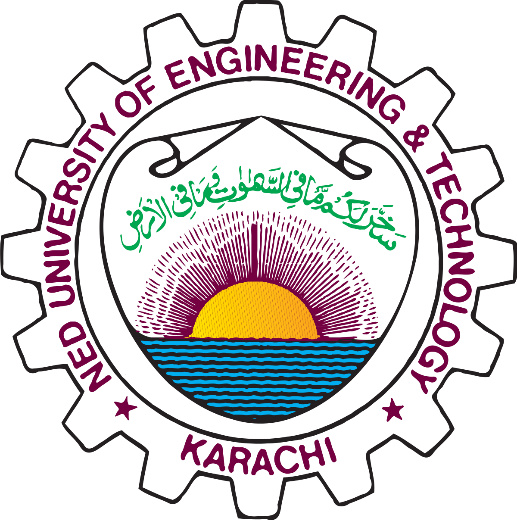
**CT-541 – NETWORK SECURITY**MS-IS 004 2019/20– Evening Fall 2019

**CT-541 NS Assignment-01**

**ARP Spoofing, DoS , Redirection**



**STUDENT NAME: MUHAMMAD UMAR TARIQ**

**STUDENT ID: IS 004 2019/20**

**COURSE INSTRUCTOR: Dr. Mubashir M Khan**

**DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY**

**NED UNIVERSITY, KARACHI CAMPUS**

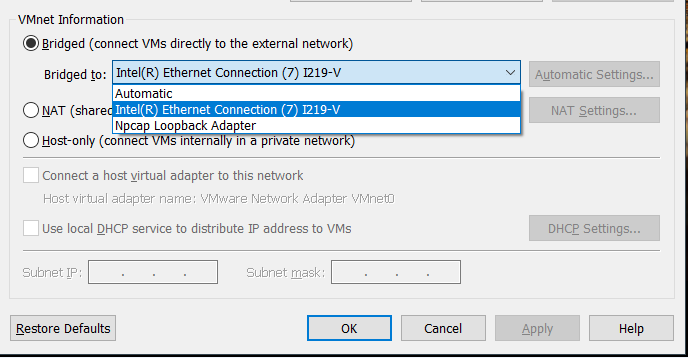
**Virtual Machines:**

1. **VM1:** Ubuntu 20.04 LTS 64 Bit **[Attacker, Bridged Networking Mode]**
2. **VM2:** Ubuntu 20.04 LTS 64 Bit [**Victim1, Bridged Networking Mode**]
3. **VM3:** Ubuntu 20.04 LTS 64 Bit [**Victim2, Bridged Networking Mode**]

**Tools Used For ARP Spoofing:**

1. **Ettercap**: [**https://www.ettercap-project.org/**](https://www.ettercap-project.org/)
2. **Tcpdump:** for capturing network traffic
3. **Wireshark:** for capturing network traffic

**Virtual Network Editor Configuration:**



**After Configuring Bridged Networking on All Three Virtual Machines**



**VM1 - Attacker Network Info:**

IP = 192.168.100.127

MAC = 00:0c:29:70:95:04

**VM2 – Victim Virtual Machine 1**:

IP = 192.168.100.128

MAC = 00:0C:29:9B:95:B5

**VM3 – Victim Virtual Machine 2**:

IP = 192.168.100.129

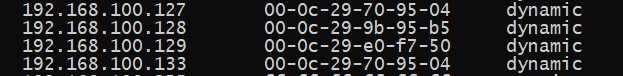
MAC = 00:0C:29:E0:F7:50

Arp table with only 3 Virtual Machines :

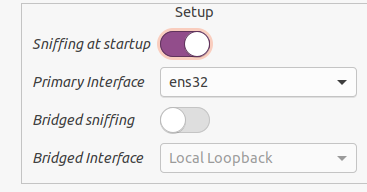


ARP Table with unused IP of network added (Non-Existent and link it to the MAC Address of our machine … VM1 is the Attacker Machine

Non-Existent Machine = 192.168.100.133

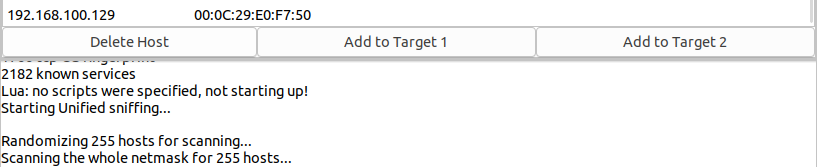


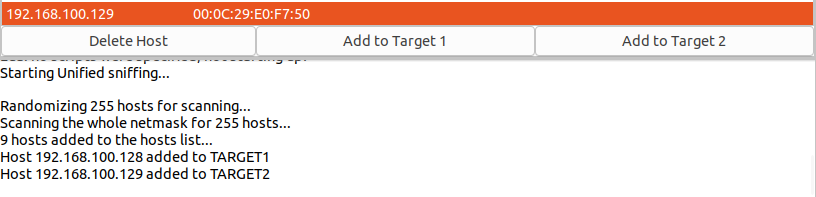
Virtual Machine 1 – Attacker VM is Ubuntu 20 with Ettercap GUI.



