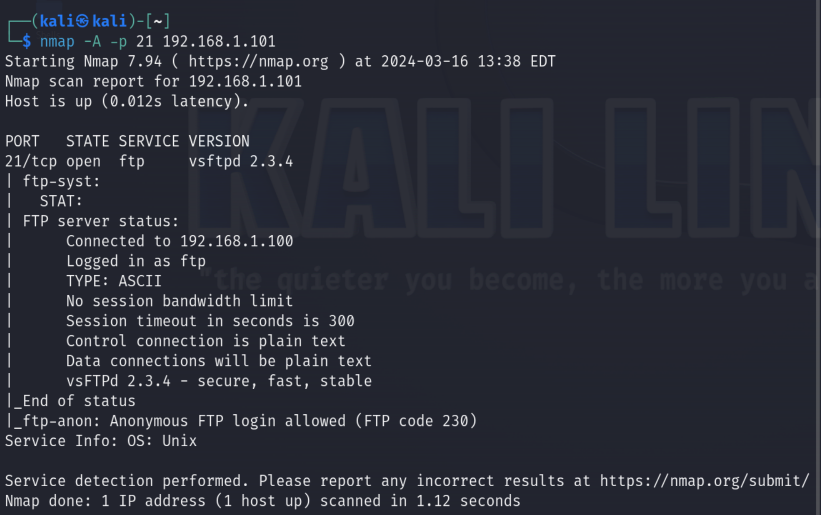
# Network Penetration Testing

## 1. Exploiting a vulnerable service on a Linux system

**Step 1:** Power on both the Kali Linux and the Metasploitable VMs and make sure they are connected to PFSense.

**Step 2:** Use Nmap to determine if there is an available FTP port.



**Step 3:** Research the vulnerabilities with VSFTPD 2.3.4 (the FTP version running).

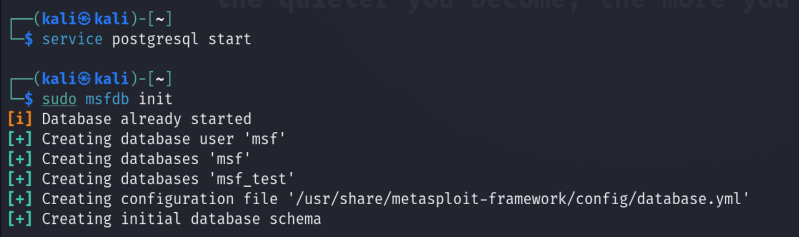
There appear to be several sites containing exploits, this site contains a Python exploit: <https://www.exploit-db.com/exploits/49757>

Here is the following information about the code exploit discovered:

* Exploit Title: VSFTPD 2.3.4 - Backdoor Command Execution
* Date: 9-04-2021
* Exploit Author: HerculesRD
* Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
* Version: VSFTPD 2.3.4
* Tested on: Debian
* CVE: CVE-2011-2523

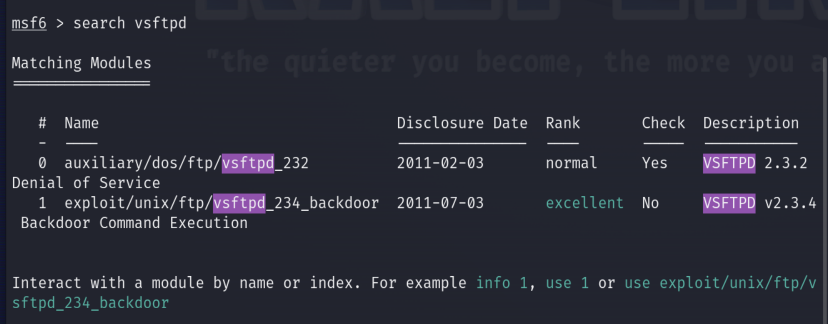
Instead of using the online option, we will use Rapid 7’s testing framework “Metasploit”.

