Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

AN EMPIRICAL ANALYSIS OF ETHICAL HACKING

SHAHID ALI
Department of Computer Science, Superior University, Lahore, Pakistan.
Email: shahid5232@gmail.com&msse-s21-003@superior.edu.pk

SHAHARYAR RAFIQ
Department of Computer Science, Superior University, Lahore, Pakistan.
Email: msse-s21-004@gmail.com

SYED ZAIN UL HASSAN
Department of Software Engineering, Superior University, Lahore, Pakistan
Email: zain.ravian@gmail.com

ASMA ARSHAD
Computer Science Department, The Institute of Management Sciences (Pak-AIMS), Lahore, Pakistan.
Email: asma.Arshad@pakaims.edu.pk

MUHAMMAD WASEEM IQBAL
Department of Software Engineering, Superior University, Lahore, Pakistan.
Email: waseem.iqbal@superior.edu.pk

SHAHERYAR
Department of Computer Science, Superior University, Lahore, Pakistan.
Email: shaheryarchattha362@gmail.com

Abstract
Cyber threats will arrive from many angles as new technologies are being ingrained in many facets of life. Business associations relocate a larger amount of their fundamental skills to the Internet, offenders have a greater ability and driving power across the online application to access sensitive data. The Public Network is the world's most popular and fastest alternative for spreading attacks all over the world. Malicious hacking has earned hacking a poor reputation over the years, but hacking was not meant to be an illegal operation from the outset. It could also be ethical, lawful and appropriate, while hacking could be malicious. Hacking is a method that is pursued to identify the system's flaws or holes for self-profit or pleasure. Most hackers steal data to ruin the credibility and development of companies in the industry. We have an ethical hacking process to protect our networks against attack. It is the act of using hacking methods, expertise and tools to uncover bugs and locate knowledge loopholes. Ethical hackers are those certified persons who work legitimately. This article discusses ethical hacking, various forms of hackers, and the hacking stages that ethical hackers pursue to protect a network or system.

Keywords: Ethical hacking, Ethical hackers, Sorts of hackers, Empirical analysis

1. INTRODUCTION

The prevalence and extent of data breaches have risen over the past decade. No one control will eliminate risks to security and no magic bullet. A mixture of monitoring, mitigation, and institutional controls combines multiple security architectures that are complex [1]. The Internet is still evolving, and progress is being made by online companies. The immense advancement of the Internet has brought various wonderful items like electronic commerce, email, easy access to tremendous stores of reference material, and so forth. The administration, the private sector, and the daily computer

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

customer are worried about their knowledge or private data being contained by a malicious hacker because of the Internet's propelling innovation [2].A smart mobile interface enables mobility to be developed and simultaneous activities to be developed to satisfy the idea of "computing anywhere or at any time" The relentless demand for these devices from smartphones has made them grow constantly, making a vast number of users available. They are used to store sensitive records, maintain the daily schedule, search the internet, save photos, create photographs, create personal or technical documents, and carry out financial operations [3].Cybersecurity is an increasingly advancing science that has been constantly in the headlines for the last decade, as the danger grows and cyber offenders continuously attempt to keep a step ahead of the authorization of the law [4].

There are billions of computers and networks linked to the internet. Online customers have access to millions of websites and millions of apps. All online tend to be interested in one or the other method of downloading. Anyways copying has been made unconstitutional, but this does not mean that downloading can be considered a crime [5].Cybercriminals are exploiting creativity at a rate that cannot be matched by many target organizations and defense hawkers[6]. Information protection protects against multiple risks the secrecy, credibility, and availability of information properties. To provide information security, technological safety mechanisms are not appropriate. Other steps must be implemented. To ascertain stable and smart data management, operational, ethical, social science, and legal steps should be thought of in addition to technological measures [6][7].Hacking is the technique in which people are all interlopers attempting to get into your networks and systems, calling them spies, crackers, intruders, or attackers [8]. Hacking is not a simple operation or charging scheme where the same number of people believe. Hacking is just a skill. Software hacking is the act of modifying computer devices and code to fulfill a purpose beyond the unique reason for the maker. Hackers are regularly named people who engage in computer hacking activities. Hacker is a hacker who hacks through the programming framework or knowledge of another person without authorization [2].

It is important to stress that to be able to conduct ethical hacking the pen tester or hacker must have a strong understanding of technology [3]. A hacker is exceptionally effective in taking data from the system to which he is illegal, such as financial details, human information, money-dependent data, credit card data, username & password. These intelligent programmers have outstanding abilities, the ability to build computer programs and to investigate computer programs and equipment. Their motivation may be either to do illegal activities for fun, or they are paying to hack in some cases [4]. The media started using the word "hacker" to describe criminals who broke into computers instead of using the more descriptive term "computer criminal" [9].Although ethical conduct is implied by the name "Ethical Hacker," this may not always be the case. For example, an ethical hacker needs to keep their knowledge of exploits up-to-date, and to gain this knowledge, they will probably need to go "underground." The primary purpose of ethical hacking is to test an organization's security controls and validate it. This likely results in an attempt to gain access to the organization's confidential and sensitive information [1].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

Additionally, called "Penetration Hacking" or "Intrusion Testing" or "Red Teaming" is moral hacking. Without malicious intent, ethical hacking is described as the art of hacking. Ethical hackers and malicious hackers differ from each other and play important security roles. A way to do a safety assessment is ethical hacking. An ethical hack is a random sample, like all other assessments, and passing an ethical hack does not mean that there are no security problems. Ethical hacking fits perfectly into the life cycle of security [8].By recruiting a specialist or team of experts to target an enterprise as a malicious hacker does, penetration testing plays an important part. The need to ensure acceptable ethical behavior is crucial with the increased demand for ethical hackers as part of a multi-layered defense program coupled with the possible sensitive and classified information to which an ethical hacker might obtain access [1].Behind ethical hacking, there are positive and constructive motives that will shield any company, product, or individual from those that plan to do any harm. Throughout these years several companies have experienced damage due to the stealing of their valuable records. Others have lost their clients' trust due to inadequate safety measures. Companies and organizations have begun hiring ethical hackers to check their network security and reduce possible vulnerabilities to prevent these consequences. In reducing cyber-crime in society and fostering a criminal-free climate, ethical hackers play a critical role [10] [17].

