CSI4139 LAB 5 Report

Name: Iyanu Aketepe

Student No: 300170701

Nmap Task:

Relevant command:

-Pn - Allows me to scan a given host
-p - Allows me to check whether a port for a host is open or closed
-ssh - allows me to remote access a given host
-ls (l) - lets me check the files/directories for a user
-cat - outputs the contents of a file

```
Starting Nmap 7.01 ( https://nmap.org ) at 2024-10-10 20:28 UTC
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.70 seconds
ubuntu@mycomputer:~$ nmap -Pn friedshrimp

Starting Nmap 7.01 ( https://nmap.org ) at 2024-10-10 20:28 UTC
Nmap scan report for friedshrimp (172.25.0.5)
Host is up (0.00038s latency).
rDNS record for 172.25.0.5: nmap-discovery.friedshrimp.student.i
ntranet
All 1000 scanned ports on friedshrimp (172.25.0.5) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

I scanned friedshrimp to get more information on it. I was able to find its ip address as a result, along with knowing that the first 1000 ports are closed.

```
ubuntu@mycomputer:~$ nmap -p 2000-3000 friedshrimp

Starting Nmap 7.01 ( https://nmap.org ) at 2024-10-10 20:42 UTC
Nmap scan report for friedshrimp (172.25.0.5)
Host is up (0.00060s latency).
rDNS record for 172.25.0.5: nmap-discovery.friedshrimp.student.i
ntranet
Not shown: 1000 closed ports
PORT     STATE SERVICE
2660/tcp open  unknown
```

I checked friedshrimps ports, specifically those in the 2000-3000 range, to see which ones were open. Thankfully, there was an open port called 2660.

```
ubuntu@mycomputer:~$ ssh ubuntu@friedshrimp
ssh: connect to host friedshrimp port 22: Connection refused
ubuntu@mycomputer:~$ ssh -p 2660 172.25.0.5
The authenticity of host '[172.25.0.5]:2660 ([172.25.0.5]:2660)'
 can't be established.
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU
2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? S
```

Afterward, I try to remote access the friedshrimp host using the 2660 port.

```
ubuntu@mycomputer:~$ ssh -p 2660 172.25.0.5
ubuntu@172.25.0.5's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 6.8.0-35-generic x86_64
)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in t
he
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitte
```

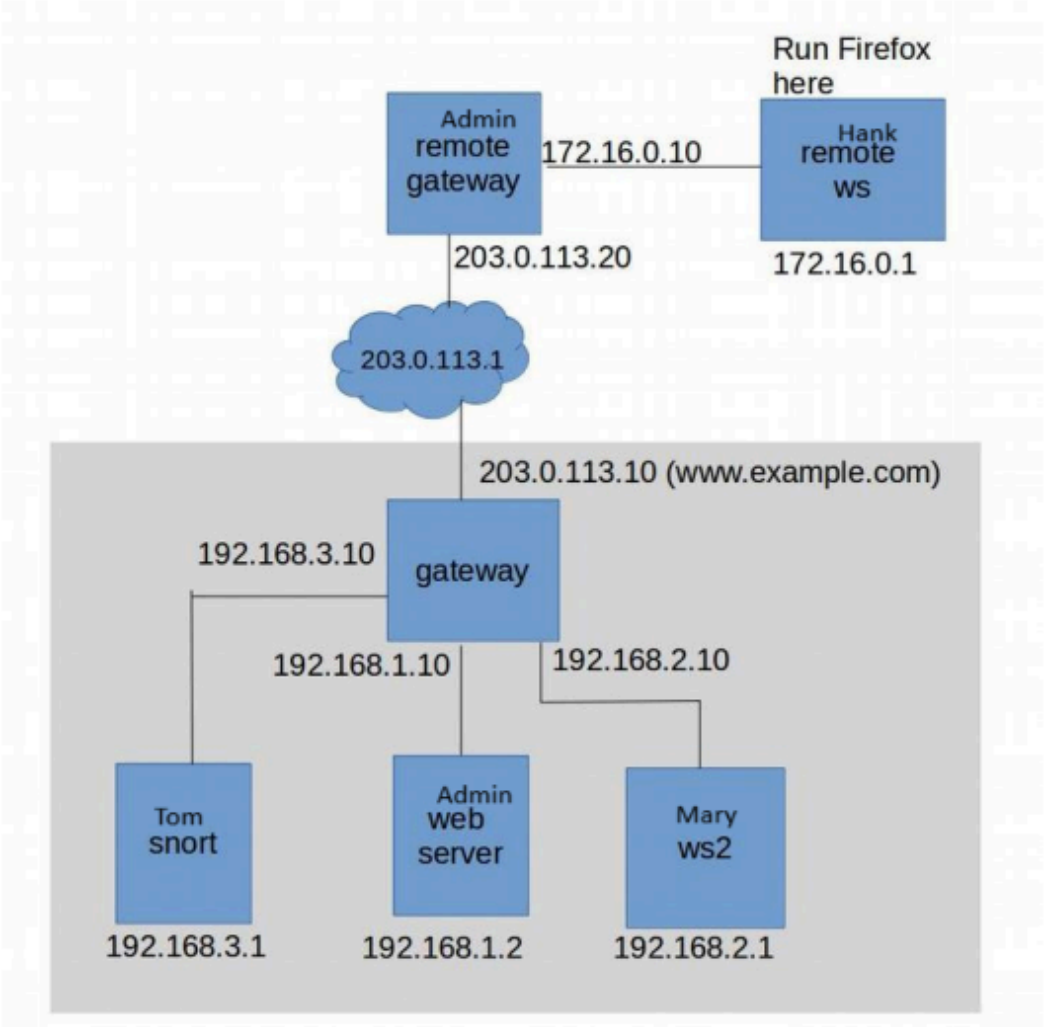
I type in my credentials and log in.

