Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 10 October-2024, Page No.- 5335-5337

DOI: 10.47191/etj/v9i10.12, I.F. – 8.227

© 2024, ETJ

Understanding Penetration Testing for Evaluating Vulnerabilities and Enhancing Cyber Security

Rohith Vallabhaneni[1], Vinod Veeramachaneni[2]

[1]School of Computer and Information Sciences, University of the Cumberlands
ORCID: 0009-0003-3719-2704
[2]School of Computer and Information Sciences, Colorado Technical University, USA
ORCID: 0009-0006-6282-6133

ABSTRACT: In response to the increasing incidence of cyber-attacks, organizations are prioritizing security testing for their software applications and products. Among the most effective methods for identifying vulnerabilities is penetration testing, which involves simulated attacks on systems to uncover weaknesses that could be exploited by malicious actors. This method not only aids in identifying and remediating security flaws but also evaluates a system's ability to withstand unexpected threats. This paper provides an in-depth exploration of penetration testing, detailing its stages, methodologies, and the role of web application firewalls. A penetration test systematically assesses the security of IT infrastructures by exploiting vulnerabilities in systems, applications, and user behaviours. The findings from these tests are essential for IT management, guiding strategic decisions and prioritizing remediation efforts. Ultimately, the primary aim of penetration testing is to evaluate the risk of a system breach and its potential impact on organizational resources and operations.

KEYWORDS: Penetration Testing, Cyber Security, Vulnerability Assessment, IT Infrastructure, Security Flaws, Web Application Firewalls, Risk Management, Security Compliance, Exploitation Techniques.

INTRODUCTION

Firms have begun to concentrate on undertaking security testing of their software applications and goods as a result of the rising number of cyber-attacks. Among the most prevalent and commonly utilized approaches for identifying susceptible sections of a program is penetration testing. It entails deliberate attacks on the system to uncover weak points that might allow hostile or unapproved personnel to attack the system and modify its authenticity and validity. This approach aids in the remediation of a variety of security flaws. It also aids in assessing the system's capacity to defend against unforeseen hostile assaults. We'll go through penetration testing in detail in this paper, covering stages, methods, and web applications firewalls.

Penetration Testing

A penetration test is an effort to assess the security of an IT infrastructure by exploiting weaknesses in a secure manner (Collins, 2021). These defects might be found in computer systems, servers, and applications, as well as incorrect setups and unsafe end-user conduct. These tests may also be used to verify the effectiveness of defensive systems and end-user compliance with security regulations. Penetration testing is used to breach servers methodically, interfaces, wireless systems, networking equipment, and other possible sources of vulnerability using human or automated methods (Al Shebli, & Beheshti, 2018).

Once a vulnerability has been properly exploited on one framework, the testing team may use the exploited program to initiate successive vulnerabilities on other centralized resources, particularly by using privilege escalation to gain progressively increased degrees of security clearance and greater depth availability of electronic systems and data. Details on any security flaws effectively exploited via penetration testing are often gathered and delivered to IT and network system management to assist them in reaching strategic recommendations and prioritizing remedial activities. The primary goal of penetration testing is to assess the likelihood of a system breach, as well as any potential ramifications for the resources or activities incorporated.

Five Stages of Penetration Testing

Penetration testing allows you to detect the most vulnerable security flaws before others discover them (Vallabhaneni, 2023). There's much more to it than the act of intrusion, though. Pen testing is a multi-phased undertaking that requires a lot of effort and planning (Adamović, 2019). Reconnaissance is the initial step. The safety analyst gathers knowledge on the subject at this stage (Koroniotis et.al, 2021). This can be performed actively, passively, or both simultaneously. It enables security businesses to collect data on the target network, networking devices, operational machines, system software specifics, and so on. This exercise may be carried out utilizing publicly accessible data and a variety of technologies.

Scanning is the second process. This is an equipment-based stage as opposed to a manual one. The pentester uses one or more scanning instruments to learn more concerning the subject. Pen testers gather as many security flaws as possible using numerous scanners like war dialers (system software that recognizes contact information), network mappers, and security flaws scanners (that detect systemic issues). This allows them to attack a target in a more complex manner.

Gaining access is the third stage. The pen tester seeks to link with the target and leverage the weaknesses discovered in the previous step in this stage. Buffer overflow attacks, denial of service (DoS) attacks, and other types of attacks are possible (Guzman & Gupta, 2017). Generally, a pentester gains access to a system and harvest data and confidential material through various methods. This is proceeded by the fourth step, which is access maintenance. The pentester seeks to develop a doorway for himself in this step. It aids the pentester in locating hidden flaws in the system. The fifth phase is now covering tracks. The pen tester attempts to erase all logs and traces in this step so that the administrator can detect his involvement. This enables the Pentester to behave similarly to an attacker and take remedial steps to counteract the behaviors.

