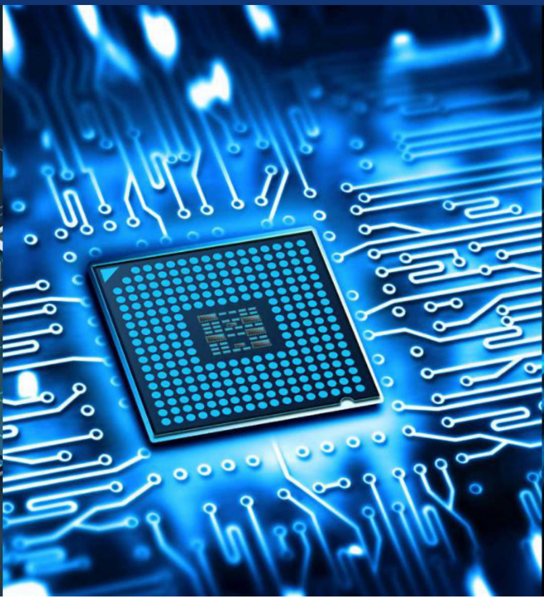
IJIRCCE

ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.771

Volume 13, Issue 3, March 2025

www.ijircce.com ✉ ijircce@gmail.com ☎ +91-9940572462 ☎ +91 63819 07438 www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Design and Implementation of a Vulnerability and Penetration Tool

Abdulrasak Mahi, Dr. Popoola, Victor Olusegun, Olalere, Sherifdeen Abiodun, Aliu Aishat Oluwapelumi

Computer Science Department, Espam-Formation University, Campus 2, Porto-Novo, Benin Republic

Computer Science Department, Kingstar Institute of Management Science & Technology, Ibadan Oyo-State, Nigeria

Computer Science Department, Espam-Formation University, Campus 2, Porto-Novo, Benin Republic

Computer Science Department, Espam-Formation University, Campus 2, Porto-Novo, Benin Republic

ABSTRACT: With the increasing reliance on digital infrastructure, cybersecurity threats have become more sophisticated, necessitating proactive security measures. This study presents the design and implementation of a vulnerability and penetration testing tool, aimed at identifying and mitigating security flaws in computing systems. The tool integrates network scanning, automated vulnerability assessment, and exploitation techniques to provide a comprehensive security evaluation. By leveraging Nmap for network scanning, Metasploit for penetration testing, and Nikto for web vulnerability analysis, the system offers a streamlined approach for security professionals. The research details the architecture, implementation methodology, and testing procedures of the developed tool, highlighting its effectiveness in detecting and mitigating security threats. The findings demonstrate that automated penetration testing tools enhance security auditing, improve threat detection, and assist organizations in fortifying their digital assets against cyberattacks. The study concludes with recommendations for future improvements, integration with AI-driven threat intelligence, and policy considerations for ethical cybersecurity practices.

KEYWORDS; Vulnerability and penetration testing (VAPT), Cybersecurity threat detection, Automated security assessment tools, Network and web application security, Ethical hacking and penetration testing, AI-driven cybersecurity solutions

I. INTRODUCTION

Cybersecurity is of paramount importance in the digital age where reliance on computing systems is pervasive and ever-increasing. Nearly all organizations in the present day have an IT infrastructure which is used to handle sensitive information. Assuring the integrity and safety of this information is of utmost importance. The burgeoning prevalence of newer, more sophisticated cyber threats is leading to an increase in both the number of incidents and the scale of damage caused by them. Attackers with malicious intent typically concentrate on finding and exploiting weaknesses in computer systems for personal gains or other undesirable purposes. The crimes committed can range from stealing a requestor's sensitive information, hijacking their communication to launching large scale Distributed Denial-of-Service (DDoS) attacks on a website, rendering it unusable. To alleviate vulnerabilities and secure the sensitive information on IT systems and networks, there is a need for automated tools which are able to pinpoint weak spots before attackers can, while for ethical hackers, it's important to also be able to exploit those weaknesses after such a discovery to communicate the risks clearly to defenders, so potentially dangerous security holes can be mitigated swiftly (Happe & Cito, 2023).

