Journal of Autonomous Intelligence(2024) Volume 7 Issue 1
doi:10.32629/jai.v7i1.1246

ORIGINAL RESEARCH ARTICLE

Evaluation of the extent and demanding roles of ethical hacking in cybersecurity

Jambi Ratna Raja Kumar[1,*], D. G. Bhalke[2], Swati Nikam[3], Santoshkumar Chobe[3], Swati Khidse[4], Kiran Kale[5]

[1] *Department of Computer Engineering, Genba Sopanrao College of Engineering, Pune 411045, India*

[2] *Department of Electronics and Telecommunication, Dr. D. Y. Patil Institute Technology, Pimpri, Pune 411018, India*

[3] *Department of Computer Engineering, Pimpri Chinchwad College of Engineering and Research (PCCOE&R), Pune 412101, India*

[4] *Dr. Babasaheb Ambedkar Marathwada University, Aurangabad 431004, India*

[5] *Department of Master of Business Administration, Dr. D. Y. Patil Institute of Technology, Pune 411018, India*

*** Corresponding author:** Jambi Ratna Raja Kumar, ratnaraj.jambi@gmail.com

ABSTRACT

A permitted effort to acquire unlawful connection to computing systems, programs, or information is referred to as ethical hacking. Software developers must check for flaws, compartment focus, define needs and objectives, and create a method that makes the most of their resources. The rationale for this kind of vulnerability evaluation has a direct impact on the overall assessment's estimate. More specifically, it is known that technological gadgets are necessary to prevent computer criminals from breaking into web applications to control their operations and gain access to confidential knowledge for unintended objectives. This research study provides an analysis to determine the scope and challenging responsibilities of ethical hacking employed in cyber security. Network monitoring is a legitimate need in which authorized developers attempt to breach a company's frameworks or arrangements for the convenience of the owners to uncover security flaws. It provides information on how organizations may use computer forensics, such as vulnerability assessments using open-source devices, to safeguard their program's administrators and operations. Numerous tools have been explored for security auditing of the networks which involves Nmap, Nessus, Brutus, Acunetix, etc. As a result, safeguards were put in place to identify these flaws and protect sensitive data from cyber-attacks. Ethical hacking has a bright future for detecting system or application vulnerabilities effectively. Nevertheless, tools utilized in the cyber security field for network or computer application secrecy have some limits namely growing complexity, high cost, security measures restrictions, etc. Hence, there is a wide scope to build new cost-effective cyber secrecy tools for the enhanced secrecy of user data in real time.

Keywords: cyber; ethical; hacking; information; security

ARTICLE INFO

Received: 15 September 2023
Accepted: 18 September 2023
Available online: 28 September 2023

1. Introduction

Ethical phishing is the technique of imitating the purpose and behavior of malevolent attackers to uncover flaws and exploits in computing and communication. The phrase "ethical hackers" refers to a method of identifying flaws and weaknesses in computer and information systems by imitating the goals and behaviors of malicious hackers. It entails using computer hacker skills to identify and categorize potential flaws, as well as to close security gaps before they can be exploited. It's also known as red enrolling, interrupting examination, or entry running tests. When everything is said and done, hackers may be divided into two types: malicious hackers and

vulnerability testing, often white or yellowish cap and dark cap hackers[1–3].

An ethical programmer is a software developer who adheres to a set of ethical principles and values while designing, coding, and maintaining software applications. These principles guide their behavior and decision-making throughout the software development process. While the specific ethical principles can vary from person to person and organization to organization. For hacking to be considered ethically, the developer must get permission from the organization's owner to examine their network and attempt to identify possible safety threats. Many organizations have recently been subjected to cyber-attacks, necessitating the growing demand for skilled ethical programming that can protect their platforms[4–6]. As machines became more widely accessible at institutions, user groups expanded to transcend engineers and computing scientists to include anybody who saw the machine as a strangely versatile instrument. Although they configured the machines to conduct this keep playing, create drawings, or assist employees with the much more boring elements of their regular job, there wasn't a shortage of people who wanted to use machines and when they were accessible.

