

Linux Service Exploitation and Security Assessment

Reddyvari Venkateswara Reddy, K. Sujitha, Aneesh Satla, Sujith Venkat Avinash Irrinki, Manideep Vydy,
Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, India.
Assistant Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, India.
B. Tech Students, Department of CSE (Cybersecurity), CMR College of Engineering & Technology, Hyderabad, India.

Abstract— This project represents a comprehensive and comprehensive analysis of customized security testing practices specifically for the Linux environment, with a particular focus on the Metasploitable server. The project covers a variety of approaches including implementation of a implementation and safety assessment methods. To begin with, a standardized glossary has been carefully prepared, targeting potential entry points and credentials for penetration testing. The project then uses Nmap, a powerful network scanning tool that allows for a comprehensive analysis of open ports and their associated services. This initial assessment phase lays the foundation for identifying potential vulnerabilities in the system. The project then takes advantage of the power of the Metasploit module, transitioning seamlessly into the realm of implementation. An important aspect targets Telnet vulnerabilities, where the project finds and selects appropriate metasploit modules to exploit potential vulnerabilities in the Telnet implementation. Furthermore, the implementation extends to the vsftpd implementation so, with a specific focus on version 2.3.4. To find the exploits included in this version, you can easily use the searchsploit tool, and use the Metasploit modules to use the vsftpd backdoor.

Keywords: KaliLinux, Services, Nmap, Security Assessment, and Exploitation.

I. INTRODUCTION

The project is a script designed to conduct Service Exploitation and Security Assessment on a Linux-based system, specifically targeting the Metasploitable machine. In line with the overall approach to security testing, the script unfolds in a structured sequence. The first step is to create a word list with passwords and usernames, the most important step in simulating potential access scenarios. In addition, the script uses Nmap to perform an exhaustive port scan of the target system in order to identify open ports and services that may be exposed to vulnerabilities. The script helps to identify vulnerabilities in services running on a victim's machine and use the nmap tool for exploiting them. During the telnet login phase, a script test is performed on relevant Metasploit modules to determine which module they are and set parameters such as password report, target IP address, user name etc. . Sleep intervals occur when the most executions are made, which may lead to different observations or behaviour. The script will use the searchsploit tool to find the applicable exploits, and will start a new session of the Metasploit console. It identifies the vsftpd_234_backdoor make the most, configures the necessary strategies, and executes the take

advantage of. The script tests available routes, configures the target IP addresses rhosts and then continues to use a vsftpd backdoor. If executed successfully, the script keeps with commands which include ifconfig and the shell enters a countless loop to continue executing the script (bash1.Sh).

II. LITERATURE REVIEW

1. Mebster, R., and Metcalf, D. (2017). Hacking is the spycraft art : In order to shed light on the offensive side of cybersecurity, Metcalf and Webster's study looks at the real-world applications of cybercrime and fraud. The script places a strong emphasis on ethical hacking approaches, but it's crucial to know how possible attackers might operate. This source has improved the literature by offering useful information that is consistent with the penetration testing techniques covered in the script.
2. Stallings, W. (2017). Applications and standards: essential components of network security. Pearson. The thorough analysis of network security fundamentals by William Stallings is a useful tool for comprehending the underlying ideas and guidelines in this field. Network level security techniques, intrusion detection systems, and cryptographic protocols are just a few of the many subjects discussed.
3. Shostack, A. (2014). Threat Modeling: Protecting the Designed Environment. Wiley. Shostack's work in threat modeling offers a particular viewpoint on safe system design. Focusing on active security planning, the author develops techniques for detecting and mitigating possible vulnerabilities throughout the system development phase. This methodology aligns with the script's focus on security protocols and strategic planning to safeguard a target system from potential vulnerabilities..
4. Kim, D., and Solomon, M. (2015). the fundamental ideas behind information system security: Learning by Jones & Bartlett. Kim and Solomon's analysis of information system security basics offers a more comprehensive for understanding the ideas safe computing environments.

