IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 1, January 2020

Ethical Hacking: Impacts on Society

Sankardas P D[1], Mohammed Raeez[2], Bibitha Baby[3]

Student, Bachelor of Computer Applications, SNGIST Arts and Science College Manakkapady, N.Paravur, India[1,2]

Assistant Professor, Department of Computer Applications,

SNGIST Arts and Science College Manakkapady, N.Paravur, India[3]

Abstract: During the growth of the Internet, computer network security has become a major concern for businesses and government authorities. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked." At the same time, the regular customers of these services were afraid about maintaining control of personal information that includes credit card numbers to social security numbers and other personal details. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "white hackers" or "ethical hackers" would employ the same tools and techniques that the intruders also implement, but these ethical hackers would never damage the target systems nor steal information. Instead, they would evaluate the target systems security and report back to the concerned authorities with the information they found and instructions for how to free themselves from the hacked situation.

Keywords: Ethical hacking, white hackers, Methodology, Impacts

I. INTRODUCTION

Ethical hacking involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is not illegal. It is the way through which an ethical hacker will discover some vulnerability from the hacker's point of view so that the system can be made more secure and safe.Ethical hacking, as the name indicates a hacking which is ethical. It is also called penetration testing. This is the technique which is being used by a lot of professionals to do hacking but that is not illegal it is preferably ethical. That is the reason it is to be called ethical hacking. Though all the tools, tricks and techniques are used in this regard are the same as being used in hacking, but it is done with the consent of the target, that's why is not hacking it is ethical hacking[1]. It is the way through which an ethical hacker will discover some vulnerability from the hacker's point of view so that the system can be made more secure and safe. Ethical hacking also makes sure that the claim made by target should be genuine. It's part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

II. WHAT IS ETHICAL HACKING ?

According to the ethical hackers they know every detail about the company and they can destroy the system. The major skill of the ethical hacker is trustworthiness and the other is patience. The information found by the hacker can't be abused. The ethical hacker should be more trustworthy for the maintenance of the safety and security of the system. Gaining access to somebody's computer system or network without their permission is crime and that is not ethical.

III. HACKERS

Hackers are the people who have a great Knowledge on operating systems and network technologies. The hackers who are hacking a system illegally are known as black-hat hackers. But ethical hackers hack the system in an ethical way. An ethical hacker should see sensitive information and needs to be extremely trustworthy. Lots of companies don't believe in hiring hackers. The black-hat hackers hack the systems for their own gains mean while the ethical hackers hack the systems to find the vulnerabilities in the system and improve the security of the system.

IV. TYPES OF ETHICAL HACKING

There are mainly four different types of ethical hackers .They are Cyberwarrior, White box penetration testers, certified ethical hacker / licensed penetration tester.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 1, January 2020

A. Hacktivists: In this segment a hacker is hacking into s system illegally for any reason that may be social or political. This may lead to the hacking of a system without the consent of the target. It may have many social messages like ethical hacking is ethical or not which may attract a number of users and they can participate in the discussion.

B. Cyberwarrior: It is a kind of hacker who is being hired by an organisation or by an individual to creep into the system or computer network. Cyber Warrior will act as a wicked hacker. They do not have prior knowledge of systems or computer networks.

C. White Box Penetration Testers: White Box Penetration Testers are also called as white box hackers. They are hired by the organisations to break into their current system or computer network. They are working the same as the cyber warriors. The only difference is the cyber warriors do not have knowledge of the system or computer network whereas white box hackers are having full knowledge of the system or computer network of the target.

V. CERTIFIED ETHICAL HACKER

Certified Ethical Hackers are the licensed professionals in the field of hacking. They are performing both the duties of black box hackers and white box hackers. These certifications or licenses are given by the International Council of E-Commerce.

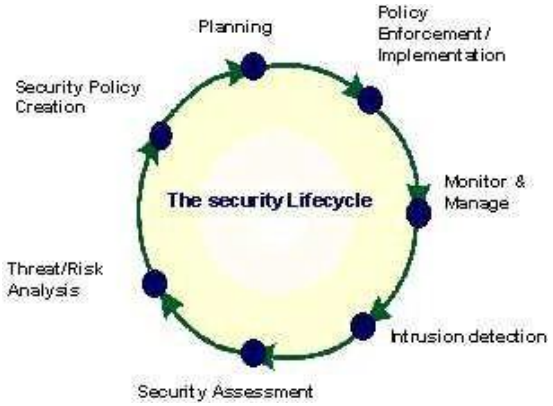

Figure 1.Security Life Cycle[2]

VI. ETHICAL HACKING METHODOLOGY

Ethical hacking procedure has basically five different stages:-

- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Clearing tasks

A. Reconnaissance: In this stage the hacker is supposed to collect all the information of the company whose data is to be hacked and it is called footprinting. The hacker ensures all the information to be collected and it is the pre attacking phase in hacking. Tools like network mapping and network vulnerability scanning are used.

B. Scanning: In this technique a penetration tester can easily find out the open doors for any network. Hacker makes an outline of the target network in this stage. Outlines include the IP addresses of the end or target network, other services which are running on those systems and so on. There are three types of scanning; Port scanning, Network scanning, Vulnerability scanning

C. Gaining Access: This is the most important phase where attackers will get access to the system or network and have the ability to spoil the system completely. Gaining access also known as owning the system in the hacker world which means now the attacker or hacker will have full access to the target system. Here a hacker uses a special type of software called “zombie” which can be distributed and can lead to damage to many machines.