Being able to explore, develop, analyze the results of algorithms used in both the vulnerability and penetration-testing sector is pivotal. This allows cyber defense applications to benefit academia by laying down foundation for new algorithms, and traditions, while also allowing scholars to test novel methods on well-defined real-world problems. Such cross-pollination of information can potentially make and create better automated security assessment tools which can alleviate the outburst of cyber-attacks. It is highly desired to have insight from both academicians and practitioners in the vulnerability and penetration-testing fields to bridge the gap and move forward in this continuously evolving domain. Human-aspects of recent studies and unresolved issues, which if addressed could decrease the number of incidents, are also briefly discussed.

II. BACKGROUND AND SIGNIFICANCE

Vulnerability and penetration testing have been practised for some time, primarily using network scanning tools such as Nessus (Valli et al., 2014). A natural evolution is for these network scanning tools to be ported to smaller form factor devices to allow small rudimentary health checks of client security postures. Such tools offer a valuable service opportunity for new business models in penetration testing, the difficulty isn't just in performing the tests themselves but the interpretation of the results and deciding how to action them becomes the real art. Threats against networks, systems, and other digital assets are continually evolving, raising the number of vulnerabilities found in these assets (Happe & Cito, 2023). This situation has brought increasing concern to users, enterprises, and governments incentivising a review how these assets are secured.

A pragmatic perspective is that any network, device, application, or other digital asset could be vulnerable, and this vulnerability will be impossible to detect without an appropriate assessment tool. Without the ability to determine if an asset is vulnerable, it is not possible to design and deploy mitigation actions. The holistic proposition, therefore, is for the security industry to construct though continued Research & Development and heightened market competition better suites of vulnerability and penetration testing tools. Current security vendor tool suites are not diverse enough or capable enough in automated testing ability, they are expensive, and in many instances provide redundant testing. Focused toolsets based on differing vendor suites performing different testing methodologies could yield appreciably improved testing results and costs-savings to the user. Rather than simple counting of discovered vulnerabilities, sophisticated future studies should analyse the effectiveness of the vulnerability and penetration testing results in regard to addressing current open issues and increasing the overall network security posture of the organisation under evaluation.

III. LITERATURE REVIEW

For organizations and companies to be safe from cyberattacks, an essential part in their structure is vulnerability and penetration testing (VAPT). There is the need to have a knowledge base for the decision-makers to choose which tool or company to search about the weaknesses in the systems, as well as to understand the outputs, how to implement them, and how to test the safety of these outputs. A review of a system is completed as a user interface that runs the company's algorithm. Data is collected by the user interface, turned into a certain format, and organized in the correct files. Then, the algorithm is run using the raw data. The raw data is used by the algorithm tools, producing safety weaknesses and attack outputs in opposition to these weaknesses. Attack and defense outputs are transformed into reports that all parties can recognize. The resulting reports are reviewed and translated into a list of measures that can be used to change the system and remove the resultant safety weaknesses (Ventura et al., 2023). Research into cybersecurity audits, tools, and automation could be utilized to optimize the VAPT process with the introduction of an OWASP-based VAPT algorithm by professionals or those skilled in the art, as well as exams on the already existing VAPT frameworks, kinds, definitions of "benchmarks" in addition to how these benchmarks should be used based on the testification (Straub, 2023). With the rising digitalization, the number of current and former online businesses is also growing. It is known that the most significant aspect of these firms is the exposure of their digital core. It is well known that cyber security requiring regular checks and maintenance is done with VAPT services. With the change in customer behavior in daily life, it is accepted that instead of the old habits, the new generation is interested in technological platforms and the number of start-ups is increasing. With new ventures coming online, the need for digital security is increasing, and the trend in new start-ups is to be digital security. With the increasing demand for VAPT experts, the indispensable parts of the VAPT service are examined, and it is aimed to introduce a program that can perform the checks and outputs that a professional VAPT expert can do using an already established algorithm. The method is the application and commercialization of VAPT framework algorithms. Organizations have a digital side of the business and all technical structures of the business in the online environment are predefined in the system. At least once in six months, the first situation is that regular checks are made to check the safety of these systems.

