

Penetration Testing Report

Prepared By

Swagat Aryal

Table of Contents

1. Introduction............................................................................................03
2. Objectives...............................................................................................03
3. Environment...........................................................................................03

3.1 VMWare........................................................................................................03

3.2 Kioptrix and parrot........................................................................................03

3.3 Network.........................................................................................................03

1. Methodology..........................................................................................03

4.1 Information Gathering...................................................................................04

4.1.1 Network Scanning......................................................................................04

4.1.2 Tools and Techniques Used...........................................................04

1. Findings..................................................................................................04

5.1 Information Gathering...............................................................................................04

5.1.1 Network Scanning......................................................................................04

5.1.2 Service Enumeration...................................................................................05

5.2 Vulnerability Assessment...........................................................................................05

5.2.1 Web Application Analysis...........................................................................05

5.2.2 Service Vulnerability Analysis....................................................................06

5.3 Exploitation.................................................................................................................07

5.3.1 Gaining Initial Access using Metasploit for samba.....................................08

5.3.2 Gaining Initial Access of Apache 1.3.20.....................................................09

References.....................................................................................................13

1.Introduction

Kioptrix Level 1 is a vulnerable virtual machine designed for practicing penetration testing and ethical hacking skills. It provides a realistic environment to test your security knowledge and techniques.  
  
Overview

Kioptrix Level 1 simulates a basic Linux server that contains multiple vulnerabilities that can be exploited to gain unauthorized access. The goal is to identify these vulnerabilities and exploit them to escalate privileges and gain control over the system.

2. Objectives of the Pentesting Report

The primary objectives of this pentesting report are to document the methodology used to assess the security of Kioptrix Level 1, identify vulnerabilities, exploit those vulnerabilities, and demonstrate privilege escalation techniques.

**3. Environment/ requirement:**

1. VMware: VMware is required to run kioptrix and parrot.
2. Kioptrix and parrot : installed kioptrix and parrot from the below link

Kioptrix: <https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>

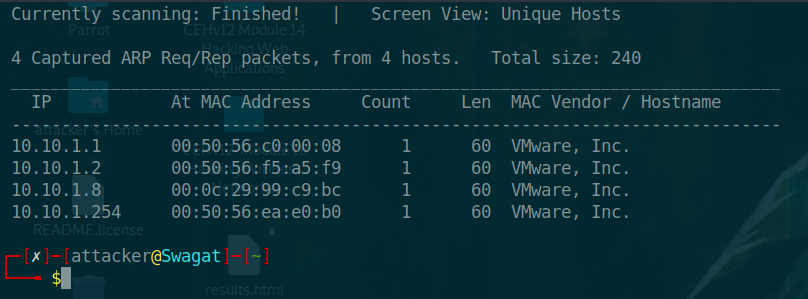
Parrot :[Parrot Security](https://www.parrotsec.org/download/)

