Design and Implementation of an Integrated Internal and External Vulnerability Assessment and Penetration Testing Technique

Saheed K. A.
Department of Computer Science
Babcock University
Illishan-Remo, Nigeria
saheed0099@pg.babcock.edu.ng

Ogunlere S. O.
Department of Information Technology
Babcock University
Illishan-Remo, Nigeria
ogunleres@babcock.edu.ng

Abstract:

The existence of zero-day vulnerabilities and Advanced Persistent Threats (APTs) makes it critical to explore the internal and external Vulnerability Assessment and Penetration Testing Technique (VAPT), testing strategy which can identify the most severe cybersecurity flaws and risks. Various VAPT methods has been established, but there is no model that was designed to integrate the internal and external VAPT testing strategy to mitigate attack and reduce vulnerabilities. From the findings, there are a total of 10 (ten) vulnerabilities in the application environment. 2 (two) were discovered to be of Critical severity, 1 (one) of high severity, 3 (three) of medium severity, 4 (four) low severity. The vulnerabilities which have different risk ratings were unknown to the vendor or developer of the application which in turn led to zero-day vulnerabilities from the findings of this research work. In the final analysis, the practical model design of hybrid VAPTs testing strategy was discovered to be more efficient and effective in identifying and mitigating the most severe cybersecurity flaws such as the zero-day vulnerability before being exploited by a malicious hacker, and thus reduces the risk of holes in application.

Keywords: *Internal VAPT, External VAPT, Application security testing, Risk ratings, Vulnerabilities*

1.0 INTRODUCTION

The protection of information is a critical function for all enterprises, industries, and modern societies. According to ISACA (2017), information security entails information irrespective of the format such as paper records, digital and intellectual property in people's minds, and verbal or visual communications. The protection of digital assets that is, everything within network hardware, software and information that is processed, stored within isolated systems, or transported by internetworked information environments is termed cybersecurity. Cybersecurity is a component of information security. Cybersecurity usually relates to an entity initiating threats due to the existence of a global cyberspace that is Internet (ISACA, 2017). Cybersecurity requires stakeholders in the cyberspace area to be active in security, beyond the protection of their own assets. They should be prepared to identify and address emerging risk and challenges to keep assets protected. Cybersecurity works with information security and is beyond merely Internet, network and/or application security. It requires working with all these components to keep the cyberspace useful and trustworthy.

Cybersecurity via ethical hacking plays a key part in the strengthening of organization security posture and also Internet Services. Improving cybersecurity and guarding critical information infrastructures are vital to each country's security and economic good fortune. Making the customer information's harmless and guarding Internet users most especially in the digital world has become essential to the growth of new services. Ethical hacking is simply allowing good hackers to obtain access to organization infrastructures and systems to avert the bad hacker from doing harm. The US Department of Defense, which is one of the world's most secured organization, has permitted their systems to ethical hacking. An ethical hacker is also called white hat hacker, they analyze data security structures by means of penetration testing to detect weaknesses in applications, systems, and networks. They present companies with insights to proactively handle the safety of their assets and information (Banerjee, 2019).

The core duty of cybersecurity is to identify, mitigate and manage cyber-risk to an organization's digital assets. Cyber-risk is that portion of overall risk management that solely focuses on risk that manifests in the cyber (Interconnected Information Environments) domain. Knowing how to determine, measure, and reduce risk effectively is crucial in the context of cybersecurity. One of the most crucial tasks of a cybersecurity organization is evaluating risk.

Understanding the risk and threats an organization is dealing with are all reliant on efficient policies, security executions, resource allocation and incident response readiness. Applying a risk-based method to cybersecurity permits more informed decision-making to safeguard the organization and to use limited budgets and resources effectively. If controls are not applied based on awareness of actual risk, so valuable organizational assets will not be sufficiently safeguarded while other assets will be inefficiently overprotected (Anderson, 2018).

2.0 RELATED WORK

The field of ethical hacking has been of interest to a lot of researchers and several VAPT life cycles have been introduced.

Ahmad and Sanjudharan (2020) proposed that ethical hacking is a huge prospect in the near future as a career that the study opens new entryway into a huge career in the field of ethical hacking. Chandrakant and Prakash (2019) concentrated on creating cyber security awareness and its significance at numerous levels of an organization for acceptance of required up to date security measures by the organization to stay secure from countless cyberattacks. Shahidullah (2019) and Božić et al, (2019) work mentioned that internal and external testing are the two ways weaknesses seen however there is no practical model that was designed to implement the internal testing, and external testing strategy.

