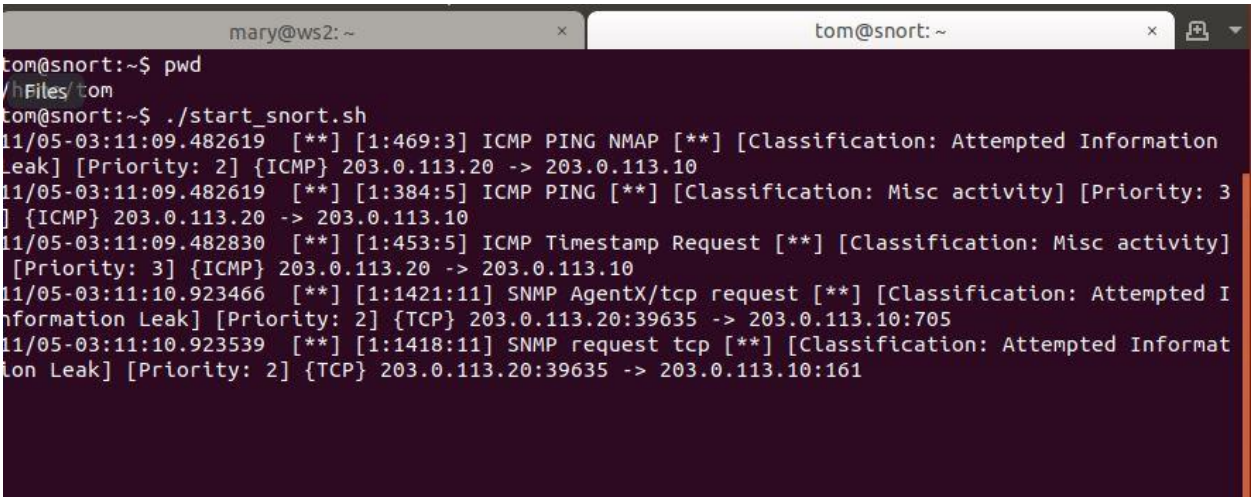
Homework 5 – Snort

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

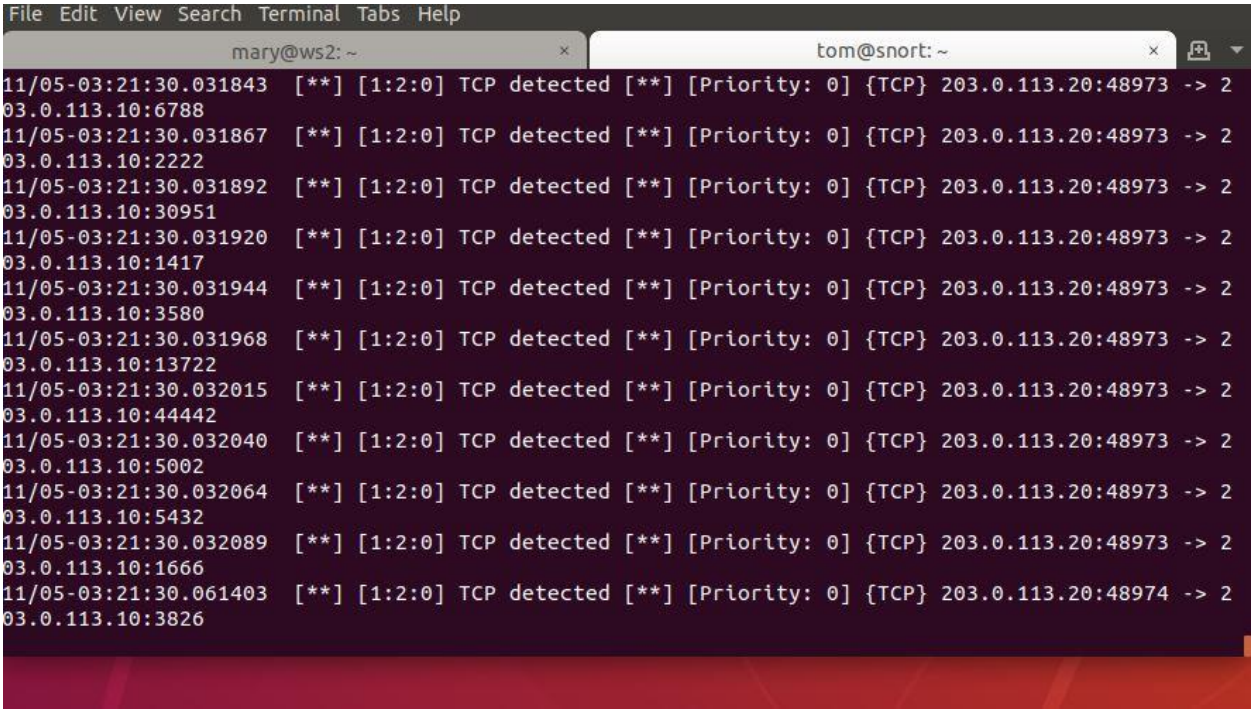
- Follow the instructions in sec 4.2 and perform an nmap scan of www.example.com from the remote workstation. Take a screenshot of the ouput *on the snort terminal*.