And configured in vm

1. Network: we configured the network of both parrot and kioptrix as NAT.

4. Methodology for Pentesting

4.1 Information Gathering

4.1.1 Network Scanning

4.1.2 Tools and Techniques Used

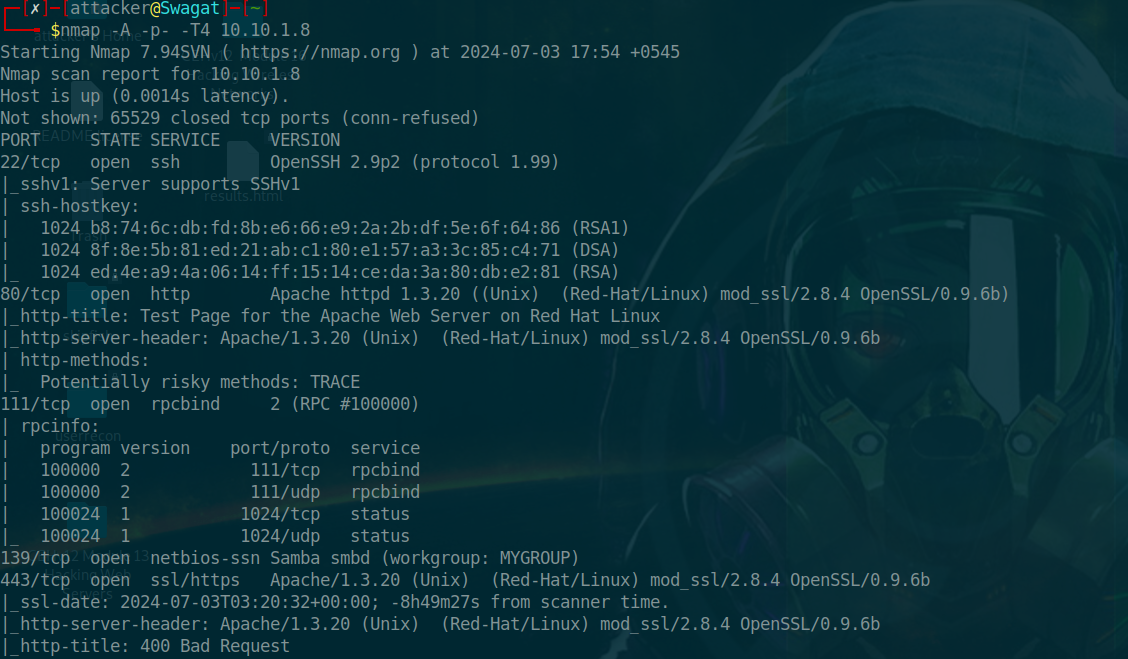
Various tools and techniques such as Nmap for network scanning, Metasploit for exploitation, Nikto for web server scanning, and manual enumeration will be utilized during the pentest to uncover vulnerabilities and weaknesses in the system.

5. Findings:

5.1 **Information Gathering**

**5.1.1 Network Scanning**

Performed an Nmap scan to identify open ports and services:



**Open Ports Identified**:

* Port 22: SSH
* Port 80: HTTP
* Port 111: RPC
* Port 139: Samba
* Port 443: SSL

5.1.2 **Service Enumeration**

* **HTTP (Port 80)**: The web server is running Apache 2.0.52.
* **smb (Port 139)**: Running samba

