FINAL EXAM REPORT

9th February 2025

Cybersploit: 1

Name : Sarthak Das

Session : 9th November 2024 – 18th January 2025

For the class of Ethical Hacking, taught by

Oihik Mitra

Abstract

This report is a documentation of my walk-through of the **Cybersploit: 1** room in Vulnhub where the goal is to capture three flags. The link for the same can be found here: https://www.vulnhub.com/entry/cybersploit-1,506/. The upcoming sections will cover my capture of each of the three flags. This was submitted as a part of my final examination for the course.

Contents

1 The First Flag

Figure 1: As a first step, I downloaded the Cybersploit 1 OVA file and spun up a virtual machine on VMWare Player 17. As I could see, this was not a cold boot but the user named *cybersploit* already had an active session running.

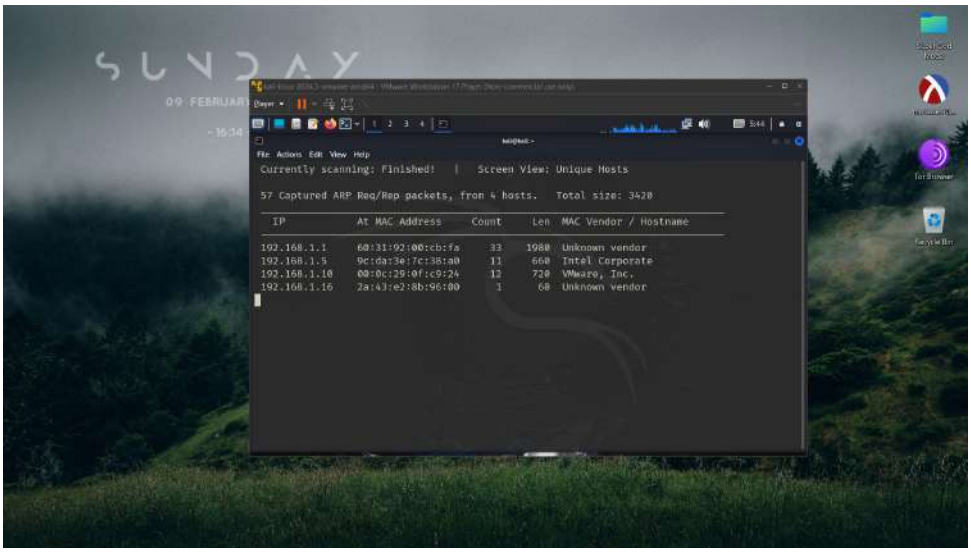

Figure 2: So the next step was to spin up my Kali Linux VM and run the commands *ifconfig* (which gave my IP address 192.168.1.7) and *netdiscover -r 192.168.1.7* to detect the cybersploit VM in the network. There was only one machine with VMWare as the vendor, so this must be my target machine. The target IP was 192.168.1.10.

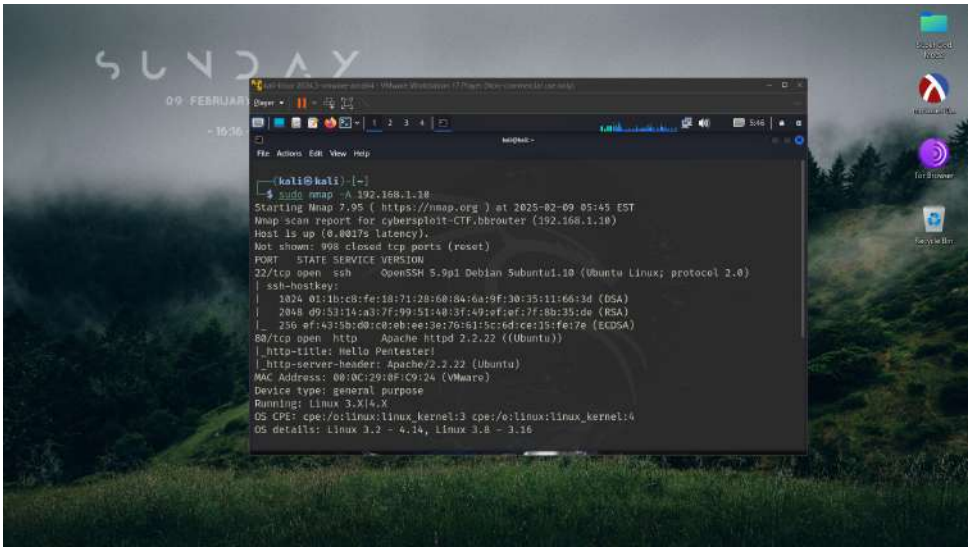

Figure 3: An aggressive nmap scan on the target IP (*sudo nmap -A 192.168.1.10*) showed that it was running not only an HTTP service (port 80) but also an SSH service (port 22), meaning that I could potentially SSH into the system if I found the password.

