NJESR/December-2022/Volume-4/Issue-12 E-ISSN-2582-5836
DOI-10.53571/NJESR.2022.4.12.107-117

Ethical Hacking And Their Attacks In Cloud Network

Biju Peter[*1], Jiby P.Joseph[*2]
Head, Lecturer
Department Of Computer Engineering
Government Polytechnic College
Perumbavoor[*1&*2]

(Received:10November2022/Revised:20November2022/Accepted:30November2022/Published:31December2022)

Abstract

Since all information is now accessible online, a large number of users access it. Some of them use it to learn new things, while others use it to learn how to destroy or steal data from websites or databases without the owner's knowledge. This paper aims to explain what hacking is, who hackers are, ethical hacking, the code of conduct of ethical hackers, and why they are needed. This paper provides a brief introduction to the Linux operating system. The Kali Linux Linux operating system is used for all of the methods. An ethical hacker is a computer and network specialist who attacks security systems on behalf of their owner in search of weaknesses that could be exploited by a malicious hacker. The rapid expansion of the Internet has resulted in numerous positive outcomes: e-commerce, e-mail, collaborative computing, and brand-new areas for the dissemination of information and advertisements Businesses and governments are increasingly concerned about ethical hacking, also known as "red teaming," "intrusion testing," and "penetration testing." Potential customers are concerned about maintaining control over personal information, and organizations are concerned about the likelihood of being "hacked." Programmers are ordered by their work and information. The ethical hackers are known as white hat hackers. Hacking methods are used by ethical hackers to guarantee safety. Moral hacking is expected to shield the framework from the programmer's harm. The primary objective of the ethical hacking study is to evaluate the system's security and provide a report to the system's owner. The various aspects of ethical hacking are briefly discussed in this paper.

KeyWords: Cybercrimes, Clearing Tracks, Computer Security, Ethical Hacking, Scanning And Enumeration.

Introduction

Ethical hacking innovation spreads to assorted everyday issues and specifically to each stroll of the PC business. The appropriate technology should be used to communicate the necessity to safeguard common data. Ethical hacking emerged as the most recent and cutting-edge computer technology as a result of the cleverness of hackers[1]. Every organization, no matter how big or small uses this as the first layer of security to safeguard their data. In today's world, it's hard to know what the general public really wants, and it's even harder to know why every ethical hacker enters vulnerable networks or systems. People are finding resources that support the ever-increasing use of technology. If these devices are used by the wrong people, they could cause good trouble and violate our constitutional right to privacy, dignity, and free will. With the rise of cybercrime, ethical hacking is becoming an effective policy for combating online threats[2]. In general, ethical hackers are those who are permitted to breach supposedly "secure" computer systems without malicious intent but with the intention of discovering vulnerabilities in order to carry out better preservation activities. Sometimes, a company's local IT security officers or managers are informed that a "penetration test" is about to take place. They might even be able to look over the hacker's shoulder, but most of the time, they are not. The senior staff, sometimes just two or three board members, are the only ones who know about the attack. Many ethical hackers are wage-earning employees who regularly carry out scheduled hacking programs for consultants and others[3]. There are a number of subfields within the prevalent field of ethical hacking: As a result, it would be impossible to classify all "hackers" in the same way. A celebrity who hacks without malicious intent and assists businesses in securing their systems is known as an ethical hacker, also known as a white-hat sneaker or hacker. A "black-hat" hacker, on the other hand, uses their skills to commit cybercrimes, typically for financial gain. In the meantime, the "grey-hat" hacker has been identified and is searching for compromised systems and informing the company[4]. As computer technology develops, it also has its negative aspects; HACKERS. Data security is the main issue in today's world because of the size of the internet and the large volume of data being transferred online. The internet has increased the risk of data security by increasing the digitization of various processes like banking, online transactions, online money transfers, and online data sending and receiving. Nowadays, hackers use a variety of hacking techniques to target a large number of businesses, organizations, banks, and websites.

When we hear the term "hacker," we typically associate it with malicious computer professionals who attempt to steal, leak, or destroy someone else's confidential or valuable data without their knowledge. They are computer-savvy individuals who attempt to gain access to another person's personal information by breaking into their security, but it is never like that. Ethical hackers, who are also computer experts like hackers but have good intentions or are restricted by a set of rules and regulations set by various organizations, are in the industry to mitigate the risk of being hacked. These are the individuals who work to safeguard owner-owned online moving data from a variety of hacker attacks. In addition, this paper provides additional information regarding hackers, ethical hackers, and the Linux operating system (Kali Linux), and makes you aware of some cyber attacks carried out by hackers online.

