Design of Secure Computer Systems

Lab 08

SNORT

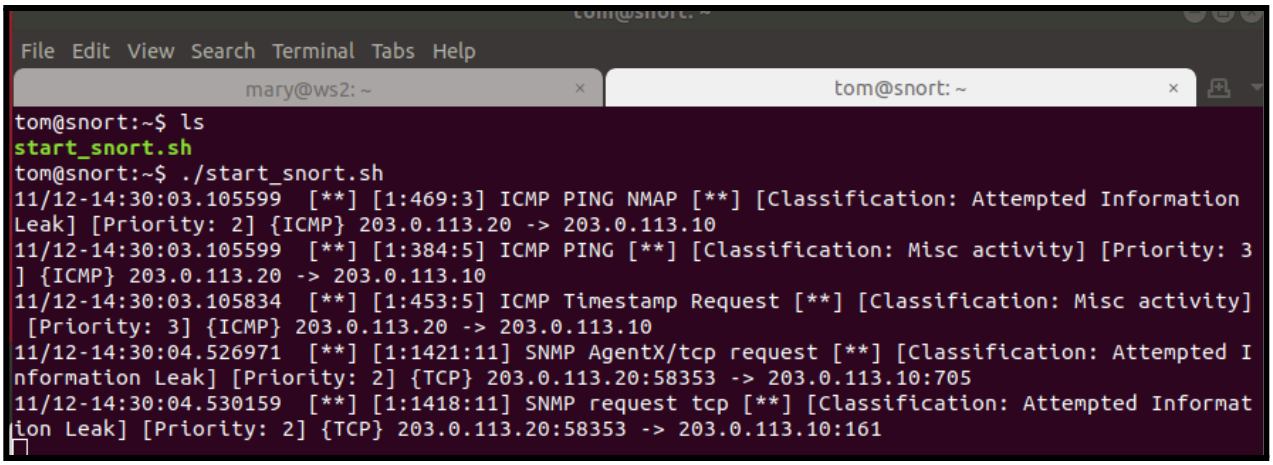
This LAB will introduce the use of the snort system to provide intrusion detection within a Linux environment.

Name: Rakshita Mathur

Snort

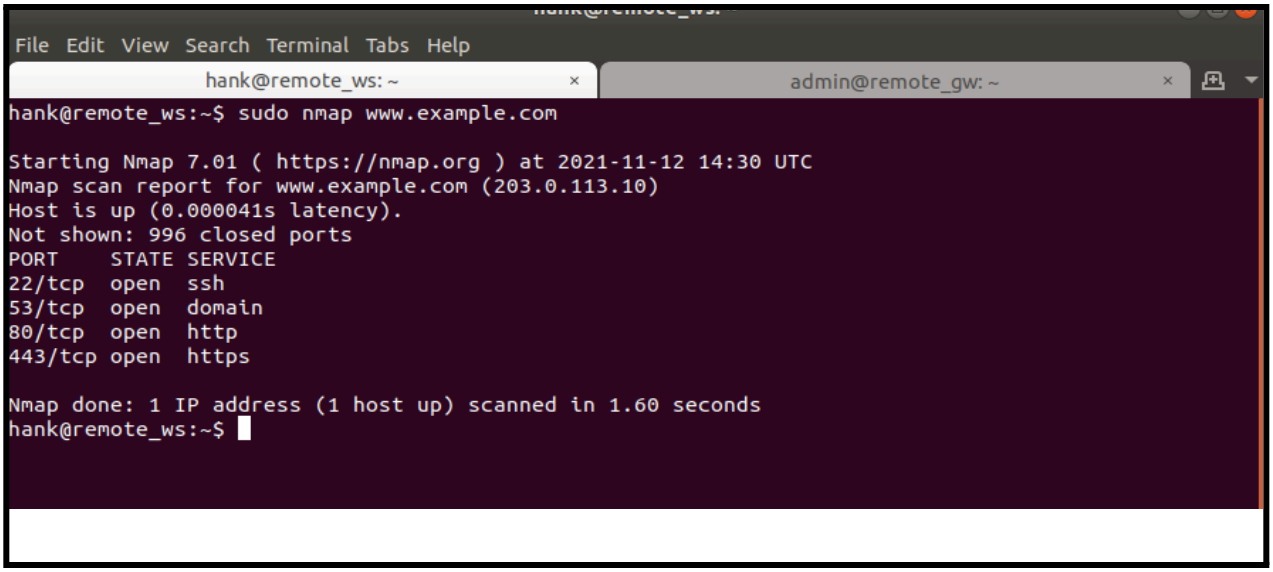
1. Starting and stopping Snort

Snort is installed and working
Command used: **./ start_snort.sh** in tom@snort window
And to get back to the sport command we use ctrl+c



