IP-SEC Tutorial

Objective: To see IP-SEC framework in action by establishing Host – To – Host IPSEC VPN Tunnel.

Required VMs: Can be found at /virtual/ipsec/

- VM1 | Centos 7 - VM2 | Centos 7 - Kali Linux | Kali Linux

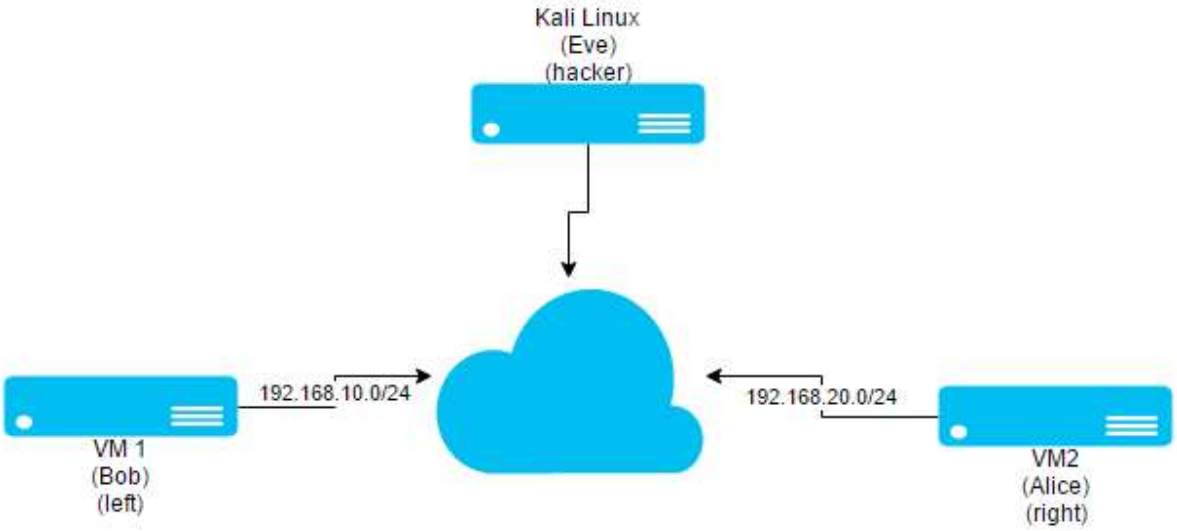
If you do not see the files use the following cmd:-

scp -r [UTORID]@dh2020pc22.utm.utoronto.ca:/virtual/ipsec /virtual/ipsec

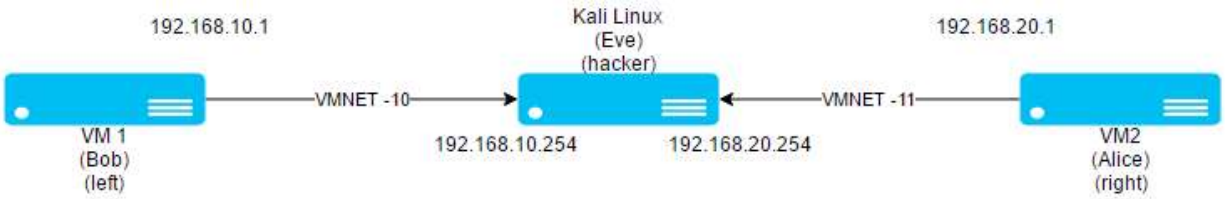
Required Software: Already installed for you on the VMs: -

- IPSEC Tools - WireShark - libreswan

Scenario



How we emulate this: -



VM access details: -

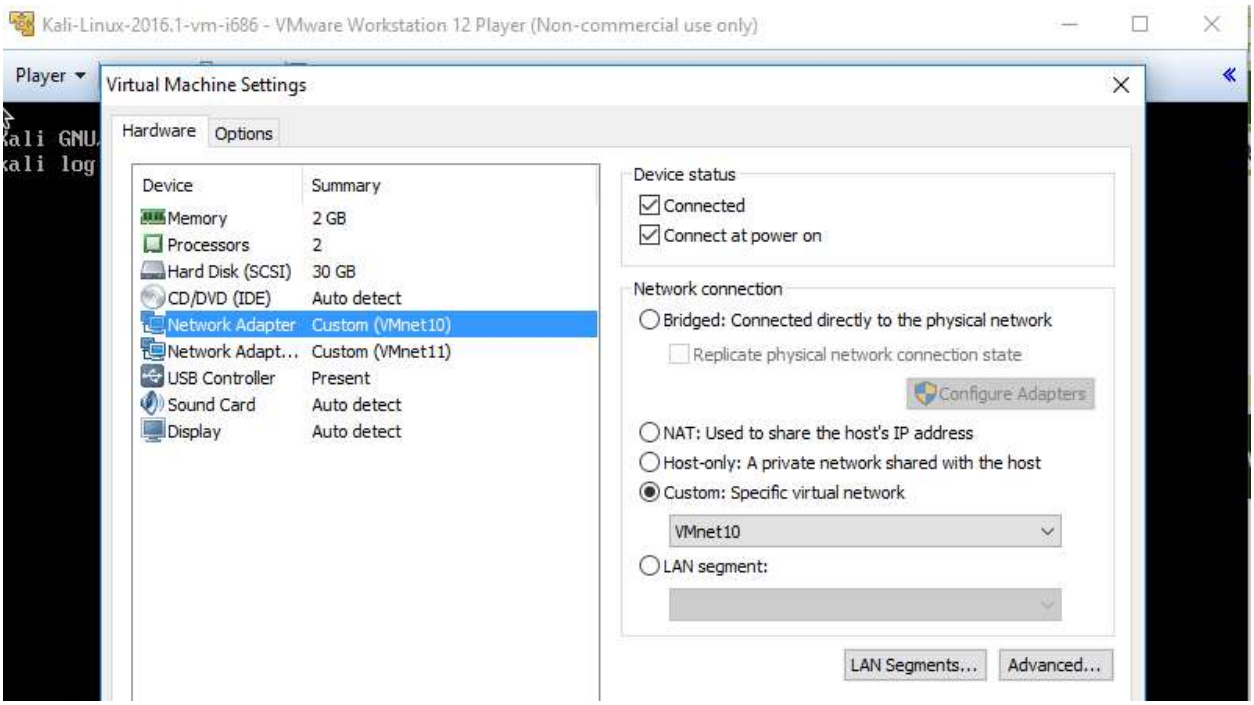
- Kali Linux: root/toor
- VM1: root/root
- VM2: root/root

SETUP: Please turn on all the VMs and login. For VM1 and VM2 you may use startx to use the terminal in GUI so that you can copy paste directly in the VMS as VMware tools is installed on all VMs.

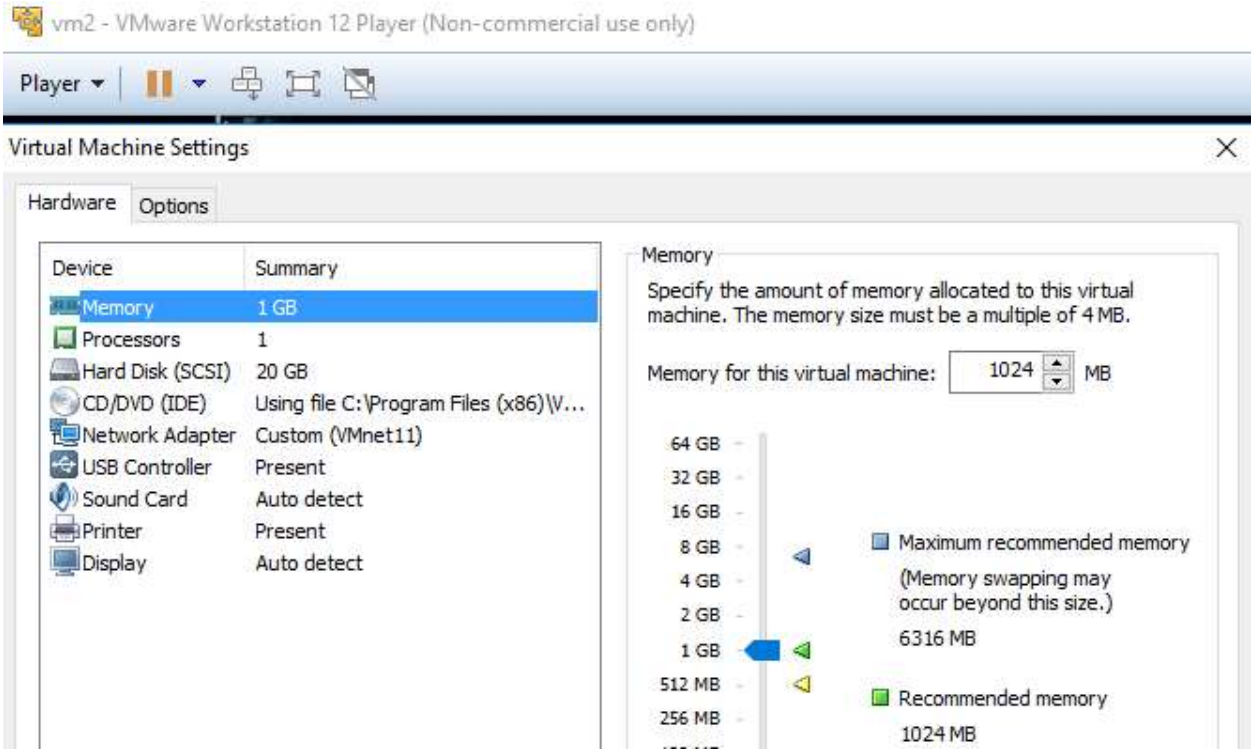
```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

vm2 login: root
Password:
Last login: Sun Mar 27 21:46:14 on tty1
[root@vm2 ~]#
[root@vm2 ~]#
[root@vm2 ~]# startx
```