5.2 Vulnerability Assessment

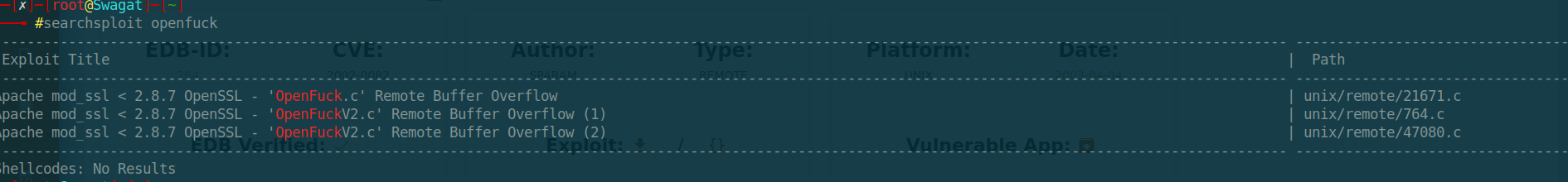
5.2.1 Web Application Analysis

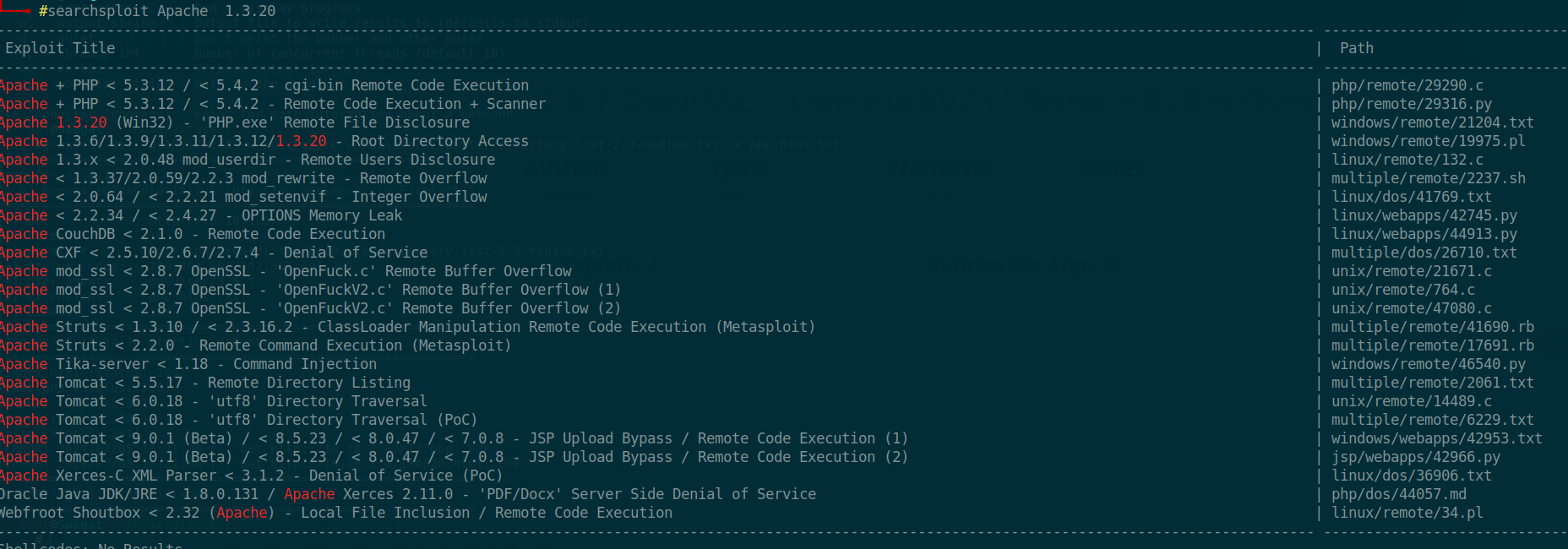
Used Nikto to scan the web server for vulnerabilities:



5.2.2 Service Vulnerability Analysis

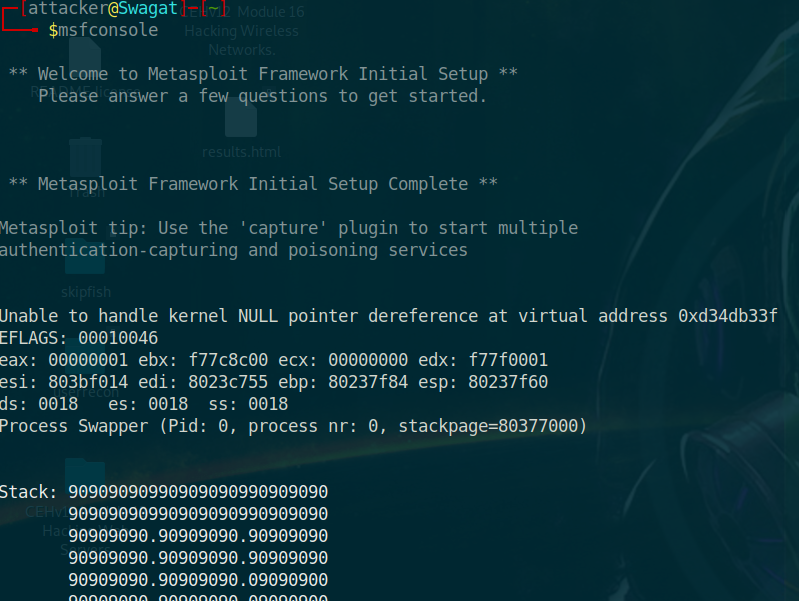
Checked for known exploits in Searchsploit

