**Assessment 2 – Protocol Demonstration and Report**

# Introduction

The ICMP (Internet Control Message Protocol) is a network layer protocol which is responsible for communicating information about the network. The ICMP protocol generates control messages that depict the condition of the networks and report on issues such as dropped packets during data transmission, connectivity failure, and redirect a sending host to another router. The ICMP protocol is mostly well known as a message protocol through the use of the ping command to check if devices are connected to the same network or outside it. A ping command is issued by the sending device and transmits an ICMP echo request to the target machine.

The target machine then responds with an echo reply depicting the connection is established. As aforementioned earlier, the ICMP works on the network layer but also has two more important protocols ensuring the network accepts and delivers packets known as the Internet Protocol (IP) and Address Resolution Protocol (ARP). Firstly, the most significant IP protocol is the standard for routing packets between and across networks, hence, follows an encapsulating process where the contents are placed in the IP packet and then the entire IP packet is placed into an Ethernet frame. The ICMP messages are wrapped within the IP protocol, acting as a user of the IP protocol.

Secondly, the Address Resolution Protocol is responsible to map mac addresses to their associated IP addresses. Whenever, the sender host would send packet to another host, it first will broadcast an ARP packet. The ARP packet contains a basic question asking the mac address of the associated IP. The host that has been associated with the MAC address would then respond with an ARP packet containing that request.

The attack demonstrated in this report is a Smurf attack that is a network layer distributed denial-of-service attack (DDoS). The Smurf attack is similar to a ping flood of ICMP echo requests to the target machine, the purpose being to amplify the attacking vector that can damage the host situated on the broadcast network. The Smurf attack works by sending s fake ICMP echo request that contains a spoofed IP address, usually the target host address. The request is send over the broadcast network and then is transmitted to all network hosts. Every host on the network sends an ICMP response on the spoofed source address and with so many responses, overloads the server altogether. The attacker would use the Smurf attack as an advantage to amplify network traffic, which could allow him to spoof malicious malware without anywhere knowing where it came from.

# Normal Behavior

To demonstrate the normal behavior of the ICMP protocol, some tools, techniques, and guidelines were used to conduct the experiment

## Tools

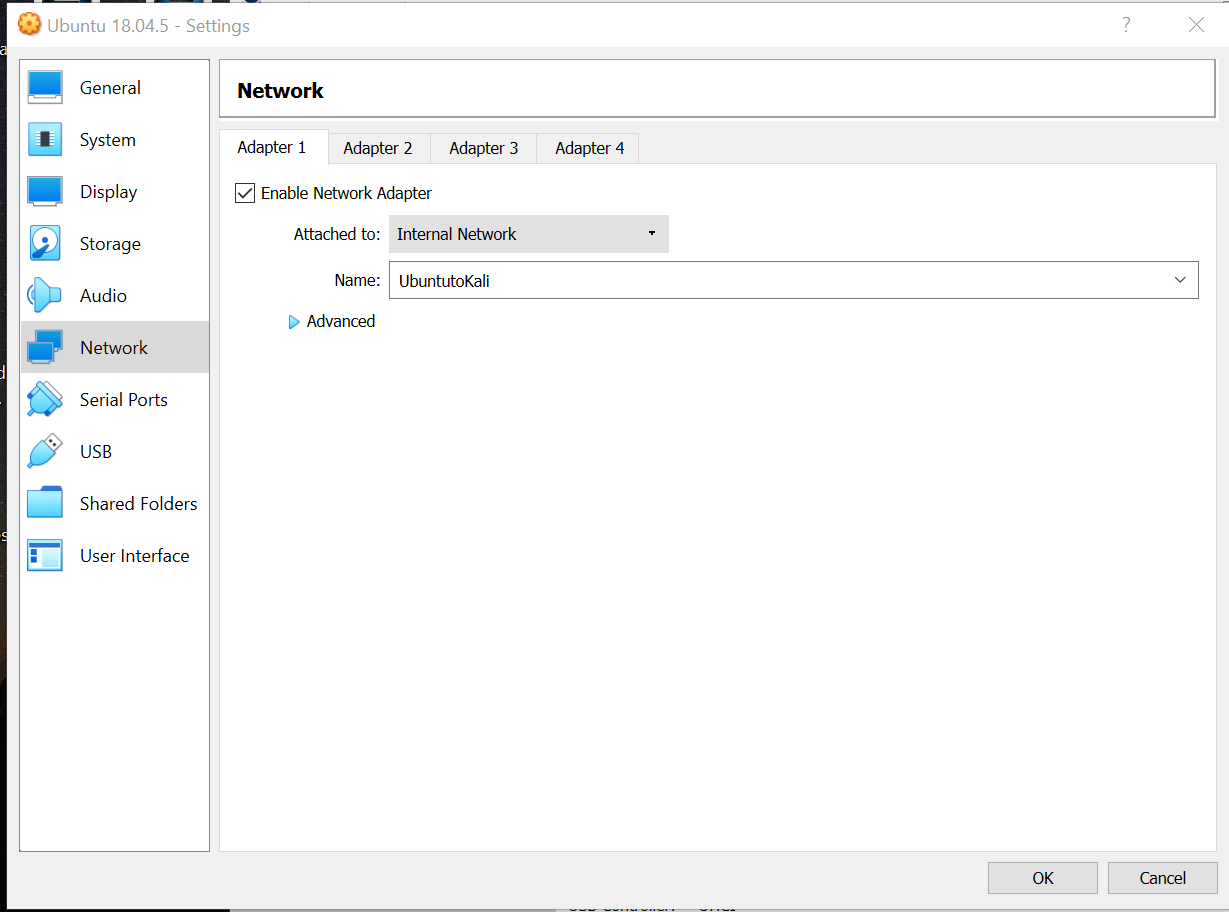
* Kali Linux (Attacker machine)
* Ubuntu (Victim Machine)
* Oracle Virtual Box