D. Maintaining Access: After gaining access by a hacker it would be very easy for him to use the system itself and all its resources and exploit them. Hackers can be able to make this system as a launchpad and can scan other systems and damage them. By this an entire organisation can be exploited. They use backdoor or Trojan to get the access to the system.

E. Clearing Tasks: This is the last and final stage where the hacker removes or destroys all evidence of their presence and activities for various reasons such as maintaining access.

VII. IMPACTS OF ETHICAL HACKING IN SOCIETY

Hackers have a great impact on society. They are focusing on the youth. Ethical hacking is not a bad thing but we should know what the ethical hackers are doing in society .There are many areas in information technology where the ethical hackers made a great impact. Today the entire world is in the hands of information technology and we can't even think about a life without the internet. Now a day's internet has become the connecting link for a mobile device to the world. This made the hackers attack the world.

A. Impact on Education

Teaching hacking students is a hard process. Students are always interested in learning new technologies. Whenever a teacher is teaching the students about the hacking he/she can ensure that how the student will take the concept, it is possible that the student may intend to hack other devices or do bad things with this. In the class, the 95% students may take lessons in a good manner but the remaining 5% may have bad intentions. "A very big problem with undergraduate students to teach this approach is that a teacher is effectively providing a loaded gun to them "[3]. The major problem is that the students really don't know the importance and impacts of hacking, but they will try to do hacking it can be for a good or bad purpose. Nowadays the number of the students who are intended for the security courses are increasing. They want to learn hacking easily and earn its benefits. They are attracted to new hacking technologies where they can hack computers and other devices. We have to make them understand that ethical hacking is bad if it does not contain any ethics. We can conduct workshops, seminars and awareness programs to lead them to a good way.

B. Impact on Business

Nowadays we use a lot of IT applications in business. We live in a digital world and thus all of the data is digitized. As a result the whole transactions are done today electronically. The growth and availability of the internet made people do digital transactions. As a result the rate of the customers who are using the e-commerce sites has increased. To an ethical hacker it is very easy to buy products from these sites. In one way he may hack the site and buy the products or he can hack a person's account and use it for the payments. Also there are some good and ethical programmers doing their job neatly. But they can use their talent for bad intentions. They can attack business persons or companies systems, tap the phone calls, create virus codes, etc. We can't predict the intentions of an ethical hacker. As technology increases, ethical hackers will increase. We can't stop them but we can advise them to work for good intentions.

C. Impact on Workplace and its Security

Today most of the companies store their data in the digital form. So the ethical hacker can hack the data and can use it for his own purpose. The hacker can access the information of the staff of the company. Sometimes the hacker may attack the company's servers and access the server data. For this purpose they use virus code. To prevent the hacking we have to improve the security of the existing system; it can be achieved by finding the information used by the hackers to hack the system and correct those weak points to increase the security. The hacker may attack the company's server data to gain a large amount. But now the companies have several mechanisms to prevent ethical hackers.

D. Impact on Technology

In this modern world almost nothing is secure. Almost all information is available at our finger point. Anybody can easily get the information related to any system. So ethical hackers can easily get the IP addresses of any system and may attack it. There are several tools for ethical hackers to do their work easily. The most used tool is the Nmap, it helps an ethical hacker to find open ports of the different systems. Another one is Acunetix, it is used to find vulnerabilities. These two tools are being used by an ethical hacker without any prejudice. Hackers may use them for crimes where the ethical hackers will use them to find the weaknesses and imperfections in the network security.

E. Impact on Confidential Information

Today confidential information in society is not at all safe in the existence of hackers. So many ethical hackers are working in several institutions where financial transactions take place. There for the hacker can access the important data about the account holders. He can use the data to make transactions for his own purpose or steal the money of account holders. The hackers mainly hack our accounts using fake emails and advertisements. There is a great problem for an ethical hacker to track all the outlines. The hacking is different from ethical hacking. But sometimes because of all access with ethical hackers, they may also come into this circle. And sometimes for an ethical hacker it is very difficult to prove that he is not the illegal hacker. For example, if an ethical hacker is hired to check the vulnerabilities in a system of confidential information and a few days later some data is leaked from that system then everybody will blame the ethical hacker and will make him a black–hat hacker.

VIII. CONCLUSION

Hacking can be legal or illegal, but both of these have their own benefits and risks. The fight between white-hat hackers and black-hat hackers never going to end, it will continue as the technologies in the world increases. If we consider hacking as a coin then the ethical hackers and the malicious hackers are two sides of the coin. Hacking may become good or bad, it will depend on the nature of the hacker. The black-hat hacker hacks our system for his personal gains mean while the white-hat hacker helps us to keep our system secure. We can't stop hacking, as the new technologies come out, the hackers will try to find a new way to hack it down. So be alert always on your data.

ACKNOWLEDGMENT

We got a lot of help from our friends and teachers to choose and complete this topic; we sincerely thank all, who helped us to do this research. The research was our college SNGIST ARTS and Science College, Manakkapady, N.Paravur. We also thank our guide **Ms.Bibitha Baby** and our Head of Department **Mr.Praveen Kumar** sir for their guidance to complete this journal. We are kindly requesting that if any errors are found in this journal, it is all own and should not stain the reputations of these esteemed persons.

REFERENCES

[1]. Meenaak hi N.Munjal, "Ethical Hacking: an Impact on Society", https://www.researchgate.net/publication/262726769_Ethical_Hacking_An_Impact_On_Society
[2]. Tom Wulf, 2003, "Teaching Ethics in Undergraduate Network", Consortium for Computing Science in College, Vol 19 Issue 1, 2-3.