```
ubuntu@friedshrimp:~$ l
friedshrimp.txt
ubuntu@friedshrimp:~$ cat friedshrimp.txt
My summary notes from the fried shrimp project:

Fried Shrimp Project: We concluded it is better to
buy than to build.

==================================================

Congratulations! You managed to find the summary file
for “fired shrimp”and impress Randall.
ubuntu@friedshrimp:~$
```

I check the files and directories of ubuntu@friedshrimp and the output the contents of the friedshrimp file.

Snort Task:

4



4.1
Mapped names to the network topology

```
mary@ws2: ~                                    tom@snort: ~
          RX bytes:8816 (8.8 KB)  TX bytes:126 (126.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

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

Started the snort program

4.2

```
hank@remote_ws:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2024-10-10 21:13 UTC
Nmap scan report for www.example.com (203.0.113.10)
Host is up (0.000050s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 3.12 seconds
```

Used nmap to scan www.example.com, brought up four open ports.

```
10/10-21:13:34.505636  [**] [1:469:3] ICMP PING NMAP [**] [Class
ification: Attempted Information Leak] [Priority: 2] {ICMP} 203.
0.113.20 -> 203.0.113.10
10/10-21:13:34.505636  [**] [1:384:5] ICMP PING [**] [Classifica
tion: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.
113.10
10/10-21:13:34.514197  [**] [1:453:5] ICMP Timestamp Request [**
] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113
.20 -> 203.0.113.10
10/10-21:13:35.871616  [**] [1:1421:11] SNMP AgentX/tcp request
[**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 203.0.113.20:43020 -> 203.0.113.10:705
10/10-21:13:37.395740  [**] [1:1418:11] SNMP request tcp [**] [C
lassification: Attempted Information Leak] [Priority: 2] {TCP} 2
```

I checked snort, it has notified me of an nmap scan.

```
cd /etc/snort/rules
tom@snort:/etc/snort/rules$ l
attack-responses.rules          icmp-info.rules
backdoor.rules                  icmp.rules
bad-traffic.rules               imap.rules
chat.rules                      info.rules
community-bot.rules             local.rules
community-deleted.rules         misc.rules
community-dos.rules             multimedia.rules
community-exploit.rules         mysql.rules
community-ftp.rules             netbios.rules
community-web-dos.rules         tftp.rules
community-web-iis.rules         virus.rules
community-web-misc.rules        web-attacks.rules
community-web-php.rules         web-cgi.rules
ddos.rules                      web-client.rules
deleted.rules                   web-coldfusion.rules
dns.rules                       web-frontpage.rules
dos.rules                       web-iis.rules
experimental.rules              web-misc.rules
exploit.rules                   web-php.rules
finger.rules                    x11.rules
ftp.rules
tom@snort:/etc/snort/rules$
```

I changed the directory on the user tom so I could observe the rules, I then checked the list of rules.

