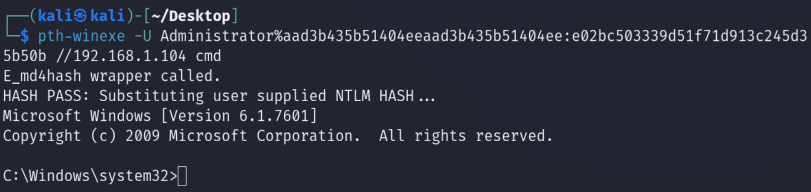
# Network Penetration Testing

## 3. Pass the Hash

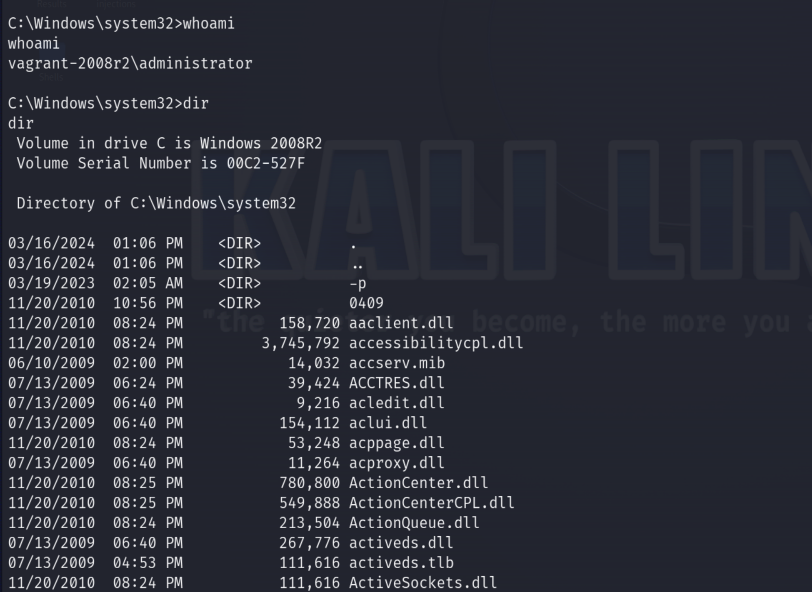
### A. Getting a Shell with PTH-WinExe

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

**Step 2:** Gain access to the Windows Command Prompt shell on our Kali Linux machine by passing the hashes of the Administrator account.



**Step 3:** Run Windows-based commands from the Kali terminal.



### B. Using Impacket

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

**Step 2:** Gain access to the Windows Command Prompt shell on our Kali Linux machine by passing the hashes of the Administrator account.



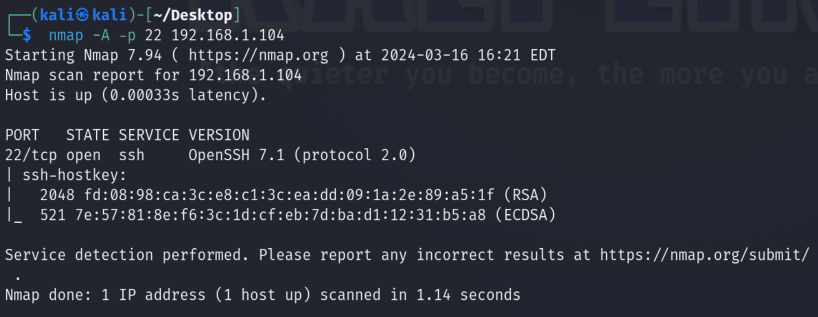
**Step 3:** Run Windows-based commands from the Kali terminal.



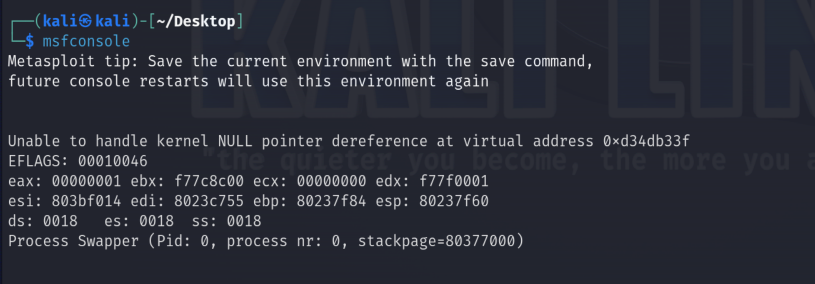
## 4. Gaining Access by Exploiting SSH

**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 do a port scan to determine whether SSH is running on port 22.



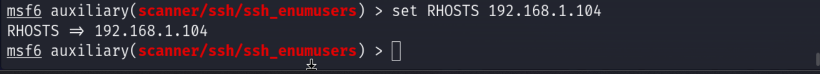
**Step 3:** Start the Metasploit exploitation dev. framework for the SSH user enumeration.