**Step 4:** Initalize and begin running Rapid 7’s Metasploit.

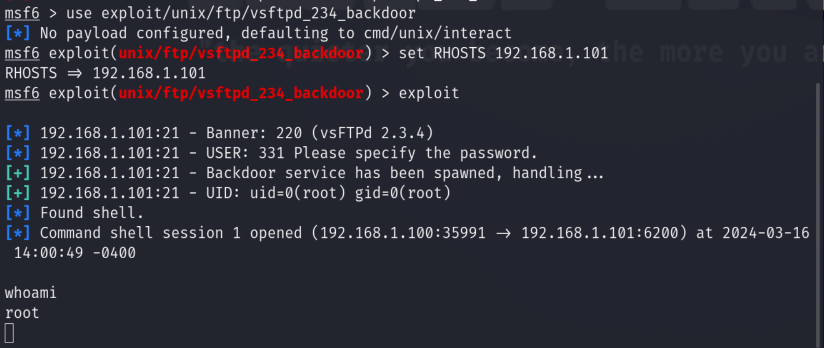




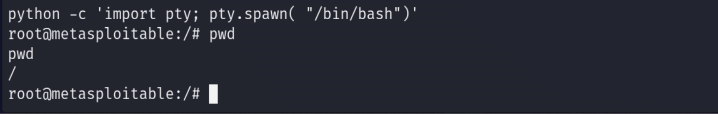
**Step 5:** Use the search command in Metasploit to find vsftpd-related models.



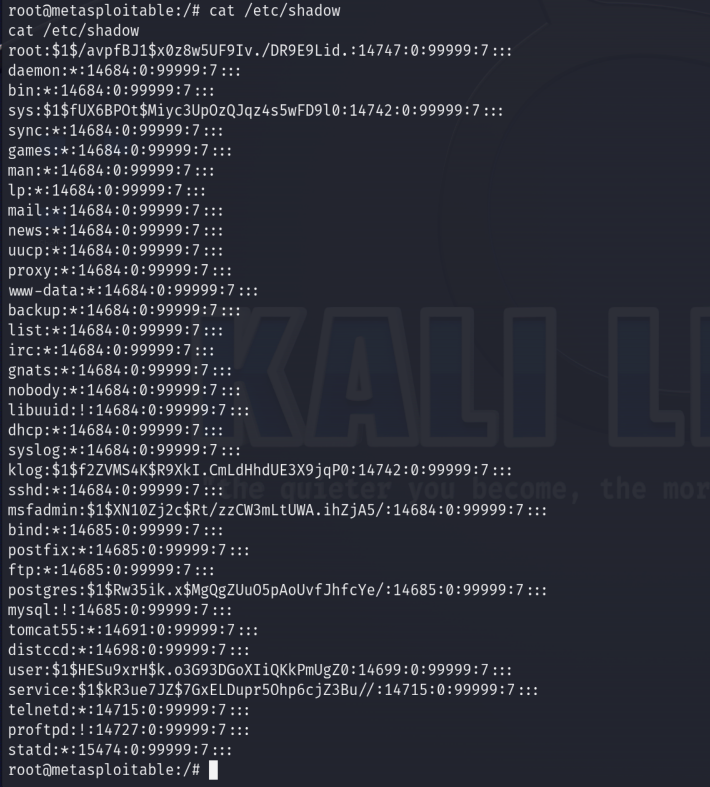
**Step 6:** Set the remote target's IP address (192.168.1.101), and launch the exploit.



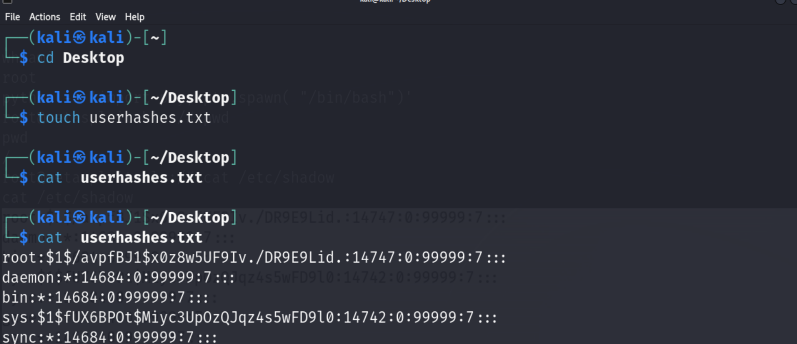
**Step 7:** Spawn the pseudo-bash terminal.



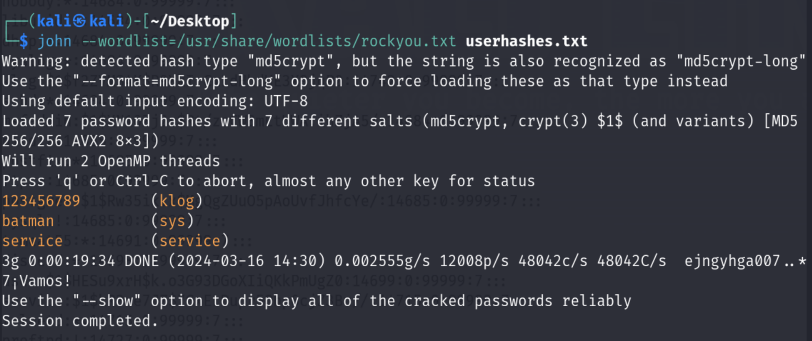
**Step 8:** Examine the /etc/shadow file to see usernames and hashes.