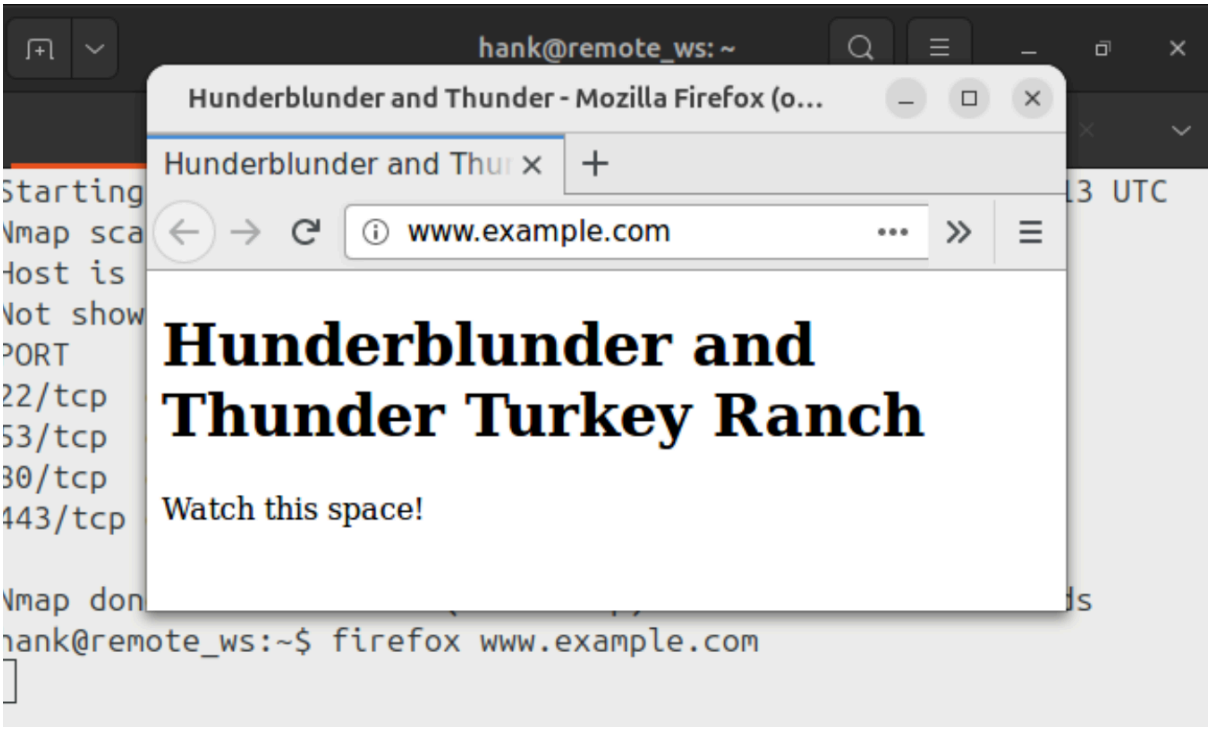
4.3

```
tom@snort:/etc/snort/rules$ nano local.rules
```

```
  GNU nano 2.5.3        File: 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 y$
# additions here.
alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)
```

I used nano to edit local.rules, adding in a custom rule to alert for each packet in a TCP stream

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



Hank is searching up the example website on firefox.

