

## Development Tools Assignment

### Module 3 – Network Authentication Tools

1. Write a config file so that wpa\_supplicant can associate to FT Dot1x WLAN .

Answer:

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
```

```
update_config=1
```

```
network={
```

```
    ssid="Varun_5G" \\ name of wifi
```

```
    key_mgmt=FT-EAP \\ key management type sets it to FTDot1x
```

```
    pairwise=CCMP \\ enables pairwise cipher in ccmp.
```

```
    group=CCMP \\ enables group cipher in ccmp.
```

```
    proto=RSN \\ specifies RSN protocol
```

```
    eap=PEAP \\ specifies PEAP protocol
```

```
    identity="adhithya" \\ username
```

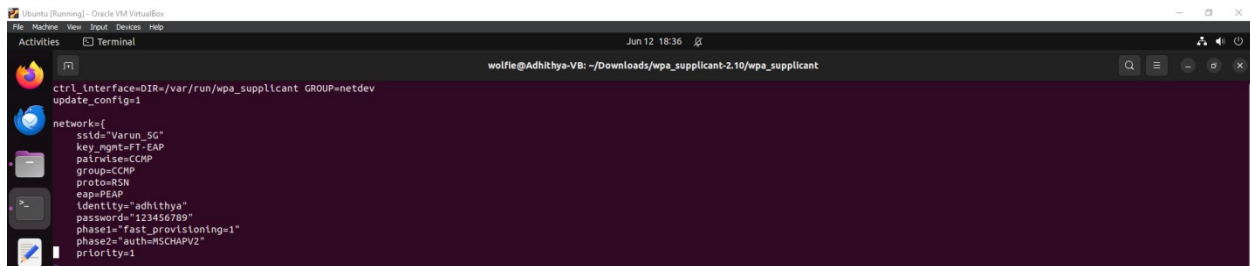
```
    password="123456789" \\ password
```

```
    phase1="fast_provisioning=1" \\option enables in-line provisioning of EAP- FAST credentials
```

```
    phase2="auth=MSCHAPV2" \\ configures inner authentication method
```

```
    priority=1 \\ corresponds to priority of the network
```

```
}
```

A screenshot of a terminal window in a virtual machine. The terminal shows the configuration for wpa\_supplicant. The configuration includes: ctrl\_interface=DIR=/var/run/wpa\_supplicant GROUP=netdev, update\_config=1, and a network block with ssid="Varun\_5G", key\_mgmt=FT-EAP, pairwise=CCMP, group=CCMP, proto=RSN, eap=PEAP, identity="adhithya", password="123456789", phase1="fast\_provisioning=1", phase2="auth=MSCHAPV2", and priority=1. The terminal window has a title bar that says "Ubuntu (Running) - Oracle VM VirtualBox" and a status bar that says "Jun 12 18:36". The terminal prompt is "wolfie@Adhithya-VB: ~/Downloads/wpa\_supplicant-2.10/wpa\_supplicant".

```
wolfie@Adhithya-VB: ~/Downloads/wpa_supplicant-2.10/wpa_supplicant
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
network={
    ssid="Varun_5G"
    key_mgmt=FT-EAP
    pairwise=CCMP
    group=CCMP
    proto=RSN
    eap=PEAP
    identity="adhithya"
    password="123456789"
    phase1="fast_provisioning=1"
    phase2="auth=MSCHAPV2"
    priority=1
}
```

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.

Answer:

### **WPA\_SUPPLICANT**

#### **eapol\_test.conf**

