

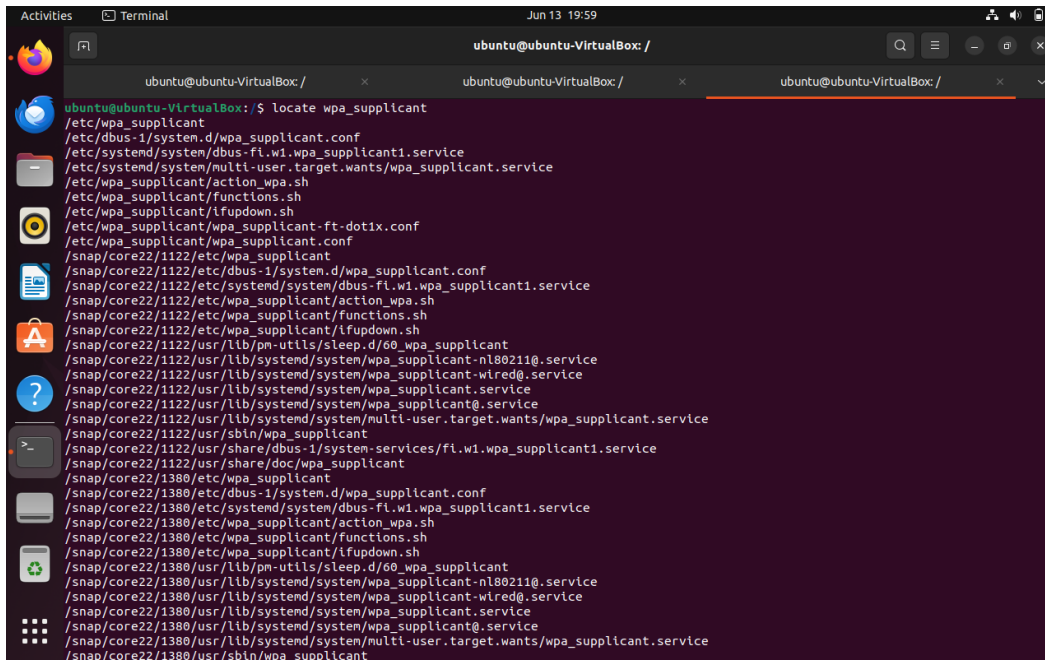
## Development Tools Assignment

### Module 3 – Network Authentication Tools

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

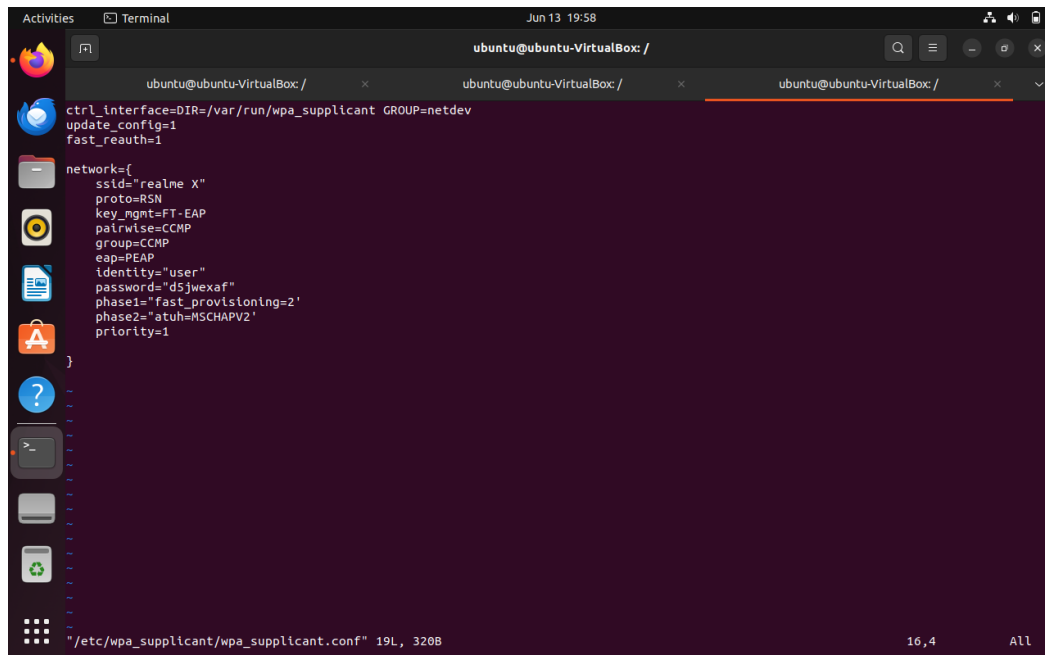
Solution:

Step 1: Installing wpa\_supplicant and locating its path



```
ubuntu@ubuntu-VirtualBox: /  
$ locate wpa_supplicant  
/etc/wpa_supplicant  
/etc/dbus-1/system.d/wpa_supplicant.conf  
/etc/systemd/system/dbus-fl.w1.wpa_supplicant1.service  
/etc/systemd/system/multi-user.target.wants/wpa_supplicant.service  
/etc/wpa_supplicant/action_wpa.sh  
/etc/wpa_supplicant/functions.sh  
/etc/wpa_supplicant/ifupdown.sh  
/etc/wpa_supplicant/wpa_supplicant-ft-dot1x.conf  
/etc/wpa_supplicant/wpa_supplicant.conf  
/snap/core22/1122/etc/wpa_supplicant  
/snap/core22/1122/etc/dbus-1/system.d/wpa_supplicant.conf  
/snap/core22/1122/etc/systemd/system/dbus-fl.w1.wpa_supplicant1.service  
/snap/core22/1122/etc/wpa_supplicant/action_wpa.sh  
/snap/core22/1122/etc/wpa_supplicant/functions.sh  
/snap/core22/1122/etc/wpa_supplicant/ifupdown.sh  
/snap/core22/1122/usr/lib/pm-utils/sleep.d/60_wpa_supplicant  
/snap/core22/1122/usr/lib/systemd/system/wpa_supplicant-nl80211@.service  
/snap/core22/1122/usr/lib/systemd/system/wpa_supplicant-wired@.service  
/snap/core22/1122/usr/lib/systemd/system/wpa_supplicant.service  
/snap/core22/1122/usr/lib/systemd/system/wpa_supplicant@.service  
/snap/core22/1122/usr/lib/systemd/system/multi-user.target.wants/wpa_supplicant.service  
/snap/core22/1122/usr/sbin/wpa_supplicant  
/snap/core22/1122/usr/share/dbus-1/system-services/fl.w1.wpa_supplicant1.service  
/snap/core22/1122/usr/share/doc/wpa_supplicant  
/snap/core22/1380/etc/wpa_supplicant  
/snap/core22/1380/etc/dbus-1/system.d/wpa_supplicant.conf  
/snap/core22/1380/etc/systemd/system/dbus-fl.w1.wpa_supplicant1.service  
/snap/core22/1380/etc/wpa_supplicant/action_wpa.sh  
/snap/core22/1380/etc/wpa_supplicant/functions.sh  
/snap/core22/1380/etc/wpa_supplicant/ifupdown.sh  
/snap/core22/1380/usr/lib/pm-utils/sleep.d/60_wpa_supplicant  
/snap/core22/1380/usr/lib/systemd/system/wpa_supplicant-nl80211@.service  
/snap/core22/1380/usr/lib/systemd/system/wpa_supplicant-wired@.service  
/snap/core22/1380/usr/lib/systemd/system/wpa_supplicant.service  
/snap/core22/1380/usr/lib/systemd/system/wpa_supplicant@.service  
/snap/core22/1380/usr/lib/systemd/system/multi-user.target.wants/wpa_supplicant.service  
/snap/core22/1380/usr/sbin/wpa_supplicant
```

