DOI: https://doi.org/10.51846/vol5iss4pp29-35 **Pakistan Journal of Engineering and Technology, PakJET**
ISSN (p): 2664-2042, ISSN (e): 2664-2050
Volume: 5, Number: 4, Pages: 29- 35, Year: 2022

The Impacts of Ethical Hacking and its Security Mechanisms

Hafiz Burhan Ul Haq[1], Muhammad Zulkifl Hassan[2], Muhammad Zunnurain Hussain[3], Rabia Aslam Khan[1], Sabreena Nawaz[1], Hassan Raza Khokhar[1] and Mahnoor Arshad[1]

[1]Department of Information Technology, Faculty of Computer Sciences, Lahore Garrison University, Lahore Pakistan
[2]Department of Computer Sciences, Faculty of Computer Science and Information Technology, University of Central Punjab, Lahore, Pakistan
[3]Department of Computer Science Bahria University Lahore Campus, Lahore, Pakistan

Corresponding author: Hafiz Burhan Ul Haq (email: burhanhashmi64@lgu.edu.pk).
Received: 07-08-2022 Revised: 18-11-2022 Accepted: 16-2022

Abstract- **Hacking is a typical method for breaching personal and confidential information. As a result, hacking is also known as infiltration. Intrusions, on the other hand, were not always recognized as theft and were employed for productive purposes. A person or corporation that does ethical hacking and receives incentives from a network or system owner for testing can enter an apparatus (system or network) to locate, repair, and expose network flaws. Most ethical hackers, also known as black hat hackers, test systems using different approaches, methodologies, and tools. Because today's life is lived in a digital world, we need to protect our privacy from cyber-attacks. The proposed paper discussed ethical hacking and its ramifications, in which black hackers "hack" networks. The proposed research emphasizes ethical hacking tactics. This research also examines the impact of ethical hacking on business, education, health, society, the workplace, technology, sensitive information, and human life. Finally, a brief survey based on certain questions is better to grasp the public's understanding of ethical hacking. In summary, this research offers the user fascinating and helpful information when working on ethical hacking.**

***Index Terms*--** **Ethical Hacking, Unauthorized, Security, Penetration testing.**

I. INTRODUCTION

Ethical hacking validates the security of networks and systems [1]. The central mission of ethical hackers is to protect your data from unethical hackers. The ethical hacker uses the same methods as black-hat hackers, except with network administrator privileges. We must protect our data in today's evolving digital world, where biometric signatures are also digitized. Imagine hackers having stolen data and biometrics and causing financial and moral harm. Different companies pay millions to ethical hackers. Various companies lose billions of dollars annually after these payments due to these hacking activities [2]. Hacking can be defined as unauthorized or privileged access to a system, using software and computer technology to discover system threats and penetrate the system [3] introduces students to 4,444 modern defence mechanisms built on the organization's assets. Determine the tools and mechanisms needed to maintain the support and infrastructure of various organizations. These include processes, protocols, laws, employees, partnerships, and more required to house assets and your organization's infrastructure. Determine the hardware, machine, operating system, and software requirements for every test.

Similarly, defining and implementing in real-world scenarios that model an organization's assets and the protections for those assets for testing, and also determining the limits of those protections. Furthermore, identifying the data and results obtained from the test. It is also verified that the security check result complies with the interaction rules and does not give false results related to the impact of ethical hacking.

•The goal of ethical hacking.
•The legal implications of using ethical hacks outside the deployed environment.
•Use ethical hacking as a defence process.
•The handiness of the exercises and their ease of implementation.
•The use of practical exercises outside the laboratory.
•Build their practice exercises [4].
•The main reason for ethical hacking is to assess the target system's security, system infrastructure, or network and identify weaknesses. This process finds and exploits the vulnerability and determines whether it can be accessed by unauthorized persons or other malicious activity.

