A Comparison Study of Penetration Testing Tools in Linux

Mr. Lijo Zachariah, Prof. Sudeshna Roy

Abstract-- Penetration testing also known as Pen Test is very searing concept in the area of security testing nowadays. With the change in the way computer systems are used and built these days, security takes the limelight. It is the sequence of activities which is accomplished by authorized simulated attack on computer system, network or web application to find vulnerabilities and susceptibilities that an attacker could exploit. It helps to confirm the proficiency and efficacy of the various security measures that have been implemented.In the domain 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 available in Linux.

Key Words--cyber security, testing, network

1. INTRODUCTION

Penetration Testing is a method of testing in which the areas of weakness and flaws in the software systems in terms of security are put to test to fix, if the 'weak-point' is indeed one, that can be broken into or not on various Websites/Servers/Networks.
using the same tools and techniques as malicious attackers thus endeavoring to identify vulnerabilities before an attack befalls or occurs.

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

Steps Performed in Penetration Testing:

Step #1. It is initiated with a enlisting the Vulnerabilities or potential problem or threat areas that would cause a security breach for the system.
Step #2. List of items are ranked as per order of priority or criticality
Step #3. Plan penetration tests that would work (attack your system) from both within the network and outside (externally) are done to determine if you can access data, network, server, website unauthorized.
Step #4. If any unauthorized access is possible, then the system has to be corrected and the series of steps need to be re-run until the problem area is fixed. [3]

Comprehensive list of the best Penetration Testing tools are as follows:

1. Nmap
2. Netcat
3. Unicornscan
4. OpenVAS
5. Nikto
6. WPScan
7. CMSMap
8. Fluxion
9. Aircrack-ng

2. OBJECTIVES

Objective of the Study is to compare various security testing tools featuresparticularly used in penetration testing in Linux.

3. LITERATURE SURVEY

The literature study of the penetration testing will project the 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.

4. METHODOLOGY

The idea behind this particular section is to disclose the reason for the research methodology, the method and strategy adopted in collecting data for the research. This part also seeks to reveal the comparision 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.

5. BRIEF OVERVIEW OF OTHER TOOLS

5.1 Nmap

Also known as "**Network Mapped**", is an open source licensed and free tool for the network discovery. It is widely used in security auditing. A Network administrator's responsibility vitally includes managing service upgrade schedules, network inventory, monitoring service or host up time etc. Besides network administrators, Nmap is also used by system which includes raw IP packets which are in a novel and unique way to determine what the hosts have available on the network and which services those hosts are actually contributing.
Zenmap is an authorized graphical user interface (GUI) tool for the Nmap Security Scanner. It is a multi-platform tooland open-source tool which is designed and intended to make Nmap easy for learners to usage while providing innovative features for experienced Nmap users.

5.2 Netcat

Netcat is a network exploration application that is not only predominant among those in the security industry, but also in the network and system administration fields.

Ncat: is a debugging tool, redirection and the utility for comparing the scan results-Ndiff. It comprises a packet generation and the response analysis tool which is known as Nping.

- Host discovery: used for discovery hosts in any network
- Port scanning: helps in enumerate or count open ports on the local or remote host
- OS detection: useful for fetching or getting operating system details and hardware
  information about any connected device
- App version detection: permits to decide application name and version number
- Scriptable interaction: extends Nmap default competencies by using Nmap Scripting Engine (NSE)

It is principally used for outbound and inbound network inspection and port investigation; it's also valuable when used in combination with programming languages like Perl or C, or with bash scripts.

Netcat's main features include:

- TCP and UDP port analysis
- Inbound and outbound network sniffing
- Reverse and forward DNS analysis
- Scan local and remote ports
- Fully integrated with terminal standard input
- UDP and TCP tunneling mode

5.3 Unicornscan

Unicornscan is used for information gathering and data correlation. It compromises advanced asynchronous TCP and UDP scanning features along with very useful network discovery patterns that will help you to find remote hosts. It can also disclose details about the software running by each one of them.