Step 2: wpa\_supplicant.conf file



```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev  
update_config=1  
fast_reauth=1  
  
network={  
    ssid="realme X"  
    proto=RSN  
    key_mgmt=FT-EAP  
    pairwise=CCMP  
    group=CCMP  
    eap=PEAP  
    identity="user"  
    password="d5jwexaf"  
    phase1="fast_provisioning=2"  
    phase2="atuh=MSCHAPV2"  
    priority=1  
}  
  
"/etc/wpa_supplicant/wpa_supplicant.conf" 19L, 320B 16,4 All
```

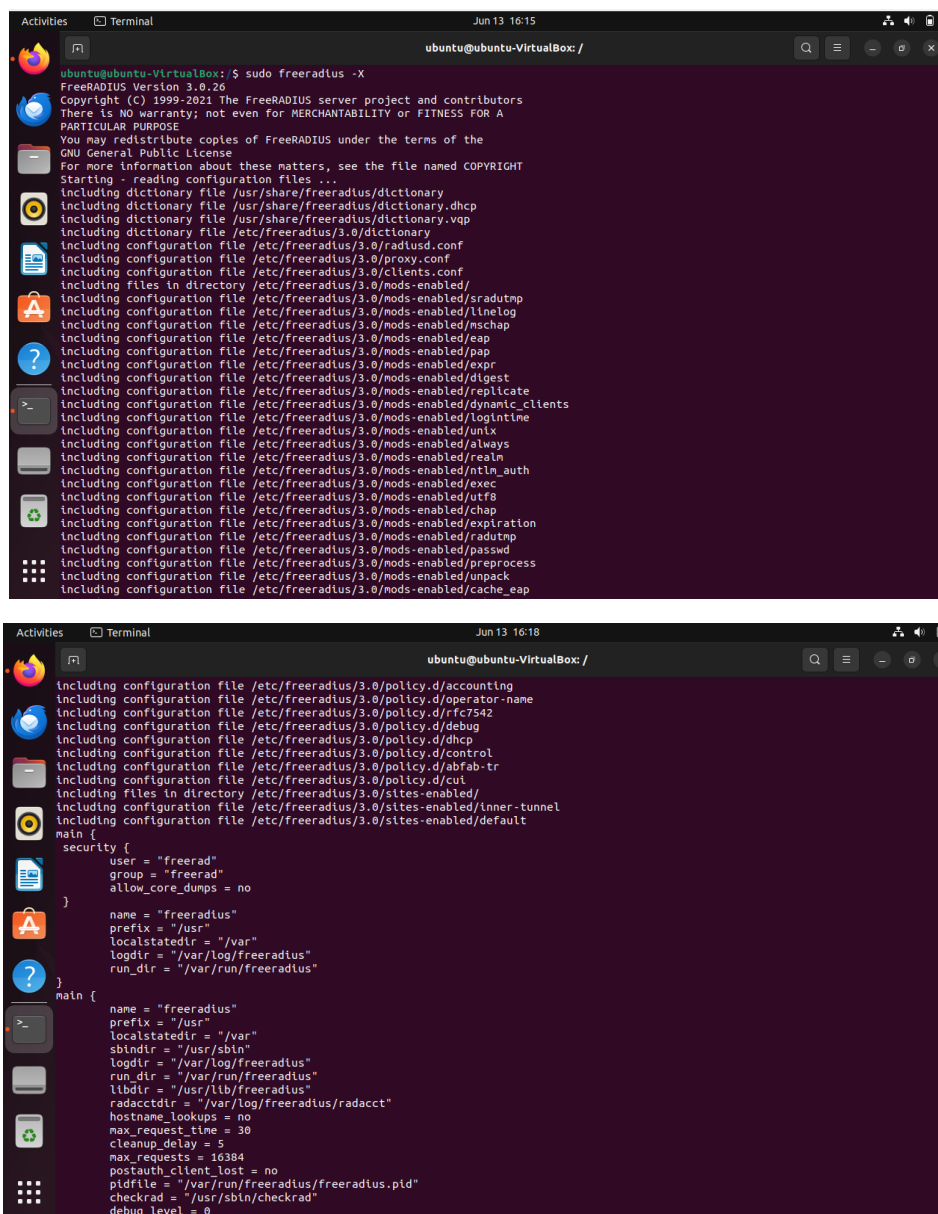
2. Bring up a Freeradius, wpa\_supplicant in linux machine, use "eapol\_test" utility in wpa\_supplicant and try connecting successfully to the Freeradius. Also, please capture the radius packets that is exchanged between eapol\_test and Freeradius using "tcpdump" command.