Finally, strong ethical hacker applicants are more motivated and patient than the average person. Unlike how anyone hacks into a machine in the media, unethical hacking' job takes a long time and requires a lot of patience. This is an important characteristic since criminal attackers are renowned for being incredibly meticulous and ready to examine networks for days at a time while awaiting an opening. A standard assessment might take many days of laborious, hard work. To minimize interference with operations at "live" targets or to imitate the time of an actual assault, certain elements of the assessment must be completed even outside the usual hours worked.

When penetration testers come across a technology with which they are acquainted, they will take the initiative to study it and look for flaws. Finally, staying current with the environment of computer networks necessitates ongoing training and study. The talents we've outlined may just as readily belong to a malicious hacker as they could to an application programmer. Information about your opposition's talents and strategies is critical to your effectiveness, just as it is in athletics or combat. In the world of electronic cybersecurity, the unethical hacker's work is the most difficult. Everybody may become a kidnapper, a graffiti artist, or a mugger in conventional crime. Their possible candidates are typically simple to see and tend to be restricted to a certain area. Local law administration officers must understand how cybercriminals operate or how to disrupt them. Anyone may get professional hacking tools online and use them to start breaking into networks all around the globe. Ethical hackers must understand the strategies used by malicious hackers, as well as how their operations may be recognized and stopped.

Accessibility to desktops was frequently limited due to the rising demand for machines and their continuously expensive price. Some customers would contest the security authority policies that were already established if they were denied connection to the internet. They could peer over individuals else's shoulders to gain unauthorized or payment information, examine the network for vulnerabilities that would allow them to get around the regulations, or even gain ownership of the entire network. They'd do these actions to be able to complete the applications they wanted, or simply to adjust the constraints that their computers were operating under[7].

These earliest attempts serve as excellent instances of ethical hacking. Ethical hacking has a diverse set of abilities. They should, first and most importantly, be scrupulously honest. When a network administrator is checking the protection of a company's networks, he or she may come across knowledge about the company that should have been kept private. If this knowledge is made public, genuine attackers may penetrate the networks, resulting in substantial damages. Because the systems analyst often possesses the "keys to the organization" during an examination, he or she must be allowed to maintain strict discipline over any knowledge about a subject that may be abused. Depending on the selectivity of the data gleaned throughout an appraisal, highly secured actions must be taken to make sure the safeguards of data used by penetration testers

part of individual, narrow labs with physiological cybersecurity and full breadboard walls, numerous secure online relationships, a safe to store consumer transaction logs, powerful algorithms to preserve automated outcome, and separated channels for checking[8,9].

Ethical hacking usually has advanced computing and computer abilities, as well as experience in the computing and communications industry. They may also set up and operate systems that run on the most common operating systems that are utilized on target computers. These fundamental abilities are supplemented by in-depth awareness of the equipment and applications offered by the most well-known laptop and communications gear manufacturers. It should be emphasized that a protection specialist is not always required, since strong abilities in other areas suggest a thorough awareness of how protection is managed on diverse platforms[10,11].

1.1. Security issues

Although not a capability, everybody's behavior is involved. Safety should be addressed in every information technology (IT) office education and capability. Technicians, for example, should be aware of the need for secured code. At the code levels, this facilitates the supervision of protection against roots. Recognizing the many ways in which the software might be sold off and then encircling cybersecurity is a great strategy. Secure operating concepts may be investigated by admins. Every IT department should approach everything they buy, do, and implement from a cybersecurity standpoint. Developing a deep specialty area competency is a prerequisite for nascent defense professionals[12].

1.1.1. Networking security issues

The most serious concern is network safety. Hacking takes data from people, companies, and governments. Nation-states engage in digital espionage by hacking into the equipment of other countries.

1.1.2. Cloud computing security challenges

Many network technology vulnerabilities exist among application service providers (ASPs), cloud service providers (CSPs), internet service providers (ISPs), and customers confidence boundaries in the area of cloud services. Cloud technology and the online, such as servers and programs (Google Docs) and computers via the internet (Amazon EC3), must be protected.

1.1.3. Problems with online storage and backup

Cybersecurity breaches occur in every aspect of data operations. Even smart apps (Android) have had their encryption breached and are being targeted by Trojans. In multi-organizational governance, governance, privacy, and quality of the service challenges must be handled. Separating of monitoring and information surfaces helps address the security problem.

