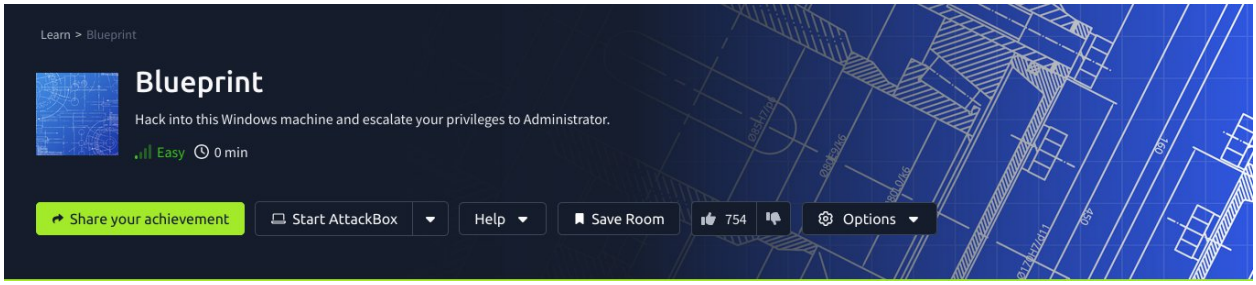
THM Blueprint Writeup



This room is called **Blueprint**, a THM CTF room. It is based on Windows machine privilege escalation. Here, I explain my experience regarding the vulnerabilities I discovered, how I gained shell access, and retrieved flags.

