Automated Penetration Testing to Enhance Security Decisions

Haya ahmed AlAgil† **Prof.Turki AlGamdi††**

†UQU College of Computing KSA , Makkah
††UQU College of Computing KSA , Makkah

Summary
Penetration testing is known as pen testing, is a fabricated attack used to identify the vulnerabilities in a system to check the exploiting vulnerabilities. Pen testing is usually accomplished by professional testers to find out the security risks and weaknesses involved in a system. Also, pen testing can be recognized as a pretend attack, performed to ensure that the system is secure and vulnerability-free. Pen testing is important for organizations because it detects weaknesses as well as makes the staff awareness high against those weaknesses. In one type of PEN testing, the expert engineer must test the risk of a system and its vulnerability manually. Another type is performing PEN testing and checking the risk of a machine in an automated way. The automated method enables organizations to achieve fast, easy, reliable, and efficient results. This thesis aims to introduce automated penetration testing tools and provide a platform that has multiple features of existing automated tools that meet the user requirements and are employed in a system to prevent security breaches. It also aims to reduce time, costs, and human resources. This framework contains multiple tools, and the results will be analyzed by comparing the time consumption.

Keywords:
Penetration testing, vulnerability, ethical hacking.

1. Introduction

Currently, the focal point of any organization is data protection due to the rapid growth of its data. This protection guarantees the safety and privacy of critical data from any unauthorized activities, including inspection, modification, recording, and any disruption or destruction. Testing is a term that is defined as the ability to detect and figure out faults and defects that may exist in a system. PEN testing necessitates an aim to crack the security of the application, which a developer cannot do. It involves the process of finding weaknesses in applications with the use of open-source tools that produce a report including the risks that could lead to a vulnerability in an application. Determining the vulnerabilities in a system is the main goal of penetration testing, which can be exploited and gain unauthorized access to an application, if any so that can be considered as a risk and threat.

This paper is divided into six sections. Section 1 gives a brief introduction to the topic. While **Section 2** introduces the technical background. Then **Section 3** reviews the related work in the field of penetration testing. **Section 4** describes the methodology of the automated penetration testing and introduces the proposed system. **Section 5** discussed system design and implementation. **Section 6** presents the implementation results and future work.

2. Technical Background

Security basics: For many years, the information security field has been built using the three fundamental components of confidentiality, integrity, and availability. Using these elements to define security gives the word a more practical significance and helps it move away from an abstract concept, emotion-based meaning to one denoting something solid, tangible, and measurable. Not all systems and not all data need an equal level of protection. Therefore, security controls must be enough to keep important data safe from unauthenticated access, which includes changes, disclosure, and destruction, and the performed test should ensure that the whole data is under protective controls, as well as the protections work properly, and the data cannot be breach by an attacker. So, an organization will set up a security grouping scheme that identifies and labels data according to the required level of protection.

Penetration testing: Testing is a keyword or term defined as “An ability to find fault and defects that may be present in a system or an application whether mobile or web” [16]. The security of data and information is the most important thing and is at the top of the priority list for companies. To build a competitive advantage, all businesses must protect their data, and ensure that they follow the security regulations and standards.

Manuscript received May 5, 2025
Manuscript revised May 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.5.10

In general, penetration testing inspects systems using multiple attempts of hacking to find vulnerabilities to exploit them and using relevant malicious code that helps to discover bugs through the implementation. The penetration test, as defined in [5], is the acting of a real-world crack against a system target or network. It also refers to simulating the attack strategy that attackers take on the application or network and completely testing the security and at-risk parts of the system to inspect the issues such as weaknesses of a system or network, and hardware and the defects of configuration of a software.
On the other hand, the basis of PEN testing is knowledge, the tester's attack is likely to be more successful the more knowledge they have. A penetration test is the authorized, scheduled, and systematic process of using known vulnerabilities to perform an intrusion into host, network, or application resources [4]. Organizations or individuals use PEN testing to test a network, web application, or computer system to identify bugs, and unprotected parts that cause vulnerabilities that an attacker can attack.

Manual and automated PEN testing:

- Manual testing:

PEN testing is a targeted and well-planned series of strategies, it is not just a disjoint of random steps. The steps build on each other to perform a successful attack. As mentioned before, the most important point in PEN testing is knowledge. Being aware of the enemy, the target, the resources, and the methods and finally knowing how to apply those steps effectively.