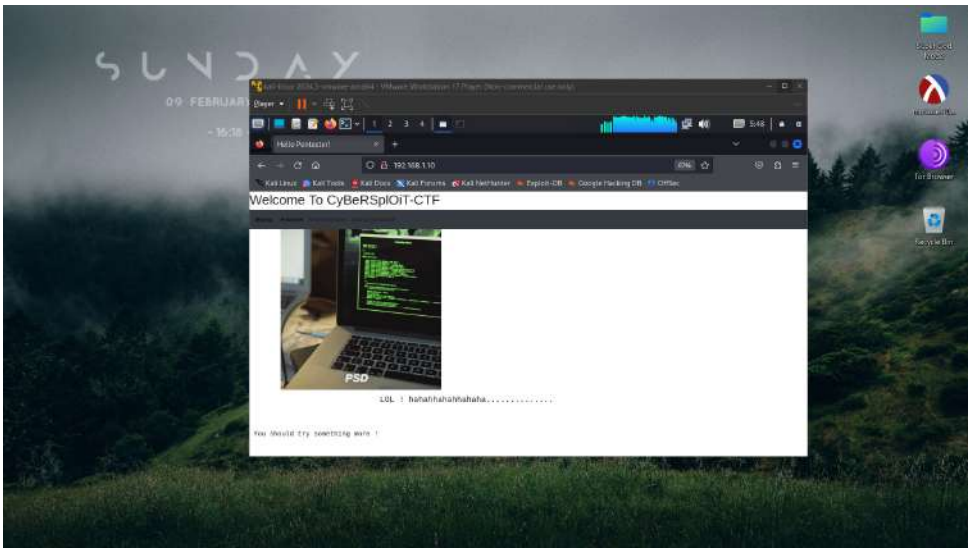

Figure 4: The first logical thing to do from here on was to open up Firefox and visit the IP address. The webpage titled 'Hello Pentester!' showed me that I was on the right track but needed something more.

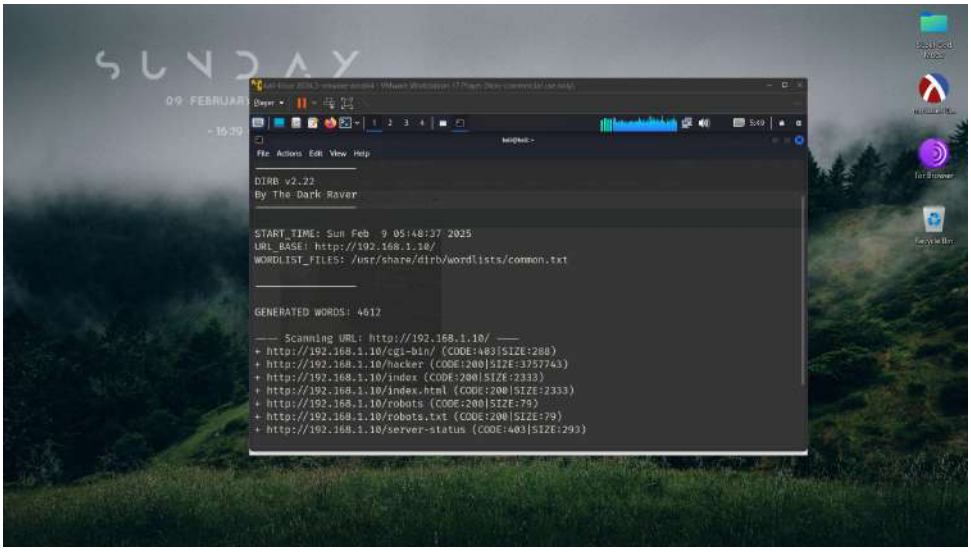

Figure 5: So I ran a directory enumeration scan on the server (*dirb http://192.168.1.14/*) and found out that it has a text file titled *robots.txt*, besides the usual *index.html*.