What Is Hacking

Finding vulnerabilities in computer systems or networks and taking advantage of them to gain unauthorized access to data or modify the systems' or networks' features is known as hacking. Hacking is the process of altering computer software, hardware, or networks to achieve objectives that are in opposition to the user's objectives. On the other hand, it is also known as breaking into someone's security and stealing their personal or secret data, such as phone numbers, credit card information, addresses, and passwords for online banking, among other things.

Criminals

In popular media, the person who uses bugs and exploits to break into another person's security or uses his expertise to act maliciously or productively is referred to as a "HACKER." Hackers are software and hardware specialists in computers. A hacker is an expert in networks, security, programming languages, and computer nerdiness. He is the kind of person who enjoys learning new technologies, computer details, and improving his capabilities and skills. HACKERS can be divided into three groups based on their methods of operation or intentions:

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

1. White Hat Hackers

A computer security expert known as a white hat hacker exploits security flaws in an organization's or company's computer systems or protected networks by breaking in and

repairing them. White Cap Programmers utilize their abilities and information to safeguard the association before vindictive or awful programmers find it and make any damage to the organization or the association. Although their methods are comparable to those of bad hackers, White Hat Hackers are the authorized individuals in the industry. However, they do so with permission from the organization or business that employs them.

2. Black Hat Hackers

A computer hardware and software expert known as a "Black Hat Hacker," also known as a "Cracker," enters someone's security with the malicious intent of stealing or damaging their important or secret information, compromising the security of large organizations, and disrupting or modifying functions of websites and networks. They break the security of the computer for their own benefit. These are people who, typically in an effort to demonstrate their extensive computer knowledge, engage in a variety of cybercrimes, such as identity theft and credit card fraud.

3.Grey Hat Hackers

A computer hacker or security expert known as a "grey hat" hacker may occasionally break the law, but unlike black hat hackers, they do not intend to harm others. While the black hat hacker illegally exploits the computer system or network to find vulnerabilities and instructs others on how to do so, the grey hat hacker neither illegally exploits it nor instructs anyone on how to do so. This distinction gives rise to the term "Grey Hat," which is derived from the terms "Black Hat" and "White Hat." The term "Grey Hat Hackers" distinguishes between "white hat" hackers, who work to safeguard computer systems, and "black hat" hackers, who do so with malicious intent.

Reconnaissance

Reconnaissance is the process of gathering information about the target system. Finding the ways that have been left vulnerable is part of the procedure, which includes locating vulnerabilities in the computer system. If the hacker discovers a way to gain access to the system, they continue the hacking process. The hacker has a lot of information at the end of the reconnaissance phase that he can use to build a promising attack on the target system.

Scanning

Before launching an attack, a hacker needs to know what applications are running on the system, which versions of those applications are being used, and so on. Finding a way into the system is the goal of scanning, which includes searching all open and closed ports. It includes getting the target's IP address, user accounts, and other information. In this stage the data assembled in the observation stage is utilized to look at the organization and apparatuses like Dialers, Port scanners and so on. are in use. The popular, powerful, and free scanning software known as Nmap.

Gaining Control

This is the actual stage of the hacking process, during which the information gathered in the previous two phases is used to physically or through the network gain access to the target system and take control of it. This stage is additionally called "Possessing the Framework".

Maintaining Access

After gaining access to the system in the previous step, the hacker keeps that access for future attacks and makes changes to the system to prevent any other security personnel or hackers from entering the compromised system. The situation in which this occurs is referred to as the "Zombie System."

Clearing Logs

It is a method for capturing the hacker by removing any remaining log files or other evidence from the compromised system. There are different devices in the moral hacking strategies from which a programmer can be discovered like entrance testing. In the wake of learning about hacking and the shades of programmers there ought to be some way or some procedure of safeguarding the PC framework or the PC networks structure the noxious programmers, thusly the expressions "Moral Hacking" and "Moral Programmers" came into the business.

Hacking With Ethics

Moral hacking is a part of data security. White Hat Hacking and Penetration Testing are other names for it. It is a kind of hacking that can be done by an individual or a business to help find threats and security holes in the organization's computer system or network. The methods or techniques used in ethical hacking are very similar to those used in malicious hacking, but the difference is that ethical hacking is legal and uses them for good. The information gathered

through ethical hacking is used to keep the security of the system up to date and protect it from future attacks.

Hackers With Morals: -

The "Ethical Hackers" are the White Hat hackers. They are compensated experts. As previously stated, they are experts in computer hacking who identify and address any security issues in a computer system or network before the bad hackers who attempt to break in or commit other malicious acts notice them.