```
ctrl_interface=/var/run/wpa_supplicant
```

```
update_config=1
```

```
network={
```

```
    ssid="Varun"
```

```
    key_mgmt=WPA-EAP
```

```
    eap=PEAP
```

```
    identity="adhithya"
```

```
    password="testing"
```

```
    phase2="auth=MSCHAPV2"
```

```
}
```

### **FREERADIUS**

#### **clients.conf**

```
client localhost {
```

```
    ipaddr = 127.0.0.1
```

```
    secret = testing
```

```
}
```

#### **users**

```
adhithya Cleartext-Password := "testing"
```

These are the changes in configuration files of wpa\_supplicant and freeradius.

## **COMMANDS FOR INITIALIZING SERVICES**

### **FREERADIUS**

Systemctl start freeradius

This will start the freeradius server and it will start listening on port 1812

### **WPA\_SUPPLICANT**

eapol\_test -c /etc/wpa\_supplicant/wpa\_supplicant.conf -a 127.0.0.1 -s testing

This will start the eapol test.

### **TCPDUMP**

sudo tcpdump -i lo -nn -s 0 -v port 1812

This command captures all packets on loopback interface.

```
root@Adhithya-VB: /home/wolfie/Downloads/wpa_supplicant-2.10/wpa_supplicant

EAPOL: SUPP_BE entering state RECEIVE
Received 176 bytes from RADIUS server
Received RADIUS message
RADIUS message: code=2 (Access-Accept) identifier=9 length=176
Attribute 26 (Vendor-Specific): length=58
Value: 00001317134841733ff519149c18ee56d3d362d0c911ed881a0b923a9122ecdefe4e23f892e5dc9b72e0f31cf20d7a9b25179472513a
Attribute 26 (Vendor-Specific): length=58
Value: 0000131710348e26422cbe70dd61fc9da4b9dee8703c0461cac4ffa029b76c8f8ee8bbf2a2662b31d1fce0e3bc883d40cb7c37e40f6dfff
Attribute 79 (EAP-Message): length=6
Value: 03d40004
Attribute 80 (Message-Authenticator): length=18
Value: 97560fbd4073ab3202c013dbd97978f
Attribute 1 (User-Name): length=10
Value: 'adhithya'
Attribute 12 (Framed-MTU): length=6
Value: 994
STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station
MS-MPPE-Send-Key (sign) - hexdump(len=32): cb 33 f8 77 bd 86 9e 6d 05 a1 62 97 e1 40 06 95 e1 97 18 32 30 12 03 6d 79 11 0c e9 89 64 61 45
MS-MPPE-Recv-Key (crypt) - hexdump(len=32): ca 69 9d a9 65 8b 44 1f 92 13 e9 92 4c fb ee 60 05 a8 73 13 9e 9b fd f6 da 74 22 c0 db e8 cf af
decapsulated EAP packet (code=3 id=212 len=4) from RADIUS server: EAP Success
EAPOL: Received EAP-Packet Frame
EAPOL: SUPP_BE entering state REQUEST
EAPOL: getSuppRsp
EAP: EAP entering state RECEIVED
EAP: Received EAP-Success
EAP: Status notification: completion (param=success)
EAP: EAP entering state SUCCESS
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
EAPOL: IEEE 802.1X for plaintext connection; no EAPOL-Key frames required
WPA: EAPOL processing complete
Cancelling authentication timeout
State: DISCONNECTED -> COMPLETED
EAPOL: SUPP_PAE entering state AUTHENTICATED
EAPOL: SUPP_BE entering state RECEIVE
EAPOL: SUPP_BE entering state SUCCESS
EAPOL: SUPP_BE entering state IDLE
eapol_sm_ctx: result=1
EAPOL: Successfully fetched key (len=32)
PMK from EAPOL - hexdump(len=32): ca 69 9d a9 65 8b 44 1f 92 13 e9 92 4c fb ee 60 05 a8 73 13 9e 9b fd f6 da 74 22 c0 db e8 cf af
No EAP-Key-Name received from server
Writing configuration file 'wpa_supplicant.conf.tmp'
Configuration file 'wpa_supplicant.conf' written successfully
WPA: Clear old PMK and PTK
EAP: deinitLate previously used EAP method (25, PEAP) at EAP deinit
ENGINE: engine deinit
MPPE keys OK: 1 mismatch: 0
SUCCESS
root@Adhithya-VB: /home/wolfie/Downloads/wpa_supplicant-2.10/wpa_supplicant
```

## WPA\_SUPPLICANT TERMINAL OUTPUT