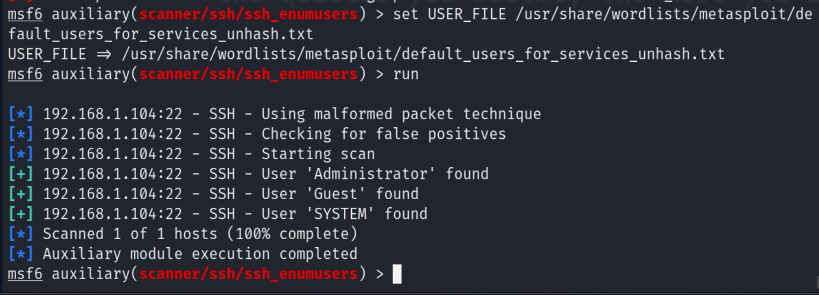
**Step 4:** Invoke the SSH user enumeration module.



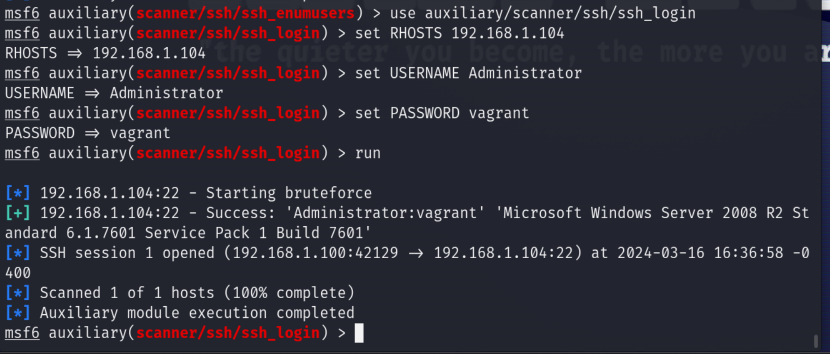
**Step 5:** Set the target's address.



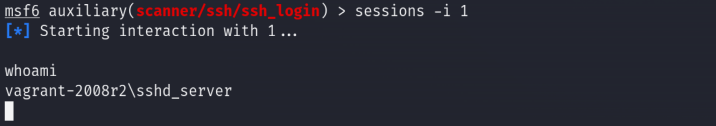
**Step 6:** Set the wordlist that contains a list of possible usernames and run the module.



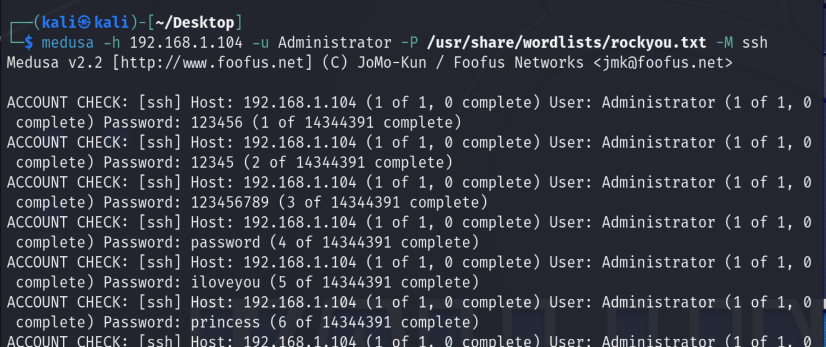
**Step 7:** Use the SSH login module to attempt to login using the Administrator’s credentials already discovered.



