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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13205

A STUDY OF ETHICAL HACKING AND HACKING ATTACK

G. Divya[1], M. Nasrin Thaslima[2]

PG Student, Department of Computer Science, R.B. Gothi Jain College for Women, Red hills, Chennai-52[1,2]

Abstract: The world of the security on the internet is very poor and getting worse. One of the fastest growing areas in network security, and certainly an area that generates much discussion is that of ethical hacking and hacking attack. Ethical hacking is an identical activity which amines to find and sort out the weakness and susceptibility in the system. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. As nowadays all the information is available online, 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 database without the knowledge of the owner. Thus the need of protecting the system from the nuisance of hacking generated by the hackers is to promote the person who will punch back the illegal attacks on our computer system. The main purpose of this study is to reveal the brief idea of the ethical hacking and hacking attack its affairs with the corporate security. Group of hackers are **white hats, black hats, gray hats.** This paper describes what ethical hacking and hackers attack is, what it can do, an ethical hacking tools which can be used for n ethical hack. This paper tries to develop the centralized idea of the ethical hacking and hacking attack all its aspects as a whole.

Keywords: Criminals, loophole, security, zombie system, network.

I. INTRODUCTION

As the computer technology advances, it is a darker side also; HACKERS. The huge growth of Internet has brought many good things link electronic commerce, email; easy access has limitless stores of reference material etc... As, with the bulk of technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are known as black hat hackers.

The internet has led to the increase in the digitization of various processes like banking, online transaction, online money transfer, online sending and receiving of various forms of data and websites are risk of the data security. Ethical hacker performs the hacks as security tests for their system. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, which are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations. This type of hacking is legal and trustworthy. Further, this paper tells you more about hackers, ethical hackers and aware you about some attacks performed by the hackers on the internet.

ETHICAL HACKING

It is also called “infiltration testing “ or “white-hat hacking” or “Red Teaming”. Ethical hacking is defined as the involved in hacking without malicious intent. The Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security. The poor growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. So, to up come from these major issues, another category of hackers came into existing and these hackers are termed as ethical hackers or white hat hackers. Ethical hacking is a way of doing a security impression. Ethical hacking is legal. The project of ethical hacking is to find vulnerabilities from a hacker's perspective so frameworks can be better secured.

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.

DOI: 10.17148/IJARCCE.2024.13205

Hackers: -

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.

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

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.

Black Hat Hackers:-

A Black Hat Hacker also called as a “Cracker” or Malicious Hackers Other than white hats and black hats. It is a 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 data, compromising the security of big organizations, shutting down or altering functions of websites and networks. They deface the websites, steal the information, and estimate the security. They crack the programs and passwords get entry in the unauthorized network or system

Gray Hat Hackers: -

Another type of hacking is a Grey Hat**.** A Grey Hat Hacker is a computer hacker or security expert who sometimes contravenes 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. The white hat hackers find out the vulnerabilities in the computer system or the networks and doesn’t tells nobody 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. A Gray Hat may breach the organizations’ computer security, and may exploit and deface it. But usually they make changes in the existing programs that can be repaired. They hack or gain unauthorized entry in the network just for fun and not with an intension to harm the Organizations’ network

II. HACKING PROCESS

The Ethical hacking needs to be planned the process before itself. Planning is essential for any of testing – from a simple password test to all out penetration test on a web application. Backup off data must be secure, otherwise the testing may be called off unexpectedly if someone claims they never authorizes for the tests.

1. Specific systems to be tested.
2. Risks that are involved.
3. Preparing schedule to carry test and overall timeline.
4. Gather and explore knowledge of the systems we have before testing.
5. What is done when a major vulnerability is discovered?
6. The particular deliverables- this includes security assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with counter measures that should be implemented when selecting systems to test, start with the most critical or vulnerable systems.

