Security of computer systems and Networks

*Aristodimos Avdeliodis 2202*

*Ioanna Papagianni 2790*

**Man-in-the-middle attack**

A man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.

Steps:

* Firstly, we download the zip file MYE007-L2 and we extract it on a USB(8GB).
* We run Linux 64-bit(MYE007L2).vmx with VMWare Player with username : root and password : mye007
* Inside our virtual machine(MYE007L2) we will find two other virtual machines c1 and c2 with *192.168.122.105* IP for c1 and *192.168.122.57* IP for c2*.* We open two terminals and we start the machines with the following commands accordingly

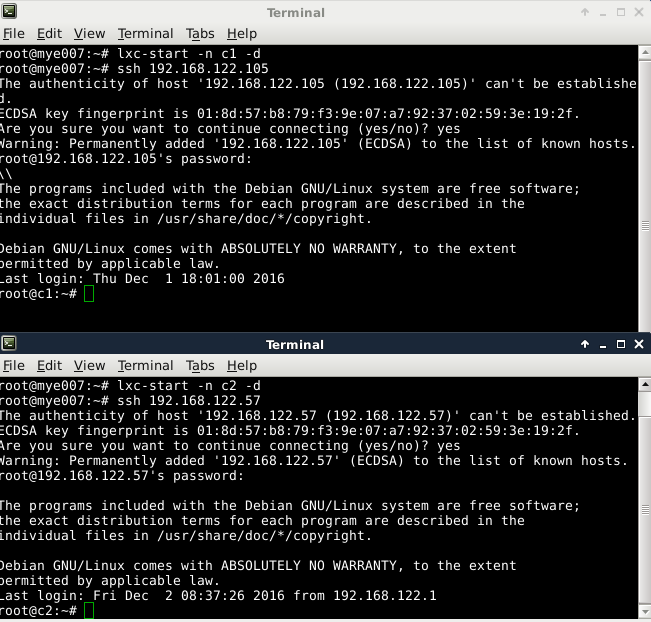
*> lxc-start –n c1 –d*

> *lxc-start –n c2 -d*

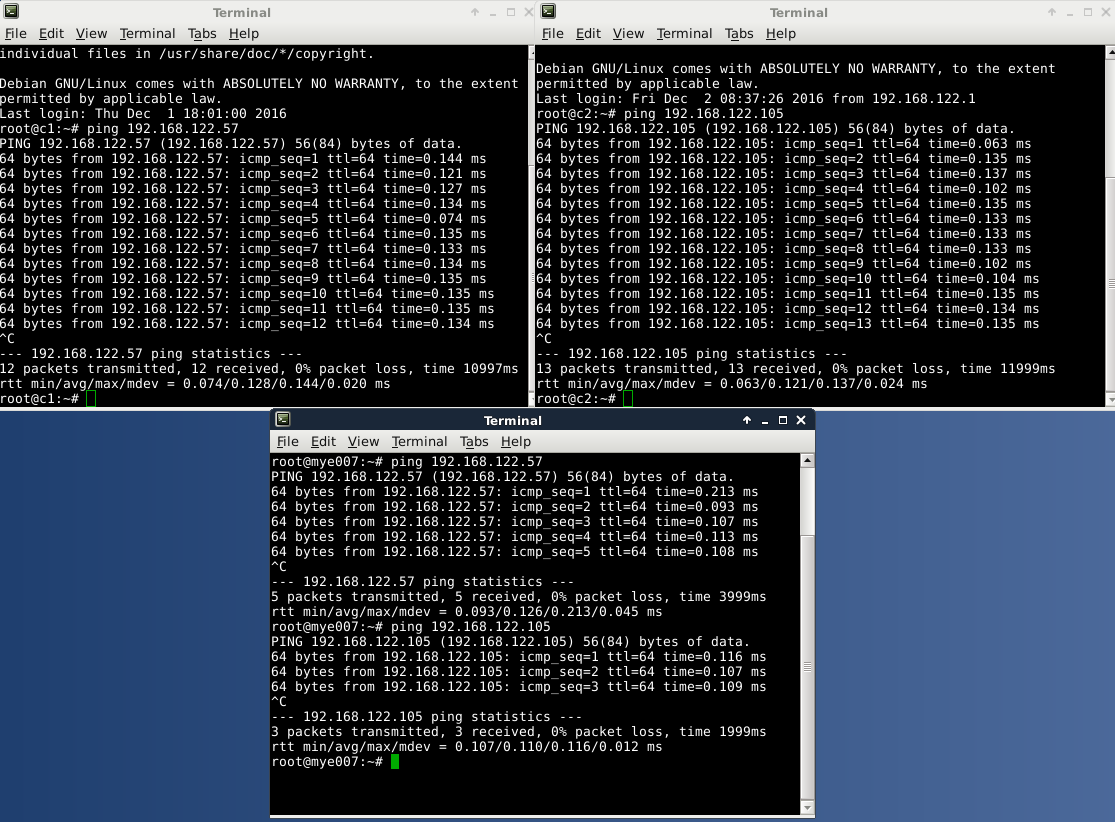
Then we can connect to each one with

> *ssh 192.168.122.105*

*> ssh 192.168.122.57*



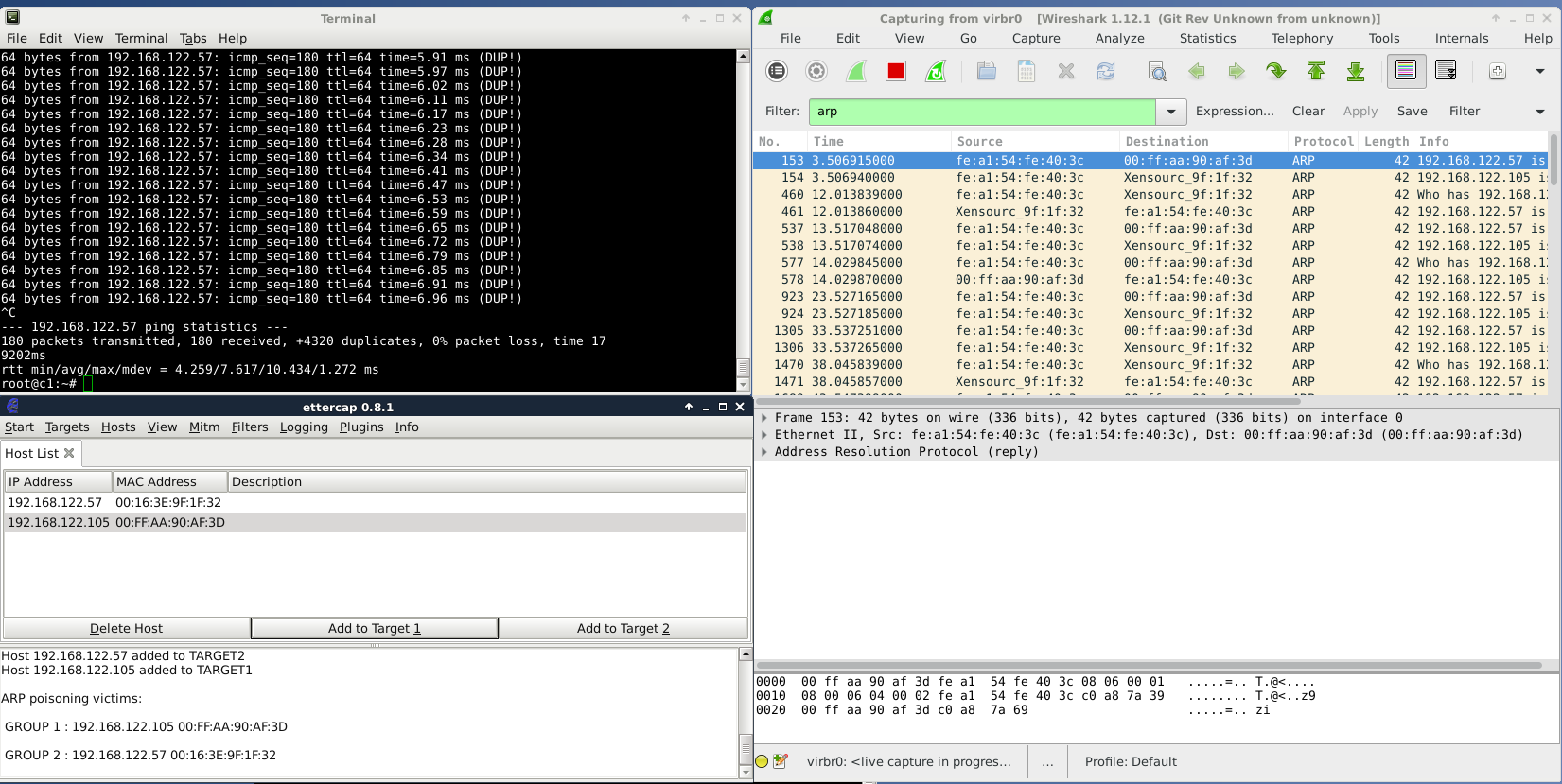
* We use the commands *ping 192.168.122.57* from c1 , *ping 192.168.122.105* from c2 and *ping 192.168.122.105 , ping 192.168.122.57* from mye007 to confirm that all three machines can talk to each other.



