IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

Exploring the Efficacy and Ethical Implications of Penetration Testing in Network Security

Viraj Mehta[1], Dr. A. Rengarajan[2]

Student of MCA, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India [1]

Professor, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India[2]

ABSTRACT: In today's landscape, cybersecurity reigns supreme as cybercrimes surge. Businesses are on high alert, striving to shield themselves from online threats like hacking and data breaches. Various safeguards are in place to brace for such scenarios. However, penetration testing emerges as the ultimate litmus test to gauge the efficacy of these security measures. A penetration tester must meticulously select the appropriate tools, considering factors like budget, time, and scope. This study scrutinizes the effectiveness of scanning tools within a Kali Linux environment. The overarching objective of penetration testing is to ensure networks and systems remain impervious to security threats, preventing unauthorized access to resources. This paper delves into the intricacies of planning and executing a penetration test, targeting project managers or directors contemplating such an endeavor. Undoubtedly, conducting a penetration test is a complex undertaking, and organizations must weigh the suitability of this method for their specific needs..

KEYWORDS: Penetration testing, Network security, Ethical hacking, Cybersecurity assessment, Vulnerability assessment, Security testing, Risk management, Ethical implications, Legal considerations, Compliance standards .

I. INTRODUCTION

Security stands as a colossal hurdle within information systems. The pressing need for software security is intensified by the rapid interconnectedness of computers, the continual expansion of systems, and the unbridled growth of system complexity, surpassing past eras. Moreover, ensuring the safeguarding of an entity's information assets to maintain seamless business operations demands a methodical, systematic approach that delivers resilient protection against potential threats. In reaction to this critical need, security specialists have concocted a myriad of security assurance strategies, such as proof of correctness, layered design, software engineering environments, and penetration testing, all aimed at tackling security apprehensions and maintaining essential security standards. It's abundantly clear that businesses, organizations, and entities handling sensitive data, regardless of their industry, confront significant security hazards. Often, these entities grapple with understanding the immense complexities of their communication networks, exerting minimal oversight. Furthermore, when factoring in applications utilizing their computing infrastructures, these risks skyrocket. Unchecked dangers have the potential to escalate the frequency of security breaches, resulting in significant financial setbacks. Broadly, security hinges on three fundamental measures: prevention, detection, and response. Prevention endeavors to hinder unauthorized access to system resources. Detection intervenes when a hacker breaches the system or is in the process of doing so. Response, the ultimate defense, aims to rectify the shortcomings of previous mechanisms by stopping or hindering further harm or unauthorized access to facilities.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

II. RESEARCH METHODOLOGY

1.1 What Is Penetration Testing? Penetration testing, also known as ethical hacking or pen testing, mimics cyberattacks to uncover and exploit security weaknesses in a computer system. Think of it as hiring a security specialist to attempt system breaches and pinpoint vulnerabilities before malicious attackers do. The aim of penetration testing is to fortify system security by detecting and rectifying flaws before they can be exploited by malevolent entities. Penetration testers wield the same authorization as actual attackers, utilizing identical tools and methodologies under the system owner's consent.

1.2 WHY PERFORM A PENETRATION TEST? The primary objective of pen testing is to discover and exploit vulnerabilities before malicious actors do. It functions as a proactive measure, akin to a controlled fire drill that exposes hidden security weaknesses. Enhancing your security posture is crucial: Identifying and remedying weaknesses enables you to repel assaults more effectively. By plugging the gaps in your defenses through pen testing, hackers encounter significant obstacles in their attempts to breach your sensitive information and systems.

2 PHASES IN PENETRATION TESTING:

Planning and Preparation: The penetration test's objectives and scope are established at this step. The customer and the pen testing team work together to comprehend the objectives, assets that need to be safeguarded, and prospective dangers. Aside from that, ethical and legal issues are covered, such as getting the right permission to administer the test.