**Step 9:** Copy usernames and hashes into a text file to crack the hashes.



**Step 10:** Use John the Ripper for password cracking on the password hashes. This uses a dictionary-based attack with the rockyou.txt wordlist.

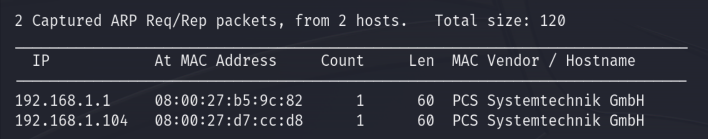


## 

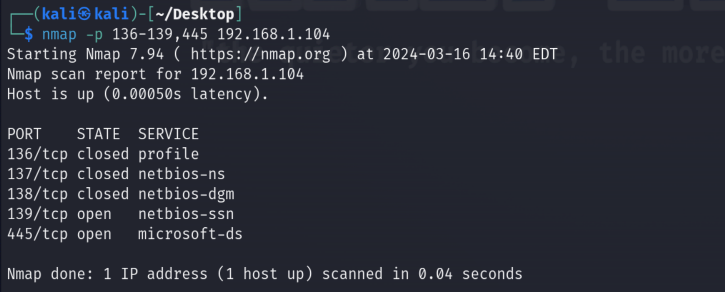
## 2. Exploiting SMB in Microsoft Windows

### A. ExternalBlue

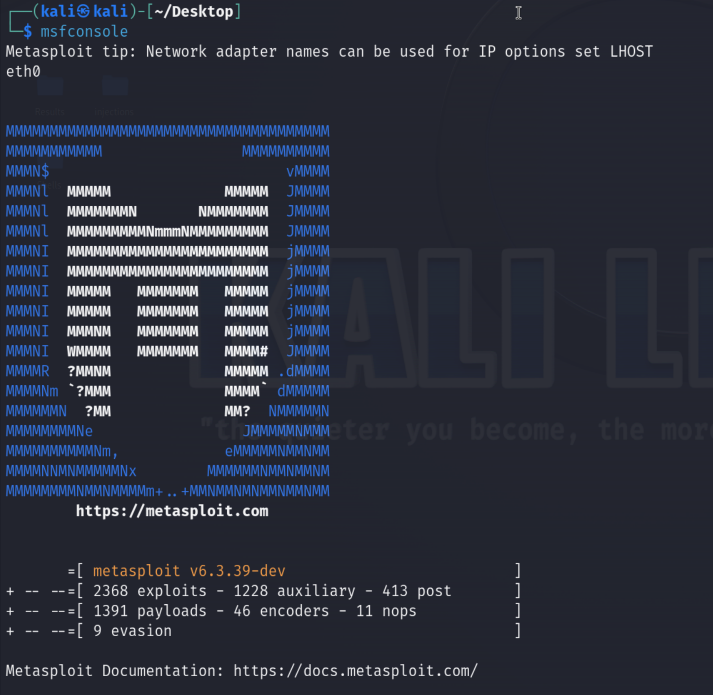
**Step 1:** Power on both the Kali Linux and the Metasploitable 3 VMs and make sure they are connected to PFSense.



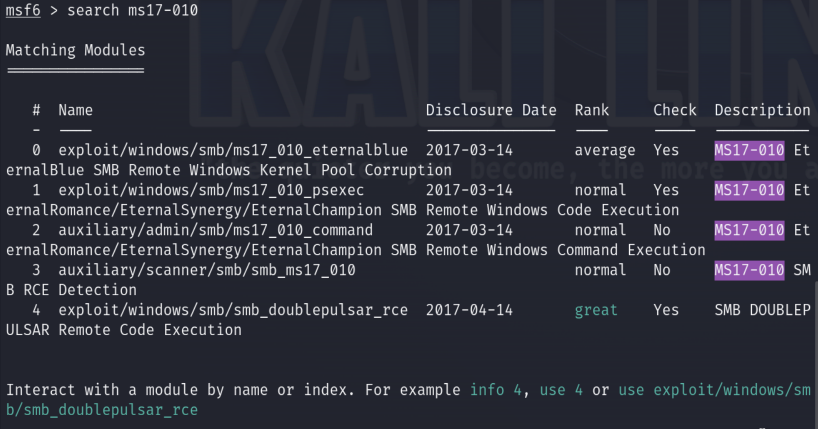
**Step 2:** Use Nmap to discover whether service ports 136, 137, 138, 139, and 445 are open on Metasploitable 3.