This burgeoning economy of information security certifications has produced the CEH certificate. Since at least the mid-1960s, when the U.S. military and other organizations started employing "red teams" or "penetration testers" to try information security exploits and thereby help detect and mitigate flaws, ethical hacking has become a professional activity. Intense School, a company founded in 1997 by two brothers and IT advisors, David and Barry Kaufmann, and their cousin, Ron Rubens, was the first organization to provide CEH training [11]. Otherwise, it is called penetration research or hacking of white-hats. Before the horrible people have a chance to exploit them, the art of checking the machines and device for security bugs and stopping the holes you uncover. Ethical hacking should also guarantee that the cases of dealers surrounding the protection of their goods are legitimate [2]. The increase of malignant initiates, cybercrimes, and the presence of multiple forms of cutting-edge assaults entail the need for penetration analyzers to join, plan and prevent future danger and redress operations against these aggressive assaults [4].A "Network penetration (pen) test" is considered a standard ethical hacking engagement and will typically include a physical aspect as well. Then, a successful hacker can assault doors, unlock them, and gain entry without damaging the key, either by locking, shimming, or by subverting the computerized badge system [12] [18].According to the shades or colors of the hat, hacking can be divided into three distinct groups. The term Hat came from old western movies where "White" was the color of the Hero's cap and "Black" was the cap of the villains. It can also be seen that the brighter the color, the less dangerous the intensity is [8]. Since any approach needs a few dedicated resources and methods to accomplish the task, the hacking process often requires the right tools [10].

The idea of teaching information technology classes at HE universities has also been proposed by advocates of ethical hacking. This includes teaching how to hack and how

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

these techniques have legal and ethical implications [13]. Ethical hacking does not constitute a felony. Much as hacking was not a felony from the outset when actual hacking was synonymous with learning programming languages and computer programs in the hope of making new technologies to solve problems [5]. A usage analysis performed by Garfinkel and Miller notes that despite having secure passwords, many users could still be vulnerable [14] [19].The black hat hacker is the most well-known type of hacker. The black hat hacker, popularized by TV, film, and sometimes in the media, has intentions that are deemed malicious [1]. Crackers are a well-known term for black hackers. They have abilities close to those of white hackers. They use their talent for the wrong reason, though. Their primary intent is to steal unauthorized access to the records. They primarily threaten corporate data, violate privacy, disrupt the infrastructure, and block the contact channel of the network [15].

Black hat hackers are hackers who exploit for their purposes [6].For political purposes, criminal intent, or sometimes just for notoriety or fun, hacking is often carried out [16].Ethical/moral Hackers" could be well-known name for white hackers. They have in-depth knowledge of networking protocols, software and hardware features, and professionally trained administrators." Like all Administrator-like rights. We conduct penetration testing and vulnerability evaluations. They work and are well paid for by the organization [15]. A white-hat hacker is a hacker who does ethical hacking and writes what he has done for the report [1].Blends of both White Hackers and Black Hackers are Gray Hat Hackers. They do the hacking without the owners' permission. Their main intention is to take advantage of a system's security weakness and bring problems to the attention of the owners. The combination of black hat and white hat hackers are grey hat hackers [6].

To detect technological flaws, it is possible to use a range of automatic methods or manual techniques. Similarly, technologies can be used to carry out attacks on individuals, as seen in 'phishing' schemes focused on email, or where an attacker uses a phone to contact or give a possible target an SMS message. In-person, attacks will also take place when a hacker manages to obtain access to a physical building. The vulnerabilities are used by malicious hackers to typically carry out attacks for financial gain, personal gain, or to cause mischief [1].Awareness of applications and networks is not necessary to complete the process of hacking. Unique instruments and technical systems are committed to the detailed execution of ethical hacking [10].

There are various forms of threats, such as non-technical assaults, assaults by the Network Foundation, operating system assaults and frameworks, and other specific assaults. Like a Trojan horse, malware, worm, and sniffer, there are a few regular methods used by tech criminals to penetrate the network. Usually, a hacker acknowledges the use of equipment. Any hackers make their computers. Here are the main hacking apparatuses some of them are NMAP, Wireshark and Putty, etc. Ethical hackers such as Backtrack and Kali Linux etc. use various types of the operating system. Hacking is not a mechanism in a single-phase [10] [20]. Hacking may be achieved through identification, scanning, machine ownership, zombie system, and destruction of evidence after these five phases [8].Reconnaissance gathers as much

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

information as possible about the goal. In this step, we will discover the loopholes present in it by scanning the target. Once we reach through the hole with the second stage that scans if any holes are present and discover that they are accessible, this is gaining entry. The hacker holds some backdoors to reach the machine after obtaining entry, as he wants to access in the future in this owned system. This is the final hacking step. This purpose is to delete all the things that we have achieved in the above stages [6].

2. BACKGROUND AND LITERATURE REVIEW

In the 1960s, programmers at MIT coined the term hacker to describe someone who was able to understand and manipulate technology. Since then, while hackers still manipulate technology to a large extent, the role and type of hackers have evolved [17]. He points out that there are currently ethical hacking degree programs offered by a variety of UK universities. Abertay, which has a high-performance rate, was the first of these, with 88% of students having a technical or administrative job within six months of graduating [18].

Bhawana Sahare, Ankit Naik, and Shashikala Khandey describe in their paper study of ethical hacking that hacking is a process that is used to find out the flaw for sake of personal profit and they are known by different names like “cracker, intruder” or attackers”. In this era, most other public/private organizations have transferred their applications like electronic commerce, marketing database access, etc. to the internet so lawbreakers can easily obtain all the confidential information through the web app. So, there is a need to protect the system through ethical hacking there is a security life cycle that also works in ethical hacking because it is also known as a security calculation. They discuss ethical hacking, classes of ethical hacking, the dissimilar impact of ethical hacking in government and business that hacking let the businesses to lost millions of dollars and the loss of a company’s data also reduce client’s trusts. There are limitations of ethical hacking, and also different stages of hacking are there e. g: reconnaissance, scanning, owning the system, zombie system, and evidence removal. The authors elucidate about different kinds of hackers e.g: black hat, white hat, grey hat hacker. They argue that hacking is both risky and valuable as it can ruin a company or rises the profits of a company. There is a clash between both black and white hacker’s former is for security needs while later can unlawfully mischief the network for private benefits. There are a lot of benefits as well as limitations of ethical hacking although ethical hackers follow different testing techniques to find the issues and avoid data from hackers. Finally, they concluded that hacking is a crucial factor in this world and it has both worthy and immoral sides so it is difficult to fulfill the hole between ethical and malicious hacking because the human mind cannot be captured but the security can be tightened [8].

