ELEC567-Spring 2014: Project- Part II: Network Intrusion Analysis and Defense (25%)

(Due April 10/2014)

Network traffic sample collected over several days' activities is provided in TCPDUMP format (as a separate file: elec567.pcap). The collected data include traces of a real attack conducted by an external hacker against an organization network (the IP address of the organization has been changed for privacy and security reasons). Your task in this subproject is to analyze the network capture of the hacker's activity and decode the hacker's actions.

For this subproject, you are expected to conduct network intrusion investigation by carrying the following two phases:

Phase 1: Attack Intelligence Extraction (15%)

It is your responsibility to analyze the network traffic and extract the attack intelligence. More specifically, provide answers to the following questions:

1. List all the hosts involved in this attack, for each host list the following (2%):
   - Host IP address, and Port(s)
   - Role of the host (e.g. attacker, victim, or stepping stone)
   - Operating System
   - Geo Location
2. Indicate which specific service or services were the target of the attack (2%).
3. What specific vulnerability was exploited in the attack? (2%)
4. Was there malware involved? If yes, what is the name of the malware and the role played by it in the attack? (2%)
5. Indicate whether this was a manual or an automated attack? Justify your answer. (1%)
6. Describe the strategy (attack steps and actions) used by the hacker to attack the victim? Use a sketch to illustrate your answer and highlight the attack timeline. (6%)

Phase 2: Defense Strategies (10%)

Gathering attack intelligence is a cornerstone for implementing and developing network defense strategies to prevent similar attacks from succeeding in the future. In the second phase you will use the attack intelligence obtained in phase 1 to implement adequate defense strategy to prevent or detect similar attack in the future. In particular you must do the following:

1. This network uses Snort as the primary IDS. Create a set of rules to enable Snort to detect all the attack steps discovered in phase 1. Make sure your SNORT rules do not over-fit the attack scenario (5%).
2. Do you think we can prevent this attack or part of it using a network firewall? If yes, which firewall will you use and what are the rules? If no, explain why (4%).
3. Could you suggest any additional defense strategy to protect the FTP server? (1%)

Notes:

- The tcpdump data may be read using any of the following tools (or combination of): snort, wireshark, tcpdump or windump. Wireshark provides a GUI while the other tools are command-line-based.
- Tutorials # 8-10 may be helpful in completing the project.
- Ensure that you follow the submission template for subproject II.