1.1.4. Venture security

Venture security is perplexing and ever-evolving. The cost of protection should be considered not only in terms of the break-in scenario but also in terms of the organization's advanced guidance. Organizations' insatiable need to communicate with their customers, agents, investors, and other partners through innovative technology comes with an inherent security risk. The costs of security are also brought into its domain by the objectives of these sophisticated structures. The investigation arises as a typical development in the way of thinking for allocating expenditures to safety because there are no genuine protection occurrences once every day. It's an apparent explanation for the existence of protection features such as seat belts and a protecting hat. There are also a variety of encryption approaches used in various sectors such as transportation, fabrication, and so on[13]. When private information is considered in conjunction with the sophisticated approach that the firm has imagined, it becomes a part of the enterprise. Safety will no longer be an afterthought in the future[14].

1.2. Security tools

Overall, security technologies are crucial for guaranteeing the trustworthiness, conformity, as well as confidentiality of business IT infrastructures[15]. Through utilizing such strategies, businesses may lessen interruptions, defend against cyber-attacks, as well as guarantee the security and overall dependability associated with their networks and infrastructure[16]. Computer firewalls, antivirus programs, along intruder monitoring devices are examples of cybersecurity solutions that may aid in preventing invasions along with information losses[17,18]. Computers may be kept functioning properly by using instruments like system surveillance programs, which can assist in spotting concerns early on before they turn into serious ones. Numerous cybersecurity products are made to assist firms in adhering to laws as well as guidelines including U.S. Federal law; Health Insurance Portability and Accountability Act (HIPAA), Payment card industry data; Data Security Standard (DSS), as well as European Union (EU) regulation: General Data Protection Regulation (GDPR), etc.[19,20].

In the area of IT system protection, reproducibility as well as generalizability constitute essential ideas. Reproducibility means that individuals may confidently confirm as well as expand upon one another's work, whereas generalizability means that an instrument can be used in a variety of settings as well as circumstances. To assure computing repeatability, a variety of instruments and methodologies can be utilized[21,22]. **Figure 1** shows the different security tools. We must safeguard our IT environments using the best accessible tools. Every business should take protection extremely carefully. Hacker's assaults are common, and they harm organizations of all levels.

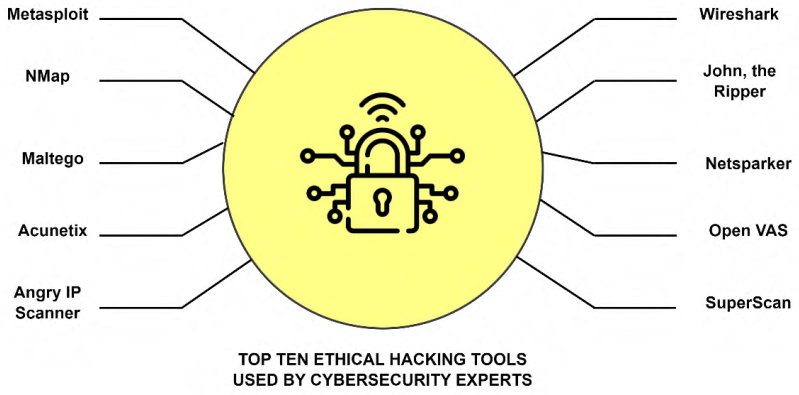

Figure 1. Shows the diverse security tools[shine].

1.3. Challenges for Chief Information Security Officers (CISOs)

Transparency of the essential IT protection expenditure plans isn't a challenge for CISOs in the face of growing digitalization. The exam is whether or not you understand why a certain protection device is useful. Many cybersecurity specialists cannot see a problem, comprehend it, and then apply the appropriate viewpoint to find a solution. Denying the reality that a firewall has already been installed, an intrusion prevention system (IPS) is essentially necessary for some serious systems attacks[23]. The protection professionals should have a thorough understanding of the protection elements and requirements to observe how the intrusions are carried out, identified, captured, and then remedied. Regrettably, this understanding is lacking in a few organizations that lack the necessary admission examination to get to the root of the problem. The concerns are fully grasped, and an almost foolproof organizational plan is presented. The development is a result of the recent wave of payment-processing-related attacks, as well as the looming hazards that lurk as cybercriminals become more figured out[24,25].