Khera et al, (2019) work proposed that due to digitalization and increasing cyber-attacks that there is need to skill up and for more security. Maurushat (2019) study is about hacking companies per se, however case studies from several incidences were explored. Incidents of security weakness were reviewed. Teimoor (2019) described how hackers collect information's and why they are not caught by others and explained every step by which to protect and when we will know how the hackers enter organization system and how they control any network and how we can stop them.

Ding et al, (2019) study carried out qualitative research supported by literature expert and survey interviews to explore how Bug Bounty Programs (BBP) and Responsible Disclosure (RD) can ease the practice of identifying, classifying, prioritizing, remediating, and mitigating IoT vulnerabilities in cost-efficient and an effective manner. Gartner (2018) research assists risk management and security heads identify the best Security Operation Centre (SOC) model for their firm. The research suggested the use managed security services (MSSs) to relief the cost of 24/7 SOC operations and to fill coverage and skills gaps, either tactically or as part of the long-term strategy.

Pandey (2018) study proposed a hypothetical concept to the rise in development and digital revolution and proposed using AI to prevent hackers to access network either by computer network or IoTs. Singh and Singh (2017) created a framework to exam the tools and to offer a mechanism to secure the system from being hacked. This study used various tools from Kali Linus OS and used on a created framework to provide a suitable method(s) to defend the systems. The outcomes from the several tools established that if the system is not secure, then there is the possibility of hacking.

Goel and Mehtre (2015) proposed that a new VAPT techniques and tools could be developed for future work, that their work would be very helpful for future academics to obtain far-reaching knowledge of VAPT techniques, tools, and process. Panikar (2015) study focused on information gathering of a network using Metasploit. Definite techniques and measures are being proposed in this study to determine and avert exploitation of Attacks with Manual Pen testing.

Umrao and Kaur (2012) study focused on the penetration and vulnerability tests that give security, a proper way to recognize and assess system flaws and then lessen the risks depending on the outcomes of such tests. However, the study proposed a concentrate on practical implementation of VAPT by means of tools like CAIN & ABEL, NMAP, METASPLOIT, WIRESHAPR, ETTERCAP, and NESSUS. There is lack of concentrate on practical implementation of VAPT using suitable baseline tools.

However, from the literature review there is no detail research on the security testing method that is hybrid in nature (external and internal VAPT) security testing strategy. There is the need to proactively prevent persistent cybersecurity attacks such as APTs and zero-day attacks.

2.1 Limitations or gaps of the existing techniques

The disadvantages of the existing techniques are as follow:

1. There is no practical model that was designed to implement the internal testing, and external testing strategy.
2. The existing techniques presented did not take care of increasing cyberattack such as APTs caused by zero-day vulnerability.
3. There is inadequate external testing research to exploit vulnerabilities that could be discovered by a hacker from the internet. Hence, this can lead to ineffective discovery of loopholes.
4. There is the absence of hands-on measures in identification, exploitation, remediating, and mitigating of cybercrime, attacks and websites hacking tricks.
5. There is lack of simulation of attack on the internal and external network by mimicking the actions of an actual threat actor.
6. There is insufficient test that would display whether the applied security actions are sufficient to protect a company and to evaluate its ability to guard against any outside attack.

3.0 THE CONCEPTUAL DESIGN OF THE PROPOSED MODEL

The proposed detailed technique of the hybrid VAPT security testing strategy and model for mitigating against real attack in achieving the stated objectives of this research is discussed in this section.

3.1 Analysis of the proposed technique

A VAPT exercise will typically encompass the following phases: Intelligence Gathering, Vulnerability Analysis (Scanning), Exploitation, Post Exploitation and Reporting. The practice of testing for the cybersecurity vulnerabilities of application system, software, wireless systems, and employees, networks, computers, and devices, is termed ethical hacking. They could be either external or internal subject on the aim of the task but for more effective and quick identification of vulnerabilities and remediation both external and internal testing can be combined. An external VAPT testing research which scan for and exploit weaknesses that could be executed by an external ethical hacker with appropriate consent from the organization. While the internal VAPT testing is like a vulnerability assessment and tries penetration within the organization, it takes a scan one step further by trying to exploit the weaknesses and determine what information is unprotected.