## Techniques

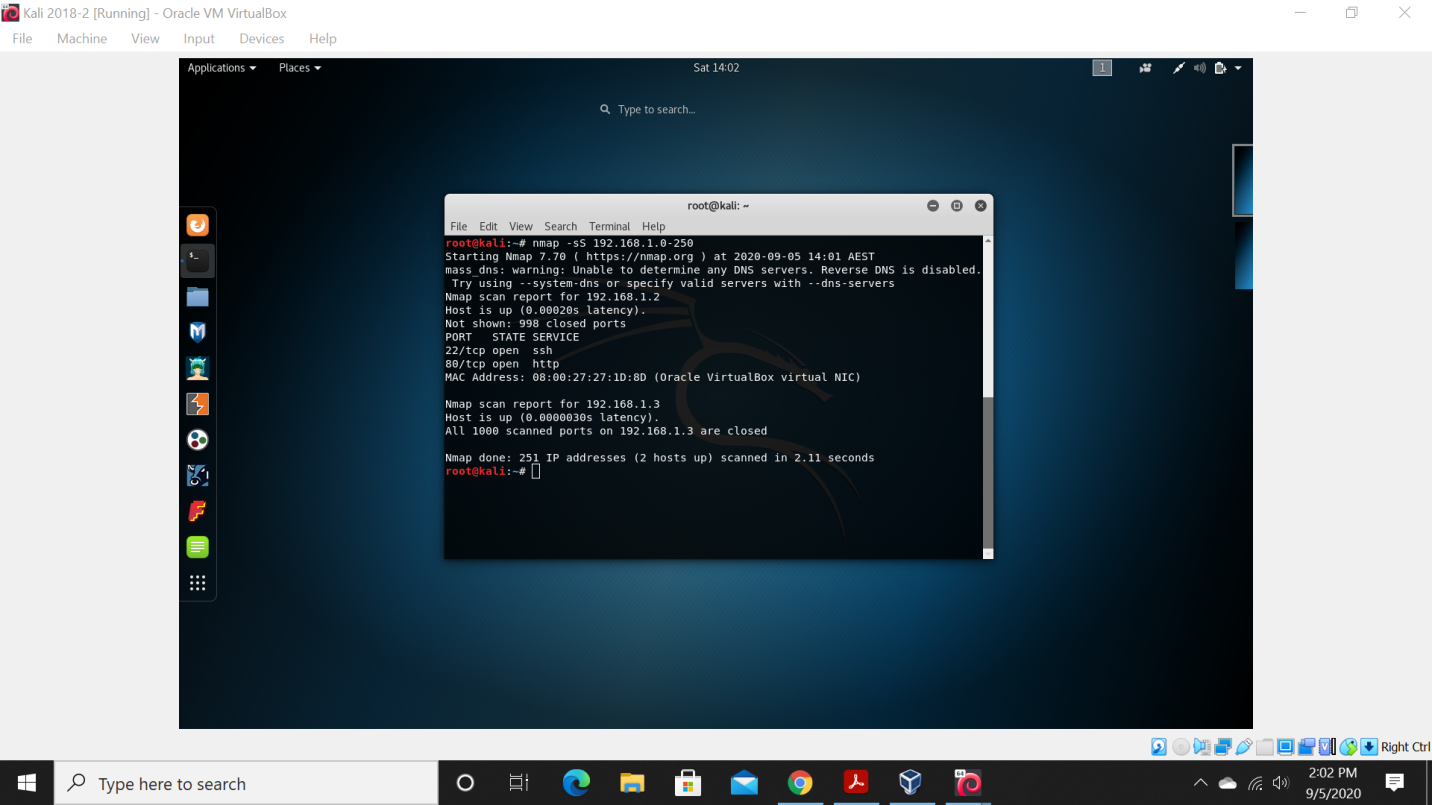
* Using hping3 to send ICMP echo requests to victim machine and also attacking it
* Ping to check network connection
* NMAP (Network Mapping) to check live hosts over our network connection
* Wireshark to capture and analyze network traffic behavior
* Assigning static IP addresses to both Kali and Ubuntu machines