DOI: 10.17148/IJARCCE.2024.13205

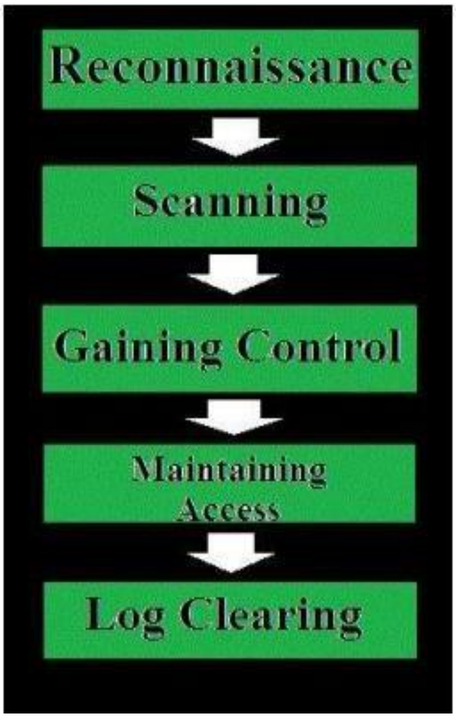

Figure -1 Phases of Ethical Hacking

Reconnaissance:

The process of collecting information gathering about the target system is called reconnaissance. The process includes finding susceptibility in the computer system, which means find, the plan to which is left vulnerable.

Scanning:

In Scanning Phase, First gathered the information in phase 1 is used to examine the network. In scanning, finding of all open, as well as closed ports, is done means searching a way to enter the system. The tools like Dialers', Port Scanners Etc.

Gaining Control:

This is gain a phase 3 process. This is part of real and actual hacking procedure where the gathered information in the previous two phases is used to enter and take control of the target system through the network or physically. In earlier 2 process to attack and enter into the Local Area Network, Local pc address, Internet or offline. This process is also called as "Owning the System"

Maintaining Access:

After secure a entry in the system in the above step the hacker maintains the access to system for the future attacks and make changes in the system in such a way that any other security personal or any other hacker doesn't get the entry into the system into which is hacked. This is the situation in which the attacked system is also called as the "Zombie System".

Log Clearing:

It is the technique of disconnect any leftover log files or any other types of proof on the hacked system from which the hacker can be caught. There are different tools in the ethical hacking techniques from which a hacker can be caught like penetration testing. After reading about hacking and the shades of hackers there should be some way or some technique of protecting the computer system or the computer networks form the malicious hackers, therefore the terms "Ethical Hacking" and "Ethical Hackers" came into the industry.

DOI: 10.17148/IJARCCE.2024.13205

III. CONCLUSION

In today's digital landscape, ethical hacking is essential for organization to ensure the security and protection of their data and systems. It provides numerous benefits and can help to prevent devastating consequences such as data breaches and financial loss.

REFERENCES

[1]. B. McMahan et al., "Communication-Efficient Learning of Deep Networks From Decentralized Data", *Artificial Intelligence and Statistics Proc. PMLR*,vol. 10, no. 1, pp. 1273-82, 2017.

[2]. C. En Guo, S.-C. Zhu and Y. N. Wu, "Primal Sketch: Integrating Structure and Texture", *Computer Vision and Image Understanding*, vol. 106, no. 1, pp. 5-19, 2007.

[3]. Long Zhang ; Kai Zhao; "Study on Security of Next Generation Network"; IEEE International Conference on Service Operations and Logistics, and Informatics; Volume 1; Page(s): 538 - 541; IEEE Conference Publications;2008

[4]. Monique J. Moroow; "IP NGN - Foundation for Ubiquitous Networking"; Cisco Systems; ITU Ubiquitous Networking Societies Workshop; Geneva; April 7,2005.

[5]. Telecommunication Security. X.805, Security architecture for systems providing end-to-end communications.

[6]. M. Hayeri Khyavi; "Elliptic Security Model"; 4th Information Security Managemetn System"; Tehran, Iran ;2006

[7]. Rui Huang, Danfeng Yan,Fangchun Yang; "Research of Security Metric Architecture For Next Generation Network"; IEEE International Conference on Network Infrastructure and Digital Content ; Page(s): 207 – 212; IEEE Conference Publications;2009

[8]. Napoleon D. and Praneesh M. "Detection of Brain Tumor using Kernel Induced Possiblistic C-Means Clustering", volume no.3, issue no.9, pp 436-438, 2013

[9]. Cisco Systems; "IP Next-Generation Network Security for Service Providers"; http://www.cisco.com/c/dam/en/us/solutions/collateral/service- provider/secure-infrastructure/net_implementation_white_paper0900aecd803fcbbe.pdf;

[10]. A. L. Corte, M. Scata; " Security and QoS Analysis for Next Generation Networks" ; , International Conference on Information Society(i-Society), IEEE; pages: 248-253; June 2011