IV. METHODOLOGY

4.1. Requirements Analysis

To find out the requirements for a vulnerability scanner, it is customary to examine the software applications themselves and the general context in which vulnerability scanners exist. During the investigation, it is necessary to evaluate the structure and the elements of the software architecture of the applications while trying to identify the peculiarities of the software it is contemplated to scan. Preliminary results from the study of the vulnerabilities and the related software architecture of several applications were already gathered. This section revisits the main aspects of vulnerabilities considered to be essential for the requirements gathering and identifies several interesting operating software systems that may best demonstrate the capabilities of vulnerability scanners . (Alazmi & De Leon, 2022)

A vulnerability scan is an audit that is essentially a measurement of the security level of the computer that still reflects what the security posture actually appears to represent. At the present time, scanners are known as tools that perform security policy audit monitoring activities. The majority of these tools scan the system by giving the computer directions that are necessary for determining the proper implementation of the security policy. The scanner applies sophisticated algorithms and searches for unused or hidden accounts, directories, and files; the scanner uses filenames to determine that the application being run is, in fact, spoofed. The two types of internal outputs from the scanners are the files and the results crosschecked with the list of items to disclose various types of vulnerabilities . (Alazmi & De Leon, 2022)

4.2. Design Phase

In the design phase, requirements meeting functional and quality aspects are elicited in interviews, a group session, and direct observations. Initially, a group session was conducted in an informal meeting with the customer group where participants understood and analyzed the work context and requirements in order to improve the design of the tool to be developed. Afterwards, a semi-structured case study was conducted using interviews and direct observations with users who have different organizational roles and levels of experience to elicit both functional and quality requirements. Functional requirements are modeled as use cases, which give an operational purview of different groups of users of the tool. The use cases are formally represented by the use case diagram, each one specifying the interaction of some group of actors with the tool . (Tang et al., 2022)

The quality requirements, described as non-functional requirements, are modeled in a scenario-based style, complemented by a short narrative. The use of safety, effectiveness, deployment characteristics, human engineering, training, support, and inappropriate exploitation of the tool are some relevant factors in the development of these diagrams. Using the requirements, followed by a basic investigation of the theoretical aspects of similar tools, the tool was described with a simplified scenario, and a very simple demonstration was implemented. In order to serve as a seed in the interviews, the tool has a simple user interface that the user asks for remote authentication of a service, and he gets in touch with a remote attacker breaking common security features in the service by unauthorized access and/or intentional information leakage. (Javaid et al.2023)

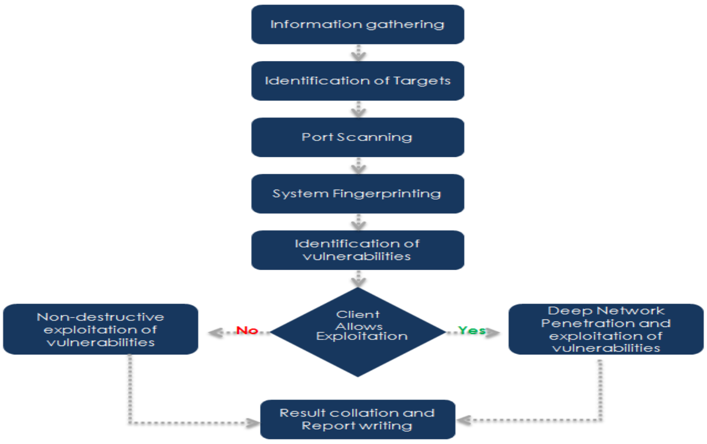

Information gathering
Identification of Targets
Port Scanning
System Fingerprinting
Identification of vulnerabilities
Non-destructive exploitation of vulnerabilities
No
Client Allows Exploitation
Yes
Deep Network Penetration and exploitation of vulnerabilities
Result collation and Report writing

Figure 1: A flowchart depicting the stages of vulnerability assessment and penetration testing, from information gathering to reporting.