The Code Of Conduct Of An Ethical Hacker

- Before hacking an organization, it is imperative that the data's confidentiality and privacy are established and that no laws or regulations are broken.
- Maintaining open communication with the organization's client or owner both before and after the hacking.
- An ethical hacker's intentions must be crystal clear: not to harm the client or the organization.
- Stick to the boundaries established by the client or the organization; don't go over them.
- Do not share with anyone else the private or confidential information you discovered during the hacking afterward.

Need Of Ethical Hackers In The Industry

Since every organization has its own confidential information that can be hacked by malicious hackers or damaged by them, the organizations' ethical hackers should be allowed to hack their own systems to protect that information. They should also be able to find flaws or loopholes in their systems and fix them before a hacker hacks it. Presently beginning with some hacking assaults performed by the programmers over the web. Before that, you need to be familiar with Linux operating systems and how they are used in hacking attacks.

Linux Working Frameworks

It is an operating system, as indicated by its name, similar to Windows and Mac. An operating system manages all of the computer's hardware resources and serves as an interface between the user and the hardware. A computer operating system (OS) is necessary for the operation of various applications. Linux is an open source operating system because it is distributed under an open source license, in contrast to Microsoft Windows and Mac. There are fewer known viruses

that can harm Linux OS, making it safer than Windows. Ubuntu, Kali Linux, Fedora, Linux Mint, and others are examples of Linux operating systems.

Further in this paper the assaults are performed on the Kali Linux Working Framework. The Linux distribution known as Kali Linux Operating System is primarily utilized for security auditing and penetration testing. Different tools for computer forensics, penetration testing, reverse engineering, and other tasks are included in Kali Linux. Offensive Security is the company that created Kali Linux.

Moving on to the Phishing Attack now: -

Kali Linux must be installed on the system in order to carry out all of these attacks.

Phishing

Phishing is a type of online fraud called a cyber attack in which a hacker tries to get the victim's password, login information, credit card numbers, email address, pin numbers for online banking, etc. Fake emails and websites that look very similar to the originals are used to commit this crime. How to carry out phishing attacks on Kali Linux: -

1 In the Kali Linux terminal, type setoolkit and hit enter.

2. After that press y and enter.

3. Now choose

1. Attacks using social engineering.4. After that, choose option number two.

entry and attack vectors for the website.

5. Now choose the 3. the credential harvester method of attack.

6. Select second2 after this. site replicator.

7. Now that the command needs the IP address, open a new terminal window, type ifconfig, copy the inet address, paste it into the previous window, and hit enter.

8. After that, press enter to type the address of the website you want to copy. The replication of the website will take some time. Open the new terminal window after the process has finished and use the command cd /var/www to navigate to the www directory.

10. Enter ls into the command line after visiting this directory and pressing enter. Enter the following command into the terminal window: cat Harvester_2017-03-20 10:37:25.332885.txt

11. There, you will find a file similar to Harvester_2016-01-01 10:37:25.332885.txt. The victim's email address and password will be displayed after they enter the previous command on the forged or copied website. The Apache2 server must be configured before any of these steps can be carried out. The local computer system or any devices connected via LAN to your computer system are required. The DoS (Denial of Service) attack is now the second type of hacking

Denial Of Services(DoS)

It is a type of cyber attack in which the attacker wants to disrupt the services of a host connected to the internet and make a machine, website, or network resource unavailable to its end users, either temporarily or indefinitely. The attack basically involves overloading the target website, server, or machine with a large number of requests, preventing the target from fulfilling all or most of the requests. Days, weeks, or even months can pass between DoS attacks. The speed at which the attacker sends requests to the target server or website is extremely fast—a few hundred mbps or gbps.

Man In The Middle Attack

In a man in the middle attack, the attacker tries to get in between two parties or devices talking so they can get all the information they've sent and received. Both the sender and the receiver of this attack believe that they are connected through the original connection; however, this is not the case because the attacker establishes a separate connection with both of the victims, gains access to the information that lies in between them, and is able to alter it. The MiTM attack is covered using the Ettercap Tool in this Kali Linux tutorial.

Types Of Cyber Hacker

1. White-hat:

White-hat hackers, also known as ethical hackers, are well-known individuals who always break into security systems with serious intent. The majority of white-hat hackers are security experts who frequently collaborate with businesses to legally identify and address security flaws.

2. **Black-hat:**

The ' dark cap ' programmers, in some cases alluded to as a ' saltine, ' is VIP who hack with pernicious purpose and without consent. The hackers will typically engage in a variety of cybercrimes, including credit card fraud, identity theft, and piracy, in an effort to demonstrate their hacking abilities. A person with extensive computer knowledge who aims to violate or circumvent internet security is known as a black hat hacker[9].