**Step 3:** Start Metasploit on Kali Linux.

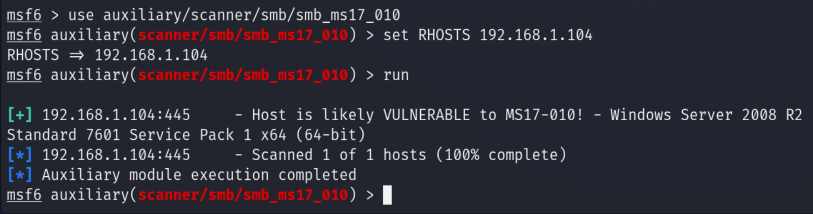


**Step 4:** Search for any relatable modules.

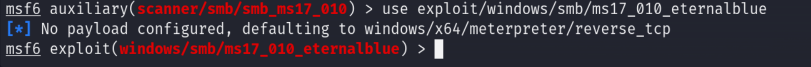


**Step 5:** Use the auxiliary scanner module to determine whether the target is vulnerable

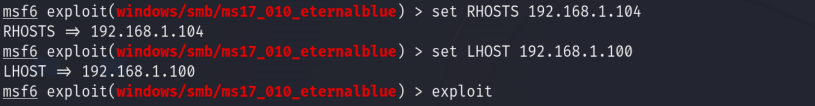
to EternalBlue.



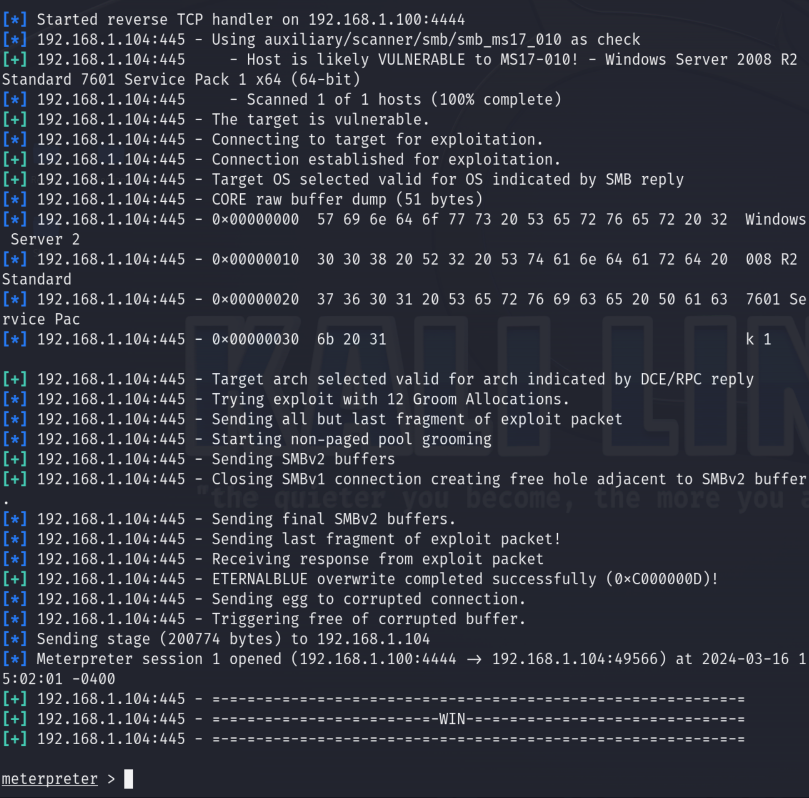
**Step 6:** Use an exploit that was discovered in step 4.



**Step 7:** Set RHOSTS (target), LHOST (Kali Linux), and launch the attack.



Output:



**Step 8:** Use the hashdump command within your Meterpreter shell to dump the contents of the Security Account Manager (SAM) file.