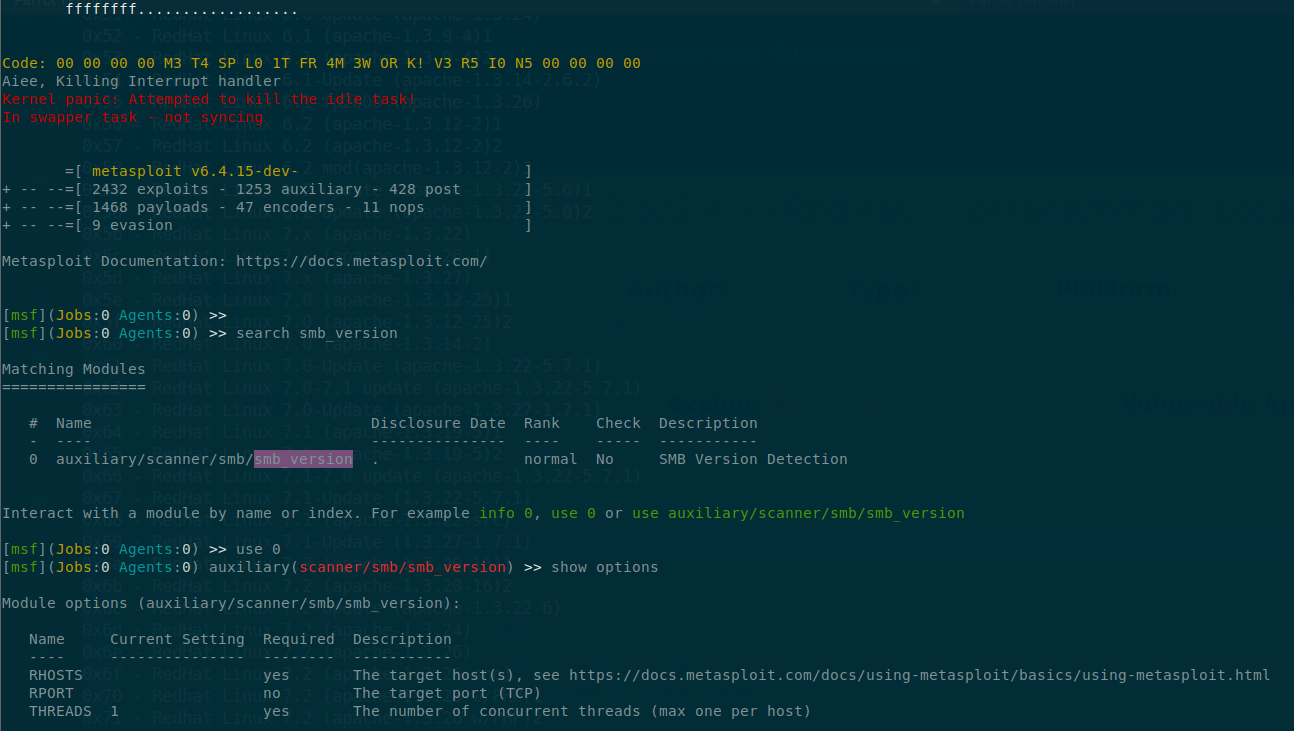


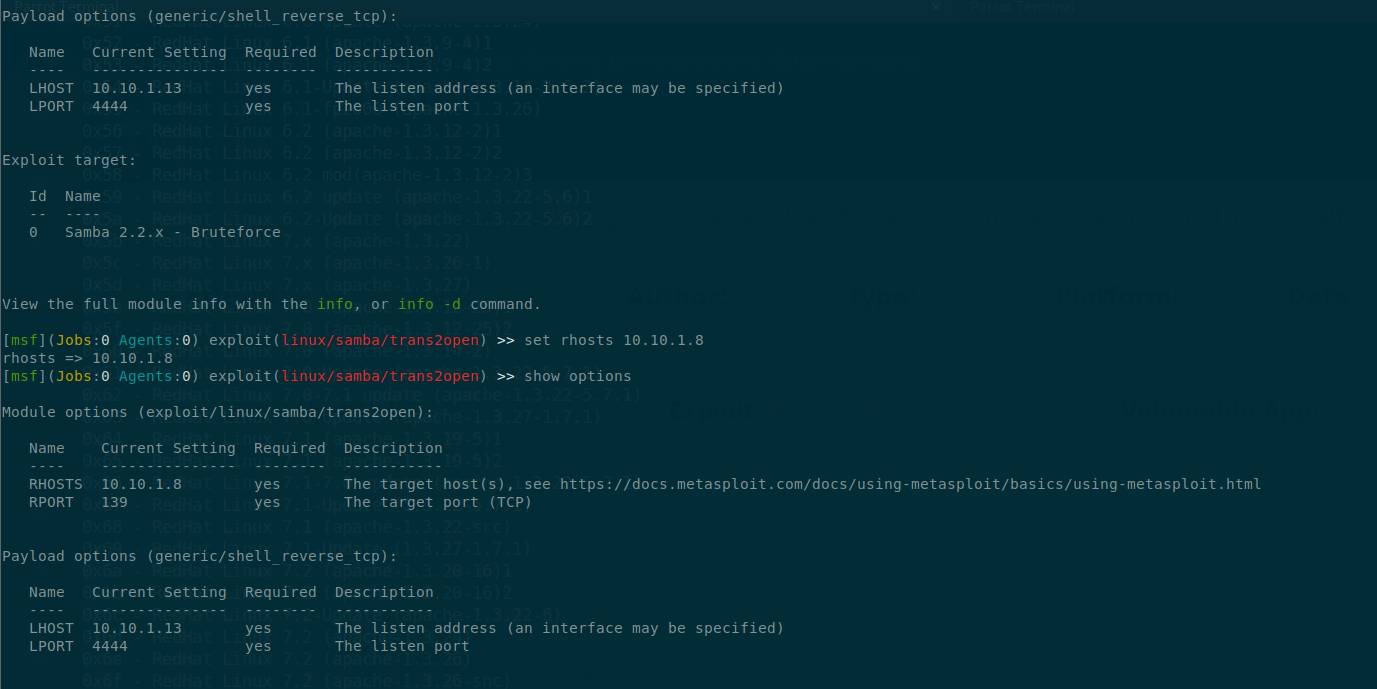


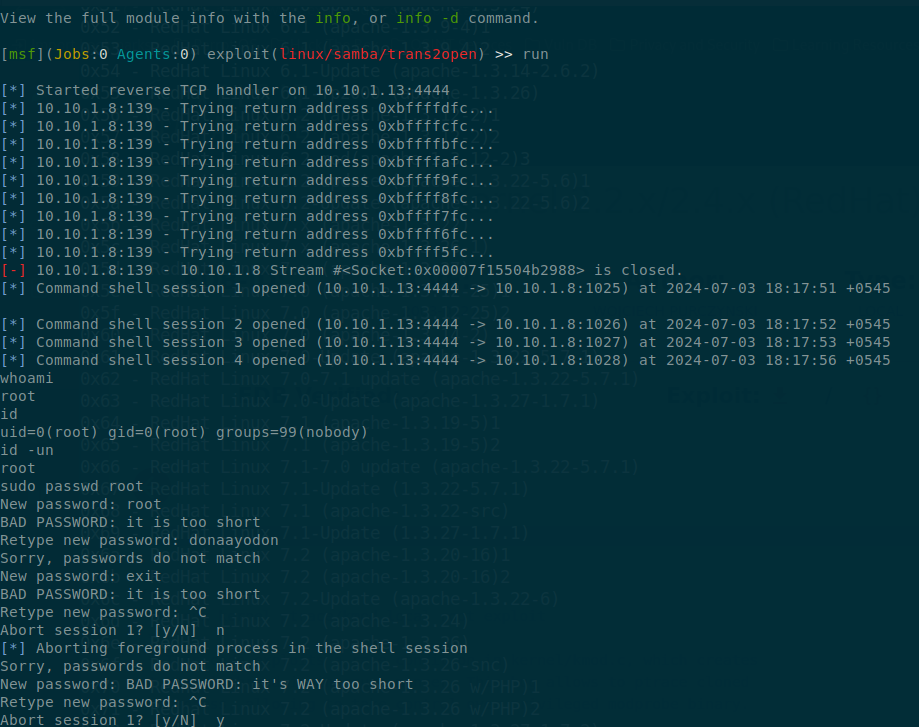