The researcher Azhar Ushmani in his article argues hacking is a practice that is used by hackers to crack the secrecy to identify gaps and flaws in a system to access all confidential information. He claims that hacking is known as “unauthorized intrusion”. Hacking is not always used unlawfully it can be used for worthy intentions then this kind

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

of hacking can be said as ethical hacking. With the progression of swiftly rolling technology-oriented future and technical systems, ethical hacking is needed. There are two basic categories of hacker's black hat hackers and white hat hackers who have dissimilar objectives. The author clearly expresses that ethical hackers which are also known as white hat hackers are not convenient because they are supposed as unlawful hackers so there is a need to aware society of ethical hackers for security as ethical hackers are different then malicious hackers because they are dynamic and enthused. Ethical hackers are professionally certified ("Certified Ethical Hacker - CEH Certification | EC-Council") and dissimilar organizations appoint them to keep on checking their security issues. Ethical hackers have the same kind of skills the other hackers but we can trust them because they are trustable. Cybercrime can be reduced through ethical hacking. Hackers use a certain types of abilities, devices, and tools so the way of thinking is the same for both hackers. The elementary approaches and procedures unit of measurement area unit there that hackers have to be compelled to grasp unit of measurement area unit" HTTP, HTTP, and any network proprieties, network and firewall constructions, port data, authentication ways that, web app, net servers' configurations, info setup and different cryptography languages like" HTML, Ruby, Python, Javascript".The five phases of hacking are there reconnaissance, scanning, gaining access, maintaining access, and clearing tracks which help in successful hacking. Finally, he concluded that if honest hackers' services are used by organizations security issues can reduce at the greatest level [10] [21].

The researcher Rebecca Slayton in the paper certifying ethical hacking explains how the fears regarding hackers and the ethics of professional knowledge are that ethical hackers follow different methods and abilities. Expertise/Technology staff also encouraged the growth of information security certifications in the 1990s. Review the formation and early commercialization of CEH trying to show how the certificate tried to appropriate the technological authority and strangeness of hackers and the U.S. military even without the embarrassment of the common crime association of hackers. Then explore how the certification's legitimacy and reputation have been. The friction among the interests of professional competence standardizes and legalizes knowledge practices and the inventive and malicious spirit of hacking is essentially restricted. As businesses are online these days so there is a need for ethical hackers in an organization and to confirm their honesty/legality. But despite what professionalization logicians might say, the certificate of ethical hackers did not come from penetration testers demanding to regulate entrance into their field of work. In reality, certification was not targeted specifically at individuals interested, but relatively at any certified who could profit from learning to "think like a hacker." Relatively than imitating the professionalization of ethical hacking, certification arose as a way by which tycoons could advantage of learning to "think like a hacker." Hackers immediately proposed being "practical, not certified." Even while U.S. military departments implicitly approved the qualification by sending some of their employees to be trained, neither the Unit of War nor the Unit of Defense funded the certification. The certification of proprietary rights possessed by establishments such as the American Medical Association has only been issued by civilian authorities. For employers, qualification became a desirable

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

currency, but it tended to draw its reputation from the darker and more obscure military and hacking realms [11] [22].

Dr. Sunil Kumar and Dilip Agarwal in the paper “Hacking Attacks, Methods, Techniques and their Protection Measures” elucidate that different organizations including private/public all have transferred their data on the internet so there are a lot of security threats and lawbreakers can easily access data through web app so, to protect the system they need of ethical hackers arise. Ethical hacking is legitimate and it is done by objective authorization. The researchers reveal the issues of ethical hacking with business security. Ethical hacking also does well to keep the stuff of the client safe from illegal access. Hackers are ultimately IT workers who know about coding etc. They describe hacking attacks as non-technical assaults, network-foundation assaults, operating-framework assaults, applications, and other particular assaults well there are different types of hacking like inside jobs, rogue access points, back doors, denial of services, distributed Dos, Anarchists, Crackers, and Kiddies and Sniffing and Spoofing There are different hackers like white hat hackers (ethical hackers), black hat hackers, and grey hat hackers, they also discuss major ten tools used for hackers like Nmap, putty, Wireshark and HPING3, etc. and they also expose different hacking protection techniques. Ethical hacking is the best way to fill network gaps to avoid issues. Ethical hackers use different devices that are known to them and must use instruments in a way that is helpful for the network. Ethical hacking has a special part in security evaluation. So respect the ethical hackers to achieve their mission [2].

The researcher Vikas Bhaskar Vooradi, and Lavina Jadhav in this paper describe the Internet as very much in use these days and we keep all information on the internet. Information is very crucial for us. The authors claim that a hacker is an individual who tries to find security gaps just for the sake of his profit. Most of them theft because they want to get benefit from that data or they get the data of any company just to spoil their image and reputation in the market just for the sake to grow their businesses well. They elucidate ethical hacking, anticipation measures, and type of hackers. There are different forms of hackers like the white hat, black hat, gray hat, red hat, and blue hat hacker’s further Elit hackers, script kiddies, neophytes, hacktivists, and phreakers. They all are hackers with different intentions in their brains and the phases they follow are reconnaissance, scanning, owning the system, zombie system, and evidence removal. The hackers use different kinds of operating systems like backtrack, Kali Linux, Parrot-Sec forensic OS, cyborg hawk Linux, back-box, samurai web testing framework, network security toolkit, black arch Linux and Gnack track. They also describe different techniques of hacker’s e.g bait and switch, cookie theft, SQL injection, phishing, and click jacking, etc. Thereof are different kinds of viruses like file viruses, boot sector viruses, macro viruses, and source code viruses, etc. The different tools which hackers use while ethical hacking is john the ripper, Nmap, and SQL map, etc. finally they concluded that there is a progression of technology in this era and there is no controller on the activities done by the humanoid brain so there in need to follow all the prevention technique like being cautious of unrestricted wifi, create a strong password, keep on changing passwords and use patterns and pins, etc to stay safe from hacking [15] [23].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