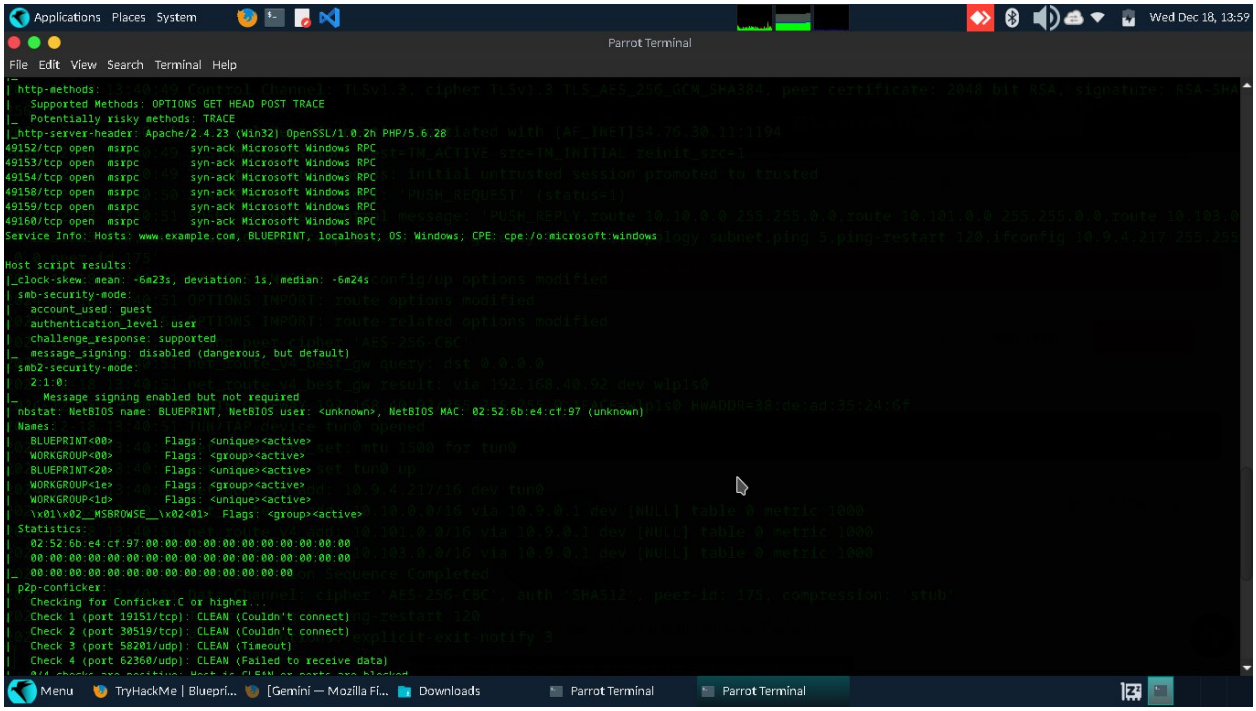
Active Reconnaissance with Nmap

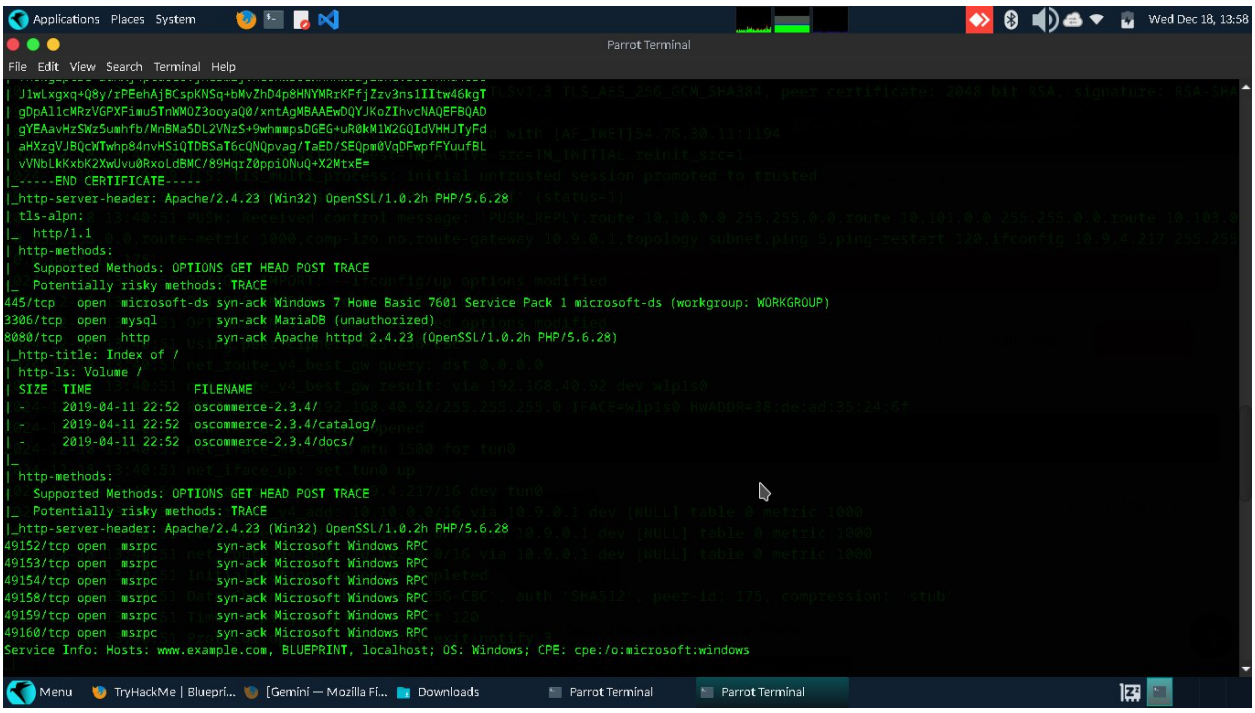
I started with active reconnaissance using the **Nmap** tool. There were several open ports on this machine, but I focused on enumerating the HTTP/HTTPS and SMB services.