```
wolfie@Adhithya-VB: ~

User-Name Attribute (1), length: 10, Value: adhithya
NAS-IP-Address Attribute (4), length: 6, Value: 127.0.0.1
Calling-Station-Id Attribute (31), length: 19, Value: 02-00-00-00-00-01
Framed-MTU Attribute (12), length: 6, Value: 1400
NAS-Port-Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
Service-Type Attribute (6), length: 6, Value: Framed
Connect-Info Attribute (77), length: 24, Value: CONNECT 11Mbps 802.11b
Called-Station-Id Attribute (30), length: 3, Value:
EAP-Message Attribute (79), length: 39, Value: Response (2), id 211, len 37
Type unknown (25)
State Attribute (24), length: 18, Value: T+..S..V.X.....
Message-Authenticator Attribute (80), length: 18, Value: 8..J..UJ..l..'pcc'
08:35:38.045200 IP (tos 0x0, ttl 64, id 15741, offset 0, flags [none], proto UDP (17), length 132)
127.0.0.1.1812 > 127.0.0.1.54873: RADIUS, length: 184
Access-Challenge (11), id: 0x08, Authenticator: 7f00c7e9690f9a6dd3c76dbf68b3597d
EAP-Message Attribute (79), length: 48, Value: Request (1), id 212, len 46
Type unknown (25)
Message-Authenticator Attribute (80), length: 18, Value: {n....J..Qe.Y..
State Attribute (24), length: 18, Value: T+..J..V.X.....
08:35:38.045630 IP (tos 0x0, ttl 64, id 44045, offset 0, flags [none], proto UDP (17), length 212)
127.0.0.1.54873 > 127.0.0.1.1812: RADIUS, length: 184
Access-Request (1), id: 0x09, Authenticator: b70fab0ffc2d0da5eeb8d6075afc1c4c
User-Name Attribute (1), length: 10, Value: adhithya
NAS-IP-Address Attribute (4), length: 6, Value: 127.0.0.1
Calling-Station-Id Attribute (31), length: 19, Value: 02-00-00-00-00-01
Framed-MTU Attribute (12), length: 6, Value: 1400
NAS-Port-Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
Service-Type Attribute (6), length: 6, Value: Framed
Connect-Info Attribute (77), length: 24, Value: CONNECT 11Mbps 802.11b
Called-Station-Id Attribute (30), length: 3, Value:
EAP-Message Attribute (79), length: 48, Value: Response (2), id 212, len 46
Type unknown (25)
State Attribute (24), length: 18, Value: T+..J..V.X.....
Message-Authenticator Attribute (80), length: 18, Value: S7+....X.....
08:35:38.045831 IP (tos 0x0, ttl 64, id 15742, offset 0, flags [none], proto UDP (17), length 204)
127.0.0.1.1812 > 127.0.0.1.54873: RADIUS, length: 176
Access-Accept (2), id: 0x09, Authenticator: c5a053a3ccf66ef1338fa157c4540
Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
Vendor Attribute: 17, length: 50, Value: ..3....I...=b.....k..i..*...N#.....f.....z.W...rQ:
Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
Vendor Attribute: 16, length: 50, Value: .8b.p.a.....pc.k.o.v.....8b.1.....=0..{7...n
EAP-Message Attribute (79), length: 6, Value: Success (3), id 212, len 4
Message-Authenticator Attribute (80), length: 18, Value: .Vo...4..,a=....
User-Name Attribute (1), length: 10, Value: adhithya
Framed-MTU Attribute (12), length: 6, Value: 994

^C
20 packets captured
40 packets received by filter
0 packets dropped by kernel
wolfie@Adhithya-VB: ~
```

## TCPDUMP output