1.4. Use of machine learning

Both hackers (to get access to secret data) and ethical engineers (to locate and assess flaws in an institution's technologies) have become increasingly reliant on entry tests. **Figure 2** shows the proposed procedure for ethical hacking. The vulnerability scanning approach breaks apart the goal clearly at first. The organization, its strengths and weaknesses, its ability to respond to the unexpected, and any other information needed to plan and execute the attack are collected. The information is gathered mostly from the organization itself, as well as from available sources. The inspection technique then starts with the website or infrastructure for weaknesses and flaws that may be exploited later for the targeted attack[26].

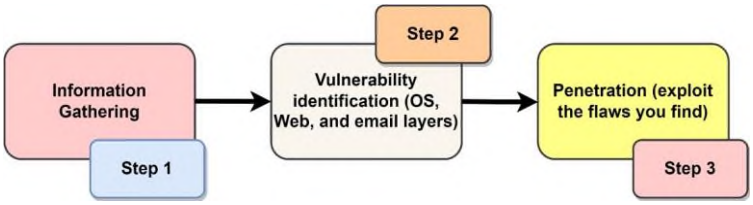

Figure 2. The above figure shows the proposed procedure for ethical hacking.

Data assembly is the focus of footprinting, which is both passive and proactive. Associated foot stamping involves examining the institution's website, but dynamic data collecting is phoning the help work area and attempting to socially develop them out of preferred data. Tapping computers, determining network domains, and port testing unique foundations are all part of the screening process. The foot fingerprinting and verifying data collection projects are quite important. A good data social gathering may be the difference between a successful pen test and one that fails to provide the client the most overwhelming advantage. Most businesses nowadays have an incredible amount of data available to them. This information is available on the organization's website, in exchange documents, on newsgroups, on income websites, and even from disgruntled employees[27].

1.5. Contributions of the study

This research study made the below-mentioned core contributions in the field of ethical hacking and cyber security.

- To investigate the recent trends and methodologies used for vulnerability detection in the arena of cyber security.
- To explore the machine learning-based models utilized for the cyber security and prevention of information breaches.
- To investigate recent research on diverse security tools adapted for cyber security.
- To provide an in-depth analysis of security threats and challenges in the field of IT business environment and mitigation scope using novel cyber security approaches.
- To discuss the ethical hacking core applications in cybersecurity.
- At last, to provide a future research direction for exploring the optimal solution of data breaches using the ethical hacking

2. Methodology

This systematic literature review is based on a Preferred Reporting Items for Systematic Reviews and Meta-Analyses, (PRISMA). This methodology has been opted for filtering the most appropriate literature based on the ethical hacking importance in the cyber security arena. The PRISMA meta-analysis serves as a guide for writers who want to describe their research methods, and findings, including plans. Furthermore, an instrument that could be employed to direct systematic assessment findings involves the PRISMA questionnaire. **Figure 3** depicts the proposed PRISMA methodology for studies inclusion and exclusion in this

research. This PRISMA meta-analysis is rooted in distinct four core steps which involve the identification of the articles, screening of the explored literature, eligibility criteria, and inclusion of the article in the literature review. Initially, there have been collected total of 1024 research and review articles through Google Scholar, Research Gate, Science Direct, Springer, conference proceedings, etc. Furthermore, 255 records are identified from other sources such as websites and many others. In the first screening of all collected records, duplicates of 651 screened records have been eliminated and a total of 628 papers are screened articles have been chosen. After that total of 530 records were excluded based on context research and a total of 98 papers were. At last, 68 research articles are eliminated based on the publication years. In this PRISMA meta-analysis, a total of 30 papers have been included which were published after 2010 for the latest research analysis in the field of cyber-security. **Figure 4** depicts the ratio of the searched studies from multiple sources. During the research, there has been chosen multiple databases for search queries were chosen to get studies in the field of ethical hacking roles and the importance in the field of cyber-security for improving user data and confidential information. In this study, many types of studies were considered which involved 54% research papers, 20% of review papers, 9% of book chapters, 10 conference proceedings, and 7% from other sources such as official websites.

