2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) | 979-8-3503-2579-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAISS58487.2023.10250659

Review on Penetration Testing Techniques in Cyber security

Masrath Parveen
Department of Information Technology
Vidya Jyothi Institute of Technology
Hyderabad, Telangana State, India
masrath19@gmail.com

Mohammed Ali Shaik
School of Computer Science &
Artificial Intelligence
SR University
Warangal, Telangana State, India
niharali@gmail.com

Abstract—**Organizations of all sizes and sectors are increasingly conducting penetration tests as a preventative step to discover and mitigate potential vulnerabilities as cyber threats continue to emerge. With a focus on penetration testing's function in cyber security, this research seeks to provide a thorough review of the practice and its numerous methodologies. The purpose is to first present the idea of penetration testing, its goals, and its applicability to contemporary cyber security. It then goes on to investigate some of the most popular penetration testing techniques, such as network scanning, vulnerability scanning, and exploitation. The paper concluded by emphasizing some of the difficulties and restrictions related to penetration testing and outlining potential future research topics. Overall, the useful resources for organizations seeking to learn concerning how penetration testing fits into the range of cyber security options.**

Keywords—Penetration Testing, Cyber Security, Cyber Threats, Vulnerabilities, Ethical Hacking

I. INTRODUCTION

Penetration testing, commonly referred to as ethical hacking, is a thorough security evaluation procedure that simulates an assault on a computer system or network. Penetration testing, in contrast to malicious hacking, is carried out with the consent and approval of an organisation or business under the terms of a written contract. The major goal is to locate systemic flaws and vulnerabilities so that the data of the organization is kept secure.

Penetration testing comprises knowledgeable and experienced testers carefully probing the system for potential flaws. They replicate actual assaults using a variety of techniques, tools, and procedures, hoping to find any potential vulnerability. These testers assist organizations in understanding their security posture and identifying areas that need attention by imitating the actions of malicious actors.

In penetration testing, confidentiality is essential. The vulnerabilities and information found during the evaluation are classified as being extremely sensitive and are not shared until all problems have been fully resolved. This guarantees that the company can respond proactively to address any weaknesses, lowering the likelihood of a successful breach.

Penetration testing used to be mostly done manually, which required a knowledgeable team to carefully explore the system, find vulnerabilities, and evaluate their potential consequences. The need for an actual presence and extensive human interaction makes this technique time- and money-consuming.

As an alternative, organizations can choose automatic penetration testing, which provides a quicker and more effective means to carry out thorough evaluations. To do numerous penetration testing activities, automated tools and technologies are used, which saves time and resources. The process can be further streamlined by reusing the parameters from earlier testing.

Automated penetration testing has a number of benefits, including greater effectiveness, reduced cost, and scalability. It's crucial to remember nevertheless that manual testing shouldn't be fully replaced. In order to find complicated vulnerabilities that automated tools may miss, professional testers' skills and critical thinking are still useful.

Penetration testing ultimately acts as a preventative measure to improve data security. Organizations can detect and fix vulnerabilities by routinely carrying out these evaluations, assuring the creation of a safe system that complies with their particular needs.

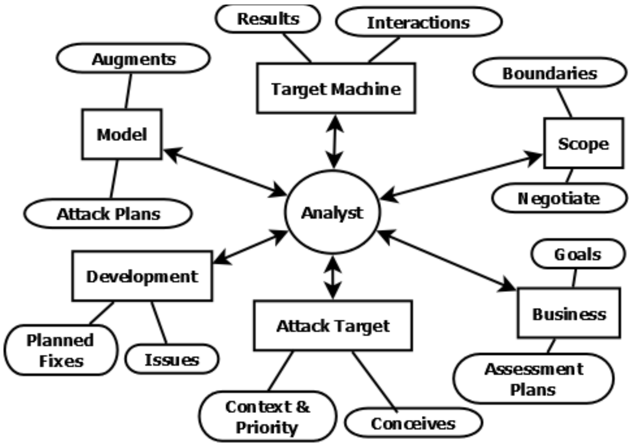

Fig. 1. Components of Penetration Testing

As shown in Figure 1 goals of a pen test are specified to testers along with varying degrees of information to reach to target system. In some cases, the pen testing team which fixes one approach initially and sticks with it to evolve its strategies as an awareness to the system that enhances during the pen test.

