Snort Lab

Name: __Eric Wellmaker________________________

1 Overview

This exercise introduces the use of the snort system to provide intrusion detection within a Linux environment. Students will configure simple snort rules and experiment with a network intrusion detection system, (IDS).

2 Lab Environment

```
	labtainer snort
```

3 Network Configuration

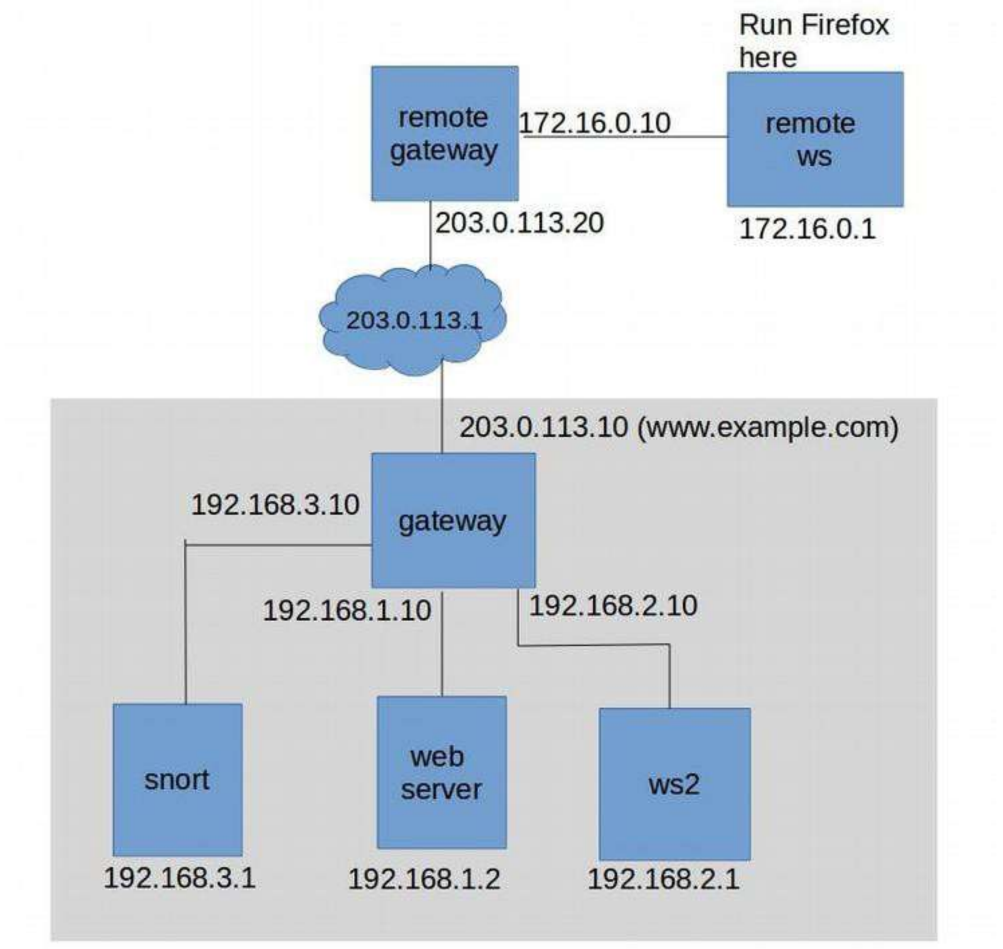
This lab includes several networked computers, one connected to each component. The title of each terminal window and the tab name indicate which system that terminal controls. The gateway is configured with iptables to use NAT to translate sources addresses of traffic from internal IP addresses, e.g., 192.168.2.1, to our external address, i.e., 203.0.113.10. The iptables in the gateway also routes web traffic (ports 80 and 443) to the web server component by translating the externally visible destination address to the internal web server address.

The gateway is also configured to mirror traffic that enters the gateway via either the 203.0.113.10 link, or the link to the web server. This mirrored traffic is routed to the snort component. This mirroring allows the snort component to reconstruct TCP sessions between the web server and external addresses.

The snort component includes the Snort IDS utility. It also includes Wireshark to help observe traffic being mirrored to the snort component.

The web server runs Apache and is configured to support SSL for web pages in the www.example.com domain.