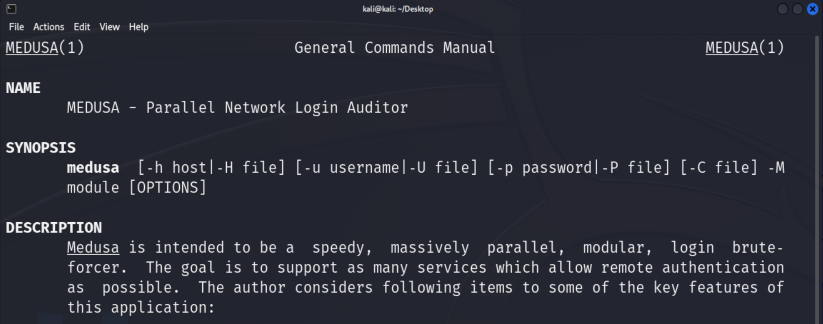
**Step 8:** Use the sessions command to see a list of active sessions and their corresponding IDs. Use -i to interact with a particular session (or foreground it).



**Step 9:** Use Medusa to gain access to the target using SSH.



Man medusa command:



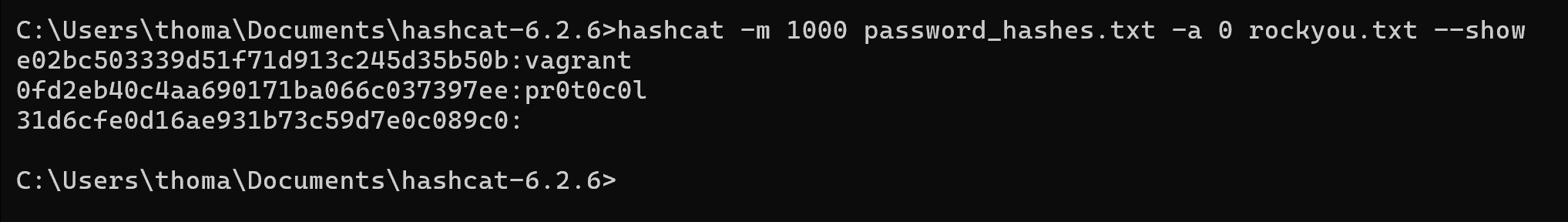
# Exercises

## Exercise 1:

**Question 1:** What username and password correspond to the NTLM hash 0fd2eb40c4aa690171ba066c037397ee?

* :pr0t0c0l

**Question 2:** How many NTLM hashes was Hashcat able to crack? Provide the usernames and corresponding passwords, if any.

Hashcat was able to crack 3.

Here are the rest I was able to find:

* 0fd2eb40c4aa690171ba066c037397ee:pr0t0c0l
* 31d6cfe0d16ae931b73c59d7e0c089c0:
* 62708455898f2d7db11cfb670042a53f:b@ckstab
* e02bc503339d51f71d913c245d35b50b:vagrant
* e7200536327ee731c7fe136af4575ed8:rwaaaaawr5
* 33ed98c5969d05a7c15c25c99e3ef951:sh00t-first
* 481e6150bde6998ed22b0e9bac82005a:use\_the\_f0rce
* 4fb77d816bce7aeee80d7c2e5e55c859:thats\_no\_moon
* 74c0a3dd06613d3240331e94ae18b001:daddy\_issues1
* 8d0a16cfc061c3359db455d00ec27035:D@rj33l1ng
* b73a851f8ecff7acafbaa4a806aea3e0:d@rk\_sid3
* c706f83a7b17a0230e55cde2f3de94fa:yipp33!!
* ce269c6b7d9e2f1522b44686b49082db:hanShotFirst!
* d60f9a4859da4feadaf160e97d200dc9:mandalorian1
* ec1dcd52077e75aef4a1930b0917c4d4:mesah\_p@ssw0rd
* fac6aada8b7afc418b3afea63b7577b4:beep\_b00p
* 8ae6a810ce203621cf9cfa6f21f14028:help\_me\_obiw@n
* 93ec4eaa63d63565f37fe7f28d99ce76:not-a-slug12