OMOYIOLA Bayo Olushola in their paper “The Legality of Ethical Hacking” describes ethical hacking as a lawful act and that hacking that is unlawful creates an immoral image of hacking but the basic purpose of hacking was not illegal action. So, hacking can be of both categories malicious and ethical/legal it’s true that not all kind of hacking is lawful but ethical hacking is acceptable and used for different reasons like reconnaissance/information gathering which is not illegal because we don’t do unapproved access, illegal license, unapproved penetrating testing, etc. instead we collect materials for investigation purposes. But in contrast to illegal hacking, we do unapproved access, illegal license, unapproved penetrating testing, etc. There are different devices connected online they share data and download software from which some are legal but some are illegal and its downloading can be lawbreaking. They also claim that hackers have done most of the inventions and technical revolutions. They also invent the PC and www (World Wide Web). Ethical hacking is not illegal because it is not done for destruction and CEO has considered unlawful hacking as criminality. There are different sorts of hackers and all hackers are not the worst some hackers are not harmful because they are not working for damaging activity they are also called “white hat hackers” and further varieties are black hats, green hats, blue hats, “suicide hackers and script kiddies” who are also involved in illegal /mischievous attacks. There is different computer lawbreaking also known as cybercrime. Cybercrime lets us use the network but computer criminality makes it probable to use the network. Computer crimes can be theft identity, scams, and cyber-attacks while cyber-attack also include cyberbullying and cyber violence, etc. Ethical hacking is helpful for inquiry and revolutions can be used to prevent illegal hacking [5].

P. Harika Reddy and Surapaneni Gopi Siva Sai Teja in the paper “cybersecurity and ethical hacking” explain that in computer science ethical hacking and cybersecurity are evolving fields. These days we are transferring data through different media like email, social media and doing shopping and banking online so here the chances of an issue because of the digital world. Maximum business is digitized so hackers can try to reveal the information illegally. Because of the use of the internet, the probabilities of criminality increase, and the most objectives are to attack computers and mobile phones. They elucidate that the companies can use the same hacking skills for ethical hacking known as white hat hacking so.it is easy to measure information assets fears. Ethical hacking uses their abilities for defense against issues and crackers use their abilities for damaging reasons but not all kind of hacking is unlawful. The three categories of hackers are black hat, white hat, and grey hat hackers. There are different kind of hackers coders, admins, script kiddies, hacktivist, and suicidal hackers and the hackers go through many phases to hack and these are:Phase I is footprinting which includes footprint using search engines, email footprinting, footprinting using google, DNS record, Whois, network Footprinting, angry IP Scanne and advances IP social engineering and competitive intelligence.Phase II is scanning used to scan and find gaps it includes port, network, and web app scans.Phase III gaining access to this process weaknesses are located. These are Directory Traversa, SQL injection, and Cross-Site Scripting, etc.Phase IV is about maintaining access and it uses the

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

Metasploit instrumentPhase V is the last phase and its clearing tracks which remove things done in previous phases [6] [16].

Brijesh Kumar Pandey and others in the paper “ETHICAL HACKING (Tools, Techniques, and Approaches)” argues that ethical hacking is important to the distress of all companies and government they are their clients are in trouble of being hacked. Ethical hackers use the same devices and methods as an intruder but they don’t destroy the system and their intention is not to theft the available information. Ethical hackers should have enough knowledge of networking and programming. Hackers do hacking just for the sake of enjoyment and welfare they have enough knowledge about coding and networking and they know the use of different operating systems like Unix and Windows Nt. IBM's rule is not to appoint the old hackers but the actual hackers have the basic abilities to work. Different weapons are used by ethical hackers like Nmap, Nessus, Nikto, Kimate, Metasploit, and Netstumblur. Different ethical hacking techniques are gathering information, Vulnerability, scanning, and test investigation. There are different approaches to ethical hacking (pen testing) the testing is of different forms like a remote network, a remote dial-up network, a local network, a stolen laptop computer, social engineering, and physical entry. The authors explain that security on the internet is much more crucial as compared to customary security where the purpose was just to find the culprit in ethical hackers who play a vital role in internet society and guard the establishments' data against being hacked. They help in the creation of the internet a secure place for companies and customers. Cybercrimes can be avoided by “cyber corps”. Finally, it is found that ethical hacking is a dynamic procedure and there are many opportunities for proficient hackers these days [14].

The researchers Muhammad Imran, Muhammad Faisal, and Noman Islam in this paper “Problems and Vulnerabilities of Ethical Hacking in Pakistan” elucidate that there is an increasing rise in IT companies in Pakistan and cybersecurity. There are a lot of issues for different organizations as data is digitized so they have to think of some strategies to prevent their confidential data. It is tested that here different issues faced using different websites so there is a must to use feeble secret code. The authors claim that Pakistan is fronting different concerns to ensure cybersecurity these issues are that there is no technical hacker available in our republic and they should need to be trained or get a certificate from out of the country which is not easy for middle-class people and the other is the disasters of employment in IT organization. There is a different kinds of programs which governments like the Ministry of Defense, the Central Ministry and the IT Ministry with the cooperation of different organizations to promote the IT industry and joblessness. Ethical hacking is used to shield from different outbreaks. The authors argue carefully that there are many issues related to security and there is a need to prevent people from hackers. There are black hat and white hat hackers in the beginning then they introduce grey hat hackers. They contend clearly that green hat hackers are their enumerated hackers in Pakistan and they know they need for safekeeping in a company. So, they are helpful to keep the information safe and they get certification from HEC-acknowledged universities. Hacking is normally considered the worst activity but it can be in both aspects worthy or immoral It can be beneficial for

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

a company or may give loss to the company but it depends on the sort of hackers. They act as the army and protect the attacks that damage security [19] [24].

3. METHODOLOGY

To undertake an ethical hacking review, which is the purpose of this report, we performed an SLR according to the methods suggested by Kitchen Ham and Charters. This approach consists of arranging, executing, and reporting phases in which there are many stages in each process. It consists of three levels.

3.1 Planning/Organization

As mentioned in the above overview, the preparation process began by defining the need for this analysis, as well as setting the targets to be reached. We determined the key goal of the analysis in this process and carried out the following tasks that clarified each move in detail.

3.2 Recognition of the Necessity for a Review

We identified in Step 1 that there was no SLR in the area of ethical hacking. This SLR aims to explain and summarize the current ethical hacking facts. Determining that ethical hacking is important. Any of this is useful for future studies. Therefore, due to the findings of the previous tests, we calculated the need to execute an SLR.

3.3 Indicate the Research Question(s)

The overarching aim of this SLR is to identify and review studies relating to ethical hacking principles conducted between2014-2020. To attain a more accurate and systematic view of this subject, the foremost objective was divided into succeeding research issues. This analysis needs to keep the door open for potential updates.

