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/csc427/

- VM1 | Centos 7 - VM2 | Centos 7

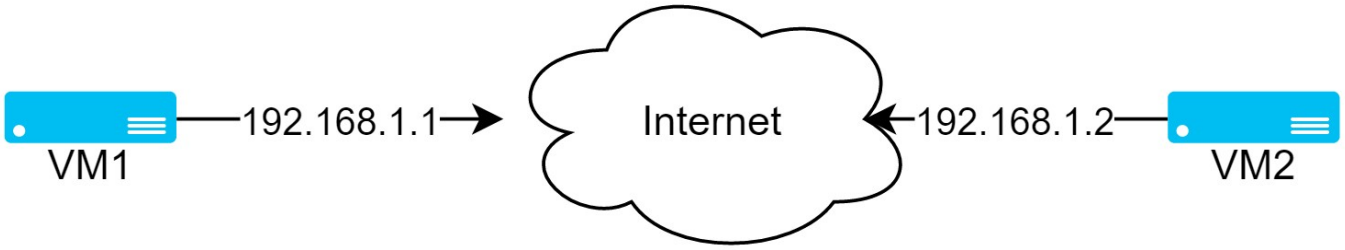
If you do not see the files use the following cmd:-

scp -r [UTORID]@dh2020pc07.utm.utoronto.ca:/virtual/ipsec /virtual/ipsec

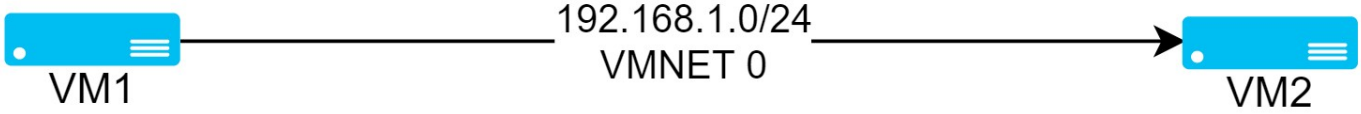
Required Software: Already installed for you on the VMs: -