This paper highlights the hacking comprehensively by elaborating on its history or background. Furthermore, types of hackers, which include black, gray, and white hat hackers, are elaborated to show how these terms are different in terms of working and understanding. Similarly, ethical hacking methods and five main phases are also discussed. After that, the impact

of ethical hacking on business, education, health, society, the workplace, technology, sensitive information, and human life is described, which indicates how the hacking occurred in the fields above. Finally, a survey is conducted based on several questions that show the level of awareness among the people.

II. TOP 10 COUNTRIES WHERE HACKERS COME FROM OVER THE YEARS

This data is difficult to obtain. The estimates below are estimates and should be treated as such. Table 1 shows the field's evolution by showing data for 2013, 2016, and 2019 and a prediction for 2022. According to the above figure, China still has a major influx of hackers. Another reason these figures are estimates is because they are based on logged traffic and do not necessarily include activity on the dark web. But in general, ratings reflect well on what's going on.

TABLE I
TOP 10 COUNTRIES WHERE HACKERS COME FROM OVER THE YEARS [5]

2013	2016	2019	2022(Prediction)
China-Approx. 41.4%	**China – 27.24%**	**China**	**China – 41%**
USA - 10%	USA – 17.12%	Brazil – 14.2%	USA – 10%
Turkey – 4.8%	Turkey – 10.24%	Russia – 4.1%	Turkey – 4.5%
Russia – 4.4%	Brazil – 8.6%	Poland – 5%	Russia – 4.1%
Taiwan – 3.8%	South Korea – 7.47%	–	–
Brazil – 3.4%	India – 6.67%	–	–
Romania – 3.4%	Spain – 6.32%	–	India – 2.3%
India – 2.3%	Thailand – 5.85%	–	Italy – 1.4%
Italy – 1.6%	Japan – 5.55%	–	Taiwan – 3.7%
Hungary – 1.4%	Russia – 5.14%	–	South Korea – 1.4%

III. HISTORY OF ETHICAL HACKING

The First Internet Security Hacker: The first hacker to get media attention was Robert Tappan Morris in 1989 [6]. He launched the first denial of service (DoS) worm attack developed by Morris at Cornell University a year ago. He was working on a digital version of a nuclear weapon. Robert said he didn't intend to do any harm, but he wanted to highlight a security flaw. Unfortunately, a bug in the code caused the worm to replicate so many times that it caused serious damage that lasted several days. The history of hacking leads us to how ethical hacking got started. This means that the history of ethical hacking precedes the history of general hacking. To get a clear picture of this, we must delve into it [7]. The past shows that being a hacker is not necessarily a bad thing. In fact, according to history, the term "MIT" first appeared in the modern context of the famous institute, the Massachusetts Institute of Technology (MIT). The term "ethical hacking" was first used by Vice President John Patrick of IBM in 1995. However, this concept spread for a long time.

In the 1960s, "hacking" was a term used by engineering students to find various ways of optimizing systems to make them more efficient. History tells us that hacking was a creative activity done by the world's smartest people. In the 1990s, when the use of the Internet spread around the world, the number of hackers surged. Personal computers gained immense popularity in the 1980s and 1990s. Many personal data and other sensitive records are stored in computer programs. This sparked the minds of hackers trying to access these systems [8]. After that, this information was sold for a great profit. Hackers were considered people who were trapped in a room all day and continued to program for hours. In the 1960s, when this was the most popular phone, no one seemed to care about hackers. Instead, most people didn't know what a hack was. Hacking has attracted media attention, but it's not positive. Hackers have been viewed as criminals (cyber criminals) who use their expertise to access private systems, steal data, and even provide substantial sums of money to blackmail companies. A hacker of this type is now known as a black hat hacker [9], and Fig. 1 depicts the hacking journey.

