International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1459-1463www.ijaem.net ISSN: 2395-5252

A Comparative Analysis of Web Penetration Testing Tools

JatinKushwah, KushagraDutt Sharma, Raj Jhunjhunwala, Tanisha Duggal, RuchiParashar

Department of Computer Science and Engineering, Dr Akhilesh Das Gupta Institute of Technology and Management, New Delhi

Submitted: 25-06-2021 Revised: 06-07-2021 Accepted: 09-07-2021

ABSTRACT: With the increased utilization of the internet and enabled services, cybersecurity has become crucial for small and big businesses. Companies around the world are withstanding cyberattacks from a range of sources. Each of them agrees that constant upgradationofthe security system to fight against cyberattacks has become the need of the hour. Vulnerability Assessment and Penetration Testing (VAPT) is amethodologyimplemented to recognise the weaknesses and test them to analyse their exploitability. This makes VAPT crucial to validate the security mechanisms of the system and the outcome of the process can be used to secure the network. This research contains an overview of some commonly used VAPT tools. It is a technique that is used for keeping the high-security levels in the system by the effective study of loopholes present in the security system.

Keywords- Vulnerability Assessment and Penetration Testing, Vulnerability Scanners, Penetration Testers

I. INTRODUCTION

Cybersecurity assessment comprises methods and procedures applied to estimate the effectiveness of cybersecurity controls in a digital system. The methods and workflows in particular are used to check for the planning, implementation and correct execution of the security controls, operating as originally intended to, and are producing the desired result concerning &meeting the security parameters specified by the asset owner(s). Cybersecurity assessment is thus far the prime reliable method of researching and concluding if a system has been, and continues to be continually configured to the correct security protocols and policy.

Primary cybersecurity assessment activities include network scanning, vulnerability scanning, and penetration testing.

II. BACKGROUND

VAPT

Vulnerability Assessment & Penetration Testing (VAPT), both cover the execution of different processes aimed to secure web application(s), however, both are closely knit with each other. Vulnerability assessment, as a procedure, caters information about potential vulnerabilities, while penetration testing procedure involvesexploiting vulnerabilities to assume a certain risk level. The mechanism for VAPT is illustrated in figure 1. as under.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1459-1463www.ijaem.net ISSN: 2395-5252

Fig. 1 - General VAPT process model

Vulnerability assessment & its tools find out the vulnerabilities present in the system, but are unable to filterflaws which are prone to exploitation and causing actualdamage, and those that cannot. Vulnerability scanners are a continuously growing set of tools which alert the user(s) about the present flaws in their system and its location(directory).

Penetration tests always look to misuse the vulnerabilities in systems to ascertain unauthorized access or other suspected activity is possible, and identify which faults pose potential threats to the application. Penetration tests discover exploitable faults and measure their severity in the system. It depicts how damaging a fault could be in a real attack.

Together, penetration testing &vulnerability assessment tools encompass a detailed analysis of the flaws that exist in an application and the risks associated with those flaws.

III. LITERARY SURVEY

S. Shah and B. Mehtre (2014) described the four phases of vulnerability assessment and penetration testing. The security process comprises of two major parts: Vulnerability Assessment (VA) and Penetration Testing (PT). This research demonstrated the various phases and methodologies of VAPT. For VAPT, various commercial and open-source tools are available. The author selected the Open-Source Tools for each of the categories of testing in VAPT. The research also presented the comparative analysis of all the methodologies and techniques which are used in VAPT with precautions and standards.

D. Rushing, J. Guidry and I. Alkadi (2015) illustrated the collaboration between penetration testing and analysis toolkits. Penetration testing commonly known as pen testing is very critical in increasing and maintaining the reliability of computer networks while decreasing their vulnerability. The value and importance of these networks have grown from an earlier time. This research described the software project surrounding network penetration testing from the collaboration standpoint. All the problems and solutions presented in it have been utilized by the network analysis tools and technologies.

