Virginia Tech ■ ECE/CS 4570: Wireless Networks and Mobile Systems ■ Spring 2006

At-home Exercise 12 (E12)

Report Due: Wednesday, April 20, 2006 (at 4:00 p.m.)

Part I – Objectives and Hardware

The objectives of this at-home exercise are to understand the mechanics of the attacks that were conducted in the in-class laboratory session and to investigate possible defenses against each.

Hardware to be used in this lab assignment:

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

Part II – At-home Laboratory Assignment

ARP cache poisoning

You are expected to perform the following tasks for the "ARP cache poisoning" experiment from the in-class laboratory.

- Use the screenshots of the routing table and ARP table together with the Ethereal capture file to explain the mechanics of this attack.
- Using the iPAQ, notebook computer, and Intel WLAN 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.

Impersonating an access point

You are expected to perform the following task for the "impersonating an access point" experiment from the in-class laboratory.

- Use the screenshots from kismet alert interface together with the dump files produced by kismet to identify broadcast 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

Your report should include results from both the in-class laboratory and the at-home exercise. Provide a report that answers each of the following questions in the order listed here.

Part I – In-class and at-home experiments

1. *ARP cache poisoning experiment* (35%)
    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 in-class 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* (40%)

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

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

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

Part II – General Conclusions (15%)

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.

Note that an additional 10% of the grade is assigned to the presentation, including the overall format, clarity of writing, grammar, and spelling.