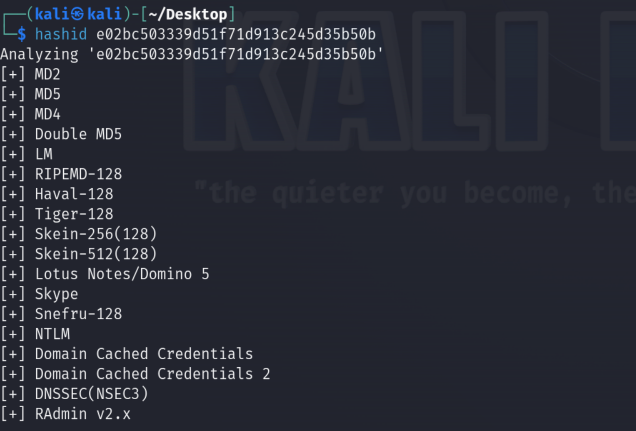


**Step 9:** Save the entire output. (Additional password cracking in the next section.)

**Step 10:** Save the Administrator account detailsfor the Passing the hash section.

Administrator:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b

**Step 11:** Identify the hash types.



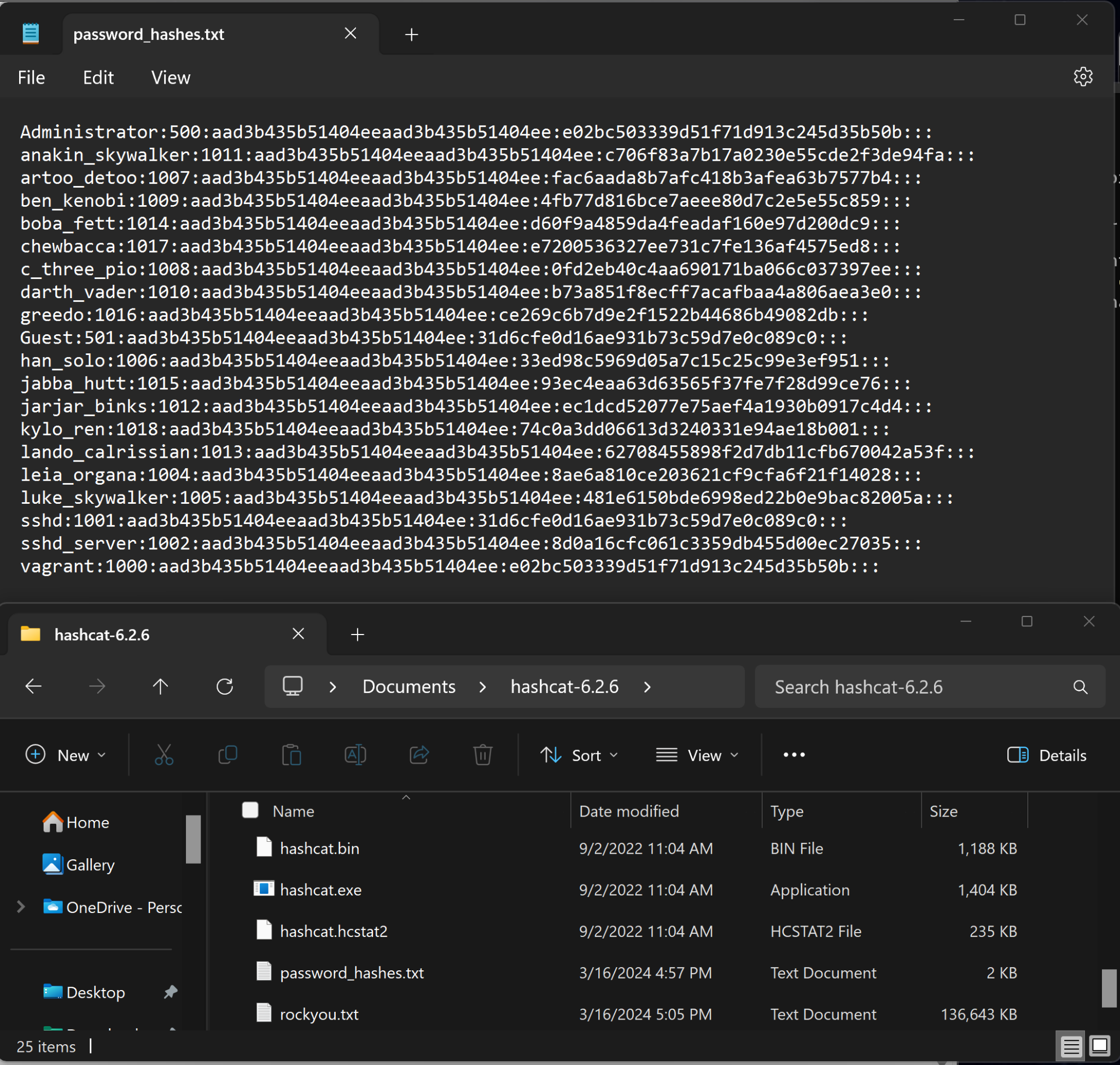
### B. Cracking Passwords

**Step 1:** Download Hashcat on the host Windows operating system. Go to https://hashcat.net/hashcat/ and download the Hashcat binaries file.