II. Literature Survey

A proactive security assessment procedure called penetration testing involves simulating an actual attack on a company's network, systems, applications, or physical infrastructure. Penetration testing's goal is to locate any potential flaws and holes in the organization's security framework and to offer workable remedies to reduce the risks involved. In this review of the literature, we will look at a variety of papers and articles that talk about penetration testing and its methods in relation to cyber security.

A penetration testing methodology that incorporates network scanning, vulnerability scanning, and exploitation techniques is proposed in the Reference [1] study. The authors stress the need for efficient communication between testers and stakeholders as well as the significance of comprehending the target system and its surroundings.

A survey is suggested in the reference [2] research to give a general understanding of the technological problems and techniques involved in penetration testing. The writers talk on the difficulties and constraints of penetration testing as well as numerous penetration testing methodologies, such as network scanning, vulnerability scanning, and exploitation.

Reference [3] research suggests comparing Nmap, Nessus, and Metasploit, three well-known penetration testing tools. The writers assess the usefulness and efficacy of these tools and make suggestions for how to use them in various situations.

In the context of cyber security, the reference [4] study suggests and explores the value of penetration testing. The authors stress the importance of efficient communication and cooperation between security teams and other stakeholders in the organisation, as well as the advantages of penetration testing, such as discovering vulnerabilities and enhancing overall security posture.

A detailed manual for penetration testing, including methods for testing websites, mobile applications, and APIs, is offered in the Reference [5] study. The authors present real-world examples and case studies that illustrate how to use the various tools and procedures used in penetration testing.

Reference [6] study proposes risks compromises of security over critical data, organisations have the greatest problem in protecting their web applications from the quickly growing cyber threats. Organisations may benefit from using vulnerability assessment and penetration testing methodologies to identify security gaps. If the organisations are unaware of this, the flaw could become an advantage for the attacker. An organisation can close security gaps and establish whether or not its security measures are effective by doing vulnerability assessments and penetration testing. Installing security patches is vital to hide the trails and lessen dangers.tools used to identify the vulnerabilities in order to protect organisations from cyber threats.

Reference [7] study proposes how to lessen the impact of expertise and knowledge on the outcomes of a pen test, it offers suggestions for assisting penetration testers. During the design phase, our objective is to produce attack pathways and test cases based on a software architecture. Once the system has been fully developed, pen testers can use the attack pathways and test cases to help them perform testing on the system under test (SUT).

Reference [8] study proposes aims to prevent unauthorised use of such assets. By taking advantage of already-existing weaknesses and software faults, attackers break into systems using automated tools and human tactics. Attack tactics, vulnerability ideas, and defence strategies need to be thoroughly studied in order to provide adequate security. This study's major goal is to demonstrate that current software programme and operating system (OS) vulnerabilities are not entirely fixed by recently released patches. A better outcome could be achieved by creating tailored patches for each organisation and repairing software flaws by being aware of the software installed on each individual system.

Reference [9] study proposes proposed “Long Short-Term Memory Recurrent Neural Network-Enabled Vulnerability Identification (LSTM-EVI)”, a framework for penetration testing based on deep learning. The framework is utilized through a cutting-edge cybersecurity testbed built in a smart airport with both physical and virtual components. This testbed as well as real-time data sources were used to evaluate the framework.

The list of attacks handled through Penetration Testing Techniques in Cyber security are: 1) Network Penetration Testing 2) Web Application Penetration Testing 3) Wireless Network Penetration Testing 4) Social Engineering Penetration Testing 5) Database Penetration Testing 6) Mobile Application Penetration Testing 7) Cloud Computing Penetration Testing 8) Email Security and Spam Filtering Penetration Testing 9) Malware Analysis and Reverse Engineering 10) Physical Security Assessment [6].

The reference [10] study suggests using the open source network attack simulator NASim to examine the effectiveness of RL-based penetration testers. To assess the effectiveness of various network improvements at deterring attackers, the process quantifies time required to relearn. The discover process will simultaneously weaken the performance of several adversaries by concentrating on altering the learning domain as a defensive tactic.

A. History

Penetration testing, commonly referred to as ethical hacking, has a long history. It got its start in the 1960s when the US government examined its computer systems for vulnerabilities. The first commercial penetration testing tools, which specialised in finding gaps in network security, initially appeared in the 1970s.

