IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

RECON Tool: An Automation of Reconnaissance & Scanning

[1]Sanya Bindlish
Department of CSE
The NorthCap University
Gurugram, India

[2]Mehak Khurana
Department of CSE
The NorthCap University
Gurugram, India
[1]Sargam Chhabra
Department of CSE
The NorthCap University
Gurugram, India

[2]Shilpa Mahajan
Department of CSE
The NorthCap University
Gurugram, India

***Abstract*— This Research Paper presents a tool which helps in automation of Reconnaissance and Scanning phase during Penetration Testing. The goal of this tool is to gather as much information about the target as one can in the least amount of time. The bash-script based tool helps in scanning for open ports, web objects, hidden directories and the content-management system used by the target website. Also, a user can add tools to the script according to their recon methodology by simply adding the command used for the tool and appending the result to the output file.**

Keywords*— *Penetration Testing, Reconnaissance, Scanning, Web Application Testing, Automation

I. INTRODUCTION

Penetration Testing, often called pen-testing, is the practice of testing a system, network or web application for vulnerabilities and risks which may impact the security of the system [1]. Pen-testing has five important phases namely the following:

A. Reconnaissance or Information Gathering Acronyms

Reconnaissance is an important first step in pen-testing as it involves gathering as much information about the target organization or system as possible.

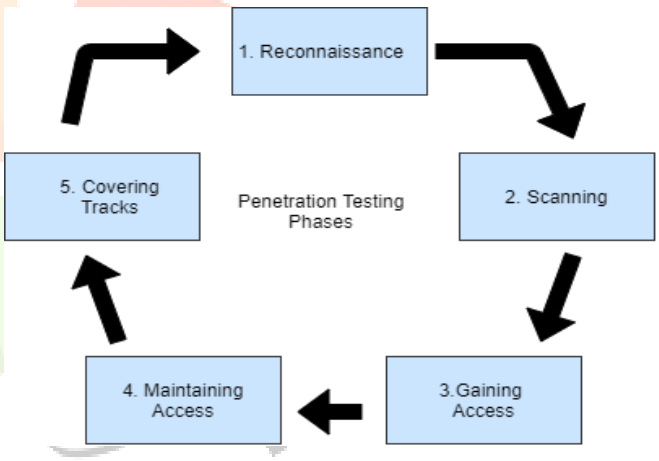

Fig. 1. Phases of Penetration Testing

B. Scanning

The next phase after Reconnaissance is Scanning, also known as Active Reconnaissance. It involves taking the information gathered in the previous phase and using it to examine the system. In this phase, the attacker interacts with the target to identify the vulnerabilities by sending requests and analyzing the response of the target to each request.

C. Maintaining Access

Maintaining Access is an extension of Gaining Access which includes setting up a backdoor or editing registries which can potentially lead to a further level of access and a deeper foothold into the victim's system.

D. Covering Tracks

After accessing the victim's computer, the next step Covering Tracks is very important as it refers to covering up all the clues and footprints that would expose the attacker's identity and his intentions. [2]

This research paper presents a tool namely RECON, made using bash scripting that helps in collecting

information about the target and focuses on the Reconnaissance and Scanning phase of penetration testing.

II. Literature Survey

In [3], authors have presented a structured overview of Penetration Testing. The paper discusses the advantages and methodologies involved in conducting Penetration Testing. It further demonstrates how to conduct penetration testing using two demo sites. The findings in the paper show that penetration testing is a three-phase methodology consisting of preparation, test, and analysis phase. The test phase includes reconnaissance, scanning and vulnerability exploitation. It can be done manually or using automated tools.

In [4], authors have proposed a tool which helps in fingerprinting an organization. The tool presented is developed using Java which locates and saves organization specific data. The paper discusses the two types of reconnaissance and OSINT. It provides the possibility of network-based passive reconnaissance.

In [5], authors discussed the approach to perform manual penetration testing in web applications and the research paper is suitable to act as a guide for testing OWASP Top 10 vulnerabilities. The paper discusses all the five phases of penetration testing. The objective of the paper is to provide knowledge about all the phases of penetration testing.

In [6], the author has discussed an approach that lines up the web application security testing practices with the basic principles of security, namely, confidentiality, integrity and availability; which are collectively known as The CIA Triad. The approach proposed first signifies the requirements of each component of the CIA, mainly focusing on confidentiality. The paper depicts the most vulnerable processes in an application while highlighting the test-intensive areas. It then derives an acceptance criteria and a thought process to develop a test strategy covering both static and dynamic code analysis. It also describes the know-how to apply the DREAD model to categorize vulnerabilities spanning from critical to low intensity vulnerabilities.

