Progress report (Iteration I) Results

Vaskovskaya Daria

February 2020

1 Goal

Study different variants of simulation platforms and set up the environment for Man In The Middle Attacks, perform some MITM attacks on simulation platforms

2 Choice of simulation platform

To perform MITM attacks and test ways to defend from them there should exist the environment to test on. For this purpose the network emulators were studied.

There are many both free/open-source and proprietary network simulators available.The choice was made out of Open-Source Network Simulators.

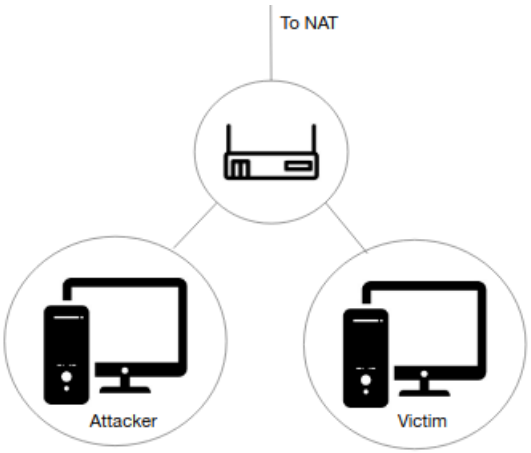
The criteria for the choice were good documentation, simplicity and flexibility.

The first choice fell on the Virtual Box [1] for its flexibility, my experience with it, and community support.

However, there are also out-of-the-box solutions. After reading documentations and launching a few of them I've chosen mininet [2] as one of the best network simulators for the good documentation and simplicity. It is also controlled by python scripts and I have some experience with python.

There would be presented a way to emulate the network in VirtualBox. And, if mininet will be capable of all the required configurations for the showcase at the end of a project, I will use mininet at the presentation because of an easier set-up.

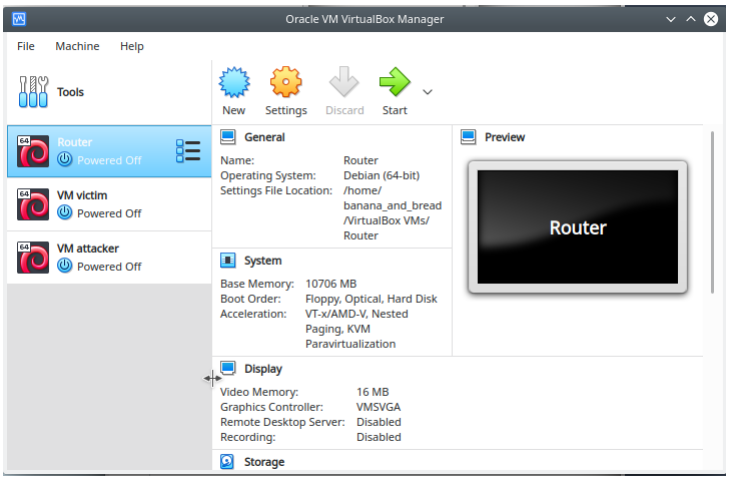
Network topology will look like this:



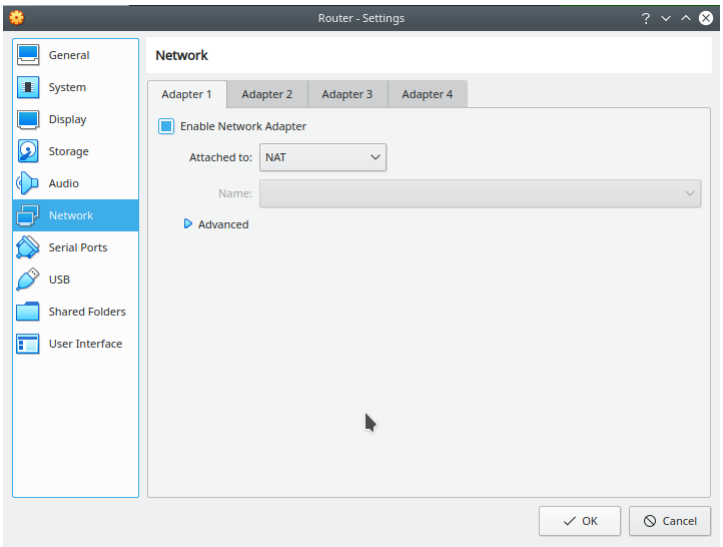
3 Virtual Box set-up

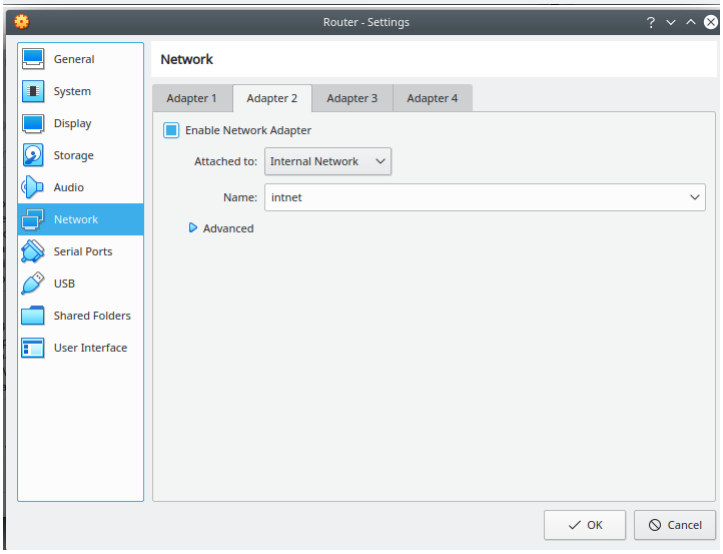
3.1 Virtual Machines and their settings

Three machines were created:

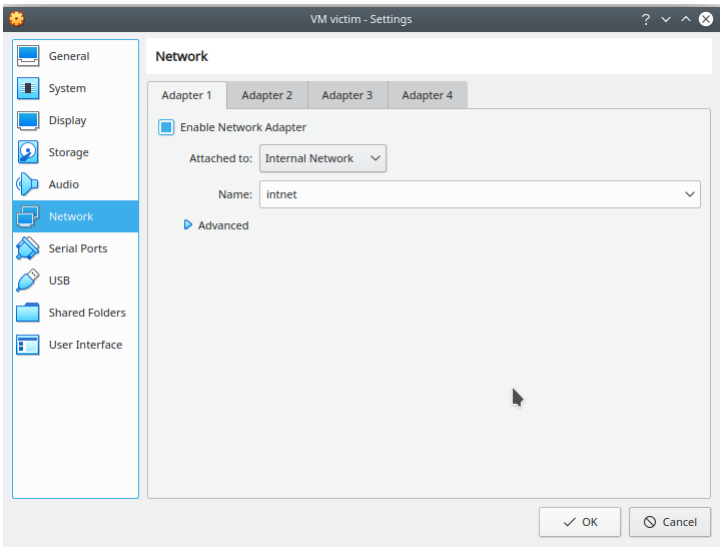


OS: linux-lite-4.6
Network settings are the following:
Router:





Other machines:



3.2 Router set up

Script for the set up is available on github.com [4]

3.2.1 Quagga

Quagga [6] is a network routing software suite providing implementations of Open Shortest Path First, Routing Information Protocol, Border Gateway Protocol and IS-IS for Unix-like platforms, particularly Linux, Solaris, FreeBSD and NetBSD.