As computer networks grew in the 1980s, penetration testing became more popular in both the business and public sectors. In response to the new problems presented by the internet in the 1990s, penetration testing expanded to encompass evaluations of the security of web applications.

Cyberattacks surged dramatically in the early 2000s, which raised demand for penetration testing services. Penetration testing has expanded as a result of industry standards and frameworks like the “Payment Card Industry Data Security Standard (PCI DSS)”.

New testing approaches, such red teaming and continuous security testing, were created in the 2010s as a result of technological advancements and the popularity of cloud computing. Penetration testing became an essential part of organisational security programmes due to legal and regulatory constraints, including the “General Data Protection Regulation (GDPR)”.

Penetration testing is become a crucial component of cybersecurity plans. Employing trained individuals to evaluate the vulnerabilities in their systems, spot flaws, and offer suggestions for improvement is common practise across many industries. The industry is still developing along with new technology to maintain the security of sensitive data and digital assets.

A penetration test, commonly referred to as pen testing, simulates a cyberattack on a computer system, network, or online application in order to assess the system's security. It is carried out to find security holes that an attacker could use to access sensitive data or systems. A penetration test's objectives are to evaluate the likelihood of a malicious attack and locate any holes in the system's defences.

B. *Applications*

Systems, apps, networks, and devices can all have vulnerabilities that can be found by penetration testing. Its main objective is to replicate a real-world attack scenario and asses the resilience of an organization's defences. Penetration testing is frequently used for the following purposes [11]:

- Network penetration testing: In this type of testing, the network infrastructure security of an organisation is examined to find any holes that a hacker could exploit.
- Web application penetration testing: This entails examining the security of web applications to find flaws like SQL injection, buffer overflow, and cross-site scripting (XSS), as well as LFI (Local File Inclusion).
- Wireless network penetration testing: In this testing, wireless networks' security is examined by employing wireless network hacking techniques to find gaps that online criminals might exploit.
- Social engineering penetration testing: This entails assessing how vulnerable employees are to social engineering assaults, such as phishing schemes, on the part of the organisation.

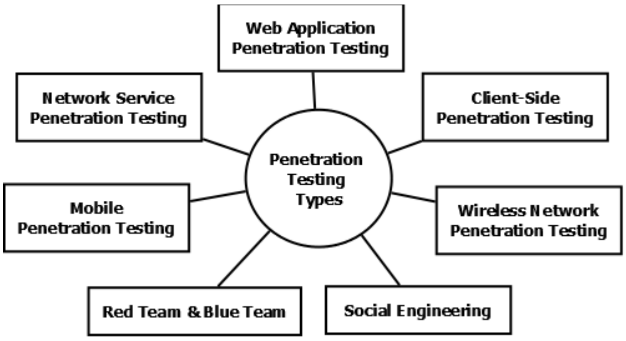
Web Application Penetration Testing
Network Service Penetration Testing
Client-Side Penetration Testing
Penetration Testing Types
Mobile Penetration Testing
Wireless Network Penetration Testing
Red Team & Blue Team
Social Engineering

Fig. 2. Types of Penetration Testing

C. *Technology used in Penetration Testing*

Penetration testing utilizes a variety of technologies to assess the security of systems and identify vulnerabilities. Here are some common technologies used in penetration testing [12]:

