FOOTHOLDER : Collection of tools and scripts used to learn and experiment the exploitation of vulnerable machines

Vyshakh Nair
Department of Networking and Communications
SRM Institute of Science and Technology,
Kattankulathur, Chennai, India
vyshakhg04@gmail.com

KP Yashwin
Department of Networking and Communications
SRM Institute of Science and Technology
Kattankulathur, Chennai, India
kpyashwin@gmail.com

Annapurani Panaiyappan K
Department of Networking and Communications
SRM Institute of Science and Technology
Kattankulathur,Chennai, India
annapook@srmist.edu.in

2023 International Conference on Networking and Communications (ICNWC) | 979-8-3503-3600-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICNWC57852.2023.10127486

***Abstract* —** People's interests in learning more about the cyber world have grown after the COVID-19. Worldwide cyber activity has risen, and it has attracted new cyber security enthusiasts to the field of ethical hacking. These enthusiasts, however, struggle to become accustomed to the Kali Linux's vulnerability and assessment tools. Additionally, individuals need to invoke each tool independently without knowing the supporting arguments.
In this paper, we suggest the creation of a single location where users may access all other significant tools and receive instruction on how to operate them.This will fill the knowledge and tool-familiarization gap for brand-new cyber aficionados. Since using a terminal [CLI] is more preferred than a graphical user interface [GUI] for using the tools, our learning would be concentrated on this interface. Network enumeration tools like nmap, NetDiscover, directory enumeration tools such as Gobuster and Dirbuster, service enumeration tools like telnet and ftp, Brute Forcing tools such as Hydra and more such tools are incorporated into this Footholder. These tools serve as the foundation for reconnaissance and planning, thus a novice should get familiar with them.

***Keywords*—** Vulnerability assessment and penetration testing, CLI- command line interface, enumeration, GUI - Graphical user interface, Nmap - Network Mapper, SSH - secure shell, FTP, Hydra- parallelized login cracker tool.

I. INTRODUCTION

Computer technology has a significant influence on the international scene as it continues to be absorbed into society. Everyone in today's contemporary world, from individual consumers to businesses to governments, is significantly impacted by computers. As long as the world maintains to store both its private and public information on computers, secure computer systems will be more important than ever. As they say, the best type of offense is a good defense [1]. Although feature-rich, modern and advanced apps often increase systems' vulnerability. A program's vulnerability is a flaw or gap that allows an attacker to exploit the user by obtaining administrative access. The attacker gains unauthorized access to sensitive information and uses it to their gain. Although a system cannot be fully free of vulnerabilities, we can improve system security and reduce the amount of lost data as much as we can [2].
A thorough, security-focused analysis of the architecture inside and out to search for any openings that an adversary may leverage would be a penetration test. By actively seeking out and making use of the current vulnerabilities, penetration testing, also known as pen testing, is a renowned proactive approach for assessing the authenticity of digital content, which can range from a windows machine to websites and networks. Observation, searching, exploitation, post-exploitation, and documentation are the phases of a penetration test. To plan an efficient pentesting, reconnaissance, or intelligence gathering effort, you must learn all that you can about the target. The scanning stage is where the actual pentesting process starts, which involves enumerating and scanning the intended network or computer system to obtain technical data [3].

The easier it is for an attacker to exploit the system's flaw, the more information about the targeted computer or network is revealed. Exploitation is the method used to take control of the system, while post-exploitation is the process of keeping access to or maintaining knowledge of the exploited system. The last stage of reporting's objective is to complete an evaluation of the machine, connectivity, and weaknesses and offer control suggestions or vulnerability fixes [3].
The standard workflow of pentesting is shown in Fig 1. Given below:

Fig 1. Phases of Pentesting

Any enthusiast for pentesting will follow these steps while checking for vulnerabilities in a computer system or network.A beginner's duty is to become acquainted with the tools offered by Kali Linux, nevertheless. They can have a hard time choosing the suitable equipment for the job.
In this paper, we put up the idea of merging all the tools needed to conduct a penetration test into a single component. This will also put a strong emphasis on introducing new users to the tools and aiding in their familiarization. Footholder integrates various enumeration tools such as nmap, and netdiscover, directory enumeration tools such as Gobuster and Dirbuster, service enumeration tools like telnet and ftp, Brute Forcing tools such as Hydra in it.

