EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration

Ammrish Singh Beker Singh
School of Technology, Forensic and Cyber Security Research Centre
Asia Pacific University of Technology and Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
TP046190@mail.apu.edu.my

Yusnita Yusof
School of Technology, Forensic and Cyber Security Research Centre
Asia Pacific University of Technology and Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
yusnita@apu.edu.my

Yogeswaran Nathan
School of Technology, Forensic and Cyber Security Research Centre
Asia Pacific University of Technology and Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
yogeswaran.nathan@apu.edu.my

2021 14th International Conference on Developments in eSystems Engineering (DeSE) | 978-1-6654-0888-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/DESE54285.2021.9719338

***Abstract*— Penetration testing is a security exercise that is carried out by penetration testers to identify and exploit vulnerabilities in a system. Many penetration testing tools are available in Command Line Interface (CLI) and this requires familiarization of commands. Beginner penetration testers might struggle to understand and choose the most suitable tools. This paper presents a Graphical User Interface (GUI)-Based Penetration Testing Tool for Scanning and Enumeration named as EAGLE. It is developed to assist beginner penetration testers. EAGLE integrates features from several scanning and enumeration tools such as Nmap, Gobuster, Hydra, Nikto, Enum4Linux and Whatweb. The tool's functions include port scanning, web server enumeration, website screenshot, service brute force and service enumeration. Users or beginner penetration testers are only required to provide an IP Address of the target system as the input. This eliminates the familiarization of extensive commands used in multiple tools. The tool displays the results in a convenient manner with a filtering feature so that it is easier to read and understand the scan results. The novelty of this work is done by comparing the output / results obtained using the CLI-based tools separately with the integrated results produced using EAGLE.**

Keywords*— *CLI, enumeration, GUI, network, penetration testing, RAD, scanning

I. INTRODUCTION

Computer networks are more vulnerable than ever to cyber threats of increasing frequency, severity, and sophistication [1]. Companies suffer catastrophic consequences and losses if the computer networks and systems were hacked by cyber criminals. A penetration test is a security-oriented systematic probing of system from internal and external to discover vulnerabilities that an attacker could exploit [2].

Penetration testing or pen testing is a well-established proactive method to evaluate the security of digital assets which varies from single computer to websites and networks, by actively searching for and exploiting the active vulnerabilities [1]. One critical factor in the success of penetration testing is its fundamental methodology.

Penetration testing method which are reconnaissance, scanning, exploitation, post-exploitation, and reporting. Reconnaissance, or information gathering involves in gathering as much information as possible about the target to help plan the actual pentesting. The scanning phase is where the actual pentesting process starts by scanning and enumerating the target system or network to gather technical information.

When there is more information about the system, executing vulnerability scanning and exploitation will be easier. Vulnerability scanning is to examine the system for known vulnerability which is based on the services detected and its version, where the services are linked to known vulnerabilities.

Exploitation phase is the method of gaining control over the system and the post-exploitation phase is maintaining access or information gathered on the exploited system. The final phase reporting is to conclude an analysis of the system, network, vulnerabilities and recommend control measures or fixes of the vulnerability [3]. The standard penetration testing methodology is as shown in Fig. 1 below.

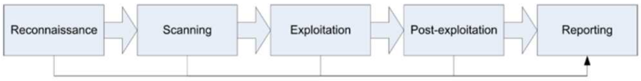


Fig. 1. Penetration Testing Methodology [3].

The scanning phase plays an important role in the penetration process because it provides crucial information about the target system to the penetration tester. The scanning phase usually involves with scanning and enumerating the target system. Scanning involves in gaining information about the target system such as device names, live hosts, ports, services, Operating System, and architecture [4].

Enumeration is the process of extracting usernames, machine names, network resources and services from the target system. The information gathered from scanning and enumerating will assist the penetration tester to identify the vulnerabilities in the target system and tries to exploit it to proceed to the following phase. Unfortunately, scanning and enumeration are difficult for beginner penetration testers because the tools mostly use CLI and this requires familiarization of the commands to utilize the tools.

Thus, the author proposed EAGLE, a GUI-based Penetration Testing Tool for Scanning and Enumeration. It provides a simple and easy to use GUI for the beginner penetration testers to use when conducting scanning and enumeration. EAGLE integrates multiple scanning and enumeration tools such as Nmap, Gobuster, Hydra, Nikto, Enum4Linux and Whatweb. EAGLE is the integrated GUI-based tool which does not require familiarization of extensive commands in multiple tools, separately.