Each of the VAPT steps that is (Intelligence Gathering, Vulnerability Analysis (Scanning), Exploitation, Post Exploitation and Reporting) is applied to both the internal and external security testing strategy and the scope is added which helps in narrowing the research work to either Network, Infrastructure, Web Application, Application Software or Data Security testing. Also, the reporting step is divided into technical report (for cybersecurity experts) and executive report (for executive or business managers) as illustrated.

- Determine the Scope.
- Conducting an External Intelligence Gathering
- Conducting an Internal Intelligence Gathering
- Conducting an External Vulnerability Analysis
- Conducting an Internal Vulnerability Analysis
- Conducting External Exploitation
- Conducting Internal Exploitation
- Conducting External Post-Exploitation
- Conducting Internal Post-Exploitation
- Technical and Executive Reporting

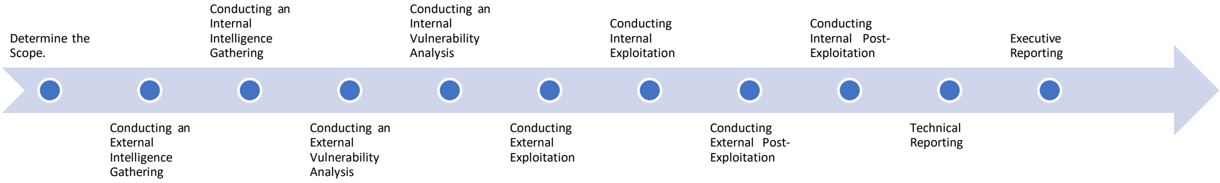
Determine the Scope.
Conducting an External Intelligence Gathering
Conducting an Internal Intelligence Gathering
Conducting an External Vulnerability Analysis
Conducting an Internal Vulnerability Analysis
Conducting External Exploitation
Conducting Internal Exploitation
Conducting External Post-Exploitation
Conducting Internal Post-Exploitation
Technical Reporting
Executive Reporting

Figure 1: Integrated External and Internal VAPT Stages. (Researcher's Model, 2022).

1. Determining the Scope: The scope of the work was determined which was limited to only application testing. An application was selected for the testing.

2. External Intelligence Gathering: Searching for web application and subdomains, find the type of web application framework, the version and type of a running web server and identify application architecture from the internet.

3. Internal Intelligence Gathering: Finding all the live host / assets related to the application, and Identify all the open ports and services from within the organization network.

4. External Vulnerability Assessment: Discovery all vulnerabilities, evaluating the security posture, finding hidden directories and file names and utilize publicly available research from the internet.

5. Internal Vulnerability Assessment: Uncover all vulnerabilities, find hidden directories and file names and utilize publicly available research from inside the organization network.

6. External Exploitation: Exploits associated vulnerabilities, analyses the source code, compromise identified vulnerable application from the internet.

7. Internal Exploitation: Exploits associated vulnerabilities, analyses the source code, compromise identified vulnerable application from inside the organization.

8. External Post-Exploitation: Escalating privilege to root user, retrieving credentials stored, utilizing the harvested credentials and removing all traces of the testing from the internet.

9. Internal Post-Exploitation: Escalating privilege to root user, retrieving credentials stored, utilizing the harvested credentials and removing all traces of the testing from inside the organization network.

10. Technical and Executive Reporting: The technical report is for cybersecurity experts and IT Security professional and executive report is business managers and executives.

4.0 IMPLEMENTATION, RESULTS AND DISCUSSION OF FINDINGS

4.1 System Requirement:

The objective of preparing the laboratory requirements is to provide better information in such a manner that ultimately leads to successful external and internal testing activities. The basic requirements (Tools, Techniques and Resources) for this technique which based on the defined scope (application testing).

4.1.1 Hardware Requirements

1. Processor: Inter® Core™ i5- 8265U CPU
2. Installed Physical Memory /Random Access Memory (RAM): 8 Gigabytes and above.
3. Hard disk: 500 Gigabytes and above.