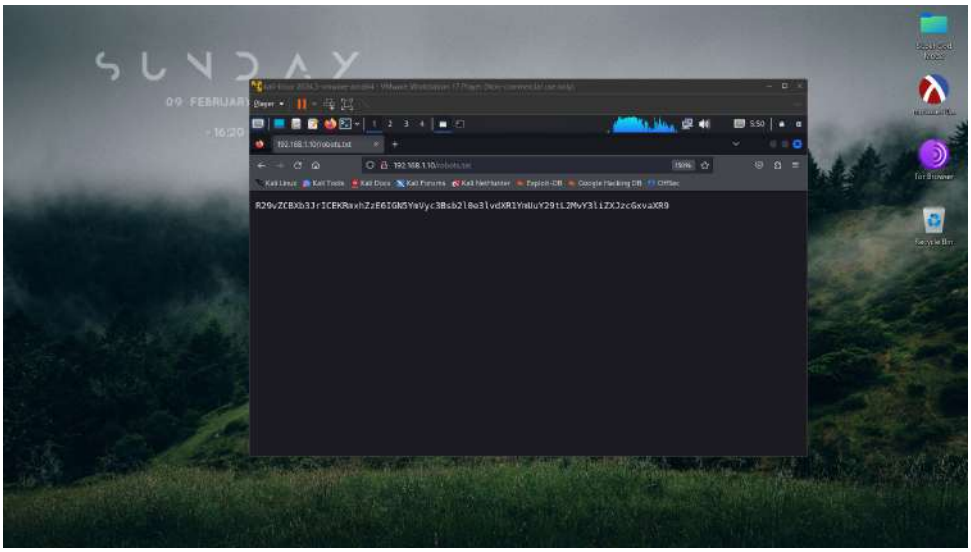

Figure 6: Visiting *http://192.168.1.10/robots.txt* gave me a BASE64 code, which I then needed to decode.

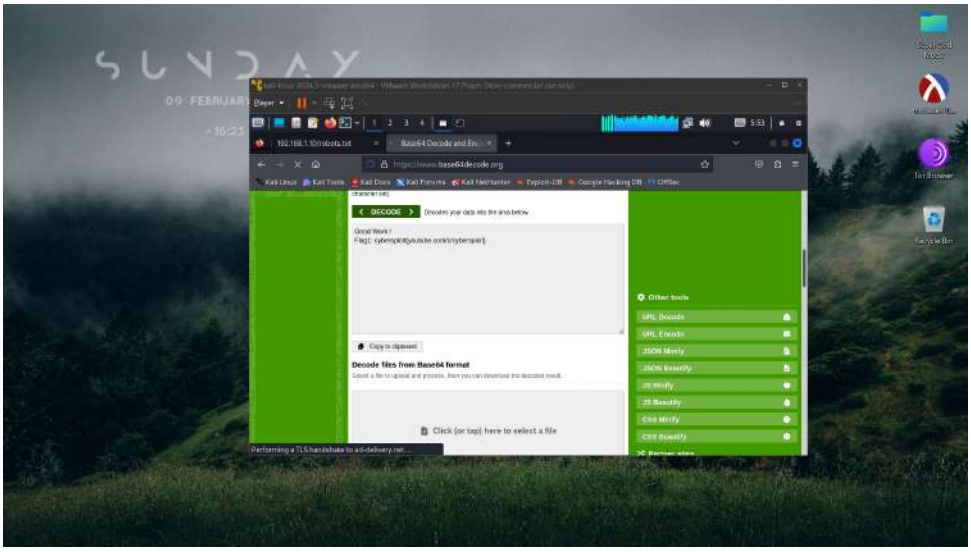

Figure 7: The code when decoded using an online BASE64 to text decoder revealed the first flag to be: **cybersploit{youtube.com/c/cybersploit}**.

2 The Second Flag

Figure 8: Upon inspecting the source code of the webpage, I found the username: *itsskv*. Taking a guess that the first flag could be the password of this user, and recalling that the SSH service was already running, I decided to attempt a remote login (*ssh itsskv@192.168.1.10*).

