CNS Assignment: Cracking WPA2-PSK and analyzing IITH Wi-Fi Network Security

Individual Assignment

PART 1: Cracking WPA2-PSK Passphrase

Find instructions of this assignment here in the PDF. Main steps are as follows:

1. Setting up your own Wi-Fi AP. You may follow steps given in the assignment (i.e., setting up stand-alone Wi-Fi AP) or use a laptop or smartphone to setup a hotspot. **Set your ROLLNO as SSID of AP and set passphrase of your choice by choosing WPA2-PSK for security**
2. Capture Wi-Fi MAC packets of your SSID using wireshark on a Linux laptop which is configured as a monitor

   How to capture Wireless frames in monitor mode?

   One approach: create monitor interface to capture management, control, and data packets. Below, mon0 is name of wireless interface. Not all cards support monitor mode, so you may need to contact TAs to borrow USB Wi-Fi dongle that supports monitor mode.

   sudo iw dev wlan0 interface add mon0 type monitor

   sudo ifconfig mon0 up

   sudo wireshark

   and select mon0 to capture in wireshark interfaces list.

3. Capture 4-way handshake b/w your AP and a test client (e.g., another laptop or phone) on the monitor laptop and save it in a pcap file. Note that 4-way handshake takes place at the time of initial client association/authentication with the AP in which both parties derive PTK from PMT.
4. Feed pcap file saved and passphrase dictionary to **aircrack-ng** to crack wpa2-psk passphrase as outlined in the assignment doc.
   a. Explain in what cases cracking fails. Demonstrate both success/failures with suitable screenshots in the assignment report
5. Repeat above steps now on a target victim AP in your neighborhood and showcase your

cracking skills. **As an ethical hacker, you immediately report this vulnerability to the owner of the target victim AP and ask him/her to set strong passphrase which you fail to crack!!**

   a. To be able to capture 4-way on the target victim's network, you need to send de-authentication packet or disassociation packet to a user on that network so that the user is forced to reconnect to the target victim AP.
      i. This requires you identifying existing users on the target victim's network by analyzing its traffic using tools like wireshark or **airodump-ng** and sending fake de-authentication or disassociation message using tools like **aireplay-ng or wifuzz**
      ii. Demonstrate main steps with suitable screenshots in the assignment report

6. Write pseudo code of aircrack-ng's passphrase cracking algorithm which takes pcap file and dictionary as inputs and returns cracked passphrase as the output.
   a. What is the space and time complexity of the algorithm?

PART 2: Analyzing IITH Wi-Fi Network Security

Follow step2 of PART 1 (i.e., setup a monitor laptop, place it close to one of IITH Wi-Fi APs) to capture all Wi-Fi MAC packets on Channel 1/6/11 (any one channel) of 2.4GHz ISM band. Ensure that captured pcap trace contains Wi-Fi MAC packets of IITH Wi-Fi network (i.e., SSID/ESSID=IITH) and answer the following queries using wireshark:

1. Identify one IITH AP (i.e., BSSID=MAC ID) and analyze RSN IE in its beacons/probe responses. Insert screenshot in your report.
2. Identify one client (i.e., MAC ID) associated with the above identified AP. Here client and AP exchange null authentication, association, 801.1X authentication and 4-way handshake messages. Insert screenshot in your report.
3. Analyze 802.1X authentication related messages in the trace to identify EAP authentication method employed in IITH network. Note that EAP supports several methods like EAP-TLS, EAP-SIM, EAP-PEAP. Insert screenshot in your report.
4. Draw message flow diagram for EAP authentication method employed in IITH network and explain what each message is for.
   a. How UID/PWD of client are used for authentication by AS/AAA (AD) server?
5. Does IITH network protect management frames?
6. Like in PART 1, is it possible to crack UID/PWD of a client in WPA2-EAP based IITH network?

7. What attacks are possible on WPA2-EAP based IITH network and how to take countermeasures against them?

Deliverables in a tar ball on GC:

- **Readable Report (PART 1) enumerating steps followed with screenshots for each of the important steps for WPA2-PSK passphrase cracking**
    - **Dictionary and pcap traces collected**
- **Readable Report with screenshots for PART 2**
    - **Pcap trace collected**

Late Policy:
20% cut in marks for each day beyond slip dates.

References

- Attacking tools
- https://www.kali.org/
- https://www.aircrack-ng.org/doku.php?id=links
- https://aircrack-ng.blogspot.in/2017/03/less-known-features-of-aircrack-ng.html
- https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/
- http://sslsrv.cs.wayne.edu/csc5991/wpa2-cracking-video.mp4
- http://sslsrv.cs.wayne.edu/csc5991/de-auth-video.mp4
- https://www.aircrack-ng.org/doku.php?id=aireplay-ng
- https://github.com/wi-fi-analyzer/wifuzz