Step-by step setup:

```
sudo apt-get update
sudo apt install quagga
sudo apt install quagga-doc
sed -i '/^#.*net.ipv4.ip_forward=1/s/^#//' /etc/sysctl.conf
cp /usr/share/doc/quagga-core/examples/vtysh.conf.sample\
/etc/quagga/vtysh.conf
cp /usr/share/doc/quagga-core/examples/zebra.conf.sample\
/etc/quagga/zebra.conf
cp /usr/share/doc/quagga-core/examples/bgpd.conf.sample\
/etc/quagga/bgpd.conf
sudo chown quagga:quagga /etc/quagga/*.conf
sudo chown quagga:quaggavty /etc/quagga/vtysh.conf
sudo chmod 640 /etc/quagga/*.conf


sudo service zebra start
```

```
sudo service bgpd start



sudo systemctl is-enabled zebra.service
sudo systemctl is-enabled bgpd.service
sudo systemctl enable zebra.service
sudo systemctl enable bgpd.service

echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
ufw disable
```

3.2.2 DHCP

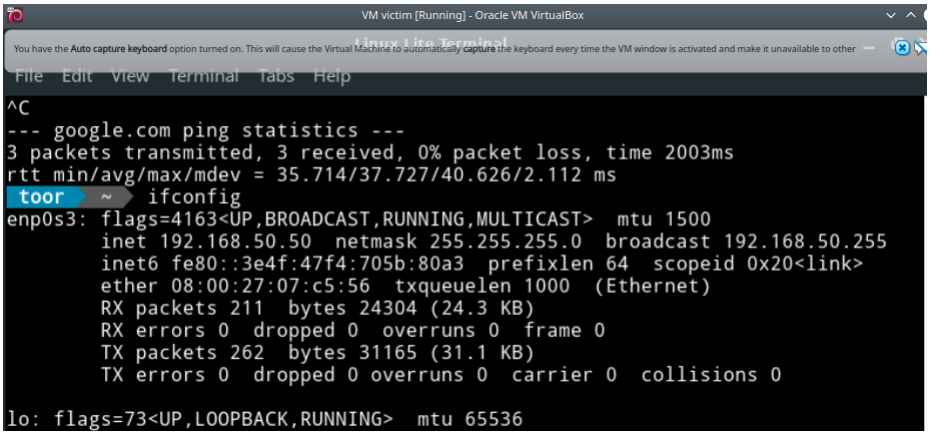
Run the the following commands to enable DHCP: :

```
sudo apt install isc-dhcp-server

echo 'default-lease-time 600;
  max-lease-time 7200;
  ddns-update-style none;
  authoritative;
  subnet 192.168.50.0 netmask 255.255.255.0 {
  range 192.168.50.50 192.168.50.100;
  option routers 192.168.50.1;
  option subnet-mask 255.255.255.0;
  option domain-name-servers 192.168.50.1,   8.8.8.8;
  }' > /etc/dhcp/dhcpd.conf
sudo systemctl restart isc-dhcp-serv



echo '
auto lo
iface lo inet loopback

auto enp0s8
iface enp0s8 inet static
        address 192.168.50.1
        netmask 255.255.255.0
        dns-nameservers 8.8.8.8
' > /etc/network/interfaces
```

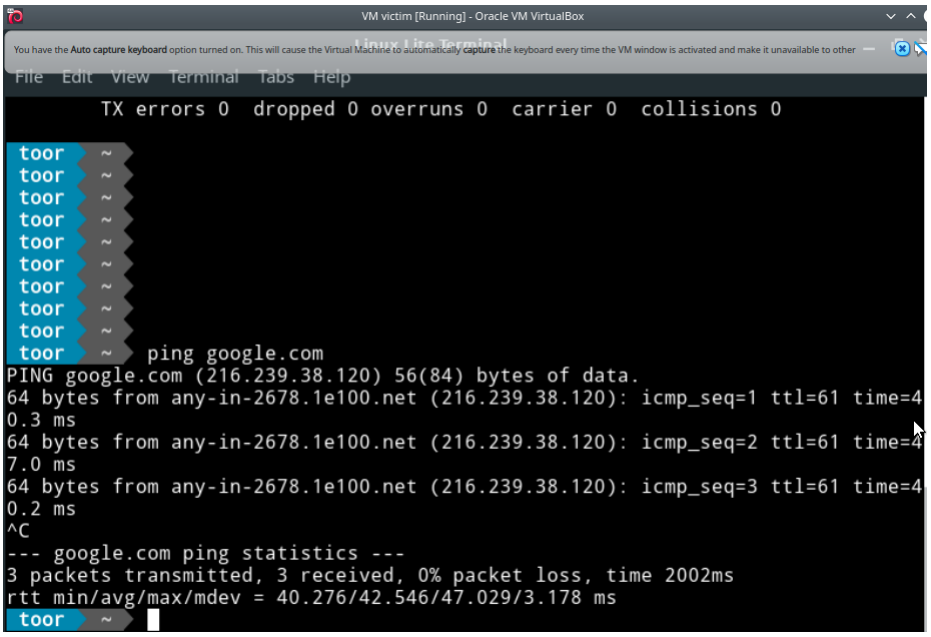
```
sudo ip a flush enp0s8
sudo systemctl restart networking.service
sudo systemctl restart isc-dhcp-server
```