Figure 1 Stages of Penetration testing

- Automated testing:

Automated PEN testing tests the risk of a system and the vulnerability automatically. So, it is fast, efficient, easy, and more reliable than the manual. It doesn't require any experience; it can be executed by a user with the least knowledge. In the meantime, there are a variety of tools that are considered efficient, which changed the meaning of PEN testing. However, the following table clarifies the major difference between manual and automated penetration testing.

Examples of existing PEN testing tools:

- Nessus
- Nmap
- Nikto
- Dirbuster
- Metasploit
- OpenVas

3. Literature review

The study [1], they have explained the fundamentals of Penetration testing in comprehensive research, that includes different types of tools and where and when it is used. In the study [6], they have studied the difference between manual and automated pen testing and show the comparison in terms of the testing process, vulnerability detection, database attacks, and network modification. They show the result that automated penetration testing is better in all mentioned aspects except finding new or zero-day exploits. In [3] they proposed a system that depends on a simulation using Ubuntu 15.4 which is installed on a target host. The PEN testing is performed during the execution of Nessus and OpenVAS. Then they displayed the comparison between these two tools, which is done by using "Common Vulnerabilities Exposure" CVE. In [5] -The purpose behind this research was to contribute - They proposed a system that uses 4 PEN testing tools, Nmap, Nessus, OpenVAS, and Metasploit. The Metasploit framework has been combined with several third-party tools to improve its capabilities, which used through the hacking and stages of PEN testing methodology as well as it is used for vulnerability exploitation to ascertain whether an attack is feasible. While Nessus tool was used during the inspection and Vulnerability Assessment stage of the PEN testing methodology. As well as they also performed a comparison between Nessus and OpenVAS, to define which scanning tool was more helpful at discovering more weaknesses than the other scanner based on the Common Vulnerability and Exposure (CVE) identifiers. As mentioned in [7], they are telling us that the one of important features of the web application is Web application Testing. The most common way to fulfill the test is the automated penetration testing tools and frameworks which will give an easy and fast result. These existing tools perform attacks to test the security of the target system, without making any harmful on that data, so these attacks will not affect the web application

database by erasing or altering any part. In addition, these tools monitor the attack results to identify which of them have succeeded. As discussed in [8], the authors described penetration testing and said that penetration testing is one of the most helpful techniques for keeping the security of system data, which is legally used to imitate unauthorized attacks. Which is the main contribution of that attack being to identify that the system has exploited the vulnerability and to show their system weaknesses. Also, in [11], the authors show us that many tools help security to make their work more easily and efficiently.

These tools played a fundamental role by transferring the necessary procedures in an automatic manner rather than a manual way. The author has used and described the free existing framework created by Spanish developers called Golismero and it is used for security automated testing. It is used to test any web application. This tool includes different tools like DNSrecon, OpenVAS, Wfuzz, and SQLMap. In [9] they provide a main overview of penetration testing and, they discuss the benefits, strategies, and methodology of performing the penetration testing. As listed in [9], there are three phases in the methodology of penetration testing; the three stages are the Preparation of the test, performing of the test, and analysis of the test. The performing stage has also three steps: information gathering, analysis, and exploitation of the vulnerabilities.

This study [12] presents a new approach based on the use of attack signatures and interface monitoring for the identification of injection vulnerabilities in web services. The developed prototype tool picks out the vulnerabilities of detection of SQL injection in SOAP web services. The proposed tool comprises an attack load generation module which is used to examine the web service and generate the attacks containing signatures. They evaluate the experiment over 21 web services, which have been provided by a vulnerabilities detection tool's benchmark and the result shows that the methodology can get more coverage of detection than other existing PEN testing tools. In [14], they described penetration testing on a Network, and how it requires time and practice to be good in implementing. The way to handle this issue is to apply Artificial intelligence (AI) to the cyber security domain and automate the penetration testing. The main purpose of this paper [10], is to perform a security analysis for Android smartphones. Nowadays, smartphone adoption and usage are rapidly growing with the different applications. These applications play critical roles like payment and mobile banking, while user usually has no awareness of the risks involved in those applications. While [13], shows the Automated Network Exploitation through the Penetration Testing tool ANEX. ANEX is a tool that combines the needed qualities from both, the vulnerability assessment tools, and the penetration testing tools. The test includes a process of identifying the paths that could be exploited in the network which can easily break the target system. Mainly, penetration testing is the procedure of compromising a network by some controlled tests.