Reconnaissance: Sometimes referred to as information gathering, this stage entails learning as much as you can about the intended system or organization. This might contain personnel information, publicly accessible data, network infrastructure, and more. Acquiring information that might be utilized to exploit weaknesses is the aim.

Scanning: After gathering enough data, the pen testers search for vulnerabilities in the target environment using both human and automated technologies.

Enumeration: During this stage, the penetration testers actively investigate the target environment in order to obtain more specific data on the users, services, and systems.

Vulnerability Analysis: The pen testers examine possible vulnerabilities to determine their impact and severity on the target environment after discovering them. This entails figuring out whether the vulnerabilities can be used to break into the system or obtain unauthorized access.

Exploitation: During this stage, the penetration testers try to enter the target system or network by taking advantage of the flaws they have found. This may entail gaining illegal access by evading security measures through the use of unique scripts.

Post-Exploitation: After gaining access, the pen testers could take additional steps to increase their level of authority, continue their persistence, or steal confidential information. This stage mimics the actions that an actual attacker may do once they are inside the target area.

Vulnerability Analysis: The pen testers examine possible vulnerabilities to determine their impact and severity on the target environment after discovering them. This entails figuring out whether the vulnerabilities can be used to break into the system or obtain unauthorized access.

1.3 Penetration Testing Tools

Nmap (Network Mapper) Nmap is an extraordinary fusion of a potent network exploration tool and a thorough security examiner. It delves deep into uncovering every intricate detail, from exposed ports and operational services to system specifications and update deficiencies. Its reputation as a versatile and comprehensive tool is equally cherished by both network administrators and system operators. What truly distinguishes Nmap is its remarkable adaptability. Users can customize scans to suit their needs, whether casting a wide net or honing in on specific targets. Personally, I seldom opt for the exhaustive approach, as it inundates with an overwhelming flood of data. Instead, I prefer a more precise strategy, focusing on particular facets like filtered ports or operating system versions, where Nmap excels. For penetration testers like us, Nmap represents our initial interaction with a system following the preliminary reconnaissance phase, typically executed with stealth. The likelihood of triggering intrusion detection systems is minimal during Nmap's operation.

Metasploit While its reign as the unrivaled ruler of the exploitation realm may have been challenged by newcomers like Atomic Red Team, Metasploit remains a dominant force in the realm of penetration testing, commanding admiration and esteem. It stands as a powerful ally in both the exploit and post-exploit phases, serving as a trusted companion, especially for newcomers venturing into the realm of penetration testing. What continues to captivate us about

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

Metasploit is its role not merely as a tool but as the ultimate go-to arsenal for crafting, testing, and executing exploit code against remote targets. Metasploit isn't just about identifying vulnerabilities; it's about scrutinizing them, capitalizing on them, and comprehending their real-world exploitability. Even for those who have transitioned to Cobalt Strike, chances are they initially cut their teeth with Metasploit due to its accessibility and user-friendly nature, not to mention its costfree availability.

Offensive distributions For a significant duration, Kali Linux stood alone as the dominant force in this domain, organizing tools meticulously to correspond with the distinct phases of a penetration test. You can practically navigate to the start menu, select your desired phase - be it OSINT, Exploit, Data Exfil, or Forensics - choose a tool, and initiate it effortlessly. However, Kali no longer holds a monopoly in this arena. Enter Parrot OS, which is swiftly gaining traction, particularly in comparison to Kali, especially with influential bodies like EC-Council backing it for their CEH certification modules and exams. Parrot OS is carving its own niche, captivating a wider audience with its intuitive interface and a streamlined environment prioritizing both performance and security. Parrot operates with greater efficiency and sheds the excess baggage often associated with similar platforms.

