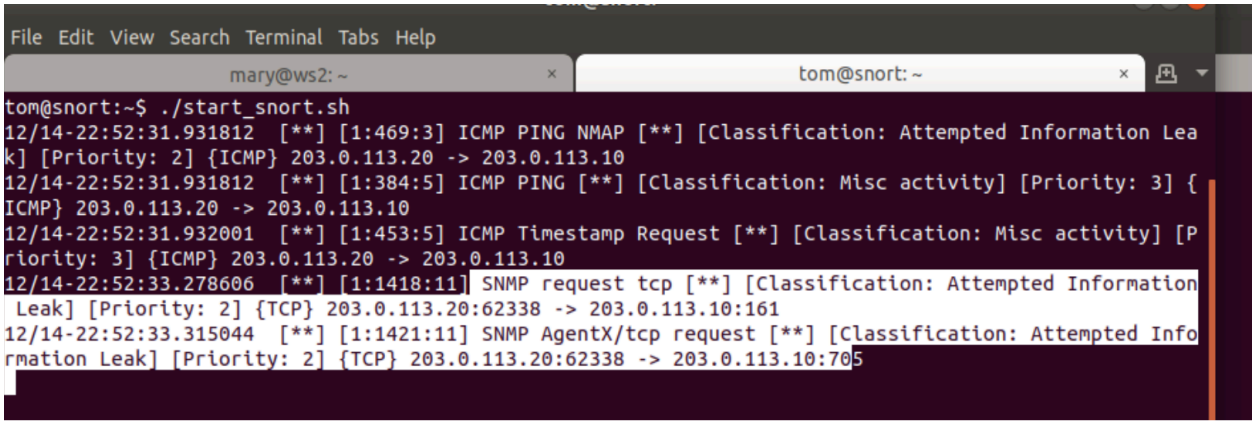
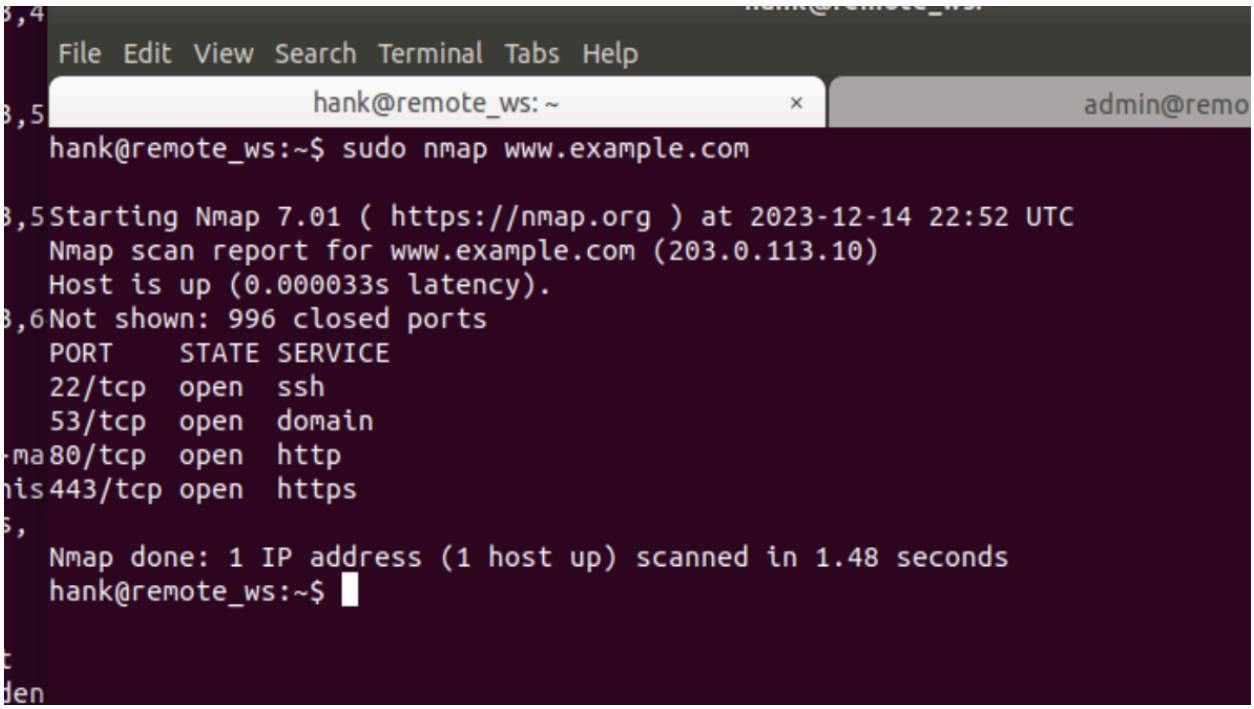
From Syed Farabi to syed, Wend , Chrisin
Lab 4- IDS
November 26, 2023
Csci 400

