International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 09 | Sept-2020 ISSN: 2582-3930

VULNERABILITY ASSESSMENT & PENETRATION TESTING FRAMEWORK

Anay Devale[1], Akshay Mahajan[2], Shrishti Singh[3]

[1]*Padmabhooshan Vasantdada Patil Institute of Technology, Savitribai Phule Pune University*

[2]*Padmabhooshan Vasantdada Patil Institute of Technology, Savitribai Phule Pune University*

[3]*Padmabhooshan Vasantdada Patil Institute of Technology, Savitribai Phule Pune University*

Abstract -The process of performing a Vulnerability Assessment and penetration test is to verify that a network or a system is not vulnerable to a security risk that could allow unauthorized access to resources. The intended users of our framework are the organizations who might be consideringhaving a penetration test performed or who wants to certify themselves according ISO standards 27001. The process of performing a penetration test is complex, hence we have developed this framework to make it easy. This framework consists of a variety of tools which helps the users of this framework to perform vulnerability assessment and thereby per-form Penetration Testing on those scanned vulnerability. In the end, a consolidated report of results from the tools will be generated in text format. Such reports are further analyzed and patched by the Security experts.

***Key Words*:**Network, Scanning, Auditing, Testing, Wireless security, Information security, Penetration, Exploitation, Assessment, Vulnerability.

1.INTRODUCTION

The primary reason for testing the security of an operational system is to identify potential vulnerabilities and subsequently repair them. Nowadays it has become a common practice for the organizations to standardise themselves according to the ISO 27001 security policies. According to the compliance of various multinational companies (top companies in the _eld), a lot of national level companies and the need to make themselves secured. A large number of industry standards regulations have included Vulnerability Assessment Penetration Testing (VAPT) as a mandatory requirement in today's market. The number of computers per person in many organizations continues to rise, increasing the demands on competent and experienced system administrators.

1.1. PROBLEM STATEMENT

1. The primary reason for testing the security of an operational system is to identify potential vulnerabilities and subsequently repair them.

2. The number of computers per person in many organizations continues to rise, increasing the demands on competent and experienced system administrators.

2.LITERATURE SURVEY

1. **Vulnerability Assessment Penetration Testing as a Cyber Defence Technology**.

Author: Narayan Goel, BM Mehtre, Computer Engineering

Department School of Computer and Information Sciences, University of Hyderabad, Hyderabad 500046, India

Abstract: Complexity of systems are increasing day by day. This leads to more and more vulnerabilities in Systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before attacker do. The power of Vulnerability assessment is usually underestimated. While Vulnerability Assessment and Penetration Testing can be used as a cyber-defence technology to provide proactive cyber defence. In this paper we proved Vulnerability Assessment and Penetration Testing (VAPT) as a Cyber defence technology, how we can provide active cyber defence using Vulnerability Assessment and Penetration Testing. We described complete life cycle of Vulnerability Assessment and Penetration Testing on systems or network and proactive action taken to resolve that vulnerability and stop possible attack. In this paper we have described prevalent Vulnerability assessment techniques and some famous premium/open source VAPT tools. We have described complete process of how to use Vulnerability Assessment and Penetration Testing as a powerful Cyber Defence Technology. In this paper we proved Vulnerability Assessment and Penetration Testing (VAPT) as a Cyber defence technology, how we can provide active cyber-defence using Vulnerability Assessment and Penetration Testing.

2. **Vulnerability Assessment and Penetration Testing**.

Author: Ankita Gupta, Kavita, Kirandeep Kaur.

Abstract: Vulnerability assessment and Penetration Testing (VAPT) is the most comprehensive service for auditing, penetration testing, reporting and patching for your c o m p a n y ' s web-based applications. With port 80 always open for web access there is always a possibility that a hacker can beat your security systems and have unauthorized access to your systems. Vulnerability assessment and penetration testing are two different and complimentary proactive approaches to assess the security posture of an information system's network.

3. An Automated Approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0.

Author: Sugandh Shah, B.M. Mehtre.

Abstract: With increasing world-wide connectivity of Information systems, and growth in accessibility of data resources, the threat to the Integrity and Confidentiality of Data and Services has also increased. Every now and then cases of Hacking and Exploitation are being observed. So, in order to remain immune and minimize such threats, the Organizations conduct regular Vulnerability Assessment and Penetration Testing (VAPT) on their Technical Assets [1]. We at IDRBT have developed a new automated VAPT Testing Tool named NetNirikshak 1.0 which will help the Organizations to assess their Application/Services and analyse their Security Posture. NetNirikshak 1.0 detects the vulnerabilities based on the applications and Services.

3.SYSTEM REQUIREMENTS

Software Requirements(minimum)
1. Operating System- Linux (Ubuntu).
2. Pre-requisites- Python libraries, Nmap, Metasploit, PostgreSQL.

Hardware Requirements(minimum)
1. Processor- Intel Pentium, Core 2duo, i3 and later.
2. For Network environments- LAN, Wi-Fi adapters.