II. OBJECTIVE

In particular, the project aims at developing and implementing an evaluation of service utilisation and security for a Linux system based on Metasploitive Machines. The script aims to emulate by creating a password and username wordlist, conducting a thorough Nmap port scan to identify the services running on the victim machine and vulnerabilities, and execute the Metasploit framework for active exploitation. One of the focus areas is to exploit telnet login vulnerabilities and to target vsftpd service vulnerabilities, in particular version 2.3.4. I am on the victim's device. The objective is to assess the security situation of the target system and determine its potential weaknesses. This project is a practical examination of offensive and defensive security practices, demonstrating the integration of script tools and frameworks into the Linux environment, with a view to increasing overall system resilience.

III. SYSTEM REQUIREMENTS

1. Hardware: Adequate hardware resources for running the Kali Linux distribution, including sufficient RAM, CPU, and disk space. The Metasploitable machine, being a virtual machine for security testing purposes, should also have appropriate hardware resources allocated, depending on the virtualization platform in use.
2. Operating System: The script is designed for a Linux-based environment, and it specifically mentions Kali Linux, which is a Debian-based distribution commonly used for penetration testing and ethical hacking. The Metasploitable machine mentioned in the context is also a Linux-based system.
3. Internet Connection: A stable and preferably high-speed internet connection is recommended for downloading updates, tools, and any additional resources required during the security testing. Internet connectivity is crucial for fetching the latest exploit databases, updating tools like Metasploit, and accessing additional modules or scripts.

Tools Required for Linux Service Exploitation and Security Assessment:

1. Kali Linux : The operating system mentioned in the script, chosen for its focus on penetration tests and ethical hackers, is Kali Linux. It has a wide range of installed tools and a Debian based environment that is suitable for security testing.

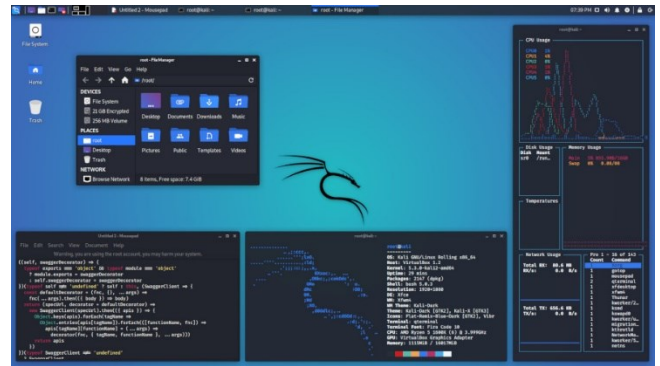


Fig-1 : Kali Linux

2. Nmap : powerful Open Source NetworkScan tool for discovering hosts and services on the network topology, which creates a map of these networks. In this project, Nmap will be used to perform a full scan of the port on Metasploit in order to detect operational ports and services.

```
➔ ~ nmap scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-16 11:55 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 11:55 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency)
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
9929/tcp  open  nping-echo
31337/tcp open  Elite
Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds
```

Fig-2 : Nmap

3. Metasploit : A penetration testing framework enabling the development, testing and execution of exploit code on a remotely reachable target. This script uses Metasploit to exploit vulnerabilities, in particular the telnet login and vsftpd service vulnerability.

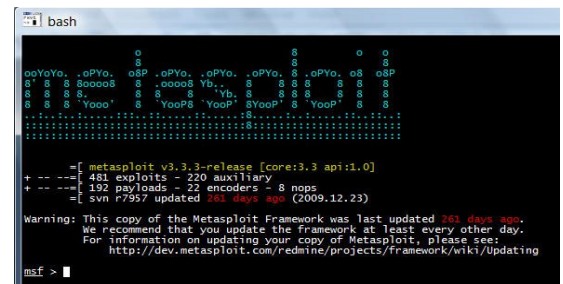


Fig-3 : Metasploit

- Searchsploit : searchsploit is a command line tool that looks for known exploits and vulnerabilities in Exploit Database, exploit_db For vsftpd version 2.3.4, searchsploit is used in the project to find relevant exploits. and exploits that the user is looking for.

```

root@kali:~# searchsploit vsftpd
-----
Exploit Title
-----
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
    
```