We start in bridged mode networking but Network Sniffing is in unified mode.

Step-1 : Scan for Hosts in our network:

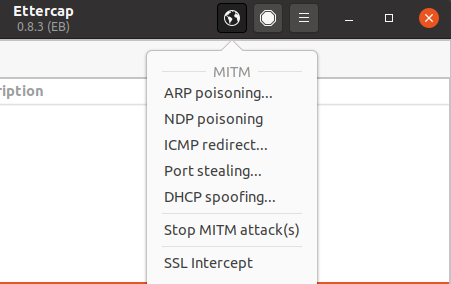




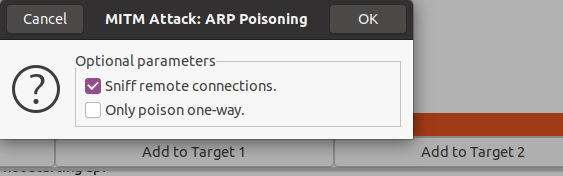
TARGETS are the victims, we can add them and then perform not only ARP Spoofing attack but other attacks as well.

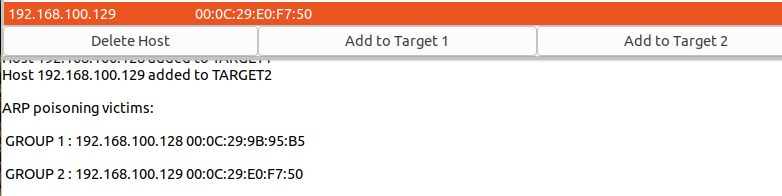
**ARP Cache Poisoning – Man in the Middle Attack:**

**Once we have added targets, go to mitm menu and select arp poisoning**



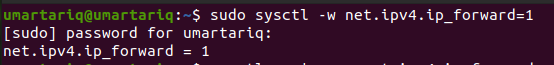
**Select Sniff Remote Connections**

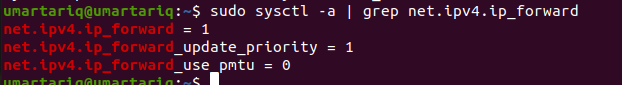




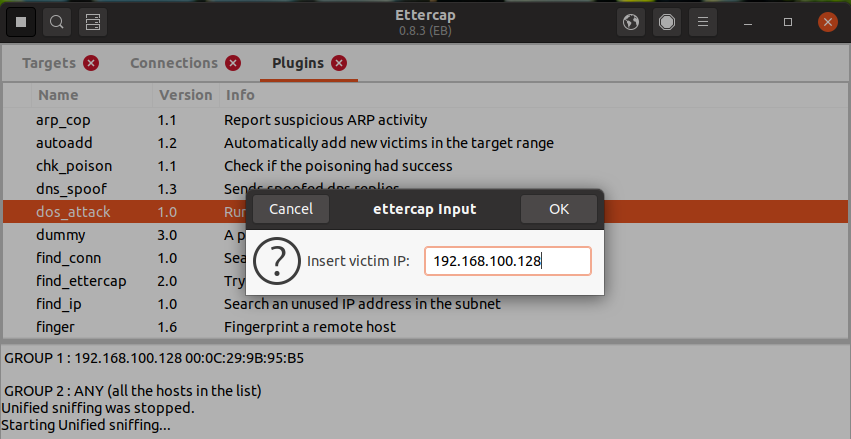
**ATTACK SCENARIO 1 AND 2 ---- ADD NON EXISTENT MAC ADDRESS AND IP ADDRESS AND DOS ATTACK :**