- Vulnerability Scanners: Networks, systems, and applications are automatically scanned for known vulnerabilities using vulnerability scanning tools like Nessus, OpenVAS, and Qualys. These programmes generate a report of potential weaknesses by comparing the software and system settings to a database of known vulnerabilities.
- Exploitation Frameworks: Frameworks like Metasploit give users access to a library of ready-made payloads, exploits, and support modules. These frameworks aid penetration testers in the controlled identification and exploitation of vulnerabilities. In order to evaluate the security of systems, they provide a variety of approaches and automated scripts.
- Password Cracking programmes: By attempting to decipher hashed or encrypted credentials, password cracking programmes like John the Ripper and Hashcat are used to test the security of passwords. To break weak or obvious passwords, these programmes use methods including dictionary attacks, brute force attacks, and rainbow table lookups.
- Network Scanners: To discover and map the network, find open ports, and gather details about network services and devices, network scanning programmes like Nmap and Netcat are utilised. These tools aid testers in comprehending the network architecture and potential exploitation sites.
- Web Application Testing Tools: Tools such as Burp Suite, OWASP ZAP, and Acunetix are made expressly for assessing the security of web applications. They help in the detection of security flaws including SQL injection, XSS, and insecure direct object references (IDOR). These programmes offer features such web application exploitation, crawling, scanning, and proxying.
- Wireless Network Security Assessment Tools: Kismet and Aircrackng are two programmes that are used to evaluate the security of wireless networks. They help with Wi-Fi network detection, network traffic analysis, breaking WEP and WPA/WPA2 encryption, and rogue access point detection.
- Forensic Tools: In penetration testing, forensic tools like EnCase and Sleuth Kit are used to collect and examine digital evidence. These tools help in the analysis of compromised systems, the retrieval of artefacts, and the assessment of an attack's scope.
- Social Engineering Tools: To simulate phishing attacks, produce malicious payloads, and run social engineering campaigns, social engineering tools like the SET (Social-Engineer Toolkit) are used. These instruments aid in determining how vulnerable a company is to assaults centred on people.

D. *Techniques for penetration testing:*

- Reconnaissance: This tactic entails gathering knowledge about the target network or system. It includes passive methods like scanning websites, network configuration analysis, and public information search. To acquire more particular information, active approaches may be used, such as port scanning, DNS enumeration, or social engineering.

- Vulnerability Scanning: To detect known vulnerabilities in a target system or network, vulnerability scanning employs automated tools or scripts. These tools generate a report on any potential weaknesses by comparing the system setup and installed software against a database of known vulnerabilities.
- Password Cracking: To evaluate the security of user passwords within the system, password cracking techniques are used. This can involve using brute-force assaults, dictionary attacks, or rainbow tables to break weak or understandable passwords.
- Exploitation: In this technique, an attacker attempts to use a known vulnerability to break into the system. A variety of techniques, including buffer overflow, cross-site scripting, SQL injection, or remote code execution, are used by skilled penetration testers to exploit flaws and take over the target system.
- Social engineering: Techniques for manipulating employees to get confidential information or acquire unauthorised access are known as social engineering. In order to take advantage of human weaknesses, this can involve strategies like phishing emails, impersonation, or physical manipulation.
- Wireless Network Testing: To find gaps in Wi-Fi security, penetration testers may concentrate on wireless networks. To evaluate the security of wireless networks, they can use strategies such as war driving, rogue access point detection, or Wi-Fi encryption cracking.
- Web application testing involves assessing the security of websites or web-based applications. This involves discovering widespread online application vulnerabilities such insecure direct object references (IDOR), cross-site scripting, SQL injection, and cross-site request spoofing.
- Post-Exploitation: Once a system has been breached, post-exploitation techniques are utilised to extend control over the compromised environment and preserve persistence. This could entail data exfiltration, privilege escalation, or lateral movement.

E. *Penetration Testing Steps*

- Information collecting: Information gathering and reconnaissance are the first steps in penetration testing. The goal of this step is to learn as much as you can about the intended system or organisation. It covers things like network mapping, social engineering, and “open-source intelligence (OSINT)” research. A variety of tools and procedures are used by skilled testers to gather data about the infrastructure, personnel, security measures, and potential vulnerabilities of the target. The tester can organise their attack and find prospective entry points by comprehending the target's environment.
- Scanning and discovery: The penetration tester enters the scanning and discovery phase when the reconnaissance phase is finished. In this step, the target's network or systems are actively scanned for flaws and vulnerabilities. To find open ports, services, and potential entry points, tools like network mappers, vulnerability scanners, and port scanners are used. Finding exploitable flaws that could be used to gain unauthorised access or increase privileges on the target system is the aim.