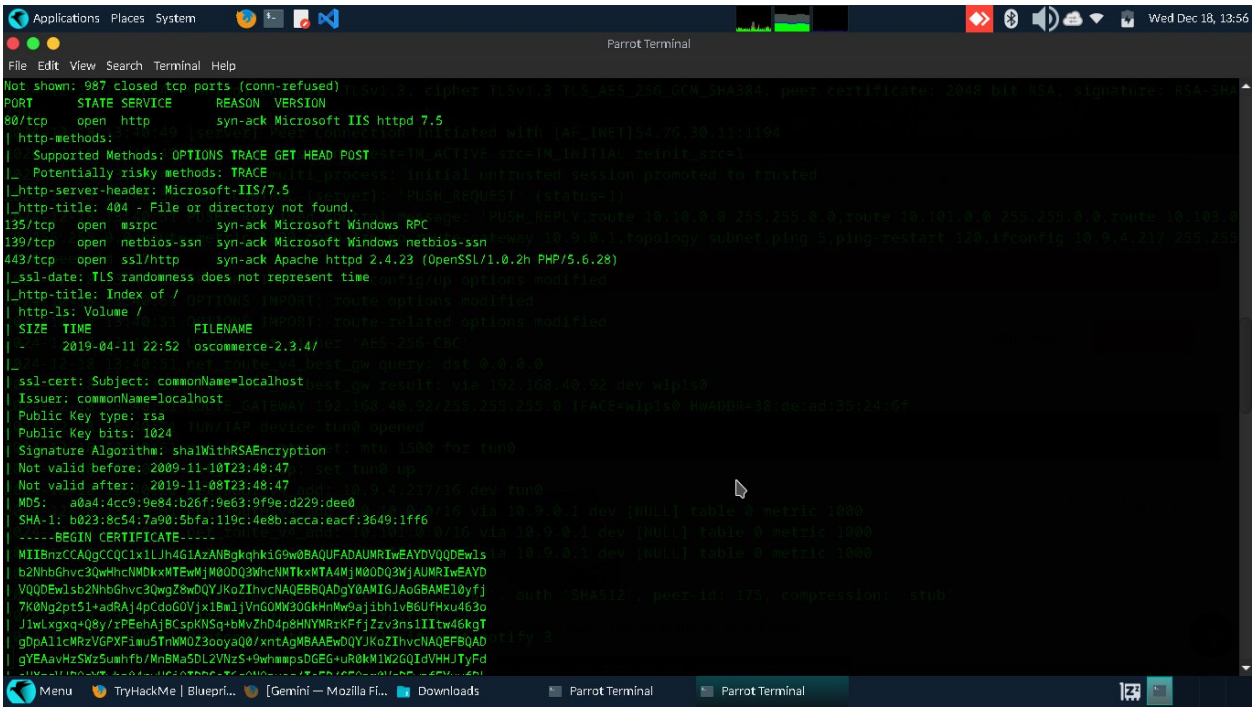
Command used:

```

**nmap –sC –sV –A  –T4 –vvv 10.10.21.130**