A. Piskozub and R. Banakh (2016) described automated and manual penetration testing which is a methodology for the ensuring security of the information. The author highlighted various benefits and drawbacks of penetration testing. In this research, penetration testing was used for determining the potential of systems that are subverted by malware and hacking schemes using the same manner as the attacker's application. Due to many different vulnerabilities in the security sections, it was concluded that manual penetrating tests were more useful and popular.

Zena and T. Hayajneh (2017) investigated various features of penetration testing which includes the attack methodologies, tools, and defence strategies. Penetration testing secures the networks and highlight the various issues of security. During this research, various penetrating tests were performed with the help of the virtualized systems and tools, private networks and devices. The tools used are within the Kali Linux suite.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1459-1463www.ijaem.net ISSN: 2395-5252

D. Bertoglio and A. Zorzo (2017) demonstrated the overview and open issues of penetration test. This research described various methodologies, tools, models, challenges, and application scenarios that are used for security testing. This research highlighted the several aspects and the solutions in relation to Pen-testing. Also, the author classified the models and tools used for it. The research through its results helped define the testing scope and evaluate the various tools and methodologies under analysis.

IV. TOOLS ANALYSIS

The security checking methodology, Vulnerability Assessment and Penetration Testing, comprises of a seriesof activities that can be implemented manually and using software tools. Along with proper subject expertise and experience, the right selection of software utilities and tools is very important for making any VAPT project successful. The following are some of the commonly used VAPT tools.

NIKTO

Nikto is a server scanning security web tool that tests a website for as many potential security issues. It checks for malicious files, misconfigured & misbehaving services, vulnerability-causing scripts and other such issues. It is open-source in nature and is robustly structured with numerous plugins to further expand the capabilities. These plugins are preferably &frequently updated with latest security checks.

Features

- SSL Support
- Full HTTP proxy support
- Scans multiple ports on a server, or multiple servers via input file
- Subdomain guessing

Advantages

- Versatile tool
- Runs on any OS
- Multiple report formats
- Open-source, so easier integration

Disadvantages

- Command line execution
- No GUI

NMAP (Network Mapper)

Nmapis an open-source scanner for discovering networks and auditing security. Countless system administrators and network admins use it for the inventory maintenance of the network, scheduling services and their upgrades, and further monitoring host and/or service uptimes. It uses unfiltered IP packets such that help in detecting the hosts at the disposal of the network, the services being offered by those hosts, the OSs they are on, the type of filters and/or firewalls for packets currently in practice, and other such characteristics is done. It is designed to accelerate the speed of scanning large networks but working finely against single hosts.

Features

- Host discovery
- Port specification and scan order
- Service detection
- OS detection
- Target detection

Advantages

- Light weight
- GUI and command line versions
- Fast and flexible

Disadvantages

- Lack of ability to export the information in a readable format
- Some scans can trigger sensitive IDS/IPS

SQLMAP

sqlmap, or SQL-MAP, is an open-source pentesting tool which enables the automation of detecting, and furthermore, exploiting the countless SQL injection faults, followed byhijacking of the database servers. It has a competitively powerful fault-detection engine, numerous niche features that aid to an ultimate penetration testing experience, along with a wide spectrum of switchesbelonging to database fingerprinting, useful in accessing the file system underlaid, and executingseveral different commands on the operating system.

Features

- Full support for DBMS
- Enumerates automatically database information
- Supports different attack vectors

Advantages

- Powerful enumeration functionalities
- Attack features allows to exploit most systems

Disadvantages

- Limited search of vulnerabilities

THEHARVESTER

TheHarvestercan be describe as a program that collects e-mail addresses, subdomains and their hosts, open ports, etc. from numerous sources available to the public, for example- search engines, key servers for PGP and computer DBs.Crafted to help Pentesters in the initial stages of penetration testing to gain insights on the customers and theirfootprintsall over the Internet. It is of immense use to anyone who wishes to unravel

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1459-1463www.ijaem.net ISSN: 2395-5252

what a potential attacker might discover about their organization.