- IPSEC Tools - WireShark - libreswan

Scenario



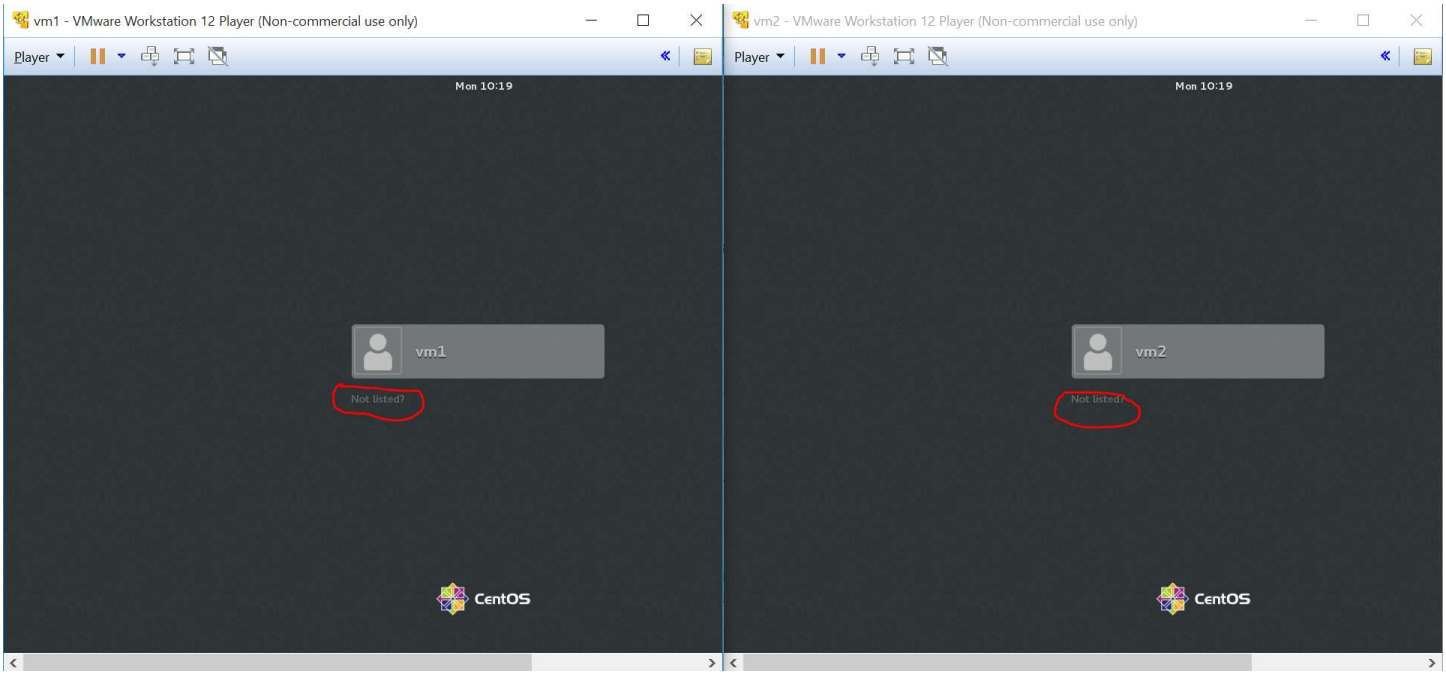
How we emulate this: -



VM access details: -

- VM1: root/root
- VM2: root/root

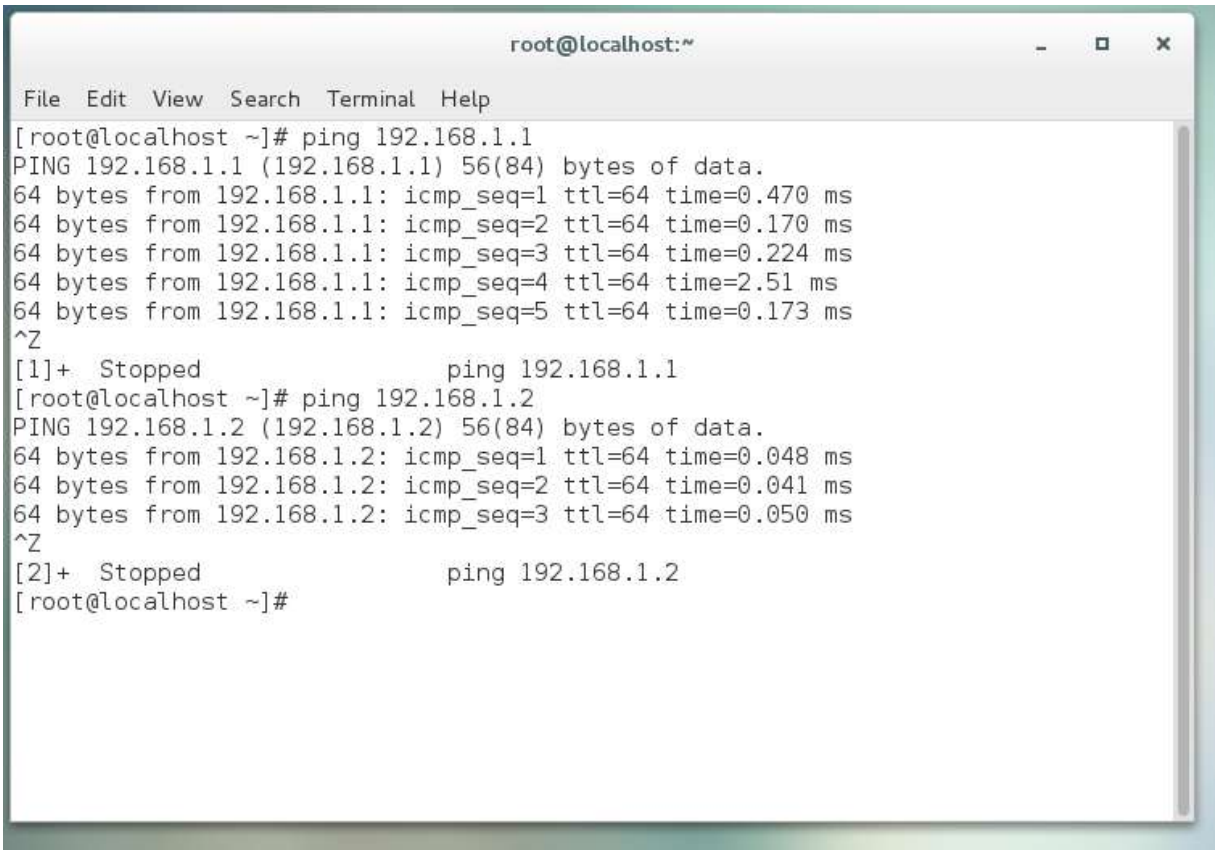
SETUP: Please turn on both VMs and login as root.



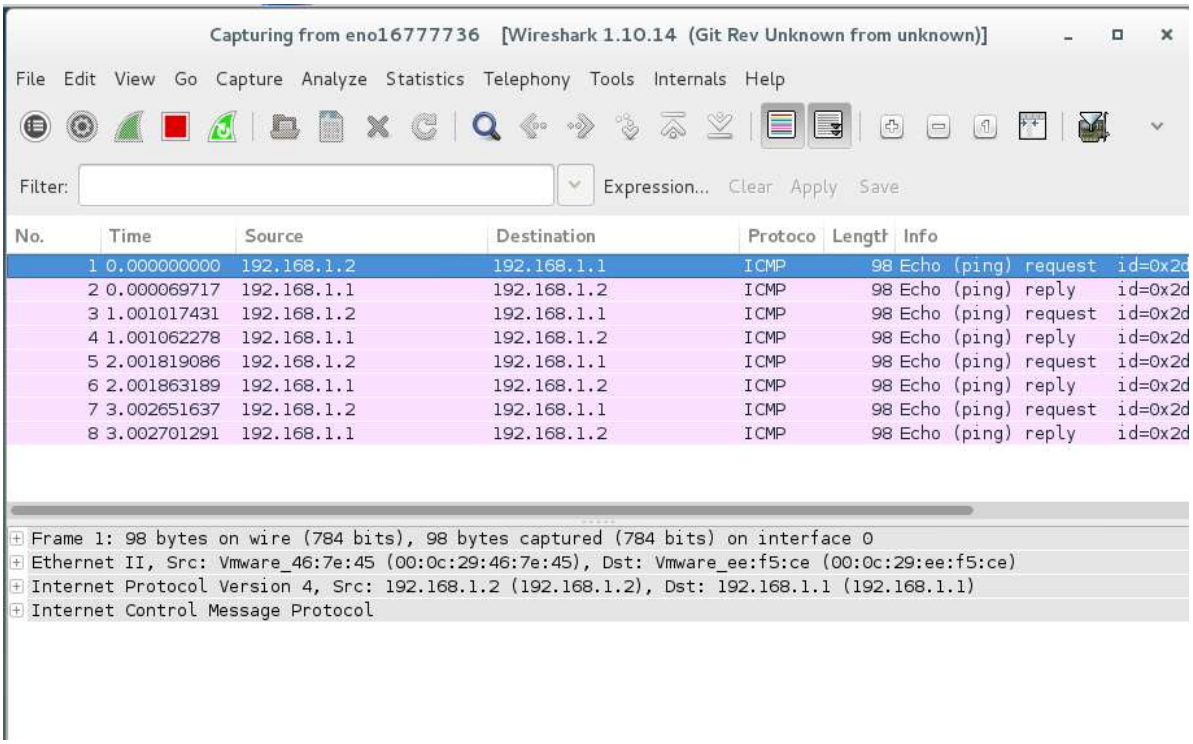
SETUP: Make sure that the VMs have the correct IPs as below:

- VM1: 192.168.1.1 | 255.255.255.0
- VM2: 192.168.1.2 | 255.255.255.0

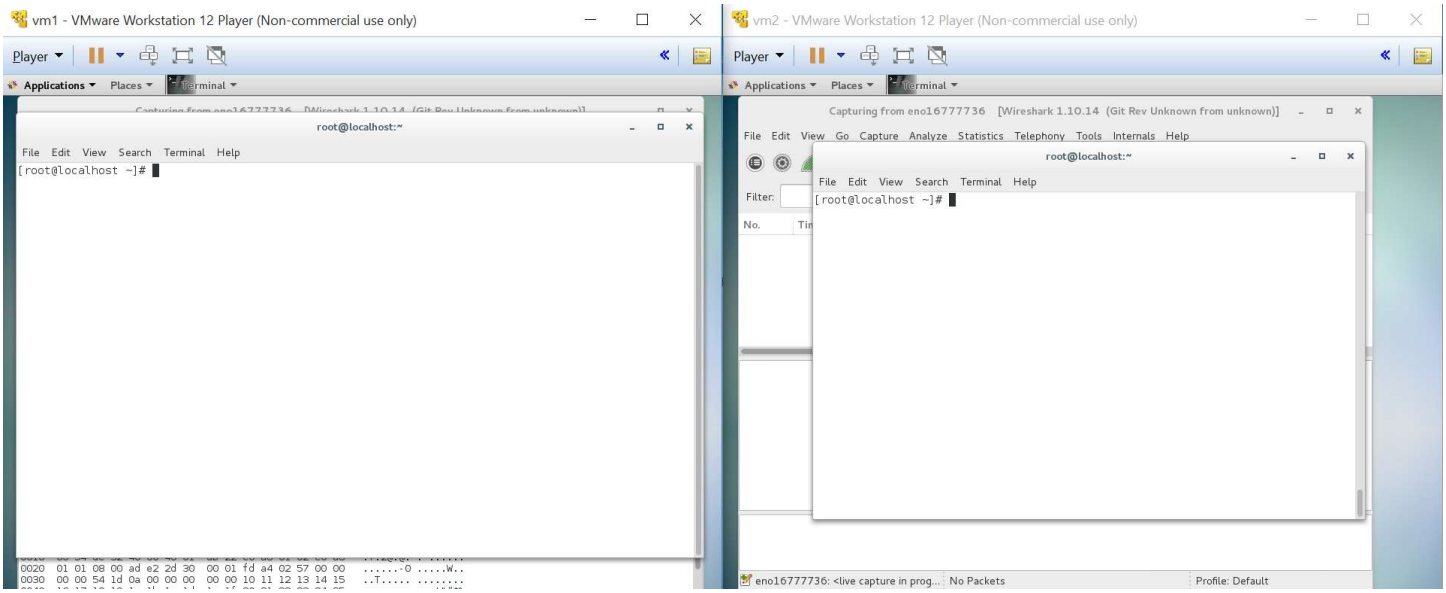
SETUP: Ensure that you can ping the other VMs from all VMs as per below:-



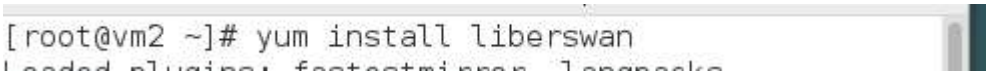
SETUP: Open Wireshark in vm2 and start capturing on the interface.



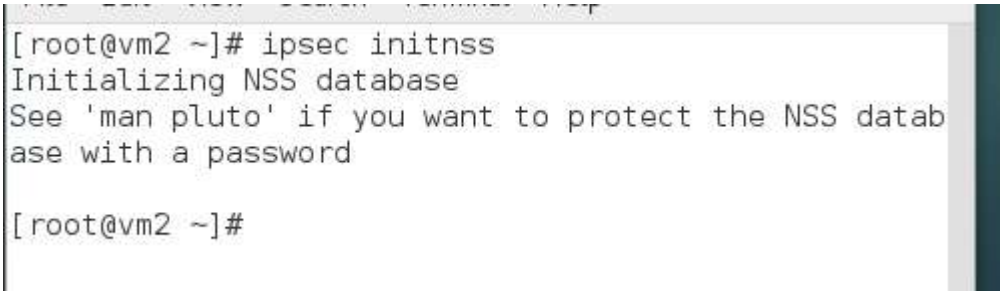
STEP: Start the terminal in both VMs.



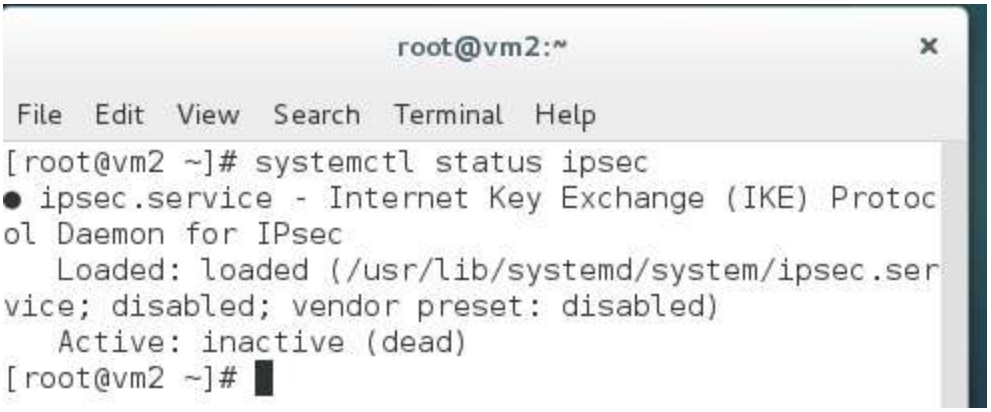
STEP: Install Libreswan (already done for you) in both VMs.



