IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115156

Study of Ethical Hacking

Sakshi Madhukar Adewar[1], Neehal B. Jiwane[2], Ashish B. Deharkar[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

Asst. Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[2]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract: We have been living in the modern technology of the world where all the data and the resource comes us in the online mode rather it is personal data or any information notice and so on as nowadays all the information are available online there are large number of user who are accessing it among some of them uses the information for gaining the knowledge and some think how to destroy or steal the data which are present in the website or database without any knowledge of the owner of the website. This paper purpose is that how the data has been stolen by someone its know as hacking who are those hackers , what code conduct of ethical hacker and need of them. As we can see that the state security on the internet is very poor hacking is the activity in which the person exploits the weakness in the system for the profit of themselves. The public and the private organization migrates the function applications such as marketing, commerce and database which are access on the internet. This paper describes about the attacks of the hacking and what is the ethical hacking and impact of ethical hacking.

Keywords: Ethical hacking, hacking, hackers, risk management

I. INTRODUCTION

As the technology of computer has been advanced, it also has the darkest side HACKERS . In global we can see that the use of the internet is growing faster and increasing rapidly day by day , a large amount of data and large number of files are moving online with help of the internet therefore as the data move the security plays the major role for securing one's data, In every field there is need of internet such as in banks, online transaction, money transfer online, sending and receiving the data of various forms as all things and process are going in an online mode but mainly the company and big organization are targeted by the various type of hacking attacks for there profit if the idea comes in the mind we think bad for that who can steal the data who can leak someone valuable data without their knowledge those persons are there with a high computer skills who try to break someone security for gaining the personal information but all the time is not same, Hence we can overcome as we have the ethical hackers who are also the expertise of the computer just like the hacker, but they have a good intention and are bounded by the set of rules and regulations in every organization. These are those persons who try to protect the online moving data by the attacks of various hackers who tries to break by keeping it safe. This paper tells us about the hacker and also the ethical hacker also to be aware of the attacks performed by the hacker while in every online moving data.

II. WHAT IS HACKING?

Hacking is technique of finding the poor link in the computer and the network system to gain the unauthorized access to someone data or to change the feature of the computer system and the network system it describes the modification in the computer system in the hardware and software for accomplish goals which is not aligned with the user, its also called that breaking someone security and stealing the personal data , secret data, records such as phone number, emails, banking password, transaction money address etc.

III. HACKERS

The hacker term is a popular term which has been described by the media who breaks the security of the data using the bugs or by using his expert knowledge they are the expert of both the hardware and the software programming, also they are masters in security and the network .

Hackers are classified into the groups

1. White Hat Hackers
2. Black Hat Hackers
3. Grey Hat Hackers

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115156

1. White Hat Hackers:

A white hacker is specialist of the computer security that breaks and find the loopholes in the protected network and also in the computer system in some organization and company and suggest them to improve the security of the data. White hat hacker uses their skill to protect the organization data before the bad hacks which will be done by the hacker the method use by them is similar as the bad hackers, but they have the permission and can authorize and get access to the data who hire them to do so.

2. Black Hat Hackers:

The black hat hackers are also known as the (cracker) of the security system with a bad intention in order to steal or leak the data. They violate the security system for their own personal gain and most of the hacker for gaining the money they do so . These are the person who typically wants to prove how expert they are in the stealing, credit, fraud etc.

3. Grey Hat Hackers:

They are also the computer hacker security expert but for sometimes violates the laws but does not have any intentions like the black hat hackers. The term gray has been derived from the Black hat and also the White hat whereas the white hacker protect the threads of security , black hacker break down the security illegally, Whereas the gray hacker neither do the illegal things nor tells anybody , They represent between the white hacker who maintain the security and black hacker who operates to exploit computer system.

IV. METHOD USED BY THE HACKER

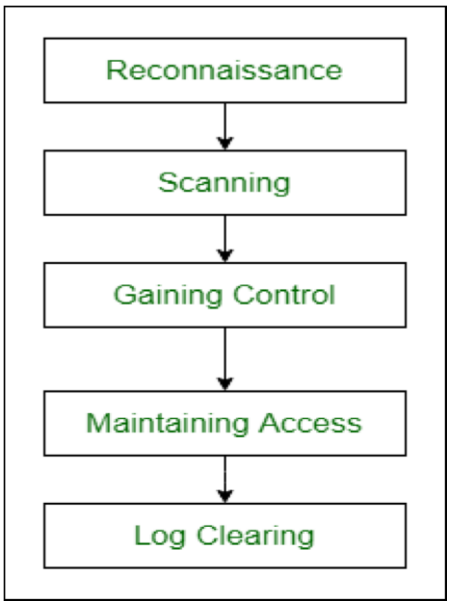

Fig.1 Method uses the hacker

1. Reconnaissance:

The process of collecting and gathering the whole information about the target system or target network is called as reconnaissance. It is the process of finding the vulnerabilities in the system it means that finding the way which is vulnerable, and then the further process is carried by the hacker if the hacker find a way access the system at end of reconnaissance phase than the hacker has the bunch of information and can construct to attack on the target .organization.

