Department of Information Technology

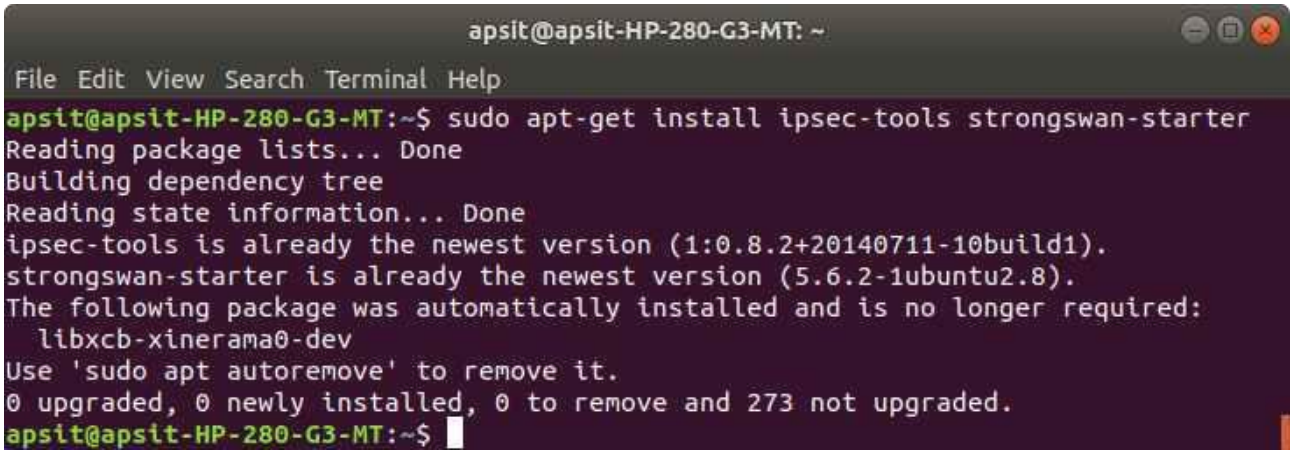
Semester: V
Academic Year: 2022-23
Class / Branch: TE IT A
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

Name of Student: Vishal Bangar
Student ID: 20104084

EXPERIMENT NO. 9

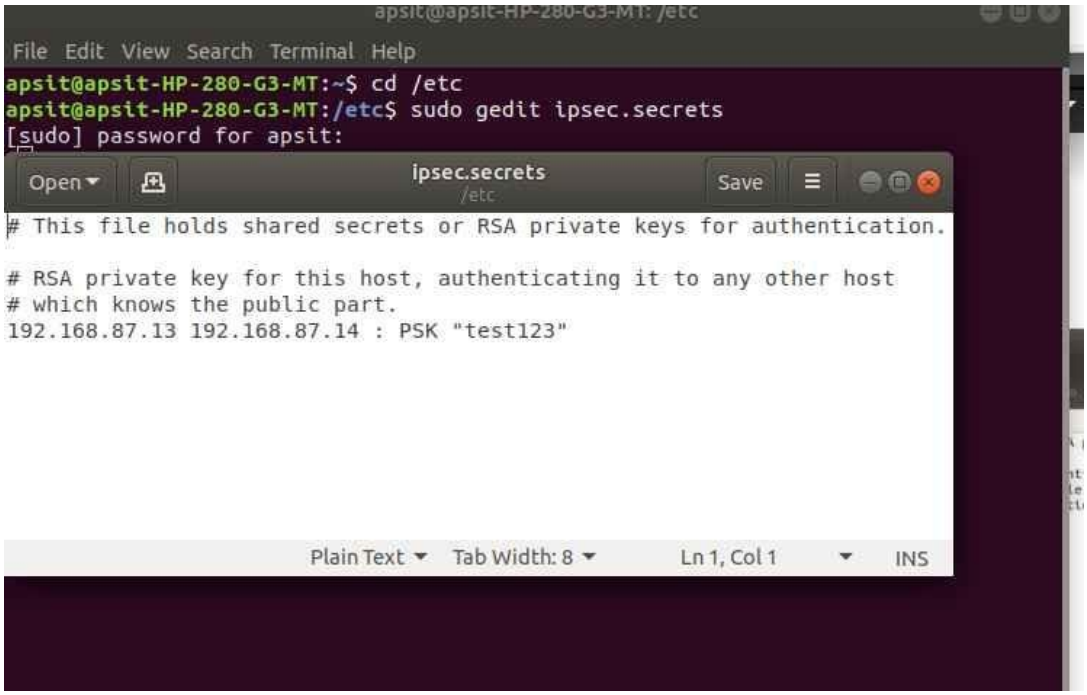
Aim: To study and implement IPSEC in Linux .

