Development Tools Assignment

Module 3 – Network Authentication Tools

1. **Write a config file so that wpa_supplicant can associate to FT Dot1x WLAN**
   config file for FT Dot1x WLAN

```
  GNU nano 6.2          /etc/wpa_supplicant/wpa_supplicant.conf
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
p2p_disabled=1

network={
    ssid="ZTE-xDSdSC"
    key_mgmt=FT-EAP
    pairwise=CCMP
    group=CCMP
    eap=PEAP
    password="sxyhcbyx"
    phase1="peaplabel=0"
    phase2="auth=MSCHAPV2"
    proactive_key_caching=1
    ieee80211w=1
    ft_eap=1
}



                          [ Read 19 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
user@user-VirtualBox:~$ sudo nano /etc/wpa_supplicant/wpa_supplicant.conf
user@user-VirtualBox:~$ sudo systemctl restart wpa_supplicant
user@user-VirtualBox:~$ sudo dhclient -v wlan0
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlan0/02:00:00:00:00:00
Sending on   LPF/wlan0/02:00:00:00:00:00
Sending on   Socket/fallback
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 3 (xid=0xb015e320)
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 5 (xid=0xb015e320)
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 9 (xid=0xb015e320)
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 21 (xid=0xb015e320)
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 16 (xid=0xb015e320)
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 16 (xid=0xb015e320)
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 12 (xid=0xb015e320)
```

2. **Bring up a Freeradius, wpa_supplicant in linux machine, use "eapol_test" utility in wpa_supplicant and try connecting successfully to the Freeradius. Also, please capture the radius packets that is exchanged between eapol_test and Freeradius using "tcpdump" command.**

```
user@user-VirtualBox:~$ sudo nano /etc/freeradius/3.0/mods-enabled/eap
user@user-VirtualBox:~$ sudo nano /etc/freeradius/3.0/sites-enabled/default
user@user-VirtualBox:~$ nano eapol_test.conf
user@user-VirtualBox:~$ sudo eapol_test -c eapol_test.conf -s testing123 -a 127.0.0.1 -p 1812 -r 3 -t 2 -M 00:11:22:33:44:55
Reading configuration file 'eapol_test.conf'
Line: 1 - start of a new network block
ssid - hexdump_ascii(len=9):
     74 65 73 74 2d 73 73 69 64                       test-ssid
key_mgmt: 0x1
eap methods - hexdump(len=16): 00 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00
identity - hexdump_ascii(len=8):
     74 65 73 74 75 73 65 72                          testuser
password - hexdump_ascii(len=8):
     70 61 73 73 77 6f 72 64                          password
phase1 - hexdump_ascii(len=11):
     70 65 61 70 6c 61 62 65 6c 3d 30                 peaplabel=0
phase2 - hexdump_ascii(len=13):
     61 75 74 68 3d 4d 53 43 48 41 50 56 32           auth=MSCHAPV2
ca_cert - hexdump_ascii(len=15):
     2f 70 61 74 68 2f 74 6f 2f 63 61 2e 70 65 6d     /path/to/ca.pem
client_cert - hexdump_ascii(len=19):
     2f 70 61 74 68 2f 74 6f 2f 63 6c 69 65 6e 74 2e  /path/to/client.
     70 65 6d                                         pem
private_key - hexdump_ascii(len=19):
     2f 70 61 74 68 2f 74 6f 2f 63 6c 69 65 6e 74 2e  /path/to/client.
     6b 65 79                                         key
Priority group 0
   id=0 ssid='test-ssid'
Authentication server 127.0.0.1:1812
RADIUS local address: 127.0.0.1:42914
ENGINE: Loading builtin engines
ENGINE: Loading builtin engines
EAPOL: SUPP_PAE entering state DISCONNECTED
EAPOL: KEY_RX entering state NO_KEY_RECEIVE
EAPOL: SUPP_BE entering state INITIALIZE
EAP: EAP entering state DISABLED
```

```
EAPOL: SUPP_PAE entering state DISCONNECTED
EAPOL: KEY_RX entering state NO_KEY_RECEIVE
EAPOL: SUPP_BE entering state INITIALIZE
EAP: EAP entering state DISABLED
EAPOL: External notification - portValid=0
EAPOL: External notification - portEnabled=1
EAPOL: SUPP_PAE entering state CONNECTING
EAPOL: SUPP_BE entering state IDLE
EAP: EAP entering state INITIALIZE
EAP: EAP entering state IDLE
Sending fake EAP-Request-Identity
EAPOL: Received EAP-Packet frame
EAPOL: SUPP_PAE entering state RESTART
EAP: EAP entering state INITIALIZE
EAP: EAP entering state IDLE
EAPOL: SUPP_PAE entering state AUTHENTICATING
EAPOL: SUPP_BE entering state REQUEST
EAPOL: getSuppRsp
EAP: EAP entering state RECEIVED
EAP: Received EAP-Request id=250 method=1 vendor=0 vendorMethod=0
EAP: EAP entering state IDENTITY
CTRL-EVENT-EAP-STARTED EAP authentication started
EAP: Status notification: started (param=)
EAP: EAP-Request Identity data - hexdump_ascii(len=0):
EAP: using real identity - hexdump_ascii(len=8):
     74 65 73 74 75 73 65 72                          testuser
EAP: EAP entering state SEND_RESPONSE
EAP: EAP entering state IDLE
EAPOL: SUPP_BE entering state RESPONSE
EAPOL: txSuppRsp
WPA: eapol_test_eapol_send(type=0 len=13)
TX EAP -> RADIUS - hexdump(len=13): 02 fa 00 0d 01 74 65 73 74 75 73 65 72
Encapsulating EAP message into a RADIUS packet
Learned identity from EAP-Response-Identity - hexdump(len=8): 74 65 73 74 75 73 65 72
Sending RADIUS message to authentication server
RADIUS message: code=1 (Access-Request) identifier=0 length=130
```

```
EAPOL: SUPP_BE entering state RESPONSE
EAPOL: txSuppRsp
WPA: eapol_test_eapol_send(type=0 len=13)
TX EAP -> RADIUS - hexdump(len=13): 02 fa 00 0d 01 74 65 73 74 75 73 65 72
Encapsulating EAP message into a RADIUS packet
Learned identity from EAP-Response-Identity - hexdump(len=8): 74 65 73 74 75 73 65 72
Sending RADIUS message to authentication server
RADIUS message: code=1 (Access-Request) identifier=0 length=130
   Attribute 1 (User-Name) length=10
      Value: 'testuser'
   Attribute 4 (NAS-IP-Address) length=6
      Value: 127.0.0.1
   Attribute 31 (Calling-Station-Id) length=19
      Value: '00-11-22-33-44-55'
   Attribute 12 (Framed-MTU) length=6
      Value: 1400
   Attribute 61 (NAS-Port-Type) length=6
      Value: 19
   Attribute 6 (Service-Type) length=6
      Value: 2
   Attribute 77 (Connect-Info) length=24
      Value: 'CONNECT 11Mbps 802.11b'
   Attribute 79 (EAP-Message) length=15
      Value: 02fa000d017465737475736572
   Attribute 80 (Message-Authenticator) length=18
      Value: eddef4bcda7e8bfd31987f6b8b2bf39d
Next RADIUS client retransmit in 3 seconds
EAPOL: SUPP_BE entering state RECEIVE
recvmsg[RADIUS]: Connection refused
EAPOL: startWhen --> 0
EAPOL test timed out
EAPOL: EAP key not available
EAPOL: EAP Session-Id not available
WPA: Clear old PMK and PTK
MPPE keys OK: 0  mismatch: 1
```