In the research [26], This study explored the status of security and the issues related to it on the websites of the Sudanese Government. However, the vulnerabilities and the security flaws in many of the Sudanese government websites have been studied and then assessed. Furthermore, websites or web applications are usually vulnerable to the attacks of the malicious aspects and files that the hackers use. Moreover, since the unpatched exploits in the government's websites allow unauthorized people to sign in to those websites, they can expose the data to cause damage. In [27], the authors proposed a framework that depends on the OWASP Benchmark, they made a comparative analysis of automated penetration testing, and they found the difference between types of penetration tools such as the performance of open-source tools better than the commercial one.

4. Methodology

The system APT is built of many existing PEN testing tools, these tools provide an automatic way of finding vulnerabilities, which are gathered to have multiple characteristics that belong to those tools, to provide a good framework for the organization, employer, or even the end user.

Tools selection: Our research depends on the selection of tools, many factors affect the selection of tools, such as the cost factor and the ease of configuration. While many tools have similar functionalities and features, these factors are different. The objective was to choose the tool based on the user requirements and many criteria i.e., availability, reliability, and the tool status, on the other hand, it depends on the availability of a licensed version of the tool and its configuration to be added to the framework, thus the definition of the easy of configuration is how easy to use the tool and to be configured in the framework. As the cost of the tool plays a major role in tool selection. The second objective was to select tools that cover –many general areas.

Nmap is considered as one of the famous tools used in PEN testing, which can easily scan large networks or just one single host. On the other hand, OpenSSL was selected because it is an open-source library that can be used to generate and test SSL certificates locally. SQLMap was chosen randomly to discover many different areas and meet a user requirement. At the same time, the user can add/remove tools to achieve his requirements. Nikto was selected as an alternative tool, as planned, Arachni is one of the A.P.T framework tools, but some changes occurred in their policies, so we thought to select another tool that met requirements like Arachni which is Nikto.

The table below shows the specifications of each used tool:

Table 1 Pen testing tool's specifications

Tool	***Specifications***
openSSL	Ensuring an SSL certificate is valid, trusted and it will be working properly for users.
Nmap	Scanning tool Manipulates with the target directly.
OWASP Zap	Proxy tool, it helps in prevention of cyber attackers from entering a private network.
SQLmap	Exploiting SQL injection flaws to assess the security of targeted applications.
Nikto	It can be run on a system with lower configuration because it is lightweight application, manipulates with the target directly as it is scanning tool.

The main objective of the thesis is to provide a framework that eases the security decision by combining those tools depending on user requirements. The programming language used to build the framework is Python.

System scenarios

The APT environment has two different scenarios. The 1st is when the user wants to check the IP address through all the consisting tools, then it creates a file that contains the result of PEN testing and shows the result in the command prompt. The 2nd is giving the user the freedom of choosing among the tools.

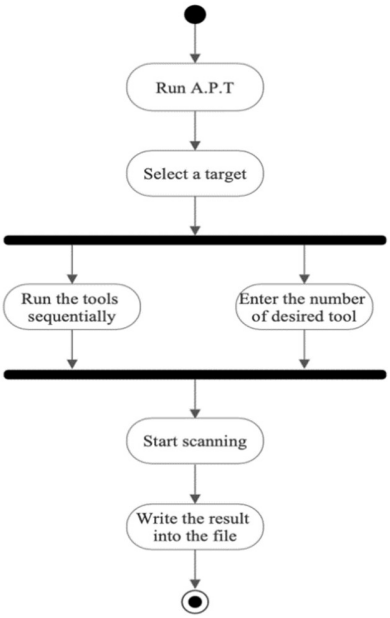

Figure 1. APT system flow

5. System Design and Implementation

A.P.T framework is built up with multiple tools that are conducted by authorized expert testers -ethical hackers- with expert knowledge of web applications as well as the newest development methodologies and the latest security risks. The framework is designed to be an open-source tool for any community, and it is used to scan a single machine at a time via IPs to the application level. It consists of multiple tools that have been collected to test the target by performing successful way of penetration testing and give results that can be relied on in a short time that help of time.

