



## Department of Information Technology

Semester: V

Academic Year: 2022-23

Class / Branch: TE IT A

Subject: Security Lab (SL)

Name of Instructor: Prof. Apeksha Mohite

Name of Student: Vishal Bangar

Student ID: 20104084

### EXPERIMENT NO. 9

Aim: To study and implement IPSEC in Linux .

#### Installing IPSEC

```
apsit@apsit-HP-280-G3-MT: ~  
File Edit View Search Terminal Help  
apsit@apsit-HP-280-G3-MT:~$ sudo apt-get install ipsec-tools strongswan-starter  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
ipsec-tools is already the newest version (1:0.8.2+20140711-10build1).  
strongswan-starter is already the newest version (5.6.2-1ubuntu2.8).  
The following package was automatically installed and is no longer required:  
  libxcb-xinerama0-dev  
Use 'sudo apt autoremove' to remove it.  
0 upgraded, 0 newly installed, 0 to remove and 273 not upgraded.  
apsit@apsit-HP-280-G3-MT:~$
```

sudo gedit ipsec.conf

```
apsit@apsit-HP-280-G3-MT: /etc  
File Edit View Search Terminal Help  
apsit@apsit-HP-280-G3-MT:~$ cd /etc  
apsit@apsit-HP-280-G3-MT:/etc$ sudo gedit ipsec.conf  
^@
```



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



```
Open ▾ ipsec.conf /etc Save
# strictipsecpolicy=yes
# uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#   leftsubnet=10.1.0.0/16
#   leftcert=selfCert.der
#   leftsendcert=never
#   right=192.168.0.2
#   rightsubnet=10.2.0.0/16
#   rightcert=peerCert.der
#   auto=start

#conn sample-with-ca-cert
#   leftsubnet=10.1.0.0/16
#   leftcert=myCert.pem
#   right=192.168.0.2
#   rightsubnet=10.2.0.0/16
#   rightid="C=CH, O=Linux strongSwan CN=peer name"
#   auto=start

conn blue-to-red
    authby=secret
    auto=route
    keyexchange=ikev2
    ike=aes128-md5-modp1024
    left=192.168.87.13
    right=192.168.87.14
    type=transport
    ah=aes128-sha-modp1024!|

Plain Text ▾ Tab Width: 8 ▾ Ln 38, Col 32 ▾ INS
```

```
apsit@apsit-HP-280-G3-MT: /etc
File Edit View Search Terminal Help
apsit@apsit-HP-280-G3-MT:~$ cd /etc
apsit@apsit-HP-280-G3-MT:/etc$ sudo gedit ipsec.secrets
[sudo] password for apsit:

Open ▾ ipsec.secrets /etc Save
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.
192.168.87.13 192.168.87.14 : PSK "test123"

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS
```



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



sudo ipsec up connection name

```
apsit@apsit-HP-280-G3-MT: /etc
File Edit View Search Terminal Help
apsit@apsit-HP-280-G3-MT:/etc$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
apsit@apsit-HP-280-G3-MT:/etc$ sudo ipsec up blue-to-red
establishing CHILD_SA blue-to-red{4}
generating CREATE_CHILD_SA request 0 [ N(USE_TRANSP) SA No KE TSr TSr ]
sending packet: from 192.168.87.14[4500] to 192.168.87.13[4500] (332 bytes)
received packet: from 192.168.87.13[4500] to 192.168.87.14[4500] (332 bytes)
parsed CREATE_CHILD_SA response 0 [ N(USE_TRANSP) SA No KE TSr TSr ]
CHILD_SA blue-to-red{4} established with SPIs c111ce18_i c3acc71e_o and TS 192.1
68.87.14/32 === 192.168.87.13/32
connection 'blue-to-red' established successfully
apsit@apsit-HP-280-G3-MT:/etc$
```

