IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 6.252

Volume 2, Issue 9, June 2022

Ethical Hacking

Kadambari Nitin Berde
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *We are all aware that the majority of users have access to the information we require online. Some users use this information to learn new things, while others learn how to use it to steal or delete data from websites or databases without the owner's knowledge. Privacy and personal information are frequently violated during the process of hacking. Private information is accessed and vulnerabilities in a system or network are found. This essay outlines ethical hackers' abilities, attitudes, and methods for finding and closing security flaws for their clients. Many of the difficulties and the ethical hacking process are described.*

Keywords: Ethical Hacking.

I. INTRODUCTION

Hackers are one of the darker aspects of computer technology as it develops. Data security is a huge problem in the modern world because of how quickly the internet is expanding and how much data is flowing online. The internet has increased the digitalization of many operations, including banking, online transactions, online money transfers, and the online sending and receiving of many types of data, raising concerns about data security.

Today, numerous businesses, institutions, financial institutions, and websites are the targets of various cyber operations. When we hear the word "hacker," we typically picture evil characters with malicious intentions who are computer gurus who want to steal, leak, or damage someone else's personal or priceless data without that person's knowledge. They are people with extremely high computer skills who attempt to breach another person's security in order to get their personal information, however this rarely happens. To reduce the risk of being hacked by hackers, the industry has ethical hackers, who are also computer specialists but have good intentions or are constrained by a set of rules and regulations by various organisations. These are the people who make an effort to defend internet moving data from various hacker attempts and keep it safe with the owner.

This positive description was frequently extended to the verb form "hacking," which was used to denote quickly creating a new programme or quickly making changes to pre-existing, typically complex software.

Computers are becoming more and more common, but they also continue to be expensive, thus access to them was typically limited. Some users would question the access restrictions that were in place when they were denied access to the machines. By peering over someone's shoulder, they would steal passwords or account numbers. They might even search the system for flaws that would allow them to circumvent the restrictions or perhaps take over the entire system. They would carry out these actions in order to run the programmes of their choice or simply to alter the restrictions placed on how such programmes may operate.

The biggest harm was caused by the theft of computer time at first, when these computer invasions were relatively benign. Sometimes these games would be played as practical jokes. But the innocuous nature of these incursions was short-lived. Sometimes the less skilled or careless intruders might unintentionally crash a system or corrupt its files, forcing the system administrators to restart it or perform repairs. Sometimes these intruders would respond with deliberate acts of destruction when they were denied access once their activities were revealed. Because of the system's visibility or the severity of the damage caused, when the quantity of these harmful computer intrusions became apparent, it became "news," and the media covered the story.

The media started using the term "hacker" to describe people who break into computers for amusement, vengeance, or profit, instead of the more precise term "computer criminal." Computer security experts prefer to refer to hackers who resort to the dark side of hacking as "crackers" or "intruders" because the term "hacker" was originally intended to be a praise. For the remainder of this study, we will refer to both types of hackers explicitly as "ethical hackers" and "criminal hackers."