2. Pre configured Snort rules

And to check whether the snort is up and working we use **nmap www.example.com** and see that snort is showing some alerts, hence it is working.



Looking at the snort rule we use the command **ls /etc/snort/rules/**

```
tom@snort:~$ ls /etc/snort/rules/
attack-responses.rules          community-web-dos.rules    policy.rules
backdoor.rules                  community-web-iis.rules    pop2.rules
bad-traffic.rules               community-web-misc.rules   pop3.rules
chat.rules                      community-web-php.rules    porn.rules
community-bot.rules             ddos.rules                 rpc.rules
community-deleted.rules         deleted.rules              rservices.rules
community-dos.rules             dns.rules                  scan.rules
community-exploit.rules         dos.rules                  shellcode.rules
community-ftp.rules             experimental.rules         smtp.rules
community-game.rules            exploit.rules              snmp.rules
community-icmp.rules            finger.rules               sql.rules
community-imap.rules            ftp.rules                  telnet.rules
community-inappropriate.rules   icmp-info.rules            tftp.rules
community-mail-client.rules     icmp.rules                 virus.rules
community-misc.rules            imap.rules                 web-attacks.rules
community-nntp.rules            info.rules                 web-cgi.rules
community-oracle.rules          local.rules                web-client.rules
community-policy.rules          misc.rules                 web-coldfusion.rules
community-sip.rules             multimedia.rules           web-frontpage.rules
community-smtp.rules            mysql.rules                web-iis.rules
community-sql-injection.rules   netbios.rules              web-misc.rules
community-virus.rules           nntp.rules                 web-php.rules
community-web-attacks.rules     oracle.rules               x11.rules
community-web-cgi.rules         other-ids.rules
community-web-client.rules      p2p.rules
tom@snort:~$
```

And as snort is an open source software it has a lot of community rules. But we are interested in local rules in which we can write our own rules.

Next we open a rule using the command **nano etc/snort/rules/icmp.rules** and see what it looks like

```
  GNU nano 2.5.3              File: /etc/snort/rules/icmp.rules

# Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
# This file may contain proprietary rules that were created, tested and
# certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
# rules that were created by Sourcefire and other third parties and
# distributed under the GNU General Public License (the "GPL Rules").  The
# VRT Certified Rules contained in this file are the property of
# Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
# The GPL Rules created by Sourcefire, Inc. are the property of
# Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
# Reserved.  All other GPL Rules are owned and copyrighted by their
# respective owners (please see www.snort.org/contributors for a list of
# owners and their respective copyrights).  In order to determine what
# rules are VRT Certified Rules or GPL Rules, please refer to the VRT
# Certified Rules License Agreement.
#
#
# $Id: icmp.rules,v 1.25.2.1.2.2 2005/05/16 22:17:51 mwatchinski Exp $
#-----------
# ICMP RULES
#-----------
#
# Description:
# These rules are potentially bad ICMP traffic.  They include most of the
# ICMP scanning tools and other "BAD" ICMP traffic (Such as redirect host)
#
# Other ICMP rules are included in icmp-info.rules

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8; content:"ISSPNGRQ$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; icode:0; itype:8; co$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize:20; icmp_id:0$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; itype:8; reference$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; dsize:0; icmp_id:666 $
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode:1; itype:5; refer$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:0; itype:5; refere$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsize:8; itype:8; cont$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; ipopts:rr; itype:0;$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; icode:0; itype:8; c$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench"; icode:0; itype:4; class$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Broadscan Smurf Scanner"; dsize:4; icmp$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING speedera"; itype:8; content:"89|3A$
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP TJPingPro1.1Build 2 Windows"; itype:8; $
                          [ Read 50 lines (Warning: No write permission) ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

3. Write a Simple (bad) rule

We open the local rule file using the command: **sudo nano etc/snort/rules/local.rules**
And wrote the (bad) rule in the local rule file.

