International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 983-986 www.ijaem.net ISSN: 2395-5252

Study on issues and challenges onadvancement of Penetration Testing

Thanes Parmesivan[1], Mohamad Fadli Zolkipli[2]
School of Computing, University Utara Malaysia, Sintok,Kedah,Malaysia.
School of Computing, University Utara Malaysia, Sintok, Kedah,Malaysia.

Submitted: 15-03-2022 Revised: 25-03-2022 Accepted: 28-03-2022

ABSTRACT—Penetration Testing is one of the ways to identify the vulnerabilities in the system and servers. It helps the pen tester to conduct real attack towards organizations. The penetration testing is authorized access where it identifies the capabilities of its IT infrastructure. The researcher explains about the challenges and issues when conducting to the penetration testing. The problem raises from all the perspectives on the penetration testing. At the same time, the penetration testing aims to address issues and gaps of the organization's system. The researcher emphasizes the importance of background verification of the penetration testing team and it's always better to hire reputable company.

Keywords: Penetration Testing, Hacking, Issues, Challenges, Pen Tester.

I. INTRODUCTION

Information Security is one of the critical elements where it includes the system, hardware, that stores data and information. Machines and computers connected to the internet are significantly increasing and so does growth of IP addresses. Many organizations are struggling to protect and secure the data and information. The purpose of Penetration testing is to simulate real attacks that will help detect the loopholes in the system and applications. Penetration testing, also part of analysis and identification of any potential vulnerabilities, misconfiguration, software vulnerabilities, and operational weakness in process and procedure and it's countermeasures. The Penetration testing is categorizedto 5 phases. First will be Reconnaissance, which is the process of collecting information and data before conducting any attack. Second phase is Enumeration, the process of analyzing the system for any potential flaws, such as insufficient or wrong system configuration, hardware, and software flaws, and procedural or technological countermeasure operating flaws. Third phase is Vulnerability Analysis, this process will be conducted to identify any potential security weakness on network, application and system. Fourth phase is Exploitation where the expert will penetrate using many techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities. Last phase is reporting, where the expert will provide comprehensive reports which include steps on how toidentify the vulnerabilities and how it's exploited. In the end of the report, the expert also will provide overall findings and mitigation plan. In other words, penetration testing will make sure that security measure is in place to secure information and data.

II. LITERATURE REVIEW

According to the (Yaacoub, Noura, Salman, & Chehab, 2021), the security attacks keep increasing and the researcher explains on the penetration testing. The objective of penetration testing is to reduce number of vulnerabilities and the effect of the attacks. The penetration testing is highly recommended to be conducted and provide the mitigation. The penetration testing will stimulate the real attack where will be identifying the vulnerabilities and exploit on the system and servers. The researcher also explains the disadvantages of penetration test. The fundamental problem with penetration testing is ineffective at detecting known vulnerabilities. The researcher also provide suggestions on adopting the anomaly detection of intrusion prevention system.

According to the (Kumar, Khera, Sujay, Garg, & Jain, 2018), hacking on cybersecurity isgrowing. The hacking can be done in many ways to disrupt the organization by stealing data and information. The researcher also explains the data breaches, probability of threat and vulnerabilities. The researcher also explains the ethical hacking which is known as Penetration Testing to find the weakness on the organization. This paper also explains different phases of ethical hacking that can be conducted. The intention of ethical hacking to test security capabilities of the organization.

According to the (Shetty & Shetty, 2019), the researcher explains about hacking and the impacttowards businesses and governments. The intention of hackers to launch hacking is to steal information for future use, manipulation of data, and disrupting the services that is offered by the government. Lastly, it is the most common approach by hackers to get ransom. Ethical hacking is one of the effective ways to find the vulnerabilities before the real attack is launched by the attacker. At the same time, it provides the solution to fix or close the security gaps. The researcher further describes the types and its impact on private businesses and government institutions.

The researcher (Chowdappa, Lakshmi, & Kumar, 2014), discuss about ethical hacking using penetration testing. This paper also explains how hacking is being conducted in different phases. The researcher made a comparisonof ethical hacking with different methods of penetration testing.

