

*This homework is due 12/18. Students may work in pairs to complete this lab.*

- Please use a word processor for your solutions and submit your solutions to the TA gmuisa666@gmail.com with "ISA 666 HW#4" as the subject in your email.
- Include both names and G-numbers at the beginning of this lab submission.

### **Introduction**

For those of you who are having issues installing or configuring snort, go ahead download and use this VMware image:

<http://www.vmware.com/vmtn/appliances/directory/185>

Please make note in your submission of the issues you encountered as well as the time you spent trying to resolve those issues.

I have extended the deadline until December 18<sup>th</sup>. Make sure to send a digital copy to gmuisa666@gmail.com with "ISA 666 HW#4" as the subject in your email.

### **Step 1**

Provide snapshots of the following:

- 1 screenshot of your OS screen.
- 4 screenshots maybe about an hour apart of (Base or SGUIL) running. I want to see traffic increasing.

### **Step 2**

Snort rules are of the following form:

*action protocol src\_ip src\_port direction dst\_ip dst\_port (options)*

Answer the following questions regarding writing snort rules:

1. List all the possible "action"s you can use in snort and what do they do?
2. What are the different "protocol"s that may be used?
3. Explain what these rules do:
  - a. log udp any any -> 10.1.1.0/24 1:1024
  - b. log tcp any any -> 10.1.1.0/24 :5000
  - c. log tcp any :1024 -> 192.168.1.0/24 500:
  - d. log tcp any any -> 192.168.1.0/24 !5000:5010
  - e. alert tcp any any -> 192.168.1.0/24 21 (content: "user root"; msg: "Alert");
4. Write a Snort rule that will display an alert when it detects both the SYN and FIN flags are set on the same time.
5. Write a Snort rule that will log all root login to any ftp box on the 10.1.1.0/24 network.