V. KEY FEATURES AND FUNCTIONS

Cybersecurity has become a major concern these days as many users are using internet. On the internet side one user has some data control and manipulation with the front end only. The back end is controlled by some administrator. It is also necessary for them to check the vulnerability and patches of while because a lot of users are using internet and the server may get down due to the overload or probably can be hacked by the attackers. In this project, it is intended to develop a penetration and testing tool that helps the own server side users to check the server status, vulnerability and the patch whereas to the other side users (Attackers) it provides the mechanisms for testing the vulnerabilities of the server and helps to hack them using the several hacking techniques. Using web server one can get all the data possible from the server side; it can scan huge data and can download the file from the server. So, it is necessary to develop a tool, which provides security so that the one side users can't hack the server (Sahil A. Bhat et al., 2019). The project is aimed to analyse the vulnerabilities on the back end provided servers.

Tools and Features

The VulnX tool integrates three primary components:

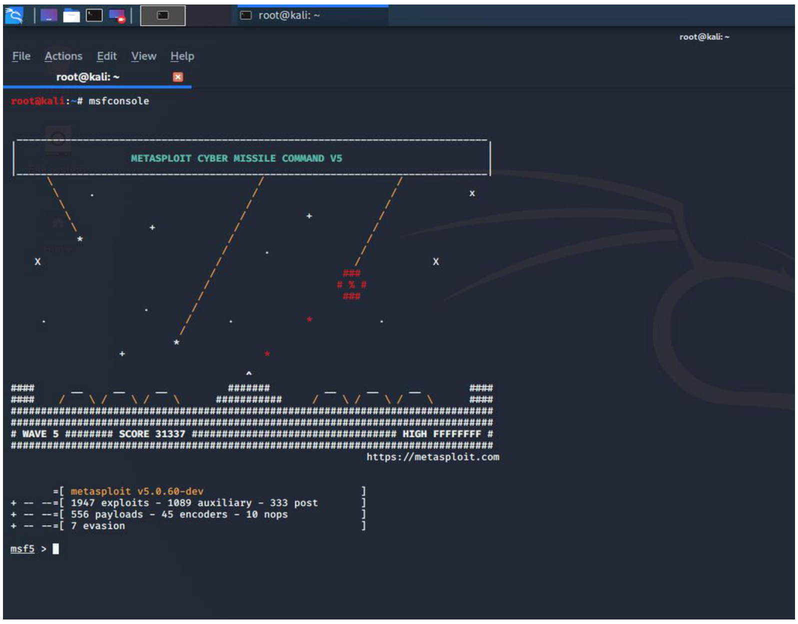
- **Nmap**: Used for comprehensive network scanning and vulnerability identification. It provides insights into network topology, open ports, and running services.
- **Metasploit**: Facilitates the exploitation of identified vulnerabilities. Its modular framework supports various attack scenarios, including privilege escalation and payload delivery.
- **Nikto**: Specializes in web vulnerability scanning, detecting misconfigurations, outdated software, and insecure files.

These components were combined into a single interface, ensuring seamless data flow and improved user experience. Additional features included automated reporting and visualization tools to aid in interpreting results.

Implementation Process

The development process involved:

