential logins. 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.

VI. TOOLSUSEDIN ETHICALHACKING

1. Tools for Reconnaissance: Google, Whois Lookup and NSLookup.
2. Tools for Scanning: Ping, Tracert, Nmap, Zenmap, Nikto Website Vulnerability Scanner, Netcraft.
3. Tools for Gaining Access: John the Ripper, Wireshark, Konboot, pwdump7, Aircrack, Fluxion, Cain and Abel.
4. Tools that are used for the Maintaining Access: Metasploit Penetration Testing Software, Beast, Cain & Abel.
5. Tools for Clearing Tracks: Metasploit Penetration Testing Software, OS Forensics.

VII. ETHICS BEHIND ETHICAL HACKING

Ethics in the broadest sense refers to the concern that humans have always had for figuring out how best to live. Ethical hacking uses the principles and techniques of hackers to help businesses protect their infrastructure and information. Secure Ideas makes a business of attempting to hack business's secure networks. This is called penetration testing, and it is a crucial part of any security plan.

Our ethical hacking protects the defenceless customers who trust their information to businesses daily, helps businesses find and fix their security vulnerabilities and ensures a more secure IT world. The ethics involved with ethical hacking are:

- Protecting the Defenceless
- Finding and Fixing Vulnerabilities
- Ensuring a More Secure World
- Trusting the potential enemy
- Risk Management
- Countering the problems

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 16, May 2023

VIII. BENEFITS OF ETHICAL HACKERS

- This helps to fight against cyber terrorism and to fight against national security breaches.
- This helps to take preventive action against hackers.
- This helps to build a system that prevents any kinds of penetration by hackers.
- This offers security to banking and financial establishments.
- This helps to identify and close the open holes in a computer system or network.

IX. LIMITATIONS OF ETHICAL HACKING

- This may corrupt the files or data of an organization.
- They might use information gained for malicious use. Subsequently, trustful programmers are expected to have achievement in this framework.
- By hiring such professionals will increase costs to the company.
- This technique can harm someone's privacy.
- This system is illegal. It hampers system operation

X. CONCLUSION

The security problems will endure as long as construct or remain committed to present systems architectures, generated without some security requirements. Proper security will not be a fact as long as there is funding for ad-hoc & security solutions for these insufficient designs & as long as the delusory results of intrusion team are recognized as evidence of computer systems security.

Regular monitoring, attentive detection of intrusion, good systems management practice & awareness of computer security that all essential components of the security effort of an organization. In any of these places, a single failure could well expose a company to cyber vandalism, loss of revenue, humiliation or even worse. Each new technology has its advantages & risks. While the ethical hackers that can help customers better appreciate their security needs, 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] 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.
[4] P. Engebretson, "Reconnaissance," in The Basics of Hacking and Penetration Testing, 2011.
[5] R. Baloch, EthicalHacking and Penetration Testing Guide. 2017