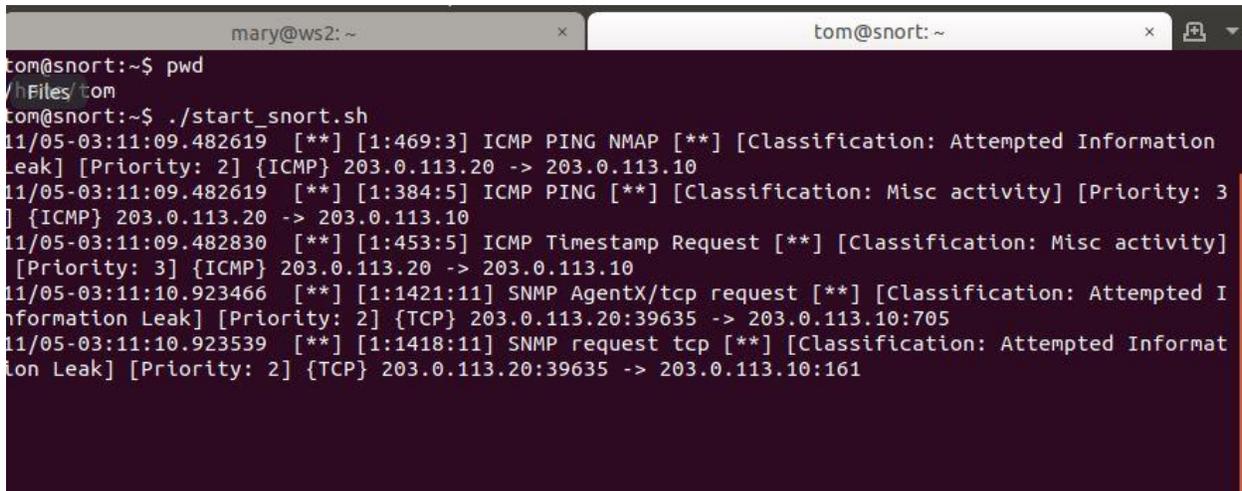


Homework 5 – Snort

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

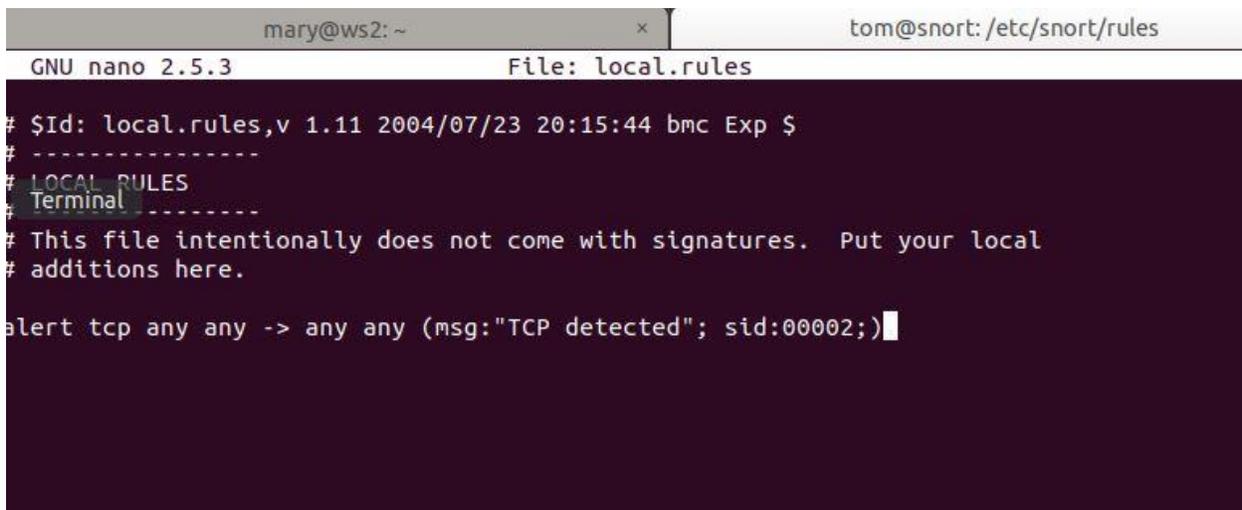
- Follow the instructions in sec 4.2 and perform an nmap scan of www.example.com from the remote workstation. Take a screenshot of the output on the snort terminal.



```
mary@ws2: ~ x tom@snort: ~ x
tom@snort:~$ pwd
/hFiles/tom
tom@snort:~$ ./start_snort.sh
11/05-03:11:09.482619  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 203.0.113.20 -> 203.0.113.10
11/05-03:11:09.482619  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
11/05-03:11:09.482830  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
11/05-03:11:10.923466  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:39635 -> 203.0.113.10:705
11/05-03:11:10.923539  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:39635 -> 203.0.113.10:161
```

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.



```
mary@ws2: ~ x tom@snort: /etc/snort/rules
GNU nano 2.5.3 File: local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# Terminal -----
# This file intentionally does not come with signatures. Put your local
# additions here.
alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)
```

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

```
File Edit View Search Terminal Tabs Help
mary@ws2: ~ x tom@snort: ~ x
11/05-03:21:30.031843  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:6788
11/05-03:21:30.031867  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:2222
11/05-03:21:30.031892  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:30951
11/05-03:21:30.031920  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:1417
11/05-03:21:30.031944  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:3580
11/05-03:21:30.031968  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:13722
11/05-03:21:30.032015  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:44442
11/05-03:21:30.032040  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:5002
11/05-03:21:30.032064  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:5432
11/05-03:21:30.032089  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48973 -> 2
03.0.113.10:1666
11/05-03:21:30.061403  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:48974 -> 2
03.0.113.10:3826
```

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](#).

```
-----
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> any any (content:"CONFIDENTIAL"; msg:"detected"; sid:00002$
```

- Restart snort and test this rule following the instructions. [Report the output displayed on the snort terminal in a screenshot](#).

```

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

```

- 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: ~ x tom@snort: ~ x
tom@snort:~$ sudo ./start_snort.sh
11/05-03:48:38.002282  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 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
```