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.

```
[root@vm2 ~]# systemctl start ipsec
[root@vm2 ~]#
```

STEP: Check the status again on both VMs.

```
[root@vm2 ~]# systemctl status ipsec
● ipsec.service - Internet Key Exchange (IKE) Protoc
ol Daemon for IPsec
   Loaded: loaded (/usr/lib/systemd/system/ipsec.ser
vice; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2016-03-27 23:
27:49 EDT; 29s ago
  Process: 4638 ExecStartPre=/usr/sbin/ipsec --check
nflog (code=exited, status=0/SUCCESS)
  Process: 4633 ExecStartPre=/usr/sbin/ipsec --check
nss (code=exited, status=0/SUCCESS)
```

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

```
[root@vm2 ~]# systemctl enable ipsec
Created symlink from /etc/systemd/system/multi-user.
target.wants/ipsec.service to /usr/lib/systemd/syste
m/ipsec.service.
[root@vm2 ~]#
```

! 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”.

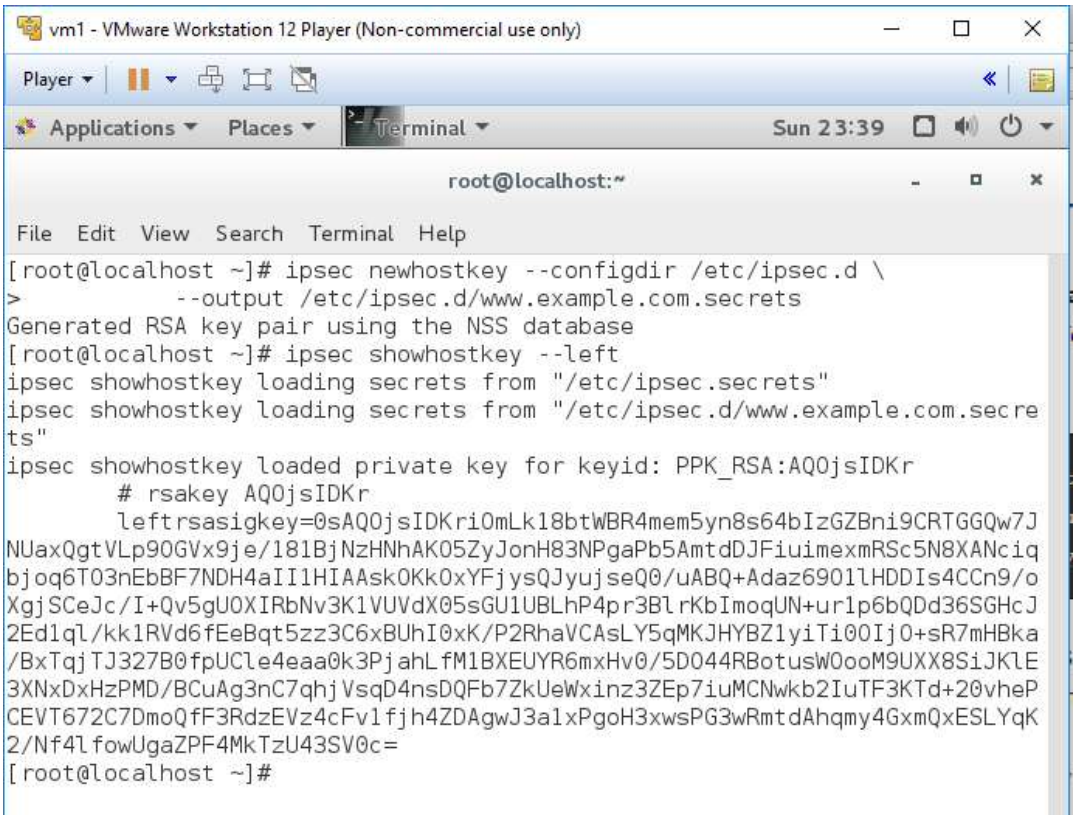
And vm2 as “right”.