SNORT

Task 4.2: Pre - configured Snort rules

Screenshot





By default snort comes with several rules and one of them is nmap scan which shown on the screenshot

Description of task and observation

First we, we start the lab with the command labtainer -r. This will open 6 terminal window. They are,

under admin@web_server: admin@web_server and ubuntu@gateway
Under mary@ws2: mary@ws2 and tom@snort:
Under hank@remote_ws : hank@remote_ws: and admin@remote_gw:

Mary is workstation 2
Admin is gateway
Remote workstation is hank and remote gateway is admin

From the tom we started snort with this command

./start_snort.sh and press enter

Then in the hank we type this command ,

sudo nmap www.example.com

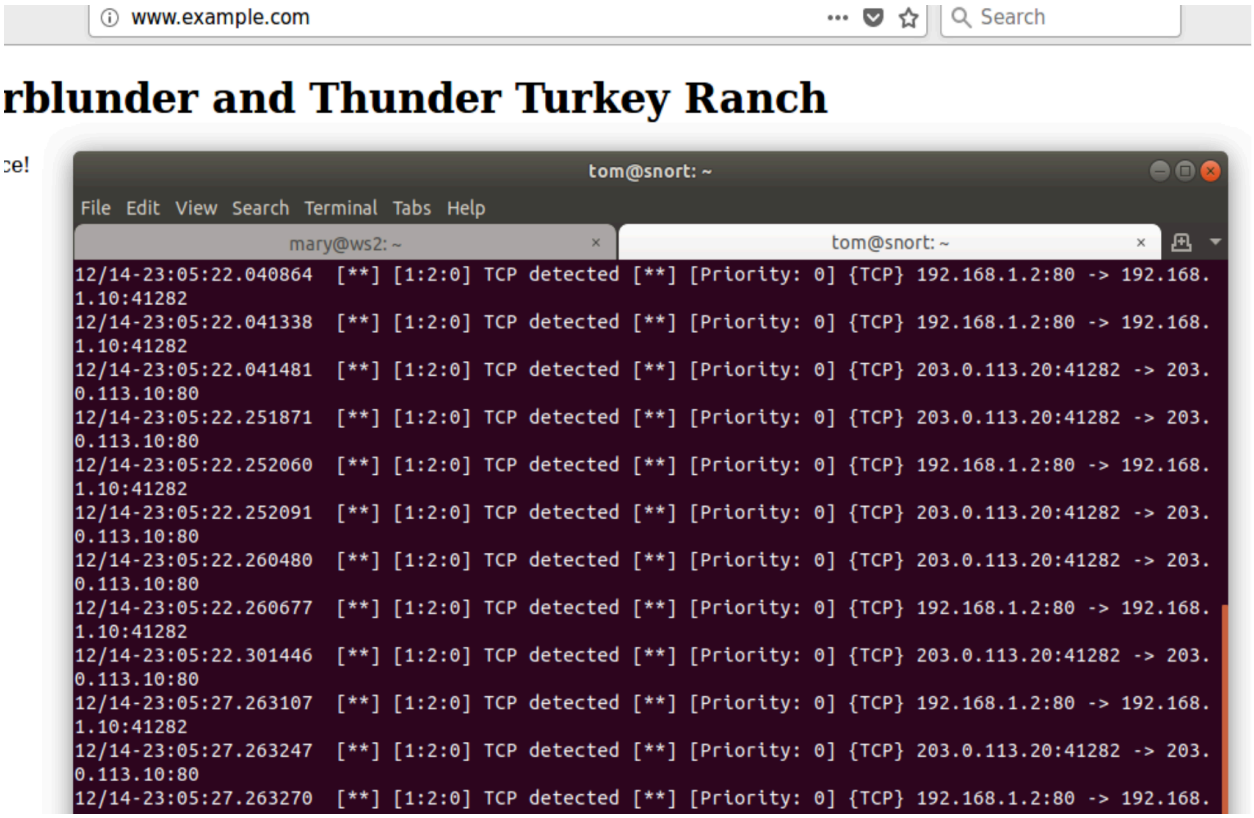
By default snort comes with several rules,and one of them is it will pick up, nmap scan