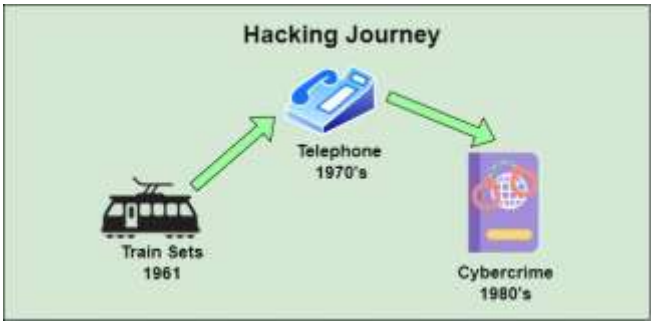

FIGURE 1. Hacking Journey

IV. HACKING DIDN'T START WITH A COMPUTER

In 1961, MIT researchers hacked a toy train to change its functionality. This was the beginning of the hack! It wasn't until later that they started hacking very expensive mainframes. There

was no internet hacking in the 1970s, and computers were used only by huge government companies and agencies. Phone services were so expensive that hackers targeted the phone system to take advantage of free calls. Computers became popular in the 1980s. The Internet was primarily used for research and defense, but as it became more widespread, so did cybercrime. The government started with measures and laws such as the US Computer Crime Control Act. The law banned access to unauthorized computers and made hacking a serious crime [10]. In the 1990s, the use of the Internet became more common. As more and more people started using the Internet, so did criminal activity.

Hackers like Kevin Mitnick and Robert Morris have been arrested for crimes such as hacking computer systems and stealing their code. As the Internet continued to expand in the 2000s, major media platforms, e-commerce, and different search engines were attacked. Even the International Space Station (ISS) has been compromised. After all, companies are worried about protecting their systems from hacking. They started hiring ethical hackers and became good guys fighting villains [10]. Many of the legendary hackers for good began as malicious actors and were imprisoned. When they got out of jail, they started using their hacking skills to protect the system instead of hacking it. Your efforts have made the cyberworld a better place for everyone. [10]. The hacking term comes from the old spaghetti western, where the bad guy wore a black cowboy hat and the good guy wore a white hat. Figure 2 demonstrates the various types of hackers.

FIGURE 2. Types of Hackers

White Hat Hackers use their power for good rather than bad. White hackers are also "ethical hackers," who may pay employees and contractors who work as security specialists in companies seeking to find holes through hacking. White hat hackers use the hacking method first with the system owner's permission. Doing so makes the process completely legal. You are working for a conscientious purpose.

On the other hand, black hat hackers are unethical hackers who use hacking methods for fraudulent purposes. This hack is illegal and is used maliciously for personal gain [11]. Grey hat hackers are a mixture of the first two, ethical and unethical. They usually work at the national level for security.

V. BECOME AN ETHICAL HACKER

To dispose of cybercrime, protecting yourself from ethical hacking is required. Ethical hackers always gain access to the system by asking permission from the user or organization to find weaknesses in the system and improve its security of the system. It then finds loopholes in the system and helps the organization solve them [13].

VI. Certified Ethical Hacker

Professionally certified ethical hackers are professionals in the hacking field. They perform the duties of a black box hacker and a white box hacker. The International E-Commerce Commission issues these certificates or licenses.

FIGURE 3. Security Life Cycle

VII. Ethical hacking method

Figure 3 shows five different phases of ethical hacking. However, the elaboration of each phase is discussed below:

A. PHASE 1 - RECONNAISSANCE

A collection of technologies such as fingerprinting, scanning, enumeration, and processes is used to discover and find information about the system's target. Ethical hackers try to gather information about a system's target during reconnaissance. Following the 7-step process related to reconnaissance:

a) GATHERING INFORMATION

The idea here is to collect information about an interesting, new, and important goal. To this end, hackers use many tools to block planned attacks. Once you've decided on the destination IP address to determine network coverage, it's time to define the network range. It is important to verify and know the maximum possible number of networks that will provide a clear plan and hacking matrix.

b) DETERMINING THE NETWORK RANGE

Once you've decided on the destination IP address, it's time to define the network range. Knowing the maximum number of networks will provide a clear plan, and the hacking matrix is important.

c) IDENTIFYING THE ACTIVE MACHINE

It would help if you found active machines in the target range of your network. This is an easy way to ping the target network.