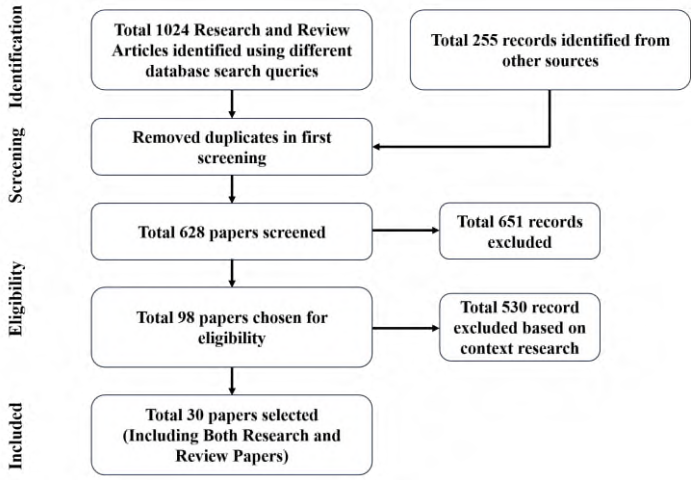

Figure 3. Depicts proposed PRISMA methodology for studies inclusion and exclusion in this research.

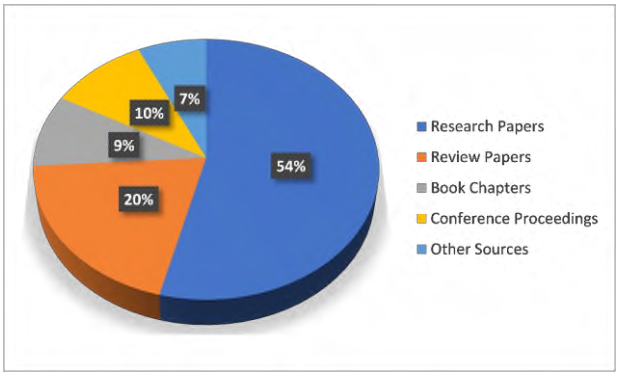

Figure 4. Depicts the ratio of the searched studies from multiple sources.

The studies are identified by using multiple keywords in context to the cyber security and ethical hacking along with (AND), or (OR), operators on distinct databases namely the Springer, Science Direct, Google Scholar, Research Gate, and many more. For instance, we have used the following search queries for the identification of the relevant articles for this survey, ("ethical hacking role in cyber security")[20] or ("cyber security using machine learning")[24], ("machine learning")[24] and ("cyber security vulnerability classification")[26], etc. **Figure 5** depicts the search queries used on Google Scholar for identification of the relevant literature.

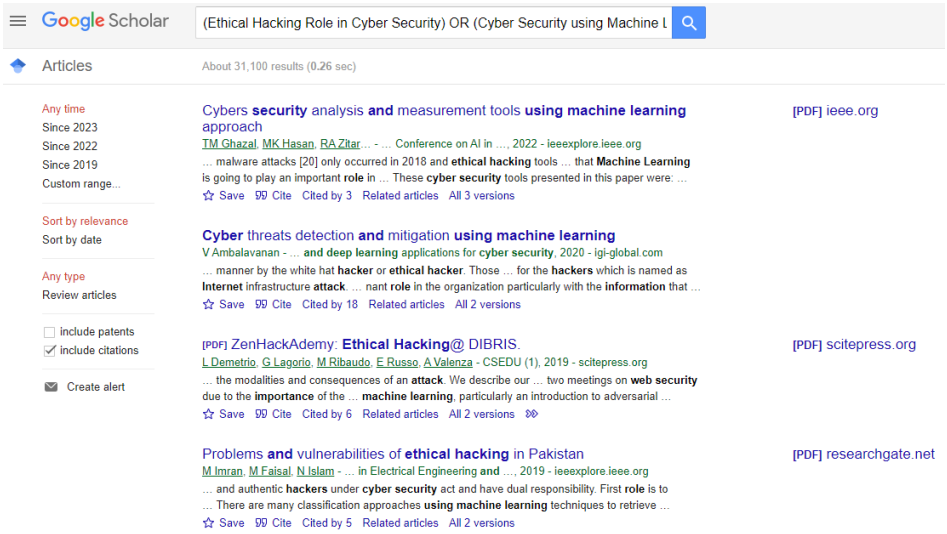

Figure 5. Depicts the search queries used on Google Scholar for identification of the relevant literature.