DOI: 10.48175/568

II. LITERATURE REVIEW

We'll briefly examine the background of hacking to better comprehend the need for preventative actions pertaining to the training of future security professionals. On the campuses of the Massachusetts Institute of Technology (MIT) and Stanford University, hacking first appeared, in large part, in the 1960s. At the time, the term "hack" was used to describe programming workarounds and was seen to be a superior approach to finish tasks quickly. These first "old school hackers" were merely interested in technology, not engaged in committing crimes (Slatalla, 2005). As the Internet has grown and changed over time and become more widely used, hackers' romantic appeal to the general population has diminished (Slatalla, 2005). Older classifications and names, including "script kiddies and coders," still exist even though fresh organisations bearing the moniker "suicide hackers" are starting to appear. The new suicide hackers are thought to be people who carry out attacks to make a statement, but unlike "hacktivists," they do not mask their tracks and are unconcerned if they are discovered (Oriyano, 2014). Recent cybersecurity incidents have been highly unsettling, and they provide proof that the security measures used by today's cybersecurity specialists need to be taken in a more proactive manner. Despite the rise in cybersecurity incidents, there have been a number of well-publicized attacks in the past year that called for highly technical expertise. For instance, the Democratic National Convention hack of 2016–2017 (DNC Hack) greatly heightened concerns about the potential for Russian-sponsored hackers attempting to sway the 2016 Presidential election. Based on their techniques and strategies, the breach believed to have been carried out by two Russian organisations known as Cozy Bear and Fancy Bear (Greene, 2016; van Der Walt, 2017). Many have argued that the main concern at hand does not actually involve the claimed system attack. The results of the suspected Russian hacker's attack led many Americans to lose faith in the American political system (van Der Walt, 2017). Numerous Internet of Things (IoT) devices were impacted by the second significant attack of 2017, known as a Dyn DDoS Attack. The attack was conducted via a "botnet," or network of computers. This form of assault is no longer dependent on traditional computers, as was the case in the past, due to the proliferation of connected gadgets. Another significant attack took place in 2016, when the Equation Group was breached by the Shadow Brokers, who subsequently acquired their tools for exploiting software flaws and essentially gave them online for free (van Der Walt, 2017). Both the Equation Group and the Shadow Brokers are thought to have ties to the NSA and Russia, respectively (National Security Agency). NSA tools were allegedly exposed by Russia, according to some theories, in an effort to humiliate them and undermine American efforts to respond to the alleged DNC attack (Greene, 2016). The NSA Shadow Brokers dump gave hackers access to the tools they needed to target security holes in computer systems all over the world. The greatest ransomware outbreak in history affected almost 100 nations. Cyberattackers gained control of the computers, encrypted the data they contained, and then demanded payment from users of $300 or more to unlock the devices (Scott & Wingfield, 2017). This attack was noteworthy because it is thought to be the first to utilise "a cyberweapon developed by the NSA" and to have been carried out by attackers on a large scale (Scott & Wingfield, 2017). The effectiveness of the attack was especially due to the ability of cybercriminals to target "big organisations with a history of not maintaining their technology systems up to date" (Scott & Wingfield, 2017).

III. CHALLENGES AND RISKS

Professionals earning six figures or more, with access and a genuine position, are considered ethical hackers. Senior corporate directors can choose if such operations should be done by clearly outlining benefits and defects, which can minimise the danger of damage. In advance, ethical hackers could look for vulnerabilities to reduce the danger. The business could run penetration tests to see whether they are open to an attack. However, ethical hackers typically have five days to complete testing, what happens if vulnerabilities are neglected. Finding vulnerabilities for businesses not only helps the organisation but also reduces the risks of assaults. Who may be held accountable for legal actions if a malevolent hacker gains access to the system if an ethical hacker fails to provide the business with the outcomes they were promised and believes the system is secure and free of flaws? The client might inquire, "So, if I address these things I'll have flawless security, right?" in a journal by IBM on ethical hacking, which is surprising. This is not the case, regrettably. The client's systems and networks are operated by people, and people make mistakes. The reliability of information regarding the security state of a client decreases with the passage of timePart of the final report's recommendations for actions the client should keep doing to lessen the impact of these errors going forward are included. [8] If information is inaccurate, there is little chance of ethical hacking occurring in the workplace. What colour is the person's hat, black or white, if a corporation has been ethically hacked? We might question ourselves what the distinctions are from utilising standard security software to accomplish the job for you against giving special privileges to users who then return with inaccurate information as Palmer [6] illustrates. Additional research revealed that properly programming systems at the beginning would enhance security.The main concern would be the cost to both manage and administer to provide great solutions. The idea of self-improving can be another issues, so to whom we can allow these improvements, the company or the ethical hackers to increase their knowledge and thus getting enough information they can get hold of and then launching attacks from different parts of the world as a ethical hacking regime that would build knowledge by posing as ethical hackers and getting information to exploit. Another way to view this is, if legitimate ethical hackers who aim to remedy security issues, whether they should be allowed to access certain information and be entered into security barriers. The best illustration of the need to use tools without hesitation to identify security vulnerabilities is Randal Schwartz, who was sentenced for nothing more than performing his job. In order to do the job we must have some wiggle room and be permitted to use specific tools to assist them with their job. Ethical hackers can spot issues, but to what extent? Even they might not notice a typical virus eating away at data; they might overlook it or let it slide because they only have a short amount of time to perform tests; ethical hackers may also be vigilant of this and compromise the network, leaving it until issues arise, raising the issue of "man on the-moon"attacks.