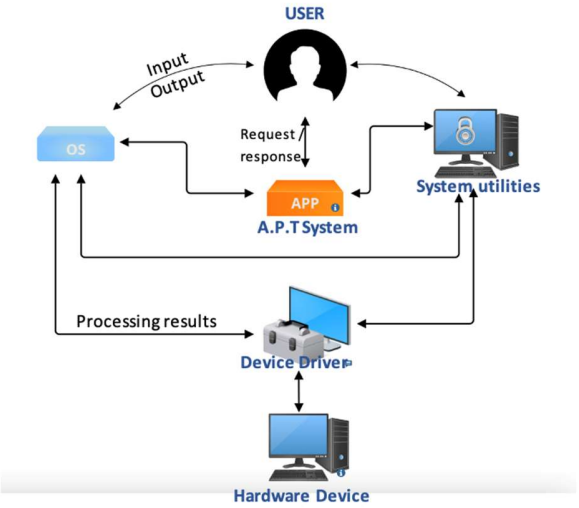

Figure 2. APT system Implementation

6. Implementation Results and Future Work

This script is an Automated Penetration Testing (A.P.T) tool that allows users to perform security scanning against a specified target using various scanning tools. The script provides a menu-based command-line interface (CLI) for selecting the desired tool and target.

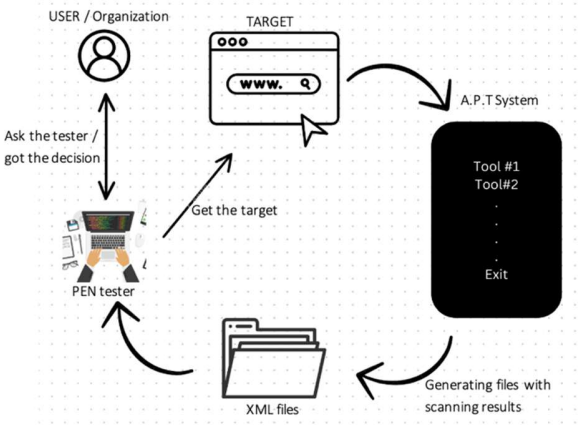

Figure 3. APT system for Desired Tool and Target.

3.1.1 Usage

To use the script, the user needs to run it from the command line. Here are the available options: apt <Target IP/URL> <Tool Name>

- target (optional): The URL or IP address of the target to scan. If not provided, the script will display a menu to select the target interactively.
- tool (optional): The name of the tool to use for scanning. If not provided, the script will display a menu to select the tool interactively.

If the target is provided without a tool, the script will run scans for all available tools in sequence. If the target and tool are not provided, the script will run in interactive mode, which displays a main menu that contains all tools.

3.1.2 Configuration

The script requires a configuration file named tool_config.json, which contains the configuration details for each scanning tool. The file should be present in the same directory as the script. The format of the configuration file is as follows:

```
{
"tool_name":
{
"executable": "path/to/executable",
"command": "{executable} command_paramaters {url_ip}"
},
  ...
 }
```

tool_name: The name of the tool.
executable: The path to the executable file of the tool.
command: The command-line command to execute the tool, where {executable} and {url_ip} are placeholders that will be replaced with the actual values.

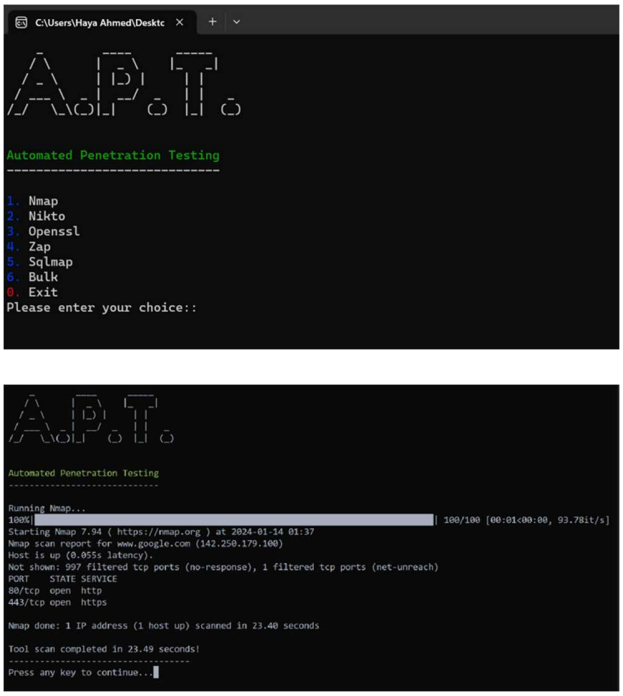

Figure 4. APT system Results

- **Case Study #1: Run all tools sequentially**

The experiment was performed by running A.P.T framework tools sequentially. The table below shows the running time -scanning duration- of one single target used as an input.