```
File  Edit  View  Search  Terminal  Tabs  Help
mary@ws2: ~                    tom@snort: ~
  GNU nano 2.5.3            File: /etc/snort/rules/local.rules                Modified

# $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;)
```

After saving the file we could see the rule by using **cat etc/snort/rules/local.rules**

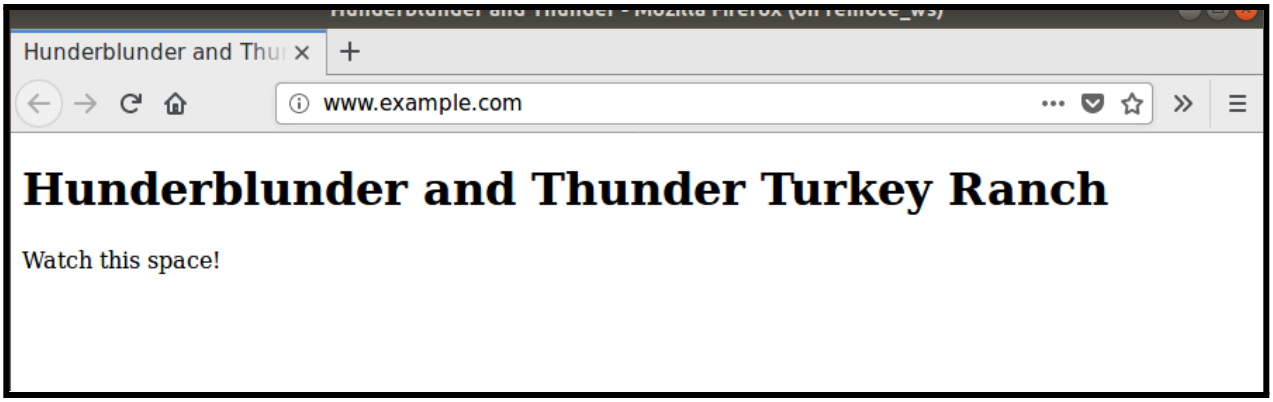
```
tom@snort:~$ cat /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)

tom@snort:~$
```

So when we open a webpage using command: **firefox www.example.com**

```
hank@remote_ws:~$ firefox www.example.com
```

The web page pops up in the browser.



But in the snort window multiple alerts were generating which was not helpful that's why it was a bad rule

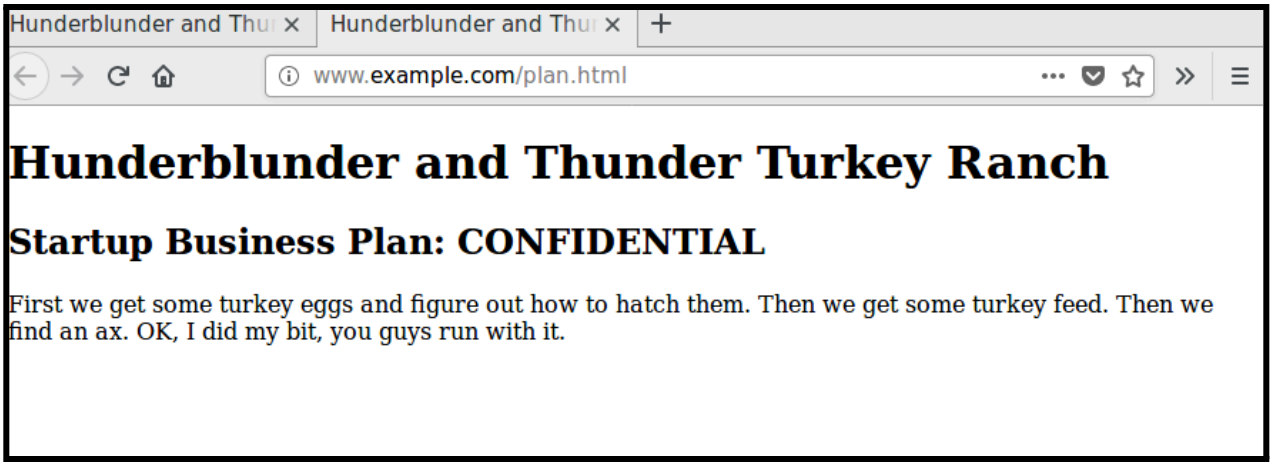
```
tom@snort:~$ ./start_snort.sh
11/12-15:10:46.752204  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:46.752298  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
11/12-15:10:46.752333  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:47.107268  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:47.107313  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
11/12-15:10:47.107728  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
11/12-15:10:47.108080  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:47.439162  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:47.439370  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
11/12-15:10:47.439403  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:47.446633  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:47.446857  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
11/12-15:10:47.490940  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:52.452512  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
11/12-15:10:52.452661  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 203.0.113.20:53270 -> 2
03.0.113.10:80
11/12-15:10:52.452690  [**] [1:2:0] TCP detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.1
68.1.10:53270
```

4. Custom rule for CONFIDENTIAL traffic

A confidential rule includes the word ”CONFIDENTIAL” in the alert message, and gives the rule its own unique sid.

We open the html page using the following command