5.3 Exploitation

5.3.1 Gaining Initial Access using Metasploit for samba

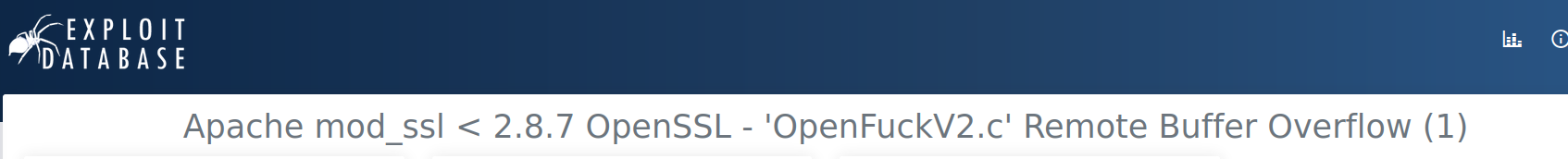




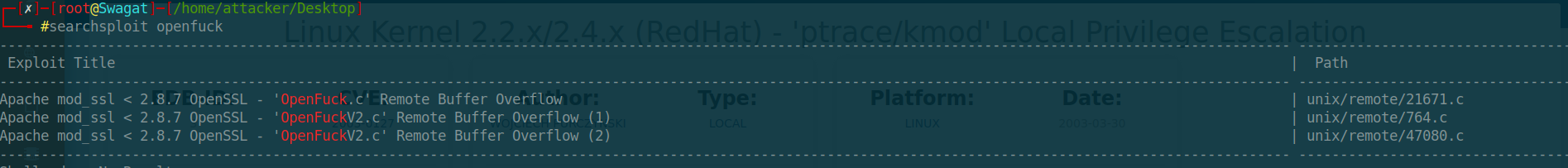




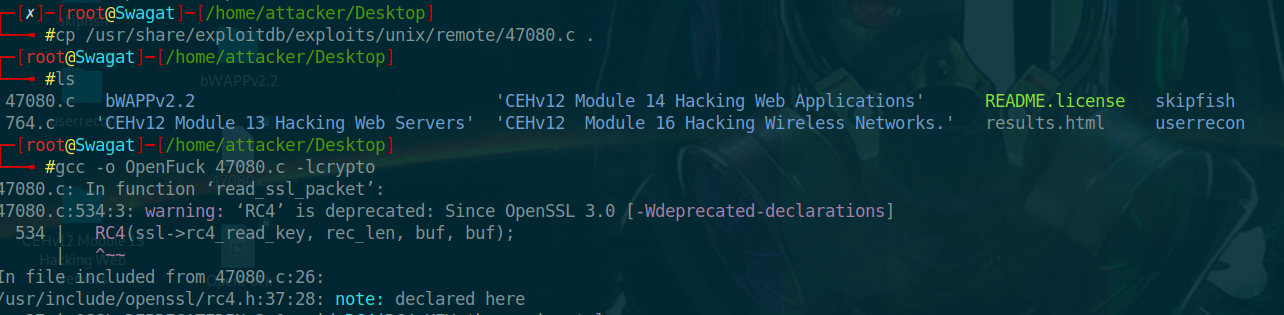
5.3.2 Gaining Initial Access of Apache 2.8.7



