Micah Wieburg - Week 6 - Research Paper

Micah L Wieburg

School Of Computer Information Sciences, University of The Cumberlands

ITS834 - B04: Emerging Threats & Countermeasures

Dr. James Webb

November 23, 2022

Organizations in modern times have placed a heavy emphasis on having strong security policies for IT infrastructure. Information contained within a company's data systems is one of the most vital and sensitive resources they possess. The consequences of a successful infiltration can lead to data breaches which can devastate companies and the user's who utilize their applications and platform. Value is placed in companies' reputations, and there is a certain level of liability for having such a large dataset. Therefore IT security systems must be reliable and resilient. Many strategies are used to test the reliability of security systems, with penetration testing being one of the most useful and popular.

Penetration testing is defined as a testing strategy that mirrors the actions of an actual attacker to implement unauthorized access to a secure information system (Ліцзян et al., 2021). It is a way to evaluate a target system's security, with the objective being to grade the security system's validity against a cyber attack (Satria et al., 2018). Objectives can include finding weaknesses, loopholes, and other exploitations which violate the security policies being tested. Penetration testing benefits have been shown at the application, operating system, and network levels, making it a diverse solution for testing security protocols (Satria et al., 2018). When analyzing and defining penetration testing, it can be broken down into three types, black-box testing, white-box testing, and grey-box testing. Black-box penetration testing occurs when the simulated attack does not know the system or networks being utilized by a company. In this type of testing, the tester's main interest is to obtain information related to the target network (López de Jiménez, 2016). White-Box penetration testing deals with a more informed tester as they initiate testing by knowing the infrastructure at the target system (Satria et al., 2018). Such pre-existing knowledge ranges from operating system details, system source code, and IP addresses (López de Jiménez, 2016). The attack that occurs during white-box testing is designed

to simulate an attack from inside an organization due to the previously mentioned knowledge that the tester already has. Grey-box penetration testing is a blend of black-box and white-box testing, as the tester only has a slight amount of details concerning the structure of the target system. A legitimate external attacker would find themselves in this scenario, which sets the objective of grey-box testing to simulate an attack of an external hacker who has acquired illegal access to a company's network.

Furthermore, a series of stages construct the procedures and steps necessary for successful penetration testing. Each stage has a unique purpose which generally pertains to issues of the systems, the system's test, and provides analysis and solutions (López de Jiménez, 2016). The penetration testing states consist of Planning & Preparation, Reconnaissance, Discovery, Analyzing Information and Risks, Active Intrusion Attempts, Final Analysis, and Report Preparation.

The planning & preparation stage is initialized by characterizing the objectives for the penetration test. These objectives typically consist of identifying vulnerabilities, gaining security validity by a third party, and increasing infrastructure security. When organizations conclude at this stage, a clearly defined set of activities should be presented in great detail, which will occur from the beginning to the end of the penetration test (Alanda et al., 2021).

In the Reconnaissance stage of penetration testing, an analysis of preliminary information is performed. During this stage, testers analyze and gather the proper intel to bridge any gaps in system knowledge and complete a pool of information to guide the penetration testing effort. Although reconnaissance has numerous goals, the main objective is to complete the details as they pertain to the information of the systems (López de Jiménez, 2016).

Next, the penetration testing goes into the Discovery stage. During the discovery stage, the tester will use any available tools to identify any weaknesses in the target system. The primary goal for the tester in this stage is to learn enough about the target system to know which resources to simulate penetration attacks against (Alanda et al., 2021).

After the Discovery stage, the Analyzing Information and Risks stage occurs. In this stage, the tester analyzes the information obtained in previous steps before performing the simulated penetration attacks (López de Jiménez, 2016). The system tester performs analysis based on the goals of the penetration test, any possible risks to the target system, and the estimated time needed to evaluate possible security defects for the forthcoming penetration test.

Then, the testing moves into the Active Intrusion Attempts stage. Activities in this stage are centered on conducting penetration tests against the weaknesses found in the discovery stage, as they carry the highest chance of failure. Within this step, the results of how secure a system is are exposed, making it a crucial stage of penetration testing to provide validation of any possible system weaknesses.

Following the Active Intrusion Attempts stage, the Final Analysis stage is conducted. Within this stage, the penetration tester reflects on the previous steps, especially the Active Intrusion Attempt stage, and provides guidance on removing the weaknesses and risks based on the penetration attack conclusions.

The final stage is the Report Preparation stage. First, the reporting begins by reviewing the testing procedures as a whole. Next, an analysis of the weaknesses and risks is reported and ranked based on the risk associated with that weakness. Additional reporting often includes a summary of the penetration testing, details of the stages and their results, details of the failings

and risks found, details of purging and correcting the tested systems, and recommendations for future security (López de Jiménez, 2016).

In line with many other aspects of IT security, penetration testing comes with its own standards and methodologies. There are a variety of methods, with Open Source Security Testing Methodology Manual (OSSTMM), NIST SP800-115, and Information Systems Security Assessment Framework (ISSAF) being among the most popular (Caselli & Kargl, 2016).

OSSTM is a complete methodology focusing on finding security tests and audits to evaluate security systems. OSSTM provides benefits to testers by creating operation modules, each with a specific objective and assignment, and explains the necessary assignments to accomplish those objectives. Every module is subject to input, which illustrates the details required to execute the assignments, and output which is the outcome of any successful assignments.