```
hank@remote_ws:~$ firefox www.example.com/plan.html
```



So now in the local rules we write our own rule to detect the word confidential and get an alert message. We save the change.

```
mary@ws2: ~                                   tom@snort: ~
  GNU nano 2.5.3            File: /etc/snort/rules/local.rules                Modified

# $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:"Detected CONFIDENTIAL"; content:"CONFIDENTIAL"; sid:000004;)
```

And see the file content using the cat command as: **cat etc/snort/rules/local.rules**

```
tom@snort:~$ cat /etc/snort/rules/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:"Detected CONFIDENTIAL"; content:"CONFIDENTIAL"; sid:000004;)
tom@snort:~$
```

Then we start snot uing **./start_snort.sh** command.

When we run the web page with no confidential information the snort did not show any alerts.

```
tom@snort:~$ ./start_snort.sh
```

Hunderblunder and Thunder - Mozilla Firefox (on remote_ws)

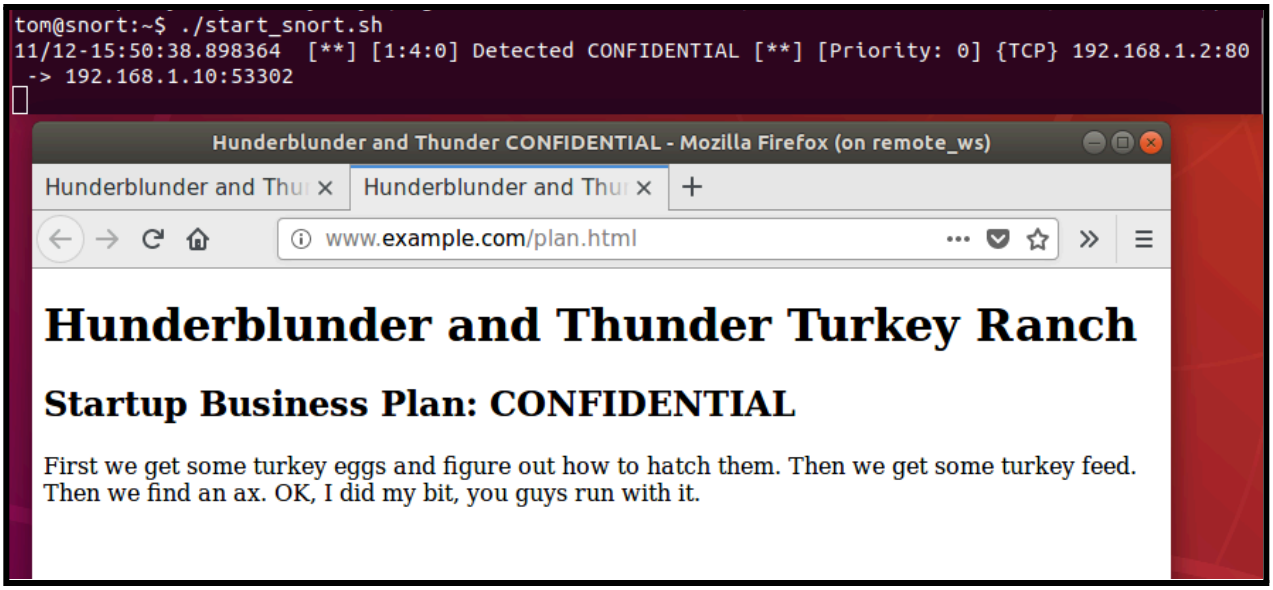
Hunderblunder and Thu

www.example.com

Hunderblunder and Thunder Turkey Ranch

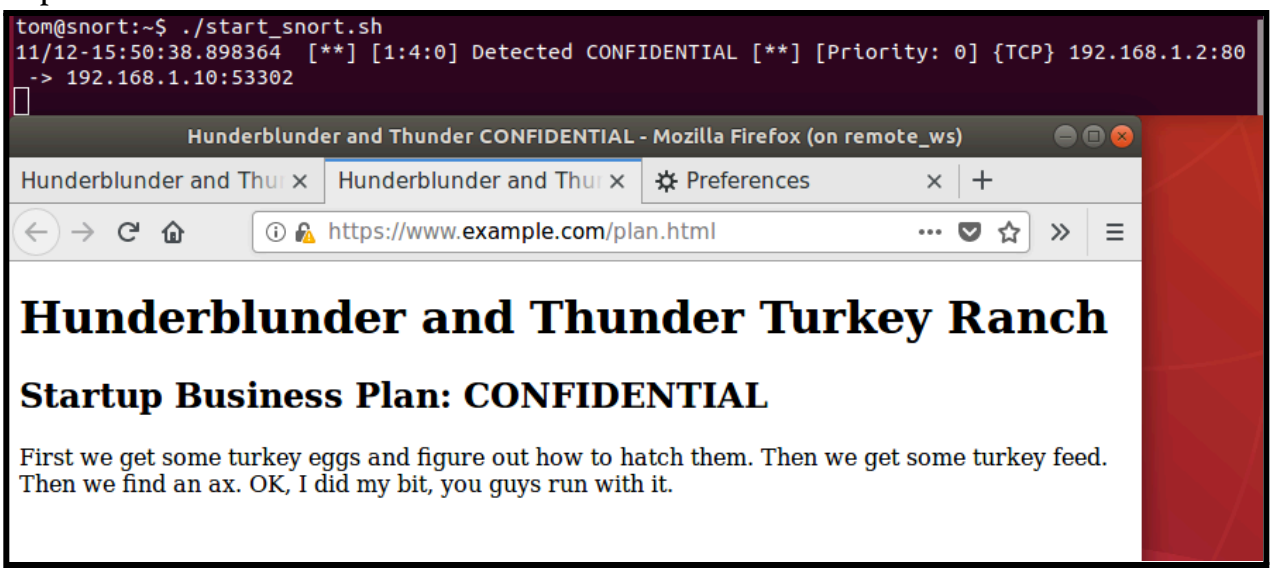
Watch this space!

As we cleared the browsing history and re-opened the page with confidential information the snort started showing alerts hence the rule was working properly.



5. Effects of encryption

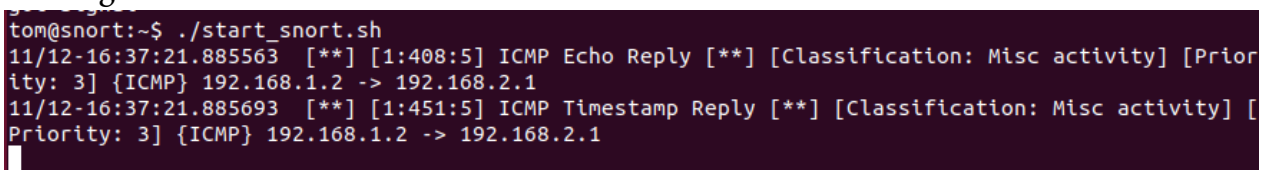
For this we will clear the history of the browser first. And instead of http we will brows with https and will see if snort can detect the alerts



We see that snort did not show any alert message as it is in the encrypted part.

6. Watching Internal traffic

If we use the nmap command on example.com : **nmap www.example.com** then the snort is showing all the alerts .