```

Proof of concept





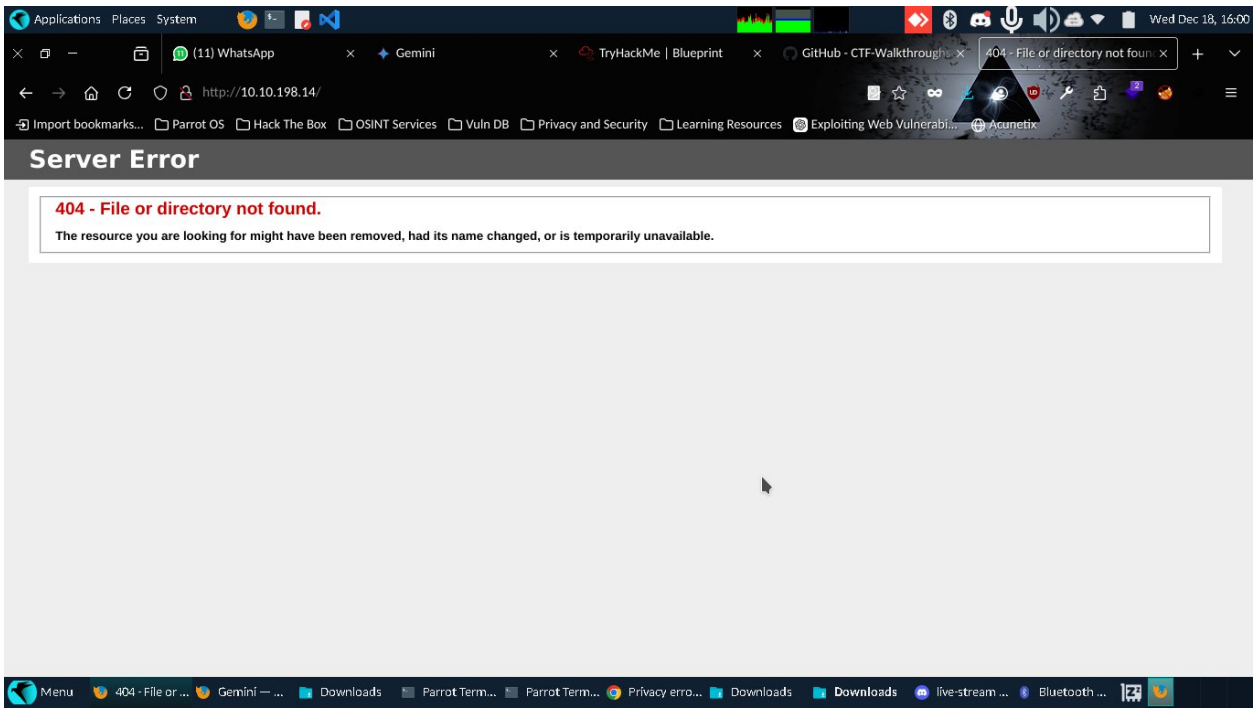


Port Scanning

1. **Port 80 (HTTP)**:

- I attempted to access port 80 but received a **404 Http-Status**.
- I also tried directory brute-forcing but didn't find any useful directories.

Proof of concept:



2. Port 139 (NetBIOS/SMB):

- Next, I enumerated port 139 using the **nbtscan** tool.
- Here, I obtained the Workgroup and Hostname.

3. SMB Enumeration:

- I proceeded with SMB enumeration using Nmap's smb-enum script.
- I discovered the following users: **Administrator**, **Guest**, and **Lab**.

4. Port 443 (HTTPS):

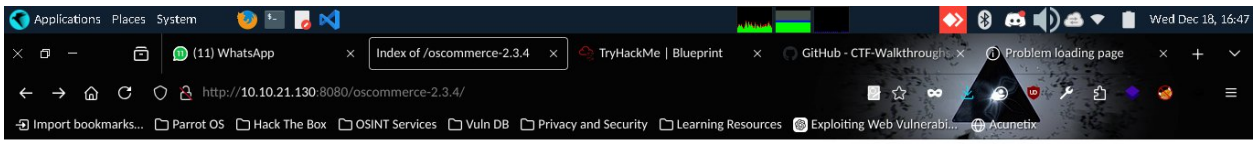
- I checked port 443 but received a bad response from the server.

5. Port 3306 (MySQL):

- When probing MySQL, I found that I didn't have permission for database access using default credentials.

6. Port 8080 (HTTP):

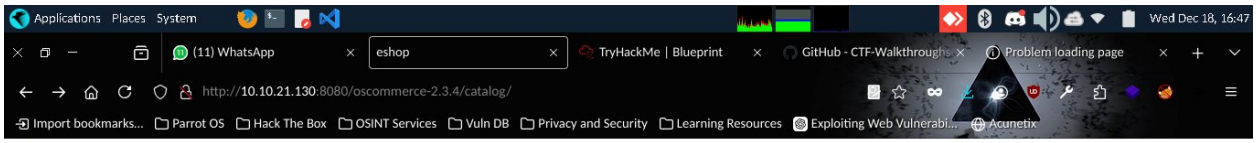
- The last port I explored was 8080, which was running an **osCommerce** service.
- Upon accessing this port, I found a directory page for **osCommerce-2.3.4**.



Index of /oscommerce-2.3.4

Name	Last modified	Size	Description
Parent Directory		-	
catalog/	2019-04-11 22:52	-	
docs/	2019-04-11 22:52	-	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.21.130 Port 8080



eshop
Cart ContentsCheckoutMy Account
Top » Catalog

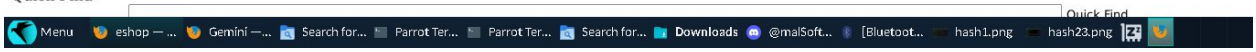
Welcome to eshop

Welcome Guest! Would you like to log yourself in? Or would you prefer to create an account?

