PenTest Lab Exercise Ex130 – EAP Wireless

Goal

Exploit a WPA2-EAP wireless network.

Tasks

1. Art Rosenbaum called Hank Hacker to let him know that Art's Tailor Shoppe has deployed several new wireless access points in their facility. They are attempting to provide reasonable security and have configured these three access points to use WPA2-EAP with TTLS and MSChapV2. Your job is to test the efficacy of these efforts to maintain security. Art has provided you with access to a machine that has a wireless adaptor in range of their network (on interface wlan0) to help you in this regard.

   Identify the appropriate access point (artstailor-ddwrt-0, artstailor-ddwrt-1, or artstailor-ddwrt-2) and find its channel number. Your Netlab pod will identify which device you should target in that pod. Kali will notify you of your pod-specified device when you log in.

2. To find the wireless channel being used, you'll want to execute
   ```
   sudo airmon-ng check kill
   ```
   then, to enable the *monitor mode* interface for your adapter, you need to run the following command, which will create a new interface (`wlan0mon`) and delete your old interface (`wlan0`)
   ```
   sudo airmon-ng start wlan0
   ```
   in order to stop processes that can interfere with your activities, then
   ```
   sudo airodump-ng wlan0mon
   ```
   to identify wireless access points and their associated channels and then
   ```
   sudo airmon-ng stop wlan0mon
   ```
   to restore the original state of the interface.

3. You may need to disable the `eth0` interface using the
   ```
   sudo ip link set dev eth0 down
   ```
   command.

4. Employ hostapd-wpe and asleap as described in Scott Miller's senior project document to identify credentials that will allow you to connect

to the wireless network. The notable differences between his document and the current Kali setup are the following:

- hostapd-wpe is installed in /home/kali/hostapd-2.6/hostapd.
- The config file, hostapd-wpe.conf in that same directory, **needs to be customized**! You will need to set the SSID. You should probably use the default channel (1) as there are only a few access points using that channel in this area.
- If you cd to that directory, you can run
  ```
  sudo ./hostapd-wpe hostapd-wpe.conf
  ```
  to capture login credentials.
- If asleap does not succeed, you may be able to use john to crack netntlm hashes.

5. After capturing and cracking credentials as described by Scott Miller, create a wpa_supplicant configuration file to allow you to connect to the EAP network where you captured credentials. Jouni Malinen provides a comprehensive wpa_supplicant config file. You will need to specify the ssid, key_mgmt method, user identity and password, eap type, and phase2 auth type (most likely MSCHAPV2), and possibly a scan_freq value corresponding to the channel of the AP (most likely channel 3 with frequency 2422MHz). If you have problems connecting, you may need to include the scan_ssid=1 parameter setting.

   So your config file will look something like this:
   ```
   network={
    ssid=...
    scan_freq=...
    key_mgmt=...
    identity=...
    password=...
    eap=...
    phase2=...
   }
   ```

6. Connect to that network using wpa_supplicant (look for the string CTRL_EVENT_CONNECTED in wpa_supplicant's output but you must keep

`wpa_supplicant` running), then employ `sudo dhclient wlan0` to establish a DHCP lease on the `wlan0` interface using the station to which you have connected. If your `wlan0` interface becomes unusable by `wpa_supplicant`, you should be able to restore it by running `sudo shutdown -r now` to reboot.

7. Check that `wlan0` is associated with a valid `192.168.0.0/24` address and that you have a default network route (use `ip a` and `ip route` to check this). If the route is not correct, you can adjust it by deleting and adding a default route.

7. Connect to the web server at `45.79.141.10` and inspect the web site to get that which you seek.

8. Write a partial penetration test to report on your activities. Identify the method you used to extract useful information and identify what might be done to prevent such information leakage. (Feel free to consult Malinen's document concerning the `ca_cert` parameter to be used when connecting via `wpa_supplicant` for ideas.)