**Step 1: Forward all network traffic through VM1 [Attacker]**

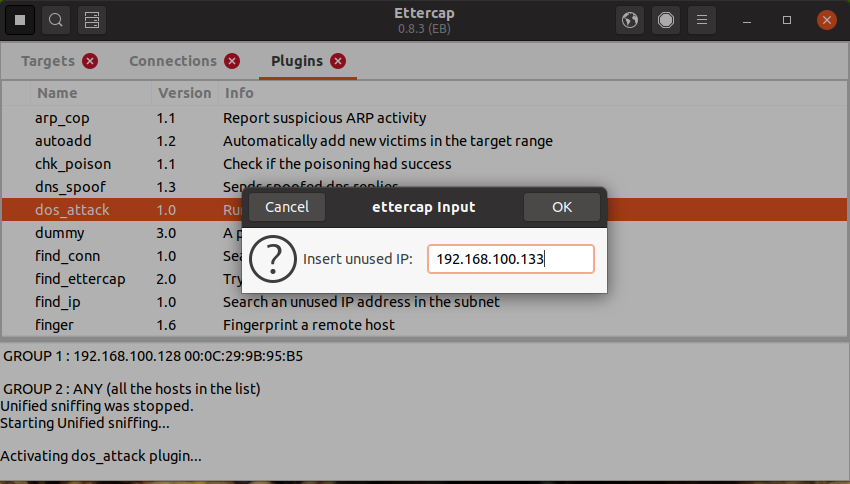


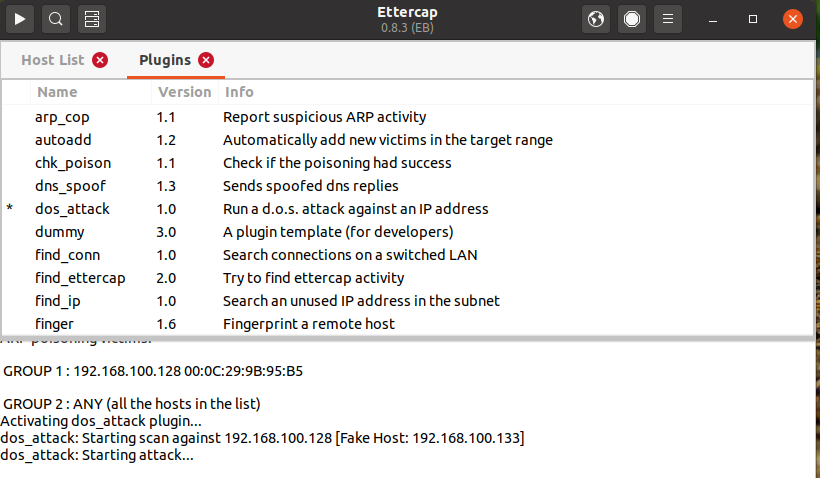


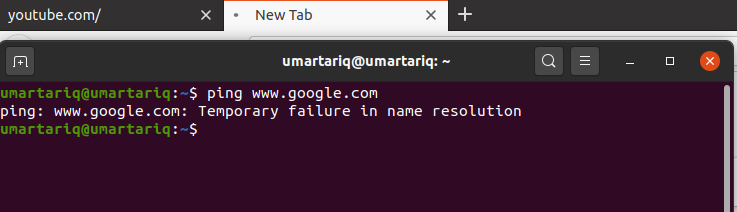
**Step2 – Add Victim IP and an unused IP on the network**