New Products For December

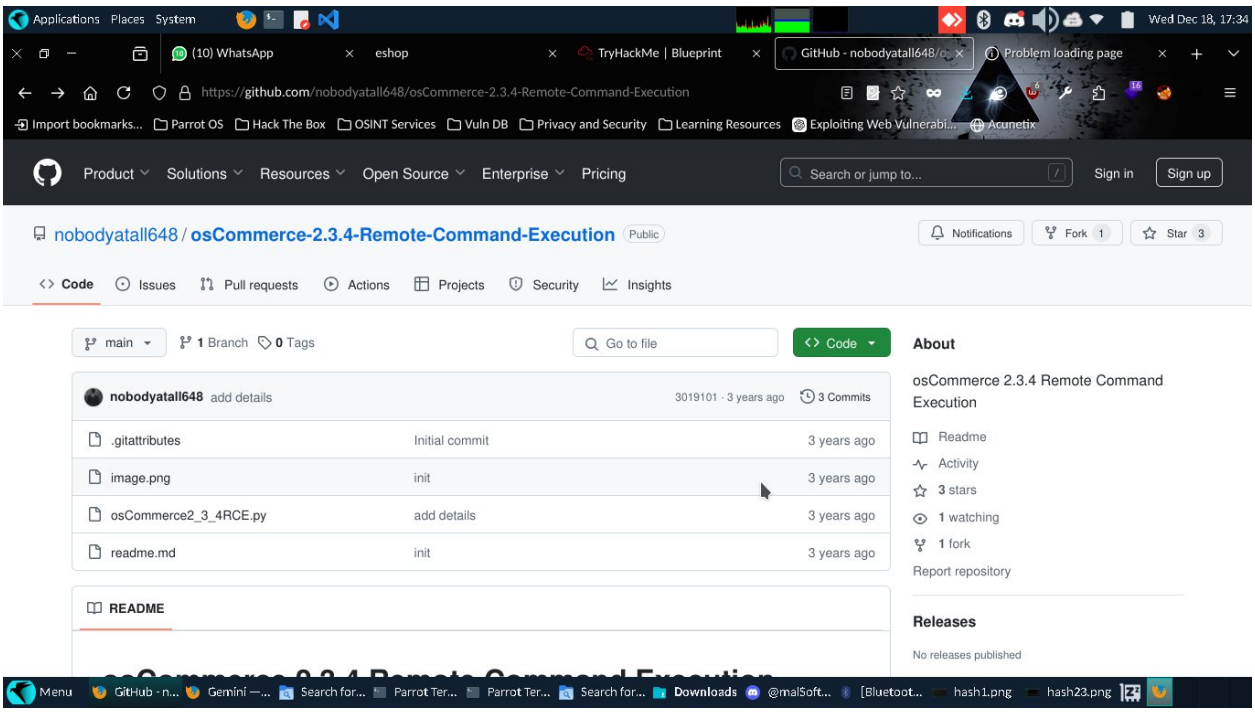
The Wheel Of Time The Wheel Of Time $99.99	Matrox G200 MMS Matrox G200 MMS $299.99	Samsung Galaxy Tab Samsung Galaxy Tab $749.99
Under Siege Under Siege $29.99	Red Corner Red Corner $32.00	Beloved Beloved $54.99
Blade Runner - Director's Cut Blade Runner - Director's Cut $30.00	Microsoft Internet Keyboard PS/2 Microsoft Internet Keyboard PS/2 $69.99	The Replacement Killers The Replacement Killers $42.00

Categories
Hardware-> (6)
Software-> (4)
DVD Movies-> (17)
Gadgets (1)
Manufacturers
Please Select
Quick Find
Quick Find



