CS 4820 – Fall 2022

Wireless and Mobile Security

Lab #2

Due: 09/22 11:30PM

In the class, we have learned about brute force attacks against WEP, WPS, and WPA/WPA2 protocols. In this lab, you will have a chance to realize brute force attacks against Wifi APs. For this lab, you are welcome to work as a team (team of 2) or by yourself. Each team tries to crack the wifi password of the same APs.

Steps and Procedures:

Figure out the security protocol each AP (Fitsec-Target-0, 1, 2) uses. (Hint: Monitor the Wifi traffic/signals in the air)

1. Start the WEP Hacking (Hint: example tool: 'aircrack')
   a. Find the AP with WEP
   b. Capture traffic/crack WEP passphrase
2. Start the WPS hacking (Hint: example tool: 'reaver')
   a. Find the target
   b. Launch the attack
3. Brute-force WPA/WPA2 passphrase (Hint: example tool: 'aircrack')
   a. Find the AP with WPA
   b. Capture traffic
   c. Run brute force to crack WPA passphrase

For WPA hacking, the wordlist is provided on Canvas where the password is one of the animal names. The password will be changed once everyone finds it. The password will then be 8-digit long and consist of numbers only.

Report Submission:

Explain what method/tool you used for each item. Provide the scripts/codes/screenshots (not photos taken by phone), if any.

Your report should include following:

Display available WiFi Access Points (with the security protocols).

Show step-by-step how you crack WEP.

Show step-by-step how you crack WPS and WPA/WPA2?

List the passwords of Fitsec-Target-0, Fitsec-Target-1, and Fitsec-Target-2 networks.

What procedure (if any) did you follow to beat the others (gain extra point)? Has it worked? If not, what went wrong? Explain in short.

Extra Credit

1. (+10) Be the first team to crack WEP.
2. (+10) Be the first team to crack WPS.
3. (+10) Be the first team to crack WPA/WPA2.
4. (+10) Be the first team to crack the updated password of WPA/WPA2.
5. (+50) Be the first team to change password of any of the AP.