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: 7.53

Volume 4, Issue 1, January 2024

Ethical Hacking – A Review

Kunal Dilipkumar Rathod[1] and Atharva Rupesh Yerawar[2]

Final Year B.E, Department of CSE[1,2]

Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India

Abstract: *Nowadays all the information is available online and a large number of users are accessing it, some of them use this information for gaining knowledge and some use it to know how to use this information to destroy or steal the data of websites or databases without the knowledge of the owner. So ensuring data security over the internet is very important and should be taken care of at utmost priority. As with most technological advances, there is also a dark side attached to it, i.e. hacking. This paper describes what is ethical hacking, types of hackers, Tools` used in ethical hacking and impact of hacking.*

Keywords: Hacking, Hackers, Ethical Hacking, Security.

I. INTRODUCTION

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills [6]. The state of security on the internet is very poor. Hacking is an activity in which, a person exploits the weakness in a system for self-profit or gratification. As public and private organizations migrate more of their critical functions or applications such as electronic commerce, marketing and database access to the Internet, then criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. Ethical hacking is an identical activity which aims to find and rectify the weakness and vulnerabilities in a system. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions [7].

II. HACKING AND ETHICAL HACKING

2.1 Hacking

Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc [1]. Hacking is a malicious activity in which a person who is known as Hacker, exploits the weaknesses and vulnerabilities in a system for self-profit or gratification. It is basically referred to gaining unwanted access to a computer to obtain sensitive information stored in it by means of password cracker software or any other techniques to get the confidential data. This is done to either point out the loopholes in the security or to intentionally sabotage the computer. This is generally considered as a kind of malicious activity. Malicious hacking is basically the unauthorized access and use of computers and associated network resources. Malicious software programs such as Trojans, malware and spyware are utilized to gain entry into an organization’s network for stealing vital information. It may result in identifying theft, loss of confidential data, loss of productivity, use of network resources such as bandwidth abuser and mail flooding, unauthorized transactions using credit or debit card numbers, selling of user’s personal details such as phone numbers, addresses, account numbers etc. However, when the hacker has clear intentions to break into a computer system to save the organization from intrusion attacks, the process is termed as Ethical Hacking [5].

2.2 Ethical Hacking

Ethical Hacking can be defined as a legal access of an Internet geek or group in any organization’s online property after their official permission [2]. It is the process which generally focuses on securing and protecting the Organization’s

DOI: 10.48175/568

confidential data as well as its computer systems and its allied devices. Independent computer security professionals break into the computer system neither to damage the target system nor to steal the information. Instead, they evaluate the target system security and report back to the owner about the threats and vulnerabilities found and the associated instructions for their remedy. Ethical Hacking is performed with the target's permission with the intention of ethically discovering the vulnerabilities from a hacker's viewpoint so that systems can be better secured. It is a part of an overall information risk management program that allows for ongoing security enhancements. Ethical Hacking can also ensure that vendors' claims about the security and authenticity of their products are legitimate. Ethical Hacking is a way of performing security assessment. An ethical hacker shows the risks faced by an information technology environment as well as the actions which can be taken to reduce certain risks or to accept them. Hence we can say that Ethical Hacking perfectly follows the security life cycle shown as below figure3. It is a way to do the security assessment which can be checked from the technical point of view. There are mainly four different types of ethical hacking depending on the knowledge and the duty of the hacker. As we already know, there are a number of hackers whose intentions for hacking a system are not to harm the organization rather they take preventive measures to maintain the security and safety of the system and to check the vulnerabilities in the current system so that the security holes can be filled and the system can be secured [5].

III. TYPES OF HACKERS

Getting access to server without the knowledge of the user. The server may be internet systems, personal computer, accessing main hub, etc, the person who is doing such an activity is termed as hacker. There are different types of Hackers around the world [4]. The term HACKER in popular media is used to describe someone who breaks in to someone else's security using bugs and exploits or use his expert knowledge to act productively or maliciously. Hackers are the computer experts in both hardware as well as software. A hacker is a computer enthusiast and master in a programming language, security, and networks. He is kind of person who loves to learn various technologies, details of the computer system and enhances his capability and skills. According to the way of working or based on their intensions HACKERS can be classified into three groups,

3.1 White Hat Hackers

A white hat hacker is a computer security specialist that breaks into and find loopholes in the protected networks or the computer systems of some organization or company and corrects them to improve the security. White Hat Hackers use their skills and knowledge to protect the organization before malicious or bad hackers find it and make any harm to the company or the organization. White Hat Hackers are the authorized persons in the industry, although the methods used by them are similar to those of bad hackers but they have permission from the organization or the company who hires them to do so [1]. White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who cannot be trusted [2]. White hat hackers are also known as sneakers. They can also be termed as Ethical Hackers.

3.2 Black Hat Hackers

A Black hat hacker is a person who is exploiting the computer system or computer network without the consent or permission from any authorized party. His main goal is to do any kind of mishap and harm to the system. They do such things for their own personal interests like money. They are also known as crackers and malicious hackers [5]. Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be [2]. These are the computer hardware and software expert who breaks into the security of someone with malicious intent or bad intentions of stealing or damaging their important or secret information, compromising the security of big organizations, shutting down or altering functions of websites and networks. They violate the computer security for their personal gain. These are persons who typically wants proves their extensive knowledge in the computers and commits various cybercrimes like identity stealing, credit card fraud etc.