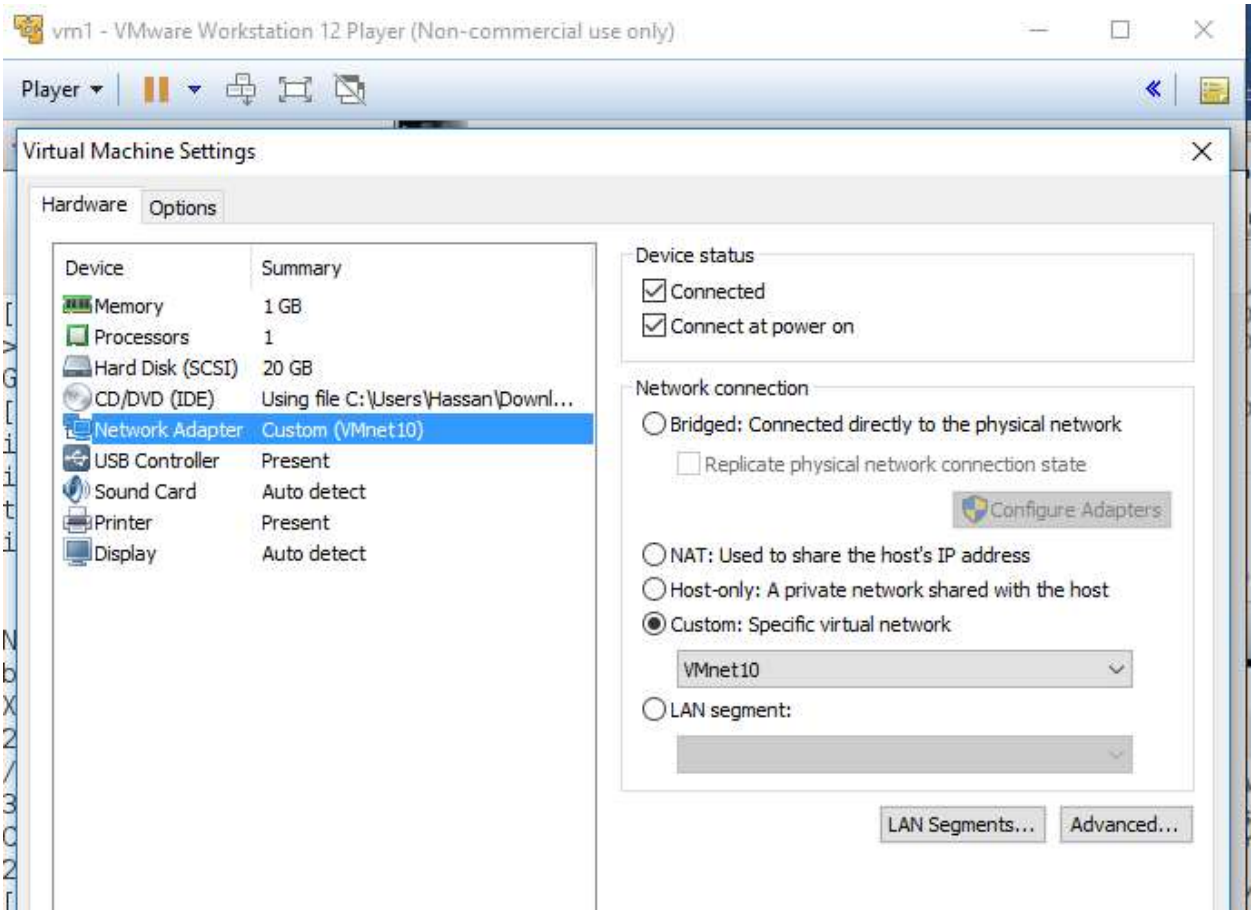
SETUP: Make sure that in Kali Linux VM Setting (the Network settings) are as below: -



SETUP: Make sure that in VM2 Setting (the Network settings) are as below: -



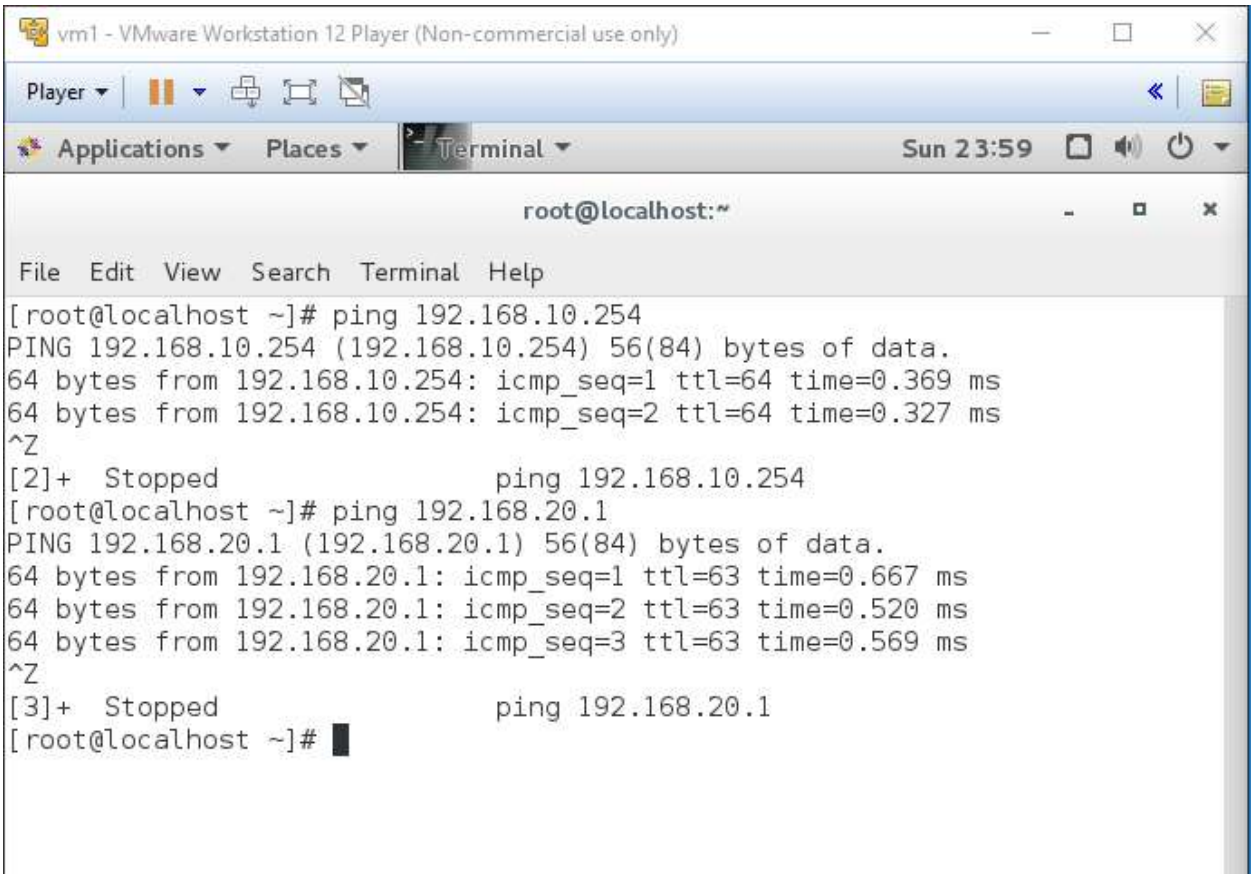
SETUP: Make sure that in Kali Linux VM1 Setting (the Network settings) are as below: -

