

A Study on Ethical Hacking

Dr. Ashish Oberoi

Assistant Professor, Department of Computer Science & Engineering, RIMT University, Mandi Gobindgarh, Punjab, India

Correspondence should be addressed to Dr. Ashish Oberoi; ashishoberoi@rimt.ac.in

Copyright © 2022 Made Dr. Ashish Oberoi. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- Though all material is now available online, numerous individuals are using it; most are using it to learn things, while many others are using it to educate both how to harm or stealing information from websites or networks without such owner's permission. The purpose of this essay is to define hacking, who programmers seem to be, what vulnerability assessment is, what ethically hacking's code of conduct is, but also why browser hijackers are required. The Linux kernel is briefly described in detail.. All of the methods are carried out on the Kali Linux operating system. Following that, the article discusses phishing attacks and denial of service attacks (Denial of Services Attack). In addition, the paper discusses what Wi-Fi is, how to secure Wi-Fi networks, and how hackers crack Wi-Fi passwords. This paper is very useful for future work as researcher can use this paper for their survey.

KEYWORDS- Computer, Data, Ethical Hacking, Hacker, Security.

I. INTRODUCTION

As computer technology improves, it also brings with it a darker side: HACKERS. Because the internet is rapidly increasing in size and a significant quantity of data is going online in today's world, data security is a key concern [1]. The internet has accelerated the Certain transactions, including as accounting, electronic payments, online cash payments, plus online mailing of many datasets, have become more digitalized, creating a larger risk to cyber theft. Hackers are currently launching various types of hacking attacks on a wide range of companies, corporations, governments, and webpages [2] [3].

Before Americans hear the term "hacker," we naturally think of malevolent computer professionals who try to extract, leak, or destroy somebody else's private or essential data without their permission. They are those with extensive computer applications that strive to breach

another's stability in order to get access to such information, albeit this is not the case (3). To prevent getting hijacked by cybercriminals, we use Ethical Hackers, who are computer experts who are similar to hackers but have good motives or are bound by a set of norms and regulations created by various organizations. These are the people who try to protect internet-moving data from various hacker attacks while keeping it secure with the owner. In addition, this article covers hacking, ethical hacking, and indeed the Macos.as well as various hacker assaults on the internet [4] [5].

A. Hacking:

Phishing is the practice of locating and abusing shortcomings or holes in electronic communications throughout order to gain unauthorized access to data or change the characteristics of the target devices and networks (5). Cyber - attack is the tampering with personal computers, applications, or networks in order to accomplish goals that are not in the users' best interests. Hackers into another's security and collecting personal data also including phone calls, card numbers, emails, and bank card usernames is indeed known as identity theft., and so on [6] [7].

B. Hacker:

In contemporary culture, a "hacking group" is one who breaks into another's vulnerability using holes and exploits, or who utilizes his technological skills proactively or negatively (6). Hackers include programmers with expertise in both equipment and software. A programmer is a computer scientist who knows how to create, as well as automation and control management. He is the kind of guy that enjoys learning new technologies and computer system specifics in order to improve his capabilities and talents[8]. HACKERS may be divided into three categories depending on their methods of operation or their intentions as shown in Figure 1 [9] [10].



Figure 1: Illustrates the categories of Hat Hackers[11]

C. White Hat Hackers:

A potential attacker is an antivirus professional who breaks into something and discovers known vulnerabilities in a secured network or computerized system and processes or corporation, then repairs them to ensure security. Attractive Targets For hackers use their skills and knowledge to protect a company before hostile or malicious hackers find it and do harm. But since their tactics are identical to those used by criminal hackers, ethical hacking Trojans have been accepted by the industry. Authorization to do so by the organization or corporation that employs them [12].

D. Black Hat Hackers:

A Malware Attack, also known as a "Popsicle," is a software product proficient who attempts to break into anyone's security with the goal of stealing or severe harm to with their important or secret information, compromising the security of major corporations, or closing down and otherwise altering this same processes of social media platforms. Social. They profit from cryptography for self gain. These are those that want to show off their skills. Vast computer expertise by committing different cybercrimes such as identity theft, credit card fraud, and so on [13].

E. Grey Hat Hackers:

They are a computers programmer or military expert who, other stealing information, sometimes defies the law and therefore has no malicious intent. White hat hackers uncover flaws in electronic communications and do not alert anybody until they are addressed, while black hat hackers unlawfully exploit information systems or networks seek find weaknesses and advise individuals on how to get there, and malicious hackers execute neither. Cybercriminals are a hybrid of cyber attackers who seek to safeguard devices and breaches of security who attempt to manipulate them. Maliciously [14] [15].

F. Ethical Hackers Need in Industry:

Because every organization has confidential information that businesses would recruit network of thousands and allow them to get moral entrance about their own facilities in exploring weaknesses or gaps and patch issues before another intruder hacks something that, in terms of protecting the knowledge from being pirated or harmed by malevolent cybercriminals (9). Later, let's look at various hacking assaults carried out by hackers on the internet. Prior to that, you must be familiar with Linux operating systems and how they are used in hacking operations [16].