3. Grey-hat:

A "grey-hat" hacker is one who combines the characteristics of both black-hat and white-hat hackers, as the color suggests. For instance, some gray-hat hackers will roam the Internet in search of compromised systems; The targeted company will be aware of any vulnerabilities and will patch them, just like the white-hat hackers, but the black-hat hackers will hack without permission, just like the grey-hat hackers.

4. Blue-hat:

Before a program is released, independent computer security specialists check it for vulnerabilities and identify weak points that can be fixed. Additionally, Microsoft's annual security convention, at which Microsoft engineers and hackers can freely communicate, is associated with blue hat. Blue hat hackers are people who don't work for a computer security consulting firm and test a system before it goes live to find vulnerabilities that can be fixed. The security executive at Microsoft is also a reference to the Blue Hat Hacker's ability to execute arbitrary code in Windows. The word was also linked to Microsoft's annual security convention and the unofficial names of blue-colored badges worn by Microsoft employees[10].

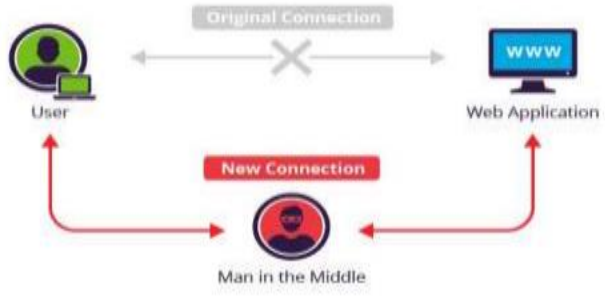
5. **Elite Assassin**

These hackers are known as the "best in the business" and are regarded as experts and innovators. Elite hackers used a new language called "Leets peak" to hide their pages from search engines. A language was one in which a few letters were substituted for one another in words by numbers or other letters that were similar to them. A common term for someone who stealthily gains access to systems and networks in order to make money is the hacker. Some people, on the other hand, practice the inventive art of hacking because the tests they take give them a sense of excitement[11].

Conclusion

The global trend toward technological advancement and the increasingly digitalization of real-world processes raises security risks. As long as the constructor continues to adhere to existing systems architectures that do not meet certain security requirements, the security issues will persist. As long as the delusional outcomes of the intrusion team are recognized as evidence of computer system security, proper security will not be a fact. Neither will funding for ad hoc and security solutions for these inadequate designs. An organization's security effort must include regular monitoring, careful intrusion detection, good systems management practices, and computer security awareness. A single mishap could put a business at risk of cyber vandalism, revenue loss, embarrassment, or worse in any of these settings. Each brand-new technology carries both benefits and risks. While ethical hackers can assist customers in better understanding their security requirements, it is up to customers to maintain their guards. This paper explained how malicious hackers, also known as crackers, attempt to illegally break into security while white hat hackers, also known as ethical hackers, attempt to maintain security. Hacking, like the computer system, deals with the positive and negative aspects of being human. In addition, the various attacks carried out by hackers are described, along with their workings, in this paper. In conclusion, it is necessary to state that ethical hacking is a tool that, when utilized appropriately, can aid in a deeper comprehension of computer systems and the enhancement of security measures.

The methodology or the path followed by the Hackers is as follows



References

[1]. Gupta, A., & Anand, A. (2017). Ethical hacking and hacking attacks. *Int. J. Eng. Comput. Sci*, *6*(6), 2319-7242.

[2]. Abhineet Anand, A. G. (2017). Ethical Hacking and Hacking Attacks. International Journal of Engineering and Computer Science, 6(4).

[3]. Baloch, R. (2017). Ethical hacking and penetration testing guide. Auerbach Publications.

[4]. Pike, R. E. (2013). The "ethics" of teaching ethical hacking. Journal of International Technology and Information Management, 22(4), 4.

[5]. Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017, September). Ethical hacking: The need for cyber security. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 1602-1606). IEEE.

[6]. Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. Solid State Technology, 63(5), 7894-7899.

[7]. Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical hacking: Educating future cybersecurity professionals. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 3857).

[8]. Lorenzini, G., Shaw, D. M., & Elger, B. S. (2022). It takes a pirate to know one: ethical hackers for healthcare cybersecurity. BMC Medical Ethics, 23(1), 1-8.

[9]. Harper, A., Linn, R., Sims, S., Baucom, M., Fernandez, D., Tejeda, H., & Frost, M. (2022). Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

[10]. Onyema, E. M., Dinar, A. E., Ghouali, S., Merabet, B., Merzougui, R., & Feham, M. (2022). Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunications Systems. In Security and Privacy in Cyberspace (pp. 25-45). Springer, Singapore.

[11]. Dhavale, S. V. (2022). Why One Should Learn Ethical Hacking. In Research Anthology on Advancements in Cybersecurity Education (pp. 231-272). IGI Global.

[12]. Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. Education and Information Technologies, 1-25.