```
mary@ws2: ~                                   tom@snort: ~
mary@ws2:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2021-11-12 16:37 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000040s 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 1.59 seconds
mary@ws2:~$
```

Now we will change the routing and will see if snort can show us the alert or not

In the gateway we see the rule using the command: **cat /etc/rc.local**

```
ubuntu@gateway:~$ cat /etc/rc.local
#!/bin/bash
route delete default
route add default gw 203.0.113.1
#
# get ethernet device names for the two lans and the wan interfaces
#
lan1=$(ifconfig | grep -B1 "inet addr:192.168.1.10" | awk '$1!="inet" && $1!="--" {print $1}')
lan2=$(ifconfig | grep -B1 "inet addr:192.168.2.10" | awk '$1!="inet" && $1!="--" {print $1}')
wan=$(ifconfig | grep -B1 "inet addr:203.0.113.10" | awk '$1!="inet" && $1!="--" {print $1}')
#
# flush and delete all chains
#
iptables --flush
iptables -t nat --flush
iptables -t mangle --flush
iptables --delete-chain
iptables -t nat --delete-chain
iptables -t mangle --delete-chain
#
# mirror incoming wan traffic to snort
```

We open the file and can see a lot of rules

```
admin@web_server:~                            ubuntu@gateway: ~
 GNU nano 2.5.3                File: /etc/rc.local

#!/bin/bash
route delete default
route add default gw 203.0.113.1
#
# get ethernet device names for the two lans and the wan interfaces
#
lan1=$(ifconfig | grep -B1 "inet addr:192.168.1.10" | awk '$1!="inet" && $1!="--" {print $1}')
lan2=$(ifconfig | grep -B1 "inet addr:192.168.2.10" | awk '$1!="inet" && $1!="--" {print $1}')
wan=$(ifconfig | grep -B1 "inet addr:203.0.113.10" | awk '$1!="inet" && $1!="--" {print $1}')
#
# flush and delete all chains
#
iptables --flush
iptables -t nat --flush
iptables -t mangle --flush
iptables --delete-chain
iptables -t nat --delete-chain
iptables -t mangle --delete-chain
                                  [ Read 52 lines ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos
```

And we added the lan 2 command in the file.
Command used: **iptables -t mangle -A PREROUTING -i $lan2 -j TEE --gateway 192.168.3.1**

```
#
iptables -t mangle -A PREROUTING -i $wan -j TEE --gateway 192.168.3.1
iptables -t mangle -A PREROUTING -i $lan1 -j TEE --gateway 192.168.3.1
iptables -t mangle -A PREROUTING -i $lan2 -j TEE --gateway 192.168.3.1

#
# Define NAT for traffic from LANs to the WAN
#
iptables --table nat -I POSTROUTING 1 --out-interface $wan -j MASQUERADE
#iptables --append FORWARD --in-interface $lan1 -j ACCEPT
#iptables --append FORWARD --in-interface $lan2 -j ACCEPT

#sudo iptables -A FORWARD -i $wan -o $lan1 -p tcp --syn --dport 80 -m conntrack --ctstate NEW -j$
#sudo iptables -A FORWARD -i $wan -o $lan1 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
#sudo iptables -A FORWARD -i $lan1 -o $wan -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -t nat -A PREROUTING -i $wan -p tcp --dport 80 -j DNAT --to-destination 192.168.1.2
sudo iptables -t nat -A POSTROUTING -o $lan1 -p tcp --dport 80 -s 192.168.0.0/16 -j RETURN
sudo iptables -t nat -A POSTROUTING -o $lan1 -p tcp --dport 80 -d 192.168.1.2 -j SNAT --to-sourc$
```

And then we apply the rule using : **sudo /etc/rc.local**

```
ubuntu@gateway:~$ sudo /etc/rc.local
[ ok ] Restarting dnsmasq (via systemctl): dnsmasq.service.
SIOCDELRT: No such process
ubuntu@gateway:~$
```

Now when we use the nmap command the snort will show more detailed alert msg than before as it is seen as an external command.