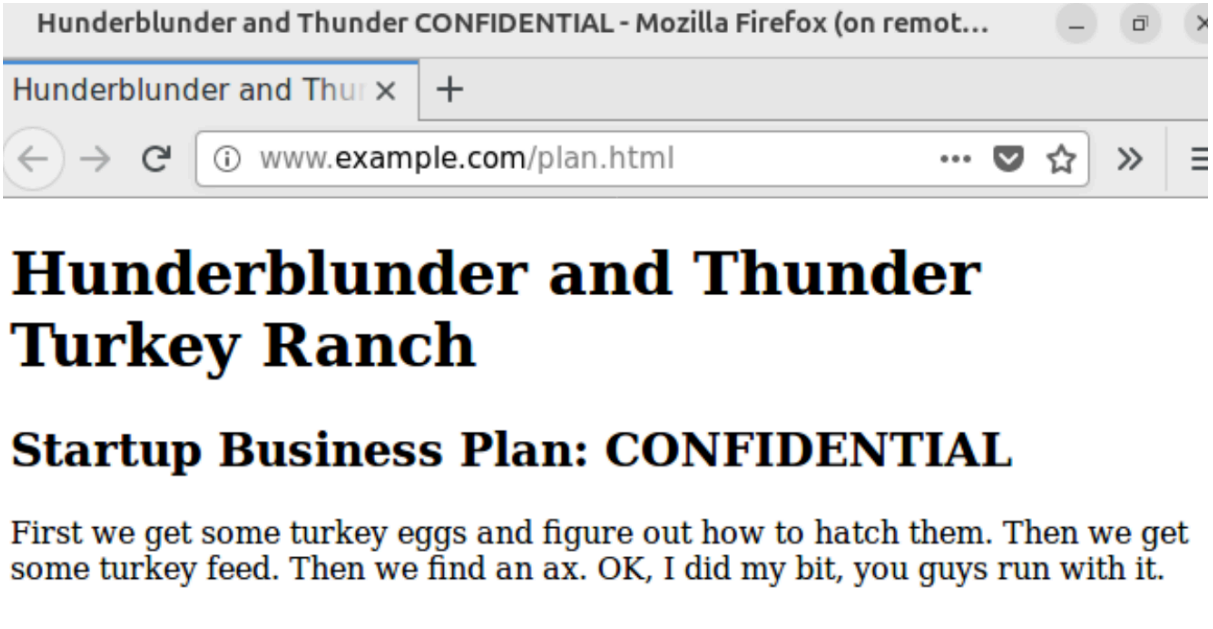
```
10/10-21:31:28.921628  [**] [1:2:0] TCP detected [**] [Priority:
 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:47038
10/10-21:31:28.925207  [**] [1:2:0] TCP detected [**] [Priority:
 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:47038
10/10-21:31:28.927185  [**] [1:2:0] TCP detected [**] [Priority:
 0] {TCP} 203.0.113.20:47038 -> 203.0.113.10:80
10/10-21:31:33.928431  [**] [1:2:0] TCP detected [**] [Priority:
 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:47038
10/10-21:31:33.929416  [**] [1:2:0] TCP detected [**] [Priority:
 0] {TCP} 203.0.113.20:47038 -> 203.0.113.10:80
10/10-21:31:33.929584  [**] [1:2:0] TCP detected [**] [Priority:
 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:47038
```

These are all the notifications that I'm getting because of the rule.

```
  GNU nano 2.5.3        File: 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 y$
# additions here.



^G Get Help ^O Write Out^W Where Is ^K Cut Text ^J Justify
^X Exit     ^R Read File^\ Replace  ^U Uncut Tex^T To Spell
```

Now, I have deleted the rule.

4.4



Hank is viewing the confidential plan.

```
tom@snort:/etc/snort/rules$ cat 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 yo
ur local
# additions here.

alert tcp any any -> any any (msg:"CONFIDENTIAL information dete
cted"; content:"CONFIDENTIAL"; sid:1000001; rev:1;)
tom@snort:/etc/snort/rules$
```

```
tom@snort:~$ ./start_snort.sh
10/10-21:48:11.699328  [**] [1:1000001:1] CONFIDENTIAL informati
on detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1
.10:51434
```

Snort alert that occurred after Hank refreshed and accessed plan.html

4.5

```
tom@snort:~$ ./start_snort.sh
10/10-21:48:11.699328  [**] [1:1000001:1] CONFIDENTIAL informati
on detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1
.10:51434
```

I don't see a new snort alert.
The reason why Snort did not alert me is because it relies on checking through the content of an unencrypted packet. However, when we access the site with the SSL function, we encrypt our access, so snort can't tell what we're doing.