Installing IPSEC

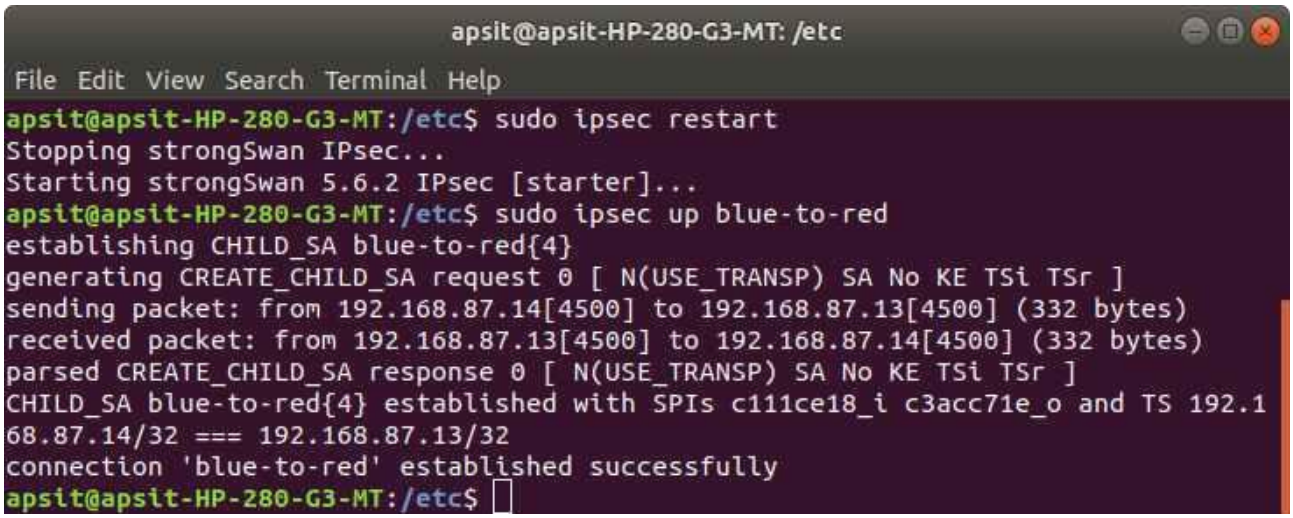


sudo gedit ipsec.conf

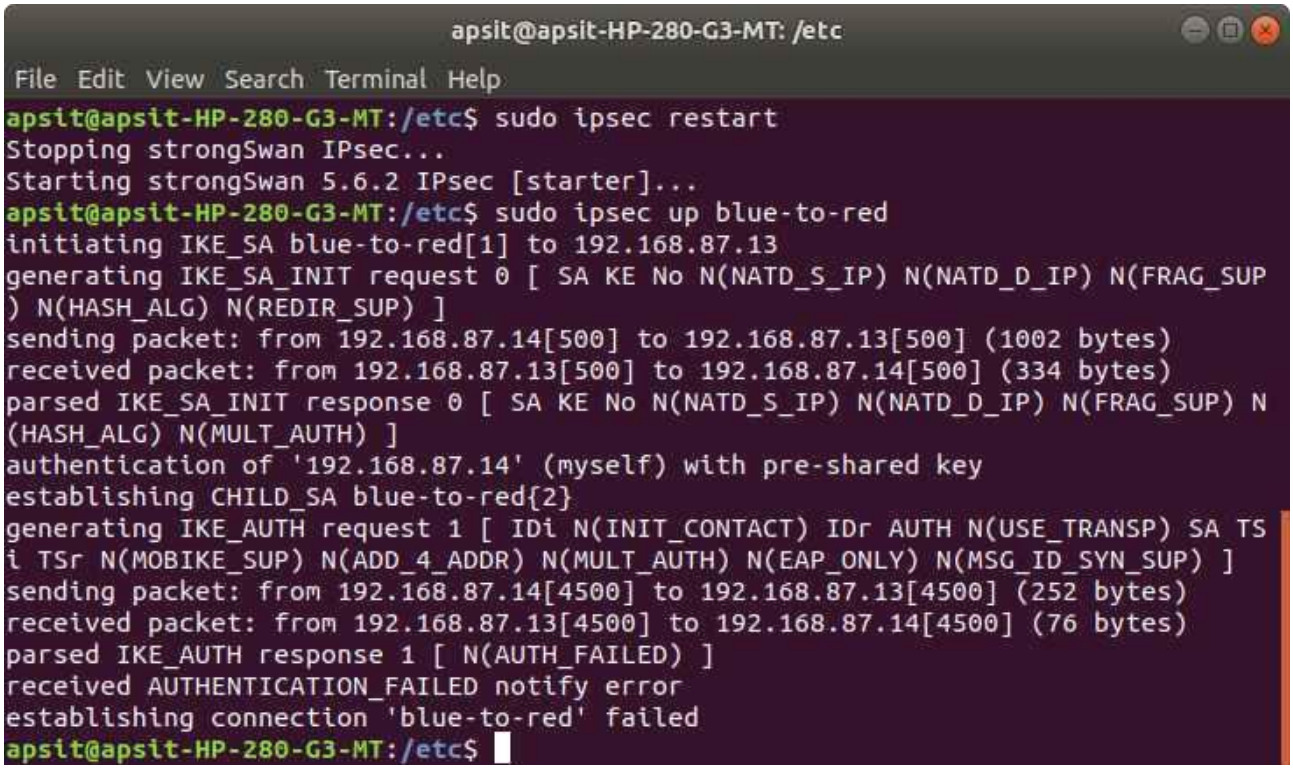

Open
ipsec.conf
/etc
Save
uniqueids = no
Add connections here.
Sample VPN connections
#conn sample-self-signed
leftsubnet=10.1.0.0/16
leftcert=selfCert.der
leftsendcert=never
right=192.168.0.2
rightsubnet=10.2.0.0/16
rightcert=peerCert.der
auto=start
#conn sample-with-ca-cert
leftsubnet=10.1.0.0/16
leftcert=myCert.pem
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


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

sudo ipsec up connection name



with different password:



By wireshark