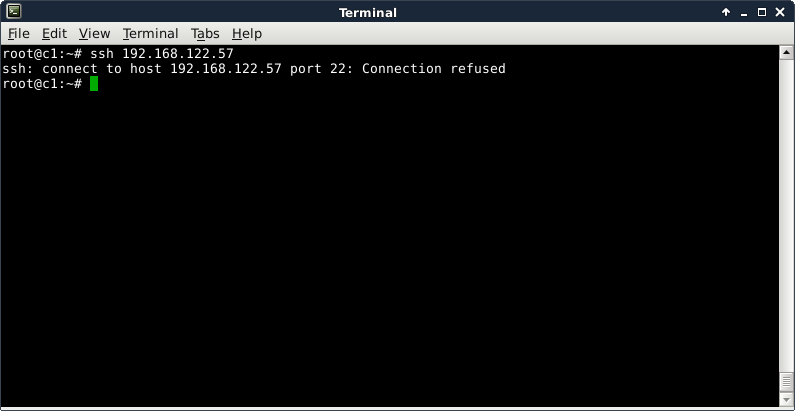
* In this step we will use a new tool called wireshark. Wireshark an [open-source](https://en.wikipedia.org/wiki/Open-source_software) [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](https://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis and software and [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) development . We will use wireshark to track down the packages that go through our network card (vibr0) and confirm that our virtual machines talk to each other. Here we will also need the MAC address of each machine. We can find them using the command *ifconfig.*

Wireshark printscreen??

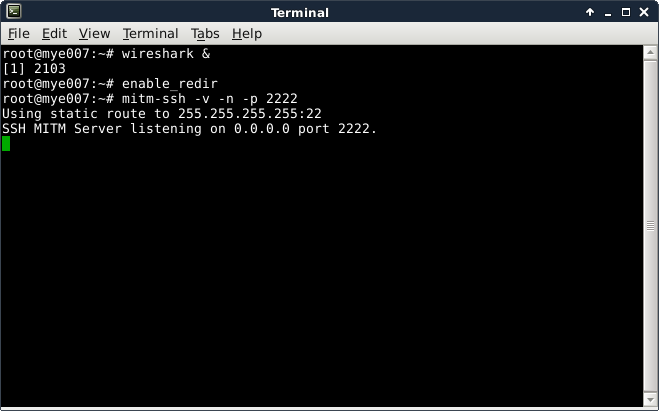
* Now it’s time to use a new tool called ettercap. Ettercap is used for computer [network protocol](https://en.wikipedia.org/wiki/Network_protocol) analysis and [security](https://en.wikipedia.org/wiki/Computer_security) [auditing](https://en.wikipedia.org/wiki/Information_technology_security_audit). We use the command *ettercap –G* to open the graphical interface of ettercap. From the menu bar we click on 'Hosts' and select 'scan for hosts'. Then we go on 'hosts list' and we add as target 1 the virtual machine with *192.168.122.105* IP and as target 2 the virtual machine with *192.168.122.57* IP*.* To start the poisoning attack we go on Mitm and then 'ARP poisoning' #####. ARP poisoning is a type of attack in which an attacker sends false ARP (Address Resolution Protocol) messages over a local network (LAN). This results in the linking of an attacker's MAC address with the IP address of a legitimate machine on the network. In our case, we want to fool c1 and make it think that we are c2 and respectively fool c2 and make it think that we are c1, when in reality, we are mye007(the attacker). We can also check wireshark to confirm that the poisoning succeeded. We ping from c1 to c2 and we see that the information goes through mye007.

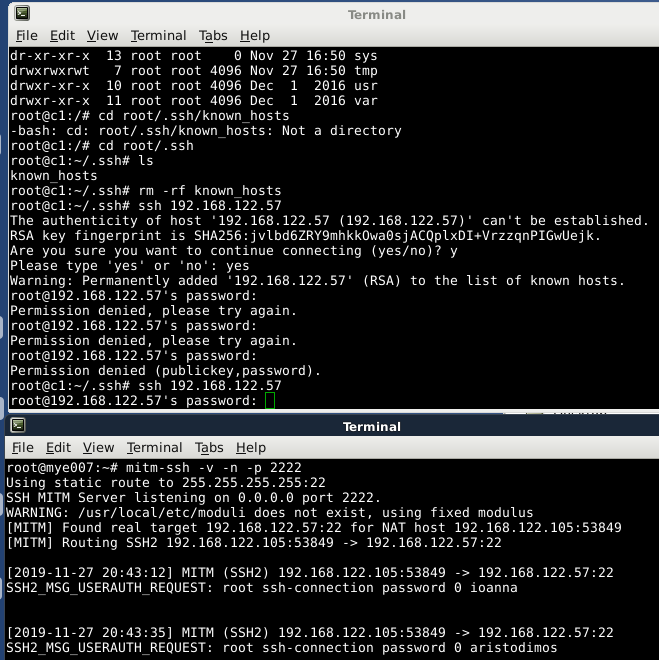


* Now we try to connect from c1 to c2 with the command ssh 192.168.122.57 and it’s unsuccessful
* Next we use the command *enable\_redir* on mye007 terminal
* We try again to connect from c1 to c2 and our connection gets refused.