3. Discussion

Even though there will be well-organized techniques for information gathering, network monitoring is mostly a disclosure method. Kali Linux is continually evolving, with more features becoming included in the platform regularly, making it one of the top vulnerability tester programs. Incursion monitoring is an approach for screening in which flaws in commercial foundations in terms of protection are discovered and exploited by moral programming or vulnerability inspectors for companies, services, or networking[28]. The core steps are discussed as follows:

Step 1: It starts with a list of privacy flaws or probable problem regions that might result in a privacy breach for the platform.

Step 2: If at all possible, this list of goods is arranged in the direction of necessity/criticality.

Step 3: Develop penetration procedures that operate (attack your frameworks) from both within the institution or exterior (wirelessly) to determine if you can access unauthorized information/arrangement/server/site.

Step 4: If unauthorized access is possible, the frameworks must be changed and the sequence of procedures must be restarted unless the problem area is resolved.

Powerlessness analysis is not similar to pentesting. Vulnerability testing's goal is to identify possible flaws, while pen-goal testing's is to attack such weaknesses. Penetration testing follows the ethical hacking technique of combined fingerprint verification and verifying steps. Using Nmap, one of the main goals of this step was to gather knowledge about the target web page. Nmap was used to conduct a networking assessment and gather information on addresses, channels, host operating methods, and networking architectures. All of the domains on the system, as well as all of the equipment attached to the system (PCs, servers, and routers), were known at first. Additional examination of each remote host revealed the need for more data concerning the dedicated server computer and, as a result, the indigenous computer searches were directed towards these two servers to gather more information such as sequence identifiers, algorithms, and hence the functions they were executing. By gaining this additional information, the chances of network flaws being found in the subsequent section of this penetration test increased. Nmap ("network mapper") is an internet backbone detection and information security tool that is free and public source (license). It's also useful for jobs like following options, controlling program update timetables, and monitoring hosts or contract length periods, according to various operations and electronic administrators[29].

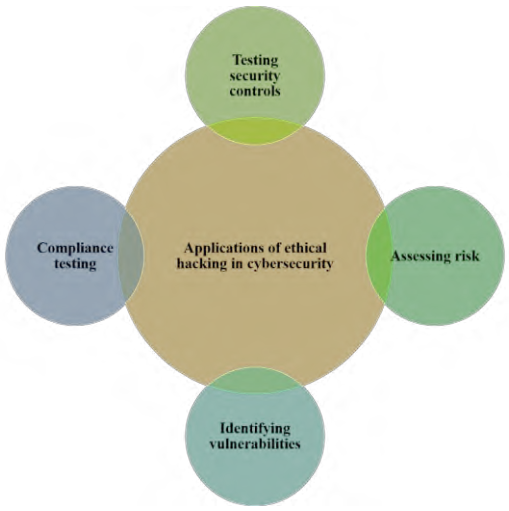

Figure 6. Depicts the ethical hacking core applications in cybersecurity.

Figure 6 depicts the ethical hacking core applications in cybersecurity. To uncover prospective breaches of information as well as networking risks, ethical hacking describes a legitimate method that involves finding flaws within a program, framework, or company's network as well as getting beyond the safety of the system. To find vulnerabilities that malevolent attackers may take advantage of or eliminate; ethical hackers search the systems effectively. To find out how to make the machine, infrastructure, and apps more secure, they gather as well as examine the data. They can strengthen the defensive imprint in this way to adequately fend off assaults or reroute things.