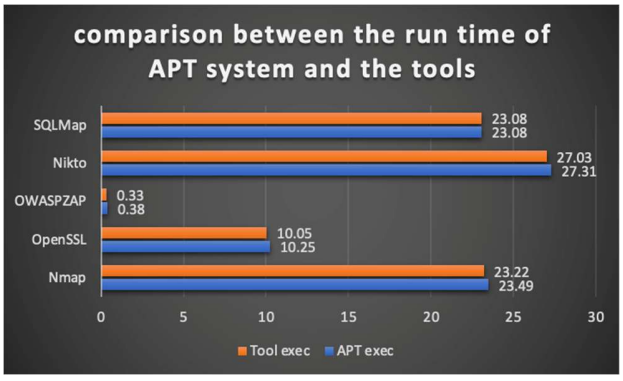

Figure 5. Comparisons of APT systems and Tools.

The graph above indicates the changes in scanning time in the case of running the tool in the A.P.T system or running it manually in the operating system. The blue line is relevant to our system running time, it indicates the time each tool runs individually, in the same way, the orange one is related to the time taken to run the tool which is installed

manually in the platform -the time to launch the tool is not computed-. Therefore, the time taken by the tool to completely scan the application is primary to recognize the efficiency.

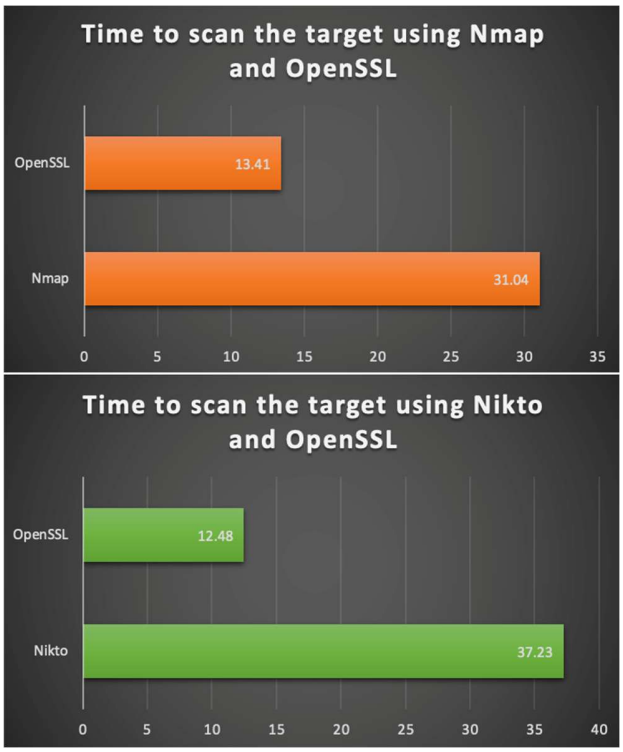

Figure 6. Time to scan the Targets.

As shown in the figures above, it was observed that case study#2 has less scanning time than the 3rd one. In the same conditions and the same target, the tools Namp+OpenSSL performed the scanning in 44.45 sec, while the tools Nikto+OpenSSL done the scanning in 49.71sec which was slower than the other group.
However, based on the results of this study, the study investigation focused on the performance of tools (Time to detect the vulnerabilities). We compared the duration time of each tool, and then performed a comparison of two groups of tools to select the faster one. And we were able to demonstrate that our methodology is effective in a small organization that has clear specifications about what it must check and what they have concerned about. It depends on the user if he wants to add some tools, he can do it easily by extracting the tool using the command line. These techniques, like choosing a tool manipulating it, and extracting it all depend on their privacy policies and configuration. In conclusion, A.P.T is a Command Line Interface based framework that is light and fast, and its features lead the developer to prefer using a framework that has many properties that leading less time and effort.