1. Identifying the core functionalities of each tool.
2. Designing a unified interface to integrate these functionalities.
3. Implementing data exchange mechanisms to enable seamless interoperability.
4. Conducting rigorous testing to validate the tool's effectiveness in real-world scenarios.



```
root@kali:~# msfconsole

 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
      \                                  /                      /
       \     .                          /                      /            x
        \                              /                      /
         \              +             /                 +    /
          \                          /                      /
           *                        /              .       /
  x                                /                      /                x
                                  /                  ###
                                 /                  # % #
                                /                    ###
   .                   .       /        .     *            .
                              /
                      +      *              *
                                        ^
####    __     __     __            #######         __     __     __        ####
####   /  \   /  \   /  \         ###########      /  \   /  \   /  \       ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                          https://metasploit.com


       =[ metasploit v5.0.60-dev                          ]
+ -- --=[ 1947 exploits - 1089 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

Figure 2; A diagram illustrating how Nmap, Metasploit, and Nikto can be used together for vulnerability scanning and exploitation.

The developed tool can be used for the server side version and should provide a local mechanism to analyze vulnerability assurance of the servers. The trading tool primary analysis the server and the stock and push in the database of the server side analyzed server. Secondary, it provides the similar mechanism to scan the server side of the back end servers. It does not actually perform the scanning web application, rather it works like same the local mechanism server side application. It development of the trading tool will be similar to the hand by other hacking mechanisms. It better to than java and the parsing will be the great for the open source combination of the web front end generally codec earlier and the back end engine provides the mechanisms as above mentioned. The paper provides server mechanism based design and test the results for server based vulnerabilities (Girotto & Francisco Zorzo, 2020).

VI. COMPARISON WITH EXISTING TOOLS

This section provides a brief overview of 19 relevant and widely used open-source and commercial assessment solutions and contrasts them with the developed engineering tool. Six criteria structures are used for the comparison to highlight the variation of user experience, the need for effectiveness benchmarks, and the challenge of coverage. Because strong variations in the feature set and the time to market occurred in different tool classes, separate comparisons of commercial and open-source tools are made. Attention is drawn to some inherent biases of the comparison methodology. The benchmark results of three case studies are outlined, with each of them comparing the tool with up to three commercial and widely used assessment products. Finally, quotes of six interviews with practitioners are used to provide an external perspective on the findings. (Bin and Kamel2021)

Upon completing a penetration test, it is common for a report to be generated by the security company which details a “general overview” section of the test, and typically, this will go something like, “We have performed an external penetration test on the IP addresses provided and found vulnerabilities on these hosts.” This approach briefly summarizes the steps taken to identify an issue on the target, what the issue was, and what the potential impact of having the issue can be (Happe & Cito, 2023). All this should be accurately reflected in the output of the tool, and the risk score can help to prioritize the remediation strategy for the client.

VII. CASE STUDIES

The following case studies demonstrated the effectiveness of a web-based vulnerability and penetration testing tool. The tool aims to provide domain-specific recommendations and methodologies to the output. The findings showed that the tool significantly enhanced the penetration testing process and showed that subjects can find and remediate the vulnerabilities more quickly with the tool output than without. There has been a higher remediation percentage of the found vulnerabilities when using the output (Dalalana Bertoglio et al., 2019).

The case studies involve several distinct institutions and organizations to evaluate the tool’s general applicability. The organizations range from a university department, a provincial health authority, and a municipal government. These organizations have vastly different network configurations and assets and have distinct uses and functions for their web presence. The collaboration and implementation process were developed in different ways depending on the organization. Different strategies for outreach, intervention, and training were employed for each case study, tailored to the needs and preferences of the organization. The penetration testing tool was implemented in the lab to evaluate the tool and demonstrate best practices and effective implementation strategies. There was significant negotiation regarding the implementation plan and what configurations and access the tool would have. A second implementation in a more complex, technically advanced organization - the provincial health authority was spearheaded by a research student with previous work experience in IT in that organization. This case study demonstrates a more involved implementation with attempted full network-wide vulnerability testing, as well as hosting provider involvement. A third case study with a municipal government smaller organization and more closely involved implementation process is presented . (Wilhelm, 2025)