IV. ETHICAL HACKING

Depending on the purpose behind the hacking process, there are two different forms of hacking. They are black-hat hacking and white-hat hacking. According to CDN, "white-hat hacking" is ethical hacking carried out with the target's consent to identify a system's vulnerability from a hacker's perspective. Such hacking is done to protect the system against black-hat hackers who are out to steal and exploit personal information. For both kinds of hacking procedures, the same tools and techniques are utilised to compromise the system. Black-hat and white-hat hackers have similar thought processes. The idea or reason for hacking any system differs between these two groups. An individual is considered an ethical hacker if their goal is to reduce security risks and stabilise corporate systems. But harmful hackers who want to steal people's personal information and invade their privacy are not regarded as ethical hackers. Given that it is carried out with the target's permission, ethical hacking is legal. The claim of numerous suppliers on the security of their goods is confirmed, in CDN's opinion, by the ethical hacking procedure. The value of ethical hacking is immeasurable since it can be used to defend critical accounts, networks, and systems against data thieves by adopting their way of thinking. It respects privacy, gives the information owner complete control, finds system weaknesses, fortifies computer security, and prevents system attacks. There is a critical need for ethical hacking given the development of technical systems and the quickly moving technology-oriented future.

Computer security is becoming a top priority for both corporations and governments due to the Internet's expansion. They want to be able to use the Internet for things like electronic commerce, advertising, information access, and other purposes, yet they are concerned about the prospect of being "hacked." The potential users of these services are concerned about keeping control of personal data, which might include everything from credit card details to social security numbers and home addresses.

In their search for a solution, corporations discovered that sending independent computer security experts to try and break into their computer systems was one of the best methods to assess the potential of intrusion to their interests. This plan is comparable to having external auditors examine an organization's books and records. These "tiger squads" or "ethical hackers" would use the same tools and techniques as the invaders in the context of computer security, but they wouldn't harm the target systems or steal any data. Instead, they would assess the security of the target systems, find any flaws, and then report back to the owners with recommendations on how to fix them.

This way of assessing a system's security has been in use since the invention of computers. The United States Air Force performed a "security review" of the Multics operating systems in an early ethical hack in order to assess their "possible usage as a two-level (secret/top secret) system." Multics was "much better than other typical systems," but it also featured "... weaknesses in hardware security, software security, and procedural security" that could be detected with "a reasonably modest degree of effort," according to their analysis. In order for their tests to realistically reflect the types of access that an intrusive party could possibly obtain, the authors conducted them in accordance with a realistic standard. They carried out tests that were straightforward exercises in information collection as well as other tests that were direct attacks on the system that would jeopardise its integrity. The audience was obviously interested in both outcomes.

With the expansion of computer networking, and the Internet in particular, the idea of utilising hacker techniques to evaluate the security of a system has probably become more widely accepted for the first time. It then went on to explain how to obtain enough data on its targets to have been able to break security if they had decided to do so, with the aim of increasing the degree of security on the Internet and intranets. There are various concrete instances of how this data could be obtained, how it could be used to control the victim, and how such an attack could be stopped.