BURP Suite Now, we're delving into the quintessential gem in my arsenal for penetration testing, particularly in the realm of web application security. BURP Suite stands as an indispensable tool for those deeply committed to unraveling the complexities of web application penetration testing. While it may not boast the same voluminous download statistics as Nessus, BURP Suite remains the steadfast companion of web application security researchers. It embodies a comprehensive solution, serving as an integrated platform renowned for its adaptability and profound capabilities. From conducting scans and spidering to launching attacks and exploiting vulnerabilities, BURP Suite excels in intercepting and manipulating data. It adeptly handles tasks like URL-encoding payloads, modifying delivery methods, and sending requests directly to target websites. As an added bonus, BURP Suite offers one of the most esteemed free training programs, empowering users with insights into leveraging the tool across a myriad of scenarios and objectives.

Nessus Make way for the colossal vulnerability scanner, Nessus, the undisputed champion in revealing network vulnerabilities. In my extensive journey, it stands out as perhaps the most downloaded, employed, and renowned vulnerability scanner in history. Nessus excels in scanning for network weaknesses, configuration discrepancies, inadequate benchmarks, and absent patches, among other critical issues. This isn't just a tool that skims the surface; it delves into the depths, providing insights and discoveries that are both invaluable and exhaustive.

John the Ripper While John the Ripper may not be my go-to tool on a daily basis within the pentesting arsenal, it's a glaring omission to overlook the timeless craft of password cracking in any roundup of pentesting tools. Seasoned pentesters often lean on sturdy tables they've meticulously constructed over the years for dictionary and rainbow table attacks. However, in the absence of such resources, John the Ripper reliably steps up to the plate. This potent password cracking tool is extensively employed to gauge password strength and can proficiently crack an array of password types. Its prowess shines particularly bright when assessing the fortitude of passwords within a network environment.

Top of Form

Wireshark Wireshark may initially be pigeonholed as merely a "packet sniffer," but its versatility and potency push it beyond the boundaries of conventional tools. It's akin to having an unfair advantage. Wireshark stands as a network protocol analyzer revered for its multifaceted utility in network troubleshooting, analysis, development, and educational pursuits. By capturing and presenting real-time data traversing a network, Wireshark facilitates in-depth exploration of network protocols, packet content, and network traffic, providing invaluable insights.

ZAP (Zed Attack Proxy) Welcome to the clandestine weapon of the web application pentesting realm. ZAP, formerly OWASP ZAP, may not enjoy household recognition, but within the inner circles of web application warriors, it commands the same reverence as Nessus does in the domain of network security. It stands as an open-source web application security scanner meticulously crafted to autonomously uncover security vulnerabilities in web applications during the development and testing phases. Operating as an intercepting proxy, ZAP positions itself between your browser and the web application, enabling meticulous scrutiny and manipulation of inbound and outbound traffic. This unique positioning empowers ZAP to detect issues ranging from flawed access control and insecure configurations to other critical vulnerabilities lurking within web applications.

SQL map Picture SQL map as the seasoned veteran of the pentesting arena, not only enduring but flourishing amidst an ever-shifting battlefield of threats. It streamlines the arduous task of pinpointing and capitalizing on SQL injection (SQLi) vulnerabilities within web applications. SQL map operates by dispatching diverse requests to the target web application and scrutinizing the ensuing responses to pinpoint potential vulnerabilities. Upon discovering a SQL injection loophole, SQL map stands ready to extract data from the database, seize administrative control over the database, or even execute remote commands on the server.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

1.4 WHAT IS INVOLVED IN PENETRATION TESTING

There are two areas that should be considered when determining the scope and objectives of penetration testing: testing strategies and testing types used.

1 Penetration Testing Strategies Penetration testing strategies come in three flavors: black box, white box, and gray box. These approaches vary based on the tester's access to information. In black box testing, the testers operate blindly, lacking insight into the test target. They must independently uncover and exploit system weaknesses. This mirrors the blind test approach, mimicking the steps and methods of a genuine attacker who is unaware of the test target. On the flip side, white box testing provides testers with full access to relevant information about the test target. This aligns with focused testing, where the organization and testing team collaborate, furnishing the tester with all necessary information upfront. Gray box testing falls in between, with some information about the test target partially disclosed. Prior to conducting the test, testers must gather additional data. Two penetration testing methodologies exist, each tailored to specific objectives: internal and external testing. External testing encompasses attacks on the test target executed by parties other than the company that owns it. The aim is to ascertain if an external attacker can infiltrate the system and the extent of their potential access. On the other hand, internal testing is performed by employees of the company owning the test target. This approach effectively simulates the potential damage a disgruntled employee could inflict. The objective of internal testing is to assess the ramifications of a successful compromise by an authorized individual with unrestricted access rights.