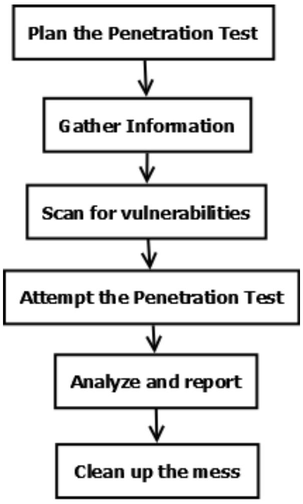

Fig. 3. Penetration Testing Process

- Attack and getting access: After identifying the system's vulnerabilities, the pen testers use security weaknesses to break into the infrastructure. They then try to exploit the system even more by giving themselves more access to the intended environment. Using the Metasploit programme, the attacker makes an effort to exploit the flaw.
- Maintaining access and penetration: The penetration tester proceeds to exploit vulnerabilities found in order to get access to the target system or network. This stage focuses on getting around security measures, using software flaws, or taking advantage of configuration errors. The tester seeks to maintain persistence and increase privileges after they get access in order to mimic a real-world attack. Various hacking methods, including as privilege escalation, lateral movement, and post-exploitation activities, are used in this step.
- Risk analysis and reporting: Following the completion of the penetration testing tasks, the tester conducts a thorough risk analysis and creates a thorough report. This entails recording the vulnerabilities found, their potential consequences, and the suggested corrective actions. The study offers insightful information about the target organization's security posture, including its strengths, shortcomings, and potential growth areas. This improves the organization's overall security posture by allowing them to efficiently prioritise and address the risks that have been discovered. In order to reduce potential vulnerabilities, the study may also

make suggestions for security measures, policy improvements, and employee training.

F. *Penetration Testing Tools*

- According to this tool, Wireshark is the most widely used network protocol analyzer. It is a packet scanner that is preinstalled on Kali Linux and is available for independent usage or download as a package for a number of operating systems. It is employed to look at network traffic, especially traffic involving TCP or UDP protocols.

- Nmap: Network Mapper is another name for Nmap. Users can find and examine network hosts and services using this robust open-source network scanning tool. It offers a variety of scanning methods to learn more about the target systems. Open ports, operating systems, vulnerabilities, and network topology can all be determined using Nmap. Both TCP and UDP scanning are supported, and it provides a variety of output formats for data processing. Users of Nmap can specify scan parameters, target ranges, and timing choices, making it very flexible. It is a crucial tool for network administrators, security experts, and ethical hackers alike due to its adaptability and effectiveness. [9].

- Burp Suite is a web application security testing tool that is employed by testing experts in the industry. It provides a full range of capabilities to pinpoint weaknesses and evaluate the security of online applications. Burp Suite's user-friendly interface enables users to modify and intercept HTTP/S requests, enabling in-depth web traffic analysis. Additionally, a variety of tools like scanner, spider, intruder, and repeater are included to help find security issues. Testing approaches supported by Burp Suite include manual testing, automated scanning, and penetration testing. Its adaptability and wide range of capabilities make it a crucial weapon in the toolbox of web security experts. [10].

- Metasploit: This robust penetration testing platform is a well-known name in the cybersecurity industry. It was created by Rapid7 and offers a complete set of tools for identifying and taking advantage of holes in computer systems and networks. By making security assessments easier to complete, Metasploit enables security experts to find vulnerabilities and evaluate their defences. It gives both criminal and ethical hackers the ability to enter target systems without authorization thanks to its extensive library of pre-built exploits and payloads. A thriving community actively contributes to the ongoing development and improvement of Metasploit, which is very extensible. It's crucial to remember that it should only be used legally since if it's done so maliciously, it can cause serious harm.

- John the Ripper is a potent password-cracking tool that is employed by both security experts and hackers. It was created at the start of the 1990s and is still in widespread usage today. By employing strategies like brute force attacks, dictionary attacks, and hybrid attacks, John the Ripper is made to evaluate the robustness and security of passwords. It supports a wide variety of password hash types and can be adjusted to meet certain cracking needs. It is a go-to tool for assessing system vulnerabilities and validating the security of passwords because to its adaptability, speed, and efficiency. However, it must only be utilised ethically, legally, and with the right permission. [2] and a few of its difficulties include:

  - False positives: Penetration testing occasionally reveals false positives, in which a vulnerability is discovered but is not there, wasting time and resources.

  - Limited scope: Penetration testing is limited to the organization's designated scope, leaving other areas open to attack.

  - Legal and ethical concerns: Penetration testing may be against the law if carried out without the necessary licence. This raises both legal and ethical questions.

  - Price: Penetration testing can be costly, especially for bigger organisations with bigger networks and applications.