Proper examples must be followed to complete the process to avoid being intercepted or rejected by the host.

d) FIND PORTS THAT ARE OPEN AND ACCESSIBLE

After determining the scope of the network and active machines, the ethical hacker goes through a port scanning process to get open TCP and UDP access ports

e) OS FINGERPRINTING

The process by which the hacker finds out the target device on which the OS is currently working. Thus, it is the phenomenon of calculating and exerting influence on a remote host ID running on the operating system. This is carried out by sending mainly crafted packets to a goal system, after which they note down their response. It is analyzed by collecting the facts to determine the goal by OS.

f) MAPPING THE NETWORK

The Study of the Network on Physical Connectivity As an ethical hacker, network mapping discovers devices and connectivity on your network. These devices should be comfortable with network discovery or enumeration, which leads to attribute discovery [14].

B. PHASE 2 - SCANNING

Using this technique, intrusion testers can easily identify open doors in any network. At this stage, the hacker creates an overview of the targeted network. The overview includes the destination network for the IP address and other services running on that system.

There are three types of scans:

- Port Scan
- Network scan
- Vulnerability scan

These steps need to be followed when running a scan:

- Which server is running?
- Specific IP address.
- Operating system
- System architecture
- Individual services are run systemically

a) PORT SCAN

In this scan, the target system is scanned for information such as open ports, active systems, and different services that are running on the host.

b) VULNERABILITY SCAN

Check targets for vulnerabilities. Automated tools usually do this.

c) NETWORK MAPPING

Searches the topology of networks, routers, firewalls, servers (if any), and host information and creates a network diagram with the available information [15].

C. PHASE 3 - GAINING ACCESS

This is the most critical step for an attacker to get your system or network access and destroy your system, also known as "system ownership," in the world of hacking. This means that the hacker has the full approach to fixing the system. Hackers can use a unique application or tool known as "zombies" to spread and damage many computers.

D. PHASE 4 -MAINTAINING ACCESS

After a hacker gains access, it is too easy to utilize and exploit all resources and the system itself. They can turn this system into a lunch pad, scanning and destroying other systems. This means that the entire organization can be abused. Hackers use backdoors or Trojan horses to access the system.

E. PHASE 5 -CLEARING TASK

The thief doesn't want to be caught. Intelligent hackers always remove all evidence, so there is no evidence leading to him at a later point. This includes changing / corrupting/deleting log values, changing registry values, uninstalling applications, and deleting created folders.

VIII. IMPACT ON SOCIETY OF ETHICAL HACKING

Hackers or attackers have a large impact on society. Ethical hacking is not bad, but you need to know what ethical hackers are doing in society. There are many areas in which information technology is involved. Ethical hackers have a big impact. Today, the whole world is in the circle of information technology, and we can't do that either. Just imagine a life without the Internet. The Internet today is a link for mobile devices to access the world. As a result, hackers attacked the world [10].

IX. IMPACT OF ETHICAL HACKING ON EDUCATION

The teaching of hacking to students is a difficult process. Students are always interested in and ready to learn about new technologies. Whenever any teacher teaches any hack, he can ensure that the student understands the concept. Students must try to hack other devices or use them to do bad things. In classes, 95% of students can take lessons well, while the remaining 5% can be malicious. "A huge problem for students trying to teach this approach is that teachers provide students with effectively loaded weapons" [14].

The main issue is that students don't know what hacking is or what it means, but they try to hack. This can be good or bad. Currently, the number of participants in safety courses is on the rise. It would be best if you learned how to hack easily and then profit from it. They are fascinated by new hacker technologies that can hack into computers and other devices. If ethics are not included, we need to clarify to them that ethical hacking is bad. You can run workshops, seminars, and awareness programs to get them on the right track.

