

## Development Tools Assignment

### Module 3 – Network Authentication Tools

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

Contents of the configuration file

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
fast_reauth=1

network={
    ssid="Suresh"
    proto=RSN
    key_mgmt=FT-EAP
    pairwise=CCMP
    group=CCMP
    eap=PEAP
    identity="ramana"
    password="testing"
    phase2="auth=MSCHAPV2"
}
```

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.

The image shows three terminal windows from a Linux virtual machine. The top-left window shows the configuration of wpa\_supplicant, including the control interface, update config flag, fast reauth flag, and a network configuration block for SSID 'Suresh' using RSN, FT-EAP, CCMP, and PEAP with identity 'ramana' and password 'testing'. The top-right window shows the output of the wpa\_supplicant command, displaying the configuration and the start of the EAP authentication process. The bottom window shows the output of the tcpdump command, capturing the EAP authentication process between the supplicant and the peer.

```
root@ramana-VirtualBox: ~  
7  
(19) EAP-Message = 0x03f20004  
(19) Message-Authenticator = 0x00000000000000000000000000000000  
(19) User-Name = "ramana"  
(19) Framed-MTU += 994  
(19) Finished request  
Waking up in 4.9 seconds.  
(10) Cleaning up request packet ID 0 with timestamp +1184 due to cleanup_delay was reached  
(11) Cleaning up request packet ID 1 with timestamp +1184 due to cleanup_delay was reached  
(12) Cleaning up request packet ID 2 with timestamp +1184 due to cleanup_delay was reached  
(13) Cleaning up request packet ID 3 with timestamp +1184 due to cleanup_delay was reached  
(14) Cleaning up request packet ID 4 with timestamp +1184 due to cleanup_delay was reached  
(15) Cleaning up request packet ID 5 with timestamp +1184 due to cleanup_delay was reached  
(16) Cleaning up request packet ID 6 with timestamp +1184 due to cleanup_delay was reached  
(17) Cleaning up request packet ID 7 with timestamp +1184 due to cleanup_delay was reached  
(18) Cleaning up request packet ID 8 with timestamp +1184 due to cleanup_delay was reached  
(19) Cleaning up request packet ID 9 with timestamp +1184 due to cleanup_delay was reached  
Ready to process requests  
  
ramana@ramana-VirtualBox: ~/Desktop$ tcpdump  
tcpdump: enp0s3: You don't have permission to perform this capture on that device  
(socket: Operation not permitted)  
ramana@ramana-VirtualBox: ~/Desktop$ sudo -i  
[sudo] password for ramana:  
root@ramana-VirtualBox:~# tcpdump -i lo -w dump.pcap port 1812  
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
^C20 packets captured  
40 packets received by filter  
0 packets dropped by kernel  
root@ramana-VirtualBox:~# ls  
dump.pcap  
root@ramana-VirtualBox:~# wireshark dump.pcap  
** (Wireshark:4678) 08:26:50.944799 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'  
root@ramana-VirtualBox:~#
```

```
Value: 'ramana'  
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): 73 62 a3 f6 c9 7d 0e b3 48 72 6a 2e 4e 13 a8 cf 28 59 da 55 cb ab 22 bd f0 31 f4 b5 80 f9 08 87  
MS-MPPE-Recv-Key (crypt) - hexdump(len=32): d1 89 29 c1 a9 da 05 33 0b 51 e1 df 66 eb 6b f9 34 62 da c1 56 a7 ac e8 cf 1d 45 9d 8d 13 ee e7  
decapsulated EAP packet (code=3 id=242 len=4) from RADIUS server: EAP Success  
EAPOL: Received EAP-Packet frame  
EAPOL: SUPP_BE entering state REQUEST  
EAPOL: NotSuppBE  
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_cb: result=1  
EAPOL: Successfully fetched key (len=32)  
PMK from EAPOL - hexdump(len=32): d1 89 29 c1 a9 da 05 33 0b 51 e1 df 66 eb 6b f9 34 62 da c1 56 a7 ac e8 cf 1d 45 9d 8d 13 ee e7  
No EAP-Key-Name received from server  
WPA: Clear old PMK and PTK  
EAP: deinitialize previously used EAP method (25, PEAP) at EAP deinit  
ENGINE: engine deinit  
MPPE keys OK: 1 mismatch: 0  
SUCCESS  
ramana@ramana-VirtualBox: ~/Downloads/wpa_supplicant-2.10/wpa_supplicant$
```