4.6

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

Starting Nmap 7.01 ( https://nmap.org ) at 2024-10-10 21:59 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.00012s 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 3.07 seconds
```

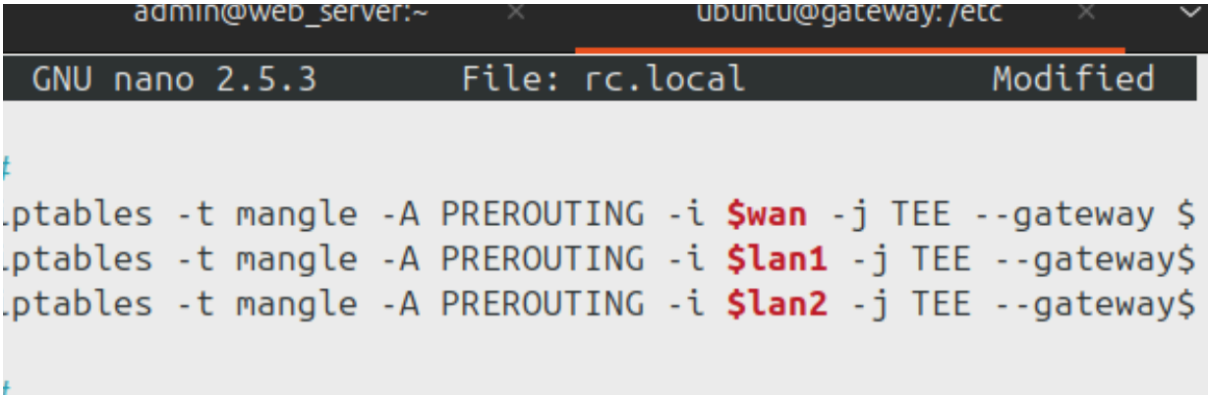
I ran an nmap scan on www.example.com