Configure FreeRADIUS Client:

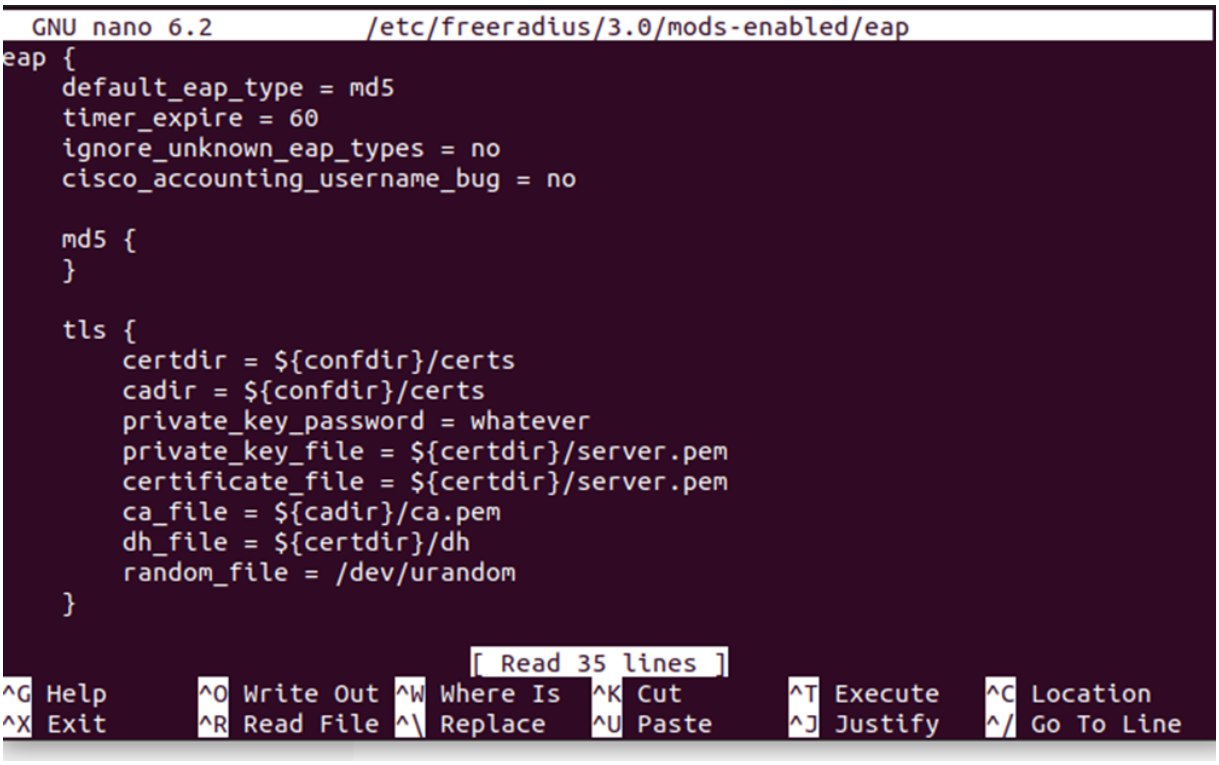
sudo nano /etc/freeradius/3.0/clients.conf