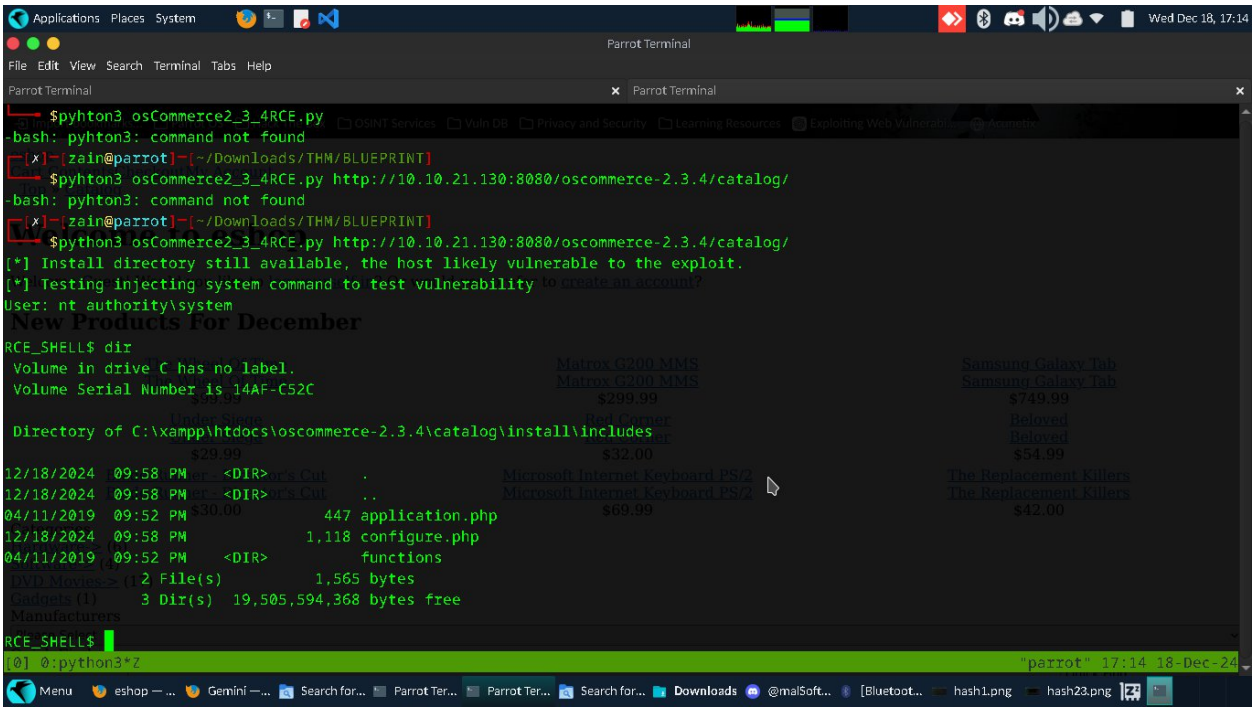
osCommerce Exploration

- After navigating to the **catalog/** directory, I observed an e-commerce site displaying products and their prices.
- I conducted research on **osCommerce vulnerabilities** form Github and found RCE (Remote Code Execution) scripts associated with this version.



Exploitation

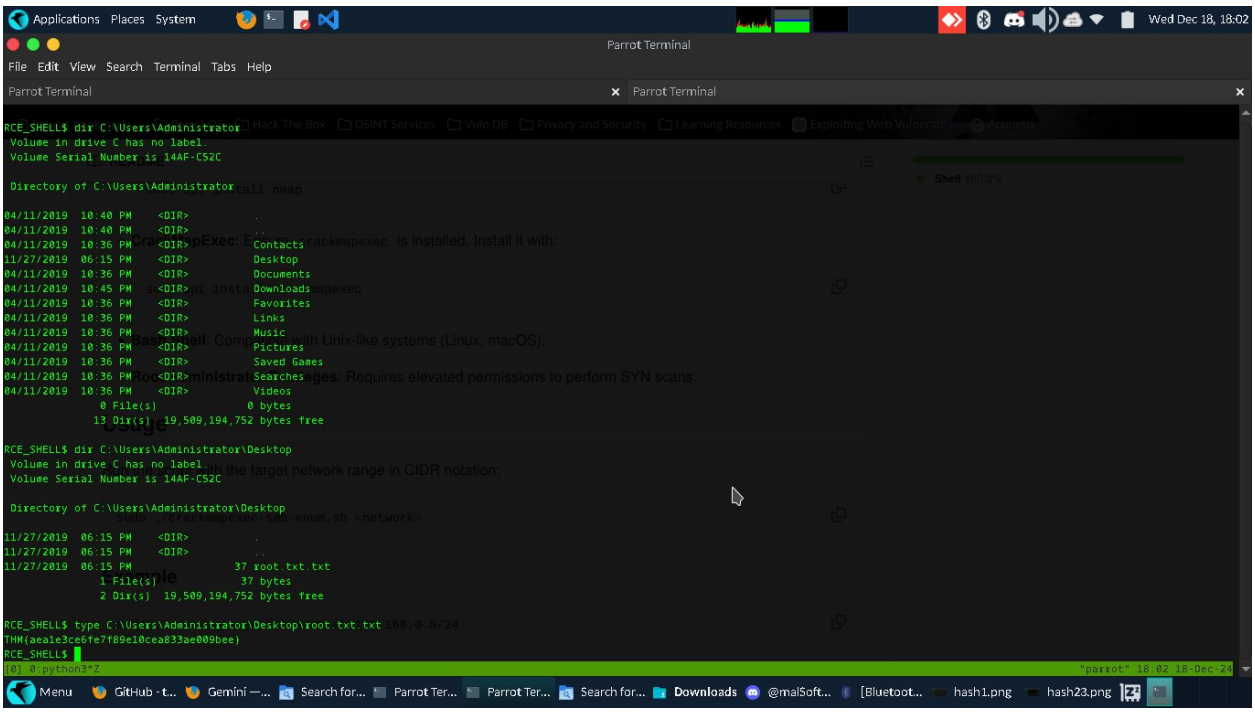
- I copied the latest Python exploit and executed it.
- I successfully gained shell access.