2. Scanning:

Before the hacking attack of hacker wants to be system should be up, that which version has been used and application used scanning, searching, of all the open and the close ports, is done that means finding the way to enter the system data, Thus it includes obtaining the target IP address, username, and the accounts related to that ,In this phase the information which is gathered in the reconnaissance are used to examine the network tools like Dialers, Port Scanners etc. are used.

3. Gaining Control:

This phase is very important for the hacker as the information gathered by the two phases are used to enter the and take the control over the target organization system through the network and physically, This phase is also called as the "Owing the system".

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115156

4.Maintaining Access:
After the entry gaining in the system in the previous phase the hacker maintain the system for future attacks and changes the system in such a way that any other security personal or any other hacker does not get entry into the system which has been hacked. This is also known as the "zombie System".

5. Log Clearing:
It is the technique in to check whether there is any leftover the log files or any other type of evidence on to hacked system by the hacker can be caught, because there are various tools and technique by which the hacker can be caught.

V. ETHICAL HACKING

Ethical hacking it's a branch of security information, it is also called as the "Penetration testing" or "white hat hackers" . The hacking performed in the particular organization or a company which helps in finding the threats happen in the computer system or network security of the organization . The technique which are used in the ethical hacking are similar to those of malicious hacking, but the only difference is they are legal they used in the productive manner information which has been gathered by the ethical hacking is used for maintaining system security before they have been noticed. The white hacker will be called the ethical hacker as today they are the expert of the computer, and also we can see them in every company and organization they are a paid and professionals they fix all the security system of the computer, and especially they have been noticed by the bad hackers who try to break the security which they have made.

VI. THE CODE CONDUCT OF AN ETHICAL HACKER

Identifying the confidentially and privacy of the data of any company and organization before hacking they should not violet any rule and regulations. There intention must be very clear so that it can not harm the organization. Maintaining the transparency with client or the owner of the company.

VII. NEED OF ETHICAL HACKER IN EVERY INDUSTRY

As every organization has its confidential information which can be hacked by the black hat hackers therefore in order to protect the organization information the ethical hackers are allows hacking their own system if you find any flaws or loopholes in there system can correct them before the hacker tries to hack it.

1. Linux operating system:
As the name tell us that it is the operating system just like Windows and Mac. The operating system is the interface between the hardware of the computer it does manages all the hardware resource available in the computer system it is required for the working of various applications which has been present in the system. But unlike of the Microsoft Windows and Mac operating system it is an open source operating system and is distributed under the source of license.

Fig. 2 Kali Linux Operating System

. It is more secure than the windows, and it's also having very less number of viruses that harms Linux Operating System some of this system Ubuntu, Kali, Fedora, Mint etc. As further in this paper the attack is performed on the Kali Linux

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115156

operating system , Which is a distribution of Linux operating system it is mainly used for the penetration testing and security auditing.

VIII. TOOLS USED BY THE ETHICAL HACKERS

TABLE I

Port Scanner	Super scan, Angry IPS Scanner, Nikto
Packet Sniffers	Wireshark, TCPdump, Ethercap
Vulnerability Exploitation	Metasploit, Sqlmap, Sqlninja
Vulnerability Scanners	Nessus, OpenVAS, Nipper
Hacking Operating System	Backtrack5r3, Kalilinux, S E Linux

IX. CONCLUSION

The whole world is moving towards the technology and towards the digitization of the real world process with increase in the security risk. The purpose of this paper is to describe the working of the malicious hackers or crackers and on the other hand who tries to break the security system and on another side white hat hacker and ethical hacker who tries to maintain the security system of the organization , As in the computer system hacking plays a vital role in both the case as good and also bad this paper tells about how the hacker attack and what are the drawbacks. In conclusion, it must say that the Ethical Hacking is tool for improving the security of the computer system.

REFERENCES

[1]. Lowlesh Nandkishor Yadav “Predictive Acknowledgement using TRE System to reduce cost and Bandwidth” Factor 7.39 Vol. 11, Issue 3, March 2022.
[2]. Ashish B Deharkar “An Approach To Reducing Cloud Cost And Bandwidth Using Tre System”