To achieve the objective of this analysis, four key questions were described as follows:

RQ1: What is hacking and the necessity of ethical hackers?

RQ2: Is ethical hacking legal and is it useful to get hackers certified?

RQ3: What are the different types of hackers?

RQ4: What are the different stages of ethical hacking?

3.4 Recognizing the Appropriate Bibliographic Databases

The available digital libraries were scanned for the appropriate papers as per the research questions: Google Scholar, Science Direct, IEEE Xplore Digital Library, ACM and Springer. The foremost motive for choosing these digital reference libraries was; they accumulate studies associated with the fields of computer science and technology they index articles from numerous publication channels like journals, conferences, books and workshops. In this article, the explorations were narrowed to articles published in the 2005-2023 journal and conference proceedings shown in Fig 1.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

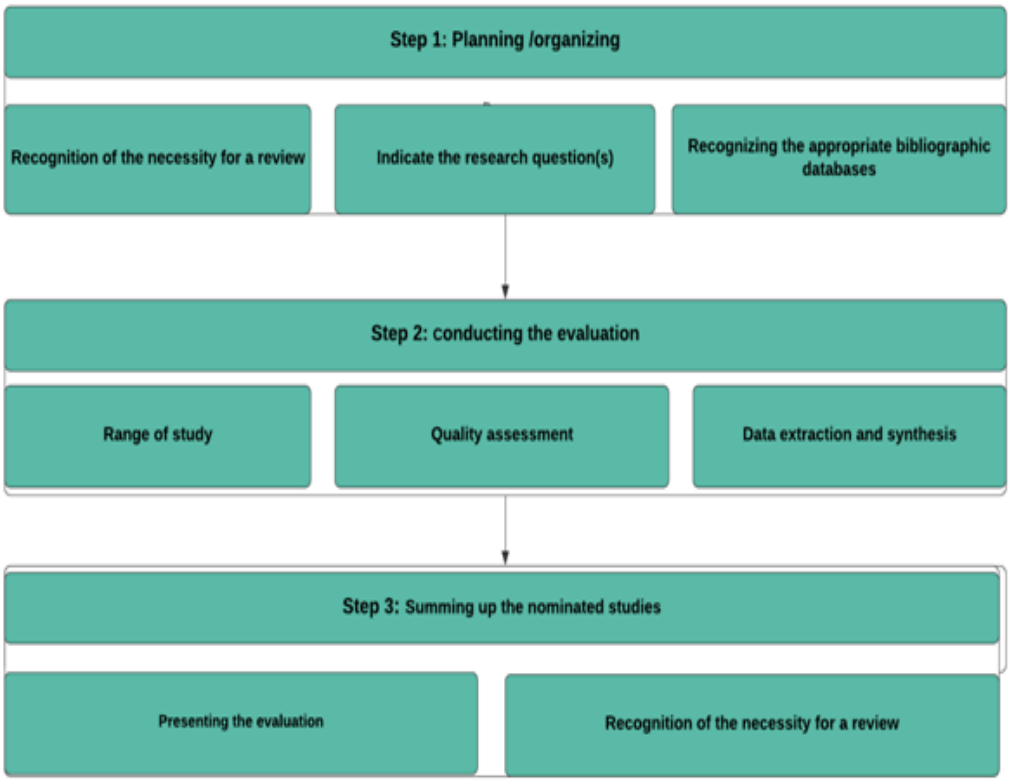

Fig 1: SLR steps and events

3.5 Conducting the Evaluation

The massive coverage can be generated by the search string, but it is a fair scale. Consequently, the keywords matching the study questions were extracted for the fortitude of the search string and the synonyms linked to the main terms were identified. To merge alternative meanings, the Boolean OR was used and the Boolean AND was used to connect the key pieces.

The entire search string collection was planned as follows:

(("ethical" AND "hacking") OR "Hacking") OR ("ethical hackers" AND "ethical hacking") OR ("ethical hacking phases" AND "procedure of hacking") OR ("ethical hacking" AND "tools of ethical hackers") OR ("techniques of ethical hacking" AND “hackers")

3.6 Range of Study

We revised the paper's abstract, introduction and conclusion/finish. We picked those that were written in English among the papers received and that fulfilled minimally one of the following measures:

- Studies should elaborate distinction between hackers and legal hacking.
- Papers that address various kinds of hackers.
- Papers that compile ethical hacking phases.
- Reports discuss the legality of ethical hacking.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

The investigator conducted a manual check of the search string results and found that advanced settings such as IEEExplore were required for some of the online databases. The researcher wants to apply to the search string alternate terms and phrases.

The requirements for inclusion and omission for this SLR are based on study questions. As this SLR is based on the test case prioritization methodology, it is important to identify inclusion and exclusion requirements to choose only appropriate documents. As follows, the inclusion conditions are:

- In English, all articles must be written.
- From 2014 to 2020, all articles must be written.
- All records must concentrate on ethical hacking and its manifestations.

Before being considered for the next step, each of the papers is screened into exclusion criteria. For this SLR, the exclusion requirements are as follows:

- Articles that have not been written in English.
- Duplicate areas of science.
- Papers that comprehend only opinion pieces, perspectives, studies on development, or partial findings.
- Articles with fewer than three pages.
- Papers that do not report any scientific analysis in their study.

3.7 Quality Assessment

Quality testing is typically designed to evaluate appropriate and impartial research. Therefore, to refine our search results and ascertain the relevance and rigorousness of the applicant papers, we determined more or less the quality assessment metrics. As follows, the questionnaires for quality evaluation are based on other SLRs

- Are the research's objectives and priorities explicitly stated?
- Is the research design specified? Yes/no/partial
- Has the researcher(s) properly carried out the process of data collection? Yes/no/partial
- Did the researcher(s) have adequate evidence to confirm their outcomes and conclusions? Yes/no/partial
- Does the experiment require comparing other techniques? yes/no

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

Fig 2: Shows the studies inclusion and exclusion.