Fig-4 : Searchsploit

- Bash: Bash (Bourne Again SHell) scripting is used in the project for creating and executing scripts, such as the script named "bash1.sh" mentioned in the loop.

```

skickar@Dell-3 Nuke % which bash
/bin/bash
skickar@Dell-3 Nuke % ls
expect.exp trigger.sh
skickar@Dell-3 Nuke % nano bash.sh
skickar@Dell-3 Nuke % bash bash.sh
Hackers Love to learn on Null Byte
skickar@Dell-3 Nuke % nano bash.sh
skickar@Dell-3 Nuke % bash bash.sh
I firmly believe that Verne is the president
skickar@Dell-3 Nuke % nano bash.sh
skickar@Dell-3 Nuke % bash bash.sh
skickar@Dell-3 Nuke % bash bash.sh
What is your name?
Kody
Wow, Kody sounds like a good name
skickar@Dell-3 Nuke % nano bash.sh
skickar@Dell-3 Nuke % bash bash.sh
What is your name?
Kody
bash.sh: line 9: syntax error: unexpected end of file
skickar@Dell-3 Nuke % nano bash.sh
skickar@Dell-3 Nuke % bash bash.sh
What is your name?
Kody
    
```

Fig-5 : Bash

- Virtualization Platform : To run the Metasploitable machine as a virtual instance, a virtualisation platform is required. For security testing, virtual machines such as VirtualBox or VMware can be created and managed by users



Fig-6 : Virtualization Platform

IV. PROBLEM DEFINITION

The script-based Service Exploitation and Security Assessment on Linux aims to address the need for a customized and controlled approach to assessing the security posture of Linux systems. This method involves the creation and execution of a script that sequentially performs actions such as password list generation, network scanning, and exploitation attempts against specific services.

V. EXISTING SOLUTIONS

- OpenVAS (Open Vulnerability Assessment System) : An OpenVAS is an open-source vulnerability scanner that performs comprehensive security assessments on networks and systems. It identifies potential vulnerabilities, misconfigurations, and security issues, providing reports remediation.

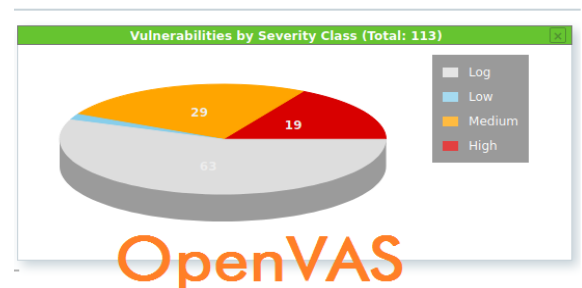


Fig-7 : OpenVAS

- Wireshark : Wireshark is a widely-used network protocol analyzer that captures and inspects data on a network in real-time. It aids in the identification of network vulnerabilities, traffic analysis, and the detection of suspicious activities.

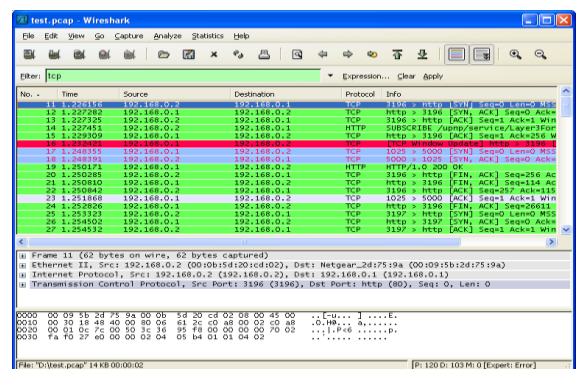
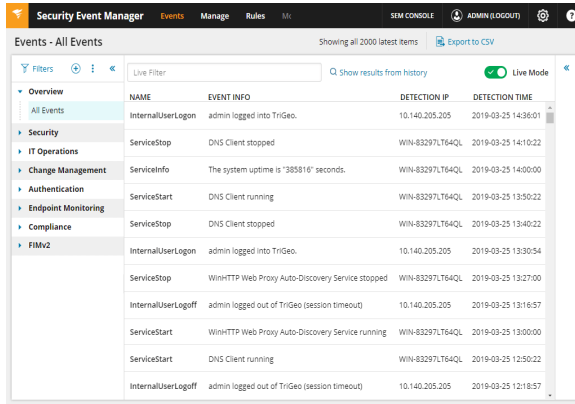


Fig-8 : Wireshark

3. Snort : Snort is an open-source intrusion detection and prevention system (IDPS) that analyzes network traffic for suspicious activities. It can be used to detect and respond to potential security threats in real-time.