VIII. FUTURE DEVELOPMENTS AND TRENDS

Introduction
New threats and attack surfaces resulting from the come of new technologies and methodologies have inspired innovation in the domain of vulnerability detection and penetration testing tools. It is essential to keep an eye on the further developments and trends in this domain to ensure the timely and appropriate evolution of tools and methodologies to adjust to the upcoming needs effectively and remain a relevant part of information security professionals' tool chain (Happe & Cito, 2023).

Emerging Technologies and Methodologies
Broadband networks, cloud services, mobile devices, and machine-to-machine communication have come up as a worry and contribution to an increase in attacks against them. These new scenarios have been observed the development and adoption of new technologies and methodologies to adapt to them in the light of the conviction that this is not merely a coming thing, but there are already various researchers and practitioners from this area acting intensely in these new contexts. So it is notably relevant to get fathom about their needs and capabilities, as also to know the trends and strategic actions they may take in confronting the strengthening threats and attack surfaces.

Adaptive Tools
Threats and tools are assumed to evolve at the hands of each other, which points to the need to foster tool development: as tools evolve, they have to be augmented with self-adaptation capabilities to take into account not only the needs detected, but also to automatically adjust to the evolution of tools. This is thought to be a discriminating feature to distinguish among tools and methodologies, which will be a useful observation to professionals.

IX. CONCLUSION AND RECOMMENDATIONS

The topic of cybersecurity is becoming increasingly important because of the growing number of businesses that are moving to online platforms. There are always new vulnerabilities and attack vectors that are being developed by malicious users. Therefore, as a part of this research, a vulnerability and penetration testing tool will be designed and implemented. This project will simulate some common attack techniques and common vulnerability entries, and it will highlight where they can be exploited or how to defend against them. This tool will be named VAPT-Tool and it is an open-source tool which will allow developers to be able to scan their web application before it goes online. It has been built to be as lightweight and flexible as possible, while also having a very clean and easy to use interface. Thus, it supports python 2.7 and 3.5+ and operating systems including Windows 7 and later, MacOS 10.14 and later, Linux Ubuntu 18.04, and Linux Debian 10. Its code is well commented, with new features while still in development to create pull requests to this initial release. The current version of the VAPT-Tool focuses on web applications and static analysis will be performed. The tool works by collecting inputs from the user like cookies or the url of the website or web page. After that based on cookie input, authentication will be performed to access hidden web pages for scanning. It randomly finds what type of input is given to the selected website and scans it. At the end of the attack, a detailed report is going to be written to the given output filename. The tool will clearly indicate if the web application is susceptible by presenting the payload that has been used. Scanning speed is fast, and with 7 sets of payloads, test cases, and multiple threads directed to a location, the admin password based on the cookies was found in less than 7 minutes. Finally, this project will help increase awareness for developers in order to enhance the security of the code and have a better understanding of scan tools from the perspective of the tool itself (Ventura et al., 2023).

REFERENCES

1. Happe, A. & Cito, J. (2023). Understanding Hackers' Work: An Empirical Study of Offensive Security Practitioners. [PDF]
2. Valli, C., Woodward, A., Hannay, P., & Johnstone, M. (2014). Why Penetration Testing is a Limited Use Choice for Sound Cyber Security Practice. [PDF]
3. Ventura, R., Jose Franco, D., & Khasro Akram, O. (2023). A Novel VAPT Algorithm: Enhancing Web Application Security Trough OWASP top 10 Optimization. [PDF]

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Straub, J. (2023). Development and Analysis of P2SCP: A Paradigm for Penetration Testing of Systems that Cannot be Subjected to the Risk of Penetration Testing. [PDF]
5. Alazmi, S. & De Leon, D. C. (2022). A systematic literature review on the characteristics and effectiveness of web application vulnerability scanners. IEEe Access. ieee.org
6. Tang, C., Irfan, M., Razzaq, A., & Dagar, V. (2022). Natural resources and financial development: Role of business regulations in testing the resource-curse hypothesis in ASEAN countries. Resources Policy. [HTML]
7. Javaid, M., Haleem, A., & Singh, R. P. (2023). ChatGPT for healthcare services: An emerging stage for an innovative perspective. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 3(1), 100105. sciencedirect.com
8. Sahil A. Bhat, M., Vitthal N. Pankar, M., Namrata Kumari, M., & Vrushali Desale, M. (2019). Testing Tool: Offensive Server Side Security Analyser. [PDF]
9. Girotto, G. & Francisco Zorzo, A. (2020). Robin: A Web Security Tool. [PDF]
10. Bin Naeem, S., & Kamel Boulos, M. N. (2021). COVID-19 misinformation online and health literacy: a brief overview. International journal of environmental research and public health, 18(15), 8091. mdpi.com
11. Dalalana Bertoglio, D., Girotto, G., Varlei Neu, C., Castagna Lunardi, R., & Avelino Francisco Zorzo, and (2019). Pentest on an Internet Mobile App: A Case Study using Tramonto. [PDF]
12. Wilhelm, T. (2025). Professional penetration testing: Creating and learning in a hacking lab. [HTML]

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com