II. TECHNICALITIES AND METHODS

To design and develop EAGLE, the technicalities and methods are explained in the subsections below.

A. *Technicalities*

For the development of the project, there are several components required. The author used Python as the programming language for the system development because has an extensive support of libraries. The IDE chosen for this tool is PyCharm. The author utilized PyQt5 – Qt Designer for the GUI development. PyQt5 and NMAP (Network Mapper) modules are utilized. The author has chosen and used SQLAlchemy for DBMS because it uses Python code to convert to SQL queries. The Operating System used is Kali Linux.

B. *Software Development Methodology*

The software development methodology for this project will be Rapid Application Development (RAD). The reason is because the project duration is three months and the average life cycle for RAD methodology is about two to three months which makes it suitable for this project. Moreover, with RAD, the system can be delivered earlier to gather the feedbacks about it from the end users and it is possible to perform any changes in the system throughout the phases in RAD. Also, RAD provides low risk for the project because the risk can be discovered in the early stage of prototyping or gathering feedbacks client and changes can be performed quickly.

The phases of RAD are requirements planning, user design, rapid construction, and transition [5-7]. Requirement planning phase is important to finalize the project requirements such as scope, project goals and objectives so that it can be agreed on. This would allow the goals and expectations for the project to be determined as well as potential problems to be addressed during the system development. User design phase is to establish and improve on the working prototype until the final system or product is ready. This phases usually involves in repeating often as necessary as the project progresses. The usage of quickly built prototypes urges for user involvement, testing and feedback on the system thus errors or bugs are far more likely to be discovered earlier and leads to bugs and errors to be reduced.

Rapid construction phase is to deliver a working system and clients still can provide suggestion, changes, or new ideas for the system. This phase is where coding, system testing, and unit integration happens where the prototype and the beta version system are converted into a working model. Feedback about the functionality of the system is gathered and each feature of the system is enhanced. The final phase transition, is where the finished system can go to launch which includes the data conversion, testing and changeover to the new system and implies user training.

C. *Research Methods*

The research method used to gather data related to the project is questionnaire. A questionnaire is a research method that is made up of open-ended questions or closed-ended question. The aim of the questionnaire is to gather appropriate data from the respondents which can be used for the research purposes [8]. The advantage of using questionnaires is there is no time constraint because the respondents could fill in the questionnaires at any time and questionnaires are easy to conduct [9]. The author used variety of questions to gather more wide-ranging data to gain a better insight on the deliverables of the proposed system. The author gathered the primary research on the respondents' expected functions and performed a comparison to the scope and deliverables of the proposed system. For features suggested by the respondents that were not in the deliverables, the author had to decide whether to add into the deliverables or consider as future enhancement.

III. Results and Discussion

A. *Primary Research Data Gathering*

The data was gathered from 30 respondents. The author received positive responses for the proposed system.

As seen in Fig. 2 below, majority of the respondents have agreed that current issues with scanning and enumeration tools are the command memorization and difficult to understand.

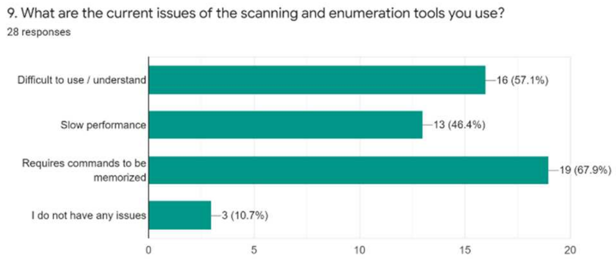


Fig. 2. Result for question on current issues of scanning and enumeration tools used.

Results from the questionnaire helped the author to determine the features that were included in this tool. The respondents are comfortable of the tool being developed with Graphical User Interface because it would be easy to use. The responses could be seen from the Fig. 3 below.

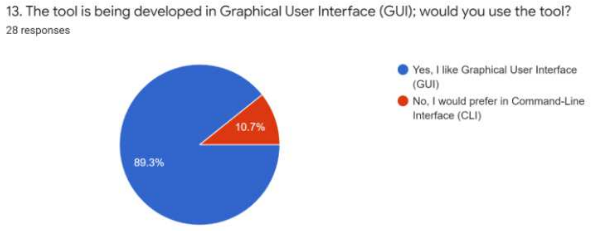


Fig. 3. Result for question on developing the tool as GUI-based.

Apart from that, all respondents would want to integrate existing scanning and enumeration tools and perform as one system as shown from the result in Fig. 4 below.