In [7], authors have proposed different strategies to deal with large number of hosts and reduce time for a specific task. This paper deals with traffic accountability and time taken to complete a task during active reconnaissance using Nmap tool. The result section of this paper presents graphs and figures to depict variations is timings when the type of scan and number of ports vary. The results show that if scan is performed without any strategy then it affects the bandwidth and time to complete scan.

III. Detailed Structure of RECON Tool

RECON Tool is made by integrating numerous tools namely WafW00f, NMap, Dirb, Whatweb, Nikto, CMSeeK, WPScan and JoomScan in a bash script. This tool also provides the relaxation of adding more tools in the script to increase its functionality just by adding the command applicable to the tool. The tools initially used in the script provide the following functionalities as displayed in the flowchart given in Fig. 2.

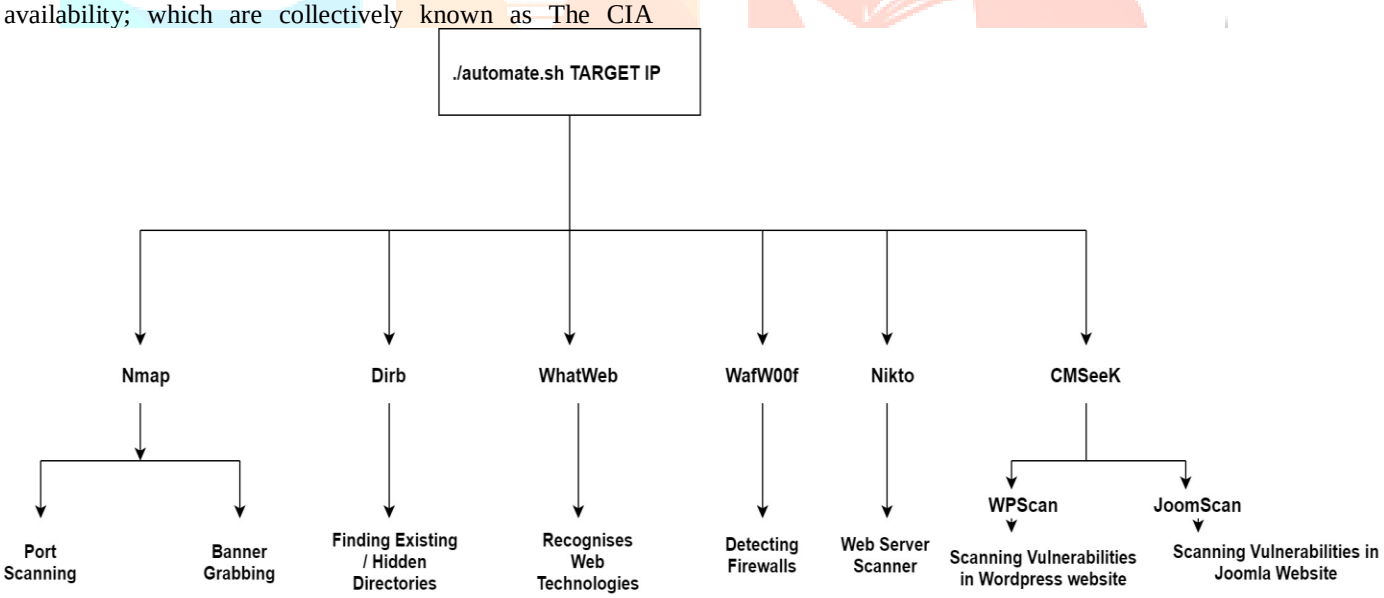

Fig. 2. Flowchart on Tool Functionalities

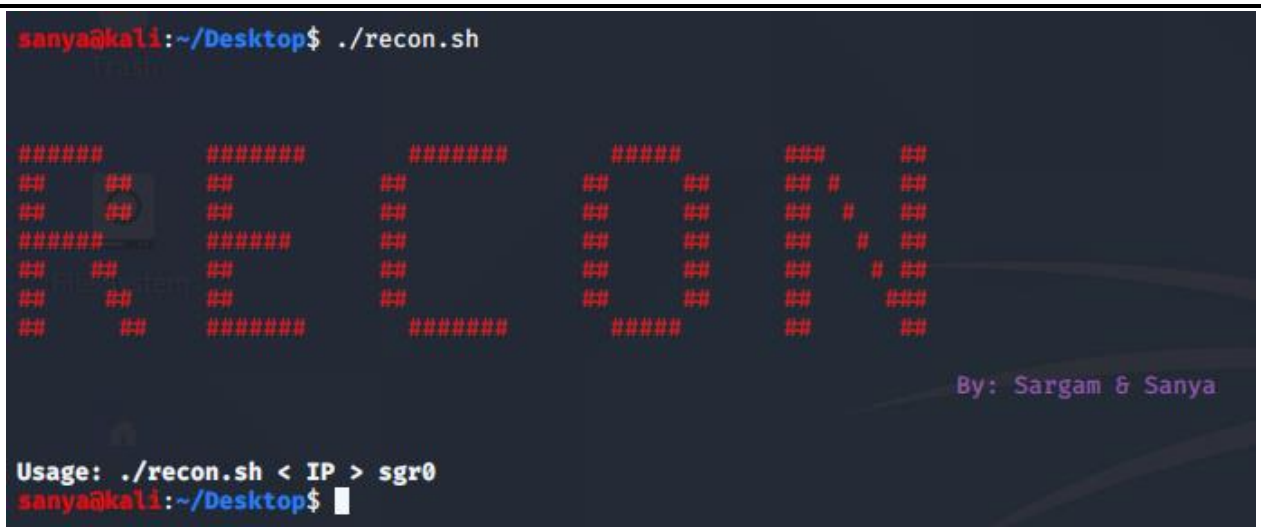

Fig. 3. Usage of the Script

The command given in Fig. 3 that is used to initialize the script should specifically include the IP address of the target and not the domain name of the web application. The IP address can be easily found using DNSLookup or some other online tool by just entering the URL of the target.

Usage: ./automate.sh < TARGET IP >

The Basic Idea behind this script was to automate the process and reduce the efforts. It is easy to run one command and store the results together rather than running all the tools separately and analysing the results.

A. *NMap*

NMap is an open source and free network scanner used to locate hosts and services on a network by sending packets and analyzing their replies.

Usage: nmap < Target URL/ IP>

- Stealth Scan: nmap -sS < Target URL/ IP>
- Identifying Hostname: nmap -sL < Target URL/ IP>
- Verbose Scan: nmap -v < Target URL/ IP>
- Aggressive Scan: nmap -A < Target URL/ IP>
- Timing Scan: nmap -T5 < Target URL/ IP>, Timing can range from T1 to T5. [8]

Features of NMap:

- Identifying and listing the hosts on the network that responds to requests.
- Listing the open ports on a target host.