II. LITERATURE SURVEY

Approaches suggested in [3] by the authors are similar, who switch from CLI (command line interface) to GUI (Graphical user interface). They conducted a poll to find out how students and newcomers in this profession felt about using the GUI vs the CLI. According to the poll, because it is convenient and simple to use, novices prefer the GUI model. This initiative was given the moniker EAGLE. It was created to help neophytes in penetration testing. Nmap, Gobuster, Hydra, Nikto, Enum4Linux, and Whatweb, among other scanning and enumeration tools, are all integrated into EAGLE.The authors of [4] covered the five steps of vulnerability assessment and the methods that were employed in doing so. Additionally, they talked about the technique, tactics, and advantages of penetration testing. Finally, they looked at the distinctions between penetration testing and vulnerability assessments.The

report [5] presented their findings and the analysis of the assaults on the telnet and SSH protocols using honeypots. They offered a quick introduction to honeypots and talked about how, when improperly setup, these services operating on their destination port be misused.This study [6] examines a variety of penetration testing-related topics, such as tools, attack methodology, and response tactics. Most frequently, authors employed Kali Linux's toolkit. This essay aimed to clarify penetration testing's application and give some conceptual frameworks.The authors of [7] use the nmap tool during in the exploration process to illustrate internet traffic transparency and the time needed to accomplish a specific task, and they offer suggestions for managing large figures of hosts and reducing both network activity and the time needed to accomplish a specific task. They recommended a scan technique that strikes a compromise between the need to investigate more ports and services as well as any network traffic constraints, such as sluggish uplinks. They advised utilizing a more requires immediate medical attention, doing port scans without looking, and carefully considering the effects of scans on network traffic, job completion time, potential effects on the victim PC, and network architecture.There are many resources accessible to carry out such tasks, even though vulnerability research looks for information about faults including well programs and applications and penetration testing tries to attack holes in environment or structure. This study [8] mostly focused on penetration testing and vulnerability assessment methods.

III. ARCHITECTURE OF FOOTHOLDER

The attacker or user of Kali Linux calls the FootHolder script to activate the FootHolder. The functioning process of the script is depicted in (Fig. 2) below:

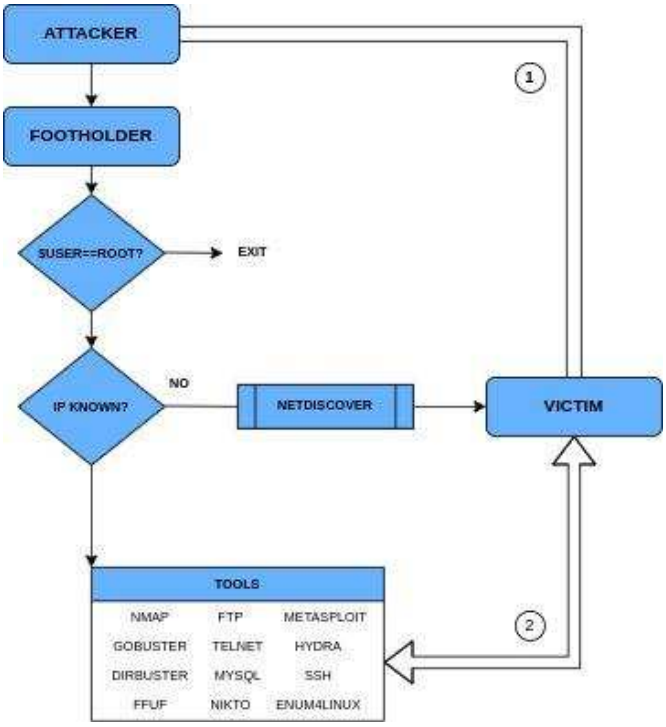

Fig.2. Working of the FootHolder

The Footholder script is used by the attacker by being invoked. The script will request root access when it is activated because the majority of enumeration and exploitation tools require root user permission. The script will terminate the session and exit if the user is not the root user.