Penetration Testing Methods

Penetration testing can be done in a variety of ways, including external pen-testing, internal pen-testing, targeted penetration testing, blind penetration testing, and double-blind penetration testing. External pen-testing is done by wirelessly accessing your IT infrastructure. Outwardly visible PCs and Web-based gadgets, as well as critical services like web servers, e-mail servers, and firewalls, are all tested throughout this sort of testing (Garg, & Bansal, 2021). The goal is to determine whether an external hacker can obtain access to your networks. It will also demonstrate how far they can explore your systems after access.

IT professionals working in an organization will frequently conduct targeted pen-testing as part of focused penetration testing. Owing to their neutrality, collaborating with a professional 'penetration testing' group will produce superior findings. These tests are sometimes referred to as 'lights-on,' since everyone participating is aware of the test and knows when it will begin and stop. Internal penetration tests are conducted within a company's firewall and use conventional access log files and credentials to simulate a real internal cyber-attack. The goal here is to figure out how much harm and effect a dishonest worker may cause utilizing their regular level of access.

A blind pen-test technique mimics the tactics of an actual cyber attacker (Vats, Mandot, & Gosain, 2020). This is accomplished by giving the tester extremely minimal information prior to the test process. Before they begin working, they may just be provided a firm name or a website URL. Lastly, double-blind pen tests are essentially an enhanced form of the blind test described earlier, in which minimal data is given before the test. This also entails being discreet about the exam as much as feasible to create an extra layer of intrigue.

Penetration Testing and Web Application Firewalls

By examining and screening traffic between each web service and the web, a web application firewall (WAF) aids safeguard a firm's online operations. A WAF is extremely useful for businesses that offer e-commerce sites, online financial services, or any internet-related commodity involving connections with clients or company associates. WAFs can be extremely beneficial in avoiding deception and information theft in these situations.

Any e-commerce website that needs to process confidential client information safely can benefit from a WAF. Companies use a WAF to protect their online applications against sophisticated and targeted assaults such as cross-site scripting (XSS) and SQL injection, which may lead to fraud or data theft (Demetrio et.al, 2020). A WAF also alleviates the administrative load of guaranteeing continuous web security testing. Application security agencies may check what can and cannot be permitted via a WAF by assisting in the preemptive setting of standards and regulations.

CONCLUSION

With cyber-attacks becoming more complex and persistent, it's more critical than ever for businesses to do frequent penetration testing to detect vulnerabilities, plug holes, and guarantee that cyber controls are functioning properly. These tests enable the business to adopt a proactive approach by identifying flaws in its equipment, programs, and individuals to establish consistently outstanding controls that stay current with the ever-changing cyber threat terrain (Vallabhaneni et.al, 2023).

REFERENCES

1. Adamović, S. (2019). Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods. In Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research (pp. 229-234). Singidunum University.
2. 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.

3. Collins, D. (2021). Pen Testing Framework for IoT Devices (Doctoral dissertation, Dublin, National College of Ireland).
4. Demetrio, L., Valenza, A., Costa, G., & Lagorio, G. (2020, March). Waf-a-mole: evading web application firewalls through adversarial machine learning. In Proceedings of the 35th Annual ACM Symposium on Applied Computing (pp. 1745-1752).
5. Garg, D., & Bansal, N. (2021, October). A Systematic Review on Penetration Testing. In 2021 2nd Global Conference for Advancement in Technology (GCAT) (pp. 1-4). IEEE.
6. Guzman, A., & Gupta, A. (2017). IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. Packt Publishing Ltd.
7. Koroniotis, N., Moustafa, N., Turnbull, B., Schiliro, F., Gauravaram, P., & Janicke, H. (2021). A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. arXiv preprint arXiv:2109.09259.
8. 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).
9. Vallabhaneni, R., Maroju, A., Vaddadi, S. A., & Dontu, S, "An Empirical Paradigm on Cybersecurity Vulnerability Mitigation Framework," ed, 2023.
10. Vallabhaneni, R. (2023). Effects of Reduced Security Integrations in Product Development on Data Integrity (Order No. 31561452). Available from ProQuest Dissertations & Theses Global; Publicly Available Content Database. (3106689562). https://www.proquest.com/dissertations-theses/effects-reduced-security-integrations-product/docview/3106689562/se-2