# Lab – TCPDUMP and Snort

Setup:

You will be using a PCAP file for all aspects of this lab. If you are not sure how to read from a PCAP file using tcpdump or snort, refer to man pages for both.

Part I

Objective: To Study the concepts of network packet analysis using TCPDUMP

1. Using the provided PCAP file, you are asked to find all packet(s) that have the Evil bit set. The Evil bit is an IP flag bit that is normally not set. You are encouraged to use TCPDUMP command line filters as it will be much faster and more efficient. Write down the TCPDUMP filter used to find such packet(s) and indicate the number of those packet(s)
2. Using the provided PCAP file, you are asked to find all Kamikaze, Nastygram, Christmas tree and lamp Test segments (Generally means TCP flags SYN, URG, PSH and FIN set). Write down the TCPDUMP filter used to find such packet(s) and indicate the number of those packet(s)
3. Using the provided PCAP file, there are packet(s) with IP options. Find those packet(s) and extract the IP options from the IP header. Explain how someone can tell if an IP header has options? Write down the TCPDUMP filter used to find such packet(s), indicate the number of packet(s) and briefly explain the nature of such options.

Part II

Objective: To study the concepts an IDS system using Snort

Setup: You are expected to write simple snort rules and be able to run snort in NIDS mode using a configuration file.

1. Using the same PCAP file provided, write a snort rule to match all SFUP (SYN, FIN, URG and PSH) flags. How many packets did you find? Is this number

agreeable with number of packet(s) found from Part I using TCPDUMP? Write down the rule used to find those packets.

2. You were told that "root" account was compromised on one of the network servers. The attacker managed to get the "root" password hash string over the network. Find the corresponding packet(s) using snort then display the hash using TCPDUMP. Write and explain all commands used.

## BONUS Question:

You are told someone was trying to brute force www.cn.ryerson.ca forum by providing some dictionary usernames and passwords. Find out the source of such attack and list the username and password being used along with the message the attacker was trying to post to the forum.

Hints: You need to find the specifics for the rule signature by inspecting the www.cn.ryerson.ca forum. Create a snort rule to extract only those packets of interest, then use TCPDUMP to display packets payload.