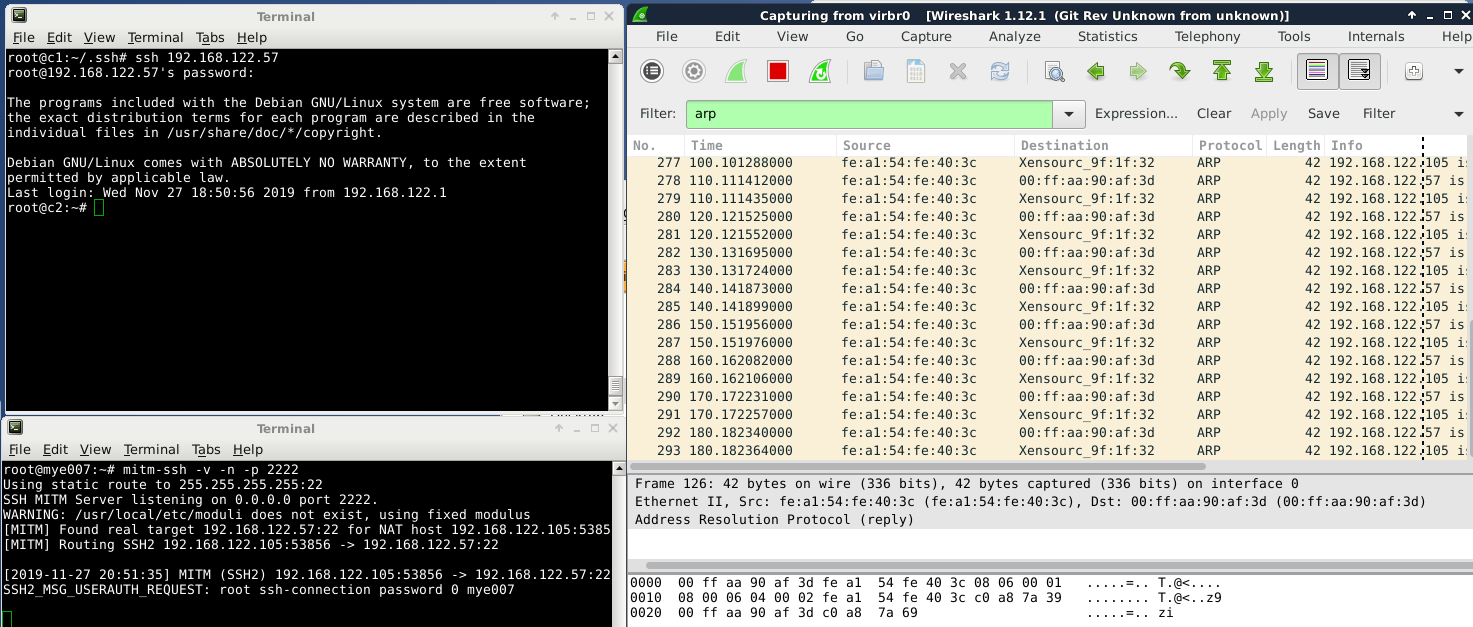


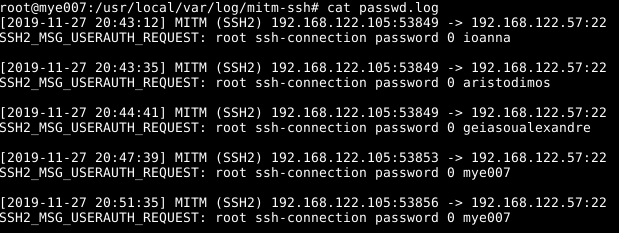
* We need to use *mitm-ssh -v -n -p 2222* command in order to redirect the connection from port 22 to port 2222.





* We need to remove *known\_hosts* file so as to avoid warning messages to c1 that the remote host has changed. We run *rm -rf known\_hosts* command
* Then, we try to connect from c1 to c2 with *ssh 192.168.122.57* and we intentionally give wrong passwords. Mye007 is able now to watch any password input.



* As we can see below, when we give the correct password we are connected.
* We follow the path */usr/local/var/log/mitm-ssh* and we open *passwd.log* file in order to view all password log history.