- Determining application name and version.
- Determining the OS and hardware traits of network devices.

B. *Nikto*

Nikto is a free command-line tool written in perl and is used to scan web servers for vulnerabilities. It checks for server configuration and installed web servers along with other items. Requests sent by Nikto to web servers are logged in log files and Intrusion Detection System. Nikto is not a stealthy tool, so any site with Intrusion Detection System or other security measures will detect that it's being scanned.

Usage: nikto -h < Target URL/ IP>

Features of Nikto:

- SSL and HTTP proxy support
- Reports can be generated in multiple formats such as HTML, CSV, XML, or plain text.
- Maximum execution time
- Identifies headers, favicons, and files. [9]

C. *WafW00f*

Wafw00f is a python-based tool used to detect firewalls used by the website. It is pre-installed in Kali and gives accurate results. To display the list of firewalls which can be detected using wafw00f use command: wafw00f -l

Usage: wafw00f < Target URL>

Features of WafW00f:

- It works by sending HTTP requests to the site and analyzing the response [10].
- If this does not work, it sends various malicious HTTP requests to know which web-application firewall is being used.

D. *Whatweb*

Whatweb is like a wappalyzer extension. It detects web technologies used such as CMS, statistics/analytics packages, web server and framework used. It supports aggression level; default level is stealthy which is used to scan public websites. Stealthy level of aggression is the fastest and sends only one HTTP request.

Usage: whatweb < Target URL>

Features of Whatweb:

- Proxy Support including TOR
- Over 1700 plugins
- Fuzzing
- Multiple formats to display results. [11]

E. *Dirb*

Dirb is used to find existing or hidden web objects. It works by launching a dictionary-based attack against the web server and analyzing the response. It is a command-line tool but a GUI version is also available known as Dirbuster.

Dirb and Dirbuster both are pre-installed in Kali Linux. It has pre-configured wordlists, but we can use our own custom wordlists. Wordlist Big.txt is the best wordlist available but common.txt is the default wordlist used by the tool [12].