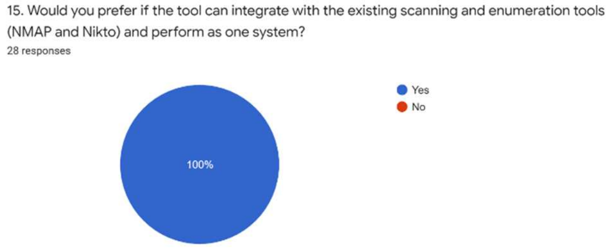


Fig. 4. Result for question on preference to integrate existing scanning and enumeration tools as one system.

This would save time from switching back and forth between each tool while keeping track of the data. The author has received several suggestions from the respondents to implement into the system. The author has implemented some of the suggestions from the respondents while the others were elaborated as future enhancement due to time constraint. The questionnaire results have helped to identify the problems and respondent's opinion towards the current scanning and enumeration tools. The proposed tool would be able to overcome or reduce the problems faced by the respondents.

Based on the data acquired from the questionnaire, the author has developed a Graphical User Interface (GUI) tool that integrates several scanning and enumeration tools. Fig. 5 shows the main interface that the user interacts after executing the program file. The interface is designed to be easy to use and simple as the user needs to provide only the IP Address of the host. The tool then performs the scanning and enumeration without having user to provide any further commands.

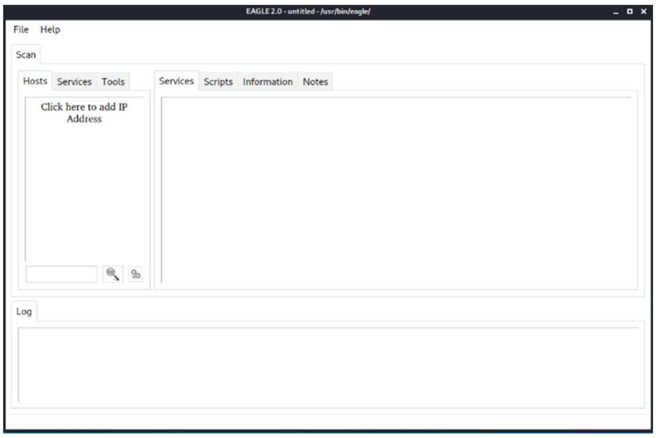
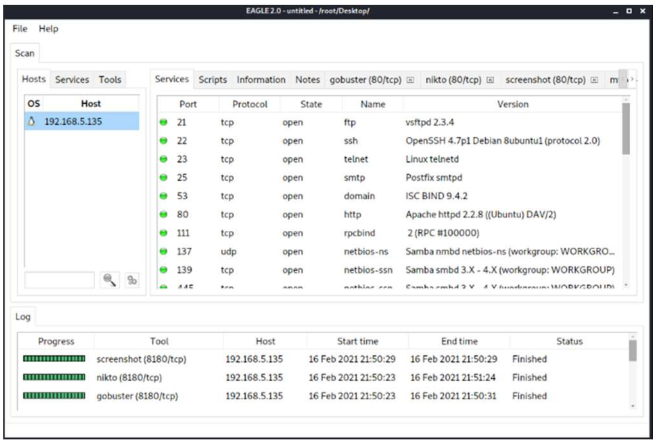

EAGLE 2.0 - untitled - /usr/bin/eagle/
File
Help
Scan
Hosts
Services
Tools
Services
Scripts
Information
Notes
Click here to add IP Address
Log

Fig. 5. Main interface for EAGLE.

Fig. 6 shows the result sample of the scanning and enumeration. The result interface is for the user to analyze and gather information about the scan. The system displays the results in a convenient manner to ensure the user could easily understand and access.



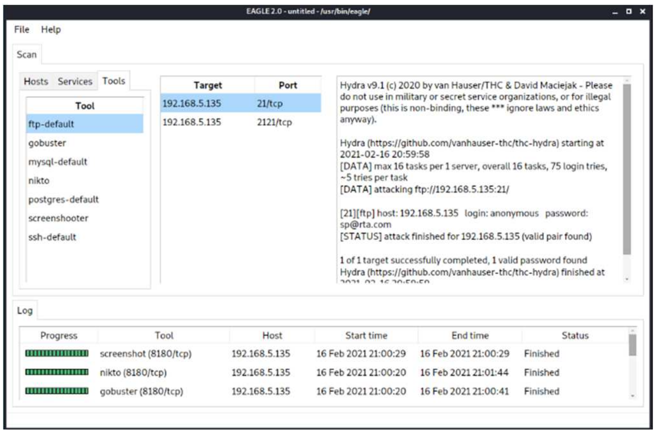
OS	Host
	192.168.5.135

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKGRO...
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Progress	Tool	Host	Start time	End time	Status
	screenshot (8180/tcp)	192.168.5.135	16 Feb 2021 21:50:29	16 Feb 2021 21:50:29	Finished
	nikto (8180/tcp)	192.168.5.135	16 Feb 2021 21:50:23	16 Feb 2021 21:51:24	Finished
	gobuster (8180/tcp)	192.168.5.135	16 Feb 2021 21:50:23	16 Feb 2021 21:50:31	Finished