Features

- Delays time between request
- Searches all available resources
- Verifies virtual hosts
- Active enumeration
- Scans open ports and banner due to integration with SHODAN computer database

Advantages

- No complex coding is involved
- Robust reporting
- Excellent user experience

Disadvantages

- Bugs
- Less flexible

Wfuzz

Wfuzz is a tool devised for brute-forcing Web Applications. It is used for discovering resources not linked (directories, servlets, scripts, etc), brute-force GET and POST parameters for checking diverse kind of injections (SQL, XSS, LDAP, etc), brute-force forming parameters (User/Password), Fuzzing, etc.

Features

- Multiple Injection points capability with multiple dictionaries
- Recursion
- Post, headers and authentication data brute forcing

Advantages

- Many customization options
- Versatile tool

Disadvantages

- RAM eater
- High CPU usage even with sort lists
- Slow

COMPARISON

Tool/ Vulnerability Exploited	Port & IP	Sub domain	Data base	Email	System details
Nikto	✓	✓			
NMAP	✓				✓
SQLMAP			✓		
TheHarvester	✓			✓	
Wfuzz		✓	✓		

V. CONCLUSION

Our thorough VAPT tool analysis concludes the usability of penetration techniques and how effectively they can help in identifying the potential quantity and scale of threats to the security system of the company with the possible ways in which they can be removed or eliminated. VAPT, therefore, is a vital method that boasts the potential of pre-stopping any kind of hacking and cyber-theft of critical data, organizational info, or any monetary theft. The likely ways and methods which are used in this technique take out an acute observation on all the aspects of collecting previously recorded data to threat verification, and proving the solution to the vulnerabilities and increasing the efficiency of the system. In the aforementioned research, we used the Kali Linux Operating System, for it provides numerous security-oriented tools that help in performing penetration testing efficiently. Furthermore, it provides several other tools that can be used in protecting the system from vulnerabilities. This research adopted tools from Kali Linux OS and then implemented a created framework to provide a proper technique(s) to protect the systems. The results from the various tools inferred that if the system is insecure, then there is a hazard of it being hacked. The system demands that it be secured by using firewall protection, the server should also be secured with encryption-based security, and many

other security measures ought to be followed for a 'completely secured' system. The individual results of the tools help in ascertaining the elements required to protect the system from unauthenticated access. The research has also explained, in-depth, the apex of time when there is a requirement of conducting penetration tests to the security system of an organization.

REFERENCES

[1]. S. Shah and B. Mehtre, "An overview of vulnerability assessment and penetration testing techniques", J ComputVirol Hack Tech
[2]. D. Rushing, J. Guidry and I. Alkadi, "Collaborative Penetration-testing and Analysis Toolkit", IEEE
[3]. Piskozub, R. Banakh and Y. Stenfinko, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency", TCSET
[4]. Zena, T. Hayajneh and M. Denis, "Penetration testing: Concepts, attack methods, and defense strategies", New York Institute of Technology
[5]. Bertoglio and A. Zorzo, "Overview and open issues on a penetration test," Dala Lana Bertoglio and Zorzo Journal of the Brazilian Computer
[6]. Nikto tool https://hackertarget.com/nikto-website-scanner/, https://www.hacking.reviews/2017/10/nikto-v216-web-server-scanner.html?m=0
[7]. NMAPtoolhttps://www.trustradius.com/products/nmap/reviews?qs=pros-and-cons
[8]. SQLMAP tool https://alpinesecurity.com/blog/sqlmap-sucking-your-whole-database-through-a-tiny-little-straw/
[9]. TheHarvestertoolhttps://tools.kali.org/informationgathering/theharvester,https://www.trustradius.com/products/harvest/reviews?qs=pros-and-cons
[10]. Wfuzz tool https://pentestbook.six2dez.com/others/web-fuzzers-comparision