7. Conclusion

Pen testing is important for organizations because it detects weaknesses as well as makes the staff awareness high against those weaknesses. In one type of PEN testing, the expert engineer must test the risk of a system and its vulnerability manually. Another type is performing PEN testing and checking the risk of a machine in an automated way. The automated method enables organizations to achieve fast, easy, reliable, and efficient results. This thesis aims to introduce automated penetration testing tools and provide a platform that has multiple features of existing automated tools that meet the user requirements and are employed in a system to prevent security breaches. It also aims to reduce time, costs, and human resources. This framework contains multiple tools, and the results will be analyzed by comparing the time consumption.

References

[1] J.Metso, “Penetration testing,” 2019.
[2] Corcoran, T. (2001). An introduction to Nmap. *Internet: http://rr. sans. org/audit/nmap2. php*.
[3] Fashoto, S. G., Ogunleye, G. O., & Adabara, I. (2018). EVALUATION OF NETWORK AND SYSTEMS SECURITY USING PENETRATION TESTING IN A SIMULATION ENVIRONMENT. *Computer Science & Telecommunications*, *54*(2).
[4] Angel, S., & Sarala, S. (2011). A study on Penetration Testing. *International Journal of Advanced Research in Computer Science*, *2*(5)
[5] Appiah, J. K. (2014). *Network and Systems Security Assessment using penetration testing in a university environment: The case of Central University College* (Doctoral dissertation).
[6] Abu-Dabaseh, F., & Alshammari, E. (2018, April). Automated penetration testing: An overview. In *The 4th international conference on natural language computing, Copenhagen, Denmark* (pp. 121-129).
[7] S. P. Kalirathinam, “Penetration Testing Tool for Web Applications Nástroj pro penetrační testování webových apli kací,” 2019.
[8] Chiem, T. P. (2014). *A study of penetration testing tools and approaches* (Doctoral dissertation, Auckland University of Technology).
[9] Bacudio, A. G., Yuan, X., Chu, B. T. B., & Jones, M. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications*, *3*(6), 19.
[10] Kumar, N., & Ul Haq, M. E. (2011). Penetration testing of android-based smartphones.
[11] Bellatriu, O. C. (2014). Penetration testing automation system.

[12] N. Antunes and M. Vieira, "Enhancing Penetration Testing with Attack Signatures and Interface Monitoring for the Detection of Injection Vulnerabilities in Web Services," *2011*

[13] Dazet, E. F. (2016). *ANEX: automated network exploitation through penetration testing*. California Polytechnic State University

[14] Schwartz, J., & Kurniawati, H. (2019). Autonomous penetration testing using reinforcement learning. *arXiv preprint arXiv:1905.05965*.

[15] Al Shebli, H. M. Z., & Beheshti, B. D. (2018, May). A study on penetration testing process and tools. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-7). IEEE.

[16] Henry, K. (2012). *Penetration testing: protecting networks and systems*. IT Governance Publishing.

[17] Mainka, C., Somorovsky, J., & Schwenk, J. (2012, June). Penetration testing tool for web services security. In *2012 IEEE Eighth World Congress on Services* (pp. 163-170). IEEE.

[18] Johari, R., Kaur, I., Tripathi, R., & Gupta, K. (2020, October). Penetration testing in IoT network. In *2020 5th International Conference on Computing, Communication and Security (ICCCS)* (pp. 1-7). IEEE.

[19] Vats, P., Mandot, M., & Gosain, A. (2020, June). A comprehensive literature review of penetration testing & its applications. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 674-680). IEEE.

[20] Abraham E. Evwiekpaefe and Isacha Habila (2021), Implementing SQL Injection Vulnerability Assessment of an E-commerce Web Application using Vega and Nikto Tools

[21] Anderson, H. (2003). Introduction to nessus. *Retrieved from Symantec*.

[22] SQLMap: An Essential Tool for Automated SQL Injection Testing, Amal Tom Parakkaden

[23] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*, 27-49

[24] Arkin, B., Stender, S., & McGraw, G. (2005). Software penetration testing. *IEEE Security & Privacy*, *3*(1), 84-87.

[25] Budiarto, R., Ramadass, S., Samsudin, A., & Noor, S. (2004, April). Development of penetration testing model for increasing network security. In *Proceedings. 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004.* (pp. 563-564). IEEE.

[26] N. O. S. Omar, "A Proposed Method for Vulnerability Discovery of Sudanese Government Websites," 2018.

[27] Shah, M. P. (2020). *Comparative analysis of the automated penetration testing tools* (Doctoral dissertation, Dublin, National College of Ireland).