Fig. 6. Scan result sample using EAGLE.

The tools tab's interface shows the tools used in the scanning and enumeration together with the result of the tools. The system is integrated with several open-source scanning and enumeration tools with different functionality. Each tool used by the system and the results from the tool are displayed in the tools tab of the system. This is as shown in Fig. 7 below.



Tool
ftp-default
gobuster
mysql-default
nikto
postgres-default
screenshooter
ssh-default

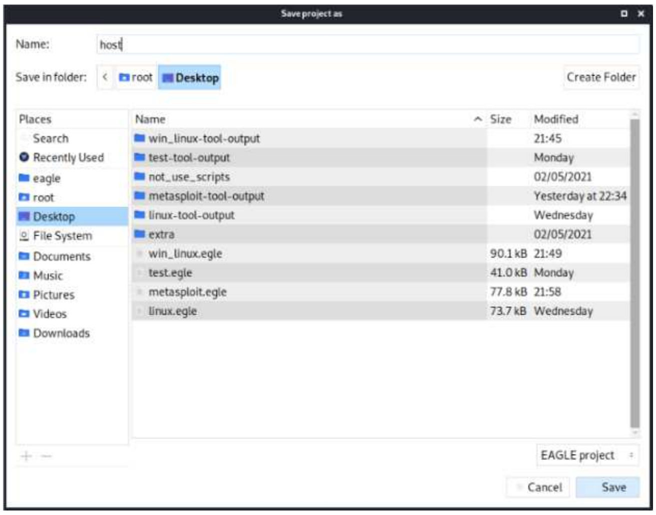
Target	Port
192.168.5.135	21/tcp
192.168.5.135	2121/tcp

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please
do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
2021-02-16 20:59:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 75 login tries,
~5 tries per task
[DATA] attacking ftp://192.168.5.135:21/

[21][ftp] host: 192.168.5.135   login: anonymous   password:
sp@rta.com
[STATUS] attack finished for 192.168.5.135 (valid pair found)

1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
```

Progress	Tool	Host	Start time	End time	Status
	screenshot (8180/tcp)	192.168.5.135	16 Feb 2021 21:00:29	16 Feb 2021 21:00:29	Finished
	nikto (8180/tcp)	192.168.5.135	16 Feb 2021 21:00:20	16 Feb 2021 21:01:44	Finished
	gobuster (8180/tcp)	192.168.5.135	16 Feb 2021 21:00:20	16 Feb 2021 21:00:41	Finished

Fig. 7. Tools tab in EAGLE.

EAGLE has the capability to save the scan results. The user needs to provide the location and filename for the scan results. This provides convenience to the user to access and view back the results anytime. This is as shown in Fig. 8 below.



Name: host

Save in folder: root Desktop

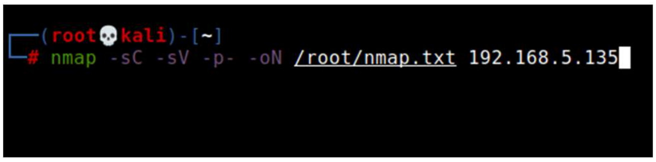
Name	Size	Modified
win_linux-tool-output		21:45
test-tool-output		Monday
not_use_scripts		02/05/2021
metasploit-tool-output		Yesterday at 22:34
linux-tool-output		Wednesday
extra		02/05/2021
win_linux.egle	90.1 kB	21:49
test.egle	41.0 kB	Monday
metasploit.egle	77.8 kB	21:58
linux.egle	73.7 kB	Wednesday

Fig. 8. Save scan results in EAGLE.

B. Critical Evaluation

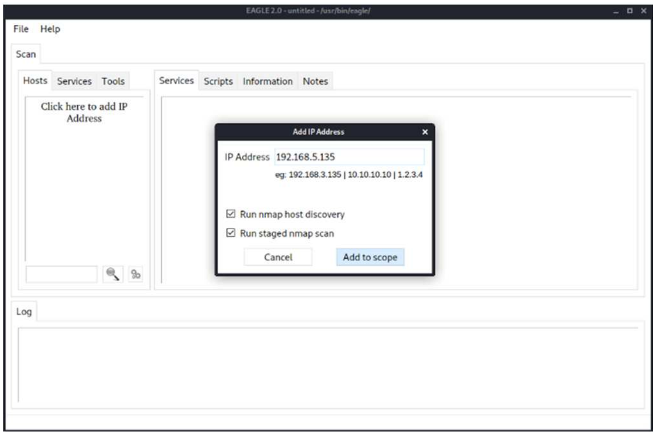
The EAGLE system was developed to integrate scanning and enumeration tools that are commonly used in penetration testing. EAGLE does not require any command memorization and it is easy to use. The following section discusses comparison of how normally these selected tools – Nmap, Gobuster and Hydra are used compared with the EAGLE system.

Firstly, Fig. 9 and Fig. 10 show the comparison when the user needs to perform a NMAP scan. In Fig. 9, it requires user to input command to perform a scan. Each command represents an option or a module that would produce the output based on those commands. The second figure, Fig. 10 performs a NMAP scan in the EAGLE system and the user is only required to provide an IP Address and no further commands are required. NMAP is integrated with the EAGLE system and the system runs the script that would perform the scan.