4.SPECIFICATION

4.1 Advantages:

- When it comes to security, VAPT excessive advantages to an organization, let's look at a few of its benefits.
- Providing the organization, a detailed view of potential threats faced by an application.
- Help the organization in identifying programming errors that leads to cyber-attacks. Provide risk management.
- Safeguards the business from loss of reputation and money.
- Secures applications from internal and external attacks.
- Protects the organizations data from malicious attacks.

4.2 Limitations:

- The framework can easily be detected by Intrusion Detection System Firewall and flag it off as a virus.
- Often fail to notice the latest vulnerabilities.

4.3 Applications:

VAPT is done on a large scale on various platforms which are as follows
- In Banking sectors, the system should be secured on a level of 100 percent accuracy rate.
- Multinational companies perform VAPT to keep their Information Security maintained.
- ISO Implementation can be done on the basis of VAPT generated reports.
- Finding security loopholes like Open TCP ports which can be used by intruders to exploit the network/system.
- Exploiting the vulnerability present in the system.
- It gives us the brief idea about how severe the attack is and what damage could it cause to our system.

5.SYSTEM ARCHITECTURE

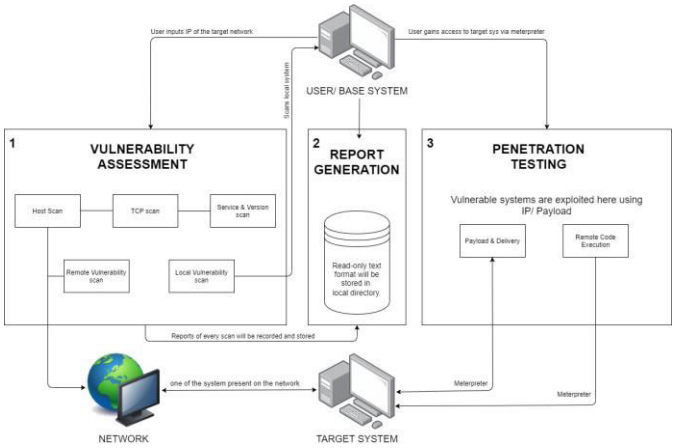

Fig -1: System Design

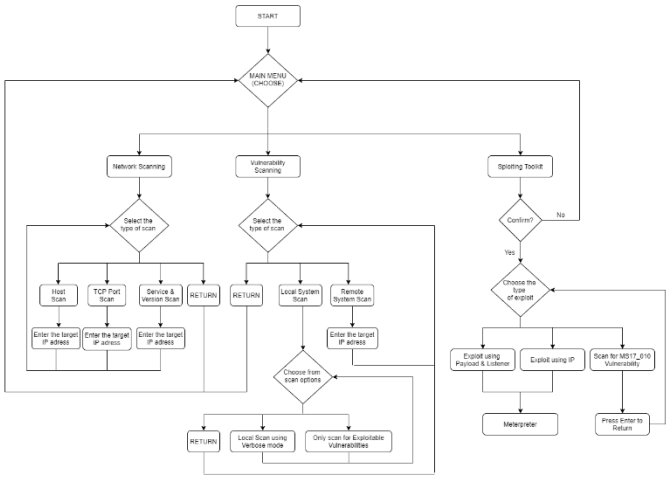

Fig -2: Flowchart

6.CONCLUSIONS

By implementing this framework in a particular organization, it helps them to certify themselves as an ISO certified organization. As this VAPT framework includes all the protocols and policies which are stated and needed according to the ISO 27001 controls. This certification also helps the organization to gain reputation in the _eld of security; due to which they can boom their businesses. Protecting and maintaining the overall Information Security of any organization is a main concern. VAPT makes sure that this main concern is addressed.

7.FUTURE WORK

- Implement the framework using the Python libraries over the internet and make it accessible from any time anywhere.
- Improvement of the GUI making it more user friendly.
- Can be implemented over a Web App currently it is running on a system's terminal.
- Provide security patches for the vulnerabilities detected.

ACKNOWLEDGEMENT

With immense pleasure, I am presenting this preliminary report on “Vulnerability Assessment and Penetration Testing” as part of the curriculum of B.E. Computer Engineering. I wish to thank all the people who gave me an unending support right from the stage the idea was conceived. I am thankful to my Guide Prof. S. R. Javheri for her great support throughout the course of this report activity. I am also thankful to our Seminar Coordinator Prof. P. P. Dandavate for conduction of report activity. I also thank all to those who have directly or indirectly guided and helped in preparation of this report. I express a profound thanks to our respected Head of the Department Dr. B. K. Sarkar whose advice and valuable guidance helped in making this presentation successful.

REFERENCES

[1] The Multi-Tool Web Vulnerability Scanner - The ultimate goal of this program is to solve this problem through automation. https://github.com/skavngr/rapidscan

[2] Vulmap Online Local Vulnerability Scanners Project- Vulmap is an open source online local vulnerability scanner project. It consists of online local vulnerability scanning programs for Windows and Linux operating systems. These scripts can be used for defensive and offensive purposes. It is possible to make vulnerability assessments using these scripts. https://vulmon.com

[3] Cyber security analysis using vulnerability assessment and penetration testing. Published in: 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Start-up Conclave).

[4] The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. https://en.wikipedia.org/wiki/MetasploitProject