RESEARCH ARTICLE OPEN ACCESS

Ethical Hacking

Azhar Ushmani
Cyber Security
Western Governor University
Salt Lake City, Utah
USA

ABSTRACT
Hacking is common process which results in the breaching of one's privacy and confidential information. The weaknesses of a system or loopholes in a network are identified and private details are accessed. Therefore, hacking is also known as unauthorized intrusion ("What Is Hacking? | Ethical Hacking"). However, hacking was not always perceived as theft and used for productive causes. Such type of hacking that involves good intentions is known as ethical hacking.
Keywords:- Ethical Hacking, Hackers

I. DEFINING ETHICAL HACKING

The term hacking is divided into two types depending on the intention behind hacking process. The two types are white-hat hacking and black-hat hacking. According to CDN, white-hat hacking refers to ethical hacking which is performed with the target's agreement to discover system's vulnerability from a hacker's perspective. Such type of hacking is done to secure the system from black-hat hackers who have malicious intentions of stealing and exploiting personal information. The tools and tricks used to hack the system are the same for both types of hacking processes ("Cdn.ttgtmedia.com"). Therefore, the white-hat and black-hat hackers think alike. The difference between these two categories is the idea or purpose behind hacking any system. If this purpose is to serve greater good like reducing security issues and stabilize organizational systems, the hacker is known as an ethical hacker. On the other hand, hackers with malicious intentions of stealing personal details and hurting privacy are not considered as ethical hackers.

Ethical hacking is legal since it is performed after acquiring the target's consent. According to CDN, the process of ethical hacking confirms the claim of multiple vendors about the security of their products. The significance of ethical hacking is boundless since it comes in handy for protecting crucial systems, networks, and accounts from data thieves by thinking exactly like them. It provides full control to the information owner, detects system flaws, strengthens computer security, prevents system attacks, and respects privacy (Babbar, Jain and Kang). With the advancement of technical systems and rapidly progressing technology-oriented future, there is a dire need of ethical hacking.

II. ETHICAL HACKERS AND THEIR PURPOSE

The people who specialize in ethical hacking process are known as ethical hackers. They are the professionals who hack into a system or network to locate possible faults, pitfalls, and vulnerabilities that may be exploited by black-hat hackers or crackers (Babbar, Jain and Kang). The skills and mindset of ethical hackers are equal to hackers with malicious intentions but they can be trusted. Ethical hackers are certified and authorized for performing hacking on target systems ("Certified Ethical Hacker - CEH Certification | EC-Council"). An ethical hacker has legal permission to access target's personal details and modify target system. The talents possessed by an ethical hacker can be used to limit cyber crime.

Along with the white-hat and black-hat hackers, another category of hackers was also discovered who work in close affiliation with ethical hackers yet face some social consequences. These hackers are known as gray-hat hackers who hack technical and network systems for good causes like helping organizations to fix security issues, but are unauthorized (Radziwill et al.). Gray-hat hackers implement ethical hacking but their unauthorized approach leads to lack of social acceptance. Ethical hackers are hired by agencies,

companies, and organizations to keep their security in check.

III. HACKING PHASE

Hacking is not a single-phase process. Five phases are carried out in order to complete the process of hacking ("Phases Of Hacking | Ethical Hacking");

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

It is not necessary for a hacker to follow these phases in a sequential order. However, implementation of these phases in the same order can result in accurate hacking. In the first phase, maximum information about network, hosts, and people involved is collected to perform footprinting or reconnaissance ("Phases Of Hacking | Ethical Hacking"). This can be done either by directly approaching the target and gaining knowledge or by using indirect methods such as websites, social sites, etc without approaching the target directly ("Phases Of Hacking | Ethical Hacking"). Data collection provides a deep insight to the system under observation.

The second phase involves thorough scanning of the target. Three processes are involved in scanning phase; port scanning, vulnerability scanning, and network mapping ("Phases Of Hacking | Ethical Hacking"). Technical tools are implemented to further process the target, for instance, vulnerability scanner is installed on the target network to determine safety threats ("Summarizing The Five Phases Of Penetration Testing - Cybrary"). In the third phase, the hacker finally gains access to the target system or network by using various techniques and tools. When the system is accessed, the hacker is required to reach administrator level to modify or install the data according to the requirement ("Phases Of Hacking | Ethical Hacking"). Modification in network or system data takes place after installing a dedicated application that allows the hacker to change network settings.

The process of maintaining access is quite important as once target access is lost, the process of gaining it will be repeated all over again. Certain access maintaining files are used for this purpose if the task of a hacker is not yet completed ("Phases Of Hacking | Ethical Hacking"). Otherwise, if the hacker has made necessary changes in the system, the access does not need to be maintained. The last phase of hacking involves track clearing to erase all traces and evidence that the system was hacked. All the folders created, applications installed, and the registry values that were modified are deleted in this step ("Phases Of Hacking | Ethical Hacking"). The changes are made unrecognizable so that the hacking process is not detectable.