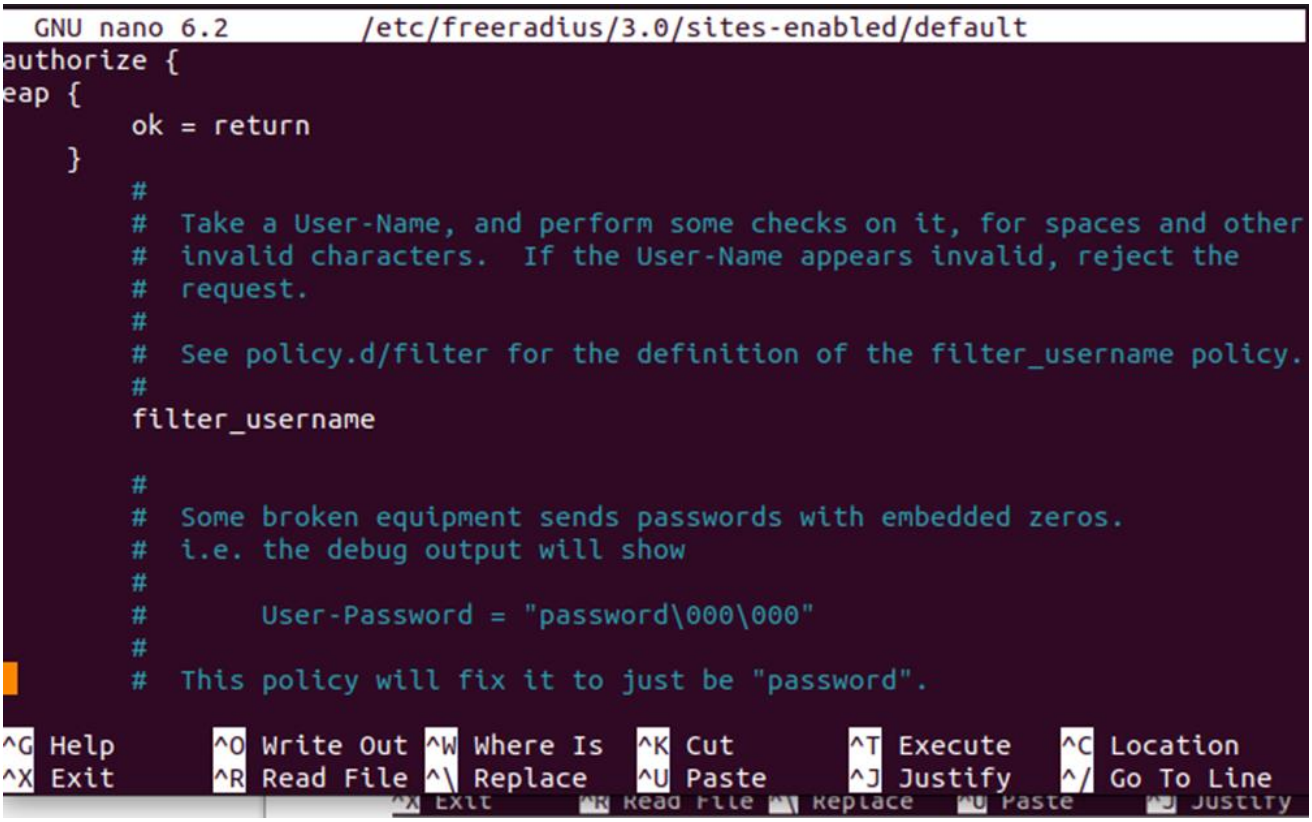
```
  GNU nano 6.2              /etc/freeradius/3.0/clients.conf
client localhost {
    ipaddr = 127.0.0.1
    secret = testing123
}

                          [ Read 4 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Create User in FreeRADIUS:

sudo nano /etc/freeradius/3.0/mods-config/files/authorize





Create Configuration File for eapol_test

sudo nano eapol_test.conf