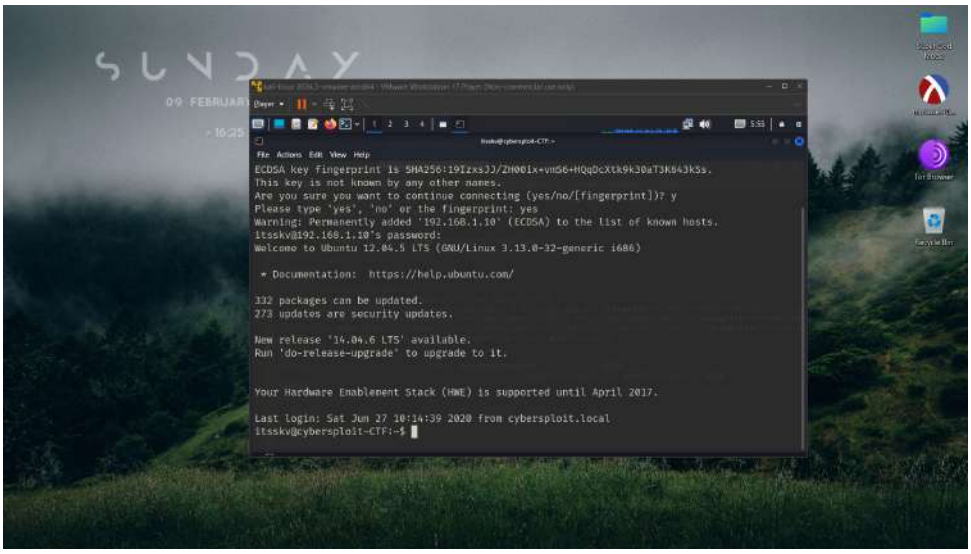

Figure 9: The first flag was indeed the password, and I was successfully logged into the system.

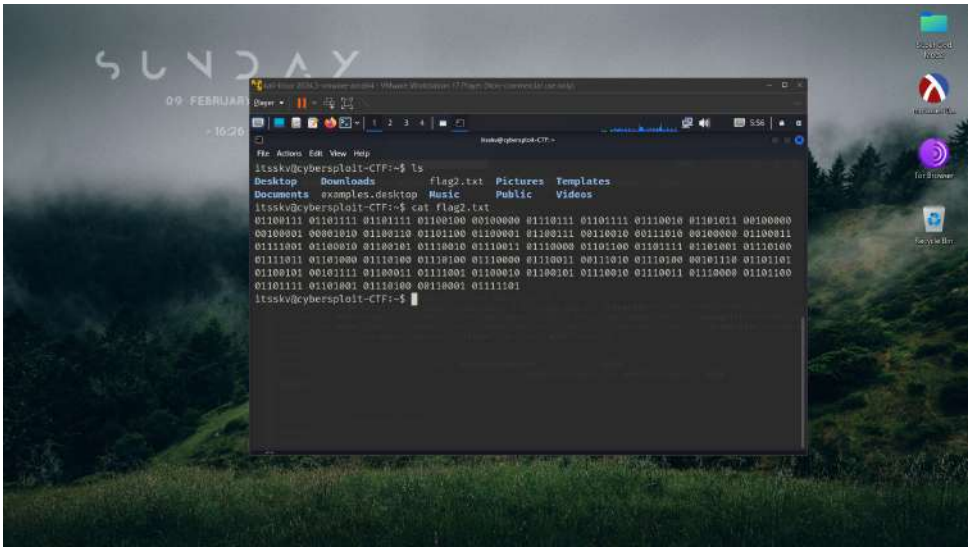

Figure 10: Upon listing the directory contents using *ls*, I discovered that there was a text file titled *flag2.txt*. Without ado, I inspected the contents of the file and found a binary code.

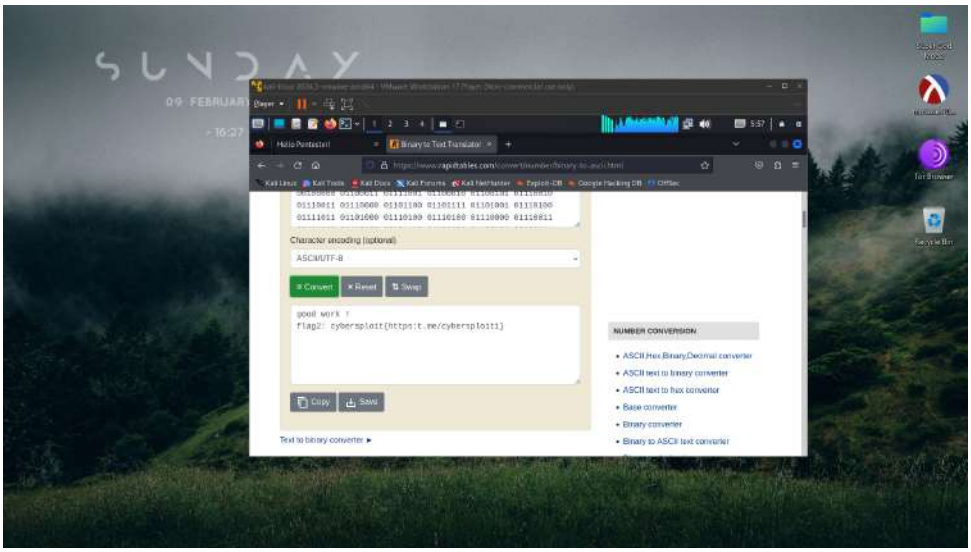

Figure 11: A simple binary to unicode conversion revealed the second flag: **cybersploit{https:t.me/cybersploit1}**. The website didn't do much but redirected me to a Telegram channel, so I dropped that line of thought and proceeded to think about alternatives to capture the final flag.