Privilege Escalation

In Windows, the **authority\system** account represents root privileges. After obtaining the remote shell, I searched the Administrator directory for the root flag.

- I retrieved the root flag.



NTLM Hash Decoding

Next, I needed to decode the NTLM hash for the Lab user.

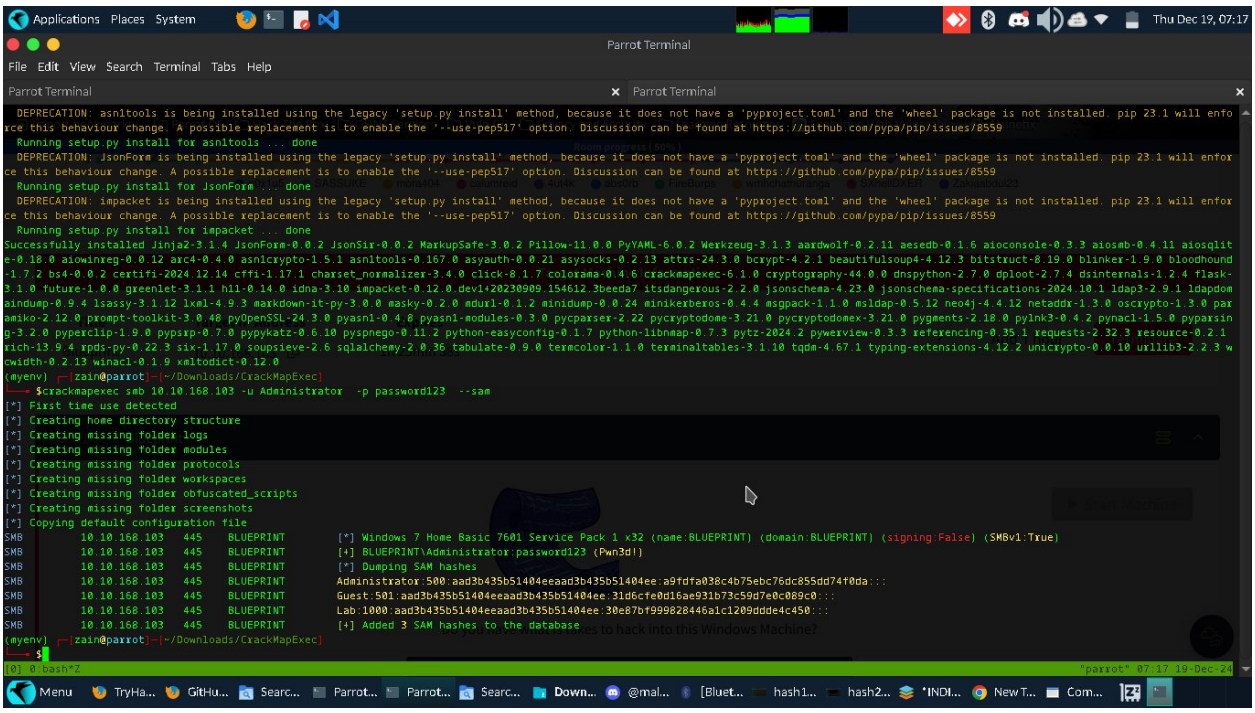
Hash Extraction

- The NTLM hashes are stored in a binary format in the Windows registry files located in `System32/config/` with names **SAM**, **SECURITY**, **SYSTEM**, and **Default**.
- I used **CrackMapExec** to extract these files and copied them to my local machine.