2 Penetration Testing Types In penetration testing, three elements need to be tested: the system's reaction or workflow, its logical structure, and its physical structure. The scope and methods of penetration testing are defined by these three domains: Network Application Social media manipulation Unearthing security vulnerabilities or other weaknesses within the organization's network architecture, implementation, or operation can be achieved through ethical and secure means via network penetration testing. Testers analyze and exploit potential vulnerabilities to assess whether modems, remote access devices, and maintenance connections could be leveraged to breach the test target. Application penetration testing involves simulating attacks to highlight the severity of genuine, exploitable vulnerabilities, showcasing the effectiveness of an application's security measures. Despite corporations employing monitoring and firewall systems to safeguard information, security can still be compromised due to the potential allowance of traffic flow through the firewall. In the November 2011 edition of the International Journal of Network Security & Its Applications (IJNSA), Volume 3, Number 6, social engineering is discussed as a strategy for acquiring or compromising information pertaining to a company and its computer systems through exploiting human interaction. Its purpose is to gauge the level of security awareness among employees of the company owning the system under scrutiny. This aids in assessing the organization's capability to defend against unauthorized access to its data and data systems.

III. BACKGROUND

. In today's digital landscape, where cyber threats loom large, organizations face constant pressure to safeguard their sensitive data and critical infrastructure from malicious actors. Penetration testing, often referred to as ethical hacking, has emerged as a crucial tool in the arsenal of cybersecurity professionals. It involves simulating real-world cyber attacks to identify vulnerabilities in systems, networks, and applications before they can be exploited by attackers.

Penetration testing serves as a proactive measure to assess the security posture of an organization, helping to identify weaknesses and prioritize remediation efforts. By uncovering vulnerabilities and potential entry points, organizations can fortify their defenses, reduce the risk of breaches, and safeguard their assets.

However, the practice of penetration testing raises important ethical considerations. While the primary objective is to enhance security, ethical hackers must navigate a complex landscape of legal, moral, and privacy concerns. They must ensure that their actions are conducted with integrity, respect for privacy rights, and adherence to applicable laws and regulations.

Exploring the efficacy and ethical implications of penetration testing in network security requires a comprehensive analysis of various factors. This includes evaluating the effectiveness of different testing methodologies, understanding the evolving threat landscape, and examining the ethical dilemmas faced by security professionals.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

Additionally, it is essential to consider the broader implications of penetration testing on organizational security strategies, risk management practices, and regulatory compliance efforts. By gaining insights into the efficacy and ethical considerations of penetration testing, organizations can optimize their security posture while upholding ethical standards and legal requirements.

IV. ANALYSIS AND DESIGN

Efficacy of Penetration Testing:

Effectiveness of Different Testing Methodologies: Evaluate the efficacy of various penetration testing methodologies, such as black-box, white-box, and grey-box testing, in identifying vulnerabilities in network security.

Comparative Analysis: Conduct a comparative analysis of the strengths and weaknesses of different testing approaches to determine which method yields the most comprehensive results.

Impact on Security Posture:

Vulnerability Discovery and Mitigation: Assess the impact of penetration testing on the discovery and mitigation of vulnerabilities within network infrastructures. Measure the effectiveness of penetration testing in improving the overall security posture of organizations.

Reduction of Security Risks: Analyze how penetration testing contributes to the reduction of security risks by identifying and addressing potential entry points for cyber attacks.

Ethical Considerations:

Informed Consent: Explore the ethical implications of conducting penetration testing, particularly regarding obtaining informed consent from stakeholders. Discuss strategies for ensuring transparency and ethical conduct throughout the testing process.