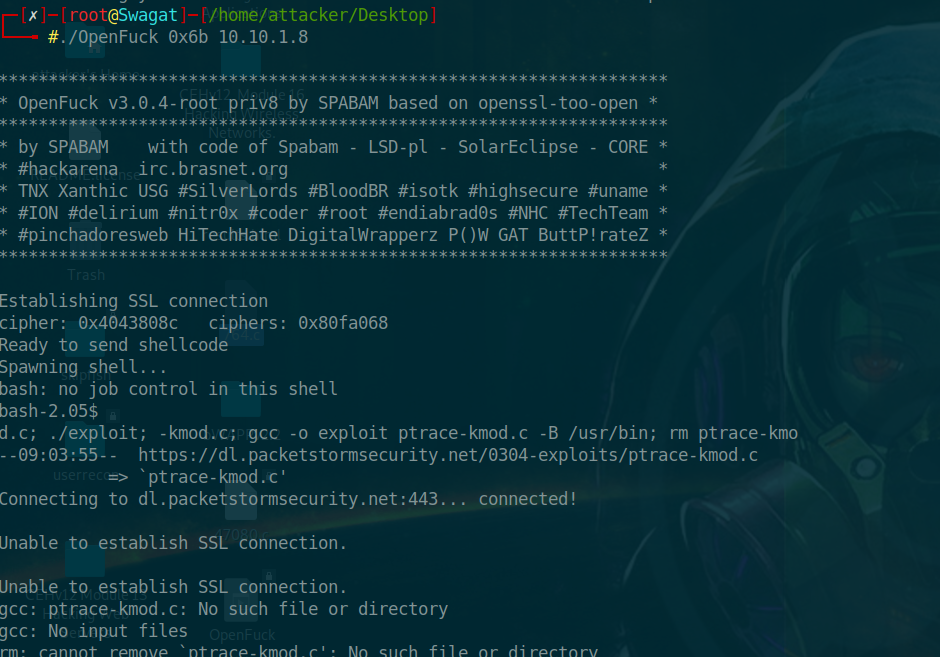
Found Apache 2.8.7 as ”OpenFuck” in exploit database



Search OpenFuck in searchsploit and got exploits.



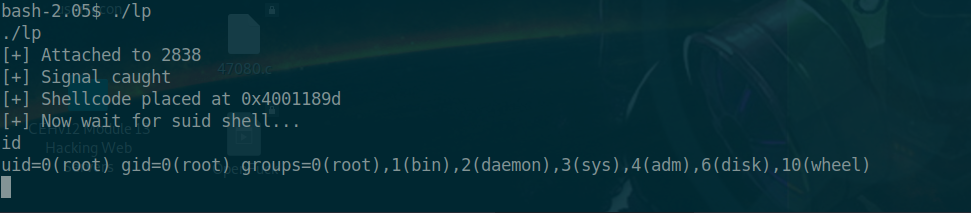
While running./OpenFuck got this thigs:



Runed. /OpenFuck 0x6b with kipoyrix ip and got this result.



Used wget command to download the exploit and execute it and got the root access.



Reference

[Sample-Penetration-Test-Report-PurpleSec[1].pdf](file:///C:/Users/swaga/AppData/Local/Microsoft/Windows/INetCache/IE/DT9F1LGW/Sample-Penetration-Test-Report-PurpleSec%5b1%5d.pdf)

<https://www.exploit-db.com/exploits/3>

<https://www.exploit-db.com/exploits/764>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835>

[Kioptrix (notion.site)](https://oasis-coat-c98.notion.site/Kioptrix-47dc2e9564454eef85fbe0d36e08f48a)

[Hacking Kioptrix Level 1 Write-up | by Cybertech Maven | Medium](https://medium.com/@jbtechmaven/hacking-kioptrix-level-1-write-up-78875f67e60a)