V. ETHICAL HACKERS

A number of abilities are required for ethical hacking success. They must, first and foremost, be fully trustworthy. An ethical hacker could come upon information about a client when assessing the security of their systems that ought to be kept private. In many instances, if this information were made public, actual hackers could enter the networks and cause losses. As the "keys to the corporation" during an examination, the ethical hacker must be trusted to maintain strict control over everything. any details concerning a target that might be abused. Because the information gathered during an evaluation is sensitive, strong precautions must be taken to ensure the security of the systems being used by the ethical hackers themselves. These precautions include isolated networks for testing, multiple secure Internet connections, limited-access labs with physical security protection and full ceiling-to-floor walls, a safe to hold client paper documentation, and strong cryptography.

Since they have been working in the computer and networking industries for a while, ethical hackers often possess very good programming and computer networking skills. They are also skilled at setting up and maintaining systems that use the most well-liked operating systems used on target systems (for example, UNIX or Windows NT). Detailed understanding of the hardware and software offered by the more well-known computer and networking gear providers is added to these foundational skills. As excellent abilities in the other fields suggest, a very solid awareness of how the security on various systems is maintained, it should be highlighted that an additional expertise in security is not always required. These systems management abilities are essential for the vulnerability testing itself, but they are crucial for writing the report for the client after the test as well. Finally, qualified applicants for ethical hacking are more motivated and persistent than the majority of people. The work that ethical hackers undertake takes a lot of effort and perseverance, unlike how someone breaks into a computer in a movie. This is a crucial quality since malicious hackers are known for their extraordinary patience and willingness to watch systems for days or even weeks while they wait for an opening. An average examination could take many days of painstaking work that is challenging to automate. In order to imitate the time of an actual attack or avoid interfering with production at "live" targets, some evaluations must be completed outside of regular business hours. Ethical hackers will take the time to research a system before coming across it in order to attempt and identify any holes.

The clients themselves requested that such a restriction be observed, which makes keeping up with the rapidly evolving computer industry justifiable at the time the service was first made available. Numerous ex-hackers have transitioned into security consultants and media spokespersons since IBM's ethical hacking squad was established. Even though they could have truly turned away from the "evil side," there will always be room for uncertainty.

Your success depends heavily on your opponent's tactics. The task of an ethical hacker is more difficult in the field of computer security. When it comes to classic crime, anyone may become a mugger, a graffiti artist, or a shoplifter. Typically, their potential victims are localised and simple to identify. The local law enforcement officials must be aware of the criminals' methods of operation and how to stop them. Anyone can access the Internet and download malicious hacker tools to try and get into computers anywhere in the world. Hackers who adhere to ethical standards must be aware of criminal hackers' methods as well as ways to detect and thwart them.

How does one go about locating people who meet these requirements, given these qualifications? The top candidates for ethical hacker positions will have had success with academic publications or the public release of widely used open-source security programmes. Since its work is so important, the computer security community strongly self-polices. Most ethical hackers and many of the top specialists in computer and network security did not want to concentrate on these problems. The majority of them were computer users who came from a variety of academic backgrounds, including astronomy and physics, mathematics, computer science, philosophy, or the liberal arts, and who took it personally when someone interfered with their work with a hack.

