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

Ethical Hacking: The Story of a White Hat Hacker

Shivanshi Sinha. Dr. Yojna Arora

ABSTRACT- Massive growth of the Internet has brought in many good things such as e-commerce, easy access to extensive sources of learning material, collaborative computing, e-mail, and new avenues for enlightenment and information distribution to name a few. Today, since almost all the work is done over the internet, crucial data is sent over the web and other information is placed over the internet. 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. Hacking is an activity in which a person (namely hackers) exploits the weaknesses and vulnerabilities in a system for self profit or gratification. With the growing movement of the world from offline to online culture like shopping, banking, sharing information access to sensitive information through the web applications has increased. Thus the need of protecting the systems from hacking arises to promote the persons who will punch back the illegal attacks on the computer systems and will ensure data security. As every coin has two faces, this coin also has one another face which generally acts as a life saver for the victims of hacking. This lifeguard technique is called ethical hacking.

Ethical hacking is a technique which is used to identify the weaknesses and vulnerabilities in the system or computer network in order to strengthen the system further to prevent the data. The main reason behind studying ethical hacking is to evaluate target system security. This paper helps to generate a brief idea of ethical hacking and all aspects.

KEYWORDS- Hacking, Hacker, Hacking, Ethical Hacking, Red Hat Hacker

Manuscript received April 24, 2020

Shivanshi Sinha, Student, Department of Computer Science and Engineering, Amity University, Gurugram, Haryana, India, 9911193360, (email:schaudhary@ggna.amity.edu)

Dr. Yojna Arora, Assistant Professor, Department of Computer Science and Engineering, Amity University, Gurugram, Haryana, India,

I. INTRODUCTION

Data security is the major area of concern in today's era where internet use is very vast and also expanding rapidly. Every organization is concerned related to security about their sensitive and confidential data. This is only because of hacking .Hacking is committed by a person who has wrong intentions. Just as every coin possesses two sides, basically there are two types of hackers, one who has rights of securing data while using hacking techniques and the other who uses his knowledge to break the security layer to harm the organization. These hackers are categorized into two categories: Ethical hackers and malicious hackers [3][4][5][6]. Hacking is a process of anonymously controlling the system of an organization without the knowledge of the organization members. In contrast it is called breaking the security layer to steal the sensitive and confidential information such as credit card numbers, telephone numbers, home addresses, bank account numbers etc. that are available on their network. This describes that security is a discipline which protects the confidentiality, integrity and availability of resources. It refers to this era as a "Security era" not because we are very much concerned about security but due to the maximum need of security. Ethical hacking is the only solution for this. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover the vulnerabilities and loop-holes in the security and firewall of a computer system from the viewpoint of the hacker so that systems can be better secured. This is a part of an overall information risk management program that allows for ongoing and extended security improvements. Ethical hacking can also ensure that vendors claiming about the security and authenticity of their products are legitimate [7][8][9][11].

A. Survey On Ic3 Report

I have discovered a report from a government website which is about "Internet Crime Current Report". The Internet Crime complaint center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NWC3).According to the current 2019 report by IC3 and as depicted in the graph above (figure1), till 2019 the number of complaints of hacking has increased at an exponential rate. Moreover, it has affected mostly the people who are generally of age over 60 years. The above graph depicts the total counts of

victims of hacking. As we can see, a large number of people of every age group are rapidly and increasingly becoming the victims of hacking. This shows how essential and vulnerable the data security is in this era of the cyber world. [2]

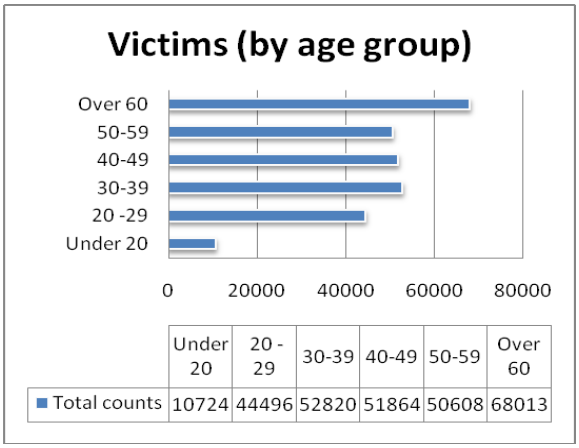

Fig 1: Total victims of Hacking

II. HACKING

During 1971, John Draper (also known as Captain Crunch) one of the best known early phone hackers and one of the few personalities who is known as the father of hacking." Hacking is a malicious activity in which a person (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.[3][8][11][12]

Fig 2: Concept of Hacking

III. ETHICAL HACKING

Ethical Hacking is the process which generally focuses on securing and protecting the Organization's 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 [5][6][7][8]. 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 [9][12][14].