Main features include:

- TCP asynchronous scan
- Asynchronous UDP scan
- Asynchronous TCP banner detection
- OS, application and system service detection
- Ability to use custom data sets
- Support for SQL relational output

5.4 OpenVAS

OpenVAS (Open Vulnerability Assessment System) was developed by Nessus vulnerability scanner. It is Licensed under the GLP license, it's free software that anyone can use to explore local or remote network vulnerabilities which allows you to write and integrate your own security plugins to the OpenVAS platform

Main features:

- Simultaneous host discovery
- Network mapper and port scanner
- Support for OpenVAS Transfer Protocol
- Fully integrated with SQL Databases like SQLite
- Scheduled daily or weekly scans
- Exports results into XML, HTML, Latex file formats
- Ability to stop, pause and resume scans
- Full support for Linux and Windows

5.5 Nikto

It is written in Perl and included in Kali Linux, Nikto works as a complement to OpenVAS. It allows penetration testers and ethical hackers to perform a full web server scan to discover security flaws and vulnerabilities. This security scan collectsthe results by detecting insecure file and app patterns, outdated server software and default file names as well as server and software misconfigurations.

It comprises support for proxies, host-based authentication, SSL encryption and much more.

Main features include:

- Scans multiple ports on a server
- IDS evasion techniques

- Sends the Output results into TXT, XML, HTML, NBE or CSV.
- Apache and cgiwrap username enumeration
- Classifies installed software via headers, favicons and files
- Scans specified CGI directories
- Uses custom configuration files
- Debug and verbose output.

5.6 WPScan

WPScan is recommended for auditing your WordPress installation security. By using WPScan you can check and verify if your WordPress setup is vulnerable to certain types of attacks, or if it's revealing too much information in your core, plugin or theme files.

This tool also helps to find any weak passwords for all registered users, and even run a brute force attack against it to see which ones can be cracked.

WPScan features are as follows:

- Non-intrusive security scans
- WP username enumeration
- WP bruteforce attack & weak password cracking
- WP plugins vulnerability enumeration
- Schedule WordPress security scans

5.7 CMSMap

CMSMap aims to be a central solution for up to four of the most popular CMS in relation of vulnerability detection, unlike WPScan.

It is an open source project written in Python that aids automate the process of vulnerability scanning and detection in WordPress, Joomla, Drupal, and Moodle.

This tool is not only useful for detecting security flaws in these four popular CMS but also for running actual brute force attacks and launching exploits once a vulnerability has been found.

Main features include:

- Provisionsfor multiple scan threats
- Ability to set custom user-agent and header
- Support for SSL encryption.
- Verbose mode for debugging purposes
- Saves output in a text file.

5.8 Fluxion

It is a WiFi analyzer that specializes in MITM WPA attacks.

It allows you to scan wireless networks, searching for security flaws in corporate or personal networks.

Unlike other WiFi cracking tools, Fluxion does not launch any brute force cracking attempts that usually take a lot of time.

Instead, it spawns an MDK3 process which forces all users connected to the target network to de-authenticate. Once this is done, the user is prompted to connect to a fake access point, where they will enter the WiFi password. Then the program reports the password to you, so you can gain access.

5.9 Aircrack-ng

It is a wireless security software suite which consists of a network packet analyzer, a WEP network cracker, and WPA / WPA2-PSK along with another set of wireless auditing tools. Suite Includes following :

- Airmon-Ng: transforms your wireless card into a wireless card in a promiscuous way
- Airmon-Ng: captures packages of desired specification, and is useful in deciphering or decoding the passwords
- Aircrack-Ng: mainly used to decrypt passwords via statistical techniques to decipher WEP and dictionaries for WPA and WPA2 after capturing the WPA handshake
- Aireplay-Ng: used to create or accelerate traffic in an access point
- Airdecap-Ng: decrypts wireless traffic once we the key is deciphered or decoded[4]

6. COMPARISON OF VARIOUS TOOLS

TABLE 1
COMPARISON OF VARIOUS TOOLS

Features	Nmap	Ncat	Unicorn scan	Open VAS	Nikto	WP Scan	CMS Map	Fluxion	Aircrack-ng
Flexible	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Powerful	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Portable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Free	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet Sniffer and Injector	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Tunnel Supported	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password Recovery	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Support for WEP, WPA/WPA2-PSK passwords		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password List Management				Yes		Yes	Yes		
Brute Force	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

7. 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 must be taken as soon as possible to protect the network.

REFERENCES

[1] https://tools.kali.org/information-gathering/nmap
[2] https://www.itgovernance.co.uk/iso27001_pen_testing
[3] https://www.softwaretestinghelp.com/penetration-testing-tools/
[4] https://securitytrails.com/blog/kali-linux-penetration-testing-tools
[5] https://www.synopsys.com/blogs/software-security/top-10-free-hacking-tools-for-penetration-testers/
[6] https://hackertarget.com/10-open-source-security-tools/