And some of the benefits are:

- Finding vulnerabilities: Penetration testing can identify weaknesses and vulnerabilities in an organization's software, networks, applications, and infrastructure, allowing the organisation to patch them up before they are used against them.

- Increasing cybersecurity defences: By spotting holes and addressing them, penetration testing can assist organisations in enhancing their cybersecurity defences.

- Compliance: To ensure compliance with cybersecurity regulations, regulatory organisations and industry standards frequently demand penetration testing.

- Reputation protection: By spotting weaknesses, penetration testing can help organisations maintain their goodwill.

- ROI: By averting possible cyberattacks and the costs involved, penetration testing can produce a profitable return on investment.

- Assessing incident response: Organisations can assess how successfully they can respond to a cyberattack by using penetration testing to test their incident response policies.

- Why Customer trust: By demonstrating their dedication to cybersecurity and safeguarding sensitive data, organisations can gain customers' trust through penetration testing.

III. CONCLUSION

We conclude that the penetration testing is important factor for any organization's cybersecurity strategy. It helps organizations find vulnerabilities and weakness in their systems, applications, networks, and devices, enabling them to strengthen their cybersecurity defenses. Although it faces challenges such as false positives, legal and ethical issues, and cost, the benefits of penetration testing such as identifying vulnerabilities, improving cybersecurity defenses, compliance, protecting reputation, ROI, testing incident response, and customer trust outweigh these challenges. Therefore, organizations should consider integrating penetration testing as part of their cybersecurity strategy.

REFERENCES

[1] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2018, pp. 1-7, doi: 10.1109/LISAT.2018.8378035.

[2] K. Patel, "A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 320-325, doi: 10.1109/ICOEI.2019.8862767.

[3] Mohammed Ali Shaik, MD.Riyaz Ahmed, M. Sai Ram and G. Ranadheer Reddy, (2022), "Imposing Security in the Video Surveillance", International Conference on Research in Sciences, Engineering & Technology, AIP Conf. Proc. 2418, 020012-1–020012-8; https://doi.org/10.1063/5.0081720,

[4] T. Walter, "Architectural Pen-Test Generation and Vulnerability Prediction for Cyber-Physical Systems," 2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C), Honolulu, HI, USA, 2022, pp. 45-46, doi: 10.1109/ICSA-C54293.2022.00016.

[5] Ö. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," 2017 International Conference on Cyberworlds (CW), Chester, UK, 2017, pp. 222-225, doi: 10.1109/CW.2017.22.

[6] Mohammed Ali Shaik, “Time Series Forecasting using Vector quantization”, International Journal of Advanced Science and Technology (IJAST), ISSN:2005-4238,Volume-29,Issue-4 (2020), Pp.169-175.

[7] N. Koroniotis, N. Moustafa, B. Turnbull, F. Schiliro, P. Gauravaram and H. Janicke, "A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments," 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 2021, pp. 887-894, doi: 10.1109/TrustCom53373.2021.00125.

[8] M. A. Shaik, S. k. Koppula, M. Rafiuddin and B. S. Preethi, "COVID-19 Detector Using Deep Learning," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 443-449, doi: 10.1109/ICAAIC53929.2022.9792694.

[9] S. Bera, L. Glenn, A. Raghavan, E. Meno, T. Cody and P. A. Beling, "Deterring Adversarial Learning in Penetration Testing by Exploiting Domain Adaptation Theory," 2023 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2023, pp. 314-318, doi: 10.1109/SIEDS58326.2023.10137792.

[10] Sahu, S., & Deo, R. C. (2017). Penetration testing and its methodologies: A review. Journal of Information Security, 8(2), 111-120. doi: 10.4236/jis.2017.82009

[11] M. A. Shaik, R. Sreeja, S. Zainab, P. S. Sowmya, T. Akshay and S. Sindhu, “Improving Accuracy of Heart Disease Prediction through Machine Learning Algorithms”, 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 41-46, doi: 10.1109/ICIDCA56705.2023.10100244.

[12] Verma, N., & Bhaskar, P. (2018). Penetration testing: An approach towards securing computer systems. International Journal of Engineering and Technology, 7(4.18), 63-66. doi: 10.14419/ijet.v7i4.18.22775.