### Solution:

Step 1: Installing wpa\_supplicant, freeradius, tcpdump

Step 2: Adding the freeradius and wpa\_supplicant configuration files(radius name as “user” and password as “testing123”

i. After executing sudo freeradius -X command



```
ubuntu@ubuntu-VirtualBox:/$ sudo freeradius -X
FreeRADIUS Version 3.0.26
Copyright (C) 1999-2021 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the GNU General Public License
For more information about these matters, see the file named COPYRIGHT
Starting - reading configuration files ...
including dictionary file /usr/share/freeradius/dictionary
including dictionary file /usr/share/freeradius/dictionary.dhcp
including dictionary file /usr/share/freeradius/dictionary.vqp
including dictionary file /etc/freeradius/3.0/dictionary
including configuration file /etc/freeradius/3.0/radiusd.conf
including configuration file /etc/freeradius/3.0/proxy.conf
including configuration file /etc/freeradius/3.0/clients.conf
including files in directory /etc/freeradius/3.0/mods-enabled/
including configuration file /etc/freeradius/3.0/mods-enabled/sradutmp
including configuration file /etc/freeradius/3.0/mods-enabled/linelog
including configuration file /etc/freeradius/3.0/mods-enabled/mchap
including configuration file /etc/freeradius/3.0/mods-enabled/eap
including configuration file /etc/freeradius/3.0/mods-enabled/pap
including configuration file /etc/freeradius/3.0/mods-enabled/expr
including configuration file /etc/freeradius/3.0/mods-enabled/digest
including configuration file /etc/freeradius/3.0/mods-enabled/replicate
including configuration file /etc/freeradius/3.0/mods-enabled/dynamic_clients
including configuration file /etc/freeradius/3.0/mods-enabled/loginline
including configuration file /etc/freeradius/3.0/mods-enabled/unix
including configuration file /etc/freeradius/3.0/mods-enabled/always
including configuration file /etc/freeradius/3.0/mods-enabled/realn
including configuration file /etc/freeradius/3.0/mods-enabled/ntlm_auth
including configuration file /etc/freeradius/3.0/mods-enabled/exec
including configuration file /etc/freeradius/3.0/mods-enabled/utf8
including configuration file /etc/freeradius/3.0/mods-enabled/chap
including configuration file /etc/freeradius/3.0/mods-enabled/expiration
including configuration file /etc/freeradius/3.0/mods-enabled/radutmp
including configuration file /etc/freeradius/3.0/mods-enabled/passwd
including configuration file /etc/freeradius/3.0/mods-enabled/preprocess
including configuration file /etc/freeradius/3.0/mods-enabled/unpack
including configuration file /etc/freeradius/3.0/mods-enabled/cache_eap
including configuration file /etc/freeradius/3.0/policy.d/accounting
including configuration file /etc/freeradius/3.0/policy.d/operator-name
including configuration file /etc/freeradius/3.0/policy.d/rfc7542
including configuration file /etc/freeradius/3.0/policy.d/debug
including configuration file /etc/freeradius/3.0/policy.d/dhcp
including configuration file /etc/freeradius/3.0/policy.d/control
including configuration file /etc/freeradius/3.0/policy.d/abfab-tr
including configuration file /etc/freeradius/3.0/policy.d/cui
including files in directory /etc/freeradius/3.0/sites-enabled/
including configuration file /etc/freeradius/3.0/sites-enabled/inner-tunnel
including configuration file /etc/freeradius/3.0/sites-enabled/default
main {
    security {
        user = "freerad"
        group = "freerad"
        allow_core_dumps = no
    }
    name = "freeradius"
    prefix = "/usr"
    localstatedir = "/var"
    logdir = "/var/log/freeradius"
    run_dir = "/var/run/freeradius"
}
main {
    name = "freeradius"
    prefix = "/usr"
    localstatedir = "/var"
    sbindir = "/usr/sbin"
    logdir = "/var/log/freeradius"
    run_dir = "/var/run/freeradius"
    libdir = "/usr/lib/freeradius"
    radacctdir = "/var/log/freeradius/radacct"
    hostname_lookups = no
    max_request_time = 30
    cleanup_delay = 5
    max_requests = 16384
    postauth_client_lost = no
    pidfile = "/var/run/freeradius/freeradius.pid"
    checkrad = "/usr/sbin/checkrad"
    debug_level = 0
}
```

```
Activities Terminal Jun 13 16:19
ubuntu@ubuntu-VirtualBox: /

log {
    proxy_requests = yes
    stripped_names = no
    auth = no
    auth_badpass = no
    auth_goodpass = no
    colourise = yes
    msg_denied = "You are already logged in - access denied"
}
resources {
}
security {
    max_attributes = 200
    reject_delay = 1.000000
    status_server = yes
}
radiusd: ### Loading Realms and Home Servers ###
proxy_server {
    retry_delay = 5
    retry_count = 3
    default_fallback = no
    dead_time = 120
    wake_all_if_all_dead = no
}
home_server localhost {
    ipaddr = 127.0.0.1
    port = 1812
    type = "auth"
    secret = <<< secret >>>
    response_window = 20.000000
    response_timeouts = 1
    max_outstanding = 65536
    zombie_period = 40
    status_check = "status-server"
    ping_interval = 30
    check_interval = 30
    check_timeout = 4
    num_answers_to_alive = 3
    revive_interval = 120
}
```