## Step-by-Step guide

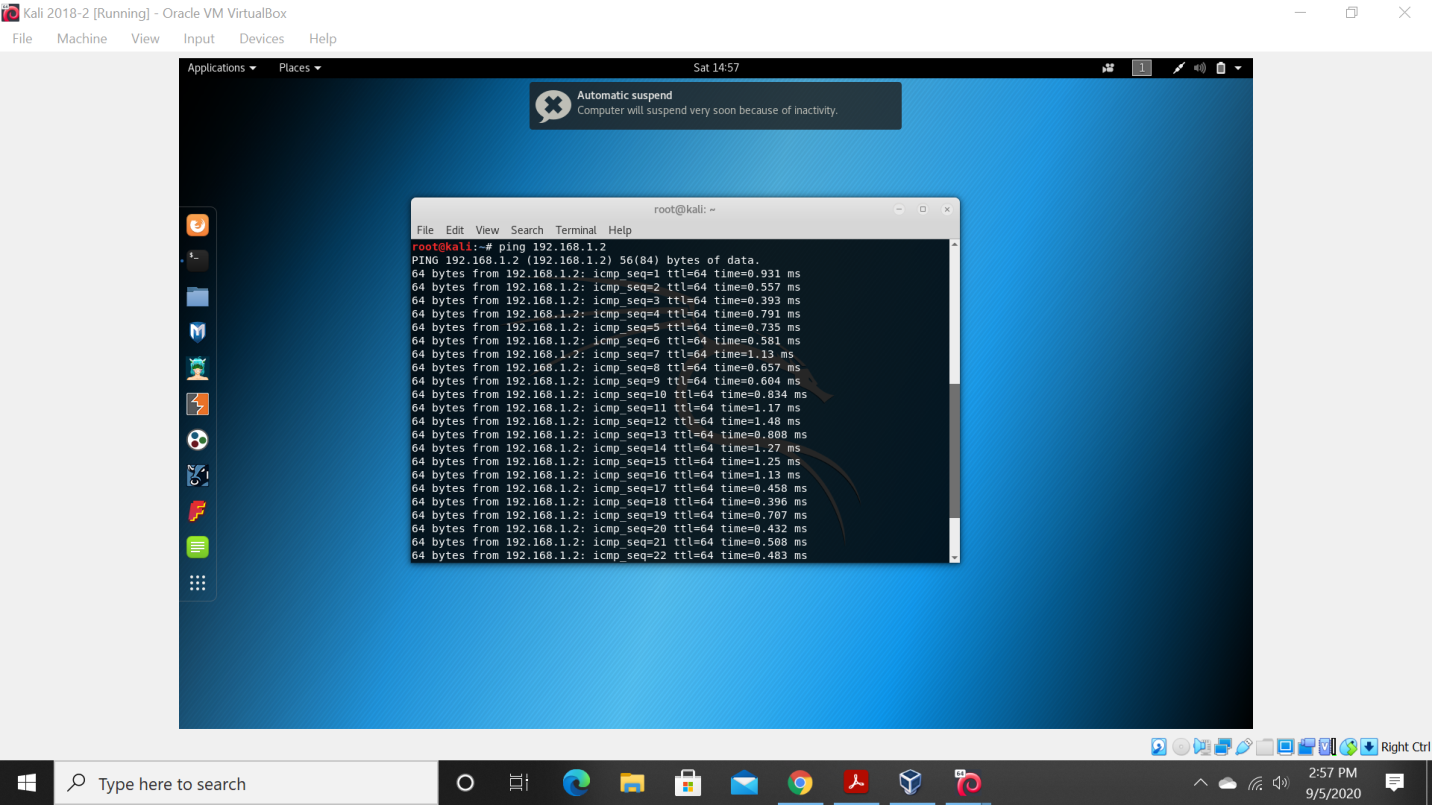
* First need to setup Virtual environment of Ubuntu and Kali machine through an internal network configuration, so that both devices are situated on the same network without being connected to the outside world and attack can be performed without affecting the network. (Attach to internal network on both machines)



