Student Name: _____

Intrusion Detection

Using Windump

GET YOUR IP

- Open a command prompt (cmd from the run line in Windows)
- Run the **ipconfig** command
- Record your IP _____

OPEN AND USE WINDUMP

- Open a command prompt (cmd from the run line in Windows)
- Change to the C:\ directory.
- Execute the **windump –D** command (finds the interface number for your eth card)
- Record the number of your primary network interface. _____
- Execute the **windump** command (this will capture traffic on your default interface) Do you see any packets? _____
- You can stop the capture by entering **CTRL-C**

CAPTURE AND ANALYSE WEB TRAFFIC

- In command prompt enter the command: windump –i "put your Primary interface number here" port(80)). The command should look like this: **windump –i 1 port(80)**
- Open a web browser and visit a website
- What type of traffic does the port(80) filter capture? _____
- Are websites sending and reciveing information to and from your machine? _____ How do you know?_____

CAPTURE A PING

- Open another Windows command prompt window, #2.
- In command prompt window #1, enter the command: windump –i "put your Primary interface number here" –n host "put your ip address here). The command should look like this: **windump –i 1 –n host 10.123.10.56** (this will capture traffic to your address only (no broadcast traffic))
- In command prompt window #2, enter the command: **ping** "some other IP Address". The command should look like: **ping 10.123.10.2**
- Observe the captured network traffic in command prompt window #1. What is the protocol used for a Windows ping._____
- What was the purpose of the **–n** switch used with windump? _____