The remote ws component includes the Firefox browser, and a local `/etc/hosts` file that maps www.example.com to the external address of the gateway, i.e., 203.0.113.10. The internal workstation (ws2) also includes Firefox and an entry in `/etc/hosts` for www.example.com. Both workstations also include the nmap utility.



4 Tasks

Review the network topology. In particular, consider the iptables settings on the gateway. These can be seen by reviewing the commands in `/etc/rc.local`, which are used to define the NAT translations and, critically for this lab, mirror traffic to the snort component.

4.1 Starting and stopping snort

The Snort utility is installed on the snort component. The home directory includes a `start snort.sh` script that will start the utility in *Network Intrustion Dection Mode*, and display alerts to the console. For this lab, you are required to start snort with:

```
        ./start_snort.sh
```

When starting snort you will not receive any type of menu or message. Alerts will be displayed when triggered by rules.

When it comes time to stop snort, e.g., to add rules, simply use `CTL-C`.

4.2 Pre-configured Snort rules

The Snort utility includes a set of pre-configured rules that create alerts for known suspicious network activity. The configuration on the snort component is largely as it exists after initial installation of the snort utility. To see an example of some of the preconfigured rules, ensure you have snort running and perform an nmap scan of www.example.com from the remote workstation:

```
sudo nmap www.example.com
```

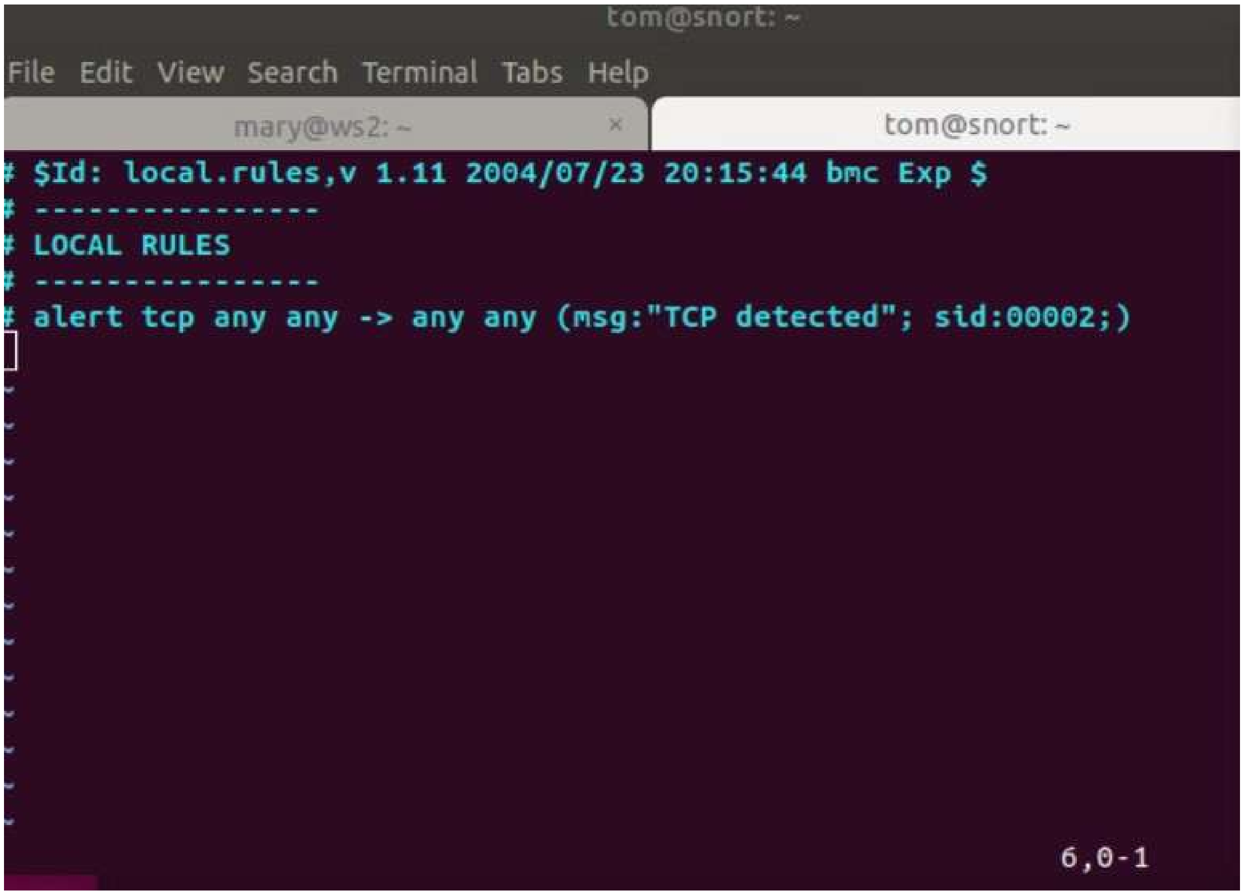
Note the alerts displayed at the snort console. The rules that generate these alerts can be seen, along with all rules, in `/etc/snort/rules/`