A computing machine or network may have weaknesses that unethical hackers might utilize against it. These flaws are frequently found through the practice of ethical hacking. IT companies can take action to repair these weaknesses as well as strengthen their overall safety record by discovering issues. The efficacy of privacy measures like firewalls, invasion monitoring platforms, and antivirus programs might be evaluated through ethical hacking. IT companies may accomplish this to make sure existing safety mechanisms are operating as planned. The entire danger to the information systems of a company could be evaluated via ethical hacking[30]. Corporations may initiate action to reduce hazards while improving their overall protection by detecting possible vulnerabilities as well as faults. A company's adherence to laws and guidelines like HIPAA, DSS, as well as GDPR is capable of being tested through ethical hacking. IT companies may be certain they are fulfilling their statutory under the law as well as regulations through doing this. In summary, ethical hacking helps firms find weaknesses, evaluate security measures, evaluate hazards, as well as assure compliance with laws as well as guidelines, all of which are critical aspects of cybersecurity.

4. Conclusion

The author has concluded the analysis to determine the scope and challenging responsibilities of ethical hacking employed in cyber security. Ethical hacking will be used by the firms to identify possible protection faults and exploits in their corporate networks. It's possible to put procedures in motion to remedy issues after they've been identified. It was also revealed that using various free methodologies increases the likelihood of detecting networking weaknesses and, by doing so, prevents a malevolent attacker from gaining access to important and secret information. Vulnerability testing was used to see whether any of the documented flaws might be attacked by malevolent attackers. This might include breaking into the patient's infrastructure and attempting to escalate permissions in the manner of a black-hat hacker. Small firms with slightly budgets will be able to handle better realistic computer networks by using freely downloadable solutions. This study investigates the recent methodologies used for vulnerability detection in the arena of cyber security and diverse security tools adapted for cyber security. Also, the research study provides an in-depth analysis to the readers

regarding the security threats and challenges in the field of IT business environment and mitigation scope using novel cyber security approaches. We may argue that the data gathered from the penetrating test enabled a company to improve its computer protection and prevent unwanted entry by black-hat criminals through cyber assaults. As a result, free open-source programming is often used to improve the safety of enterprises' platforms and to strengthen their cyberspace defense protocols. The future scope of ethical hacking is very bright for exploring the optimal solutions of data breaches using ethical hacking in the sector of IT business environment.

Author contributions

Conceptualization JRRK and DGB; methodology, JRRK; software, JRRK; validation, DGB, SN and SK; formal analysis, JRRK; investigation, JRRK; resources, DGB; data curation, KK; writing—original draft preparation, JRRK; writing—review and editing, SK; visualization, SK; supervision, JRK; project administration, JRRK; funding acquisition, JRRK. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Yadav K, Agrawal R. Ethical hacking and web security: Approach interpretation. In: Proceedings of the 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS); 23–25 February 2022; Coimbatore, India. pp. 1382–1384.
2. Hartley R, Medlin D, Houlik Z. Ethical hacking: Educating future cybersecurity professionals. In: Proceedings of the 2017 EDSIG Conference; Austin, Texas, USA. pp. 1–9.
3. Hartley RD. Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management* 2015; 24(4): 95–104. doi: 10.58729/1941-6679.1055
4. Omoyiola BO. The legality of ethical hacking. *IOSR Journal of Computer Engineering (IOSR-JCE)* 2018; 20(1): 61–63. doi: 10.9790/0661-2001016163
5. Utomo GA. Ethical hacking. *Cyber Security dan Forensik Digital* 2019; 2(1): 8–15.doi: 10.14421/csecurity.2019.2.1.1418
6. Vignesh R, Rohini K. Analysis to determine the scope and challenging responsibilities of ethical hacking employed in cyber security. *International Journal of Engineering & Technology* 2018; 7(3): 196–199.doi: 10.14419/ijet.v7i3.27.17759
7. Georg T, Oliver B, Gregory L. Issues of implied trust in ethical hacking. *The ORBIT Journal* 2018; 2(1): 1–19.doi: 10.29297/orbit.v2i1.77
8. Chowdappa KB, Lakshmi SS, Pavan Kumar PNVS. Ethical hacking techniques with penetration testing. *International Journal of Computer Science and Information Technologies* 2014; 5(3); 3389–3393.
9. Palmer CC. Ethical hacking. *IBM Systems Journal* 2001; 40(3): 769–780.doi: 10.1147/sj.403.0769
10. Munjal MN. Ethical hacking: An impact on society. *Cyber Times International Journal of Technology &Managemen* 2013; 7(1): 922–931.
11. Wang Y, McCoey M, Hu Q. Developing an undergraduate course curriculum for ethical hacking. In: Proceedings of the 21st Annual Conference on Information Technology Education; 7–9 October 2020; USA. pp. 330–335.
12. Trabelsi Z, McCoey M. Ethical hacking in information security curricula. *International Journal of Information and Communication Technology Education* 2016; 12(1): 1–10.doi: 10.4018/IJICTE.2016010101
13. Cisar P, Pinter R. Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical Educational Sciences* 2019; 9(4): 129–149. doi: 10.24368/jates.v9i4.139
14. Sarumi JA, Ogunjimi OLA, Adekunle YA, Ebiesuwa S. Ethical hacking and cyber security in nigerian telecommunication industry. Available online: https://www.academia.edu/84127841/Ethical_Hacking_and_Cyber_Security_in_Nigerian_Telecommunication_Industry (accessed on 15 September 2023).
15. Gandhi F, Pansaniya D, Naik PS. Ethical hacking: Types of hackers, cyber attacks and security. *International Research Journal of Innovations in Engineering and Technology (IRJIET)* 2022; 6(1): 28–32. doi: 10.47001/IRJIET/2022.601007
16. Del-Real C, Mesa MJR. From black to white: The regulation of ethical hacking in Spain. *Information & Communications Technology Law* 2022; 32(2): 207–239.doi: 10.1080/13600834.2022.2132595