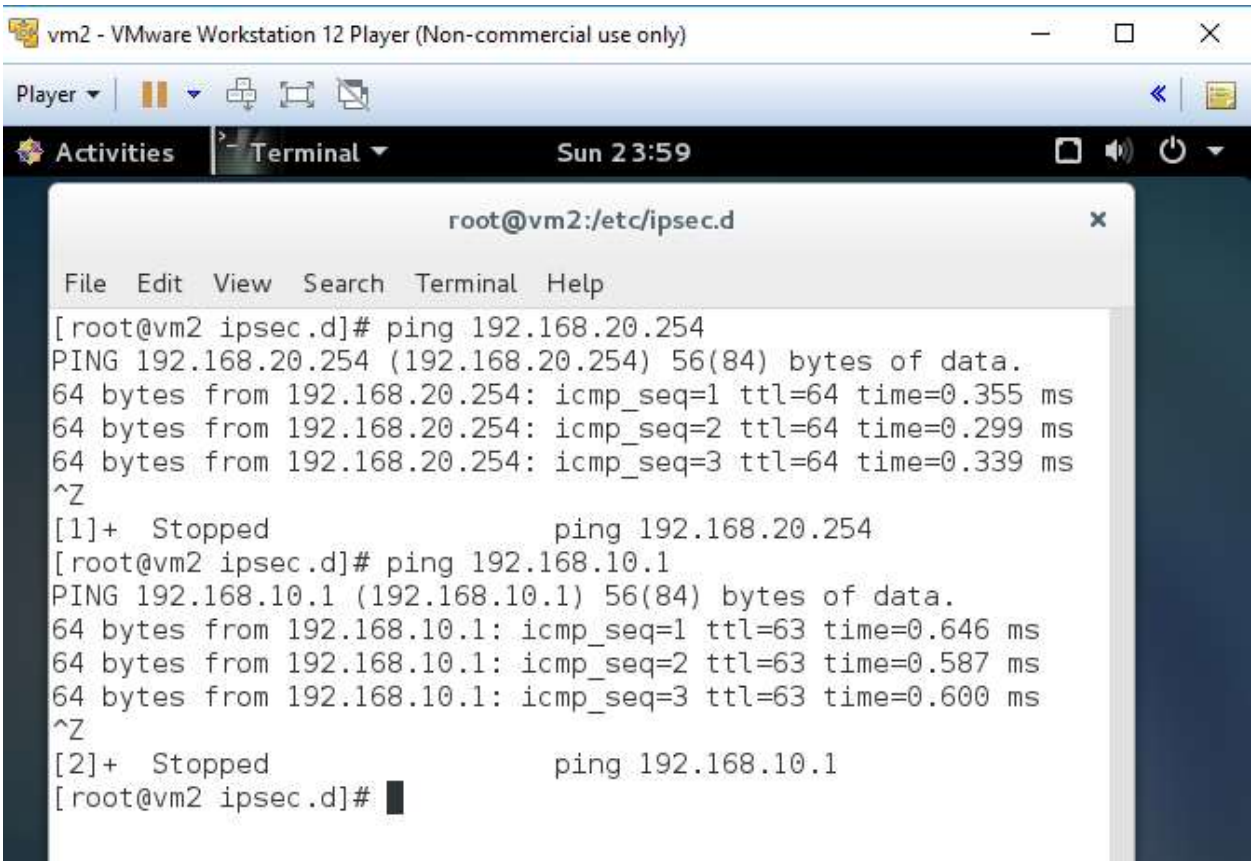


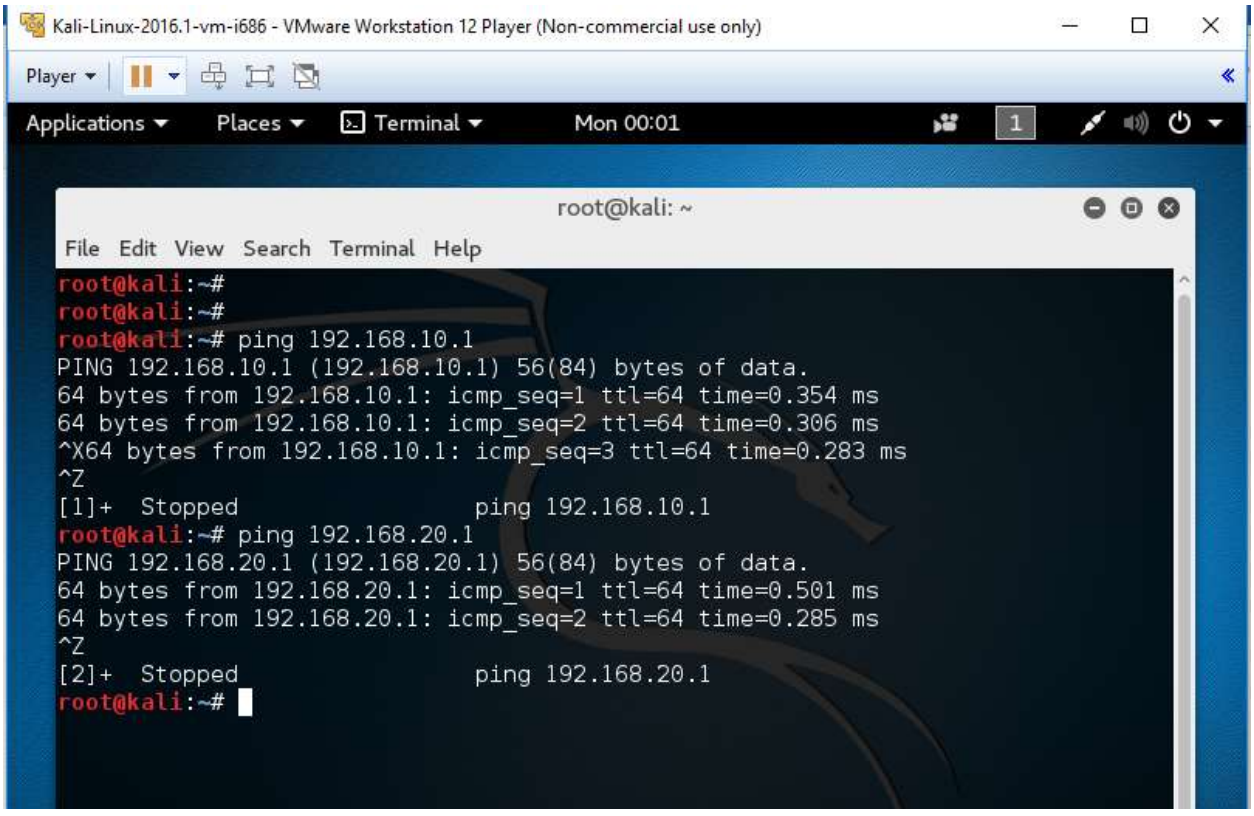
SETUP: Make sure that all the VMs have the correct IPs as below:

- VM1: 192.168.10.1 | 255.255.255.0 | 192.168.10.254
- VM2: 192.168.20.1 | 255.255.255.0 | 192.168.20.254
- Kali Linux: eth1: 192.168.20.254 | 255.255.255.0
- Kali Linux: eth0: 192.168.10.254 | 255.255.255.0

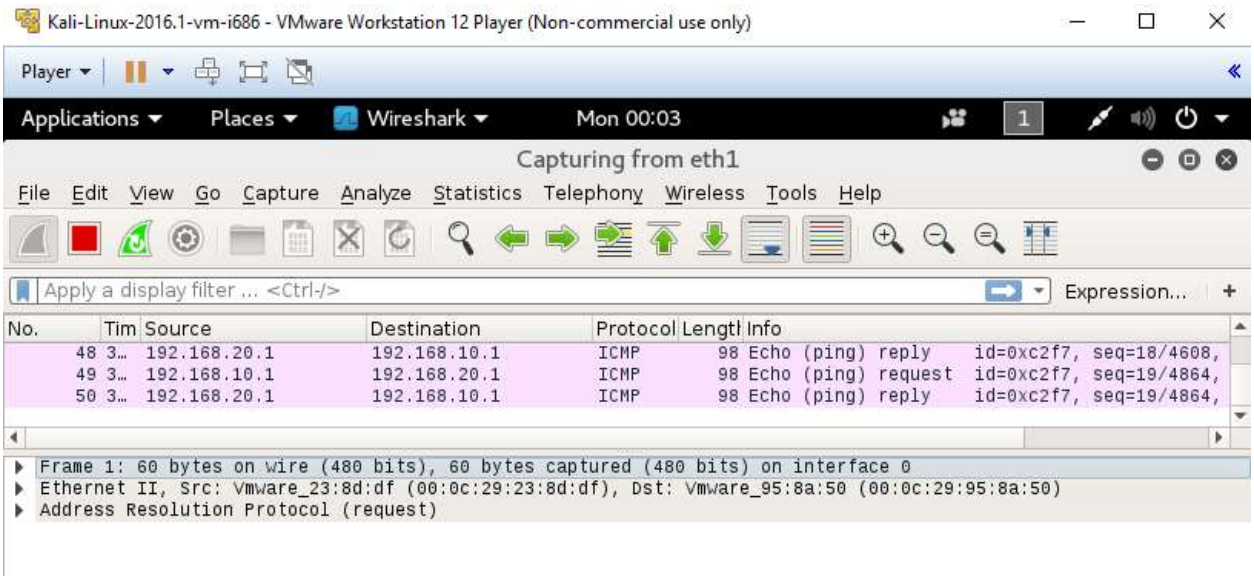
Ensure that you can ping the other VMs from all VMs as per below:-



