Assignment 7 : Cracking WPA2-PSK and analyzing Security of IITH Wi-Fi

Group Assignment: Max of 2 students per group who did not pair up for earlier assignments. At least one of the students in the group should have a Wi-Fi radio that could be configurable in Monitor mode for Wi-Fi packet capture, inject spurious Wi-Fi packets onto the channel, etc.

PART A: Cracking WPA2-PSK Passphrase

Find more detailed instructions of this assignment here and here. The 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 set up a hotspot. **Set your two ROLLNOs 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 having a Wi-Fi radio configured in the monitor mode.

   How to capture Wireless frames in monitor mode?

   One approach: create a monitor interface to capture management, control, and data packets. Below, mon0 is the name of a wireless interface. Not all cards support monitor mode, so you need to choose a partner who has a radio that could be configurable in monitor mode.

   ```
   sudo iw dev wlan0 interface add mon0 type monitor

   sudo ifconfig mon0 up

   sudo wireshark
   ```

   and select mon0 to capture in the wireshark interfaces list.

   Other approach: use **airodump-ng tool**

3. Capture 4-way handshake b/w your AP and a test client (e.g., another laptop or phone) on the monitoring 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 PMK. So, you may need to launch a DeAuth attack to force a fresh handshake between client and AP.
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 and failure cases with suitable screenshots in the assignment report

5. Repeat above steps now on a target victim AP in your neighborhood to 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 a strong passphrase which you should fail to crack!!**
   a. To be able to capture 4-way on the target victim's network, you need to send a deAuth 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 all these steps with suitable screenshots in the assignment report
6. Write a pseudo code (1-page max) of aircrack-ng's passphrase cracking algorithm which takes a pcap file and dictionary as inputs and returns cracked passphrase as the output.
   a. What is the space and time complexity of the algorithm?

There is a small dictionary that comes with aircrack-ng - "password.lst". This file can be found in the "test" directory of the aircrack-ng source code. The Wiki FAQ has an extensive list of dictionary sources. You can use John the Ripper (JTR) to generate your own list and pipe them into aircrack-ng.

PART B: Analyzing IITH Wi-Fi Network Security

Capture **1-3 minute pcap trace of IITH Wi-Fi network by using Wi-Fi radio (Monitor mode) of your laptop.** You can use airmon-ng, tcpdump or wireshark for this purpose. Use snaplength option to ensure only the header fields of packets are collected in the trace. The pcap trace should have Wi-Fi authentication related MAC packets of IITH Wi-Fi network (i.e., SSID/ESSID=IITH or IITH-Guest-PWD-IITH@2022) when you try connecting one of your laptops/smartphones to IITH or IITH_Guest Wi-Fi networks. Answer the following queries by analyzing the trace using wireshark:

1. Identify IITH AP (i.e., BSSID=MAC ID) to which your client device is connected to and analyze RSN IE in its beacons/probe responses. Insert screenshot in your report.
2. Identify your own client (i.e., MAC ID and EAP Identity Value) 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 a message flow diagram for the EAP authentication method employed in IITH network and explain what each message is for.
    a. How UID/PWD of clients are used for authentication by AS/AAA (AD) server?
5. Here you enter some wrong password when connecting to IITH Wi-Fi network and observe what kind of authentication related messages are exchanged. Insert a screenshot highlighting the difference between successful and unsuccessful cases in your report.
6. Does IITH network protect management frames?
7. Like in PART 1, is it possible to crack the UID/PWD of a client in a WPA2-EAP based IITH network?
8. What attacks are still possible on the WPA2-EAP based IITH network and how to take countermeasures against them?
9. For the packets that belong to IITH Guest Wi-Fi network (SSID=IITH-Guest-PWD-IITH@2022) in the pcap trace, comment on its authentication mechanism and potential risks for users that connect to this network and how to mitigate them.
10. Here you enter some wrong password when connecting to IITH Guest Wi-Fi network and observe what kind of authentication related messages are exchanged. Insert a screenshot highlighting the difference between successful and unsuccessful cases in your report. Also comment how the call-flow differs compared to connecting to IITH Wi-Fi network.
11. Analyze the RSN IE in beacons/probe responses of your own trace (i.e., one of SSIDs is your two ROLLNOs) collected in PART A of this assignment. Insert screenshot in your report.
12. Comment on how IITH, IITH Guest and your own AP fare against in terms of security mechanisms employed and which one of them is the most secure in your opinion, why?

Deliverables

Deliverables in a tar ball on GC (Single submission by one you would suffice):

- **Readable Report (PART A) enumerating steps followed with screenshots for each of the important steps for WPA2-PSK passphrase cracking**
    - **Dictionary Used**
    - **Pcap traces collected**
- **Readable Report with screenshots for PART B**
    - **Pcap trace collected**

- **Credit Statement (1-pager): share an accurate and detailed description of each of the group member's contributions to the assignment**

References

- Attacking tools
- https://www.aircrack-ng.org/doku.php?id=cracking_wpa
- https://www.aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists
- https://www.ins1gn1a.com/understanding-wpa-psk-cracking/
- 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

ANTI-PLAGIARISM Statement <Include it in your report>

We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. We pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, We understand my responsibility to report honor violations by other students if we become aware of it.

Names and Roll Nos:

Date:

Signature: <keep your initials here>