Privacy Rights and Data Protection: Examine the ethical considerations related to privacy rights and data protection when conducting penetration tests. Address concerns about the potential exposure of sensitive information during testing activities.

Legal and Regulatory Compliance:

Compliance with Laws and Regulations: Investigate the legal requirements and regulatory frameworks governing penetration testing activities, such as the Computer Fraud and Abuse Act (CFAA) and the General Data Protection Regulation (GDPR). Analyze the implications of non-compliance and potential legal risks associated with penetration testing.

Organizational Impact:

Integration with Security Strategies: Assess how penetration testing integrates with organizational security strategies and risk management practices. Explore the role of penetration testing in informing decision-making processes and resource allocation for cybersecurity initiatives.

Cultural and Organizational Readiness: Examine organizational readiness and cultural factors that influence the adoption and implementation of penetration testing. Evaluate the level of executive support, resource allocation, and commitment to cybersecurity best practices within organizations.

Continuous Improvement:

Lessons Learned and Best Practices: Identify lessons learned from past penetration testing engagements and establish best practices for future testing activities. Discuss strategies for continuous improvement, such as knowledge sharing, skills development, and collaboration with external security experts.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

V. TECHNICAL AND ECONOMIC ANALYSIS

The examination findings must include suggestions for mitigating or eliminating vulnerabilities. This is what sets apart a security audit from a penetration test. Priority should be given to addressing the most critical vulnerabilities, with a set timeline for verifying the completion of fixes. The identified vulnerabilities, potential business impact if exploited, and the cost-effectiveness of available solutions will all shape the implementation of remedies. To ensure stringent security measures, one option is to subject a new system hosting a web server to a vulnerability assessment before permitting the firewall to open the web port. Alternatively, all domain emails could be routed through a central mail server, which would subsequently distribute them to local host systems. Addressing certain vulnerabilities may simply require enforcing existing policies. For instance, the organization might already prohibit the usage of remote administration software for desktop security. However, additional efforts are necessary to ensure full compliance.

1. Benefits of Penetration Testing from Business Perspective

From a business perspective, penetration testing safeguards the company against failure by preventing financial losses, showcasing compliance and due diligence to shareholders, customers, and industry regulators, and upholding corporate reputation, rendering information security a more sensible financial investment. Organizations invest millions of dollars in recovering from security breaches due to expenses linked with notifications, remediation, lost revenue, and decreased productivity. As per the CSI study, the cost of recovery alone for each incident amounts to $167,713.00. Penetration testing aids in halting financial losses resulting from security breaches by identifying and mitigating risks proactively. In the realm of computing systems, regulatory constraints have been imposed, and non-compliance could lead to severe penalties, including hefty fines, imprisonment, or even business collapse. Penetration testing serves as a proactive measure, providing invaluable insights to help the organization meet regulatory requirements effectively. A single breach of customer data can spell catastrophe, risking not only customer trust but also the reputation and survival of the entire company. Penetration testing fosters heightened awareness of security across all organizational levels, aiding in the prevention of security incidents that could tarnish the company's reputation, harm its corporate image, and erode client loyalty. Penetration testing assesses the efficiency of current security solutions and furnishes compelling reasons for potential investment in or enhancement of security technologies. It serves as concrete evidence of existing vulnerabilities and presents a robust justification for proposing security technology upgrades to senior management.

2. Benefits of Penetration Testing from Operational Perspective Operationally,

penetration testing plays a pivotal role in shaping information security strategy by swiftly and accurately uncovering vulnerabilities, proactively mitigating identified risks, implementing corrective measures, and enhancing IT proficiency. Integrating penetration testing into an organization's security protocols and principles yields exhaustive insights into genuine, exploitable security hazards. Penetration testing aids a company in fine-tuning and validating configuration adjustments or remedies to preemptively address identified risks, providing essential insights to isolate and prioritize vulnerabilities efficiently and effectively. Additionally, a company can leverage penetration testing to assess the impact and likelihood of vulnerabilities, enabling them to categorize reported vulnerabilities as known and implement appropriate corrective measures. Undertaking a penetration test demands a substantial investment of time, effort, and expertise to navigate the complexities of the testing environment. Consequently, penetration testing elevates the overall level of expertise and comprehension across the board.

