**Homework 5 – Snort**

- This is an individual assignment and worth 20 points.
- The due is Saturday, October 29, midnight.
- Please zoom in on the outputs.
- Use the accompanying output document to report your results.
- Follow the naming convention.
- YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS.

**Overview**

- The objective of this assignment is to learn how to use snort within a Linux environment. Students will configure simple snort rules and experiment with different scenarios.
- The learning objective is evaluated by examining the outputs captured in screenshots after performing the tasks.

**Background on Snort**

- Snort tutorial
  - https://www.snort.org/
- Snort lab manual
  - Posted on the BB snort folder

**Tasks**

- This assignment is based on the **Labtainer snort** lab manual.
- When you need to execute commands with a superuser permission, use *sudo <command>*. Alternatively, switch into a super user by typing *sudo su*.
- When the Labtainer does not start or work properly, I recommend deleting existing VM and reimport "LabtainerVM-VMWare.ova" or "LabtainerVM-VirtualBox.ova."

**Task 1. Start and stop Snort (sec 4.1 & 4.2)**

- Follow the instructions in sec 4.1 and start **snort**.
- Type **pwd** to check the present working directory (pwd). You need to remember this directory.
- Follow the instructions in sec 4.2 and perform an nmap scan of www.example.com from the remote workstation. Take a screenshot of the ouput *on the snort terminal*.

**Task 2. Write a sample bad rule (sec 4.3)**

- On the snort terminal, move to /etc/snort/rules directory.
- Type: "sudo chmod 777 local.rules". This is to allow changes to the local.rules file. You should know what chmod 777 means.
- Open the local.rules file with nano editor. Add a rule following the instructions in sec 4.3. Take a screenshot of the rule you created.
- Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.
- After the testing, you need to delete the rule you added. You can manually delete the rule or simply add # at the beginning of the rule to comment out. I recommend the second method.

**Task 3. Create a custom rule for confidential traffic (sec 4.4)**

- Open the local.rules file with nano editor. Add a rule following the instructions in sec 4.4. Confirm that this rule is working and take a screenshot of the rule you created.
- To create the rule that captures activities related to confidential business plan document, you need to refer to the class slides on Snort. At the end, the syntax of snort rules is explained in detail.
- Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.

Sec 4.5 is skipped.

**Task 4. Watch internet traffic (sec 4.6)**

- Go to the ws2 (mary) terminal and run nmap: "sudo nmap www.example.com".
- Explain why the output does not include the ICMP PING NMAP alerts that you saw when the remote workstation ran nmap.
- On the gateway terminal, move to /etc directory.
- Type: "sudo chmod 777 rc.local". This allows you to make changes to the file.
- Make a change to the rc.local file following the instructions in sec 4.6.
- Run the script to replace the iptables rules with your new rules: "sudo /etc/rc.local".
- Now restart snort and again run nmap from mary's ws2 computer. Report the output on the snort terminal in a screenshot. Explain why you now can see the ICMP PING NMAP alerts.