```
10/10-22:01:07.960418  [**] [1:408:5] ICMP Echo Reply [**] [Clas
sification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 1
92.168.2.1
10/10-22:01:07.961048  [**] [1:451:5] ICMP Timestamp Reply [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2
 -> 192.168.2.1
```

It seems like snort catches the nmap scan, though it doesn't add in the ICMP PING NMAP. It only says that there was an echo reply.

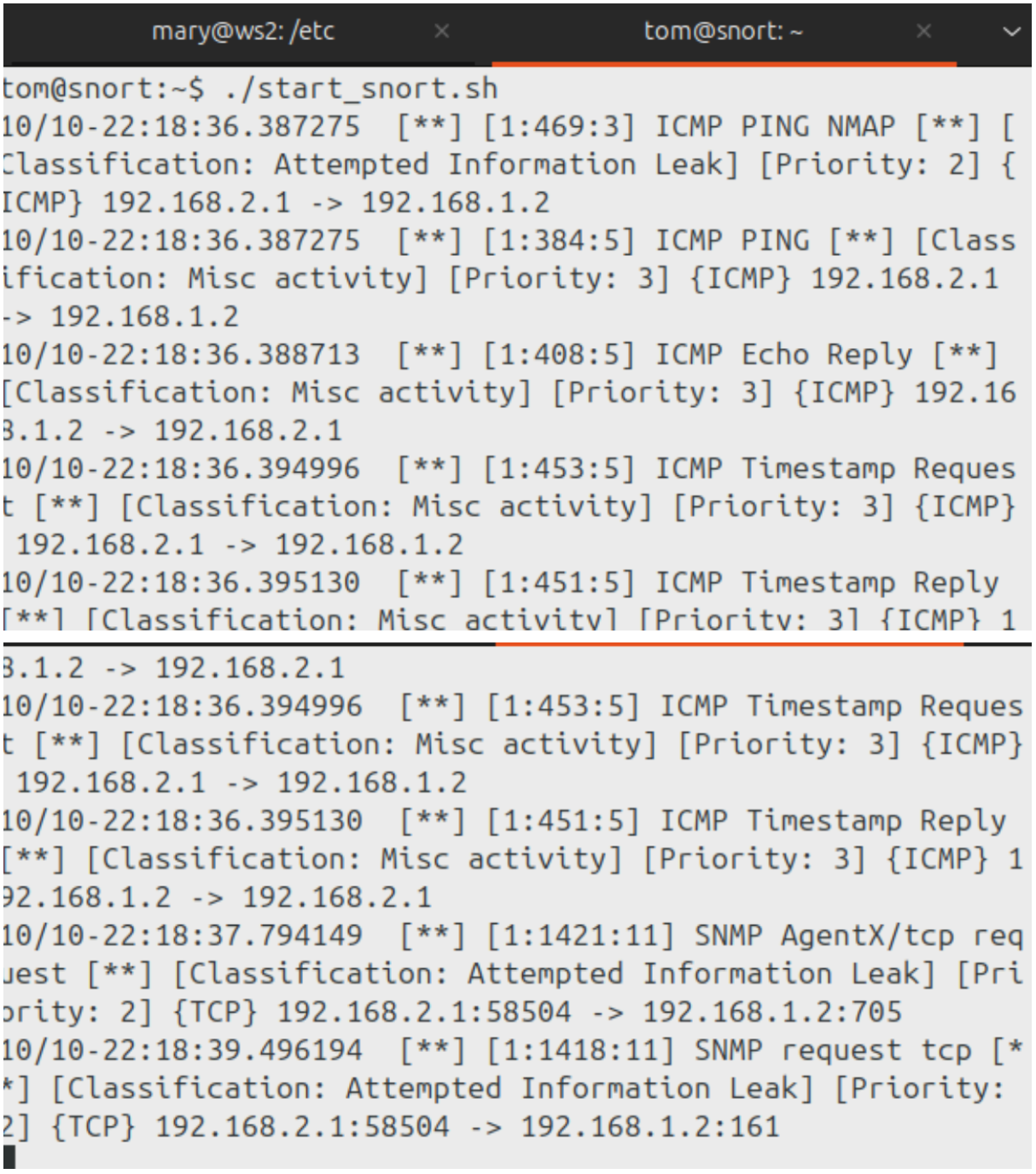
I'm not sure why there was a difference in messages. However, it may have something to do with how mary is a user on the ws2 host.

I edited the gateway rc.local file with nano

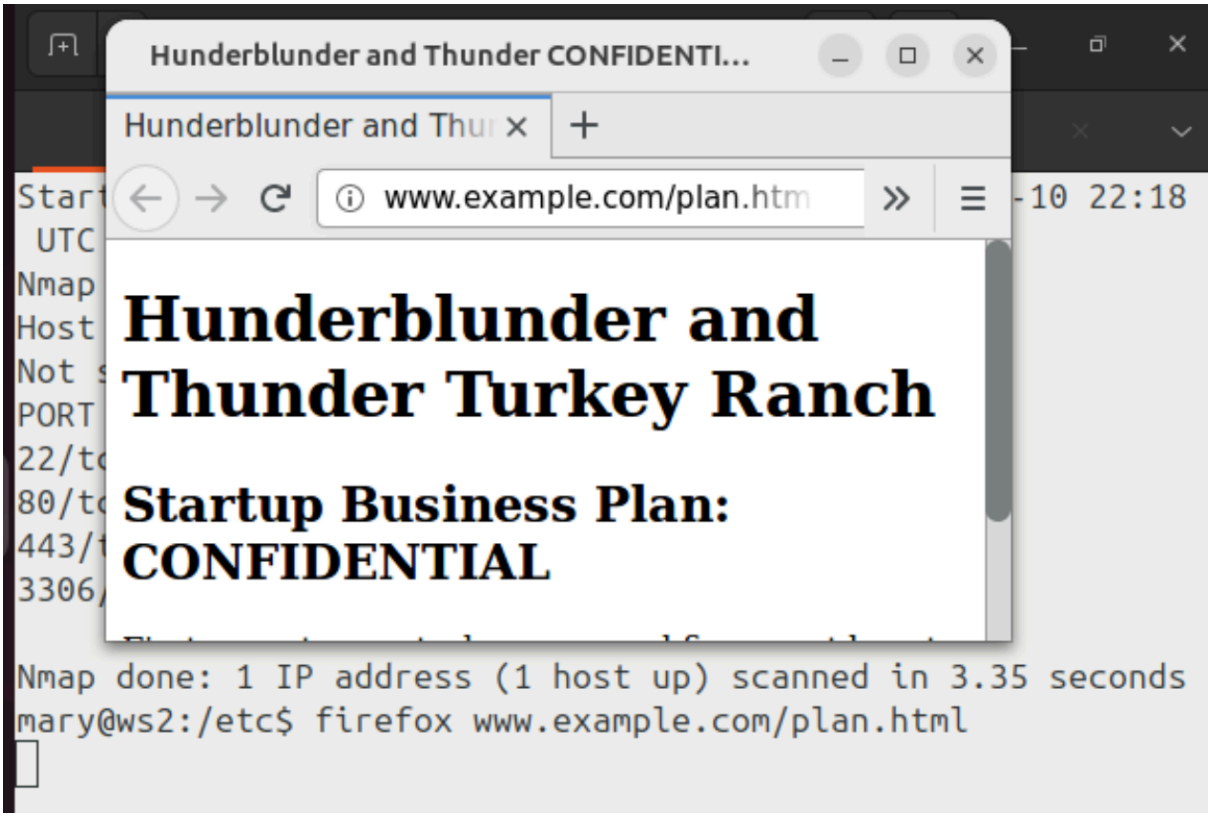


Added in the packet mirroring line from the lab document.

I restarted snort and ran nmap and here is the result tom sees:


mary@ws2: /etc
tom@snort: ~
tom@snort:~$ ./start_snort.sh
10/10-22:18:36.387275 [**] [1:469:3] ICMP PING NMAP [**] [
Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.2.1 -> 192.168.1.2
10/10-22:18:36.387275 [**] [1:384:5] ICMP PING [**] [Class
ification: Misc activity] [Priority: 3] {ICMP} 192.168.2.1