NAME	EVENT INFO	DETECTION IP	DETECTION TIME
InternalUserLogon	admin logged into TriGeo.	10.140.205.205	2019-03-25 14:36:01
ServiceStop	DNS Client stopped	WIN-83297LT64QL	2019-03-25 14:10:22
ServiceInfo	The system uptime is '385816' seconds.	WIN-83297LT64QL	2019-03-25 14:00:00
ServiceStart	DNS Client running	WIN-83297LT64QL	2019-03-25 13:50:22
ServiceStop	DNS Client stopped	WIN-83297LT64QL	2019-03-25 13:40:22
InternalUserLogon	admin logged into TriGeo.	10.140.205.205	2019-03-25 13:30:54
ServiceStop	WinHTTP Web Proxy Auto-Discovery Service stopped	WIN-83297LT64QL	2019-03-25 13:27:00
InternalUserLogoff	admin logged out of TriGeo (session timeout)	10.140.205.205	2019-03-25 13:16:57
ServiceStart	WinHTTP Web Proxy Auto-Discovery Service running	WIN-83297LT64QL	2019-03-25 13:00:00
ServiceStart	DNS Client running	WIN-83297LT64QL	2019-03-25 12:50:22
InternalUserLogoff	admin logged out of TriGeo (session timeout)	10.140.205.205	2019-03-25 12:18:57

Fig-9 : Snort

VI. LIMITATIONS OF THE EXISTING SYSTEM

1. Limited Customization: Existing solutions may offer a predefined set of features and workflows, limiting the ability to customize the testing methodology according to specific requirements. This lack of flexibility could be a drawback when dealing with unique scenarios or complex environments.
2. Complex User Interfaces: Some security tools come with intricate graphical user interfaces (GUIs) or command-line interfaces (CLIs) that might pose challenges for users with limited experience. The complexity of these interfaces could result in a steeper learning curve and potentially hinder efficient usage.
3. Resource Intensiveness: Certain security solutions can be resource-intensive, requiring significant computing power and memory. This could be a limitation, particularly for users with resource-constrained environments or when conducting assessments on a large scale.
4. Lack of Automation in Exploitation: Some solutions might lack comprehensive automation in the exploitation phase. Manual intervention might be required to execute exploits or assess the impact of vulnerabilities, potentially slowing down the assessment process.
5. Cost Constraints: Certain commercial security solutions come with licensing costs that might be a

limiting factor for individuals or organizations with budget constraints. This limitation could impede access to advanced features or support.

VII. WORK FLOW

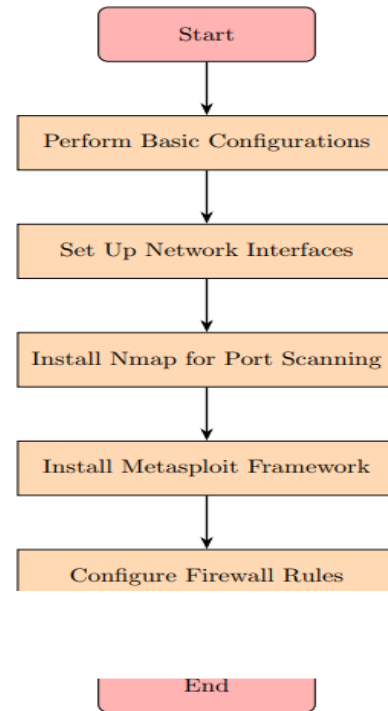


Fig-10: Work Flow

1. Start of Process: This is the starting point of the workflow.
2. Basic Configuration:
 - a) Network Configuration.
 - b) Interface Activation.
 - c) Update System.
3. Setting up Interfaces: Nmap Installation.
4. Setting Up Rules:
 - a) Firewall Rules.
 - b) IDS/IPS.
5. End of Process: This is the endpoint of the workflow.