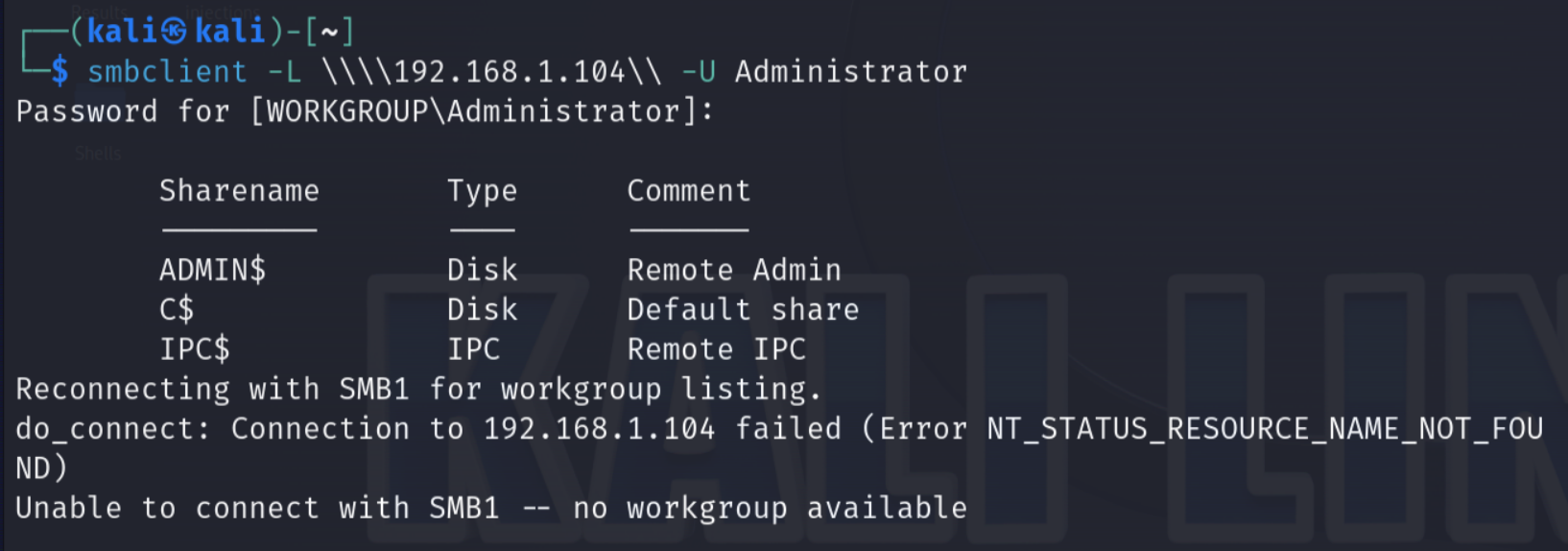
## Exercise 2:

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

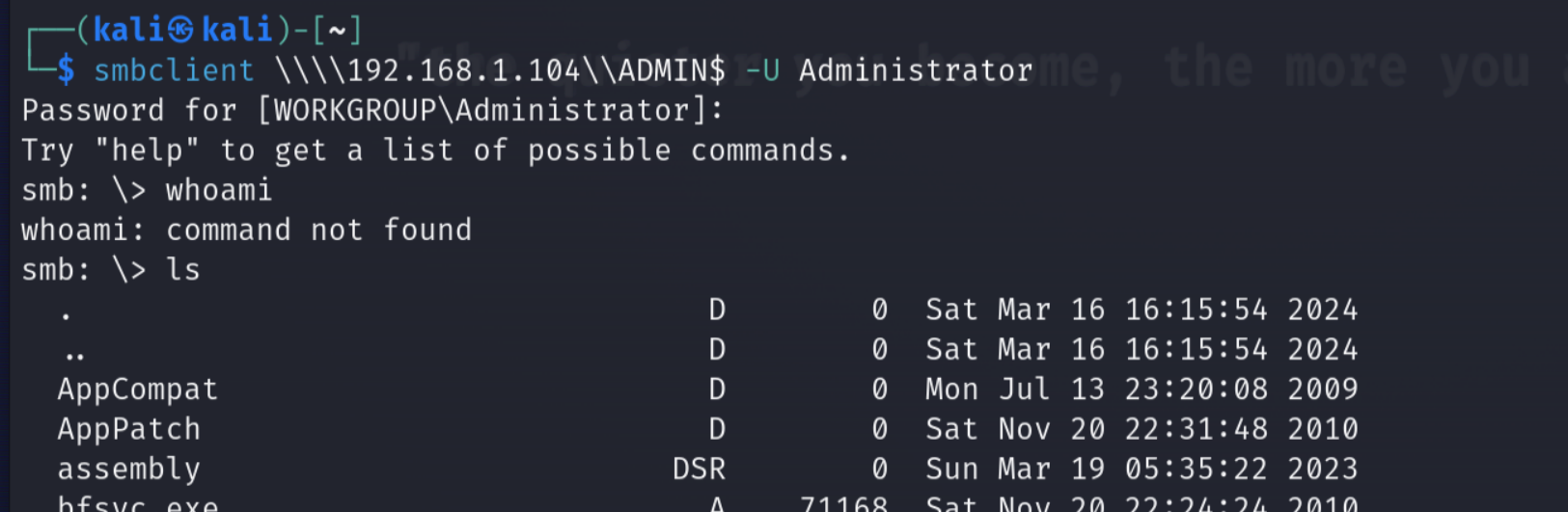
**Step 2:** Use the following SMBclient command to list the remote file shares exposed on