-> 192.168.1.2
10/10-22:18:36.388713 [**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 192.16
8.1.2 -> 192.168.2.1
10/10-22:18:36.394996 [**] [1:453:5] ICMP Timestamp Reques
t [**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.2.1 -> 192.168.1.2
10/10-22:18:36.395130 [**] [1:451:5] ICMP Timestamp Reply
8.1.2 -> 192.168.2.1
10/10-22:18:36.394996 [**] [1:453:5] ICMP Timestamp Reques
t [**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.2.1 -> 192.168.1.2
10/10-22:18:36.395130 [**] [1:451:5] ICMP Timestamp Reply
[**] [Classification: Misc activity] [Priority: 3] {ICMP} 1
92.168.1.2 -> 192.168.2.1
10/10-22:18:37.794149 [**] [1:1421:11] SNMP AgentX/tcp req
uest [**] [Classification: Attempted Information Leak] [Pri
ority: 2] {TCP} 192.168.2.1:58504 -> 192.168.1.2:705
10/10-22:18:39.496194 [**] [1:1418:11] SNMP request tcp [*
*] [Classification: Attempted Information Leak] [Priority:
2] {TCP} 192.168.2.1:58504 -> 192.168.1.2:161

4.7

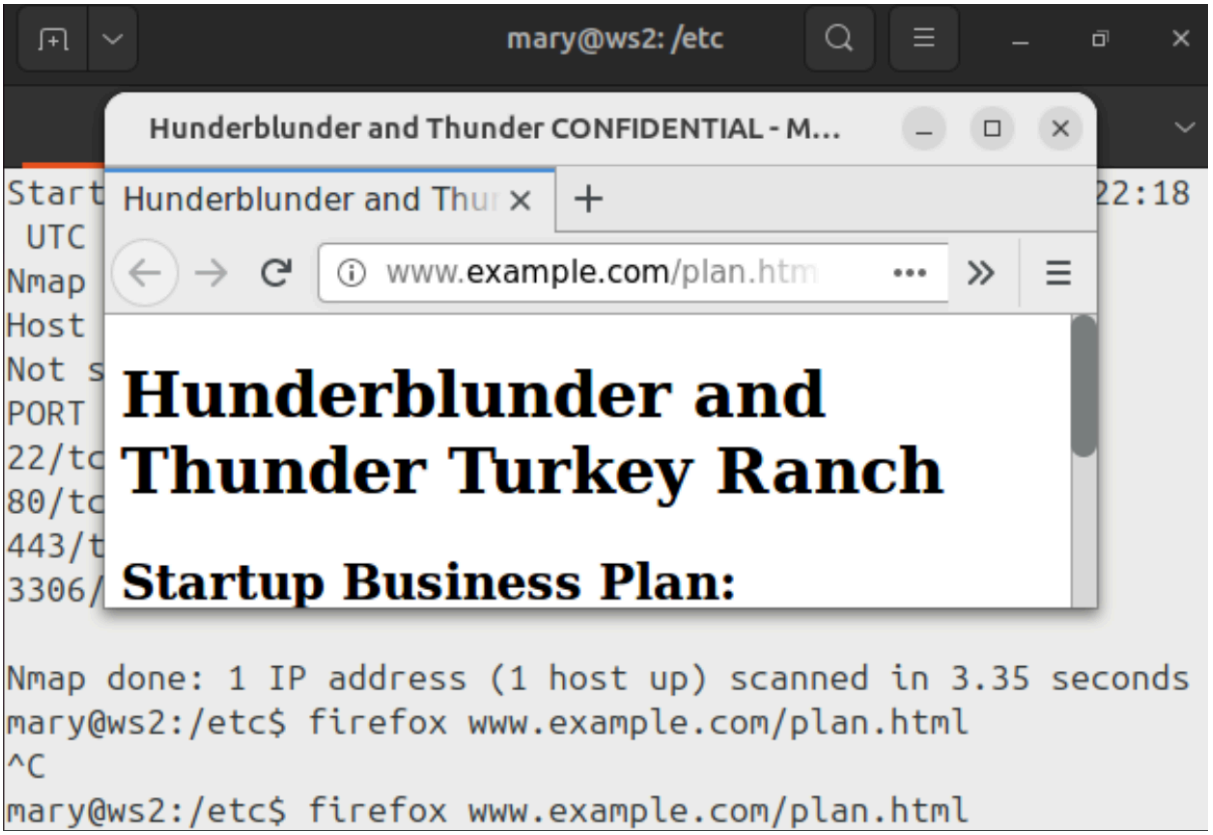


Mary is observing the plan

Updating snort rules

