■ **ECE/CS 4984: Wireless Networks and Mobile Systems** ■

Laboratory 11 At-Home Exercise (E11)

Part I – Objectives

The objective of this exercise is to understand the mechanics of the attacks that were conducted in the in-class lab and investigate possible defenses.

Hardware to be used in this lab assignment:

- Dell notebook with 802.11b card.
- Compaq iPAQ with a dual card sleeve and 802.11b card.
- Intel WLAN gateway.

Part II – At-home Lab Assignment and Report

You are expected to perform the following tasks for the "*ARP cache poisoning"* experiment from the in-class lab:

- Use the screenshots of routing table and ARP table together with the Ethereal capture file to explain the mechanics of this attack.
- Using the iPAQ, notebook, and Intel gateway replicate the attack scenario. Have the iPAQ act as the attacker and use the notebook to record similar observations from the routing and ARP tables.

You are expected to perform the following task for the "*impersonating an access point"* experiment from the in-class lab:

- Use the screenshots from kismet alert interface together with the dumb files produced by kismet to identify broadcasted deassociation messages spoofed by the rogue AP.
- Explain how this attack was made possible and suggest any defenses against it, including any features of WiFi Protected Access (WPA).

Part III – Report

This report will include both in-class and take-home aspects of this lab assignment. Provide a report that answers each of the following questions in order:

Part I – In-class experiments

1. *ARP cache poisoning experiment*
    a. Include the screenshots of the routing and ARP tables from the in-class experiment.
    b. Include the screenshots of the routing and ARP tables from the at-home experiment you conducted.
    c. Provide a brief of explanation of the mechanics of this attack. Refer to the screenshots from the in-class experiment and packets captured by Ethereal to support your explanation.

d. Suggest any possible defenses against this type of attacks.

2. *Impersonating an access point*

   a. Include the screenshots from the kismet alert interface that shows the *broadcasted deassociation messages*.

   b. Provide an explanation of this attack. How was it made possible? Do you suggest any defenses against it, including any features of WiFi Protected Access (WPA)?

   c. If the attacker targeted only a single notebook for his/her DoS attack, do you think the attack would have been detected by the IDS?

Part II – General Conclusions

This is the free-form portion of your report. Provide a summary of lessons learned in this lab, general observations on how each of the tools illustrated by the experiments can be used to launch attacks or provide defense from the network. Feel free to suggest improvements to the experiments.