17. Malik N. A study on different software used to perform cyber crime. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)* 2021; 9(XII): 879–882. doi: 10.22214/ijraset.2021.39395
18. Rathore N. Ethical hacking and security against cyber crime. *i-manager's Journal on Information Technology* 2016; 5(1): 13–17. doi: 10.26634/jit.5.1.4796
19. Patil S, Jangra A, BhaleM, et al. Ethical hacking: The need for cyber security. In: Proceedings of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI); 21–22 September 2017; Chennai, India. pp. 1602–1606.
20. Reddy PH. Cyber security and ethical hacking. *International Journal for Research in Applied Science and Engineering Technology* 2018. doi: 10.22214/ijraset.2018.6261
21. Sahu IK. Ethical hacking: The need for cyber security.*International Journal of Scientific Research and Management* 2023; 7(1); 1–3. doi: 10.55041/ijsrem17502
22. Al-Hawamleh AM, Alorfi ASM, Al-Gaswneh JA, Al-Rawashdeh G. Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology* 2020; 63(5).
23. Berger H, Jones A. Cyber security & ethical hacking for SMEs. In: Proceedings of the 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society; 25–28 July 2016; Hagen, Germany. pp. 1–6.
24. Mathoosoothenen VN, Sundaram JS, Palanichamy RA, Brohi SN. An integrated real-time simulated ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform. In: Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence; 5–7 December 2017; Jakarta, Indonesia. pp. 199–202.
25. Heiding F, Lagerström R. Ethical principles for designing responsible offensive cyber security training. In: Friedewald M, Schiffner S, Krenn S (editors). *Privacy and Identity Management*. Springer; 2021.
26. Yaacoub JPA, Noura HN, Salman O, Chehab A. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems* 2023; 3: 280–308. doi: 10.1016/j.iotcps.2023.04.002
27. Swathi S, Smitha G. The basic of hacking. *International Journal of Scientific Research in Engineering and Management* 2022; 6(6). doi: 10.55041/ijsrem14218
28. Pushpa CM, Udaya Lakshmi KVM, Hepsibha S. Ethical hacking: Roles, phases and impact on various sectors of the economy. *International Journal of Scientific Research in Computer Science Engineering and Information Technology* 2021; 7(6): 38–43. doi: 10.32628/cseit21765
29. Pattison J. From defence to offence: The ethics of private cybersecurity. *European Journal of International Security* 2020; 5(2): 233–254. doi: 10.1017/eis.2020.6
30. Okereafor K, Manny P. Understanding cybersecurity challenges of telecommunting and video conferencing applications in the COVID-19 pandemic. *International Journal in IT & Engineering* 2020; 8(6): 13–23. doi: 10.6084/m9.figshare.12421049