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

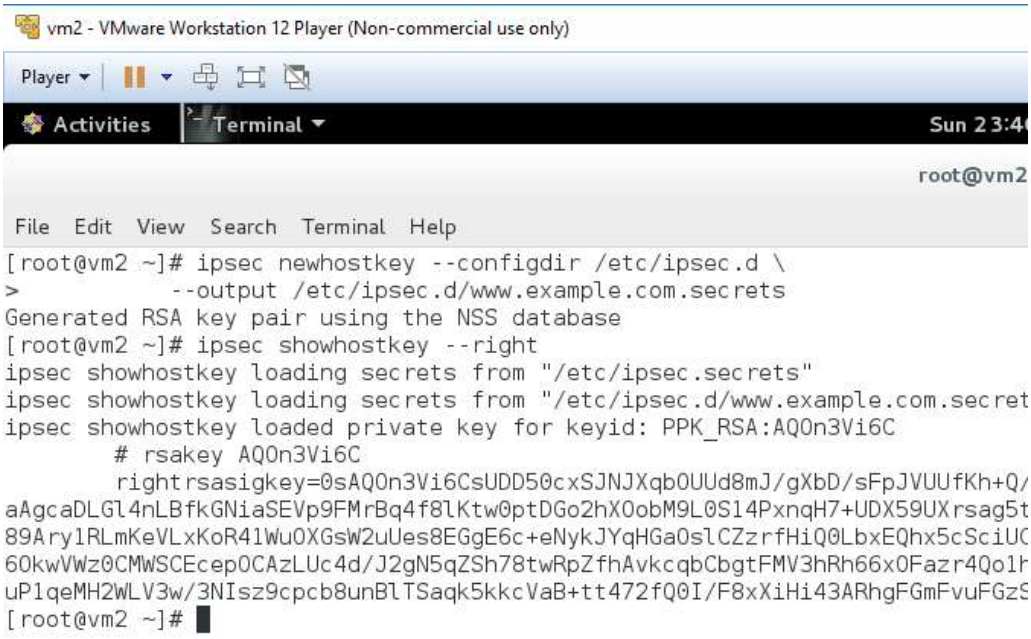


STEP: Generate rsa key for VM2 as per below: -

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

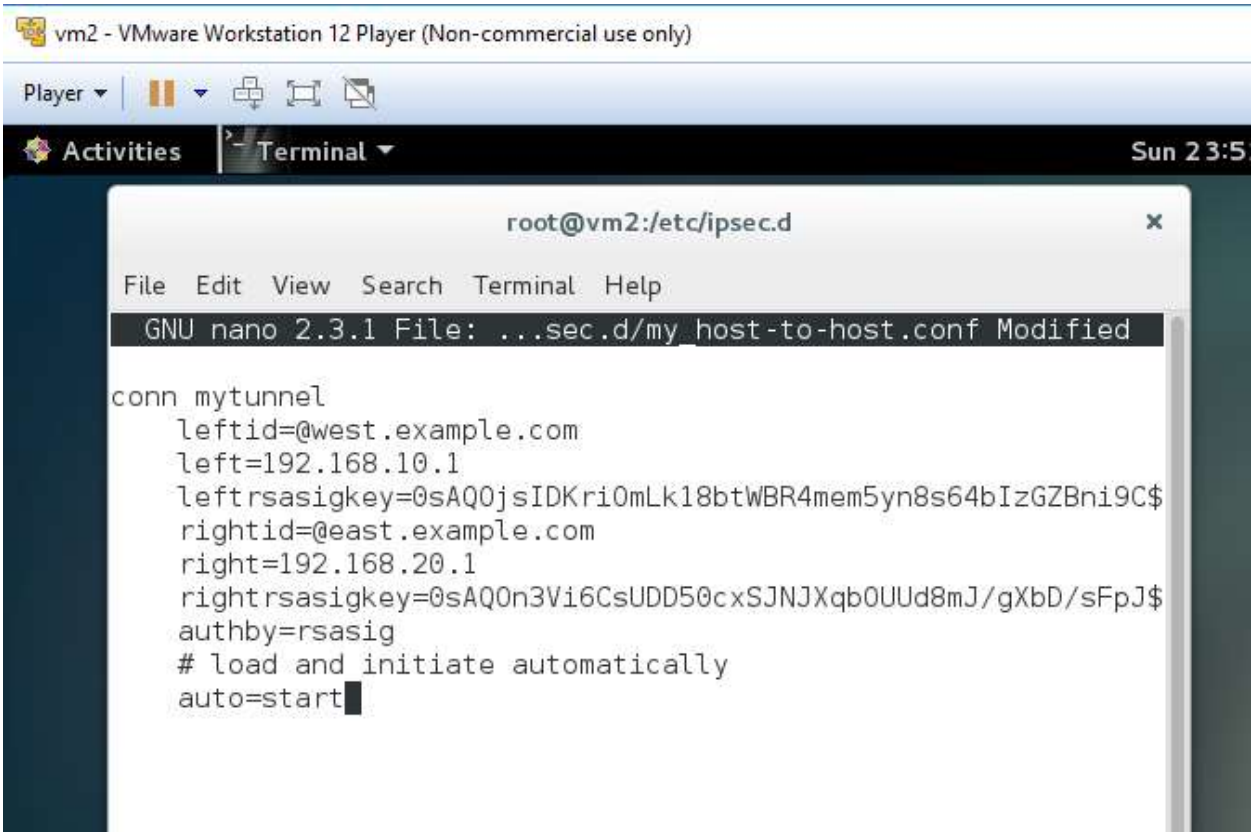
right=192.1.2.45

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

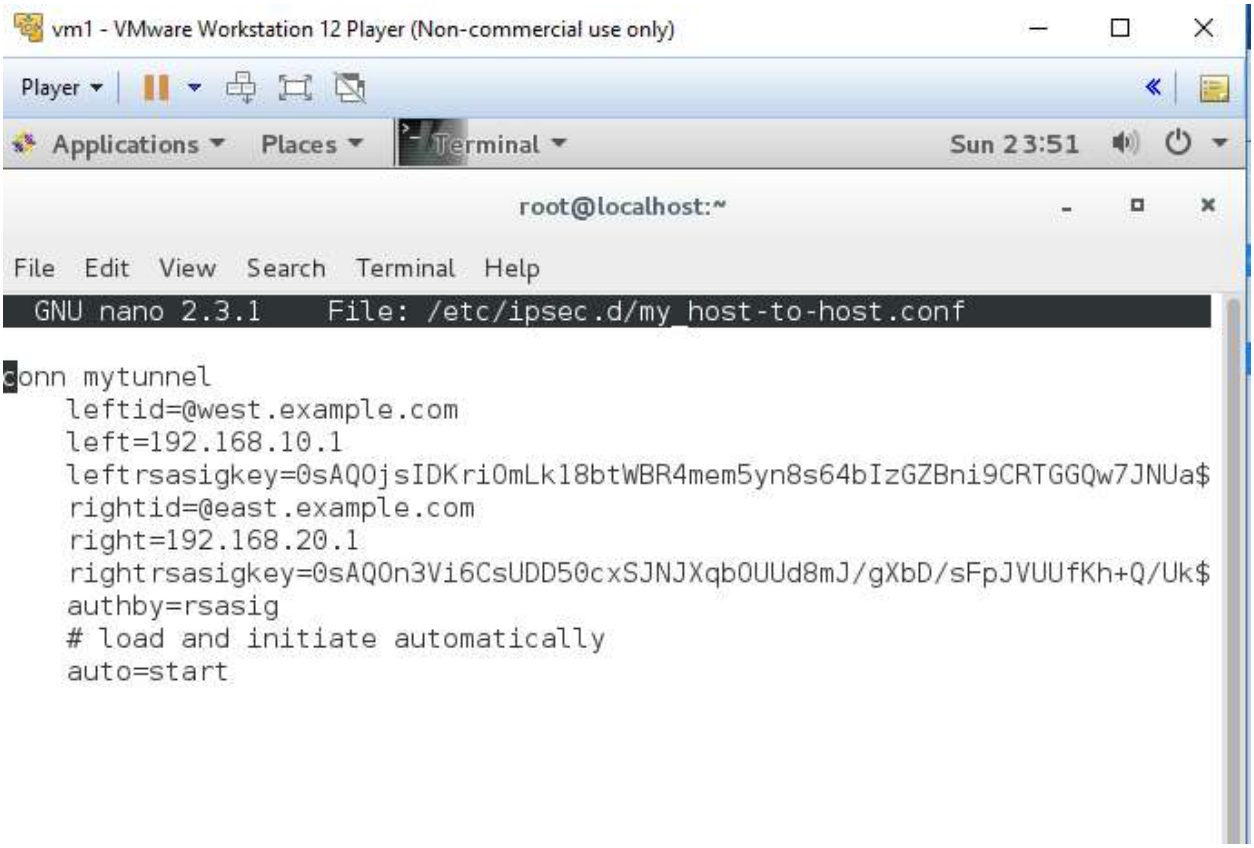
authby=rsasig