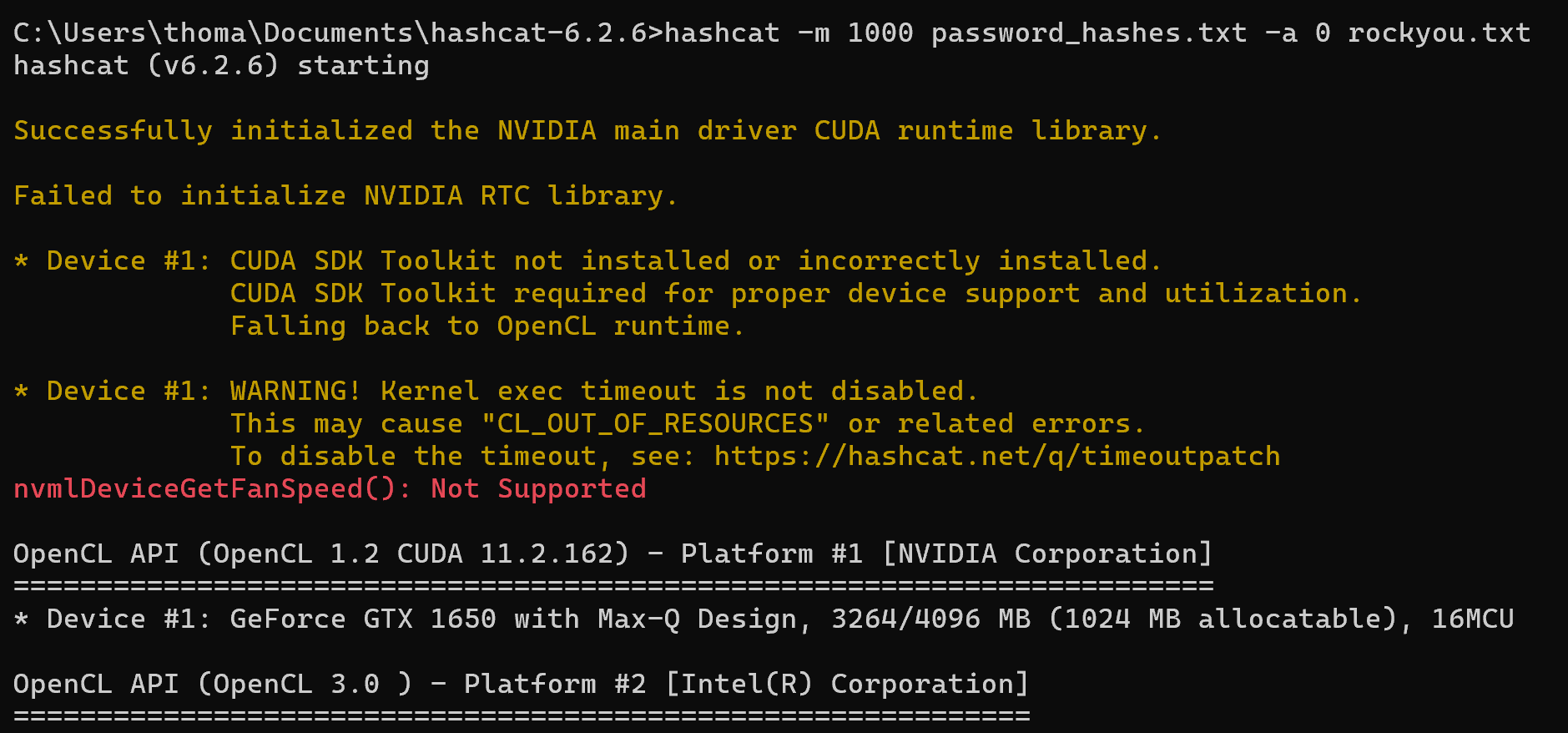
**Step 2:** Once the download is complete, use an unzipping tool to extract the files.