Hash Dumping

To extract the hash values, I used **CrackMapExec**, a reliable tool for hash dumping.

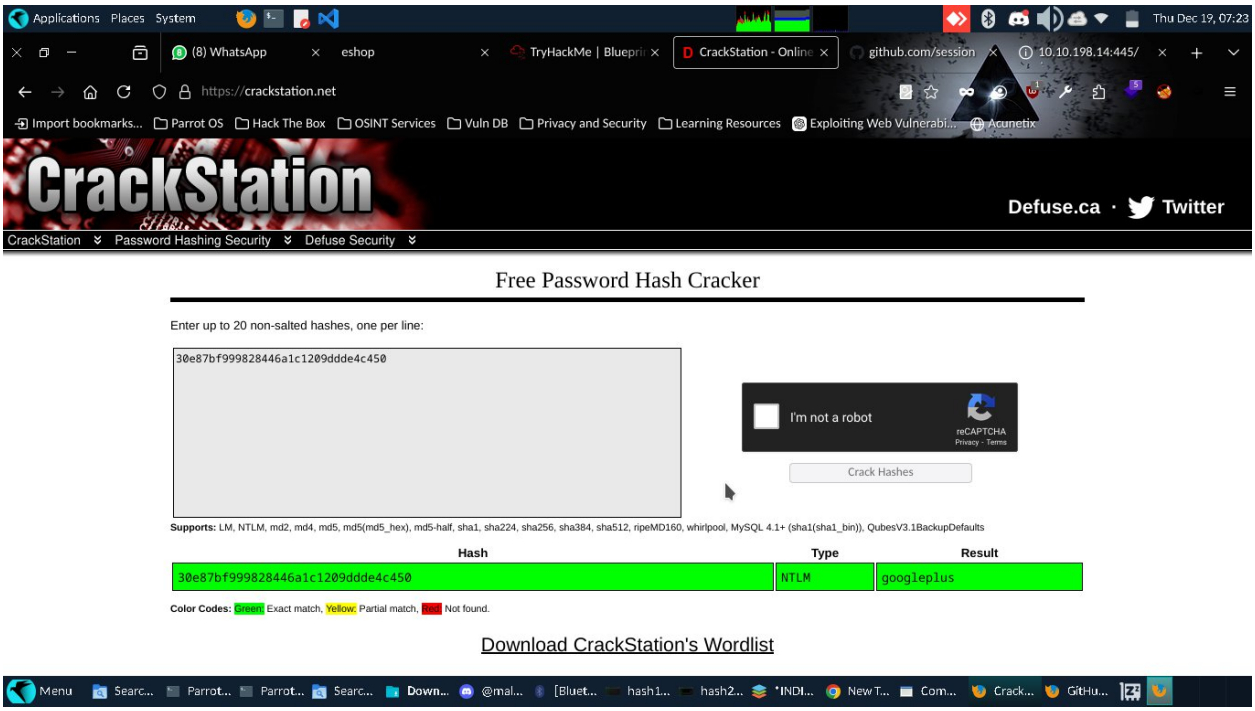
- I successfully dumped the hashes for all three users, where the first hash is the LM hash code, and the second (after the ":") is the NT hash code.



Hash Cracking

I took the LM code for the Lab user and decoded it using **CrackStation**. You can also use offline tools like **JohnTheRipper** or **Hashcat** for this purpose.

- After decoding, I obtained the Lab user's password.



Conclusion

In this write-up, I detailed my journey through the **Blueprint** room on TryHackMe, focusing on the various stages of exploitation and privilege escalation within a Windows environment.