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

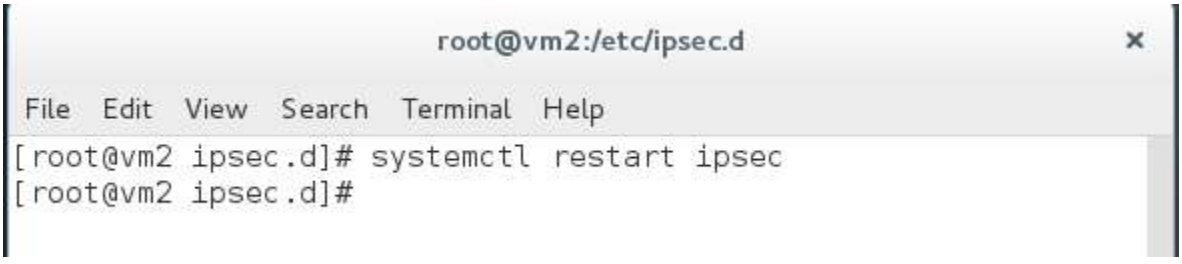
And Ensure that (should be at the end of the main config file): -

include /etc/ipsec.d/*.conf

is not commented out.

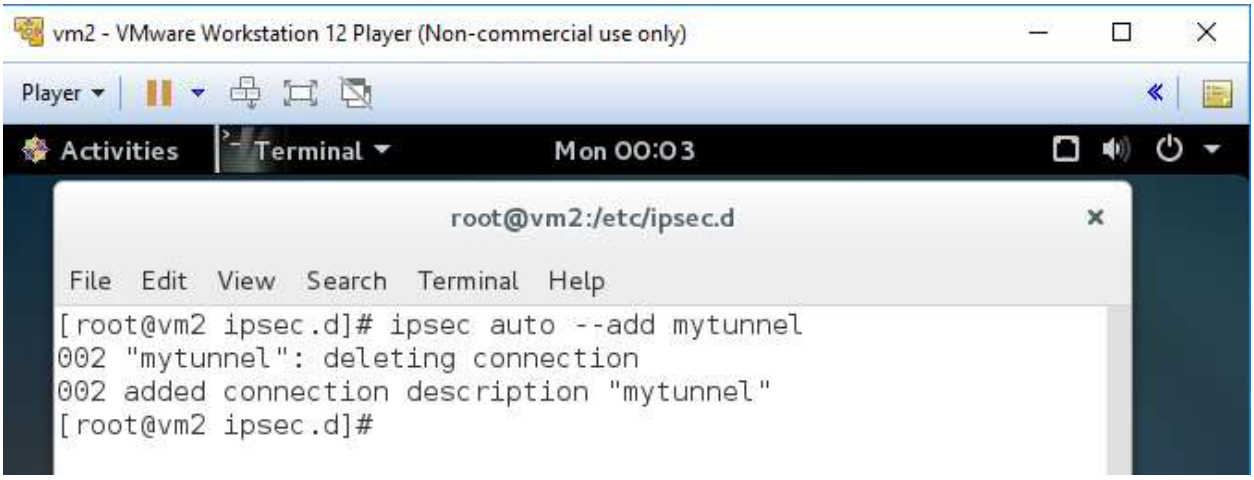
STEP: Restart the IPSEC service on both VMs so that they can pick up the config file that we created.