Metasploitable 3 using the identity of the Administrator user

**Step 3:**

****

**Step 4:** Explore the interesting files Sharename files. (ADMIN$ and C$ because these are both Disks.)

****

**ADMIN$ has the following XML files:**

diagerr.xml A 1908 Sun Mar 19 05:04:59 2023

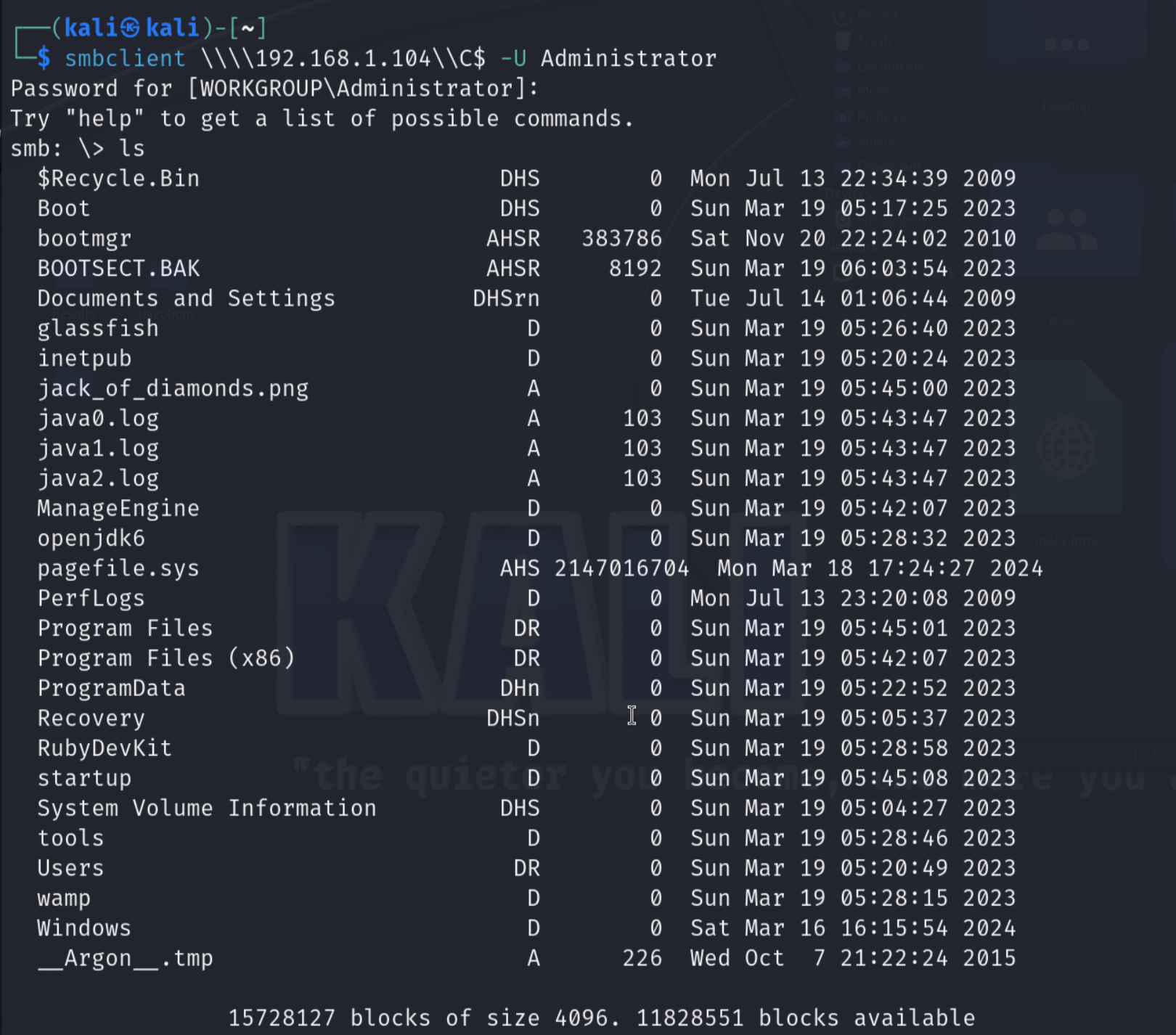
diagwrn.xml A 1908 Sun Mar 19 05:04:59 2023