A. Ethical Hacking Methodology

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 [3][7][10][15].

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

Fig. 3: Methodology of Ethical Hacking

B. Reconnaissance

Reconnaissance is the first stage of attack by the ethical hacker in which the hacker is supposed to collect all the information of the target company whose data need to be hacked. This procedure is also known as footprinting. The literal meaning of reconnaissance means preliminary survey to gain the information. In this stage the hacker must ensure that all the required information has been collected. This stage can also be termed as a pre-attacking phase in hacking. Reconnaissance can be active or passive. In passive reconnaissance, the information is gathered regarding the target without knowledge of the targeted company (or individual). It can be done by identifying the source which can reveal and provide all the useful information to the hacker. This process is also called "information gathering". In this approach, a hacker does not attack the system or network of the company to gather information. On the other hand, in active reconnaissance, the hacker enters into the network to find various details about hosts, IP addresses and network services. This process is also called "rattling the doorknobs". In this method, there is a high risk of being caught as compared to passive reconnaissance.

During this phase different types of tools like network mapping (like Cheops to generate network graphs for internal ethical hacking) and network vulnerability scanning can be used.

C.Scanning

In scanning technique, a penetration tester can easily figure out the security holes for any network. The hacker tries to make an outline of the target network. The outline includes the IP addresses of the end or target network which are live, other services which are running on those systems and so on.

In the scanning phase, the information gathered in the reconnaissance phase is used to examine the network. Tools like Dialers, Port Scanners etc. are used by the hacker to examine the network and get into the target system. There are three types of scanning:

D. Port Scanning

i. With the help of modern port scanning which uses TCP protocol an ethical hacker can get to know which operating system is running on the particular hosts. In the technological term port scanning is mainly used to find out the vulnerabilities and weak points in the used port in the network. For port scanning, there are many network mapper tools available on the internet like netscantools, superscan, unicornscan, scanrand, portscan 2000 and many more.

E. Network Scanner

In the network scanning, the ethical hacker can identify all the active hosts which are present on a network. The purpose of network scanning is either to attack the identified active hosts or to access the network security. The hacker can easily get to know about the IP addresses of individual hosts. All the network scanning tools can be used to know about the active hosts and their corresponding IP addresses on the network.

ii. F. Vulnerability scanning

iii. In the vulnerability scanning the hacker can get to know about the operating system of the target system and other related details about the operating system such as its version, service, pack if it is installed. The vulnerability scanner will identify the weaknesses of the operating system which can be later attacked. Vulnerability scanning generally refers to the scanning of the system that is connected to the internet.

G. Gaining Access

This is the most important phase in which the attacker will get the access of the system or network and get the ability to damage the system completely. This is the stage in which the real hacking takes place. During this phase, those weak points and vulnerabilities which are exposed during the reconnaissance and scanning phase are further exploited to gain access in the target system. The method of connection which is used by an attacker or hacker to damage the system can be local area network, local access to computer and internet. Some of the examples of access gaining techniques are stack based buffer overflows, session hijacking and denial of service etc. This phase of gaining access to the system is also known as the phase of owning the system in which the attacker or hacker have full access to the target system. One of the most harmful types of denial-of-service attacks, where a hacker uses a special type of software called "zombie" and he distributes it on a number of systems on the internet in such an organized manner so that maximum number of systems over the network can be damaged.

H. Zombie System

After gaining access over the target system by a hacker it would be very convenient for a hacker to use the system and all its resources and exploit them. In such a situation, the owned system is then referred to as the "Zombie System". There are so many attackers or hackers who believe to be undetected and maintain their access on the owned system. The attackers can use the backdoor or Trojan to get the repeated access in the target system. With the help of Trojan horse, hackers are able to have the usernames, passwords

and other confidential information of the target which helps them in maintaining long term access on the target system. Thus, this phase is also known as the "phase of maintaining access".