Usage: dirb < Target URL/ IP>

F. CMSeeK

CMSeeK is built using python and is currently compatible with only unix-based systems. It can detect over 170 CMS. Also, it has advanced wordpress and joomla scan functionality. It can detect version used and enumerate users, themes and plugins. It has a modular bruteforce system, we can either use the default bruteforce system or create and integrate our own bruteforce system.

Usage: python3 cmseek.py -u < Target URL> [13]

Features of CMSeeK:

- Database of over 170 CMS
- Advanced scans
- Modern bruteforce system

G. WPScan

WPScan is Wordpress Security Scanner and is pre-installed in Kali. It is built using Ruby. It uses wpvulndb.com database to scan for vulnerabilities in a website built using wordpress.

Usage: wpscan --url < Target URL>

Features of WPScan:

- To enumerate plugins: wpscan --url <Target URL> --enumerate p
- To enumerate themes: wpscan --url <Target URL> --enumerate t
- To enumerate username: wpscan --url <Target URL> --enumerate u
- To bruteforce password: wpscan --url <Target URL> -U username -P < path of wordlist > [14]

H. JoomScan

JoomScan is a tool developed by OWASP in the Perl programming language to detect vulnerabilities in websites using Joomla CMS and analyze them. It is not pre-installed in the latest version of Kali linux [15].

Usage: joomscan -u <Target URL>

Features of JoomScan:

- To enumerate Version
- To enumerate Vulnerability
- Firewall Detector
- Finding Log files and backup files

Note: *As CMSeeK and Joomscan are not pre-installed in Kali linux version 2020.2 so a user cannot simply integrate the above-mentioned usage commands in the script. To run recon script at any location, the user has to mention the entire path of the tool.*

Integrated commands:

- *For CMSeeK*
  python3 < path of CMSeeK folder >/cmseek.py -u <Target> [13]
- *For JoomScan*
  perl <path of joomscan folder>/joomscan.pl -u <Target> [15]

IV. PROPOSED RECON TOOL

a) Enter "./recon.sh <Target IP>" on the terminal, if no Target IP is specified it prints the usage example.

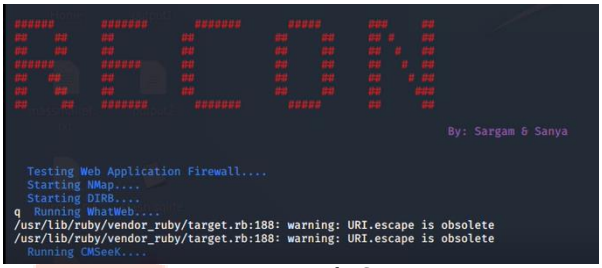

Fig. 4. Running the Script

b) Recon scripts first checks for Web Application Firewall which is done using the tool "WafW00f".

c) Then it scans for open ports using "NMap".

Note: *One can specify the type of scans: SYN scan, TCP connect scan, UDP scan. Apart from port scanning, one can also use nmap for OS fingerprinting by using the flag -O. For more details about the various flags used in nmap, use the command "man nmap".*

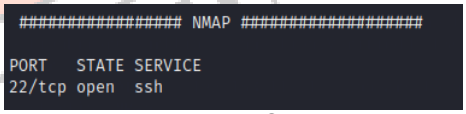

Fig. 5. NMap Output

d) After Port scanning, it scans for existing/hidden directories using "Dirb".

e) Next it moves on to web technology scanning using "Whatweb".

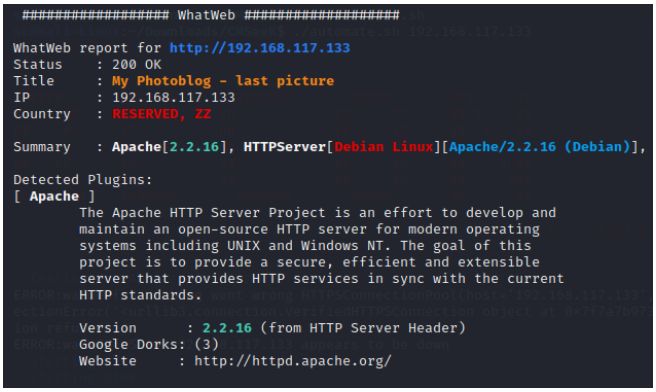

Fig. 6. Whatweb Output

f) Then it scans for CMS if any, using CMSeeK.