ServerStandard.xml A 73429 Wed Jun 10 16:31:01 2009

ServerWeb.xml A 73395 Wed Jun 10 16:31:01 2009

**C$ did not have .xml files in the main directory.**

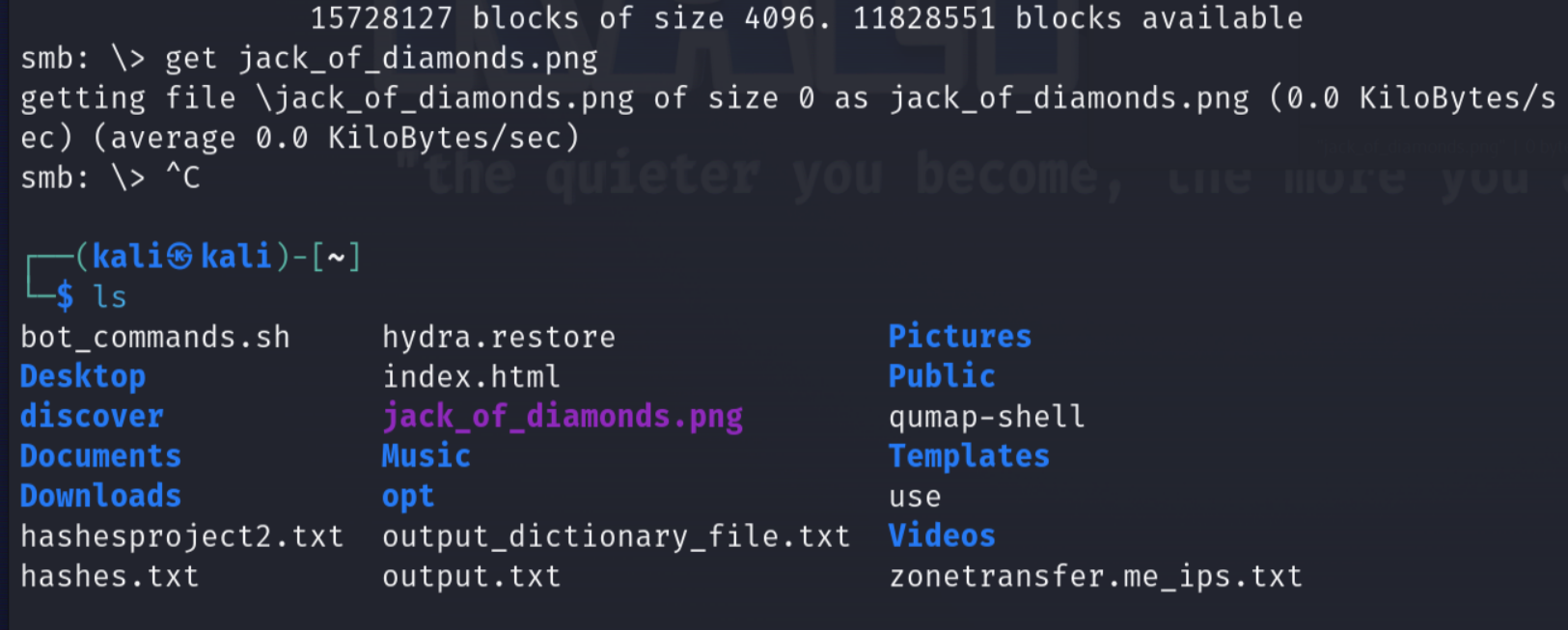
**Step 5:** Connect to C$ and use the ls command to look at the files. Are there any image files?



One image found:

jack\_of\_diamonds.png A 0 Sun Mar 19 05:45:00 2023

**Step 6:** Use the get command to download the file. Open and say what was listed.



Finding: The file jack\_of\_diamonds.png was empty.