NISTSP800-115 is a method supplying directions on executing and analyzing IT security testing and planning (Caselli & Kargl, 2016). About penetration testing, NISTSP800-115 gives guidance and details on the technical aspects of the process. Three phases have been identified within the NISTSP800-115 method. These methods are planning, execution, and post-execution. The planning phase concentrates on gathering information about system security details such as threats, assets, and pre-existing security strategies. Execution is concerned with identifying vulnerabilities and how those weaknesses can be exploited. In the execution phase, penetration testing exists in three steps: review techniques, target identification and analysis techniques, and target vulnerability (Caselli & Kargl, 2016). The review technique sub-step of the NISTSP800-115 will analyze assets and pre-existing security policies, the target identification and analysis

techniques step will define ways to find possible targets, and the target vulnerability step determines ways to test the weaknesses found (Caselli & Kargl, 2016).

ISSAF is a methodology that encompasses several facets of security evaluations, primarily security assessments, and lives as a critiqued and organized framework. Security assessments covered by the method can range from critical business assets to pragmatic approaches such as testing user details and system infrastructure security. Meeting the assessment requirements of participating companies tends to serve as the focal point in this methodology (López de Jiménez, 2016). ISSAF provides three stages and nine assessment steps for penetration testing (Caselli & Kargl, 2016). Planning and preparation, Assessment, and Reporting clean-up and destroy artifacts comprise the three stages (Caselli & Kargl, 2016). Practical operations are utilized to find and take advantage of system weaknesses during the nine assessment steps. ISSAF defines these nine assessment steps: Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromising Remote User Sites, Maintaining Access, and Covering Tracks (Caselli & Kargl, 2016).

Web applications have become an essential requirement in the modern digital era that has grown in importance parallel with internet usage (Alanda et al., 2021). Since web applications exist on the open web, a high level of security is required to preserve and protect the integrity of any connected data storage infrastructure against potential cyber-attacks. To stay present with threats against web applications, the Open Web Application Security Project (OWASP) exists to recognize and contest threats impacting software by executing security assessments and investigations. OWASP efforts include the production of the OWASP Guide and a document containing the most impactful vulnerabilities, known as the OWASP Top 10 (López de Jiménez,

2016). While OWASP provides a comprehensive list of web applications vulnerabilities, penetration testing can also be performed on web applications against those threats mentioned in the OWASP Top 10. Web penetration testing is a strategy used to test an application's code, back-end vulnerabilities, the current operating system, and data accessed by the application (Shebli & Beheshti, 2018).

Firewalls often serve as the first line of defense against a cyber attack. They must be resilient enough and sophisticated to repel unauthorized activities. For validation of this layer of security, firewall penetration is commonly applied. Firewall penetration testing is used to penetrate system firewalls to discover vulnerabilities in the firewall configuration (Shebli & Beheshti, 2018). Testing results supplement efforts to identify errors in the firewall configuration and areas in which it can be fortified.

Penetration testing is a strategy that provides an abundance of benefits to organizations attempting to eliminate critical vulnerabilities in their systems. Attack simulations give a clear picture of the issues and ways to mitigate the impact discovered during the penetration test. The various stages and methods deployed along with penetration testing create a diverse and capable approach to strengthening security systems in a world with constantly evolving cyber threats.

References

Ліцзян, Д., Вейлін, Ц., Рабчан, Я., Давидов, В., & Мірошніченко, Н. (2021). ANALYSIS AND COMPARATIVE STUDIES OF SOFTWARE PENETRATION TESTING METHODS. *Advanced Information Systems*, *5*(2), 136–140. https://doi.org/10.20998/2522-9052.2021.2.20

Satria, D., Alanda, A., Erianda, A., & Prayama, D. (2018). Network Security Assessment Using Internal Network Penetration Testing Methodology. *JOIV : International Journal on Informatics Visualization*, *2*(4–2), Article 4–2. https://doi.org/10.30630/joiv.2.4-2.190

López de Jiménez, R. E. (2016). Pentesting on web applications using ethical - hacking. *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, 1–6. https://doi.org/10.1109/CONCAPAN.2016.7942364

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021). Web Application Penetration Testing Using SQL Injection Attack. *JOIV : International Journal on Informatics Visualization*, *5*(3), Article 3. https://doi.org/10.30630/joiv.5.3.470

Caselli, M., & Kargl, F. (2016). *A Security Assessment Methodology for Critical Infrastructures*. 332–343. https://doi.org/10.1007/978-3-319-31664-2_34

Shebli, H. M. Z. A., & Beheshti, B. D. (2018). A study on penetration testing process and tools. *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–7. https://doi.org/10.1109/LISAT.2018.8378035

Pradeep, I., & Sakthivel, G. (2021). Ethical hacking and penetration testing for securing us form Hackers. *Journal of Physics: Conference Series*, *1831*(1), 012004. https://doi.org/10.1088/1742-6596/1831/1/012004

Alchinov, A. I., Polovneva, S. I., & Ivashchenko, G. A. (2021). Methods of testing computer systems for various kinds of penetration. *Journal of Physics: Conference Series*, *2032*(1), 012134. https://doi.org/10.1088/1742-6596/2032/1/012134

Ghanem, M. C., & Chen, T. M. (2020). Reinforcement Learning for Efficient Network Penetration Testing. *Information*, *11*(1), Article 1. https://doi.org/10.3390/info11010006

Zhou, S., Liu, J., Hou, D., Zhong, X., & Zhang, Y. (2021). Autonomous Penetration Testing Based on Improved Deep Q-Network. *Applied Sciences*, *11*(19), Article 19. https://doi.org/10.3390/app11198823