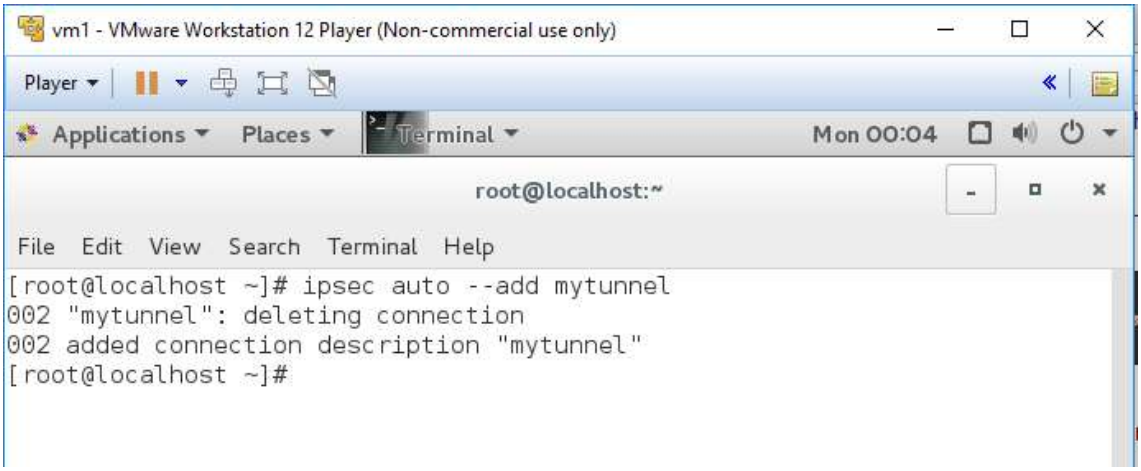
systemctl restart ipsec



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

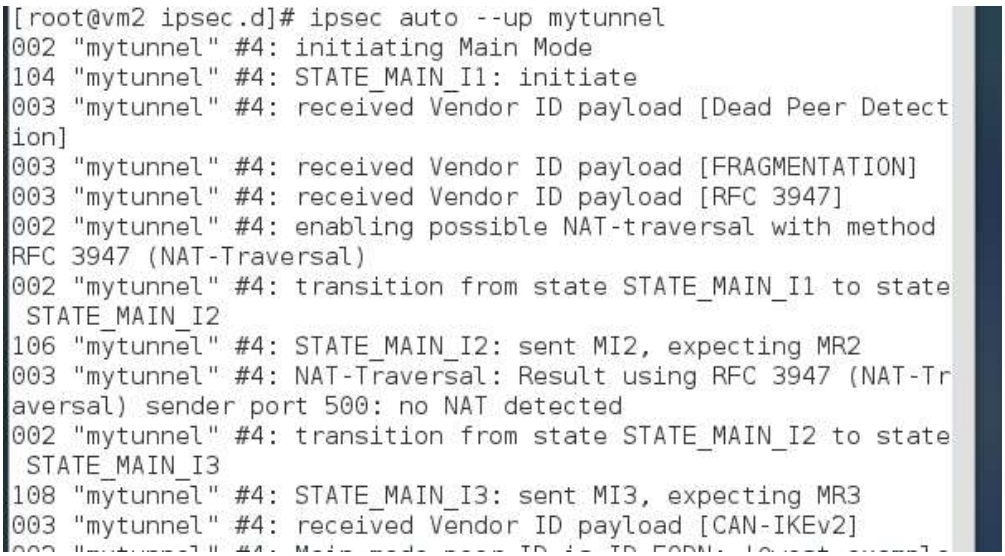
ipsec auto --add mytunnel



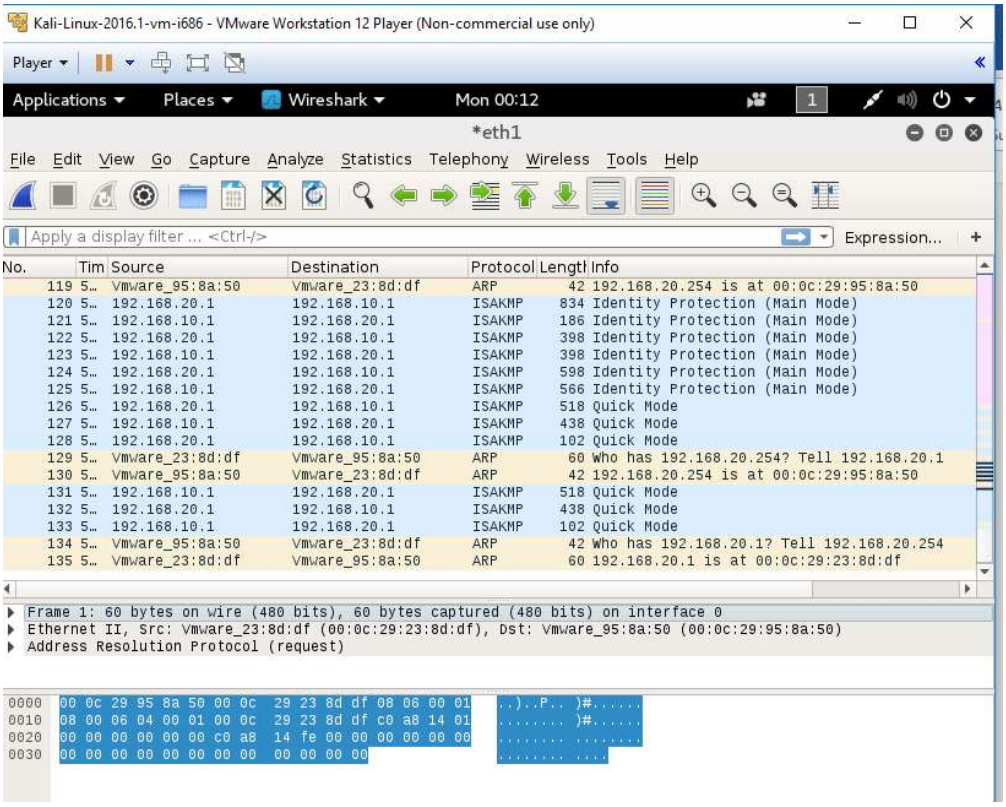


STEP: On any “ONE” of the VM turn on the connection: -

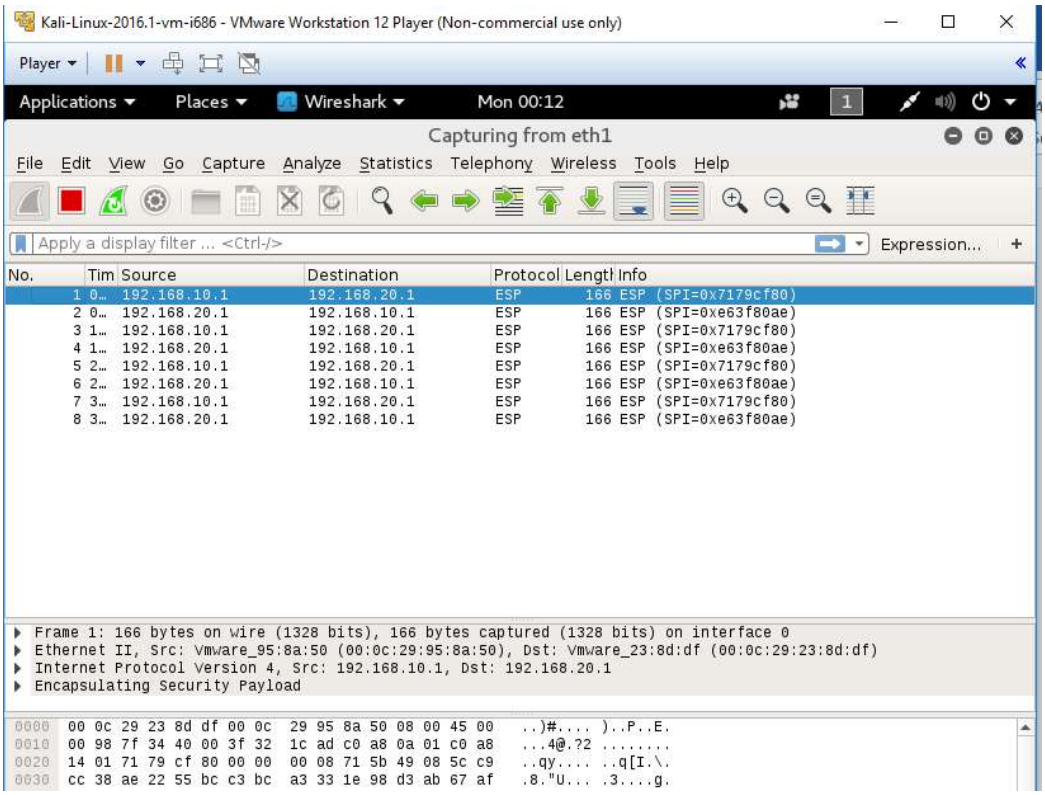