```
┌──(root💀kali)-[~]
└─# nmap -sC -sV -p- -oN /root/nmap.txt 192.168.5.135
```

Fig. 9.   NMAP scan without EAGLE system.



IP Address 192.168.5.135

eg: 192.168.3.135 | 10.10.10.10 | 1.2.3.4

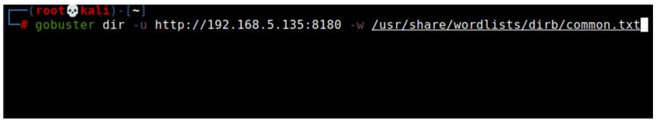
☑ Run nmap host discovery

☑ Run staged nmap scan

Cancel   Add to scope

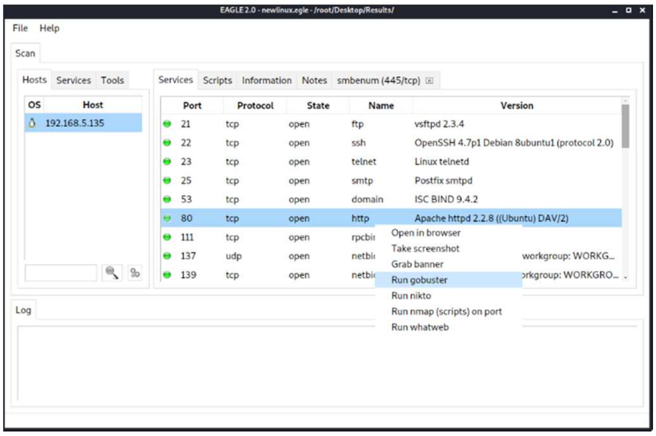
Fig. 10. NMAP scan with EAGLE system.

Secondly, Fig. 11 presents the utilization of Gobuster by providing commands on the terminal and Fig. 12 presents the utilization of Gobuster with a click of a button. In Fig. 12, the user just needs to click to run Gobuster using EAGLE system compared to the earlier Fig. 11 which requires the user to provide commands. The EAGLE system save users' time and does not require the user to memorize commands when performing Gobuster.