4.1.2 Software Requirements

1. Operating System (OS): Window 10 Pro (64 bit)
2. A system with Virtual box (preferably)
3. Kali Linux which can be downloaded from https://www.kali.org/downloads/.
4. Access to proprietary tool
5. Good Internet Access.
6. Search engine hacking (google)

4.2 Summary of Key Findings

Each vulnerability or risk identified has been categorized as a Critical, High, Medium, or Low risk. The risk involved in harboring the threat and how it would be easier for a hacker to exploit the issues and a recommendation.

A total of 10 (ten) vulnerabilities in the application environment. 2 (two) vulnerabilities were discovered to be of Critical severity, 1 (one) vulnerability was discovered to be of high severity, 3 (three) vulnerabilities were discovered to be of medium severity, 4 (four) vulnerabilities were discovered to be of low severity. Find below a summary of key findings discovered.

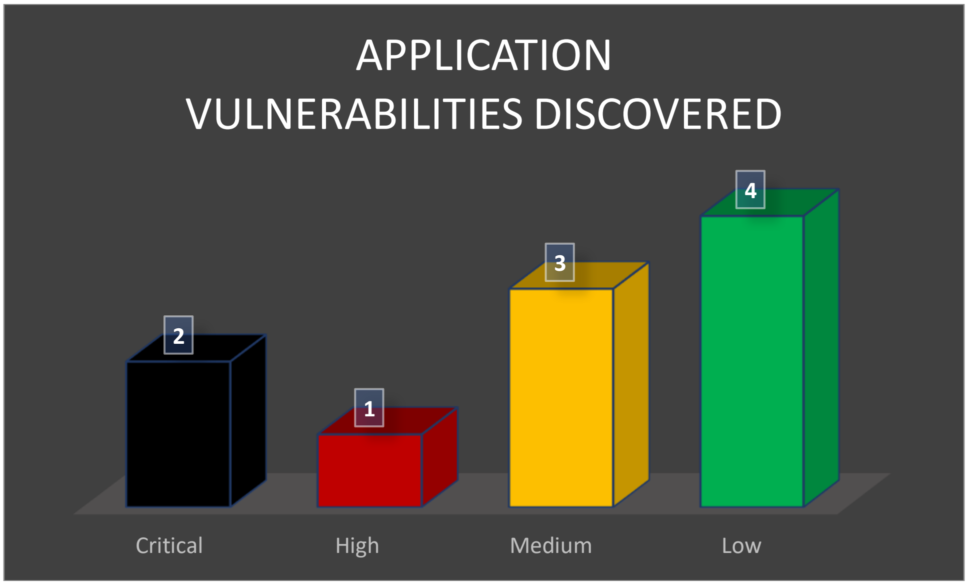

Figure 2: Application Vulnerabilities Discovered

4.3 Vulnerability Remediation Steps and Roadmap

1. The SameSite attribute should be set to either ‘lax’ or ideally ‘strict’ for all cookies.
2. The cookie should be passed using an encrypted channel and the secure flag is set for cookies containing such sensitive information.
3. The javaScript source files should be loaded from only trusted sources and the sources should not be controlled by the end users of the application.
4. The web browser’s XSS filter should be enabled by setting the X-XSS-Protection HTTP response header to ‘1’.
5. The Content Security Policy, X-Frame-Options and Permissions Policy should be enabled and configured on the application.
6. Use a server side, secure, built-in session manager that generates a new random session ID.
7. Applying a system that provide a unique error reference to the user browser while logging the details on the server side and not exposing them to the end user.
8. Upgrade the Apache Tomcat version to new version supported by the application.
9. The use of an encoding library that is Microsoft Anti-cross-site scripting or OWASP ESAPI.
10. Use parameterized queries and the data access layer (DAL) within the architecture, the use of DAL will help centralize the issue and ease its resolution.

5.0 SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

The existence of zero-day vulnerabilities and advanced persistent threats (APTs) made it critical to integrate the internal VAPT, and external VAPT security testing strategy which was applied to identify vulnerabilities in the application before hacker exploit them unknowingly. The purpose of the study was to; design and implement an integrated internal VAPT, and external VAPT security testing model with focus on application security testing.

The vulnerabilities discovered in the web application environment which have different risk ratings which were unknown to the vendor or developer of the application which in turn led to zero-day vulnerabilities to the company using the application on the production (live) environment. If no concrete and necessary actions are taken to identify and mitigate the vulnerability, the risk of exploit via APT increases significantly if the vulnerabilities identified are not addressed.