with different password:

```
apsit@apsit-HP-280-G3-MT: /etc
File Edit View Search Terminal Help
apsit@apsit-HP-280-G3-MT:/etc$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
apsit@apsit-HP-280-G3-MT:/etc$ sudo ipsec up blue-to-red
initiating IKE_SA blue-to-red[1] to 192.168.87.13
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP)
) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.87.14[500] to 192.168.87.13[500] (1002 bytes)
received packet: from 192.168.87.13[500] to 192.168.87.14[500] (334 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N
(HASH_ALG) N(MULT_AUTH) ]
authentication of '192.168.87.14' (myself) with pre-shared key
establishing CHILD_SA blue-to-red{2}
generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH N(USE_TRANSP) SA TS
i TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
sending packet: from 192.168.87.14[4500] to 192.168.87.13[4500] (252 bytes)
received packet: from 192.168.87.13[4500] to 192.168.87.14[4500] (76 bytes)
parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
received AUTHENTICATION_FAILED notify error
establishing connection 'blue-to-red' failed
apsit@apsit-HP-280-G3-MT:/etc$
```





PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
(All Branches NBA Accredited)



By wireshark

Wireshark packet capture analysis showing a Multicast Domain Name System (response) packet.

Packet 650: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface 0

Ethernet II, Src: HewlettP.af:0c:66 (18:60:24:af:0c:66), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)

Internet Protocol Version 4, Src: 192.168.87.13, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (response)

No.	Time	Source	Destination	Protocol	Length	Info
650	9.744100680	fe80::2c8f:9f38:f32...	ff02::fb	MDNS	124	Standard query 0x0000 SRV HP LaserJet M203dn (5c629e)..._ipps._tcp.local, "QM" question
658	9.743719353	192.168.2.91	224.0.0.251	MDNS	104	Standard query 0x0000 SRV HP LaserJet M203dn (5c629e)..._ipps._tcp.local, "QM" question
656	9.661539696	192.168.2.91	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
655	9.661497131	fe80::8ccf:4758:1c5...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
654	9.648215337	fe80::86a9:3eff:fe5...	ff02::fb	MDNS	233	Standard query response 0x0000 SRV, cache flush 0 0 631 NPI52815D.local A, cache flush 192.16
653	9.648151660	192.168.63.100	224.0.0.251	MDNS	213	Standard query response 0x0000 SRV, cache flush 0 0 631 NPI52815D.local A, cache flush 192.16
651	9.611847420	fe80::150e:18ce:7e1...	ff02::fb	MDNS	215	Standard query response 0x0000 PTR, cache flush apsit=HP-280-G3-MT-21.local AAAA, cache flush
650	9.611782906	192.168.87.13	224.0.0.251	MDNS	195	Standard query response 0x0000 PTR, cache flush apsit=HP-280-G3-MT-21.local AAAA, cache flush
648	9.604826367	fe80::ee58:eaff:fe0...	ff02::fb	MDNS	104	Standard query 0x0000 PTR _communicator._tcp.local, "QM" question
647	9.604762219	192.168.69.236	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _communicator._tcp.local, "QM" question
632	9.545379698	fe80::2c8f:9f38:f32...	ff02::fb	MDNS	124	Standard query 0x0000 TXT HP LaserJet M203dn (52815D)..._ipps._tcp.local, "QM" question
628	9.542653790	fe80::b93e:81bc:2c8...	ff02::fb	MDNS	129	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
627	9.542578760	192.168.2.105	224.0.0.251	MDNS	109	Standard query 0x0000 PTR _pdl-datastream._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
626	9.541507305	192.168.2.91	224.0.0.251	MDNS	104	Standard query 0x0000 TXT HP LaserJet M203dn (52815D)..._ipps._tcp.local, "QM" question
625	9.541115708	fe80::2c8f:9f38:f32...	ff02::fb	MDNS	124	Standard query 0x0000 SRV HP LaserJet M203dn (52815D)..._ipps._tcp.local, "QM" question
624	9.540944410	192.168.2.91	224.0.0.251	MDNS	104	Standard query 0x0000 SRV HP LaserJet M203dn (52815D)..._ipps._tcp.local, "QM" question
623	9.532987511	fe80::86a9:3eff:fe5...	ff02::fb	MDNS	792	Standard query response 0x0000 TXT, cache flush NSEC, cache flush HP LaserJet M203dn (52815D)