X. IMPACT OF ETHICAL HACKING ON BUSINESS

Today, people in business use a lot of IT-based software. All our data is digitized, as we live in a digital world. In the end, the entire transaction is now processed. The growth and accessibility of the Internet have encouraged people to make digital transactions. As a result, the percentage of customers using e-commerce sites is increasing. It is very easy for ethical hackers to buy products from these sites.

On the one hand, he can hack websites to buy products or hack other people's accounts and use them for payments. There are good, ethical programmers who do the right thing. However, they

can use their talents with malicious intent. They can attack businessmen and businesses [14]. Business is the lifeline of all economies. Every company, from Fortune 500 to local start-ups, strives to be more productive and successful. Many companies use cloud computing and other software to perform basic operations related to analytics, marketing, finance, and more. If any of these software programs were hacked, all companies (that is, users) would be at great risk. In addition, many companies are exposed to cyber threats due to poor password practices, poor network protection, and other reasons. Without ethical hackers, businesses continue to be exposed to the constant risk of cyber-attacks and cannot optimally produce and operate.

Ethical hacking provides an easy way to detect vulnerabilities in a system. Many businesses have suffered losses due to theft, and their valuable information has been lost. Others lost customer trust due to security vulnerability measurement. To avoid these consequences, companies and organizations hire ethical hackers to monitor network security and reduce potential vulnerabilities. These include computer security companies, mobile companies, and network providers. Ethical hacking experts update your system and maximize your system's safety. Information technology is rapidly advancing in modern society, and all available data is computer programs, bytes, and electronic numbers. This data needs security to increase service life and the use of electronic systems. Numerous websites and electronic marketplaces get customers online. Too many people, instead of shopping in brick-and-mortar stores. We provide the following personal information: address and bank account details; risk without the services of an ethical hacker's reliable nature.

Ethical hackers can provide a secure email environment for clients and others. If the business can win the audience's trust, it can be very beneficial. Ethical hackers play a major role in reducing cybercrime in society. Create a crime-free environment. The advantages of an ethical hacker are not yet known to the public. Some company interviews prove that not all companies use the services of ethical hackers and make a profit. Awareness is required to allow businesses to be more open to ethical hacking and product security. Ethical hackers are skilled cyber thieves. And black hat hackers, and take them over. It would be easier for the service to handle them. Only these experts can think and act like malicious hackers. It is important to promote the importance of this social [11].

XI. IMPACT ON THE WORKPLACE AND ITS SAFETY

Most companies today store their data in digital form. Therefore, ethical hackers can hack data and use it for their purposes. Hackers can access information about the employees of a company. Hackers can attack a company's server to get access to all its data. They use various virus codes for this purpose. To eliminate hacking, you must improve the security of your operating system. This target is achieved by finding the information that hackers use to hack the system and fixing these vulnerabilities to enhance security. Hackers can attack company servers and extract large amounts of data. However, businesses now have several mechanisms to deter ethical hackers [14].

XII. IMPACT ON TECHNOLOGY

Few things are safe and reliable in today's world. Almost all the information is at your fingertips. Anyone can easily get information about any system. This makes it easier for ethical hackers to obtain and attack your system's IP address. There are several tools that ethical hackers can use to get their job done easily. The most commonly used tool is Nmap, which helps ethical hackers find open ports on other systems. The other is Acunetix, which is used to find vulnerabilities. Both tools are used without prejudice by ethical hackers. Hackers can use them to commit crimes, but ethical hackers use them to find weaknesses and flaws in network security.

New technologies are not without loopholes and errors. Without the efforts of ethical hackers, these technologies are not feasible and secure for the masses. Take Amazon's Ring video doorbell as an example. Over the past year, various users of this Amazon product have seen cases where hackers use video doorbells to spy on them and their families. Many of these technologies on the market are full of errors that cause customers to hesitate to buy them. Therefore, there is no doubt that ethical hackers will play a major role in making new software, hardware, and applications safer, more reliable, and more widely accepted.