The approach adopted for this work was an integration of internal and external VAPT process. This is an approach that companies and organizations can use to discovered zero-day vulnerabilities on applications and ultimately prevent APTs attacks

5.2 Recommendations

Academic recommendations - Additional research that should be done includes:

- The use of the integrated internal and external VAPT techniques should be introduced to other area such Networking and IT Infrastructure in the future.

  Practical, real-world suggestion –

- Additional licensed VAPT tools should be purchased or subscribed to, for organizations to assist in improving the quality of VAPT process and produce fast, quick, and more reliable results.
- Also, security awareness should be increased for both cyber security experts and non-security experts on the use of the integrated internal and external VAPT techniques.

5.3 Conclusion

The result of this work can be used to prevent persistent cybersecurity attacks such as zero-day vulnerabilities efficiently and proactively which improves security of the application and system after using the model designed.

6.0 REFERENCES

Ahmad, Z. & Sanjudharan, M. (July 2020). Practice of Ethical Hacking in the Banking Sector. *Retrieved from* *https://www.researchgate.net/publication/343064340*.

Anderson, K. (2018). A Business Model for Information Security. *Retrieved from ISACA® Journal, Vol. 3,*

Banerjee, A. (2019). Ethical Hacking: Keeping Data Safe in the Financial Services Industry.

Božić, K. , Penevski, N. , Adamović, S. (2019). Penetration Testing And Vulnerability Assessment: Introduction, Phases, Tools And Methods. *DOI: 10.15308/Sinteza-2019-229-234. Retrieved from* *https://www.researchgate.net/publication/333292138.*

Chandrakant, B. & Prakash, J. (2019). Vulnerability Assessment and Penetration Testing As Cyber Defence. *Retrieved from International Journal of Engineering Applied Sciences and Technology, 2019 Vol. 4, Issue 2, ISSN No. 2455-2143, Pages 72-76 Published Online June 2019 in IJEAST (http://www.ijeast.com)*

Ding,A ., Limon, G., Janssen, M. (2019).Ethical Hacking for IoT Security:A First Look into Bug Bounty Programs and Responsible Disclosure

Gartner, Inc., (2018). Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing.

Gartner, Inc., (2018). Selecting the Right SOC Model for Your Organization. *ID: G00363821*

Goel, J & Mehtre, B. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science 57 (2015) 710 – 715 1877-0509. Published by Elsevier B.V.doi:10.1016/j.procs.2015.07.458 ScienceDirect.Available online at Retrieved from* www.sciencedirect.com *3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)*

ISACA. (2017). Cybersecurity Fundamentals Study Guide, 2nd Edition

Khera, Y. , Kumar, D. , Sujay, G. , Garg, N. (2019). Analysis and Impact of Vulnerability Assessment and Penetration Testing. *DOI: 10.1109/COMITCon.2019.8862224. Retrieved* *from* https://www.researchgate.net/publication/336439468

Maurushat, A. (2019). Ethical Hacking.University of Ottawa Press (UOP) Library and Archives Canada Cataloguing in Publication. *ISBN 9780776627915 (softcover) | ISBN 9780776627922 (PDF) | ISBN 9780776627939 (EPUB) | ISBN 9780776627946 (Kindle)*

Pandey, N. (2018). Network Security and Ethical Hacking. *J Comput Sci Syst Biol 11: 254-255. doi:10.4172/jcsb.1000282*

Panikar, S. (2015). Strengthening Infomation Security With VAPT. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 6, June 2015.*

Shahidullah,M. (2019). Vulnerability Assessment Penetration Testing (VAPT) for Web Applications. *EasyChair Preprint № 2100*

Singh, H. & Singh, J. (2017). Analysis of Various tools of Penetration Testing. *International Journal of Advanced Research in Science and Engineering (IJARSE) Volume 6 Issue 7, ISSN (O)2319-8354, ISSN (P)2319-8346, Pages 1184-1195, www.ijarse.com, July 2017.*

Teimoor,R. (2019). Ethical Hacking and Knowledge about Hacking :A Brief about Whitehat Hacking And Its Techniques. *Retrieved from https://www.researchgate.net/publication/333632435.DOI: 10.13140/RG.2.2.17344.79362*

Umrao, S. & Kaur, M. (2012). Vulnerability Assessment And Penetration Testing. *Retrieved from* https://www.researchgate.net/publication/303859587*. International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, 2012*