The Footholder will start the enumeration phase of pentesting after the user has authenticated as the root user. The user will be prompted by the script to enter the victim or the target machine's IP address. The script assists the user by launching the NetDiscover script if the user is lacking the IP address of the target computer. Now that the user is associated with a network, NetDiscover will scan that network to find all of the active machines present and collect their IP addresses. The user may now identify the IP address that will be utilized for the test.Once the attacker or user gets the target computer's IP address, they may start the basic enumeration process (2). The user will be prompted to run nmap to scan for any open ports on the specified IP address. The user may now make use of the other tools as necessary to complete additional enumeration. After Exploiting the machine the user will establish a connection with the target/victim (1).

IV. IMPLEMENTATION AND DISCUSSION

The BASH language and the CLI Terminal are used to implement the utility. The **B**ourne-**A**gain **SH**ell, sometimes known as **Bash**, is a popular command-line shell for operating systems based on Unix. It was developed by Brian Fox for the GNU Project as a free software replacement for the original Bourne shell (sh). Since then, it has achieved widespread acceptance as the default shell for Linux and macOS variations. An operating system command-line interface is offered by the high-level programming language bash. System administrators and power users frequently utilize Bash for things like managing files, automating tedious processes, and controlling system resources. It is also a potent programming language that has the ability to modify data and automate difficult processes. Bash scripts can include commands, control structures, functions, and variables. They are performed one at a time.

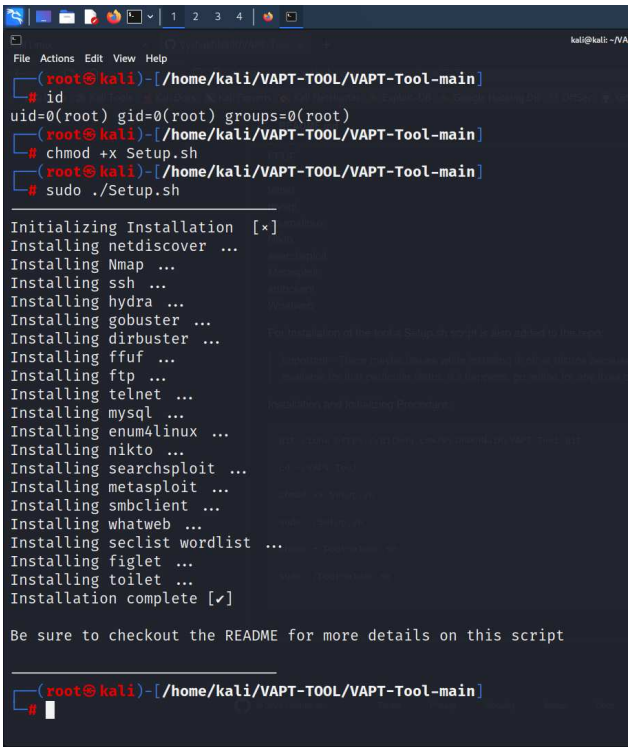

Fig 3. Initialisation and Setup

To start the tool, a few actions must be taken. Since KALI Machine is the most popular ethical hacking Linux Distro, it is preferable that the programme be operating on it during the initial step of resource confirmation.

The user will be given two files to utilize in order to configure the tools correctly. One is the setup file (Fig. 3), which, when run, checks to see if the user's computer has the necessary tools and installs them if it doesn't. When the setup file has finished running, the second file is the main tool, which is prepared for use. The important thing to keep in mind is that the user should be a ROOT user, who is regarded as having the greatest rights on the computer, while running the tool and setup file. To maximize the tool's potential for reconnaissance and exploitation, high-privilege access to the machine is required. A prompt advising executing the utility as root will be sent if a regular user attempts to run the tool.

A greeting and a request for input are displayed to the user when the tool is being used. Reconnaissance is used to identify susceptible machines in order to launch attacks against them. The user can move on to the NMAP step in the second phase if they know the IP address of the susceptible system. The Netdiscover utility (Fig. 4) is launched to recon the internal network and offer a list of IPs nearby if the user does not have the IP (Fig 5).

Fig 4. Netdiscover invoked

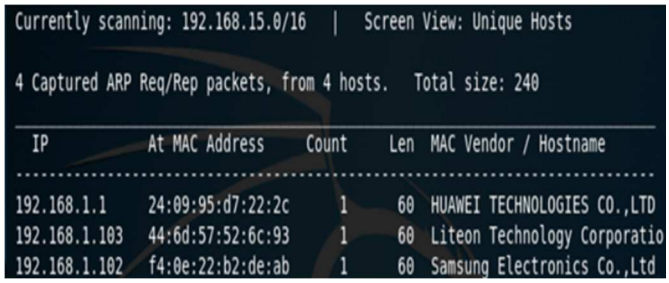

Fig 5 Results of the active devices on network

The enumeration stage comes after the objective has been determined. The NMAP utility evaluates the IP and delivers information on the weak device and open service that may be attacked.