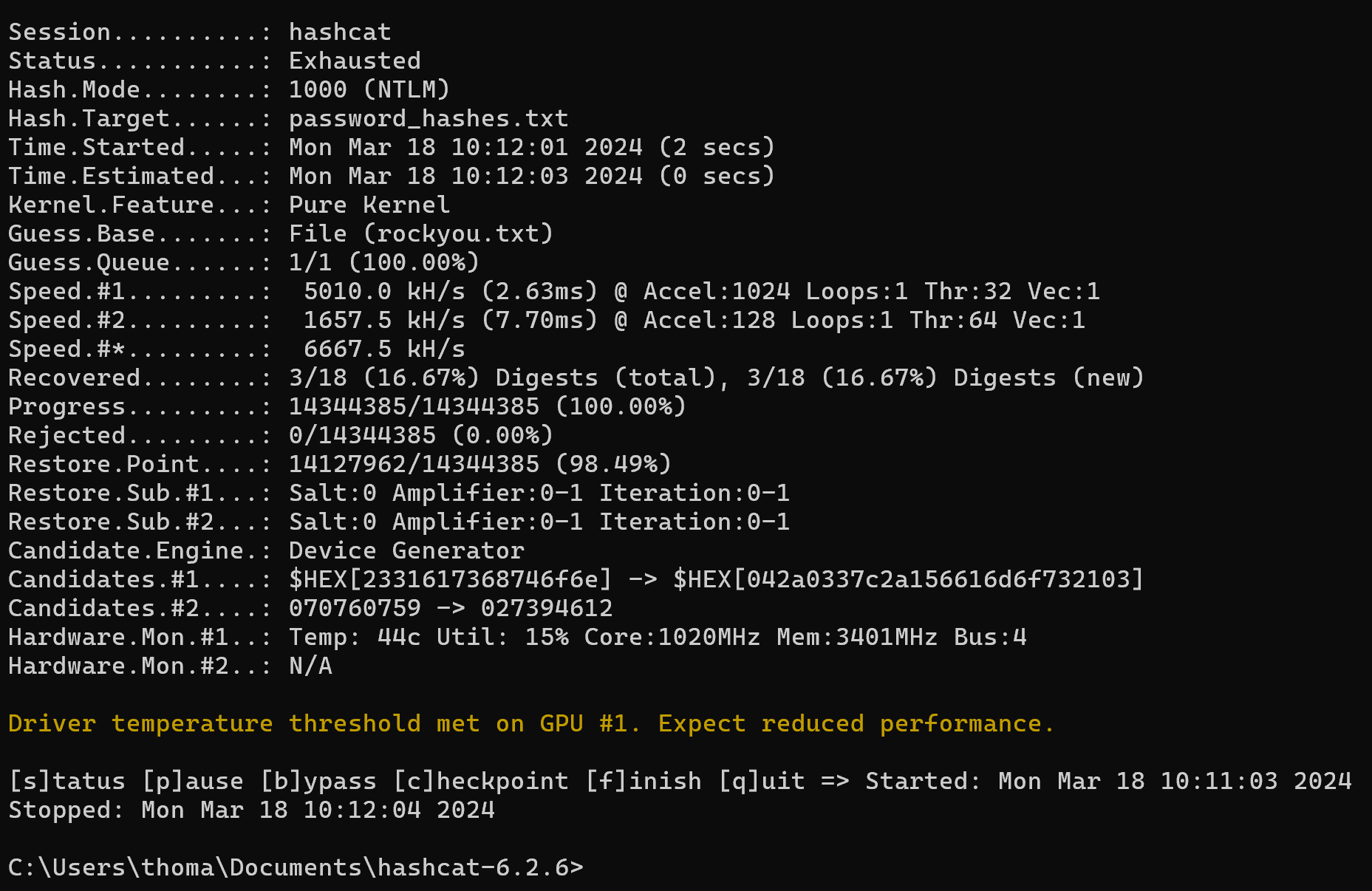
**Step 3:** Open your Windows Command Prompt and change your working directory to the extracted Hashcat folder.



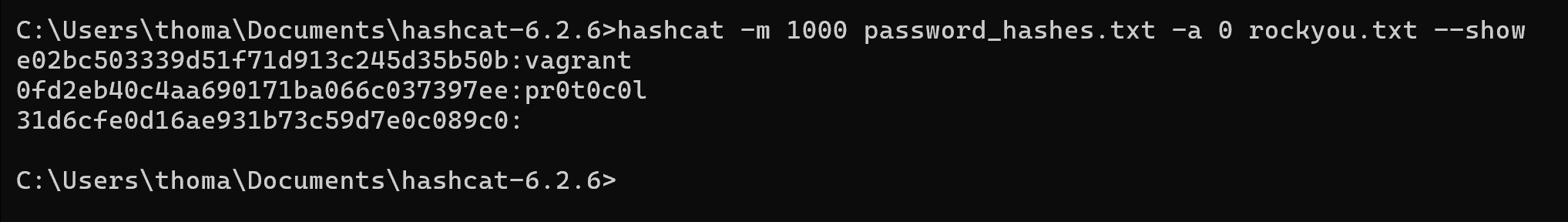
**Step 4:** Copy both the password\_hashes.txt file and the rockyou.txt wordlist from Kali into the Hashcat folder within Windows. ****

