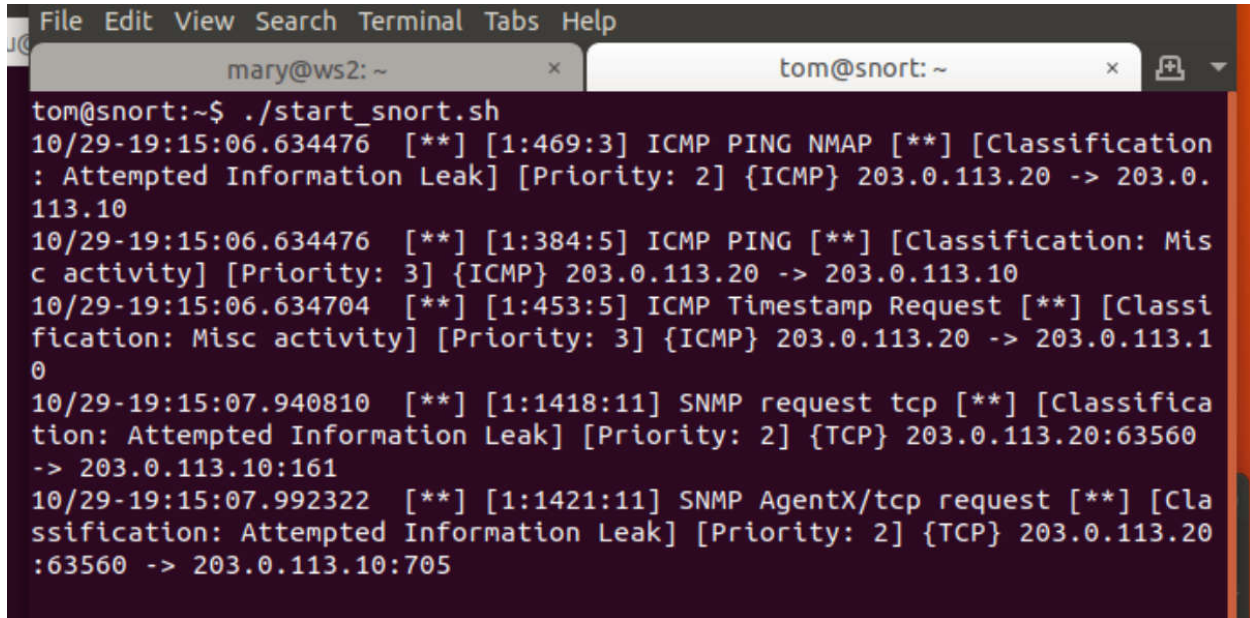


Homework 5 – Snort

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.](#)

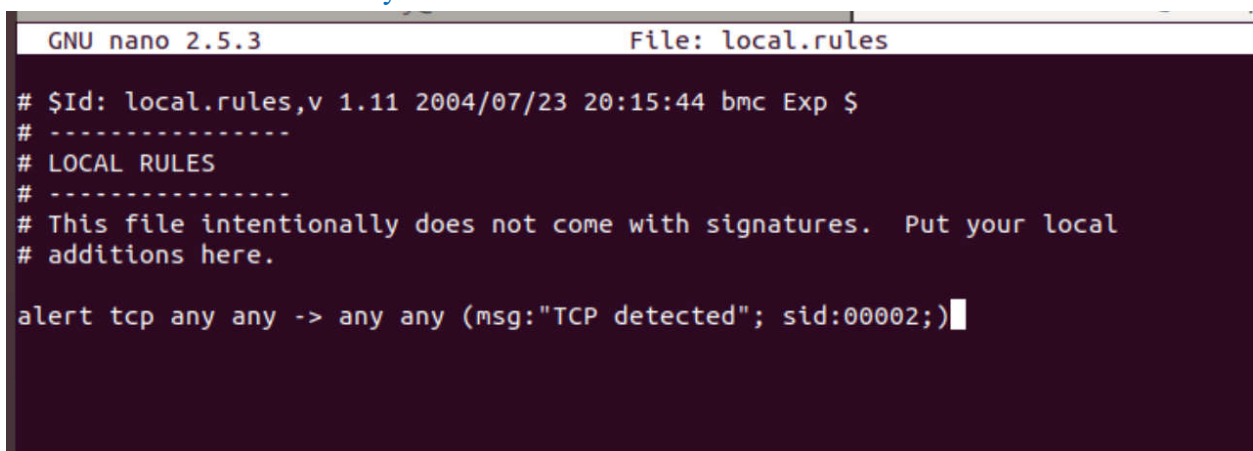


```
File Edit View Search Terminal Tabs Help
mary@ws2: ~ x tom@snort: ~ x
tom@snort:~$ ./start_snort.sh
10/29-19:15:06.634476  [**] [1:469:3] ICMP PING NMAP [**] [Classification
: Attempted Information Leak] [Priority: 2] {ICMP} 203.0.113.20 -> 203.0.
113.10
10/29-19:15:06.634476  [**] [1:384:5] ICMP PING [**] [Classification: Mis
c activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
10/29-19:15:06.634704  [**] [1:453:5] ICMP Timestamp Request [**] [Classi
fication: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.1
0
10/29-19:15:07.940810  [**] [1:1418:11] SNMP request tcp [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:63560
-> 203.0.113.10:161
10/29-19:15:07.992322  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Cla
ssification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20
:63560 -> 203.0.113.10:705
```

Pwd = /home/tom

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.](#)



```
GNU nano 2.5.3 File: local.rules
# $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 (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.](#)

```

mary@ws2: ~
tom@snort: ~
0:80
10/29-19:26:44.277959  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:58
450
10/29-19:26:44.278396  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:58
450
10/29-19:26:44.278488  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:58450 -> 203.0.113.1
0:80
10/29-19:26:44.527629  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:58450 -> 203.0.113.1
0:80
10/29-19:26:44.527846  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:58
450
10/29-19:26:44.527873  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:58450 -> 203.0.113.1
0:80
10/29-19:26:44.528958  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:58450 -> 203.0.113.1
0:80
10/29-19:26:44.529065  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:58
450
10/29-19:26:44.570528  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:58450 -> 203.0.113.1
0:80
10/29-19:26:49.533626  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:58
450
10/29-19:26:49.533786  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:58450 -> 203.0.113.1
0:80
10/29-19:26:49.533810  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:58
450

```

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](#).

```

GNU nano 2.5.3      File: local.rules
# $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:"Confidential Info Accessed"; sid:00003;)

```

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

```

tom@snort:~/etc/snort/rules$ cd ~/home/tom
tom@snort:~$ ./start_snort.sh
10/29-20:09:08.087868  [**] [1:3:0] Confidential Info Accessed [**] [Priority: 0] {TCP}
192.168.1.2:80 -> 192.168.1.10:58480

```

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. IPTABLES is not configured to route the lan2 interface that mary is on.

- 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.

```
tom@snort:~$ ./start_snort.sh
10/29-20:19:00.248586  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.2.1 -> 192.168.1.2
10/29-20:19:00.248586  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.2.1 -> 192.168.1.2
10/29-20:19:00.248615  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
10/29-20:19:00.248748  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.2.1 -> 192.168.1.2
10/29-20:19:00.248762  [**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
10/29-20:19:01.594537  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.1:53167 -> 192.168.1.2:705
10/29-20:19:01.630869  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.1:53167 -> 192.168.1.2:161
```

The IPTABLES rule we added to the gateway script specifically included the lan2 interface with “-i \$lan2” in the rule.