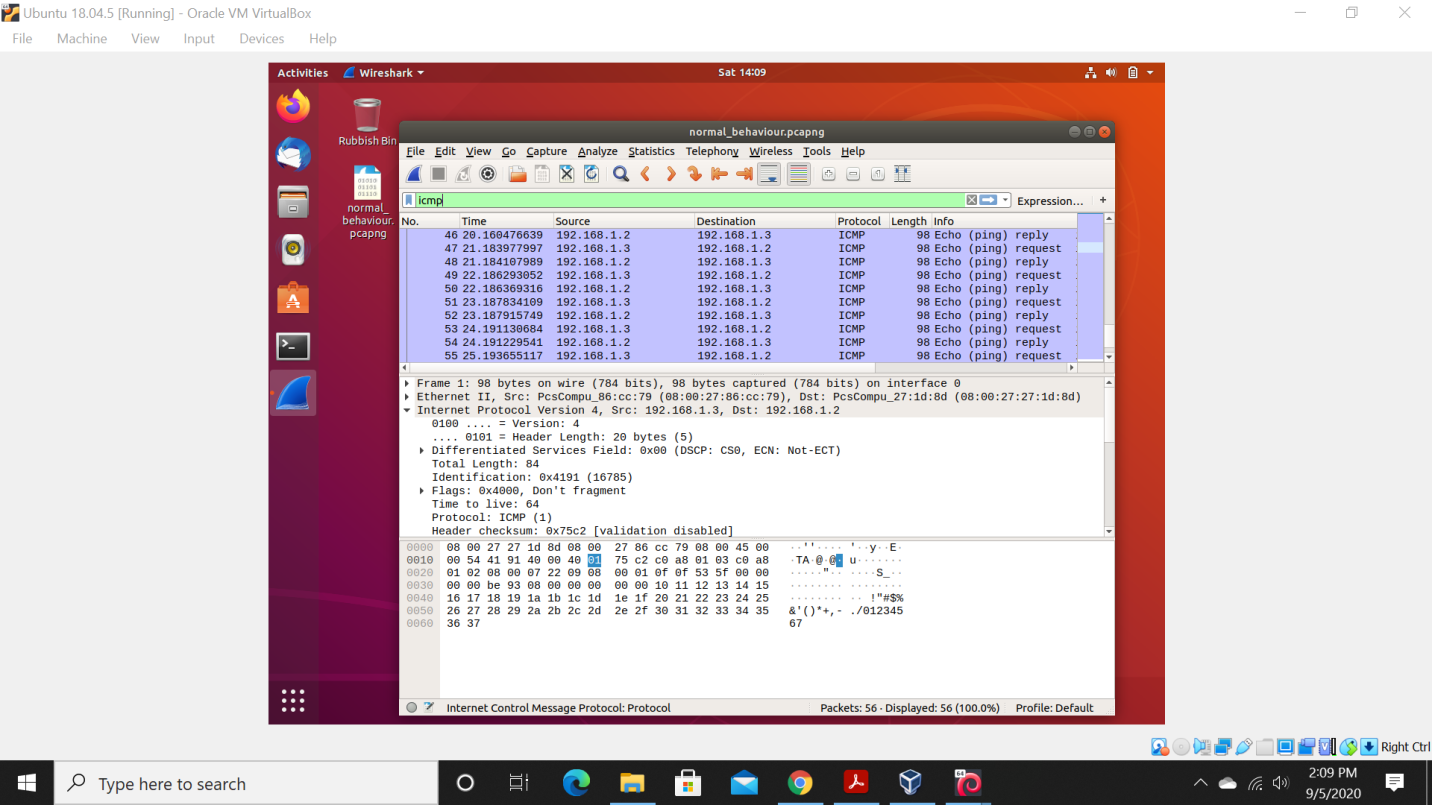
* Assign static IPs and subnet mask on both machines. (In our case Victim=192.168.1.2 and Attacker=192.168.1.3 and subnet mask=255.255.255.0)
* Enter command : Ifconfig (note down the broadcast address)
* Open terminal on Kali machine(Attack) and scan for network using command: nmap –sS 192.168.1.0-250 (This command will scan hosts on our network)