**Step 5:** Use Hashcat to find the values of the hashes.





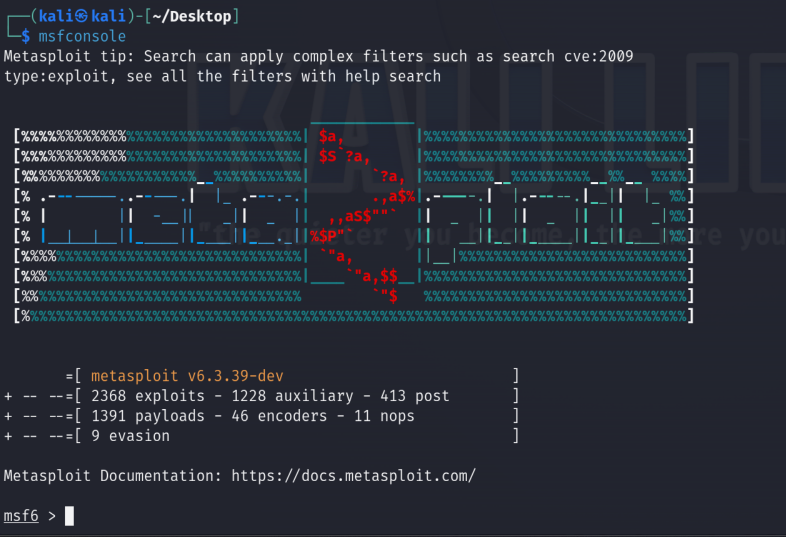
**Step 6:** Append the --show command to the end of the syntax in step 5 to view the hashes and their corresponding passwords.



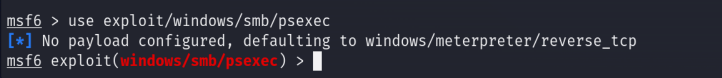
### C. Getting a Shell

**Step 1:** Power on both the Kali Linux and the Metasploitable 3 VMs and make sure they are connected to PFSense.

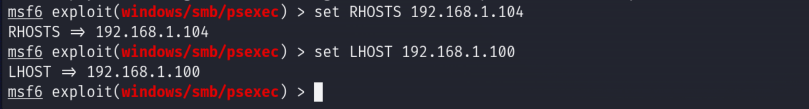
**Step 2:** On Kali, open the Terminal and start the Metasploit exploitation evelopment framework.



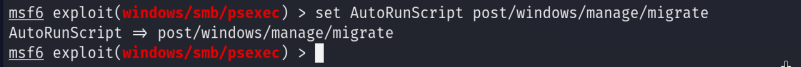
**Step 3:** Select the SMB PsExec exploit module.



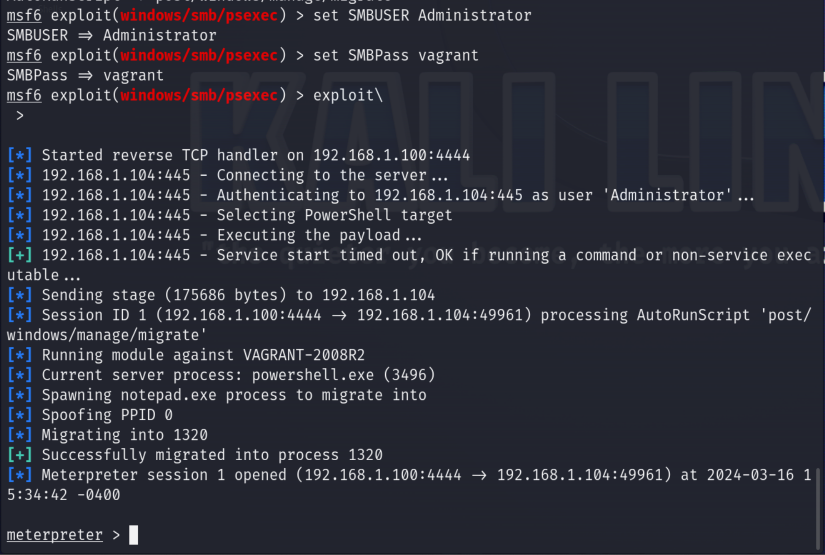
**Step 4:** Set the RHOSTS (Metasploitable 3) and LHOST (Kali Linux) machine addresses.



**Step 5:** Use AutoRunScript to automatically execute a post-exploitation payload to migrate the process of the malicious code that will be running on the target system when it's exploited.



**Step 6:** Using the options command, you will see that the SMBUSER and SMBPass parameters are needed.



**Step 7:** Use Windows-based shell commands.