```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://192.168.5.135:8180 -w /usr/share/wordlists/dirb/common.txt
```

Fig. 11. Gobuster without EAGLE system.

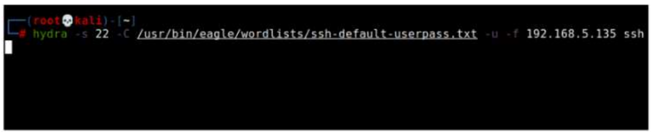


OS	Host
	192.168.5.135

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbi	
137	udp	open	netbi	workgroup: WORKG...
139	tcp	open	netbi	orkgroup: WORKGRO...

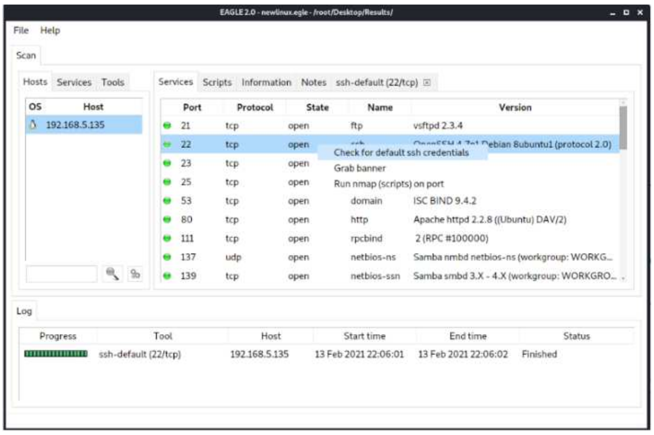
Fig. 12. Gobuster with EAGLE system.

Thirdly, comparison using Hydra on its own as a CLI-based tool compared to as an integrated tool in EAGLE. This is shown in the following Fig. 13 and Fig. 14. Fig. 13 shows the command use to crack username and password of a service using Hydra. Commands in Hydra could be difficult and confusing for beginners because of different commands used for different services such as Login Form in a Website.



```
┌──(root💀kali)-[~]
└─# hydra -s 22 -C /usr/bin/eagle/wordlists/ssh-default-userpass.txt -u -f 192.168.5.135 ssh
```

Fig. 13. Hydra without EAGLE system.



EAGLE 2.0 - newlinux.egle - /root/Desktop/Results/
File
Help
Scan
Hosts
Services
Tools
Services
Scripts
Information
Notes
ssh-default (22/tcp)
Log
Check for default ssh credentials
Grab banner
Run nmap (scripts) on port

OS	Host
	192.168.5.135

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open		ebian 8ubuntu1 (protocol 2.0)
23	tcp	open		
25	tcp	open		
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKG...
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGRO...

Progress	Tool	Host	Start time	End time	Status
	ssh-default (22/tcp)	192.168.5.135	13 Feb 2021 22:06:01	13 Feb 2021 22:06:02	Finished

Fig. 14. Hydra with EAGLE system.

In short, the tools integrated in EAGLE originally use Command Line Interface (CLI) that requires user to provide input to use the commands. Problem arises when this requires user to get familiar with the usage of commands. Therefore, EAGLE has integrated these scanning and enumeration tools as a GUI-based system. EAGLE system is an easy to use tool that ensures the user could perform scanning and enumeration without requiring the user to input and memorize further commands.

IV. Conclusion

After research and requirements gathering have been accomplished for the system, the main features of EAGLE system have been identified and designed. EAGLE was developed by integrating several tools and software which were narrowed down to ensure the appropriateness and effectiveness of the system. EAGLE has been tested to identify errors or bugs in the system and to receive users' feedback about its functionalities and room for improvement. Based on user acceptance testing, the testers have provided positive feedback and EAGLE is read to be used especially by the beginner level penetration testers.

Acknowledgment

This paper is part of the author's final year project. Therefore, the author would like to show appreciation towards all lecturers involved especially the supervisor, advisor, and project manager. The author would also like to express gratitude to his family members and friends who have provided support in completing the final year project.

References

[1] Ghanem, M. C., & Chen, T. M. (2019). Reinforcement Learning for Efficient Network. Information, 11(6), 2-23.

[2] Aar, P. (2017). Analysis of Penetration Testing Tools. International Journals of Advanced Research in, 7(9), 2-7.

[3] Keski-Korsu, P. (2016). Automated port scanning and security testing on a single network host. 69.

[4] Arora, S. (2020). Explore The 5 Phases of Ethical Hacking. Retrieved December 24, 2020, from https://www.simplilearn.com/phases-of-ethical-hacking-article

[5] Ankita, S. (2019). What Is Rapid Application Development (RAD)? Retrieved August 23, 2020, from https://blog.capterra.com/what-is-rapid-application-development/

[6] Brodle, O. (2020). What is Rapid Application Development (RAD)? Retrieved August 23, 2020, from https://codebots.com/app-development/what-is-rapid-application-development-rad

[7] Lucidchart. (2019). 4 Phases of Rapid Application Development Methodology. Retrieved August 23, 2020, from https://www.lucidchart.com/blog/rapid-application-development-methodology

[8] Ndukwu, D. (2020). Questionnaire: Types, Definition, Examples & How to Design Your Own. Retrieved December 26, 2020, from https://www.kyleads.com/blog/questionnaire/

[9] Rahman, M. (2020). Advantages and disadvantages of questionnaires. Retrieved December 26, 2020, from https://howandwhat.net/advantages-disadvantages-questionnaires/