ACKNOWLEDGMENT

Dreams do not become realities until a great deal of effort and work ethic is put into them, and no commitment produces fruit in the absence of support and direction. It takes a lot of effort to achieve this aim, and having somebody to advise and assist me is always a blessing.

I'd like to take this time to thank a few people who were instrumental in the completion and execution of this research project. To begin, I want to thank God Almighty for making my attempt a success. I'd want to convey my heartfelt gratitude to the JAIN (Deemed-to-be) University for offering superb facilities and other resources that allowed me to hone my talents. I would like to convey my heartfelt thanks to Dr. A. Rengarajan, the research guide, for his unwavering support and insightful ideas, without which the effective completion of this study would not have been possible.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203018 |

VI. CONCLUSION AND FUTURE WORK

A company can also reap rewards from penetration testing by gauging the potential fallout and likelihood of vulnerabilities, enabling them to prioritize reported vulnerabilities and implement necessary corrective actions. Carrying out a penetration test demands a substantial investment of time, effort, and expertise to navigate the intricacies of the testing environment, thereby enhancing everyone's proficiency and comprehension. The methodology outlined in this study comprises three phases: test preparation, actual testing, and test analysis. The testing phase encompasses data collection, vulnerability analysis, and vulnerability exploitation, which can be executed manually or with automated tools. The penetration testing process was exemplified using TuneStore and BOG, two online applications. When presenting test results, testers must adhere to a comprehensive framework. The remediation phase, which encompasses all essential corrective measures for identified vulnerabilities, is crucial during the test analysis process. To enable remediation personnel to replicate and adhere to the attack pattern and associated findings, the final report must provide ample information and depth.

REFERENCES

[1] Bishop, Matt. "About penetration testing." IEEE Security & Privacy 5.6 (2007): 84-87.
[2] Shah, Sugandh, and Babu M. Mehtre. "An overview of vulnerability assessment and penetration testing techniques." Journal of Computer Virology and Hacking Techniques 11 (2015): 27-49.
[3] Al Shebli, Hessa Mohammed Zaher, and Babak D. Beheshti. "A study on penetration testing process and tools." 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2018.
[4] Engebretson, Patrick. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier, 2013.
[5] Geer, Daniel, and John Harthorne. "Penetration testing: A duet." 18th Annual Computer Security Applications Conference, 2002. Proceedings.. IEEE, 2002.
[6] Whitaker, Andrew, and Daniel P. Newman. Penetration Testing and Network Defense: Penetration Testing _1. Cisco Press, 2005.
[7] Abu-Dabaseh, Farah, and Esraa Alshammari. "Automated penetration testing: An overview." The 4th International Conference on Natural Language Computing, Copenhagen, Denmark. 2018.
[8] Weidman, Georgia. Penetration testing: a hands-on introduction to hacking. No starch press, 2014.
[9] Arkin, Brad, Scott Stender, and Gary McGraw. "Software penetration testing." IEEE Security & Privacy 3.1 (2005): 84-87.
[10] Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.
[11] Baloch, Rafay. Ethical hacking and penetration testing guide. CRC Press, 2017.
[12] Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013.
[13] Bacudio, Aileen G., et al. "An overview of penetration testing." International Journal of Network Security & Its Applications 3.6 (2011): 19.
[14] Vats, Prashant, Manju Mandot, and Anjana Gosain. "A comprehensive literature review of penetration testing & its applications." 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE, 2020.
[15] Dalalana Bertoglio, Daniel, and Avelino Francisco Zorzo. "Overview and open issues on penetration test." Journal of the Brazilian Computer Society 23.1 (2017): 1-16

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details