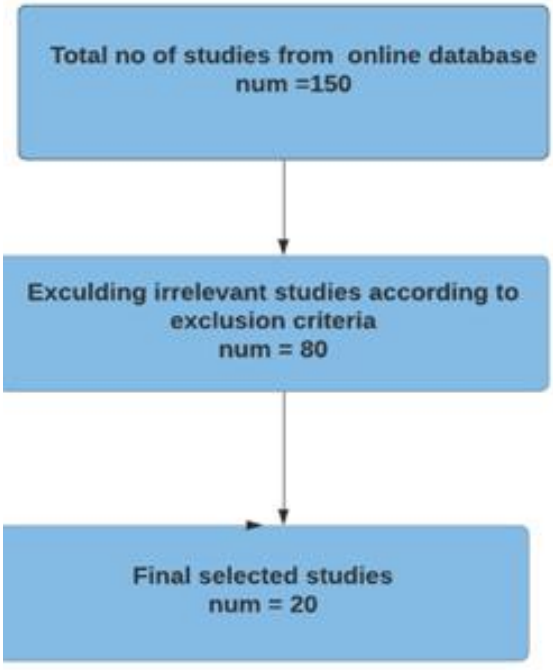

Fig 2: Studies inclusion and exclusion

3.8 Data Extraction and Synthesis

A data extraction procedure was introduced to answer the research questions to gather the appropriate data from the chosen documents.

RQ1. To respond to this research question hackers and ethical hackers were acknowledged.

RQ2. Is ethical hacking legal and is it useful to get hackers certified?

RQ3. To answer this question, all sort of hackers was identified.

RQ4. Determining the different phases followed by the ethical hacker. To synthesize the collected data and to address the study questions, various techniques were active. A narrative synthesis approach was used entirely to address research questions. In addition, based on research concerns, visualization techniques were applied.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

3.9 Results

Summing up the nominated studies: The investigator classified 150 papers using the specified search words from the first stage of the search process. Just 80 were theoretically important, after screening titles and abstracts. Any of the articles were filtered before being approved for the synthesis of evidence for comparison to inclusion and exclusion criteria. Irrelevant experiments and repeat studies have been removed at this point. If the titles and abstracts were not adequate to categorize the paper as applicable to the research field or not, the researchers read the full papers. Finally, to provide answers to the formulated study questions, 20 studies were chosen.

3.11 Presenting the Evaluation

RQ1: What is hacking and the necessity of ethical hackers?

Everyone has to be linked, as we know, and this can be possible only via the Internet. However, when sharing confidential data with a stranger, friends, or a loved one, a little caution is still needed as hacking is notorious for its adverse effect in the internet age. The harm associated with it - academically, socially, or mentally - must still be resolved by one's protection [15]. Cybercrime, cybercrime, is where the object of the crime is a device or a smartphone or where the means to commit a crime are ratified. Cyber attackers are exploiting creativity at a rate that cannot be matched by many target companies and defense hawkers. The bulk of these offenses is not new crimes. Criminals reform various methods of carrying out standard illegal acts, often involving the Internet, such as bribery, robbery, extortion, and forgery [6].

Hacking

Hacking is the strategy of which, what's in a name for the people? They are just interlopers trying to get into your networks and devices. Name them spies, crackers, intruders, or terrorists. Many do it for fun, some do it for profit, or some only do it to disturb your activities and maybe earn some attention. While they all have one thing in common; to hack it [8], they are attempting to uncover a flaw in your scheme. Hacker is a hacker who hacks through the programming framework or knowledge of another person without authorization [2].

Ethical hacking

Ethical hacking is also called penetration research or hacking of whitehats. Before the terrible people have a chance to adventure them, the talent of checking the machines and devices for safekeeping bugs and stopping the holes you uncover. Ethical hacking and ethical hacker are terminologies used by an organization or person to denote hacking to better recognize feasible hazards on a device or system [2]. Standard words are ethical hacking and penetration testing, well known for quite a while in data security environments [4]. There are 4 common types of penetration testing these are external testing, internal testing, blind testing, and double-blind testing [20]. People specializing in the process of ethical hacking are known as ethical hackers. They are the experts who break into a device or network to find potential faults, pitfalls, and bugs that blackhat hackers or crackers may be exploiting [1]. Ethical hacking is a process carried

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

out by a registered person that is hands-on. They have direct access to the device where the bugs can be tracked and the protection jerks can be redirected to the upper authority or shareholders. They are referred to as White Hackers who effort for the corporation or the company [15] [25]. Ethical hacking, as it is lawful, allowed and appropriate, should not be considered a crime. Hacking was known as a form of tinkering in the beginning. To get something different, it was a method that involved making changes to something. Over the years, though, the understanding and enthusiasm of individuals about hacking have shifted. Initially, hackers were persons who sought to deeply research computers. As a result of their activities, this group of people has brought creativity and technical breakthroughs [5].

RQ2: Is ethical hacking legal and is it beneficial to have certified hackers?

Ethical hacking does not constitute a felony. Much as hacking was not a felony from the outset, in the hope of making new technologies to fix problems, actual hacking was synonymous with learning programming languages and computer systems. Ethical hacking, as it is lawful, allowed and appropriate, should not be considered a crime. Hacking was known as a form of tinkering in the beginning. To get something different, it was a method that involved making changes to something. Although cybercrime and illegal activity may be malicious hacking, ethical hacking is never a crime. Ethical hacking is following the legislation of business and the policies of corporate IT. Malicious hacking should be avoided while promoting and permitting ethical hacking that encourages science, creativity, and technical breakthroughs. [5]. Intense School, a corporation founded in 1997 by two brothers and IT advisors, David and Barry Kaufmann, and their cousin, Ron Rubens, was the first organization to provide CEH training. This burgeoning economy of information security certifications has produced the CEH certificate. Since at least the mid-1960s, when the U.S. military and other establishments started employing "red teams" or "penetration testers" to try information security violations, ethical hacking has become a technical pursuit and thus helps in recognizing and identifying member organizations. The CEH certificate, however, was not specifically targeted at penetration testers, but reasonably at any specialist who might profit from learning to deliberate like a hacker. It distinguished itself from other certifications by promising a constructive approach to security rather than a reactive one, in which organizations were able to predict and deter breaches rather than continuously improving from and preparing for their latest breach [11] [26]. The growth in the number and complexity of cyber-attacks is the reason that these attacks remain undetected and their number extends to thousands of cyber-attacks every day. Digital security programmers are making every attempt to secure files, computer applications, devices and networks against such threats, including unwanted access, spoofing, or obliteration, to deter such attacks. Moreover, monitoring this abject state of defense in the world is still a major concern for governments and policymakers [12].