I. Clearing Tasks

This is the last and final stage where a hacker wants to remove or destroy all evidence of his/her presence. This is one of the best methods to evade track back. It is really very crucial to invaders to make the system look the same as it did before they gained access and established backdoors for their use. In this phase, the hacker removes and destroys all the evidence and traces of hacking, such as log files or intrusion detection system alarms so that he could not be caught and traced. It is really very crucial for invaders to make the system look like it was before they gained access and established backdoors for their use. Any files, which have been modified or altered, need to be changed back to their original attributes or format. Thus, this phase is also known as evidence removal phase.

Following are some activities which are present during this phase:

- Steganography
- Using a tunneling protocol
- Altering log files

RULES OF ETHICAL HACKING

- The hacker must obey all the ethical hacking rules. If they don't follow the rules then it would be dangerous for the organization.
- For an ethical hacker, time utilizing skills and patience are very important so these qualities should be there.
- Ethical hackers must have clear intentions to help the organization and not to harm the organization.
- Privacy is the major concern from the organization's point of view, thus the ethical hacker must keep all the gained information as private because their misuse can be dangerous or illegal.

VI. ETHICAL HACKERS

Generally, the term Hackers is used for the programming as well as cyber security experts who intentionally break into a computer system or over a network with a malicious intent in order to damage the system of the target organization and to steal the vital and confidential data of that organization. Some do it for fun, some do it for profit, or some simply do it to disrupt the operations and gain some recognition. They try to uncover the weaknesses and vulnerabilities in a system in order to exploit it. The vast growth of the internet has brought many good things like e-commerce, email, easy access to vast information and much more, but at the same time it has brought up thousands of opportunities for the criminal hackers. So, to overcome these major issues like hacking , another category of hackers came into existence and these hackers are generally termed as ethical hackers or white hat hackers[5][7][8][9][11].

An Ethical hacker's knowledge is very much comparable to the malicious hackers. An ethical hacker is the one who rectifies the weaknesses and vulnerabilities of an organization's system and report to the owner about the threats found and the remedies to overcome those threats and fill the holes and gaps in a system.The various types of ethical hackers are as follows:

A. Hacktivists

Hacktivists are the people who gain unauthorized access to computer systems and networks in order to further social or political ends. This is a technique through which a hacker is hacking into a computer system illegally for any reason that may be social or political. In this technique a hacker can leave an important message on the main page of any well known website so that the visitor will see the message and react accordingly. The hacker can display any kind of speech or social message which can attract the user and make them participate in some kind of discussions. The target is unaware about he

B. Cyber Warrior

Cyber warrior is hired by an individual or organization to look into the system or network. Cyber warriors generally act as a wicked hacker and will try to identify the vulnerabilities or weaknesses in the present system. This time, the hacker is not having any prior knowledge of the system or computer network in which he is gaining access. By this technique, the hacker can know about the vulnerabilities in the present system or computer network and can report to the organization or the particular individual to work upon the vulnerabilities so that the website or other data can be secured from hacking in future.

C. White Box Penetration Testers

White box penetration testers are the employees that are hired by an organization to break into their current system or computer network. They are called the legal penetration testers. They legally break into the system or computer network for the organization to report them about the vulnerabilities and weaknesses in the current system.White box testers are working in the same way as cyber warriors are working but the only difference is that cyber warriors do not have a prior knowledge of the system or computer network of the organization or of individuals whereas white box hackers have the full knowledge of the system or computer network of the target.

D. Certified Ethical Hacker

Certified Ethical hacker or licensed penetration tester are the certified or licensed professionals in the field of hacking who are performing the duties of both i.e. black box hacker and white box hacker who are performing the duties of both i.e. black box hacker and white box hackers.These certifications or licenses are given by the International Council of E-Commerce Consultants. Ethical hackers are required to recertify themselves after every three years.

E. White Hat Hackers

White Hat Hackers are authorized and paid people by the companies, with good intentions and moral standing. White hat hackers are the hackers who gain access into the system or computer network with the consent of the target

to find out the vulnerabilities and security flaws in the present system. They are also known as "IT Technicians". Their job is to safeguard the internet, businesses, computer networks and systems from crackers. Some companies hire IT professionals to attempt to hack their own serves and computers to test their security system. These types of professionals are majorly hired by computer security companies. White hat hackers are also known as sneakers. In the company when there are more than one sneaker then the group of such professions are called "tiger team". They do hacking for the benefit of the organization. In actual terms, the white hat hackers are called ethical hackers who ethically opposes all the exploitations in the computer system.