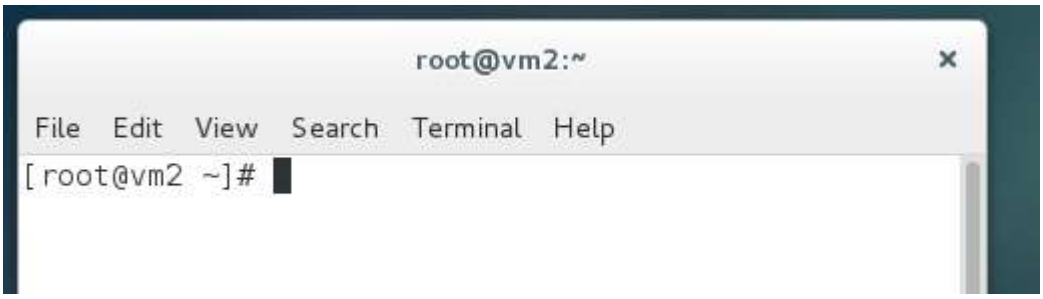

vm2 - VMware Workstation 12 Player (Non-commercial use only)
Player
Activities
Terminal
Sun 23:59
root@vm2:/etc/ipsec.d
File Edit View Search Terminal Help
[root@vm2 ipsec.d]# ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254) 56(84) bytes of data.
64 bytes from 192.168.20.254: icmp_seq=1 ttl=64 time=0.355 ms
64 bytes from 192.168.20.254: icmp_seq=2 ttl=64 time=0.299 ms
64 bytes from 192.168.20.254: icmp_seq=3 ttl=64 time=0.339 ms
^Z
[1]+ Stopped ping 192.168.20.254
[root@vm2 ipsec.d]# ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=63 time=0.646 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=63 time=0.587 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=63 time=0.600 ms
^Z
[2]+ Stopped ping 192.168.10.1
[root@vm2 ipsec.d]#


Kali-Linux-2016.1-vm-i686 - VMware Workstation 12 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Mon 00:01
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~#
root@kali:~# ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.354 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.306 ms
^X64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.283 ms
^Z
[1]+ Stopped ping 192.168.10.1
root@kali:~# ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=0.501 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=0.285 ms
^Z
[2]+ Stopped ping 192.168.20.1
root@kali:~#

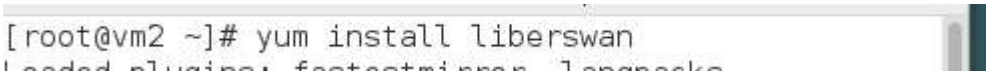
SETUP: Open Wireshark in Kali Linux. Monitor eth1 and see if you can see the ping traffic pass through the Kali Linux.



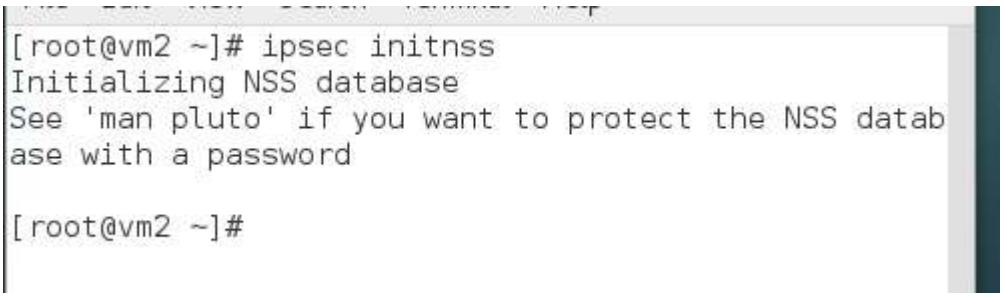
STEP: Start the terminal in VM1 and VM2.



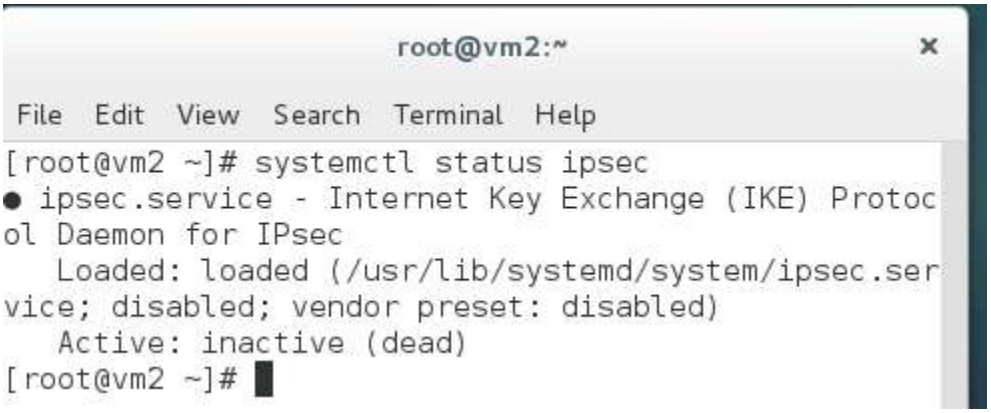
STEP: Install Libreswan (already done for you) in both VMs.



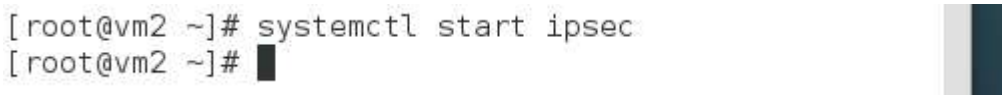
Step: Initialize a new database. If a db already exist use rm /etc/ipsec.d/*db to remove and then initialize a new one on both VMs.



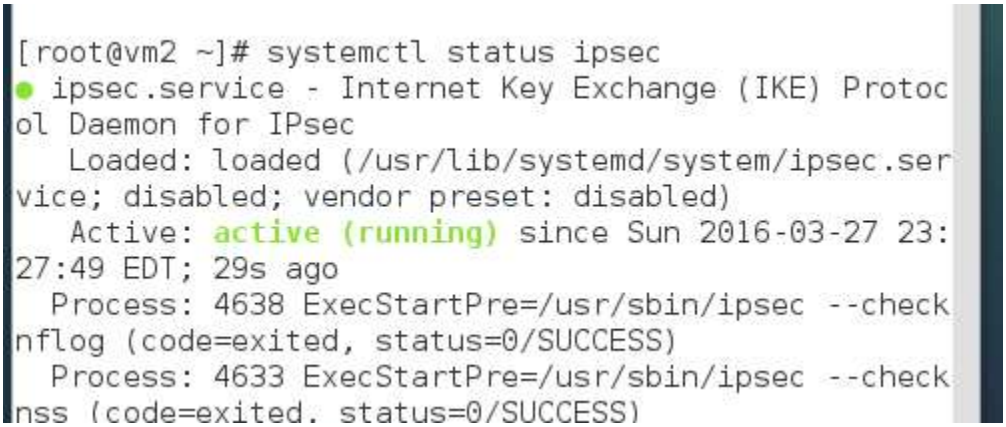
STEP: Check if IPSEC service is running on both VMs.



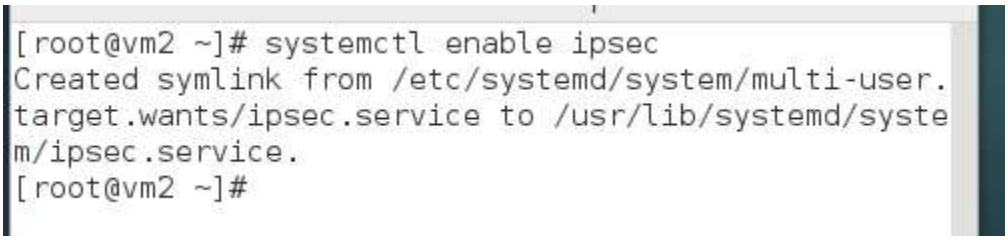
STEP: Start IPSEC Service on both VMs.