ii. eapol\_test (note: eapol\_test should be in the same path as wpa\_supplicant)

```
Activities Terminal Jun 13 19:42
ubuntu@ubuntu-VirtualBox: /

MPPE keys OK: 0 mismatch: 1
FAILURE
ubuntu@ubuntu-VirtualBox: $ eapol_test -c /etc/eapol_test/eapol_test.conf -a 127.0.0.1 -s testing123
Reading configuration file '/etc/eapol_test/eapol_test.conf'
Line: 1 - start of a new network block
ssid - hexdump_ascii(len=8):
72 65 61 6c 64 65 20 58 realme X
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=4):
75 73 65 73 user
password - hexdump_ascii(len=10):
74 65 73 74 69 6e 67 31 32 33 testing123
phase1 - hexdump_ascii(len=19):
66 61 73 74 5f 70 72 6f 76 69 73 69 6f 6e 69 6e fast_provisionin
07 3d 32 g=2
phase2 - hexdump_ascii(len=13):
61 75 74 68 3d 4d 53 43 48 41 50 56 32 auth=MSCHAPV2
Priority group 0
id=0 ssid='realme X'
Authentication server 127.0.0.1:1812
RADIUS local address: 127.0.0.1:55104
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: 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
```

Step 3: Capturing the radius packets using tcpdump

```
>_ }
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
```

## Step 4: Analyzed the radius packets through wireshark

The top screenshot shows a single RADIUS packet (No. 1) captured at 0.000000. The packet is an Access-Request from 127.0.0.1 to 127.0.0.1. The packet details pane shows the following structure:

- Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- User Datagram Protocol, Src Port: 55184, Dst Port: 1812
- RADIUS Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The packet is a RADIUS Access-Request packet.

The bottom screenshot shows four duplicate RADIUS packets (Nos. 1, 2, 3, and 4) captured at 0.000000, 2.3.005126, 3.9.008508, and 4.21.009254 respectively. All packets are from 127.0.0.1 to 127.0.0.1. The packet details pane shows the following structure:

- Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- User Datagram Protocol, Src Port: 45448, Dst Port: 1812
- RADIUS Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The packet is a RADIUS Access-Request packet.