

Homework #3 & 4  
ISA 666 Internet Security Protocols Spring 2007

This homework is due on 4/23 by 4:30 PM. Students may work in pairs to complete this Lab assignment.

**IMPORTANT: Points will be deducted from your grade if you don't follow directions.**

- Submit your solutions in either MS Word or in PDF format. Email your solutions **ONLY** to the TA at [gmuisa666@gmail.com](mailto:gmuisa666@gmail.com) with "ISA 666 HW#3 & 4" as the subject in your email. You will also need to submit a hard copy on the day the assignment is due.
- If you are working in pairs, only **ONE** submission is needed.
- Send both labs as **ONE** submission.
- Make sure to include your **name** and **G-number** in your homework submission.

### **Introduction**

These are two labs to be done in consecutive order. The purpose of the first lab (HW3) is to get you comfortable installing Snort as well as working with Linux. The purpose of the second lab (HW4) is to learn writing Snort rules. The total points for both labs is 200 points.

### **Prerequisites**

Read up on the following topics before starting this lab:

- \* Snort
- \* BASE, ACID, & SQUIL
- MySQL
- Apache
- ADODB
- \* **Focus on this.**

### **Installing Snort (HW3)**

You probably want to install Snort in VMware. You can use any Linux flavor you want. You can install either BASE, SQUIL, or ACID. This is a good guide to start you off.

[http://www.ise.gmu.edu/~duminda/classes/spring07/isa666/Snort\\_Base\\_Minimal.pdf](http://www.ise.gmu.edu/~duminda/classes/spring07/isa666/Snort_Base_Minimal.pdf)

### **Deliverables:**

Provide snapshots of the following:

- 1 screenshot of your OS screen.
- 1 screenshot of the MySQL database (similar to page 9 of the guide).
- 4 screenshots maybe about an hour apart of (BASE, ACID, or SQUIL) running. I want to see traffic increasing.

Some tools you can use to generate traffic:

nmap (<http://www.insecure.org/nmap/download.html>), or  
nessus (<http://www.nessus.org/download/>)

### **Answer the following questions:**

1. What is Snort, when and how would you use it?
2. Compare BASE, ACID, and SQUIL and discuss which you chose and why.
3. Write a statement of something significant you learned.

### **Writing Snort Rules (HW4)**

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.