XIII. IMPACT ON SENSITIVE INFORMATION

Today, sensitive information in society is by no means secure in the presence of hackers. A large number of ethical hackers work at multiple institutions where financial transactions take place. Therefore, hackers can access important data about the account's owner. Hackers can use this data to make trades or steal money from the account holder. Hackers primarily use phishing emails and advertisements to gain access to their accounts. There is a huge issue with ethical hackers following the overviews. Hacking differs from ethical hacking. However, due to all the means of entry available to ethical hackers, they may also enter this circle. Also, it can be very difficult for an ethical hacker to prove that he is a legal hacker, i.e., if an ethical hacker is hired to investigate a weakness in a sensitive information system and data leaks from the system a few days later, everyone blames the ethical hacker and turns him into an unethical hacker, which is known as a "Black Hat hacker." Confidential data such as military and personal information (PII) remains at the highest risk of being hacked. Numerous incidents of hackers hacking sensitive data, government-sponsored cyber spying, and criminal hackers leaking or stealing sensitive information have threatened society's structure. Ethical hackers use their expertise to provide digital security and data privacy for such databases and organizations.

XIV. IMPACT OF ETHICAL HACKING ON INDIVIDUALS IN SUPPORTING THEIR SAFE AND COMFORTABLE LIVES

Finally, ethical hackers indirectly affect each of us. We all use different gadgets and apps to make our lives more convenient. By making these gadgets safe, ethical hackers also protect our lives, i.e., Alexa, Google Home, and other voice support devices are installed in millions of homes. Thanks to these professionals and

their ethical hacking training, we can all sleep at night without fear of someone spying on us. In short, ethical hackers benefit society and positively affect everyone in the information age. Ethical hackers are cyber-world defenders if ethical hacking is an antidote to criminal hacking (see Fig. 4).

Furthermore, a survey shown in Fig. 5 was conducted among people of different ages and categories, such as students, instructors, employed personals, private-sector workers, armed forces personnel, etc. The following results were concluded for a few questions: The survey identifies that most are unaware of what is happening, but they want to be one of those people. Table II shows the questionnaires:

TABLE II
SURVEY CENSUS

	Questionaries'	YES	NO
1.	Do people suffer from hacking?	8	36
2.	Do people want to become and work ethically as hackers?	25	19
3.	Do people have any knowledge of hacking and penetration testing?	9	35
4.	Has anyone ever worked as a hacker or had any experience with hacking (i.e., Penetration Testing)?	6	38
5.	Do people suffer from hacking?	8	36

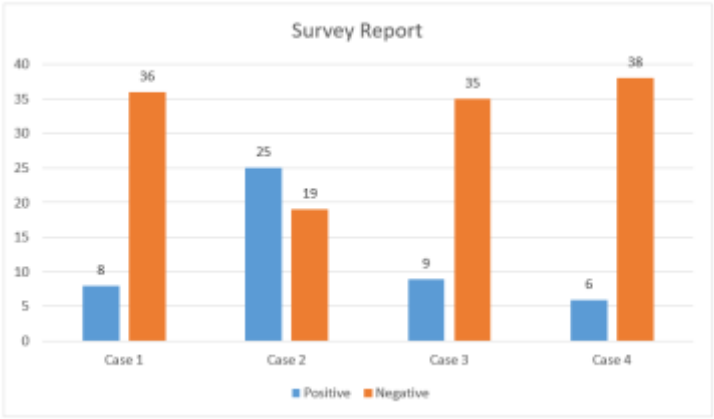

FIGURE 4. Survey Census Report

XV. CONCLUSION

This research elaborates on the implications of ethical hacking—its types, phases, methods, and implications. Hackers discover flaws and vulnerabilities in systems or change depending on your network requirements. The researchers also conducted a survey indicating that most users were unaware of ethical hacking. So, hackers need to be raised ethically to avoid product security breaches. Most information technology organizations conduct ethical hacking of wireless and wired networks, operating systems, and applications frequently used on frequent routes or in annual searches. There is no single unique set of methodologies leading to ethical hacking.