G. Linux Operating System:

It is, as the name implies, an operating system similar to Windows and Mac. An operating system serves as a link between the client and the computer's hardware, managing all of the computer's hardware resources. An operating system is needed for the operation of different programs on a computer system. Linux, unlike Microsoft Windows users are both Linux based systems that are distributed under a creative commons. It is considerably safer than Window frames and had a much lower infection count. That may damage Linux. Ubuntu, Kali Linux, Fedora, Linux Mint, and others are examples of Linux operating systems [17].

H. Phishing:

Phishers is something of a botnet or spammers where another hacker attempts to get private data from with a victim, also including identities, login credentials, card details, mailing addresses, and mobile banking passcodes. It's achieved by giving bogus emails or creating bogus websites that seem just like the genuine thing ones[18].

Steps for performing phishing on Kali Linux:

Step 1: In Kali Linux, open the terminal and type toolkit, then press enter.

Step 2: Next, hit y and then enter.

Step 3: Now choose 1. Social Engineering Attacks from the drop-down menu.

Step 4: Finally, pick the second of the two website assault routes and press enter.

Step 5: Select the third credential harvester attack technique from the drop-down menu.

Step 6: Finally, choose second 2. Site cloner.

Step 7: The Start a new command browser as well as type process. This allows; copy this inept number from there and replace it all into the earlier screen; then click yes.

Step 8: Now type the Web page you really like to clone into the address bar and press enter. It will take time to clone the website.

Step 9: Once operation is done, open a new computer process and then go to the www area using the phrase cd /vary/www.

Step ten: Type ls in to console once you've gone to this directory and press enter. Harvester 2016-01-01 10:37:25.332885.txt will be located there. Then enter the command cat in the terminal window. 2017-03-20 10:37:25.332885.txt Harvester 2017-03-20 10:37:25.332885.txt Collection 2017-03-20 10:37:25.3 Harvester

Step 11: The defendant's e - mail and passcode is shown on the fake or cloned page after entering the prior request [19].

I. DoS (Denial of Service):

It's a kind an aggressor attempts to make a workstation, blog, another file server unavailable to its subscribers for a certain timeframe or indefinitely, as well as disrupting the capabilities of a hosted connected to the web. This project will be carried out by sending a large amount of traffic to the webpage, server, or workstation, leading others to become overcrowded and being unable to complete just about all of requests. The denial-of-service attacks might last for days, weeks, or even months. The attacker's query delivery speed here to server side or page is very fast, in the billions of gigabits range (mbps) or gigabits per second (gaps) [20].

Steps for performing DoS on Kali Linux:

The following are the definitions of the various arguments in the aforementioned command:

- The application binary's name is hpin3.

- The number of packets to transmit is specified by `-c 100000`.
- The size of each packet to be delivered to the target computer is specified by `-d 120`.
- `-s` specifies that only SYN packets should be sent.
- The TCP window size is specified by `-w 64`.
- The destination port is `-p 21`. You are free to use any port here.
- `-flood` denotes transmitting packets as quickly as feasible without regard for incoming responses.
- Random Source IP Addresses are used with `-rand-source`.

Step 2: A DoS attack is launched after entering the preceding to show how the assault works. You can observe how packets are delivered to the destination by opening a new terminal and typing `tshark` and pressing enter [21].

Step 3: In the DoS attack terminal window, hit `ctrl+c` to terminate the assault. You'll be able to check how many packets were dispatched after that.

J. Stages to become a Hacker:

Following stages to become a hacker is shown in Figure 2.



Figure 2: Illustrates the various stages to become a Hacker

K. Benefits of Ethical Hacking:

- This contributes to the battle against cyber terrorism and national security breaches.
- Ethical hackers are the guys that defends people’s system
- This assists in the building of a mechanism that seems to be impenetrable to hacker's attacks.
- Intrusion.
- It offers safety to financial and economic institutions.
- It offers solution in finding the loopholes in user’s system [22].

L. Challenges of Ethical Hacking:

- It might damage the records or documents of an association.
- They could utilise the data they've obtained for nefarious reasons as little more than a consequence, in order to thrive throughout this paradigm, trustworthy designers and developers are necessary.
- Appointing expert hackers might raise the costs to the firm.
- It can damage somebody’s privacy [23].
-

II. DISCUSSION

As previously said, ethical hacking is a method of protecting our computer systems by defending them against malicious hackers. Because technology is developing at a breakneck pace and all information is now stored online, data security is critical. Professional hackers are hired by companies to discover vulnerabilities in their systems so that they can protect against bad hackers. The author has addressed hacking, ethical hacking, kinds of hackers, advantages, and difficulties of ethical hacking in this review article. People may choose ethical hacking as a profession since white hat hackers are in high demand in the police department, where they must discover criminals' information in order to identify them. Ethical hacking also opens doors to positions such as penetration tester, system administrator, and security analyst, among others. As a result, ethical hacking has a bright future since security is required to protect data from malevolent hackers [24] [25].

