International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET2310666

Unlocking Security : The World of Ethical Hacking

Suthar Bhavik[1], Mansi Luhariya[1], Dr. Darshanaben Dipakkumar Pandya[2], Dr. Abhijeetsinh Jadeja[3]

[1]Department of Computer Science, Shri C. J Patel College of Computer Studies (BCA), Sankalchand Patel University, Visnagar, Gujarat, India

[2]Associate Professor, Department of Computer Science, Shri C. J Patel College of Computer Studies (BCA), Sankalchand Patel University, Visnagar, Gujarat, India

[3]I/C Principal, Department of Computer Science, Shri C. J Patel College of Computer Studies (BCA), Sankalchand Patel University, Visnagar, Gujarat, India

ARTICLEINFO

Article History :

Accepted: 01 Jan 2024
Published: 10 Jan 2024

Publication Issue :
Volume 11, Issue 1
January-February-2024

Page Number :
41-45

ABSTRACT

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 databases without the knowledge of the owner. The purpose of this paper is to tell what is hacking, who is hackers, what is ethical hacking, what is the code of conduct of ethical hackers and the need of them. A small introduction of Linux Operating System is given in this paper. All the techniques are performed on the Linux operating system named Kali Linux. After this some basic hacking attacks covered in the paper are MiTM Attack (Man in The Middle Attack), Phishing Attack, DoS Attack (Denial of Services Attack). Further what is Wi-Fi, what are the techniques used in the Wi-Fi protection and the methods used by the hackers to hacks Wi-Fi passwords is covered in the paper.

Keywords :- Hackers, Malware, Ethical Hackers, MiTM, DoS, Phishing, Wi-Fi phishing, Code of conduct

I. INTRODUCTION

As the computer technology advances, it has its darker side also; HACKERS. In today world the size of the internet is growing at a very fast rate, a large amount of data is moving online, therefore, data security is the major issue. The internet has led to the increase in the digitization of various processes like banking, online transaction, and online money transfer, online sending and receiving of various forms of data, thus increasing the risk of the data security. Nowadays a large number of companies, organizations, banks, and websites are targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker we all think of the bad guys who are computers experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge. They are the persons with very high

computer skills who tries to break into someone else security for gaining access to their personal information, but all the times it is not like that. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, who 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. These are the persons who try to protect the online moving data by the various attacks of the hackers and keeping it safe with the owner. Further, this paper tells you more about hackers, ethical hackers and Linux operating system (kali Linux) and aware you about some attacks performed by the hackers on the internet.

What Is Hacking?

Hacking is a broad term that refers to the unauthorized access, modification, or manipulation of computer systems, networks, or devices. It involves exploring weaknesses in computer systems or networks to gain access to data, disrupt operations, or carry out other activities that were not intended by the system's owner.

Hackers:-

Hackers are individuals with advanced knowledge of computer systems and networks. They possess skills in programming, networking, and security and can use this expertise to gain unauthorized access to computer systems, exploit vulnerabilities, and manipulate or steal data. 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. Grey Hat Hackers

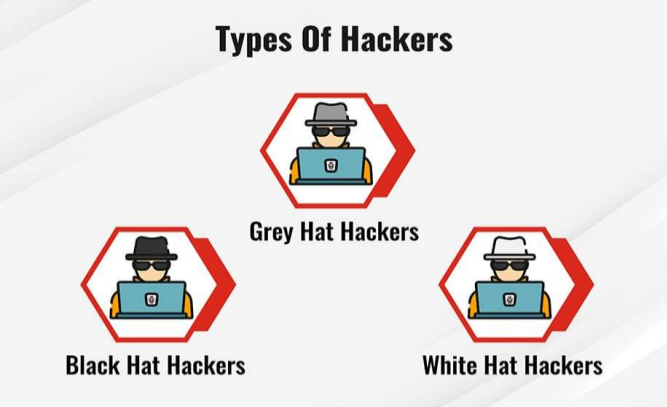

Fig 1. Types of Hackers

1. White Hat Hackers:-

These hackers use their skills for ethical purposes. They work legally, often employed by organizations to identify and fix security vulnerabilities, test systems for weaknesses, and improve cybersecurity measures.

2. Black Hat Hackers:-

These hackers engage in unauthorized and malicious activities. They break into systems for personal gain, financial profit, data theft, disruption, or other nefarious purposes. Black hat hackers are responsible for most cybercrimes.

3.Grey Hat Hackers:-

This category of hackers operates between white hat and black hat hackers. They may access systems without authorization but not with malicious intent. They might uncover vulnerabilities and disclose them to the system owner, often requesting payment for their services.

Ethical Hacking Process:-

Fig 2 : Ethical Hacking

1. **Reconnaissance:**

Understand the scope and objectives of the ethical hacking engagement. Gather information about the target system or network using non-intrusive methods such as publicly available information, network scanning, or reconnaissance tools.

2. **Scanning:**

Conduct more detailed examination of the target system's infrastructure, including networks, servers, and applications. Use specialized scanning tools to identify open ports, services, and potential vulnerabilities.

3. **Gaining Access:**

Attempt to exploit discovered vulnerabilities and weaknesses to gain access to the system or network. Utilize various methods such as password cracking, social engineering, or exploiting software vulnerabilities.

4. **Maintaining Access:**

Once initial access is achieved, ethical hackers attempt to maintain persistent access to the system to simulate the actions of a real attacker. Install backdoors or maintain control over the system to demonstrate potential risks and the extent of a successful intrusion.

5. **Clearing Tracks:**

It is very important, after gaining access and misusing the network, that the attacker cover the tracks to avoid being traced and caught. To do this, the attacker clears all kinds of logs and malicious malware related to the attack.