4.3 Write a simple (bad) rule

Custom rules are typically added to the file at `/etc/snort/rules/local.rules` Stop snort and add a rule that generates an alert for each packet within a TCP stream.

```
alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)
```

Add the above rule to the `/etc/snort/rules/local.rules` file using an editor of your choice such as `vim` or `nano`. "Generate an alert whenever a TCP packet from any address on any port is sent to any address on any port, and include the message tagged as msg:, and give the rule an identifier of 00002."



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)

~
~
~
~
~
~
~
~
~
~
~
~
~
                                                           6,0-1
```

4.4 Effects of encryption

Alter the URL to make use of the web server SSL function. Change the url to `https://www.example.com/plan.html`. You should accept the security warning as we trust the self-signed cert presented by the website.

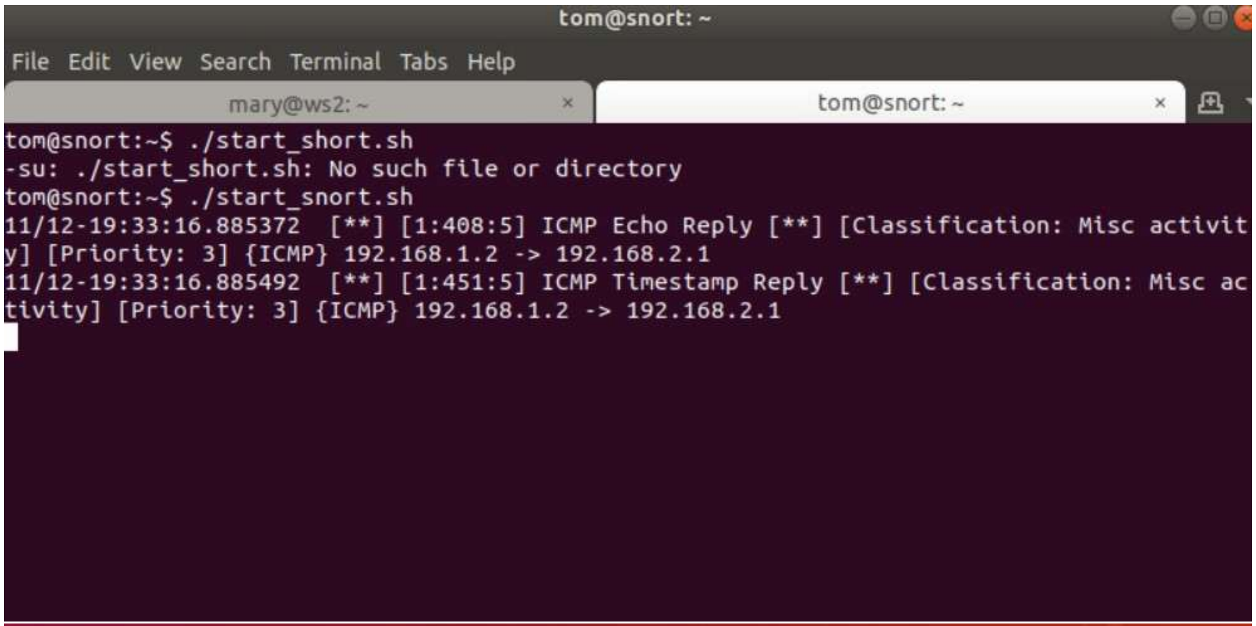
No alert because the rule was modified.

One solution to this problem is to use a reverse proxy in front of the web server. This reverse proxy would handle the incoming web traffic and manage the SSL connections. The web server would then receive only clear-text HTTP traffic, and outgoing traffic from the web server could then be mirrored to the IDS.

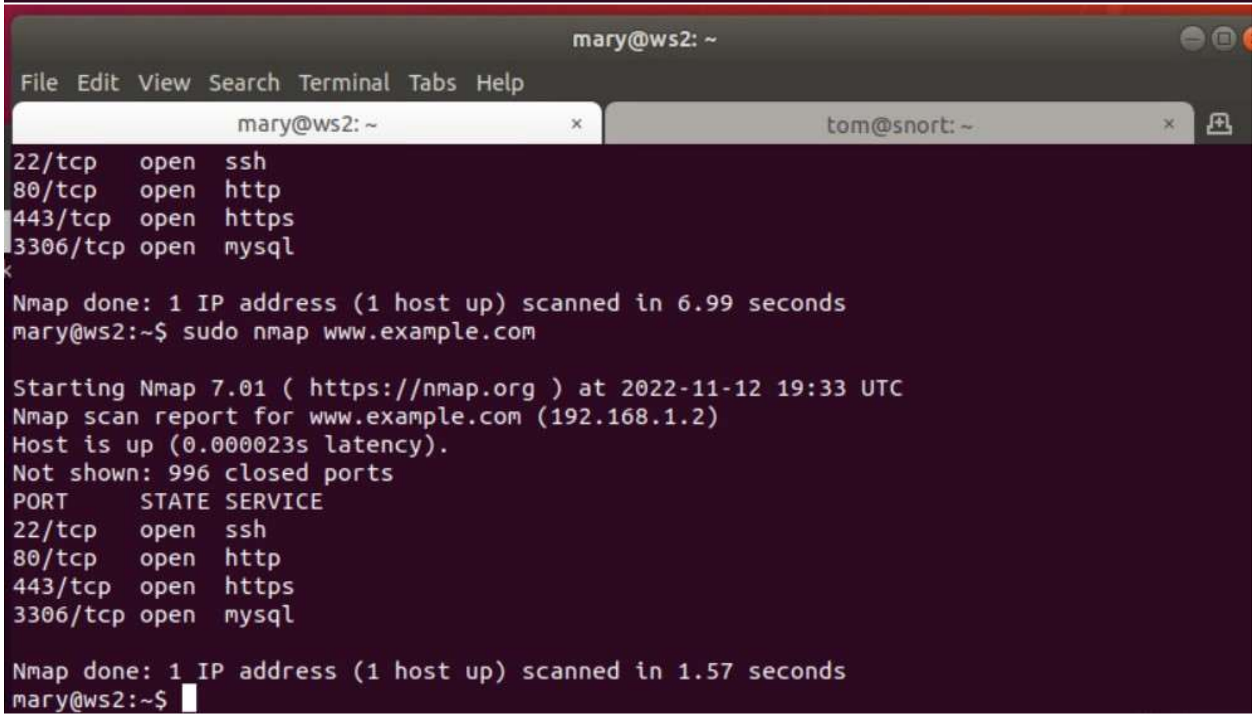
4.6 Watching internal traffic

Go to the ws2 (mary) component and run nmap:

```
sudo nmap www.example.com
```



```
tom@snort:~$ ./start_short.sh
-su: ./start_short.sh: No such file or directory
tom@snort:~$ ./start_snort.sh
11/12-19:33:16.885372  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activit
y] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
11/12-19:33:16.885492  [**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc ac
tivity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
```



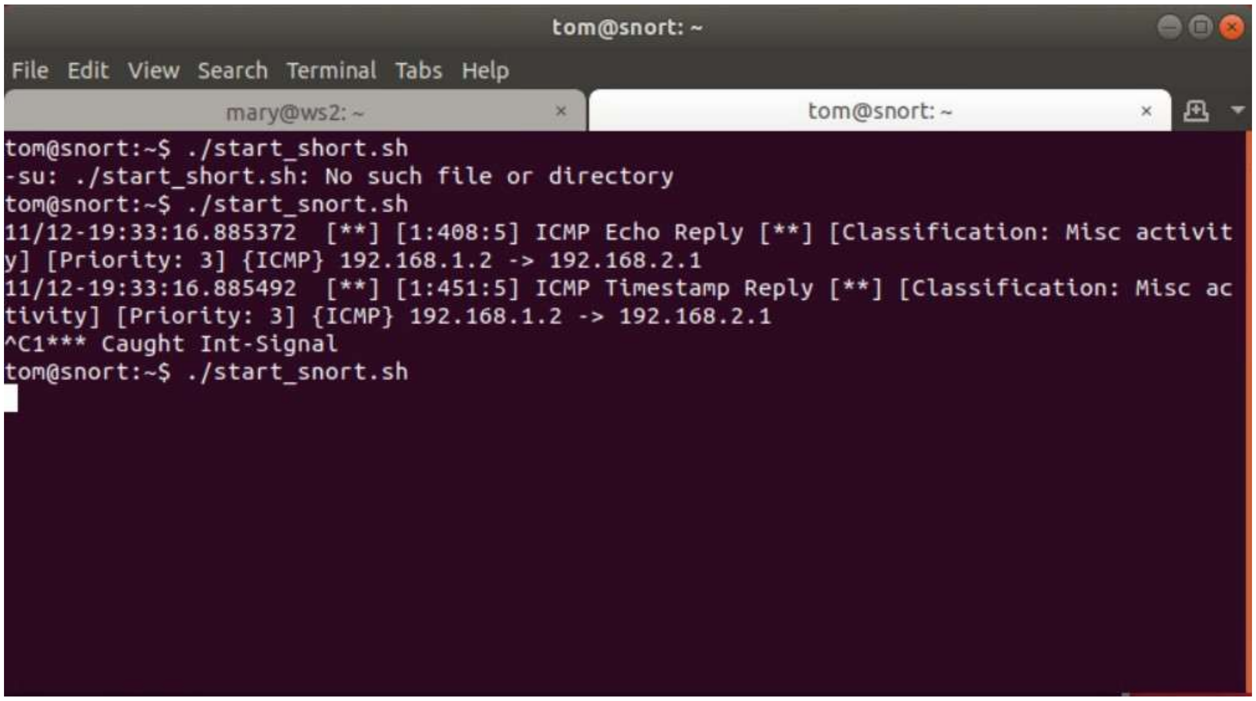
```
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds
mary@ws2:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2022-11-12 19:33 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000023s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
mary@ws2:~$
```

Go to the gateway component and edit the `/etc/rc.local` script so that traffic from Mary's work- station is mirrored to the snort component that defines the packet mirroring:

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

Running the script to replace the `iptables` rules with new rules:

```
sudo /etc/rc.local
```



```
tom@snort:~$ ./start_short.sh
-su: ./start_short.sh: No such file or directory
tom@snort:~$ ./start_snort.sh
11/12-19:33:16.885372  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activit
y] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
11/12-19:33:16.885492  [**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc ac
tivity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
^C1*** Caught Int-Signal
tom@snort:~$ ./start_snort.sh
```

4.7 Distinguishing traffic by address

Start Firefox on mary's ws2 computer to view the confidential business plan:

```
firefox www.example.com/plan.html
```

Observe the snort console. The keen minds at the startup need to view their confidential business plan without IDS alerts firing off. But they do want to monitor internal computers for suspicious traffic, e.g., nmap scans. In this task, adjust snort rule so that the CONFIDENTIAL alert only fires when the plan is accessed by addresses outside of the site.

```
alert <protocol> <source_addr> <src_port> -> \

<dest_addr> <dest_port> <rule options in parens>
```

The snort rules include two address fields: `source_addr` and `dest_addr`. These addresses are used to check the source from which the packet originated and the destination of the packet. The address may be a single IP address or a network address. For network addresses, the address is followed by a slash character and number of bits in the netmask. For example, a network address of 192.168.2.0/24 represents C class network 192.168.2.0 with 24 bits in the network mask.

Note that as a result of the use of NAT, all traffic from the web server destined for an external address will have a destination address of the gateway, (i.e., 192.168.1.10), while web traffic destined for internal users will have destination addresses that match the internal user.

```
stoplab snort------------
```

Portions of this lab were developed for the Labtainers framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under sponsorship from the National Science Foundation.