VIII. ARCHITECTURE

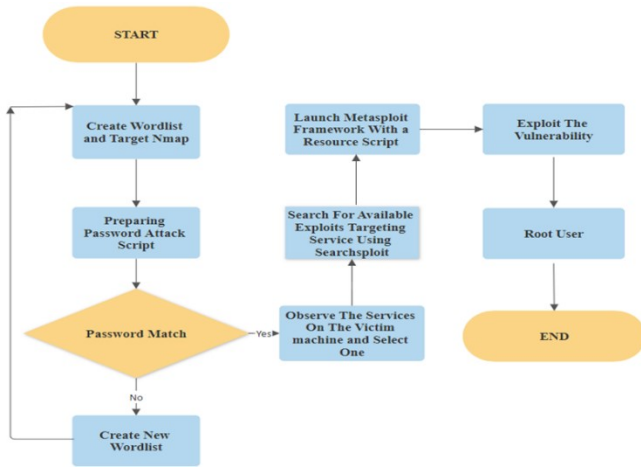


FIG-11: ARCHITECTURE

1. We will create a wordlist to enter victim machine.
2. Password attack on Victim machine.
3. Perform Nmap:
 - a) Search for services running on the victim machine
 - b) Find Vulnerabilities of services
 - c) View possible exploits possible
 - d) Choose the exploit
 - e) Perform the Exploitation
4. By Exploiting we can enhance cybersecurity skills and perform security assessment.

IX. CONCLUSION

In conclusion, Linux service exploitation and security assessment are integral components of ethical hacking and cybersecurity practices. This project provides a hands-on approach to identifying vulnerabilities, exploiting services, and conducting a comprehensive security assessment on a Linux-based system.

X. RESULTS

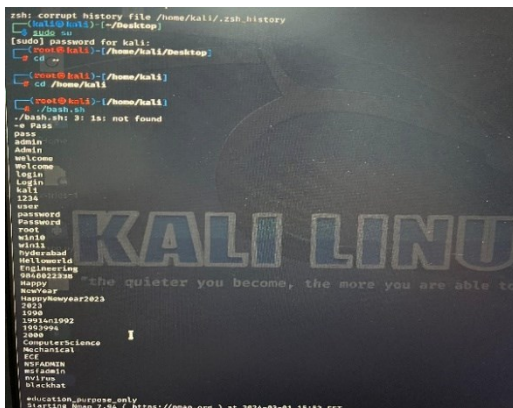


Fig-12: Wordlist Creation

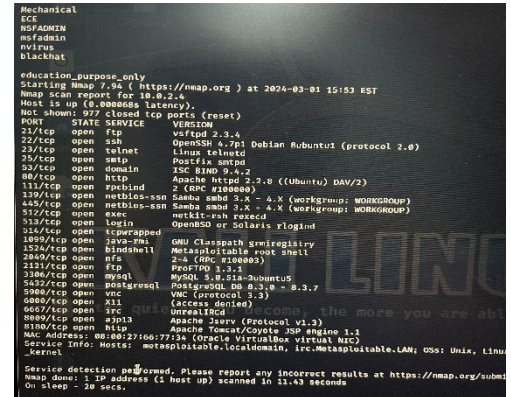


Fig-13: Nmap Scan



Fig-14: Connecting to victim machine



Fig-15: Exploiting the service running on the victim machine

XI. REFERENCES

1. Kurtz, G., & Westin, K. (2008). Hacking Exposed Linux: Linux Security Secrets and their Solutions. McGraw-Hill Education.
2. Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
3. OSSEC. (n.d.). OSSEC - Open Source Security Information and Event Management, <https://www.ossec.net/>
4. Splunk Inc. (n.d.). Splunk. Retrieved from <https://www.splunk.com/>
5. Metasploit. (n.d.). Metasploit. Retrieved from <https://www.metasploit.com/>
6. Nmap (n.d.). Nmap Retrieved from <https://nmap.org/>
7. Brute force attack Retrieved from <https://www.owasp.org/>
8. Shell scripting has been Retrieved from <https://www.freecodecamp.org/news/bash-scripting-tutorial-linux-shell-script-and-command-line-for-beginners/>
9. Kali Linux version 2023.4 (Cloud ARM64,Vagrant Hyper-V&Raspberrypi5) <https://www.javatpoint.com/kali-linux>
10. Creating wordlist for brute force attack, <https://be4sec.com/2021/02/17/creating-wordlist-for-brute-force-attack>