The NMAP tool *(Fig. 5)* prompts the user to process with basic scan and then assesses the IP and provides details about the vulnerable machine and open services that can be exploited. Nmap has the ability to take upon arguments as well which can help the user obtain detailed information about the services running on the respective ports on the target machine. The user can use the '-h' tag to get a list of arguments that can be used along with the basic nmap scan. The most commonly used nmap tags are '-sV' , '-sC' ,'-sS', '-sL', which mean to find version-trace,script-scan,TCP SYN scan and Identify Hostnames respectively.

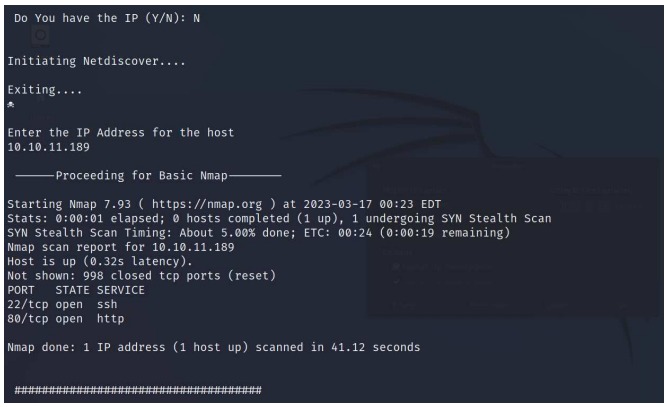

Fig 6. Results of basic Nmap Scan with IP address

The tool requests the port number of the services operating in the susceptible system once the NMAP output (Fig. 6) has been collected and offers service details and an explanation of each service's functionality (Fig. 7). The user may learn more about ports, their services, and how to get around the susceptible service by using this as an instructional tool.

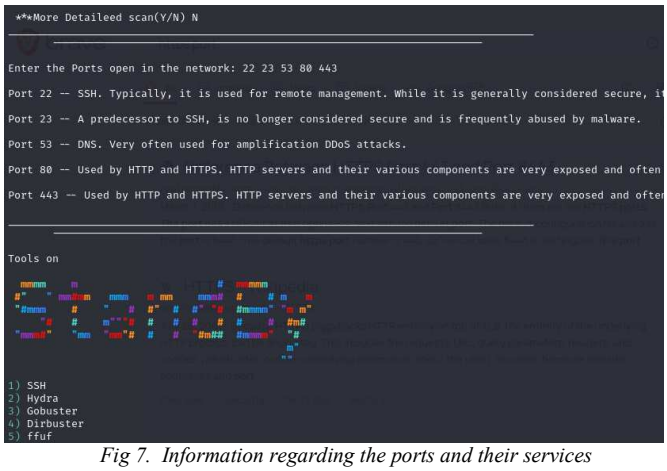

Fig 7. Information regarding the ports and their services

The user is presented with a list of available tools (Fig. 8) as numerous choices. When a choice is made, a brief explanation of the tool's features is shown, assisting the user in selecting the tool's application and strategy.

Fig 8. List of tools integrated with FootHolder

The user is given the choice to start the tool after reading the description. (Fig. 9) When started, the utility starts an xterm shell at the specified location. The user may now access the tool and run any required payloads, and the same is true for the other tools that are accessible.