STEP: Check the status again on both VMs.



STEP: Important to add IPSEC to start on startup on both VMs.



! IMPORTANT INFO !

We are implementing HOST – to – HOST IPSEC VPN Tunnel

The two hosts are refered to as “left” and “right”.

We are going to use vm1 as the “left”.

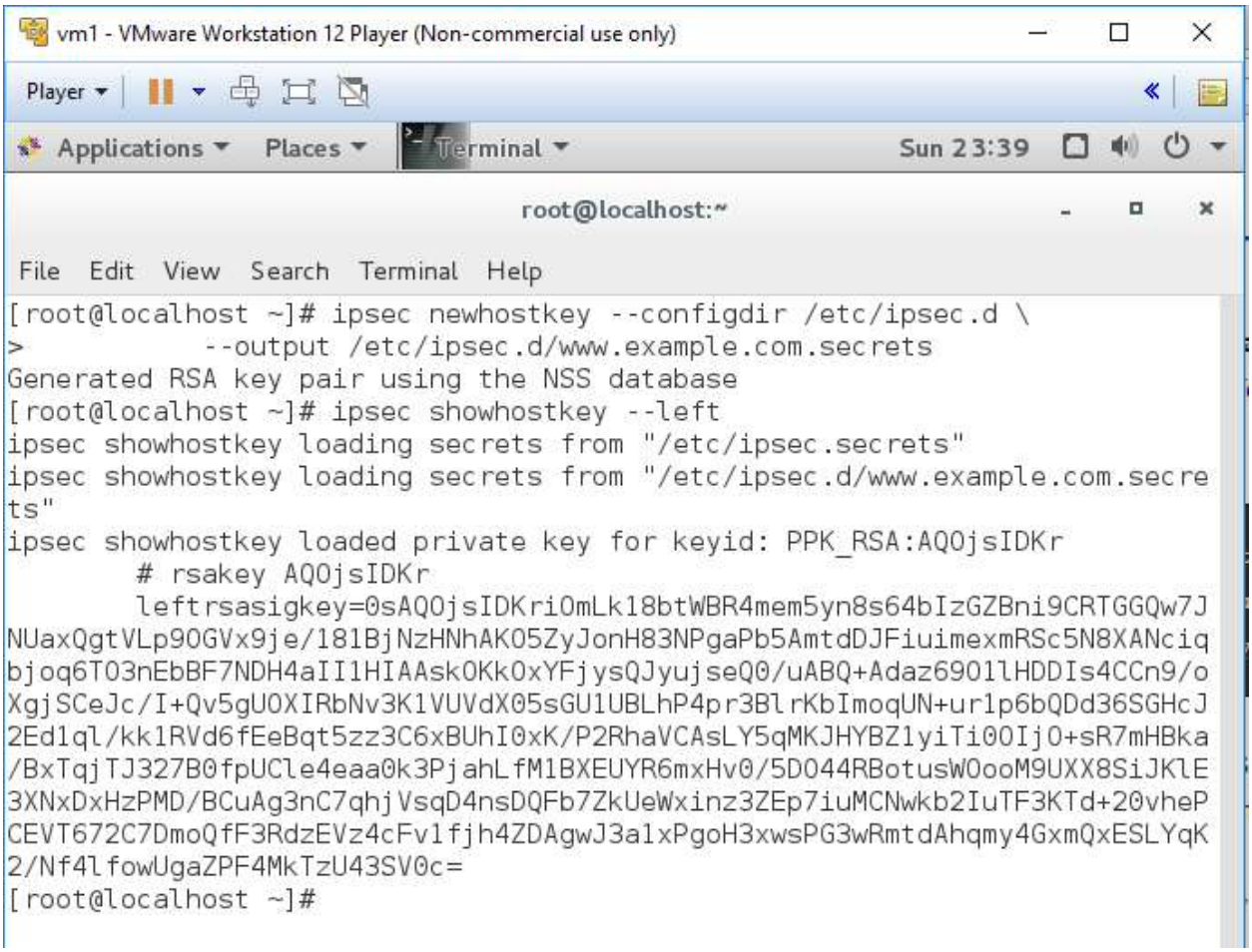
And vm2 as “right”.

STEP: Generate an rsa key for VM1 (left) as per below: -

ipsec newhostkey --configdir /etc/ipsec.d \

--output /etc/ipsec.d/www.example.com.secrets

ipsec showhostkey --left

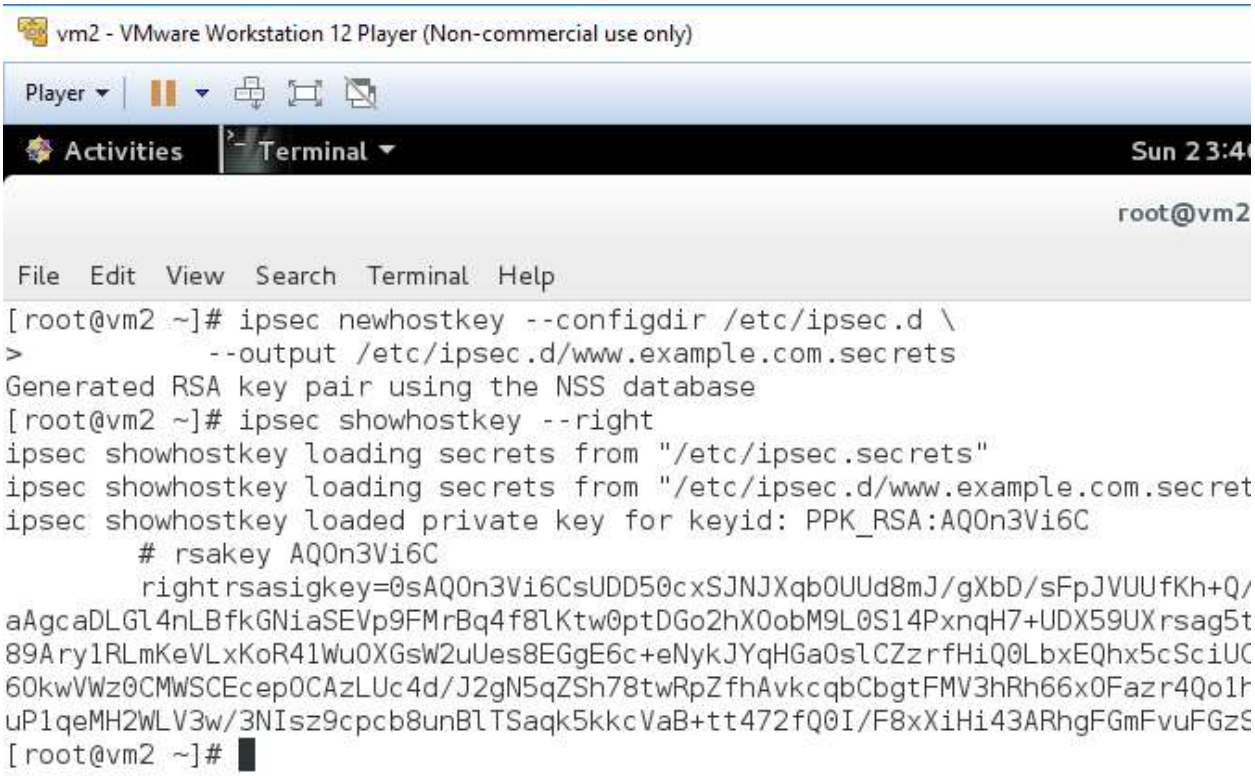


STEP: Generate rsa key for VM2 as per below: -

ipsec newhostkey --configdir /etc/ipsec.d \

--output /etc/ipsec.d/www.example.com.secrets

ipsec showhostkey –right



STEP: Create a new IPSEC config file using for favorite editor in both VMs: -

nano /etc/ipsec.d/my_host-to-host.conf

```
[root@vm2 ipsec.d]# nano /etc/ipsec.d/my_host-to-host.conf
[root@vm2 ipsec.d]#
```