VI. ETHICAL HACKING EDUCATION

The discussion will now present a summary of ethical hacking education to prepare upcoming security professionals after the definition of ethical hacking has been completed. Most experts concur that it is essential for security professionals to teach students how to hack ethically. This may be considered as a worthwhile activity. According to Pashel (2006), security experts can better avoid assaults if they are able to identify the holes in computer systems. He continues by suggesting that ethical hacking might be viewed as a critical component of a security effort (Pashel, 2006). The need of computer administrators having equivalent knowledge and abilities to attackers is being recognised by an increasing number of studies. To help students receive the proper education, it is crucial to identify the skill sets required of security professionals (Logan, & Clarkson, 2005). The researcher goes on to say that the "good guys" need all the information and assistance they can obtain given how quickly the field of information security is evolving (Greene, 2004). Numerous ethical hacking techniques can be seen as more proactive than reactive in nature. According to security educators, training "offensive approaches" rather than "defensive techniques" results in security professionals who are better equipped (Trabelsi, 2011). Researches and educators from various fields concur that practising ethical hacking techniques is essential for building the skill sets required of computer security experts. According to Trabelsi (2011), students should receive training to get them ready for career-long research and development. Continuing, he asserts, "One cannot flawlessly plan or construct defences for attacks that one has not genuinely experienced, first-hand" (Trabelsi, 2011). Trabelsi (2012) makes the claim in a different study that computer security professionals are not well equipped for their careers since they are not given information and knowledge gained via hacking. He goes on to say that educating about assaults is thought of as a crucial component of security education. An ethical hacking curriculum overview is suggested in the 2013 book Hands-On Ethical Hacking and Network Defense. The author argues for the need to define the precise role of penetration testers, offers various penetration testing models, examines what is permissible and what is not, distinguishes between federal and state regulations using case study analysis, and looks at various ethical hacking certifications (Simpson, et al., 2013In order to effectively prepare security experts, Trabelsi and Alketbi (2013) assert that a curriculum should contain ethical hacking approaches.

Conducting code of an Ethical Hacker:

- Before hacking into any organization's data, identifying and determining its secrecy and privacy, and ensuring that it's not breaking any rules or regulations.
- Keeping the customer or organization's owner informed both before and after the hack.
- An ethical hacker's intentions must be crystal apparent, i.e., they have not do harm to the customer or organisation.
- Stay within the parameters established by the client or the organisation; don't re-evaluate them.
- Following the hacking, refrain from sharing any private or personal information discovered during the hack with others.

VII. TOOLS AND TECHNOLOGY

The correct tools are necessary for the process of hacking, just as every process needs a few specialised tools and approaches to complete the work. When using ethical hacking techniques, it's critical to understand your own technical and human constraints, claims CDN. It is unlikely that utilising the appropriate tools will find every potential vulnerability in the system because every piece of equipment has little flaws. However, the likelihood of greater outcomes inaccuracy decreases as more tools are utilised in the hacking process. A hacker should be knowledgeable about HTTP, HTTPS, and other network protocols, authentication techniques, network and firewall architectures, port information, web applications, web server configurations, database setups, and programming languages like HTML, Ruby, Python, and JavaScript, among other things (Babbar, Jain and Kang). With the use of these abilities and expertise, a hacker may easily comprehend the majority of the networks and systems they are targeting. These are the fundamental skills that hackers acquire in order to comprehend their targets and act with the utmost professionalism when carrying out hacking operations.

DOI: 10.48175/568

The hacking process cannot be completed with just system and network expertise. To accurately do ethical hacking, specialised tools and software programmes are available. They make the hacking process simpler and are practical for new hackers to employ. These include application and port scanners, packet sniffers, password crackers, vulnerability scanners, hacking hardware, and password crackers. LANguard Scanner for Network Security, Internet Scanner, Nessus, Kismet, Nikto, QualysGuard, Ether Peek WebInspect, Ethereal, ToneLoc, LC4, and other commercial and open-source ethical hacking tools are also used by CDN. Professional ethical hackers can purchase these tools and equipment from commercial sources. They also include a guide for added convenience.

VIII. INFLUENCE ON BUSINESS

Finding network vulnerabilities and system weaknesses is made simple with the help of ethical hacking. Ethical hacking may defend any company, product, or person against those who wish to do them damage because it is done with positive and beneficial motives. Numerous organisations have experienced loss throughout the years as a result of the theft of their priceless data. Due to lax safety protocols, others have lost the patronage of their clients. Businesses and organisations have begun using ethical hackers to monitor network security and minimise potential vulnerabilities in order to avoid these negative effects (Munjal 922-931). To find system faults and fix them to maximise system security, computer security organisations, mobile service providers, and even network providers have invested in ethical hackers. Today's world is experiencing significant advancements in information technology, and all of the data available is stored as computer programmes, bytes, and electrical digits. To maximise the longevity and use of electronic devices, this data demands safety. Many websites and electronic markets promote online buying as an alternative to traditional brick-and-mortar stores. Since so many people give up personal information, like addresses and bank account numbers, there is a risk if ethical hackers are not used (Munjal 922-931).