IV. PROCESS, TOOLS, AND TECHNOLOGY

Since every process requires a few dedicated tools and techniques to accomplish the task, the process of hacking also requires the right tools. According to CDN, it is important to realize personal and technical limitations when it comes to utilization of ethical hacking tools. Since every equipment contains minor inaccuracies, it is not necessary that using the right tools will detect every possible vulnerability in the system. However, if more tools are used in hacking process, the chance of more inaccuracy in the results is decreased. The main skills and processes that a hacker should be aware of contain HTTP, HTTPS, and other network protocols, authentication methods, network and firewall architectures, port details, web applications, web servers configurations, database setups, and programming languages like HTML, Ruby, Python, JavaScript (Babbar, Jain and Kang). These skills and knowledge set allow a hacker to understand most of the targeted networks and systems without any complications. These are the basic abilities acquired by hacker to understand their targets and have a complete sense of professionalism while implementing hacking process.

The knowledge of systems and networks is not enough to accomplish hacking process. Specific tools and software applications are dedicated to carry out ethical hacking with accuracy (Babbar, Jain and Kang). They simplify hacking process and are convenient to use for the hackers who are at a beginning stage. Some of these tools are Vulnerability Scanners, Packet Sniffers, Password Crackers, Hacking Hardware, Application and Port Scanners. CDN enlists other commercial and open-source ethical hacking tools such as Nmap, Ether Peek

WebInspect, Ethereal, Kismet, Nikto, QualysGuard, SuperScan, ToneLoc, LC4, LANguard Scanner for Network Security, Internet Scanner, Nessus, etc. These tools and equipment are available commercially for professional ethical hackers and come along with a guide for further convenience.

V. IMPACT ON BUSINESS

Ethical Hacking provides an easy method to locate insecurities of any system and vulnerabilities of a network. There are good and productive intentions behind ethical hacking that can protect any business, product, or a person from those who intend to do any harm. Throughout these years many businesses have suffered loss due to the theft of their valuable information. Others have lost the trust of their customers due to poor safety measures. To avoid these consequences, businesses and organizations have started hiring ethical hacker to keep a check on their network security and reduce possible vulnerabilities (Munjal 922-931). Computer security companies, mobile companies, and even network providers have invested in ethical hacking professionals to detect flaws in their system and update it to maximize system security.

Information technology is progressing rapidly in today's world and all the present data is in the form of computer program, bytes, and electronic digits. This data demands safety in order to increase the longevity and usage of electronic systems. A number of sites and electronic markets are encouraging customers to turn to internet instead of offline shopping. So many people provide their personal information such as addresses and bank account details that can be threatened if the services of ethical hackers are not utilized (Munjal 922-931). The trustworthy nature of ethical hackers can provide a safe electronic environment for customers and general public. If a business is able to obtain the trust of their audience, it can prove to be quite fruitful for their business.

Ethical hackers play a vital role in diminishing cyber-crime from the society and promoting a criminal-free environment. However, it is possible that the advantages of ethical hackers are still unknown to people. Some companies were interviewed proving that not every company utilizes the services of ethical hackers and are aware of the advantages (Marsh). There is a need of awareness to allow the business to be more open towards ethical hacking and secure their products. Ethical hackers are competent against cyber thieves and black-hat hackers and by acquiring their services it will be easier to fight against them. These professionals are the only ones who can think and act like malicious hackers so it is important to promote their significance in this society.

VI. CONCLUSION

Hackers detect flaws and vulnerabilities in a system or network and modify it according to their requirements. There are two categories of hackers known as the white-hat and the black-hat who are only differentiated by their intentions towards hacking. Ethical hackers of white-hat hackers are not accepted well by the society and are perceived as general hackers who have malicious intentions. There is a need of creating awareness about ethical hackers to avoid security breaching of products. Ethical hackers are trustworthy and have positive and productive motives. They are certified professionals who are appointed by organizations to keep their security in check which is why they are important for the society and businesses. Every hacker utilizes certain tools, skills, and gadgets to carry out the hacking process. Therefore, the mindset and thinking capabilities of every hacker is the same. Five phases of hacking are required to complete target hacking successfully. If today's society and businesses started taking the services of trustworthy hackers, security threats will be greatly reduced.

REFERENCE

[1] *Cdn.ttgtmedia.com*. Web. 14 Dec. 2018.

[2] Babbar, Sahil, Rachit Jain, and Jinkeon Kang. "Ethical Hacking." *Research Gate*. N.p., 2015. Web. 14 Dec. 2018.

[3] "Certified Ethical Hacker - CEH Certification | EC-Council." *EC-Council*. N.p., 2018. Web. 14 Dec. 2018.

[4] Marsh, Devin. "Are Ethical Hackers The Best Solution For Combating The Growing World Of Cyber-Crime?." *Jewlscholar.mtsu.edu*. N.p., 2017. Web. 15 Dec. 2018.

[5] Munjal, Meenaakshi N. "ETHICAL HACKING: AN IMPACT ON SOCIETY." 7.1 (2013): 922-931. Web. 14 Dec. 2018.
[6] "Phases Of Hacking | Ethical Hacking." *Greycampus.com*. Web. 14 Dec. 2018.
[7] Radziwill, Nicole et al. "The Ethics Of Hacking: Should It Be Taught?." *Arxiv.org*. N.p., 2005. Web. 14 Dec. 2018.
[8] "Summarizing The Five Phases Of Penetration Testing - Cybrary." *Cybrary*. N.p., 2015. Web. 14 Dec. 2018.
[9] "What Is Hacking? | Ethical Hacking." *Greycampus.com*. N.p., 2018. Web. 14 Dec. 2018.