STEP: In the config file we can place the IPSEC configuration info as below in both VMs: -

conn mytunnel

leftid=@west.example.com

left=192.1.2.23

leftrsasigkey=***{Paste rsa key for left as generate above}***

rightid=@east.example.com

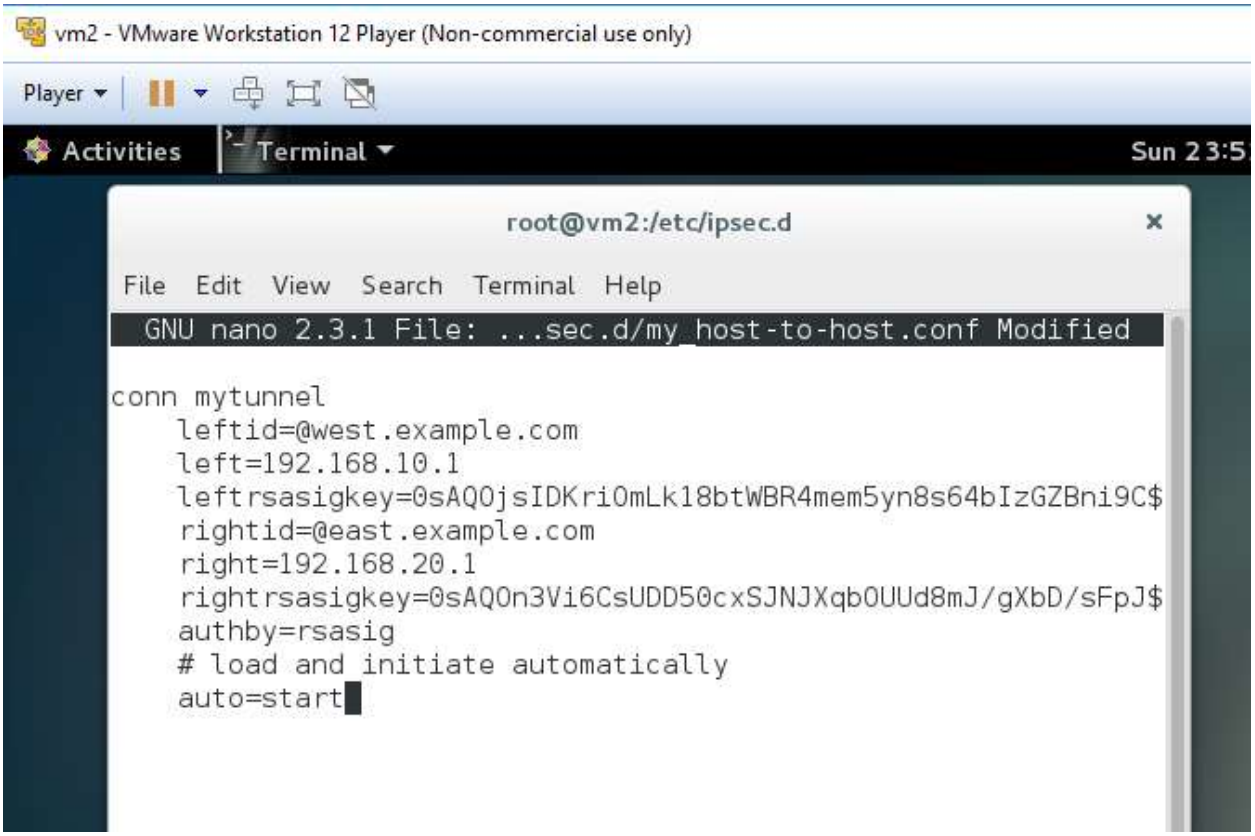
right=192.1.2.45

rightrsasigkey=***{Paste rsa key for right as generate above}***

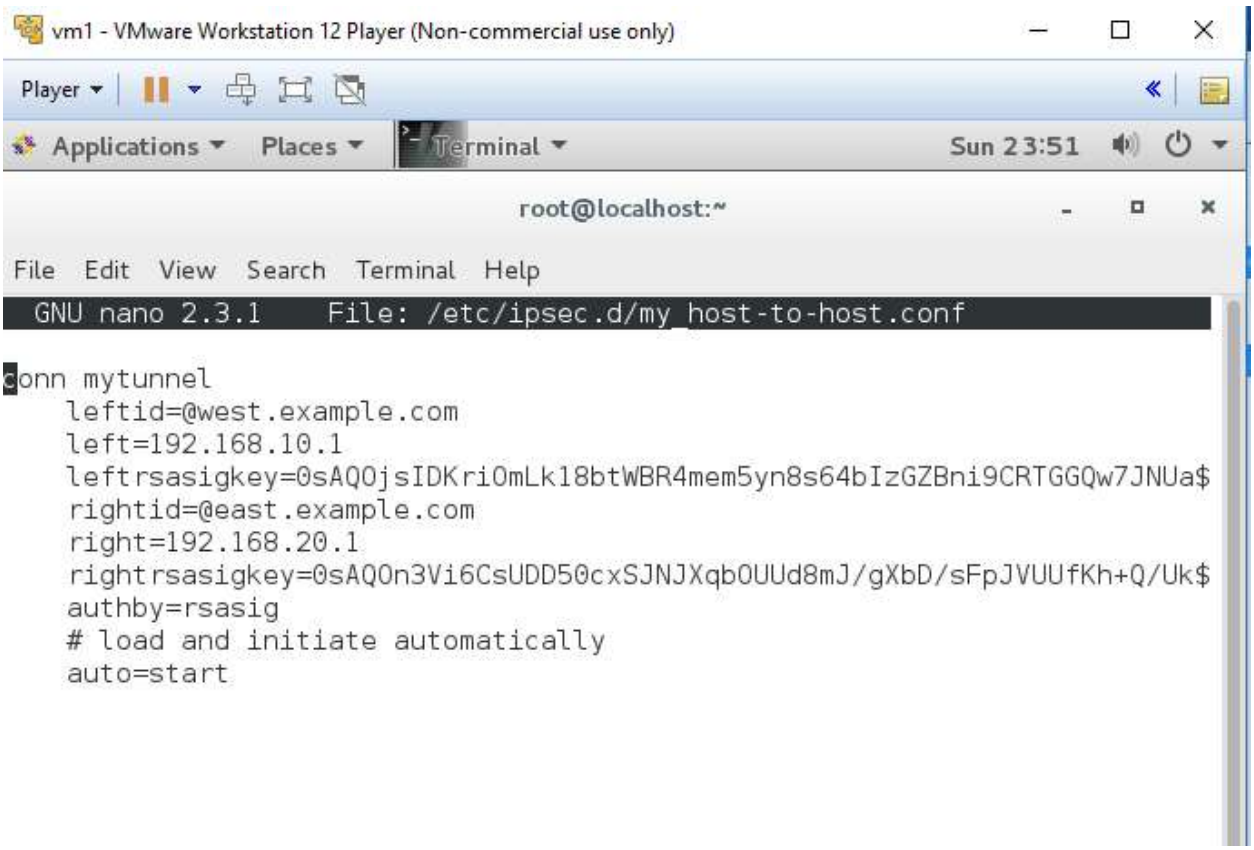
authby=rsasig

load and initiate automatically

auto=start



IMPORTANT: Ensure that both VMs have the same config file. They must be identical otherwise the SA's will fail.



BONUS: Sometimes we need to ensure that libreswan can find our custom config file. Therefore, we must ensure that the following is commented out: -

nano /etc/ipsec.conf

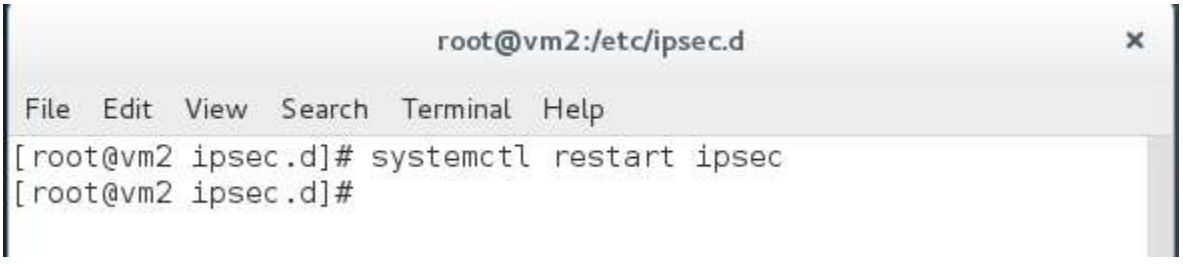
And Ensure that (should be at the end of the main config file): -

include /etc/ipsec.d/*.conf

is not commented out.