```
alert tcp any any -> !192.168.1.10/24 any (msg:"CONFIDENTIA
L information detected"; content:"CONFIDENTIAL"; sid:100000
1; rev:1;)
tom@snort:/etc/snort/rules$
```

Hank's access has been registered see below…



Mary accessed the plans and was not detected see below…

```
10/10-22:47:07.575393  [**] [1:402:7] ICMP Destination Unre
achable Port Unreachable [**] [Classification: Misc activit
y] [Priority: 3] {ICMP} 203.0.113.1 -> 203.0.113.10
10/10-22:47:25.061932  [**] [1:469:3] ICMP PING NMAP [**] [
Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.2.1 -> 192.168.1.2
10/10-22:47:25.061932  [**] [1:384:5] ICMP PING [**] [Class
ification: Misc activity] [Priority: 3] {ICMP} 192.168.2.1
-> 192.168.1.2
10/10-22:47:25.062046  [**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 192.16
8.1.2 -> 192.168.2.1
10/10-22:47:25.062378  [**] [1:453:5] ICMP Timestamp Reques
t [**] [Classification: Misc activity] [Priority: 3] {ICMP}
 192.168.2.1 -> 192.168.1.2
```

Mary used nmap and was detected. (See Above)

Hank used nmap and was detected.

```
10/10-22:49:54.000679  [**] [1:469:3] ICMP PING NMAP [**] [
Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 203.0.113.20 -> 203.0.113.10
10/10-22:49:54.000679  [**] [1:384:5] ICMP PING [**] [Class
ification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20
 -> 203.0.113.10
10/10-22:49:54.002372  [**] [1:453:5] ICMP Timestamp Reques
t [**] [Classification: Misc activity] [Priority: 3] {ICMP}
 203.0.113.20 -> 203.0.113.10
10/10-22:49:55.366261  [**] [1:1418:11] SNMP request tcp [*
*] [Classification: Attempted Information Leak] [Priority:
2] {TCP} 203.0.113.20:45740 -> 203.0.113.10:161
10/10-22:49:55.406895  [**] [1:1421:11] SNMP AgentX/tcp req
uest [**] [Classification: Attempted Information Leak] [Pri
ority: 2] {TCP} 203.0.113.20:45740 -> 203.0.113.10:705
```