Professional Competencies

Ethical Hacker has familiarity with almost all working systems, comprising all mainstream working frameworks, such as Windows, Linux, Unix, and Macintosh, which are commonly used.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

These ethical hackers specialized in system management, basic and point-by-point concepts, inventions, and equipment and programming skills for inquiry.

Moral hackers' essential has a clear order over defense areas, associated challenges, and specialist fields.

Data on more established, advanced and advanced assaults should be available [27-30].

Non-Technical Competencies

- Learning power
- Problem solving skills
- Listening ability
- Awareness of laws, standards, regulations and security policy commitments [4].

RQ3: What are the different type of hackers?

TYPES OF HACKERS

White Hat Hackers

"Ethical Hackers" is the renowned term for white hackers. They have detailed knowledge of networking protocols, software and hardware features, and are skillfully proficient administrators. Like all Administrator-like rights. We conduct penetration testing and vulnerability evaluations. All are getting a good salary. They constantly think about intruder opinionsand what an intruder can do to contaminate the target structure to gain unlicensed access to alter sensitive facts [15].

Black Hat Hackers

Crackers are the renowned name for black hackers. They have skills related to those of white hackers. They consume their abilities for the wrong determination, however. Their primary intent is to take unauthorized access to the data. They chiefly target corporate records, breach confidentiality, damage the system and block the communication station of the network [15].

Gray Hat Hackers.

Gray Hat Hackers are fusions of both White Hackers and Black Hackers. They do hacking without the approval of the Holders. Their foremost intention is to take advantage of a system's security weakness and bring problems to the thoughtfulness of the owners. To get appreciation and small rewards from the owners, they do the hacking for fun. They even offered the owners a good salary. They are not, however, in search of employment [15].

RQ4: What are the different stages of ethical hacking?

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

Stages of Ethical Hacking:

Here are the steps to do ethical hacking which consists of 5 chunks

1. Reconnaissance/Inspection
2. Scanning
3. Gaining Access/owning the system
4. Maintaining Access
5. Clearing Tracks/evidence removal

Reconnaissance/ Inspection

The first step is referred to. In this step, the attack was first passive and second active in two approaches. The attacker seeks to obtain knowledge about the target system in the passive process without indirectly being involved in the contact with the target. Collecting information is sometimes called the passive step. Much of the time, the data is gathered by a bribing gift to the person that will report the valuable knowledge employed with the targeted company. Whereas the attackers aim to obtain access to the target device through direct means in the active stage [28-35]. At this point, to determine the singular IP address, port, host, and other resources, hackers attempt to access the network. There is a high chance of being trapped during this active activity correlated with it [15]. Footprinting gathers, as far as possible, information about the target. Footprinting using Search Engines

- Email Foot Printing
- Foot Printing Using Google
- DNS record
- Whois
- Network Foot Printing
- Social engineering
- Competitive Intelligence [6].

Scanning

The intruder attempts to discover a way to obtain entrance to the target device in this scanning process by inspecting the network. Specialized methods such as dialers, port scanners, network mappers, vulnerability scanners, ping tools and other critical tools are used to gain access to the target device [15]. In this step, we can discover the loopholes present in it by scanning the target. Three of the scans are

- Port Scan
- Network Scan
- Web application Scan

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

Gaining access

It's the true hacking level for hackers. However, when using the initial two knowledge steps. The enemy is attempting to obtain access to the Objective scheme [15]. If some holes are existing and are found open, we pass in through the hole in the second stage that scans, this is gaining entry. In this phase, bugs are found.

A. Vulnerability Testing

1. Directory traversal
2. SQL injection
3. Cross-Site Scripting
4. Session hijacking
5. Cross-Site Request Forgery Denial of Service

Maintenance access

In this step, the first thing the attacker does after obtaining access to the target system is to bring the structure under their control by modifying the configuration records and privileges of the system for upcoming use. Even if they make certain that getting entry to the device does not work in the end, they make use of the backdoor's methods to obtain the right of entry. At the time of modifying the setup and privilege [21-27], the attacker makes this safe backdoor access open to himself by inserting his script, which might modify the overall authorization of the objective system to get the system underneath their control [10]. The method in this method is Metasploit [6].

Clearing tracks

At this point, the suspect attempts to track all the actions carried out on the victim's computer. Then all the events are deleted or concealed. To escape the possibility of being caught, they also overwrite the server, application, and log files [15]. This is the concluding hacking step. This purpose is to delete all the belongings that we have achieved in the above stages [16].

4. RESULTS AND DISCUSSION

The primary aim of this paper is to discuss the value of ethical hacking. The simple idea of identifying security flaws in applications and networks is based on ethical hacking. To protect our system from malicious hackers, ethical hackers are required. White-hat hackers are not well tolerated by society by ethical hackers and are viewed as general hackers with sinister intentions. To deter security breaches of merchandise, there is a need to build awareness of ethical hackers. Ethical hackers have constructive and beneficial intentions and are trustworthy. They have accredited professionals who are assigned by organizations to keep their protection in place which is why they are essential for the community and companies. Ethical hacking is never a felony. Ethical hacking is following the legislation of business and the policies of corporate IT.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

5. CONCLUSION AND FUTURE WORK

In a device or network, hackers discover bugs and weaknesses and alter them according to their specifications. There are three groups of hackers known as white-hat, black-hat and grey-hat hackers who are categorized only by their hacking purpose. White-hat hackers are not well tolerated by society by ethical hackers and are viewed as general hackers with sinister intentions. To deter security breaches of merchandise, there is a need to build awareness of ethical hackers. To carry out the hacking process, any hacker uses certain instruments, abilities, and gadgets. Hence, any hacker's mentality and thought skills are the same. To complete goal hacking successfully, five phases of hacking are required. Security vulnerabilities can be significantly minimized if today's culture and corporations begin to take over the services of trustworthy hackers.