III. CONCLUSION

The whole world is moving toward technology breakthroughs and greater digitization of real-world processes, posing a security threat. Under this articles, the results of malicious hackers or crimps, on a one hands, who

attempt to illegally loot, and ethical hacking hackers or security researchers, but from the other foot, who strive to maintain security, were described. Hacking is a kind of cybercrime. Important in the computer system since it works both with positive and negative aspects. In addition, this article discusses the different kinds, methods, and assaults used by hackers. To sum up, ethical hacking is a tool that, when correctly used, may assist in a better knowledge of computer systems as well as the improvement of security methods. Also, Ethical hacking provides job opportunities such as Penetration tester, System administrator, security analyst etc. So, the future of ethical hacking is bright as security is needed in securing the data from malicious hackers.

REFERENCES

- Jamil D. IS ETHICAL HACKING ETHICAL? 2011;3(5):3758–63.
- Hartley RD. Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack. *J Int Technol Inf Manag.* 2015;24(4).
- Jain RK, Kumar A, Singh NL, Tommasino L, Singh BK. Measurement of peak fluence of neutron beams using Bi-fission detectors. *Pramana - J Phys.* 2012;
- Vignesh R, Rohini K. Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security. *Int J Eng Technol.* 2018;
- Kumar S, Singh MK, Jain RK, Singh V. Characteristics of the projectile and target fragments produced in 8 4 Kr 3 6 - Emulsion interaction at 1 GeV per nucleon. *Int J Mod Phys E.* 2020;
- Singh MK, Kumar S, Jain RK, Singh V. Study of emission characteristics of the projectile fragments produced in the interaction of 84Kr36 with nuclear emulsion detector at 1 GeV. *Chinese J Phys.* 2020;
- Chandra N, Parida S. Quantum entanglement in photon-induced electron spectroscopy of atoms and molecules its generation, characterization, and applications. In: *Advances in Imaging and Electron Physics.* 2016.
- Tulasi Prasad S. Ethical Hacking and Types of Hackers. *Int J Emerg Technol Comput Sci Electron.* 2014;11(2).
- Duksh YS, Kaushik BK, Agarwal RP. FDTD technique based crosstalk analysis of bundled SWCNT interconnects. *J Semicond.* 2015;
- Rai J, Tripathi RC, Gulati N. A comparative study of implementing innovation in education sector due to COVID-19. In: *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020.* 2020.
- Hat Hackers.
- Mishra N, Singhal P, Kundu S. Application of IoT products in smart cities of India. In: *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020.* 2020.
- Singh S, Kumar J. Miniaturized triband circular patch antenna for X band, Ku band and K band applications. In: *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020.* 2020.
- Al-Karaki JN, Ababneh N, Hamid Y, Gawanmeh A. Evaluating the effectiveness of distance learning in higher education during covid-19 global crisis: Uae educators' perspectives. *Contemp Educ Technol.* 2021;
- Jagtap MT, Tripathi RC, Jawalkar DK. Depth accuracy determination in 3-d stereoscopic image retargeting using DMA. In: *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020.* 2020.
- Pandey B, Sharma KP. Radar Transmogrification Technology: Support for Unmanned System. In: *Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019.* 2019.
- Singh D. Robust controlling of thermal mixing procedure by means of sliding type controlling. *Int J Eng Adv Technol.* 2019;
- Chow E. Ethical Hacking & Penetration Testing. *IT Res Pap.* 2011;
- Anand V. Photovoltaic actuated induction motor for driving electric vehicle. *Int J Eng Adv Technol.* 2019;
- Solanki MS, Goswami L, Sharma KP, Sikka R. Automatic Detection of Temples in consumer Images using histogram of Gradient. In: *Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019.* 2019.
- Solanki MS, Sharma DKP, Goswami L, Sikka R, Anand V. Automatic Identification of Temples in Digital Images through Scale Invariant Feature Transform. In: *2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020.* 2020.
- Usha S, Jyothi MN, Sharadamma N, Dixit R, Devaraj VR, Nagesh babu R. Identification of microRNAs and their targets in Finger millet by high throughput sequencing. *Gene.* 2015;
- Jain A, Jain S, Jain R, Kohli DV. Coated chitosan nanoparticles encapsulating caspase 3 activator for effective treatment of colorectal cancer. *Drug Deliv Transl Res.* 2015;
- Ramos Brandão P. The Importance of Authentication and Encryption in Cloud Computing Framework Security. *Int J Data Sci Technol.* 2018;
- Sah MK, Gupta DK, Rani P. Energy Efficient Routing Protocol for Wireless Sensor Networks with Multiple Sinks. In: *Proceedings - 2015 2nd IEEE International Conference on Advances in Computing and Communication Engineering, ICACCE 2015.* 2015.