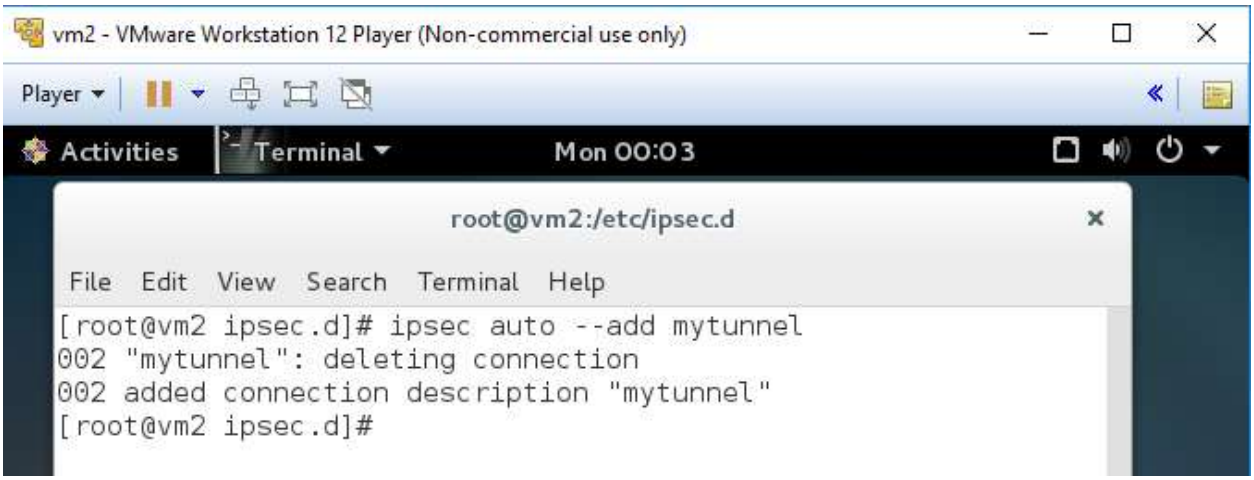
STEP: Restart the IPSEC service on both VMs so that they can pick up the config file that we created.