3.3 Tests

DHCP gave address to a victim machine:



Internet became available via router:



4 MITM framework

4.1 Choice of MITM framework

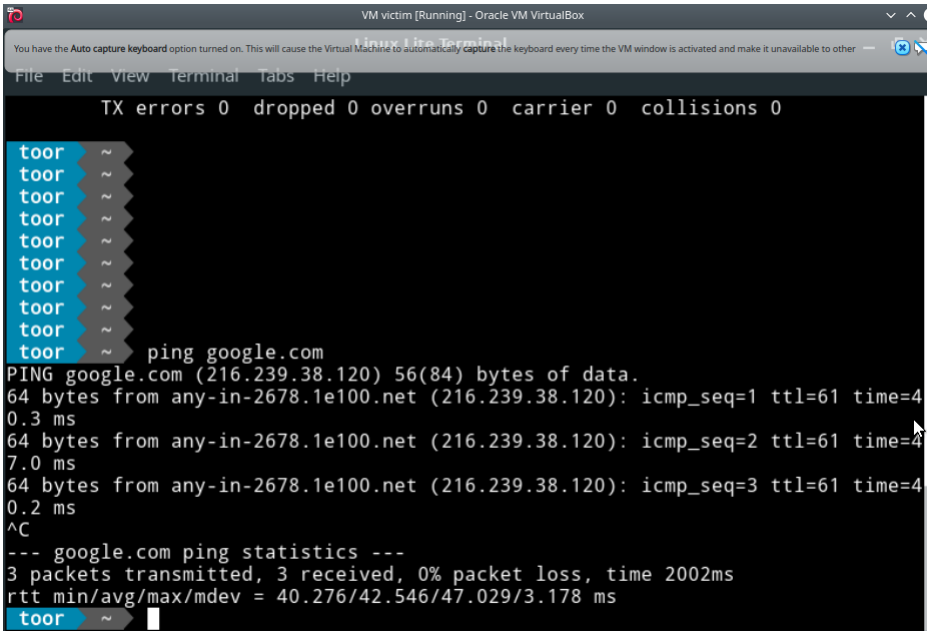
I have chosen bettercap [3], mostly because it is supported in 2020. Script for the set up is available on github.com [5]

4.2 Some attacks showcase

4.2.1 ARP spoofing

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.It is possible to make ARP spoofing attacks with Bettercap via:

set arp.spoof.targets 192.168.50.1/24
arp.spoof on
Vitim's request is seen on the attacker machine:



References

[1] VirtualBox
https://www.virtualbox.org/

[2] mininet
http://mininet.org/

[3] bettercap
https://www.bettercap.org/

[4] Script for setting up router
https://github.com/BananaAndBread/Project/blob/master/scripts/router$_s cript.sh$

[5] Script for setting up bettercap
https://github.com/BananaAndBread/Project/blob/master/scripts/bettercap$_s cript.sh$

[6] Quagga
https://www.quagga.net/