ipsec auto --up mytunnel



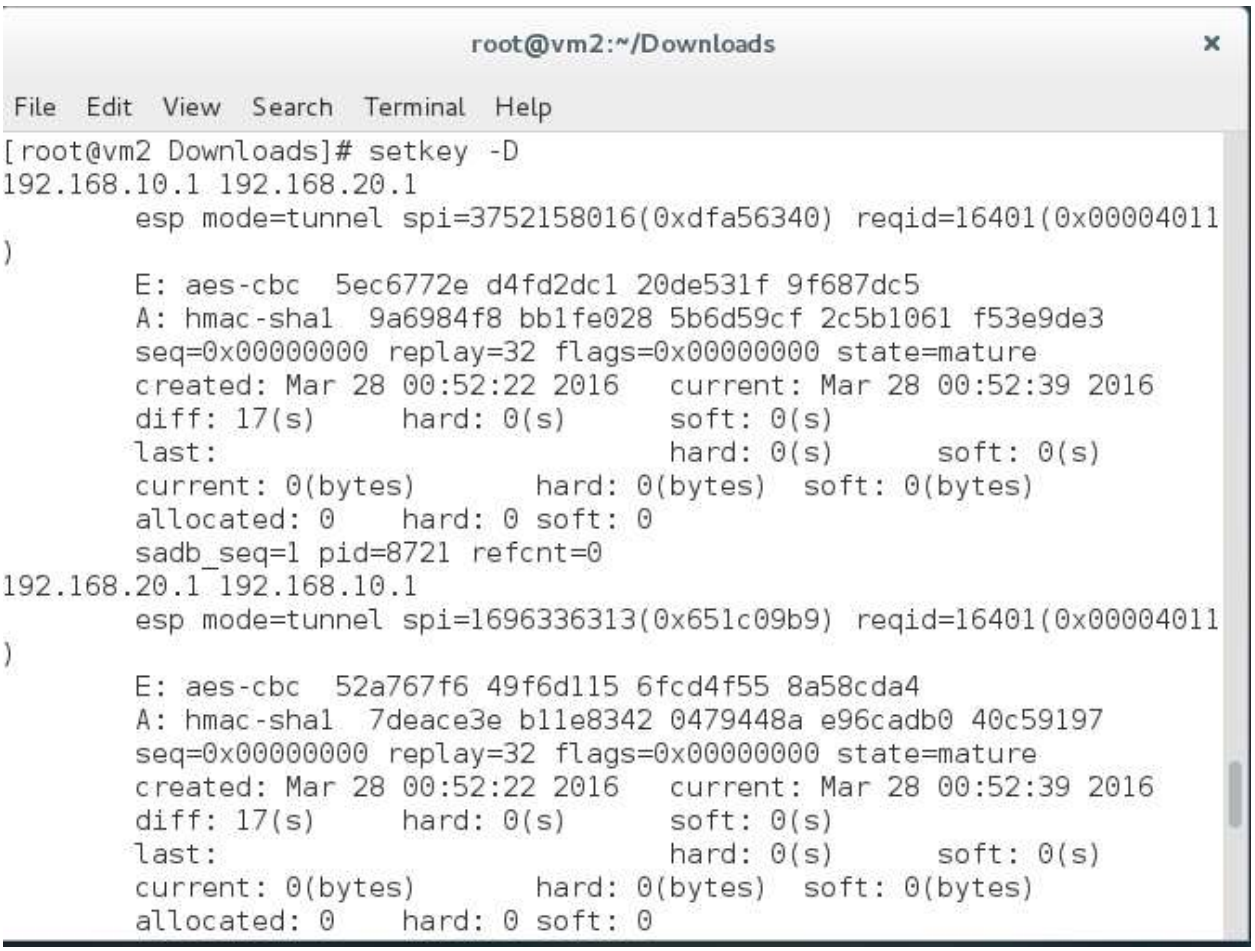
IMPORTANT: In Wireshark on VM2 you will see ISAKMP connection packets establishing the IPSEC tunnel. Please ensure that you stop once you see these packets and explore them.



STEP: Ping from either VM1 or VM2 and you can observe 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