Fig. 7. CMSeeK Output Part 1

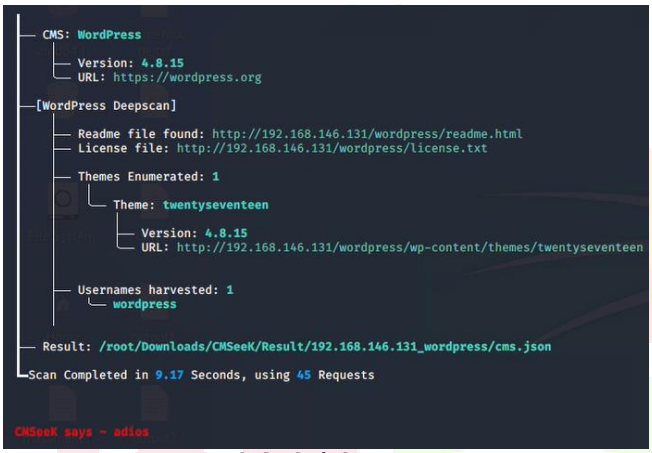

Fig. 8. CMSeek Output Part 2

g) At last, it uses Nikto for vulnerability scanning.

h) All the information is appended in output.txt which is displayed on the terminal using "cat command". Output file is created if not present and each time the script runs, it clears the previous output and saves the new output in a txt file.

V. Conclusion and Future Scope

A. *Conclusion*

Recon tool has all the commands for the above-mentioned tools, and it stores all the information in an output file. The results are appended in a txt file and displayed on the terminal using cat command. The output file displays the result of each command in a systematic manner starting with the name of the tool whose output is displayed next.

All the tools used in this script are important for gathering information about the target and provide an easy approach to perform ethical hacking. Recon tool is very simple to use which can even be utilized by amateurs and script-kiddies.

B. *Future Scope*

To use conditions and grep the name of CMS identified using CMSeeK and then use WpScan or JoomScan accordingly.

Recon Tool can be expanded to all phases of penetration testing by adding the commands of tools to the script. It can also be used to check CMS vulnerabilities of various Content Management Systems.

References

[1] Khurana M., Yadav R., Kumari M. "Buffer Overflow and SQL Injection: To Remotely Attack and Access Information". In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing, vol 729. Springer, Singapore. https://doi.org/10.1007/978-981-10-8536-9_30 (2018)

[2] Manish Shivanandhan | The Ethical Hacking Lifecycle - Five stages Of A Penetration Test.https://www.freecodecamp.org/news/ethical-hacking-lifecycle-five-stages-of-a-penetration-test/ (2020, September 9)

[3] A.G. Bacudio, X. Yuan, B.T.B.Chu and M. Jones. "An Overview of Penetration Testing". Int. Journal of Network Security & Its Applications Vol.3 (no. 6) (2011, November)

[4] A. Roy, L. Mejia, P. Helling and A. Olmsted. Automation of Cyber Reconnaissance: A java based open-source tool for information gathering (2017, December)

[5] Nagendran K, Adithyan A, Chethana R, Camillus P, Bala Sri Varshini K B. "Web Application Penetration Testing". International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-10 (2019, August 10)

[6] Bhushan B. Gupta. "Requirements Based Web Application Security Testing – A Preemptive Approach!". (2017)

[7] Mujahid Shah, Sheeraz Ahmed, Khalid Saeed, Muhammad Junaid, Hamayun Khan, Ata-ur-rehman. "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool". 2019 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019. (2019, March)

[8] Fyodor. (n.d.). Nmap | Penetration Testing Tools. Kali Tools. https://tools.kali.org/information-gathering/nmap

[9] Nikto2 | CIRT.net. (n.d.). CIRT. https://cirt.net/Nikto2

[10] Enable Security. WafW00f. GitHub. (2020, January 29)

[11] Andrew Horton & Brendan Colese. WhatWeb | Penetration Testing Tools. Kali Tools. https://tools.kali.org/web-applications/whatweb (2018, March 26).

[12] The Dark Raver. (n.d.). DIRB | Penetration Testing Tools. Kali Tools. https://tools.kali.org/web-applications/dirb

[13] Tuhin Shubhra. CMSeeK. GitHub. https://github.com/Tuhinshubhra/CMSeeK .(2018, August 7).

[14] The WPScan Team. WPScan | Penetration Testing Tools. Kali Tools. https://tools.kali.org/web-applications/wpscan.(n.d.).

[15] Mohammad Reza Espargham, Ali Razmjoo. joomscan | Penetration Testing Tools. Kali Tools. https://tools.kali.org/web-applications/joomscan.(n.d.).