3.3 Grey Hat Hackers

A Grey Hat Hacker is a computer hacker or security expert who sometimes violates the laws but does not have any malicious intentions like the black hat hackers. The term Grey Hat is derived from the Black Hat and the White Hat as the white hat hackers finds the vulnerabilities in the computer system or the networks and does not tells anybody until it is being fixed, while on the other hand the black hat hackers illegally exploits the computer system or network to find vulnerabilities and tells others how to do so whereas the grey hat hacker neither illegally exploits it nor tells anybody how to do so. Grey Hat Hackers represents between the white hat hackers who operate to maintain system security and the black hat hackers who operate maliciously to exploits computer systems [1]. Grey hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Grey-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Grey hats are self-proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly [2]. These hackers are skilled enough to work as a good or bad in both ways. They are the one who have ethics. A grey hat hacker gathers information and enters into a computer's system to breach the security, for the purpose of notifying the administrator that there are loopholes in the security and the system can be hacked. Then they themselves can offer remedies and solutions. They are well aware of what is ethical and what is unethical but sometimes they act in a negative direction. A grey hat hacker may breach the organization’s computer security, and may exploit it and deface it. They in fact inform the administrator about the organization’s security loopholes. They hack or gain unauthorized access to the network just for fun and not with the intention to harm the organization’s network.

IV. TOOLS USED IN ETHICAL HACKING

Ethical hacking is learning the conception of hacking & applying them to secure any systems, organization for any great cause. Ethical hacking procedure has basically five different stages. Any ethical hacker has to follow these steps one by one to successfully reach its goal. The figure below demonstrates the five different stages of ethical hacking which are being followed by an ethical hacker while hacking a computer system or computer network [5].

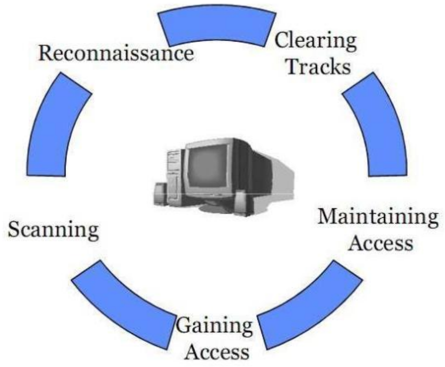

Fig. Methodology of Ethical Hacking

Now let’s see the tools used in Ethical Hacking in various stages.

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 [8].

V. IMPACT OF HACKING

Some of the most expensive and prolific victims of hacking have been businesses. Businesses are many times targeted for their customers' personal and financial data and often are targeted by their own employees, whether disgruntled or just opportunistic. Businesses lose billions of dollars yearly as a result of hacking and other computer breaches. Many times, the true cost cannot be evaluated because the effects of a security breach can linger for years after the actual attack. Companies can lose consumer confidence and in many cases are held legally responsible for any loss to their customers. The cost of recovering from an attack can spread quickly: legal fees, investigative fees, stock performance, reputation management, customer support, etc [7]. Companies, and more recently, consumers, are investing more and more money into preventing an attack before it actually happens. Businesses that hold stores of consumer's personal and financial data are especially taking extra steps to insure the data's safety.

5.1 Benefits of Ethical Hacking

Ethical hacking can provide convincing evidence of real system or network level threat exposures through proof of access. Even though these findings may be somewhat negative, by identifying any exposure you can be proactive in improving the overall security of your systems.

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

5.2 Limitations of Ethical Hacking

As every coin has two sides, everything which has benefits also has some limitations [5]. The possible drawbacks of ethical hacking include:

- It may corrupt the files of an organization.
- Ethical hackers might use information gained for malicious use. Hence trustful hackers are needed to have success in this system.
- Hiring such professionals will increase cost to the company.
- The technique can harm someone's privacy.
- Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities

VI. 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 [8].

REFERENCES

[1] Ethical Hacking and Hacking Attacks by Aman Gupta, Abhineet Anand in International Journal Of Engineering And Computer Science, ISSN:2319-7242, Volume 6 Issue 4 April 2017, Page No. 21042-21050 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.42

[2] Ethical Hacking by Vinitha K. P in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Special Issue - 2016

[3] IS ETHICAL HACKING ETHICAL? by DANISH JAMIL, MUHAMMAD NUMAN ALI KHAN in International Journal of Engineering Science and Technology (IJEST)

[4] Ethical hacking and penetration testing for securing us form Hackers by Pradeep I and Sakthivel G in International Conference on Robotics and Artificial Intelligence (RoAI) 2020, Journal of Physics: Conference Series 1831 (2021) 012004, IOP Publishing, doi:10.1088/1742-6596/1831/1/012004

[5] Ethical Hacking:The Story of a White Hat Hacker by Shivanshi Sinha. Dr. Yojna Arora in International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume-8, Issue-3, May 2020, https://doi.org/10.21276/ijircst.2020.8.3.17, www.ijircst.org

[6] Ethical Hacking Techniques with Penetration Testing by K.BalaChowdappa , S.Subba Lakshmi , P.N.V.S.Pavan Kumar in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393

[7] Study Of Ethical Hacking by Bhawana Sahare, Ankit Naik, Shashikala Khandey in International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014

[8] A REVIEW PAPER ON ETHICAL HACKING byPrabhat Kumar Sahu, Biswamohan Acharya in International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 12, December 2020, pp. 163-168, Article ID: IJARET_11_12_018, ISSN Print: 0976-6480 and ISSN Online: 0976-6499, DOI: 10.34218/IJARET.11.12.2020.018