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.

```
:om@snort:~$ sudo ./start_snort.sh
11/05-03:37:52.589909  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information
Leak] [Priority: 2] {ICMP} 203.0.113.20 -> 203.0.113.10
11/05-03:37:52.589909  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3
] {ICMP} 203.0.113.20 -> 203.0.113.10
11/05-03:37:52.590081  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
11/05-03:37:53.980962  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Informat
ion Leak] [Priority: 2] {TCP} 203.0.113.20:63049 -> 203.0.113.10:161
11/05-03:37:54.010565  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted I
nformation Leak] [Priority: 2] {TCP} 203.0.113.20:63049 -> 203.0.113.10:705
11/05-03:38:35.874575  [**] [1:2:0] detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1
10:41560
```

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.

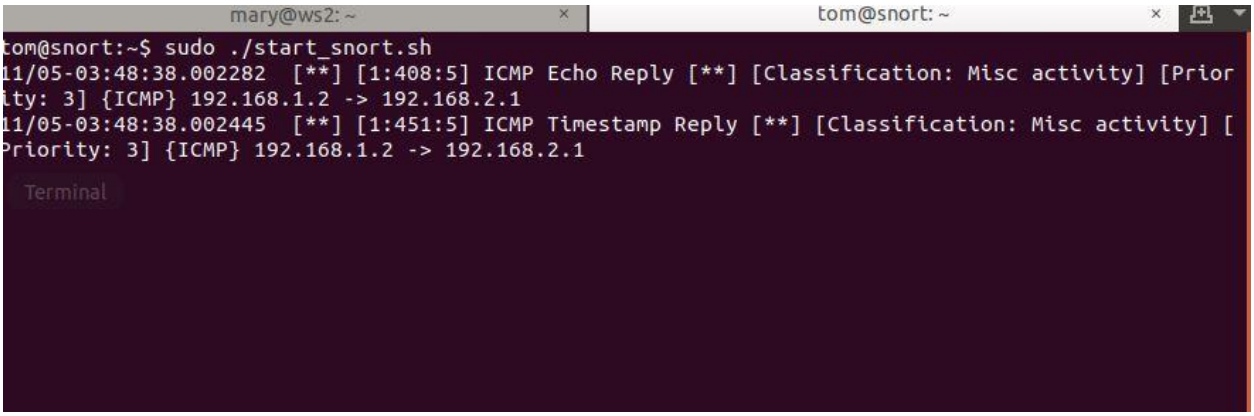
Mary's traffic is not being filtered through the snort rule that would cause that output, meaning snort is not configured for use between internal devices. It needs to be mirrored to snort for the output to be displayed correctly.

- Make a change to the rc.local file following the instructions in sec 4.6. Display the rule.

```
iptables --delete-chain
iptables -t nat --delete-chain
iptables -t mangle --delete-chain
iptables -t mangle -A PREROUTING -i $lan2 -j TEE --gateway 192.168.3.1
```

Settings

- 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.


mary@ws2: ~
tom@snort: ~
tom@snort:~$ sudo ./start_snort.sh
11/05-03:48:38.002282 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Prior
ity: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
11/05-03:48:38.002445 [**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc activity] [
Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
Terminal