International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

A Comparison Study of Open Source Penetration Testing Tools

Nilesh Bhingardeve[1], Seeza Franklin[2]
[1]Student, [2]Professor
Bharati Vidyapeeth's Institute of Management & Information Technology,
C. B. D. Belapur, Navi Mumbai, Maharashtra, India

ABSTRACT

Penetration testing also known as Pen Test is a series of activities which is performed by authorized simulated attack on computer system, network or web application to find vulnerabilities that an attacker could exploit. It helps confirm the efficiency and effectiveness of the various security measures that have been implemented. In the world of Open Source Software, even Penetration Testing is not untouched.

The purpose of this pilot study was to compare various the open source penetration testing tools.

Keywords: *cyber security, testing, network*

I. INTRODUCTION

Penetration testing should be an essential factor of cyber security strategy of any government or private organization. A penetration test doesn’t ends at simply discovering the vulnerabilities: it goes the subsequently step to enthusiastically exploit those vulnerabilities in order to confirm (or contradict) real-world attack vector s in opposition to an organization’s IT assets, data, humans, and/or physical security. [1] Penetration testers attempt to compromise systems using the same tools and techniques as malicious attackers thus attempting to identify vulnerabilities before an attack occurs.

To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing). [2]

Web Application Security with automated penetration testing tools generates relatively quick and easy results. However there are a lot of such tools, both commercial and free. In this research paper a selection of such tools are tested against a number of different test cases to compare the tools and find out the quality of such tools. There are thousands of open source security tools available in software testing market with both defensive and offensive security capabilities. The following are 6 essential security tools that will help you to secure your systems and networks. These open source security tools have been given the essential rating due to the fact that they are effective, well supported and easy to start getting value from:

1. Nmap
2. Metasploit
3. Wireshark
4. Aircrack-ng
5. John the Ripper
6. Sql map

II. OBJECTIVES

Objective of the Study is to compare various security testing tools features particularly used in penetration testing

III. LITERATURE SURVEY

The literature study of the penetration testing will address aspects regarding how much the network is vulnerable or the system and what are the loop holes to enter in the system and what effort to break in to the system whether the access is restricted or the target is remotely located.

IV. METHODOLOGY

The idea behind this particular section is to reveal the rationale for the research methodology, the method and strategy adopted in collecting data for the research. This part also seeks to reveal the comparison of security testing tools.

The researcher has used secondary data which were gathered from diverse source, including archival sources, journals, articles and internet sites and blogs.

V. BRIEF OVERVIEW OF OTHER TOOLS

1. Nmap: It also known as "**Network Mapped**": is an open source licensed and free tool for the network discovery .It is mainly also used in security auditing. Network administrator's tasks include managing service upgrade schedules, network inventory, monitoring service or host up time and much more. Besides the network administrators, Nmap is used by system which uses raw IP packets which are in a novel way determined what the hosts have available on the network and which services those hosts are actually offering. That refers to the application name and its version.

   Zenmap is the authorized graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, free and open-source tool designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

   Ncat: is a debugging tool, redirection and the utility for comparing the scan results-Ndiff. And that is not all. It is hard to catch everything that this amazing tool can achieve! It contains a packet generation and the response analysis tool which is called Nping.

2. Metasploit: Metasploit is a open source platform which enables you to develop and execute exploit on target machine. It is a platform which is used to perform tests on computer system to find out vulnerability. It performs authorized simulated attack on computer system looking for weaknesses in network. It allows the network administrator to break own system to find security issues in network. Metasploit is a security project which provide information about vulnerability in the system.

3. Wireshark: Wireshark is a network or protocol analyzer (also known as a network sniffer). Wireshark allows the user to see all the traffic being passed over the network. It is used to analyze the structure of different network protocols. It operates on Unix, Linux and Microsoft Windows operating systems. The tool essentially captures data packets moving within a network and displays them back to the end user in a human-readable form. Wireshark allows users to capture data via ethernet, Wi-Fi, NpCap adapter, bluetooth, and token ring to name the few. It even allows users to capture data from USB-attached network interfaces through USBPCAP. Wireshark even comes as a console version with name 'tshark.'

4. Aircrack-ng: Aircrack-ng is a suite of wireless password cracking tools for the 802.11a/b/g family of wireless networks that supports raw monitoring (rfmon) mode. It captures network traffic in monitor mode and once enough data is captured it runs cracking algorithms to recover WEP and WPA keys. The Aircrack-ng suite consists of various tools such as Airodump-ng (a packet capturing program), Airsnort-ng (an encryption key cracker), Aireplay-ng (for traffic generation), and Airdecap-ng (a captured file decryption tool).

5. John the Ripper: John the Ripper (often referred to as 'John' or JTR) is a very popular password cracking tool. JTR is primarily used to perform dictionary attacks to identify weak password vulnerabilities in a network. JTR is an offline password cracker that can be invoked locally or remotely. It also supports brute force and rainbow crack attacks.

6. Sqlmap: This penetration testing tool automates the process of finding and exploiting SQL injection vulnerabilities in a website's database. Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

VI. COMPARISION OF VARIOUS TOOLS

Features	Nmap	Metaploit	Wireshark	Aircrack	John the Ripper	Sqlmap
Flexible	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Powerful	*Yes*	*Yes*	*Yes*	*Yes*		
Portable	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Easy	*Yes*	*Yes*		*Yes*	*Yes*	*Yes*
Free	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Well-documented	*Yes*		*Yes*		*Yes*	
Supported	*Yes*		*Yes*		*Yes*	*Yes*
Acclaimed	*Yes*	*Yes*	*Yes*			
Popular	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

VII. CONCLUSION

The conclusion that we get from this research that efficient testing requires suitable tools that can be integrated to the security testing process. Scope of the penetration testing should be increased. Time period of penetration testing is very limited and it needs to be increased so the testing team can identify more issues and can protect the network security of an organization. After finding the vulnerability action to be taken as soon as possible to protect the network.

VIII. REFERENCES

1. https://tools.kali.org/information-gathering/nmap
2. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwi82o2sqenaAhUIyLwKHUnWCp4QFggzMAI&url=http%3A%2F%2Fmeity.gov.in%2Fcontent%2Fnational-cyber-security-policy-2013-0&usg=AOvVaw1Yk5sXhsIcfYtmG47T7_E_
3. https://www.synopsys.com/blogs/software-security/top-10-free-hacking-tools-for-penetration-testers/
4. https://hackertarget.com/10-open-source-security-tools/