F. Blak 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.

G. Grey Hat Hacker

A Grey hat hacker is 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. BENEFITS OF ETHICAL HACKING

The benefits range from simply preventing malicious hacking to preventing national security breaches [5]. The benefits include:

- 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.
- It helps to identify and close the open holes in a computer system or network.

VI. 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.
- The system is illegal..

VII. CONCLUSION

To "Hacker" is a word that carries a lot of weight. Hacking may be defined as legal or illegal, ethical or unethical. The battle of comparison between the ethical or white hat hacker and the malicious hacker or black hat hacker is a long war, which does not seem to have an end. But technology is spreading all over and growing so rapidly and it will continue to do so. With technological development, the awareness about hacking and ethical hacking techniques among the individuals and organizations are also increasing which even makes them aware about the preventable measures for hacking. Hackers will always find some way out to get into the system, irrespective of seeing good or bad intentions. And it will always be the duties of the ethical hackers to try to make the hackers fail in their bad intentions. No ethical hacker will be considered as a hacker. Also the users of this fast growing technology will understand the importance of data security and will understand it as their own responsibility to maintain the same. The paper tries to explain the difference between hacking and ethical hacking. It also includes explanations about various types of hackers, benefits, advantages and disadvantages.

REFERENCES

[1] Ethical Hacking by C.C. Palmer, IBM research division..
[2] Internet Crime Complaint Center link: https://www.ic3.gov/default.aspx
[3] Ethical Hacking by Deepak Kumar, Ankit Agarwal, Abhishek Bhardwaj, International Journal of Engineering And Computer Science ISSN: 2319-7242, Volume 4 Issue 4 April 2015, Page No. 11466-11468
[4] A Comprehensive Study On Ethical Hacking by Suriya Begum, Sujeeth Kumar, Ashhar, International Journal Of Engineering Sciences & Research, Technology, ISSN: 2277-9655 Impact Factor: 4.116
[5] Study of Ethical Hacking by Bhawana Sahare, Ankit Naik, Shashikala Khandey,International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014
[6] Ethical Hacking by Susidharthaka Satapathy, Dr.Rasmi Ranjan Patra, International Journal of

Scientific and Research Publications, Volume 5, Issue 6, June 2015 ISSN 2250-3153

[7] ETHICAL HACKING: AN IMPACT ON SOCIETY by Meenaakshi N. Munjal, Cyber Times International Journal of Technology & Management Vol. 7 Issue 1, October 2013 – March 2014

[8] Case Study on: ETHICAL HACKING, Department of Electronics & Telecommunication Engineering,VIVA Institute of technology, Virar(East), ISSN: 2581-8805

[9] Conference Paper: Ethical Hacking(Tools, Techniques and approach) by Brijesh Kumar Pandey, Lovely lakhmani Balani, Alok Singh,Conference: ICAIM-International Conference on Advancement in IT and Management, January 2015.

[10] Review on Ethical Hacking by Neeru Ahuja, International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization),Vol. 3, Issue 9, September 2015.

[11] Ethical Hacking: Types Of Ethical Hackers by V.Chandrika,International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 11 Issue 1 – November 2014.

[12] Ethical Hacking & Security Against Cyber Crime by NEERAJ RATHORE, i-manager 's , Vol. No. 1 l Journal on Information Technology 5 December 2015-February 2016.

[13] Cyber Security and Ethical Hacking by P. Harika Reddy, Surapaneni Gopi Siva Sai Teja, International Journal for Research in Applied Science & Engineering Technology (IJRASET) , ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 6 Issue VI, June 2018

[14] Ethical Hacking by Azhar Ushmani , International Journal of Information Technology (IJIT) – Volume 4 Issue 6, Nov-Dec 2018.

[15] Conceptual Oriented Analysis on the Modern Tools and Techniques to Enrich Security Vulnerabilities in Ethical Hacking by Dr.K.Sai Manoj, Ms. K. Mrudula ,Mrs G.Maanasa, Prof.K.Phani Srinivas, International Journal of Computer Science Trends and Technology (IJCST) – Volume 7 Issue 3, May - Jun 2019

