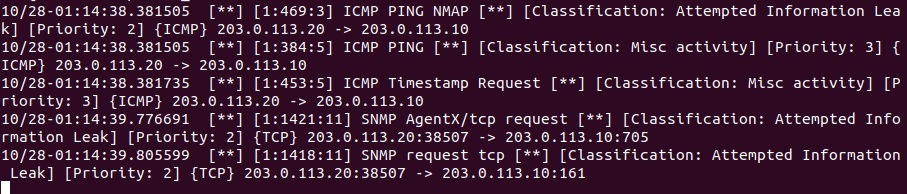
# Homework 5 – Snort

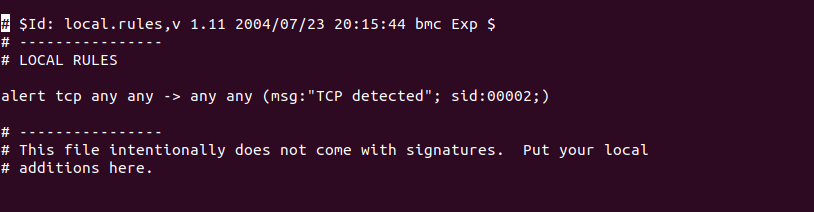
## Task 1. Start and stop Snort (sec 4.1 & 4.2)

* Follow the instructions in sec 4.2 and perform an nmap scan of [www.example.com](http://www.example.com) from the remote workstation. Take a screenshot of the ouput *on the snort terminal*.

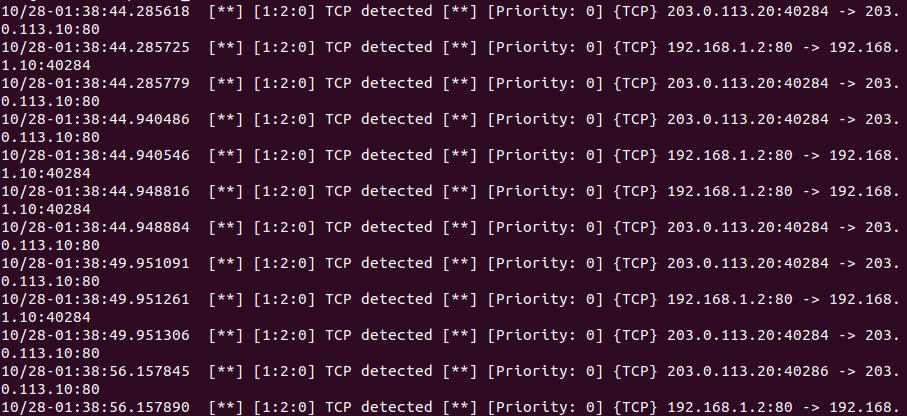


## Task 2. Write a sample bad rule (sec 4.3)

* 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.

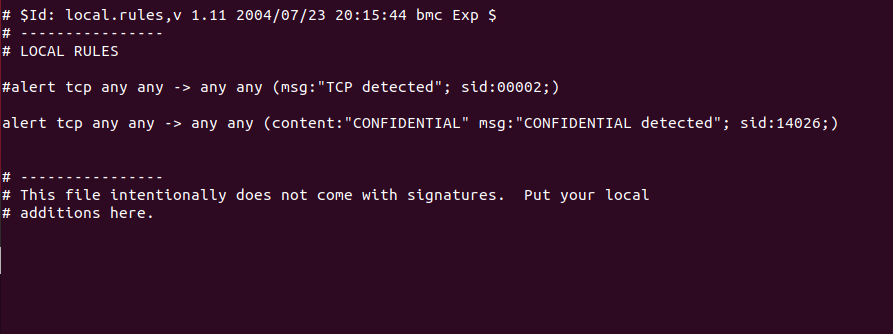


* Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.



## 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.

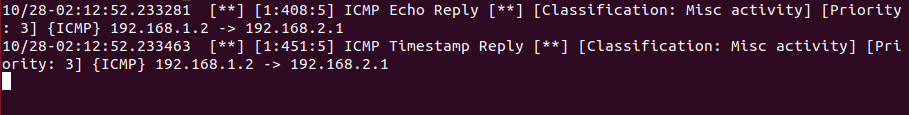


* Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.



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

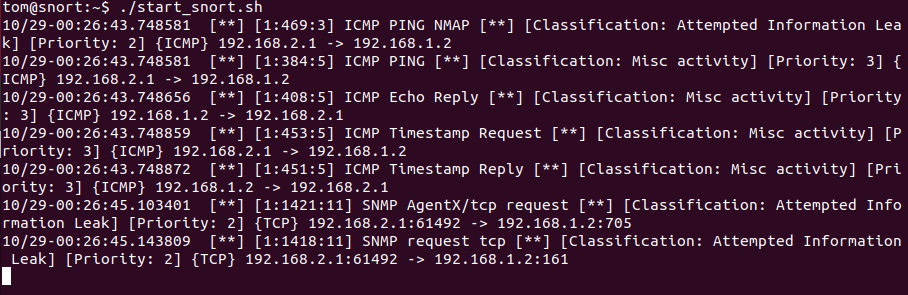
* Go to the ws2 (mary) terminal and run nmap: “sudo nmap [www.example.com](http://www.example.com)”.



* Explain why the output does not include the ICMP PING NMAP alerts that you saw when the remote workstation ran nmap.

Snort isn’t configured for internal devices

* 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.



The rule was added to allow mirrored internal traffic between machines allowing mary to nmap the site.