Customers and the general public can use the internet safely thanks to ethical hackers' trustworthy nature. It can be quite beneficial for a company's business if they are able to win over their audience's trust.

In order to reduce cybercrime and foster a society free from crime, ethical hackers are essential. It's possible that people haven't yet learned about the benefits of ethical hacking. We spoke with a few businesses to show that not all employ ethical hackers, despite being aware of their benefits (Marsh). A greater level of awareness is required to enable businesses to secure their products and be more receptive to ethical hacking.. By hiring ethical hackers, it will be simpler to combat cybertheft and black-hat hackers because they are skilled at thwarting both types of hackers. It is crucial to highlight these experts' significance in contemporary culture because they are the only ones capable of thinking and acting like hostile hackers.

IX. CONCLUSION

A system or network can be modified by hackers by finding weaknesses and vulnerabilities and exploiting them. White-hat and black-hat hackers, who are only distinguished by their motivations for hacking, are divided into two groups. In the eyes of the general public, ethical hackers and white-hat hackers are just regular hackers with bad intents. To stop products from having their security compromised, ethical hackers must be made more widely known. Trustworthy and driven by noble goals, ethical hackers hack only for good. They are hired by organisations as trained specialists to maintain their security, which makes them crucial to society and industry. Each hacker has their own set of tools and techniques that they use to complete the hacking process. As a result, every hacker has the same mentality and cognitive ability. To successfully hack a target, you must go through five phases. Security dangers would decrease if today's society and corporations began hiring reputable hackers.

As people, businesses, and societies become increasingly proficient with and dependent upon computers, the likelihood of fraud or other criminal activity increases. Teaching students ethical hacking techniques and concepts can equip them with the knowledge and abilities to address and create certain security policies and procedures as well as to provide the administrative support that may be needed to combat cybercrimes. The implementation of a security operation's specifics, which will involve both defensive and offensive activity, requires technical knowledge. Students must learn how to conduct job duties that are focused on defending the information system of the company or the personal information of the individual from attacks.

REFERENCES

[1]. Bansal, M. Arora, and (2012). Hacking ethics and social security. International Journal of Social Science Research: Radix, 1(11), 1–16.

[2]. Paper hacking by Deepak Kumar, Ankit Agarwal, and Abhishek Bhardwaj is available online at http://www.ijcstjournal.org/volume-2/issue-6/IJCST-V2I6P2.pdf.

[3]. http://www.ijecs.in/issue/v4-i4/68 percent 20ijecs.pdf is a study by Bhawana Sahare, Ankit Naik, and Shashikala Khandey titled "Study on Ethical Hacking."

[4]. Kevin Beaver, CISSP, is the author of "Hacking for Dummies" (Information Security Consultant).

[5]. http://www.speedguide.net/faq/what-is-the-typical-range-of-a-wireless-lan-330

[6]. S. Bratus, A. Shubina, & M. Locasto (2010).

[7]. Undergraduates are being taught the hacker curriculum's fundamentals. Proceedings of the 2010 SIGCSE, the 41st ACM Technical Symposium on Computer Science Education

[8]. S. Bratus, C. Masone, and (2007). How Can We Use the Hacker Curriculum in Teaching? doi:10.1109/mdso.2007.61, 8(11), IEEE Distributed Systems Online.

[9]. The authors are Dimkov, Pieters, and Hartel (2011). An assignment in computer security education that involves actually teaching pupils how to steal.

DOI: 10.48175/568