

A. P. SHAH INSTITUTE OF TECHNOLOGY



(All Branches NBA Accredited)

Student ID: 20104084

Department of Information Technology

Semester: V Name of Student: Vishal Bangar

Academic Year: 2022-23
Class / Branch: TE IT A
Subject: Security Lab (SL)

Name of Instructor: Prof. Apeksha Mohite

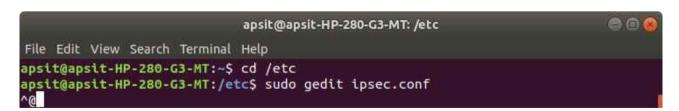
EXPERIMENT NO. 9

Aim: To study and implement IPSEC in Linux.

Installing IPSEC

```
apsit@apsit-HP-280-G3-MT: ~ \Bigcip \B
```

sudo gedit ipsec.conf



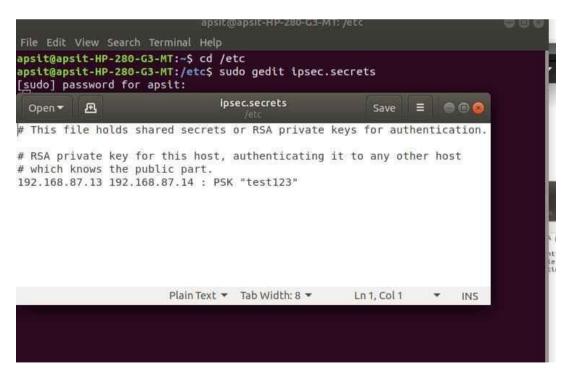


A. P. SHAH INSTITUTE OF TECHNOLOGY



(All Branches NBA Accredited)







A. P. SHAH INSTITUTE OF TECHNOLOGY



(All Branches NBA Accredited)

sudo ipsec up connection name

```
apsit@apsit-HP-280-G3-MT: /etc
                                                                            a a
File Edit View Search Terminal Help
apsit@apsit-HP-280-G3-MT:/etcS 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 TSi 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 TSi 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:/etcS
```

with different password:

```
apsit@apsit-HP-280-G3-MT: /etc
                                                                            8 6
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$
```



A. P. SHAH INSTITUTE OF TECHNOLOGY



(All Branches NBA Accredited)

By wireshark