3 The Final Flag

Figure 12: As I was already logged into *itsskv*, I attempted to *cd* into the root directory. However, *itsskv* did not have root privileges, so I had to search for a vulnerability in the system. *uname -a* showed that the kernel version was 3.13.0.32-generic. A search in the Exploit-DB search engine yielded a privilege escalation exploit, *37292.c*, which I downloaded.

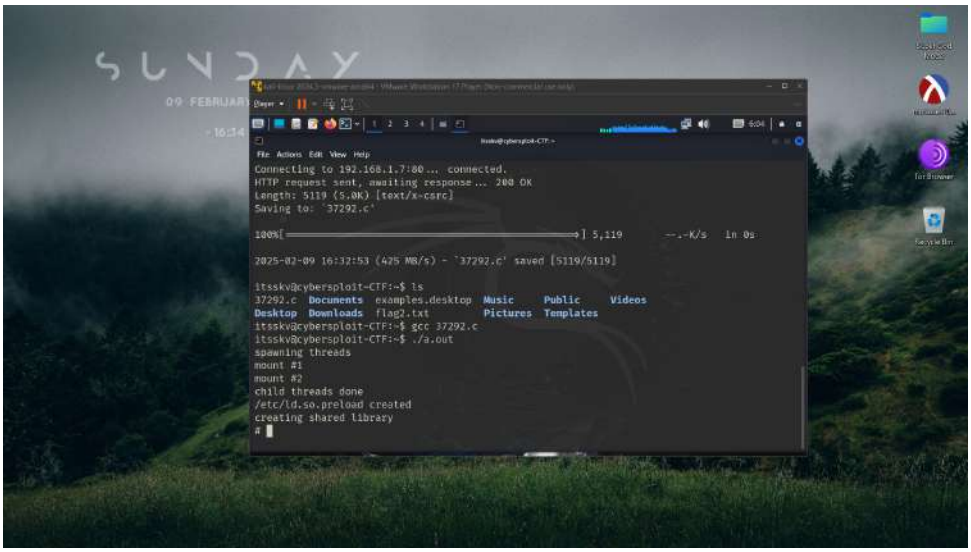

Figure 13: Hosting a simple HTTP server from the Kali Linux VM (*python -m http.server*) and running a simple *wget* from the SSH shell, I downloaded the C file. Using *gcc* to compile it, I ran the *a.out* executable and immediately gained root privileges.

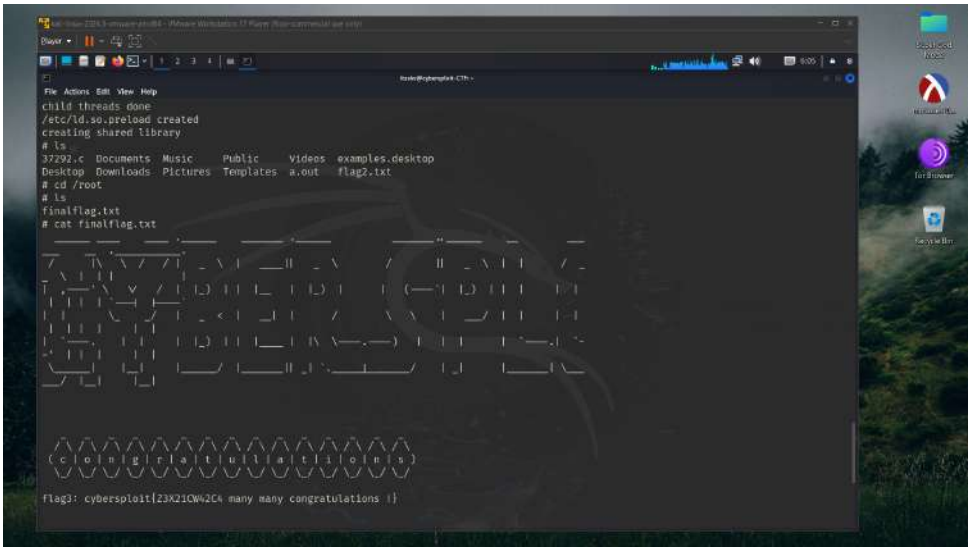

Figure 14: Now, I could *cd* into the root directory. There, I found a text file titled *finalflag.txt*, which revealed the third and final flag of the room: **cybersploit:{Z3X21CW42C4 many many congratulations !}**.