A REVIEW PAPER ON ETHICAL HACKING

ABSTRACT

An ethical hacker is the network specialist & computer who pounce some security systems on the behalf of its possessor seeking amenability that could be exploited by a malicious hacker. The Internet's explosive growth has conduct many virtuous things: e-commerce, e-mail, collaborative computing & new fields for advertisement and information distribution. Ethical hacking has become a main anxiety for businesses & governments, also known as the intrusion testing or penetration testing or red teaming. Organizations are concerned about the probability of being "hacked" & potential clients are concerned about keeping personal information under control. Hackers are classified according to their work and knowledge. The white hat hackers are the ethical hackers. Ethical hackers use hacking approaches to ensure safety. Ethical hacking is needed to protect the system from the hacker's damage. The major reason behind the ethical hacking study is to assess the security and report back to the owner of the target system. This paper provides a brief ideas of the ethical hacking & every aspects.

Key words: Cybercrimes, Clearing Tracks, Computer Security, Ethical Hacking, Scanning and Enumeration.

Cite this Article: Prabhat Kumar Sahu, Biswamohan Acharya, A Review Paper on Ethical Hacking, International Journal of Advanced Research in Engineering and Technology, 11(12), 2020, pp. 163-168.
http://iaeme.com/Home/issue/IJARET?Volume=11&Issue=12

1. INTRODUCTION

Ethical hacking technology spreads to diverse areas of life and in particular to every walks of the computer industry. The required to protect dominant data of the common should be communicate with the correct technology. Because of the smartness of hackers, ethical hacking arose as the latest and innovative computer technology [1]. 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. These devices fall into the inaccurate hands, they may create good controversy in violation of our constitutional right to seclusion, dignity & freewill.

Ethical hacking becoming a powerful policy in fighting online threats with the rise of cybercrime [2]. 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. Many ethical hackers works for consultants & others are wage-earning workers who regularly perform a scheduled hacks program [3]. In the widespread discipline of the ethical hacking, there are a number of specialisms; therefore, it is unfeasible to group every 'hackers' into the comprehensive classification. 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 [4].

2. ETHICAL HACKING

1. Ethical Hacker

A white hat ethical hackers is the hacker who exploits for some great cause (such as protecting some organization). The good people are basically ethical hackers. They have legal permission to interfere with the program of others. The ethical hacker search ports, websites & locate bugs that can be targeted by a cracker. Once the weaknesses for any device are known, the attacks can be done easily. To be safe in this internet world, user needs to learn how a hacker (cracker) can get into his network [4]. 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 [5].

- Reconnaissance
- Maintaining Access
- Scanning & Enumeration
- Gaining Access
- Clearing Tracks

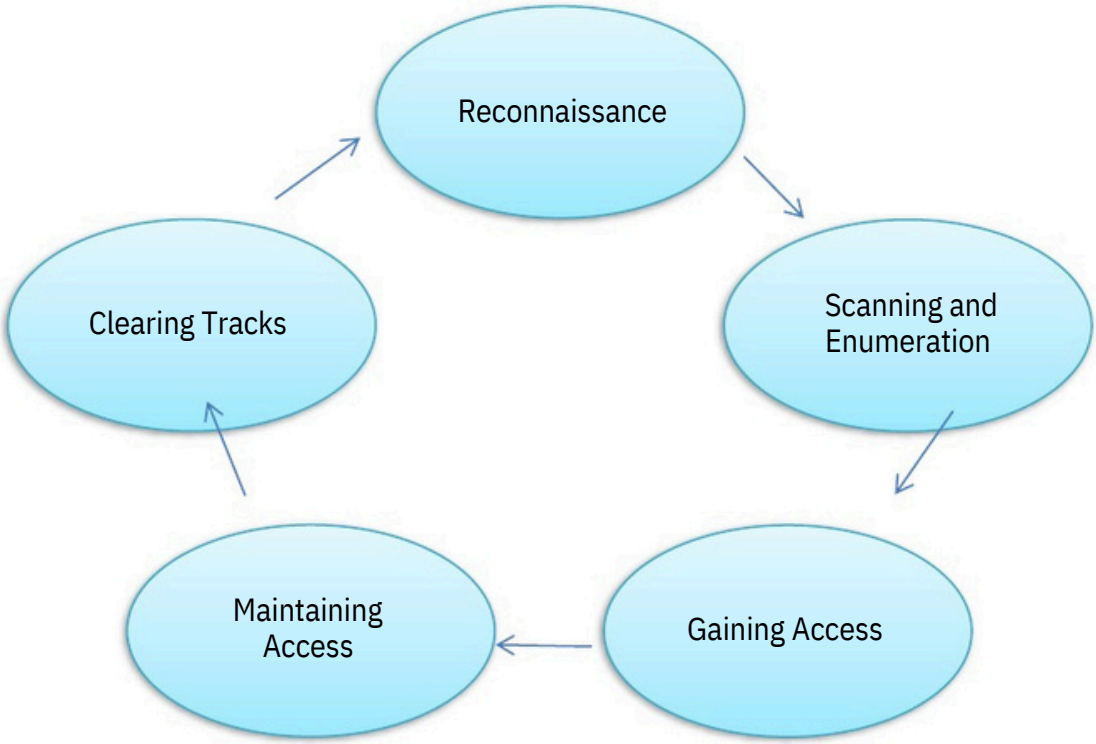

Figure 1 Ethical Hacking Steps

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 [6].

• 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 common technique that pen tester uses to find the open door. 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 the main priority network attack. Enumeration is a producer by actively connecting to it to collect information about the target machine [7].

3. Gaining Access:

Once the observation is finished & every weakness are tested, the hackers then attempts with the helps 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.

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 commend unless the company has the necessary security personnel to take advantage of the defense 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 steps 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.

3. TOOLS USED IN ETHICAL HACKING

1. Tools for Reconnaissance:

Google, Whois Lookup and NSLookup.

2. Tools for Scanning:

Ping, Tracert, Nmap, Zenmap, Nikto WebsiteVulnerability 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 [8].

4. TYPES OF CYBER HACKER

1. White-hat:

A white-hat hacker, also known as the ethical hackers, is celebrity who has non-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.

2. 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 [9].

3. 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, some grey-hat hackers will roam in the Internet; like the white-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.

4. 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 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 color [10].

5. Elite Hacker:

These type 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 [11].

5. CONCLUSION

The security problems will endure as long as constructor 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.