References

1. T. Georg, “Issues of Implied Trust in Ethical Hacking,” p. 19, 2018.
2. D. S. Kumar and D. Agarwal, “Hacking Attacks, Methods, Techniques and Their Protection Measures,” vol. 4, no. 4, p. 6, 2018.
3. M. Hernández, L. Baquero, and C. Gil, “Ethical Hacking on Mobile Devices: Considerations and Practical Uses.” vol. 13, no. 23, p. 12, 2018.
4. CM. Rakshitha, “Scope and Limitations of Ethical Hacking and Information Security,” p. 6, 2020.
5. O. B. Olushola, “The Legality of Ethical Hacking,” p. 3, 2019.
6. P. H. Reddy, “Cyber Security and Ethical Hacking,” Engineering Technology, vol. 6, p. 7.“Paper 20 Role of Ethics in Information Security 2016.pdf.”.
7. B. Sahare, “Study of Ethical Hacking,” vol. 2, no. 4, p. 5, 2014.
8. Brijesh Kumar Pandey, A. Singh, and Lovely Lakhmani Balani, “Ethical Hacking (Tools, Techniques and Approaches),” 2015, doi: 10.13140/2.1.4542.2884.“Paper 3 ethical hacking 2018.pdf.”.
9. R. Slayton, “Certifying ‘Ethical Hackers,’” vol. 47, no. 4, p. 6, 2006.
10. S. R. Ellis, “Ethical Hacking,” in Computer and Information Security Handbook, Elsevier, 2017, pp. 475–481.
11. Y. A. Younis, K. Kifayat, L. Topham, Q. Shi, and B. Askwith, “Teaching Ethical Hacking: Evaluating Students’ Levels of Achievements and Motivations,” p. 7.
12. S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, “Ethical hacking: The need for cyber security,” in 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, Sep. 2017, pp. 1602–1606, doi: 10.1109/ICPCSI.2017.8391982.
13. V. B. Vooradi and L. Jadhav, “Ethical Hacking Techniques and its Preventive Measures for Newbies,” vol. 06, no. 06, p. 8, 2019.“Paper 5 ethical hacking 2019.pdf.” .
14. S. Mansfield-Devine, “Hiring ethical hackers: the search for the right kinds of skills,” p. 6, 2017.“Mansfield-Devine - 2017 - Hiring ethical hackers the search for the right k.pdf.” .
15. M. Imran, M. Faisal, and N. Islam, “Problems and Vulnerabilities of Ethical Hacking in Pakistan,” p. 6.
16. M. Denis, C. Zena, and T. Hayajneh, “Penetration Testing: Concepts, Attack Methods, and Defense Strategies,” p. 6.

ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/2UBJ4

17. N. Rasool, S. Khan, U. Haseeb, S. Zubair, M. waseem Iqbal, and K. Hamid, “Scrum and the Agile Procedure's Impact on Software Project Management,” Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng. Technol. Ed., vol. 42, pp. 380–392, Feb. 2023, doi: 10.17605/OSF.IO/MQW9P.

18. K. Hamid, M. waseem Iqbal, Q. Niazi, M. Arif, A. Brezulianu, and O. Geman, “Cloud Computing Network Empowered by Modern Topological Invariants,” Appl. Sci., vol. 13, p. 18, Jan. 2023, doi: 10.3390/app13031399.

19. K. Hamid, M. waseem Iqbal, and Q. Niazi, “Discovering Irregularities from Computer Networks by Topological Mapping,” Appl. Sci., vol. 12, pp. 1–16, Nov. 2022, doi: 10.3390/app122312051.

20. K. Hamid et al., “Extendable Banhatti Sombor Indicesfor Modeling Certain Computer Networks. M. W. Iqbal, M. Ameer Hamza,” Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng. Technol. Ed., vol. 41, pp. 11–2022, Nov. 2022.

21. K. Hamid, M. waseem Iqbal, M. U. Ashraf, A. Gardezi, M. Alqahtani, and M. Shafiq, “Intelligent Systems and Photovoltaic Cells Empowered Topologically by Sudoku Networks,” vol. 74, pp. 4221–4238, Nov. 2022.

22. K. Hamid, S. Bhatti, N. Hussain, M. Fatima, S. Ramzan, and M. waseem Iqbal, “Irregularity Investigation of Certain Computer Networks Empowered Security,” vol. 41, pp. 75–93, Dec. 2022, doi: 10.17605/OSF.IO/TJ6XN.

23. K. Hamid and M. waseem Iqbal, “K-Banhatti Invariants Empowered Topological Investigation of Bridge Networks,” Comput. Mater. Contin., vol. 73, Jul. 2022, doi: 10.32604/cmc.2022.030927.

24. K. Hamid, M. waseem Iqbal, M. U. Ashraf, A. Alghamdi, A. Bahadad, and K. Almarhabi, “Optimized Evaluation of Mobile Base Station by Modern Topological Invariants,” Comput. Mater. Contin., vol. 74, pp. 363–378, Sep. 2022, doi: 10.32604/cmc.2023.032271.

25. K. Hamid, H. Muhammad, M. waseem Iqbal, and S. Bhatti, “Response Surface Methodologyfor the Extraction of Polyphenol Contents and HPLC Profiling of Cucumis Satisvus Peels,” Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng. Technol. Ed., vol. 41, pp. 41–52, Oct. 2022, doi: 10.17605/OSF.IO/4YFET.

26. K. Hamid, H. Muhammad, M. Basit, M. Hamza, S. Bhatti, and M. Aqeel, Topological Analysis Empowered Bridge Network Variants by Dharwad Indices. 2022.

27. K. Hamid and M. waseem Iqbal, “Topological Evaluation of Certain Computer Networks by Contraharmonic-Quadratic Indices,” Comput. Mater. Contin., vol. 74, pp. 3795–3810, Oct. 2022, doi: 10.32604/cmc.2023.033976.

28. K. Hamid, M. waseem Iqbal, H. Muhammad, Z. Fuzail, and Z. Nazir, “ANOVA Based Usability Evaluation of Kid's Mobile APPS Empowered Learning Process,” Qingdao Daxue XuebaoGongcheng JishubanJournal Qingdao Univ. Eng. Technol. Ed., vol. 41, pp. 142–169, Jun. 2022, doi: 10.17605/OSF.IO/7FNZG.

29. T.Iftikhar, S. Zubair, M. waseem Iqbal, K. Hamid, and A. Nazir, “Cost Effective About IoT-Based Accordingly to Weather Monitoring System Development and Improve Averageof Crops,” Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng. Technol. Ed., vol. 42, pp. 123–152, Feb. 2023, doi: 10.17605/OSF.IO/TKAH8.

30. H. Riasat, S. Akram, M. Aqeel, M. waseem Iqbal, K. Hamid, and S. Rafiq, “Enhancing Software Quality Through Usability Eeperience and HCI Design Principles,” vol. 42, pp. 46–75, Feb. 2023, doi: 10.17605/OSF.IO/MFE45.