According to the (Johari, Kaur, Tripathi, & Gupta, 2020), penetration testing is performed to detect security threats. The researcher identified that penetration testing stimulates cyber-attack to check on the vulnerabilities. Penetration testing is used for testing network, servers, and application and now its required to Internet of Things (IoT) as well. In the next few years, IoT will evolve and there will be increased risk on the IoT networks. On the other hand, the researcher suggested to use Vulnerability Assessment and Penetrating Testing (VAPT) approach on the Internet of Things (IoT).

In this paper, the researcher (Svenmarck, Luotsinen, Nilsson, & Schubert, 2018) discuss about the Artificial Intelligence (AI) military application and its threats. The researcher focuses on the AI based application challenges on the vulnerabilities, and the user has limited knowledge on use of the application. The researcher suggests conducting the Penetration Testing on automated application to prevent exploit of security weakness. In conclusion, the researcher also provides how to fix the challenges.

Penetration testing can be able to access the software system to find the vulnerabilities and where it can be exploited by hackers(Rahman, Akond, Williams, & Laurie, 2019).This research paper also explains on the strategies and guidance on how to get started in the domain of penetration testing. Comprehensive research would help the cyber-security community enhance the domain of cyber-security by identifying practitioners' knowledge gaps linked to penetration testing. The purpose of this study is to assist cyber-security researchers in furthering the field of cyber-security education.

III. ISSUES AND CHALLENGES

Most of the organizations want to conduct penetration testing to check in house security capabilities. An organization might hire pen tester without verifying the background of the tester. The hired pen tester should be familiar with the system and tools that are to be tested. There might be issues and risks associated without verifying the pen tester. Inexperienced pen tester might cause disastrous outage due to misuse of tools. Other technical difficulties includeusage of exploit codes that might cause services to become unavailable or systems to become unstable. After launching an attack, the pen tester shall be able to stop in the event of issues and unwanted incident towards business. The target infrastructure or system will crash during a penetration test. As a result, the penetration testing team is only allowed to utilize a limited number of ways to avoid downtime or system failures.

Limited expert and manpower can't perform penetration testing on certain domains. The penetration testing can be divided into many categories such as application, network, Internet of Things (IoT) and Artificial Intelligences domains. The skillful pen tester won't be able to conduct on certain domainswhere they don't have experiences and will give high-quality penetration test results and findings.

Cost is also one of the key challenges in conducting thepenetration testing and the organization also requires identifying and closing the security gaps on their environment (Maurushat, 2019). The penetration testing will be divided into two phase deliverables. During the first phase, the pen tester will be identifying the vulnerabilities on the environment. On the second phase, the pen tester will deliver the recommendation and mitigation plans to the organization. There will be separate charges for each phase.

The Pen tester in some scenarios, might find the vulnerabilities that can be able to open access from the backdoor of the system or server. The pen tester could open and fail to protect the backdoor and real attacker may discover it.

As penetration testing vendor face challenges when delivering reports to the clients,the test reports produced by the vendor after penetration testing may be ignored, arguing that the findings are not critical and will have no impact on their infrastructures. The client shouldn't interfere in the reporting and findings by penetration testing. At the same time, the pen tester shouldn't alter or remove the findings found in the client environment. The pen tester should always maintain their ethical integrity during the penetration testing phases (Ashraf & Habaebi, 2013).

Communication among the management and project team is a common issue running in most of the organizations. The communication plan might not be broadcasted to the engaging team and the team only discovers when the alerts are received. Most of the issues are due to internal political tension within the project, which could lead to project delay.

Conducting the Penetration Testing won't be able to identify all the vulnerabilities due time constrain and restriction. Normally, organizations will define the time frame to conduct penetration testing and its limitations. Penetration tester is also required to take screenshot with every single step and is required to be included in the final report. The attacker would take more than days and months to find the vulnerabilities even to exploit it (Shravan, Neha, & Pawan, 2014).

Some organizations won't be able to test all systems and servers because of limited scope, budget, and time constrain. Since the scope of a pen test is limited to one system, vulnerabilities arising from system interactions will not be found. Risk is there with organization due to insufficient scope of penetration testing which impacts the later stage. The penetration tester might reuse previous test findings, ensuring the reports are delivered.