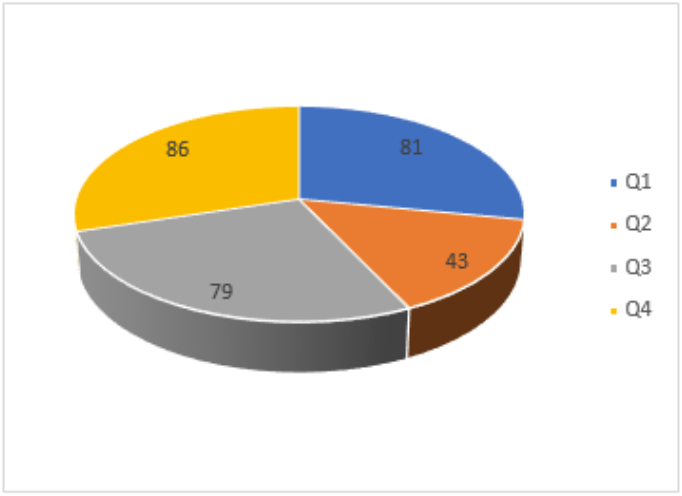

FIGURE 5. Survey Analysis Report

FUNDING STATEMENT

The authors declare they have no conflicts of interest to report regarding the present study.

CONFLICT OF INTEREST

The Authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] D. Rajesh,V. Totakura V., B.A Goud and M. I. T. Hassan- "Concepts of Ethical Hacking: A Survey" April 2020 pp. 1279-1280.

[2] C. Nagadeepa, R. Mohan, and A. Singh, "Ethical Hacking: Cyber-Crime Survival in the Digital World," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 10332–10334, Nov. 30, 2019. doi: 10.35940/ijrte.d4612.118419.

[3] P.Y. Logan and A. Clarkson. "Teaching students to hack: curriculum issues in information security." *In Proceedings of the 36th SIGCSE technical symposium on Computer science education*, 2005, pp. 157-161.

[4] Y.A. Younis, K. Kifayat, L. Topham, Q. Shi and B. Askwith. Teaching Ethical Hacking: Evaluating Students' Levels of Achievements and Motivations. *In International Conference on Technical Sciences (ICST2019)*, Vol. 6, 2019, pp. 04.

[5] M. Plis, "Top 10 countries where security hackers come from & their types," *Cyberkite*, 2021, [Online]. Available: https://www.cyberkite.com.au/post/hackers-top-10-countries-where-they-come-from-hacker-types.

[6] V. Rajiwade, "Top 10 Countries With Most Hackers in the World," *cyberyug*, 2021, [Online]. Available: https://www.cyberyug.com/post/top-10-countries-with-most-hackers-in-the-world

[7] Bscholarly, "Countries with the Best Hackers in the World 2022: Top 10 Cyber Attacks," 2021, [Online]. Available: https://bscholarly.com/countries-with-the-best-hackers/.

[8] C. Hiley, "Brief history of cybersecurity and hacking," *cybernews*, 2021. [Online]. Available: https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/.

[9] Redteamacademy, 2021 https://redteamacademy.com/blogs/history-of-ethical-hacking/

[10] CYBER COASTAL, "a brief history of ethical hacking",2020, [Online]. Available: https://cybercoastal.com/a-brief-history-of-ethical-hacking/
[11] A. Froehlich, "white hat hacker", *techtarget*, 2021, [Online]. Available: https://www.techtarget.com/searchsecurity/definition/white-hat.
[12] D. Rafter, "What is the difference between black, white and gray hat hackers?", *Norton*, *2022*, [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html.
[13] I. Pradeep and G. Sakthivel. "Ethical hacking and penetration testing for securing us form Hackers." *Journal of Physics: Conference Series*. vol. 1831. no. 1. IOP Publishing, 2021.
[14] P. Sankardas, R. Mohammed, B Bibitha "Ethical Hacking: Impacts on Society" vol. 9, no. 1, January 2020 pp. 211-214.
[15] greycampus, "Phases of Hacking", [Online]. Available: https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking .