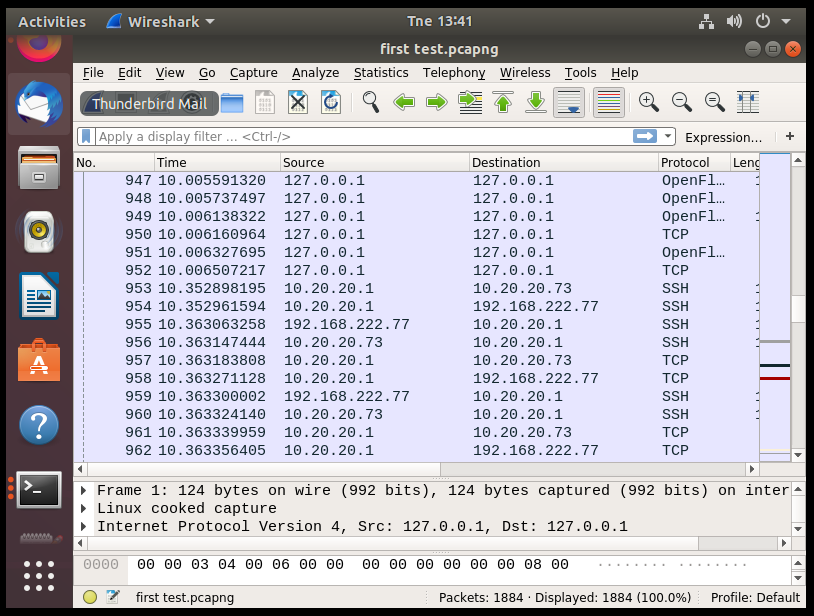
Section C – Final Report

My methodology was based on four attacks, the design of the cloud environment was a Virtual Machine which was enabled by a Linux Operating Systems, and from this OS the OpenStack server was installed and enabled, from there an instance was also created. Than another VM, a Windows 10 VM was created so the instance of OpenStack can have a communication with an external VM that can be found on the same network ID. From here Wireshark was used to sniff and gain packets from the conversation of the instance and the VM. After the Kali Linux was used to launch a Man in the Middle (MitM) using Ettercap and a vulnerability scan using Metasploit.

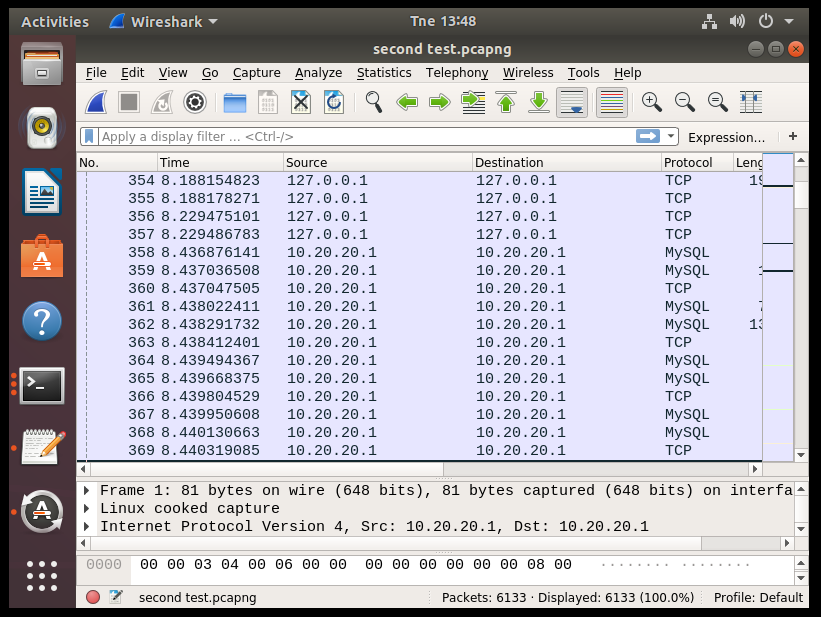
The first attack was basic, the instance sent a folder to the host, my laptop, while Wireshark was in operation. During this attack and sniffing session the results were as expected because the packets gained was from the OpenStack server which has the IP address of 10.20.20.1 and from the IP address of the host, my laptop. The packets collected from the 1st attack was 1884 and Wireshark was able to sniff the conversation, another thing was that the IP addresses were not on the same network, and Keystone, a security tool that is provided by OpenStack was not able to protect the conversation of the two different networks because the packets were sniffed by Wireshark.

Result:

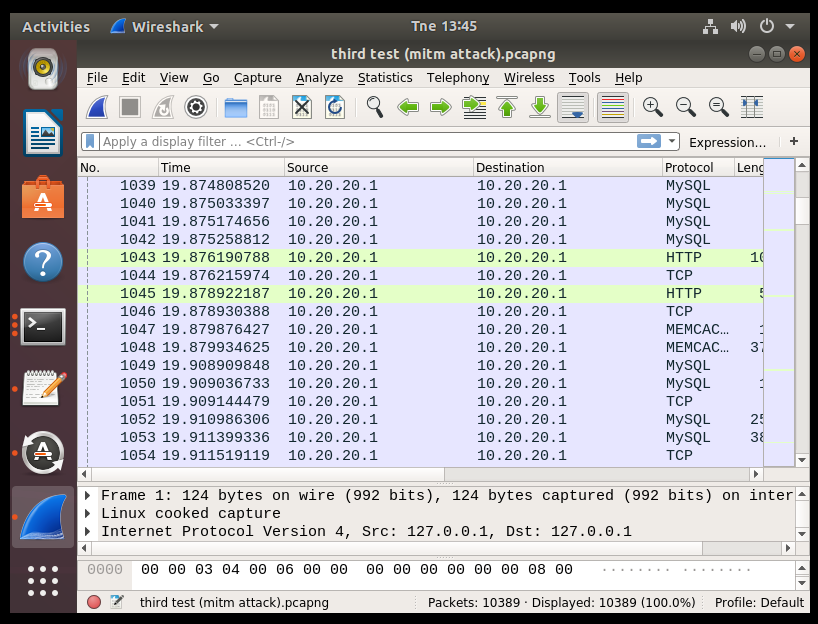


The Second attack was similar to the 1st attack but a bit different because instead of the host, the Windows 10 VM was utilized for the instance to send the folder to, while Wireshark and Keystone were in operation. The results came out different because Wireshark was not able to detect packets coming from the conversation between the instance of OpenStack and the Windows 10 VM. Another main factor was that the network ID was the same. The amount of packets that was gathered from this attack was 6133, and the amount of packets that was gained, was gained from the OpenStack server which had the IP address 10.20.20.1.

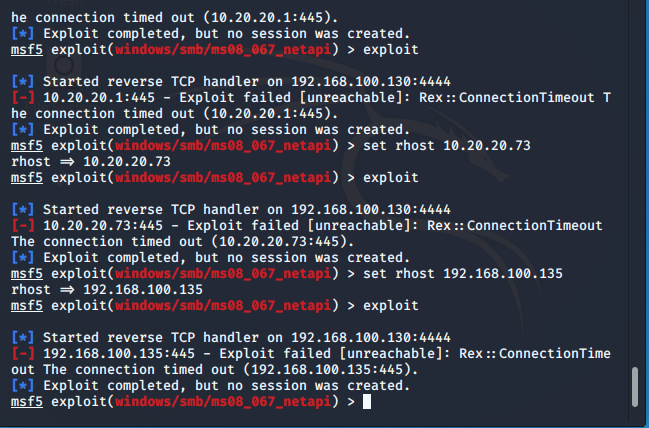
Result:



The third attack was a bit different because another Virtual Machine took place, the Kali Linux. The Kali Linux was utilized because of the tool the OS provides. The tool that was utilized was Ettercap, to launch MitM attack against the instance of OpenStack and the Windows 10 VM. Keystone was also enabled and the VMs were on the same network ID. The number of packets gained were 10389 and the result was negative because either the Wireshark and Ettercap were able to gather the packets between the conversation of the instance and the Windows 10 VM. Another important factor was although 2 tools were enabled, none of the packets were sniffed but only the packets of the OpenStack server again was sniffed which has the IP address of 10.20.20.1.



The fourth and final Attack was different because a vulnerability scan was launched for the OpenStack instance which had the IP address 10.20.20.73. The attack did not happen because the session was not created, while the attack was happening wireshark was also active and the results were that only the packets from the OpenStack server were collected, which had the IP address of 10.20.20.1



Each of these findings can relate to other studies because of the Virtual Machines and tools I used. These findings can relate to other studies because of the analyzation of the packets. The packets do not consist of only the data exchanged between the instance and the virtual machines. For example the information about the TTL (Time To Live), the size of the packet, how much was the time for the packet to be delivered, who was the source with the source’s IP address and who was the destination followed by the IP address which the destination holds. These types of information can relate to other studies because that exact information is provided to know the exact data about the packet. These findings can relate to Wide Area Networks and Wireless Networks because in those subject and studies we were comparing the packets and do many analysations of the packets and had a better understanding of how a packet works and what data can a packet hold, which such data is very important for someone who is trying to figure out information about the packet.