6. **Denial of Services (DoS)**

A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted system, network, website, or service by overwhelming it with a flood of traffic or requests. The primary goal of a DoS attack is to render the targeted system inaccessible or unusable by legitimate users.

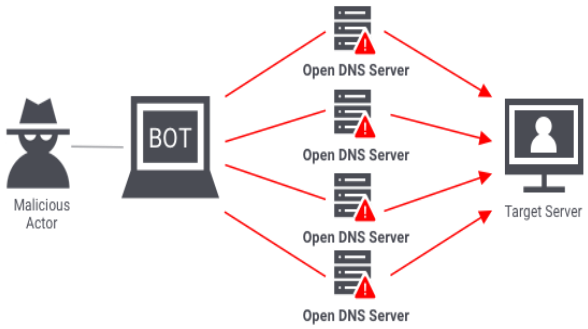

Fig 3 : Dos Attack

Steps for performing a Dos attack on Kali Linux: -

Open the terminal in kali Linux and type the command hping3 –c 100000 –d 120 –S –w 64 –p 21 –flood –rand-source (address of the target website) and press enter. In the above command meaning of different parameters are as follows:- hpin3 is the name of the application binary. –c 100000 is the number of packets to send. –d 120 is the size of each packet that is to be sent to target machine. –s means sending SYN packets only , –w 64 means the TCP window size , –p 21 is the destination port (21 being FTP port). You can use any port here , –flood means sending packets as fast as possible, without taking care to show incoming replies , –rand-source means using Random Source IP Addresses , After entering the previous the DoS attack is started to see how the attack is working open a new terminal and type tshark and press enter there you will be able to see how packets are sent to the target. Now to stop the attack press ctrl+c in the DoS attack terminal window. After that you will be able to see how many packets are sent. Some of the tools used by the ethical hackers:

Port Scanners	Nmap, Superscan, Angry IP Scanner, Nikto, Unicornscan, Autoscan.
Packet Sniffers	Wireshark, TCPdump, Ethercap, Dsniff, EtherApe.
Vulnerability Exploitation	Metasploit, Sqlmap, Sqlninja, Social Engineer Toolkit, Netsparker, BeEF, Dradis
Vulnerability Scanners	Nessus, OpenVAS, Nipper, Retina, QualysGuard, Nexpose.
Hacking Operating System	Backtrack5r3, Kalilinux, SE Linux, Knoppix, Backbox linux, Pentoo, Matriux, Krypton, NodeZero, Blackbuntu.
Intrusion Detection Systems	Snort, Netcap

II. CONCLUSION

The whole world is moving towards the enhancement of technology, and more and more digitization of the real world processes, with this the risk of security increases. This paper described the working of malicious hackers or crackers on one hand who tries to illegally break into the security and on the other hand white hat hackers or ethical hackers, who tries to maintain the security. As in the computer system, hacking plays a vital role as it deals with both sides of being good or bad. Further, this paper tells about the types, working, and various attacks performed by the hackers. In conclusion, it must be said that Ethical Hacking is a tool which when properly utilized can help in better understanding of the computer systems and improving the security techniques as well.

III. REFERENCES

[1]. Is Ethical Hacking Ethical " ?," Int. J. Eng. Sci. Technol., 2011.

[2]. S.P. Oriyano, "Introduction to Ethical Hacking," in CEHTMv9, 2017.

[3]. B. Sahare, A. Naik, and S. Khandey, "Study of Ethical Hacking," Int. J. Comput. Sci. Trends Technol., 2014.

[4]. S. Patil, A. Jan gra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security," in IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017, 2018, doi: 10.1109/ICPCSI.2017.8391982.

[5]. G. R. Lucas, "Cyber warfare," in The Ashgate Research Companion to Military Ethics, 2016.

[6]. P. Engebretson, "Reconnaissance," in The Basics of Hacking and Penetration Testing, 2011.

[7]. Ehacking, "Scanning and Enumeration- Second Step of Ethical Hacking," ehacking, 2011.

[8]. R. Baloch, Ethical Hacking and Penetration Testing Guide. 2017.

[9]. Hackers? Norton, "What is the Difference Between Black, White and Grey Hat " Emerging Threats, 2019.

[10]. S. Tulasi Prasad, "Ethical Hacking and Types of Hackers," Int. J. Emerg. Technol. Comput. Sci. Electron., 2014.

Cite this article as :

Suthar Bhavik, Mansi Luhariya, Dr. Darshanaben Dipakkumar Pandya, Dr. Abhijeetsinh Jadeja, "Unlocking Security : The World of Ethical Hacking ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 11 Issue 1, pp. 41-45, January-February 2024. Available at doi : https://doi.org/10.32628/IJSRSET2310666
Journal URL : https://ijsrset.com/IJSRSET2310666

Authors Profile:-

SUTHAR BHAVIK , PURSING BCA-4 FROM SHRI C. J. PATEL COLLEGE OF COMPUTER STUDIES (BCA) , SANKALCHAND PATEL UNIVERSITY , VISNAGAR, 384315.

MANSI LUHARIYA, PURSING BCA-4 FROM SHRI C.J PATEL COLLEGE OF COMPUTER STUDIES (BCA), SANKALCHAND PATEL UNIVERSITY, VISNAGAR, 384315.

DR. DARSHANABEN DIPAKKUMAR PANDYA, ASSOCIATE PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE , SHRI C. J PATEL COLLEGE OF COMPUTER STUDIES (BCA), SANKALCHAND PATEL UNIVERSITY , VISNAGAR, 384315..

DR. ABHIJEETSINH JADEJA, I/C Principal, DEPARTMENT OF COMPUTER SCIENCE, SHRI C. J PATEL COLLEGE OF COMPUTER STUDIES (BCA), SANKALCHAND PATEL UNIVERSITY , VISNAGAR, 384315.