```
mary@ws2:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2021-11-12 16:51 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.00088s 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
```

```
tom@snort:~$ ./start_snort.sh
11/12-16:51:20.132349  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information
Leak] [Priority: 2] {ICMP} 192.168.2.1 -> 192.168.1.2
11/12-16:51:20.132349  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3
] {ICMP} 192.168.2.1 -> 192.168.1.2
11/12-16:51:20.132378  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Prior
ity: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
11/12-16:51:20.132633  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.2.1 -> 192.168.1.2
11/12-16:51:20.132648  [**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc activity] [
Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
11/12-16:51:21.503125  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted I
nformation Leak] [Priority: 2] {TCP} 192.168.2.1:42410 -> 192.168.1.2:705
11/12-16:51:21.574068  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Informat
ion Leak] [Priority: 2] {TCP} 192.168.2.1:42410 -> 192.168.1.2:161
```

7. Distinguishing traffic by address

Now we will set snort to fire alert only on external network not on internal network.

So going into the snort rule we will just add the IP address of the gateway in the rule and will save the changes

```
mary@ws2: ~                                   tom@snort: ~
  GNU nano 2.5.3          File: /etc/snort/rules/local.rules                Modified

# $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 -> 192.168.1.10 any (msg:"Detected CONFIDENTIAL"; content:"CONFIDENTIAL"; sid:$
```

The rule is showing in the file

```
tom@snort:~$ cat /etc/snort/rules/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 -> 192.168.1.10 any (msg:"Detected CONFIDENTIAL"; content:"CONFIDENTIAL"; sid:0
00004;)
tom@snort:~$
```

Now we will start the snort and access the website with hank@remote WS

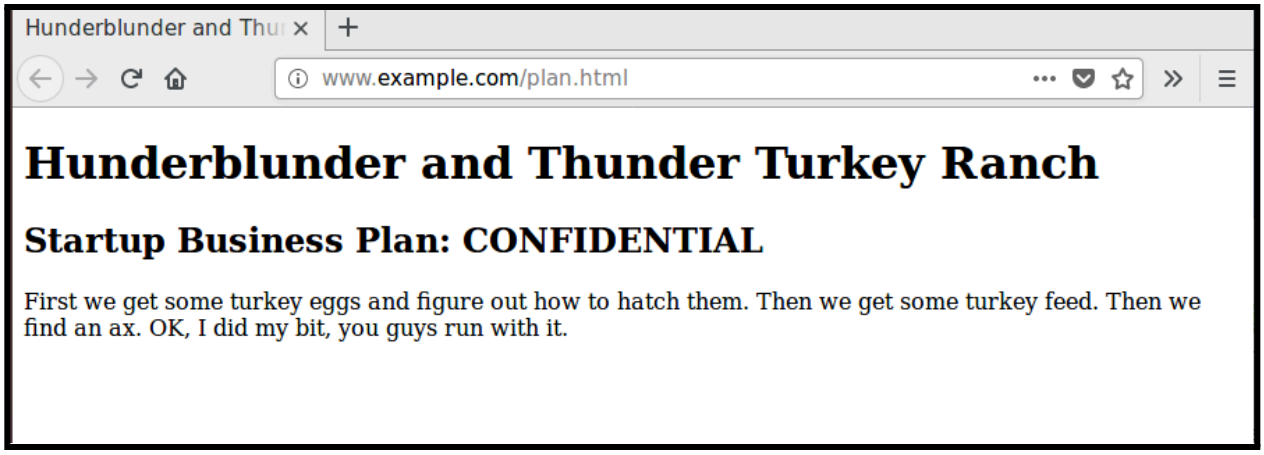
```
hank@remote_ws:~$ firefox www.example.com
```

We see an alert.

```
tom@snort:~$ ./start_snort.sh
11/12-17:11:52.329296  [**] [1:4:0] Detected CONFIDENTIAL [**] [Priority: 0] {TCP} 192.168.1.2:80
 -> 192.168.1.10:53354
```

Now if we use some different WS which are local.

```
Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
mary@ws2:~$ firefox www.example.com/plan.html
```




```
tom@snort:~$ ./start_snort.sh
11/12-17:15:09.925758  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:10.768889  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:11.141198  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:12.243770  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:14.931669  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:15.782460  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:16.143136  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:17.247395  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:19.939511  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:20.795695  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:21.153869  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:22.251809  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:24.943051  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:25.801460  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:26.159485  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:27.257058  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:29.945257  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:30.808857  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:31.162886  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:32.283415  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:34.948028  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
ication: Misc activity] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
11/12-17:15:35.813679  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classif
```

And we see that it's not generating the alert as it was doing for the external remote server accessing the confidential file.