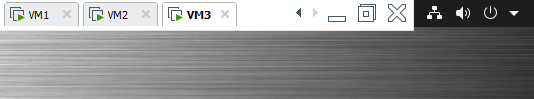


**Unused IP:**



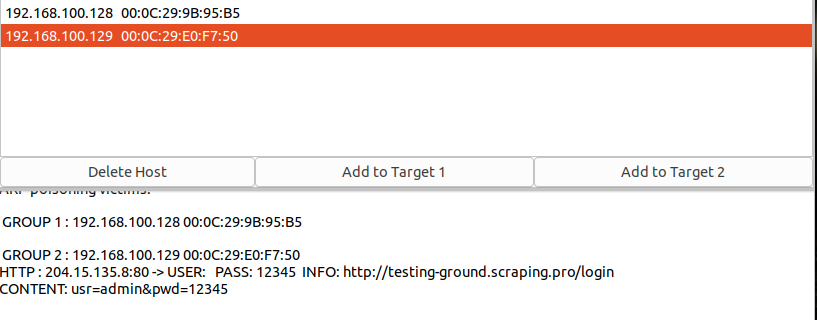




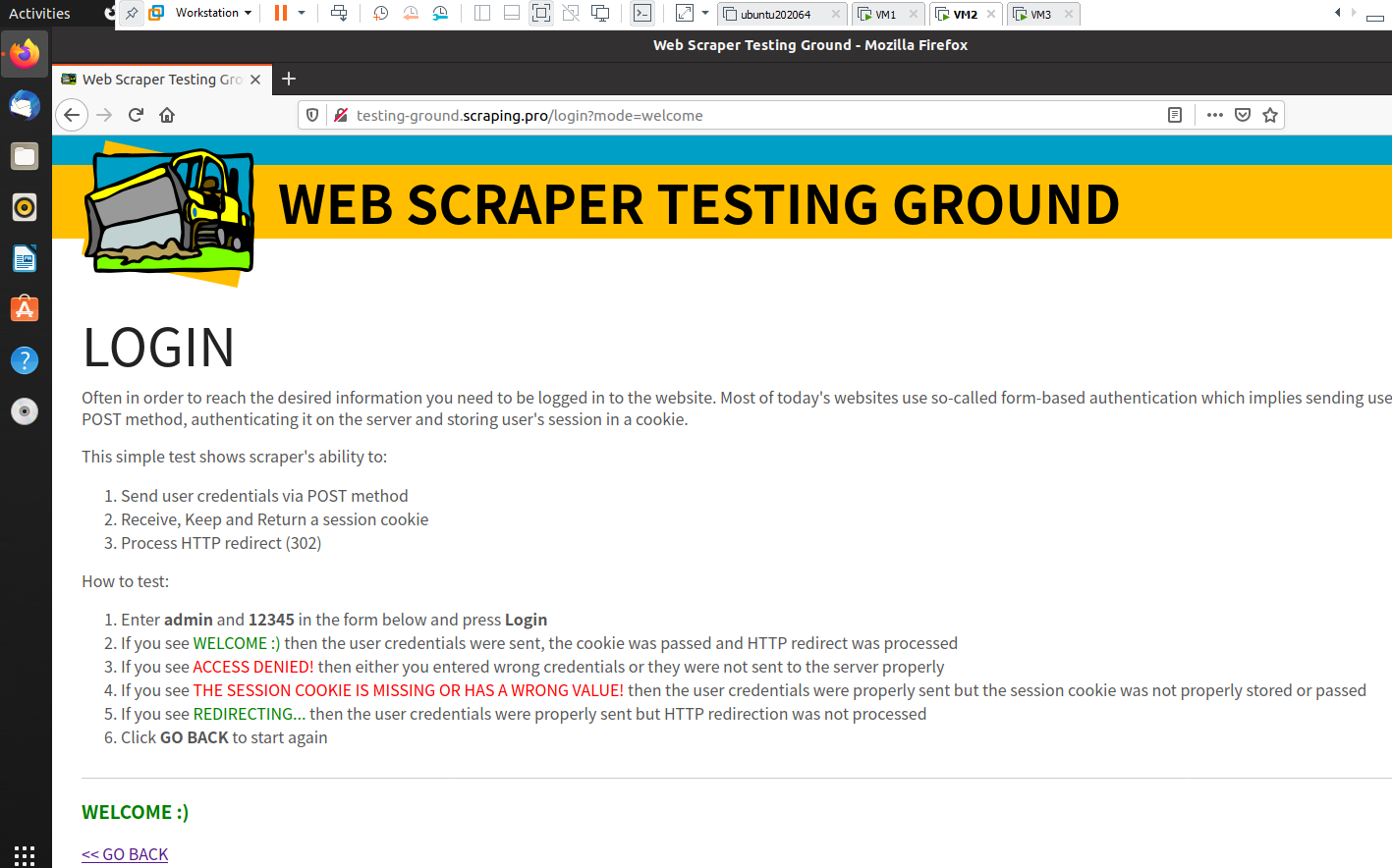


**Redirect Network Traffic from VM2 AND VM3 TO VM1:**

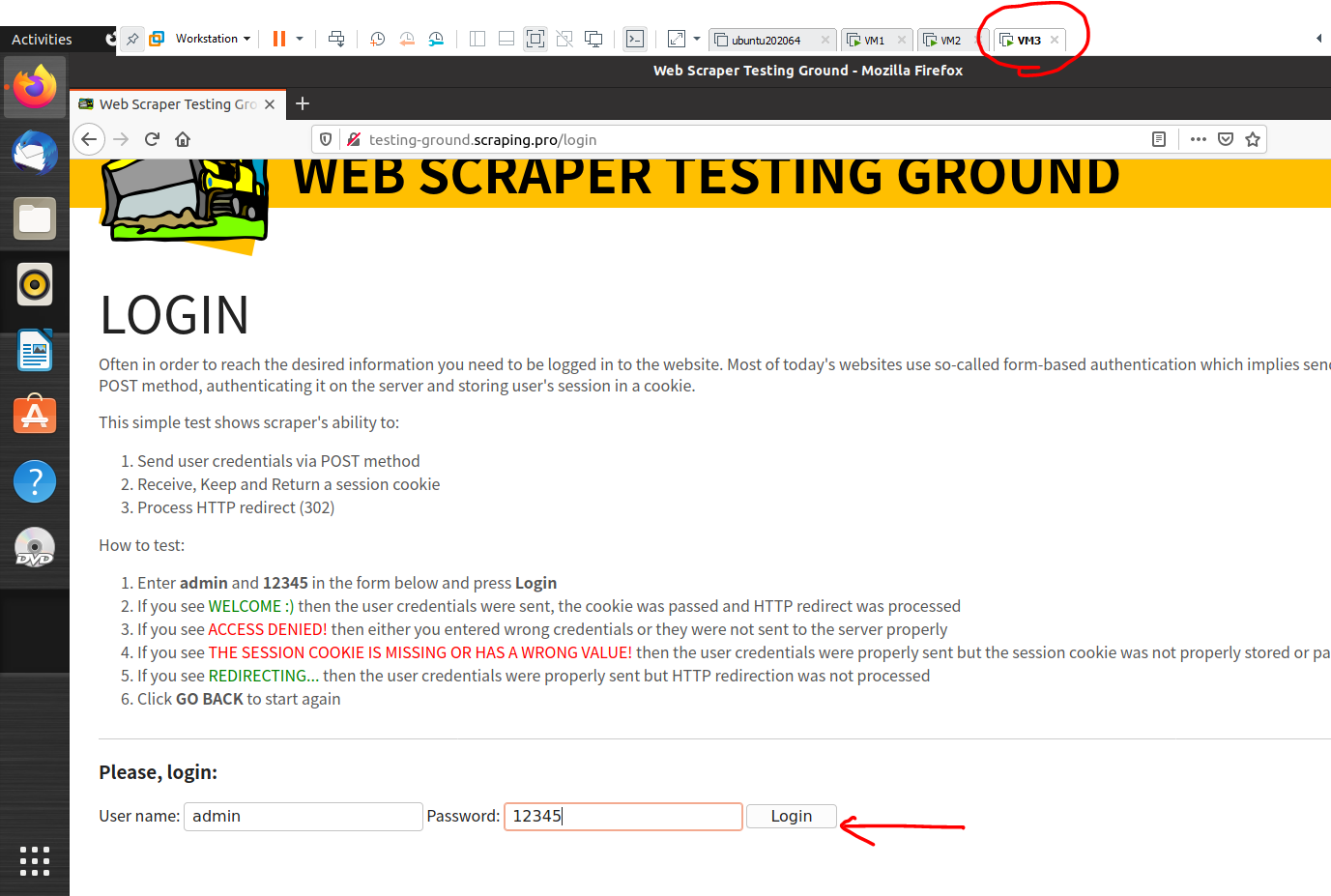
**http credentials logged in on vm2 and vm3 sniffed on vm1[Attacker]:**



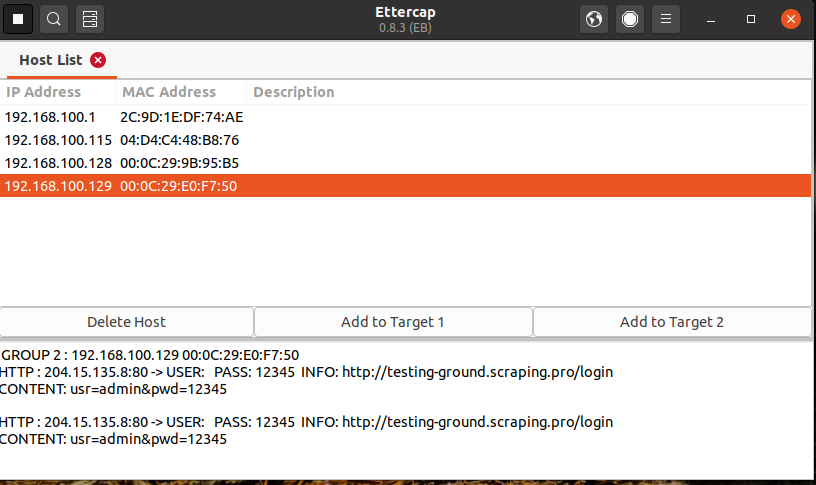
**VM2:**



**VM3:**



**Result : We can view the network traffic of VM2 AND VM3 on the Attacker VM1.**



**For Network sniffing we can use Ettercap as well as Wireshark or any other tool. For which I selected Ethernet Interface and connected to it in Bridged Mode.**