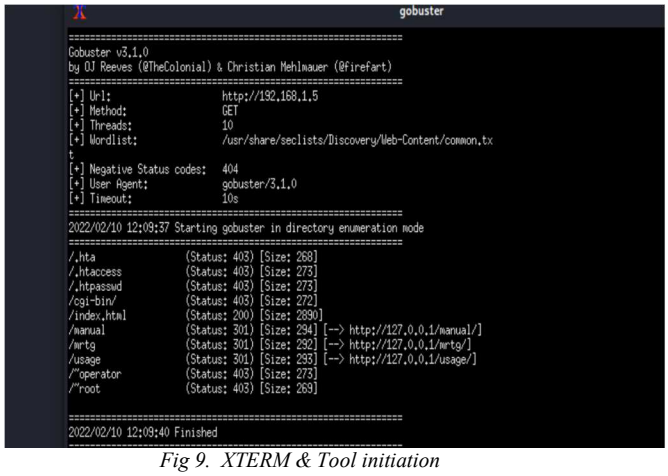

Fig 9. XTERM & Tool initiation

V. CONCLUSION

The FootHolder system is put into action after a thorough analysis of the system's needs and crucial components. It was made with the notion that by using it, the user would learn more about tools and develop competence. It was also made to be user-friendly for beginners. FootHolder was created by combining a number of tools and software components in order to guarantee the system's usability and efficacy. FootHolder has undergone testing to find any glitches or problems with the programme and to get user input on its usability and potential for development.

REFERENCES

[1] Analysis of Kali Linux Penetration Tools: A Survey of Hacking Tools
Matt Tigner,Hayden Wimmer,Carl M. Rebman, Jr. Department. of Supply Chain,Ops,and Information Management School of Business University of San Diego San Diego, CA USA.Proc. of the International Conference on Electrical, Computer and Energy Technologies (ICECET)
9-10 December 2021,

[2]Analysis and Impact of Vulnerability Assessment and Penetration Testing,Yugansh Khera, Deepansh Kumar, Sujay, Nidhi Garg Department of Computer Science Engineering Manav Rachna International Institute of Research and Studies Faridabad, India.2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con)

[3] EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration Ammrish Singh Beker Singh,Yusnita Yusof ,Yogeswaran Nathan School of Technology, Forensic and Cyber Security Research Centre Asia Pacific University of Technology and Innovation Bukit Jalil, Kuala Lumpur, Malaysia.2021 14th International Conference on Developments in eSystems Engineering (DeSE)

[4] Vulnerability Assessment and Penetration Testing,Sachin Umrao , Mandeep Kaur2 & Govind Kumar Gupta. Department of Computer Application, KIET, Ghaziabad, India. International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, 2012

[5] SSH and telnet protocols attack analysis using honeypot , Melike baser,Ebu Yusuf Guven,Istanbul University Cerrahpasa.2021 6th International Conference on Computer Science and Engineering (UBMK)

[6] Penetration Testing: Concepts, Attack Methods, and Defense Strategies Matthew Denis, Carlos Zena, Thaier Hayajneh Computer Science Department School of Engineering and Computing Sciences New York Institute of Technology Old Westbury, NY, USA. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)

[7] Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool Mujahid Shah Iqra Muhammad Junaid Hajvery University Lahore, Pakistan.2019 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019

[8] An Analysis of Vulnerability Scanners in Web Applications for VAPT Ashish Joshi ,Aditya Raturi,Santosh Kumar Security Consultants Bosch.1 st International Conference on Computational Intelligence and Sustainable Engineering Solution(CISES2022)

[9] Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation,ABDUL BASIT AJMAL, MUNAM ALI SHAH,Department of Computer Science, COMSATS University Islamabad. 10.1109/ACCESS.2021.3104260

[10] Analysis of Cyber Security Attacks using Kali Linux Gururaj H L, Lakshmi H ,Soundarya B C Computer Science and Engineering Vidyavardhaka College of Engineering Mysore, India.2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)

[11] Analysis and Overview of Information Gathering &
Tools for Pentesting : Alekya Sai Laxmi Kowta, Karan Bhowmick, Jeev Ratan Kaur, N. Jeyanthi School of Information Technology and Engineering
Vellore of Institute of Technology, Vellore, Tamil Nadu, India.2021 International Conference on Computer Communication and Informatics (ICCCI -2021)

[12] Accessing LinkedIn and Google Email Databases Using
Kali Linux and TheHarvester Zornitsa Terneva1, Ivaylo Vladimirov2.ICEST'2021

[13] Intrusion detection on software defined networking
K. Reddy, T.N., Annapurani Panaiyappan
International Journal of Engineering and Technology(UAE)-2018

[14] VPN System Tracking through Media Access Control (Mac) Address
K Debanjan Bhattacharya Dr.Annapurani Panaiyappan
International Journal of Advanced Science and Technology-2020/6

[15] Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology,Jai Narayan Goela,b,*, BM Mehtreb.3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)