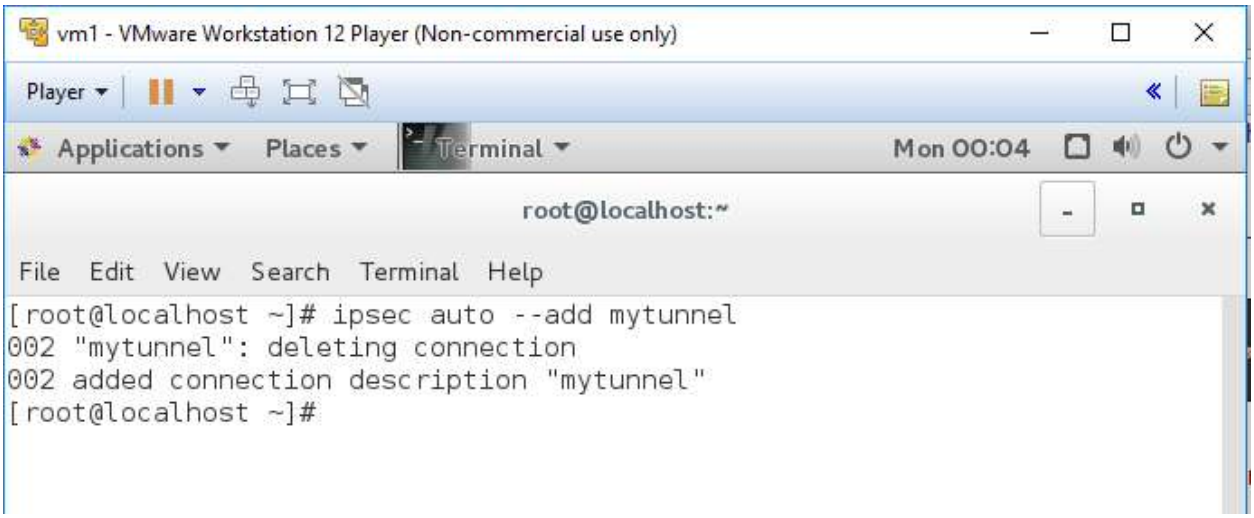
systemctl restart ipsec



STEP: On both VMs add the tunnel that we created: -

ipsec auto --add mytunnel



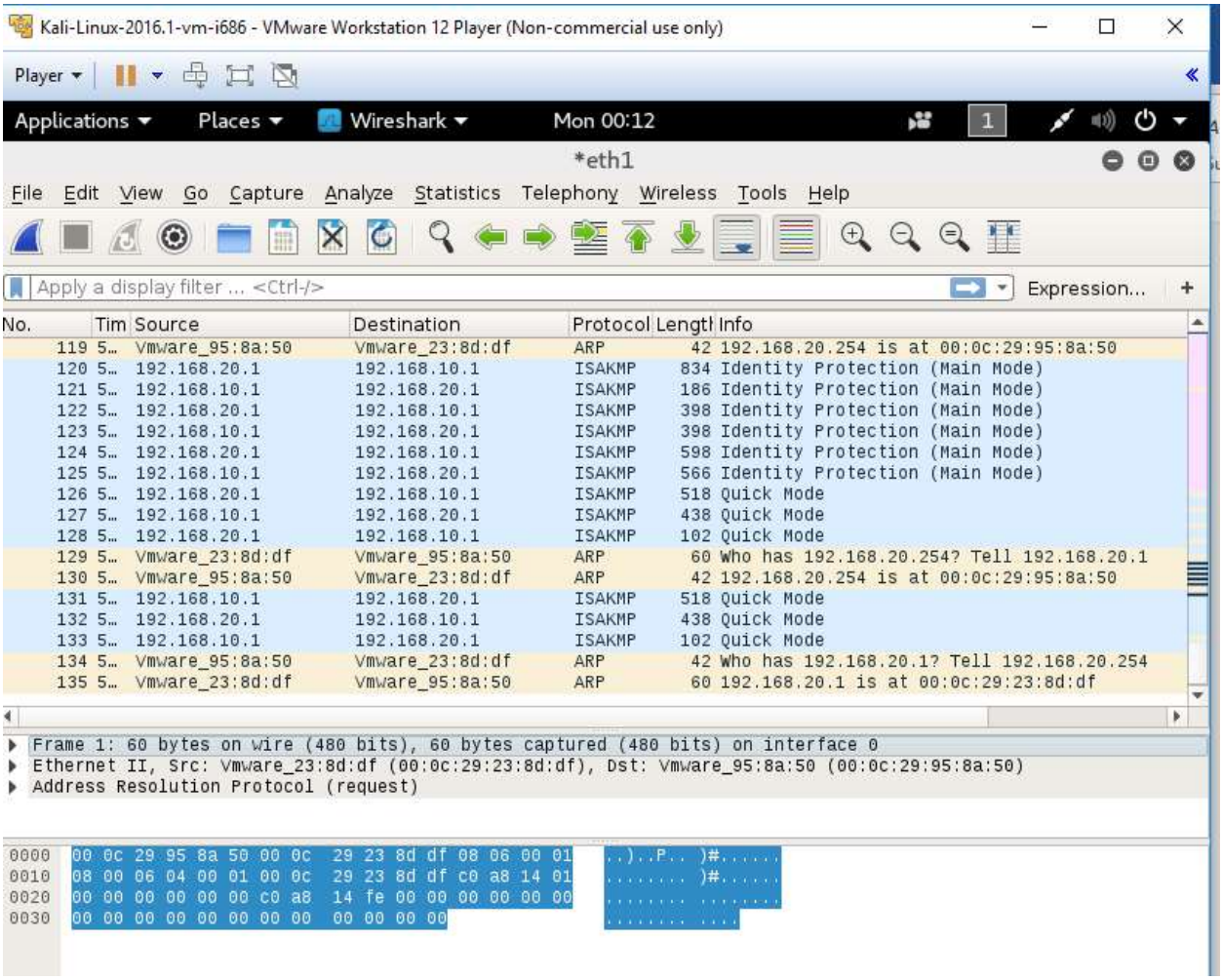


STEP: On any “ONE” of the VM turn on the connection: -

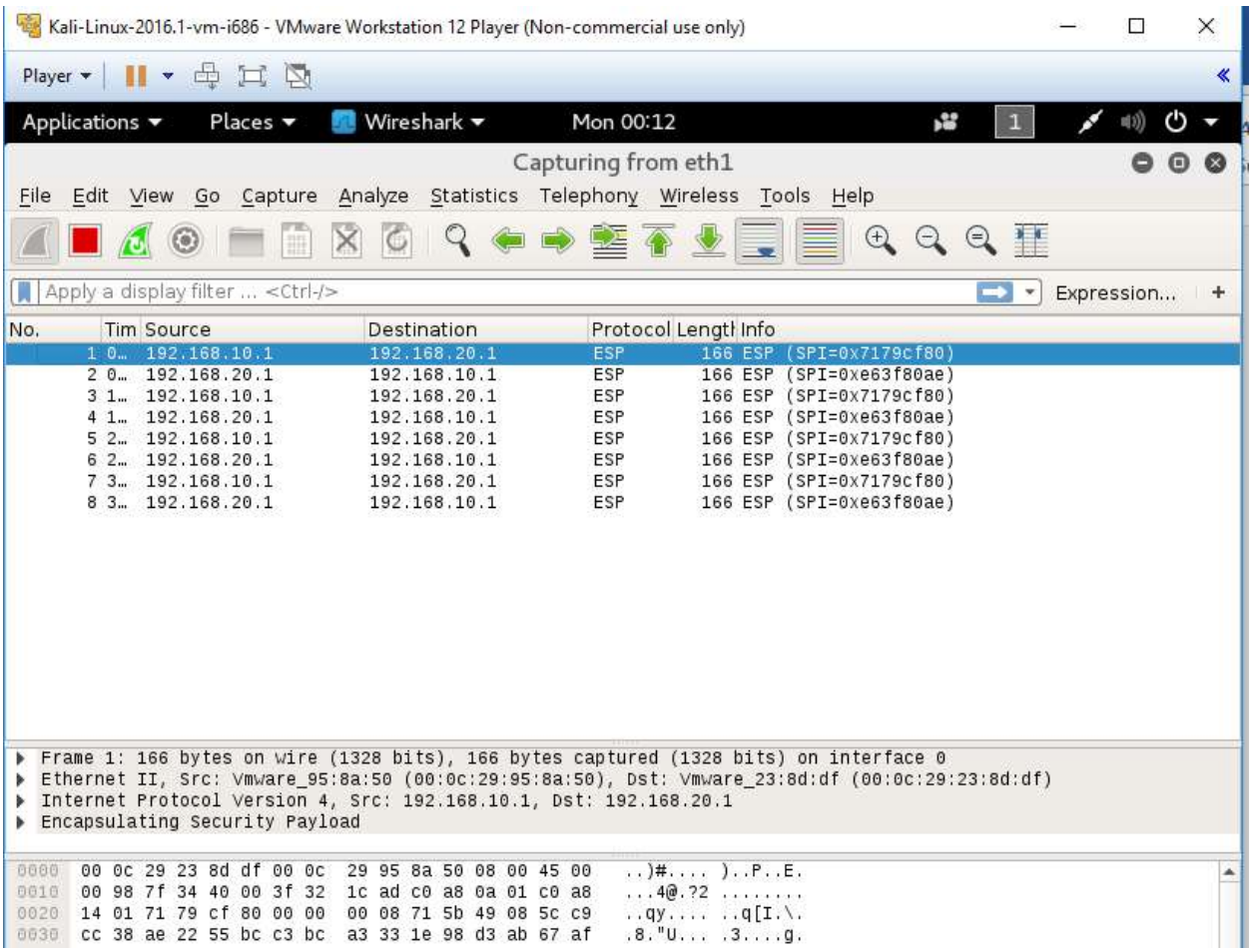
ipsec auto --up mytunnel

```
[root@vm2 ipsec.d]# ipsec auto --up mytunnel
002 "mytunnel" #4: initiating Main Mode
104 "mytunnel" #4: STATE_MAIN_I1: initiate
003 "mytunnel" #4: received Vendor ID payload [Dead Peer Detect
ion]
003 "mytunnel" #4: received Vendor ID payload [FRAGMENTATION]
003 "mytunnel" #4: received Vendor ID payload [RFC 3947]
002 "mytunnel" #4: enabling possible NAT-traversal with method
RFC 3947 (NAT-Traversal)
002 "mytunnel" #4: transition from state STATE_MAIN_I1 to state
 STATE_MAIN_I2
106 "mytunnel" #4: STATE_MAIN_I2: sent MI2, expecting MR2
003 "mytunnel" #4: NAT-Traversal: Result using RFC 3947 (NAT-Tr
aversal) sender port 500: no NAT detected
002 "mytunnel" #4: transition from state STATE_MAIN_I2 to state
 STATE_MAIN_I3
108 "mytunnel" #4: STATE_MAIN_I3: sent MI3, expecting MR3
003 "mytunnel" #4: received Vendor ID payload [CAN-IKEv2]
```

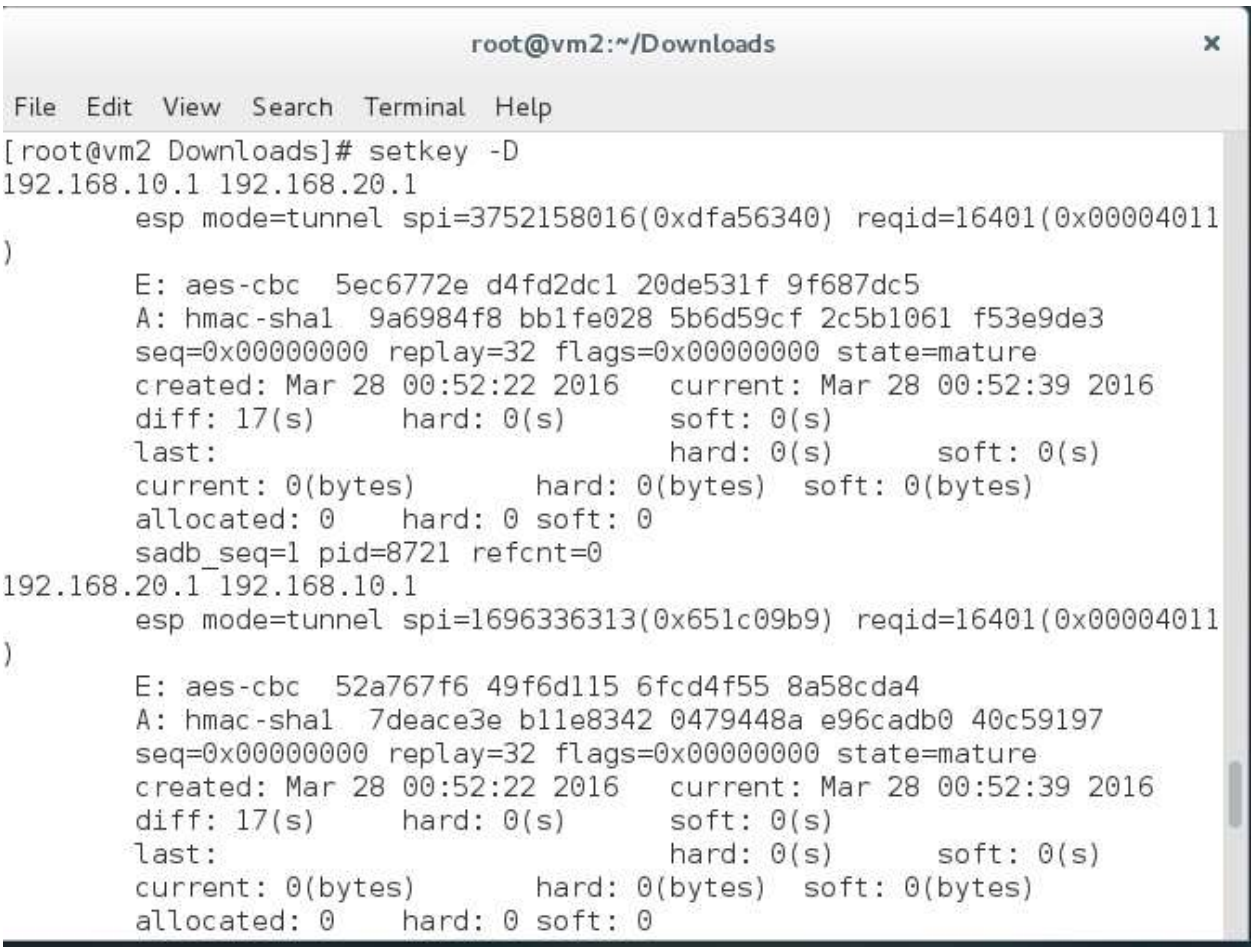
IMPORTANT: In Wireshark on Kali Linux you will see ISAKMP connection packets establishing the IPSEC tunnel. Please ensure that you stop once you see these packets and explore them.



STEP: Ping from either VM1 or VM2 and you can observe that in Kali linux you can see the ESP encrypted packets:



STEP: you can use setkey -D in both VMs to view the Security Association DB as below:-



Links:-

IP SEC Tools:-

http://ipsec-tools.sourceforge.net/

How to use IPSEC Tools:-

http://www.mad-hacking.net/documentation/linux/networking/ipsec/installation.xml

libreswan:-

https://libreswan.org/

Oakley:-

https://tools.ietf.org/html/rfc2412