In most scenarios, the penetration tester might use same exploit code to test in the client environment. The penetration team must create specific exploits that works in both safe and non-secure situations. By running specific scripts, it will help define the path of the intrusion to reach the target for a pen test and also part of creating a custom exploit. Even the penetration tester won't have sufficient time to create new exploit code which are newly identified as vulnerabilities on their client environment.

Another misconception in the organization is that by conducting the penetration testing, cyber-attack will not occur in their organization. Organization should aware that by conducting the penetration testing will only reduce the likelihood of cyber-attack which help address the vulnerabilities and gaps that found in their organization.

Most of the organizations manage to fix the issues with remediating the issues within the organization. As pen tester will provide comprehensive analysis and report without any prejudice by conducting penetration testing in specific time frame. From the organization's perspective, identifying that remediation and mitigation plans are challenging.

IV. DISCUSSION

Penetration Testing becomes achallenge and seen a lot of issues while conducting or post penetration testing to both organization and the penetration testing team or vendor. Based on the issues and challenges that were discussed earlier, organization should be clear and define the objective, scope of the system and servers, and its timeline. At the same time the penetration testing should clearly define with right frameworks. In another scenario, the challenges are associated with both parties agreement and ensuring that there is no impact towards the business interruption and less impact on the target system and servers. The organization should take care of the communication among project team and management. The scope should be defined and agreed upon by both parties before proceeding with penetration testing. The organization should hire penetration testing vendor with certified pen tester and verify their certification on the system.

Benefits	Challenges
Penetration Testing allows the detection of all system flaws and the implementation of appropriate safeguards.	Doesn't have expertise on the certain domain areas.
Red flag on the findings of the vulnerabilities.	Insufficient time to conduct penetration testing.
Penetration testing alsoaimsto complywith security requirements set out by industry norms and laws.	Due to heavy scanning and automated technologies, there have been several unforeseen technical difficulties.
Assess the abilities to defend against Cyber-Attacks	Only focused on the testing and critical system and services.

Figure 1: Benefits and Challenges

The above tableshows brief summary of the benefits and challenges on the Penetration Testing.

CONCLUSION

In this paper we have discussed the factors to consider when conducting the Penetration testing to help the organization to identify and target the vulnerabilities on the organization. At the same time, there are issues and challenges in conducting the penetration testing with both parties. The organization should properly verify and hire well known penetration tester.The company should sign Non-Disclosure Agreement with the company before proceeding with the penetration testing. The integrity of conductingpenetration testing should be maintained all throughout the process. There is a possibility that a pen tester could damage the organization's system and servers which may expose the sensitive data if something goes wrong. The organization should be always cautious and consider the limitations which can cause impact on the organization. Eliminating penetration testing is not an ideal approach, it can always put the organization at risk and the effective security procedures and processes to ensure that proper tests are carried out.

REFERENCES

[1]. Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES. A PREPRINT, 46.

[2]. Kumar, D., Khera, Y., Sujay, Garg, N., & Jain, P. (2018). TOWARDS THE IMPACT OF HACKING ON CYBER SECURITY. IIOAB Journal, 18.

[3]. Shetty, S., & Shetty, K. (2019). Ethical Hacking: The Art of Manipulation. International Journal of Advanced Scientific Research and Management, , 4.

[4]. Chowdappa, K., Lakshmi, S., & Kumar, P. (2014). Ethical Hacking Techniques with Penetration Testing. International Journal of Computer Science and Information Technologies,, 5.

[5]. Maurushat, A. (2019). Ethical Hacking. Ethical Hacking.

[6]. Ashraf, Q. M., & Habaebi, M. H. (2013). Towards Islamic Ethics in Professional Penetration Testing. Revelation and Science.

[7]. Shravan, K., Neha, B., & Pawan, B. (2014). Penetration Testing: A Review. COMPUSOFT, An international journal of advanced computer technolog, 7.

[8]. Johari, R., Kaur, I., Tripathi, R., & Gupta, K. (2020). Penetration Testing in IoT Network. IEEE.

[9]. Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018). Applications, Possibilities and Challenges for Artificial Intelligence in Military. In Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. Neuilly-sur-Seine France.

[10]. Rahman, Akond, Williams, & Laurie. (2019). A bird's eye view of knowledge needs related to penetration testing. Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security. New York, NY, USA},: Association for Computing Machinery.