* By scanning we can see out Victim IP (192.168.1.2) located on our network
* Start Wireshark on victim machine to capture network packets
* To see if our host is reachable we will launch command: ping 192.168.1.2



* We see from above that the host is reachable and now will see in Wireshark the normal network traffic

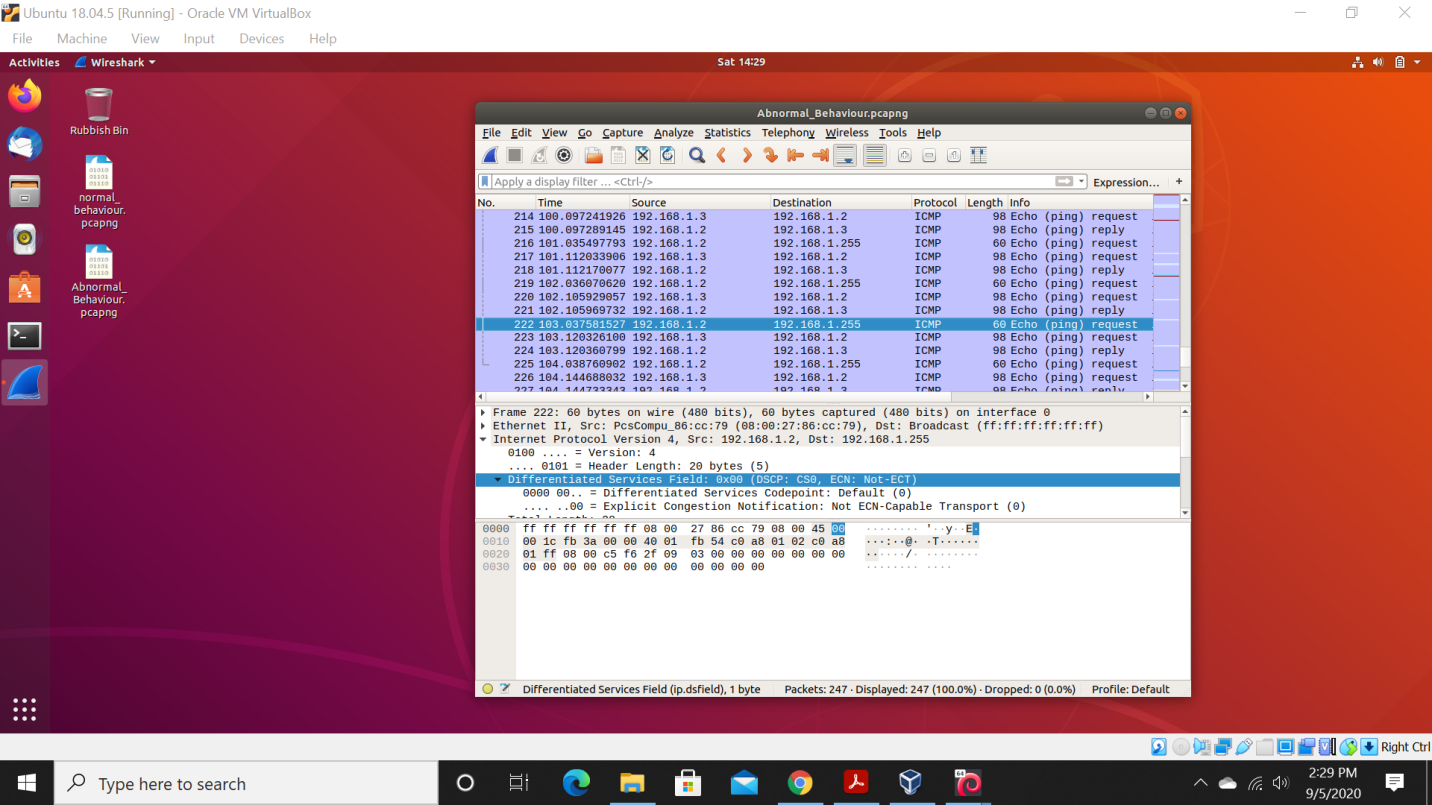


We can see from the figure above the normal activity where the function of the ping command is to send ICMP echo requests to the victim hosts. When the attacking machine sends the ping to the target host, an echo reply is received from the host. If we look at the Internet Protocol version 4 (IPv4) it states the destination and source IP address and the values representing the mac addresses (HEX) of both devices.

## Abnormal Behavior

## Step-by-Step Guide

* Need to scan hosts on network: nmap –sS 192.168.1.0-250 (range of addresses from 0-250)
* Ping network after host scan: 192.168.1.2 (Victim)
* Sudo hping3 –icmp –S –c 6 –spoof 192.168.1.2 192.168.1.255 (performing attack through hping3 and sending 6 ICMP spoofed packets on the victim machine to be broadcasted)



The Smurf attack is illustrated and evidenced in the above figure that shows how the network traffic has changed its behavior. The highlighted packet no 22 illustrates the source spoofed IP as 192.168.1.2 which is actually the victims own IP been broadcasted to the network address 192.168.1.255. In this way the attacker sends requests to every host inside the broadcasting network, alleviating the number of requests of devices over the network, as a result, leading to DDOS attack. Since only one device (Ubuntu) is situated over the network, it is the only one sending requests over the network. In real life cases a broadcast network will have many hosts connected to it; as a result, a large pool of requests will be generated, thus overloading the victim’s machines.

# Conclusion

The difficulty of this attack in a virtual environment with a lack of security features that is no firewall configuration or intrusion detection systems proved to be an easy attack. Moreover, the tools required to conduct this experiment required access of 2 virtual machines namely Ubuntu (Victim) and Kali (Attacker) situated on the same internal network and run on a virtual environment (Oracle Virtual Box). However, some technical skills were required when performing the experiment such as reconnaissance that was done through Network Mapping (NMAP), to find out the hosts available over the network. Also, we needed a packet capture tool in our experiment to depict network behavior which was done through Wireshark. All the tools described above are easily accessible through various websites without any charge.

Moreover, it also required an understanding of hping3 used to conduct our DOS attack. Furthermore, the pertinent thing is that the attack in the real world can have disastrous effects where, an IP broadcast network consisting of a vast number of hosts can send fake ICMP echo responses and, as a result, degrade the entire network infrastructure. Some solutions such as disabling ICMP responses to IP broadcast requests and configuring firewall to not allow pings originate from outside network are used to mitigate DOS attacks.