So , we can see snort respond to the nmap command and cupple of there pings

Clear hank
Clear tom, by copy pasting tom@snort:

Task 4.3: Pre - Write a simple (bad) rule

Screenshot



This screen shoot describes no matter if tcp is detected you will create an alert. Which is bad rule for a business because often business site has visitors from different time

Task and observation

Now, type sudo vi /etc/snort/rules/local.rules in tom

This will show us local rules in tom

Press i to write something there

Writing #task 4.3 as a comment
Then type this command ,

Alert tcp any any -> any any (msg:"tcp detected"; sid:00002;)

Alert for tcp
Any ip address on any port going to any ip address on any port, we will show a msg that says "TCP detected" and sid:00002. Here sid is rule id.

Type alt+shift+colon to skip, which will show : and type wq and press enter

Verify that file has been updated, using cat command

cat /etc/snort/rules/local.rules

This will show us the updated rules now,

Type clear

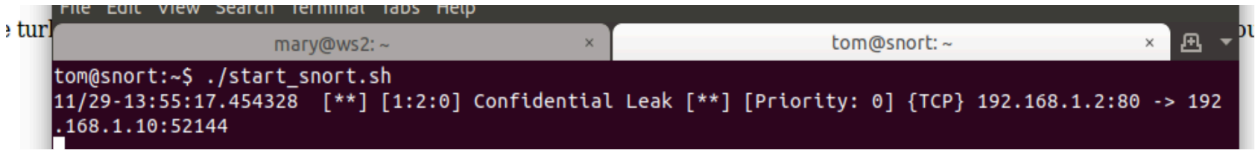
Then, type ./start_snort.sh to start the snort and press enter ,inside tom
Then , type firefox www.example.com in hank

Then will open up example.com in firefox

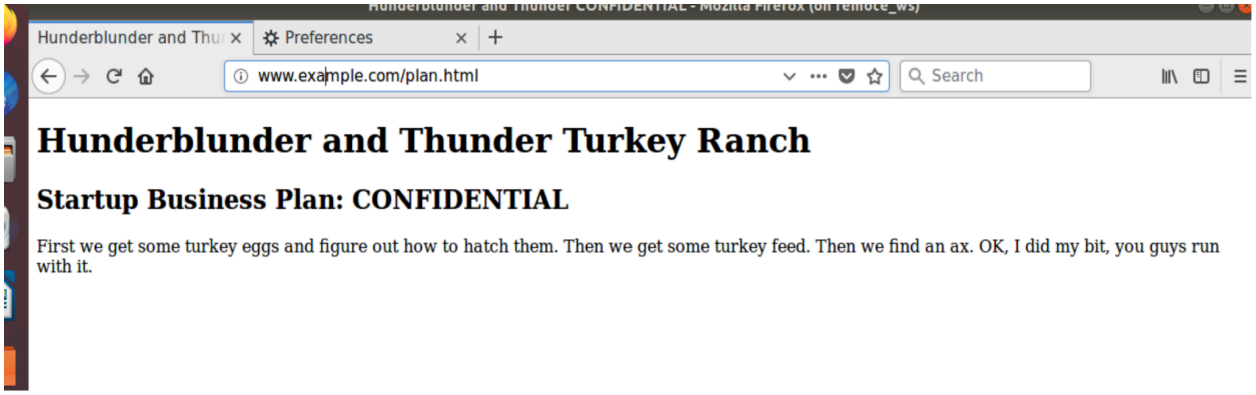
This will create a lot of tcp alert in tom because as a business site there should be multiple visitors and need to correct that rule.

Task 4.4: Custome rule for confidential traffic

Screenshot



Alert given confidential because the payload dta has confidential in it.



Task and observation
Rule: <Copy of rule added to local rules file>

**Alert tcp any any -> any any (msg:"Confidential leak;content: "CONFIDENTIAL";
sid:00003;**

Writing a rules for task 4.4

Run the the vi command in tom,

sudo vi /etc/snort/rules/local.rules

Then we press i and comment out for rules 4.3 and its command

Creating alert with this command,
**Alert tcp any any -> any any (msg:"Confidential leak;content: "CONFIDENTIAL";
sid:00003;**

Description of this command
This command will do is scan the payload of any packet going out and if it has the content confidentail then it will create an alert.

Press alt+shift+colon+wq

Just for double check,what i have wrote inside the rule,

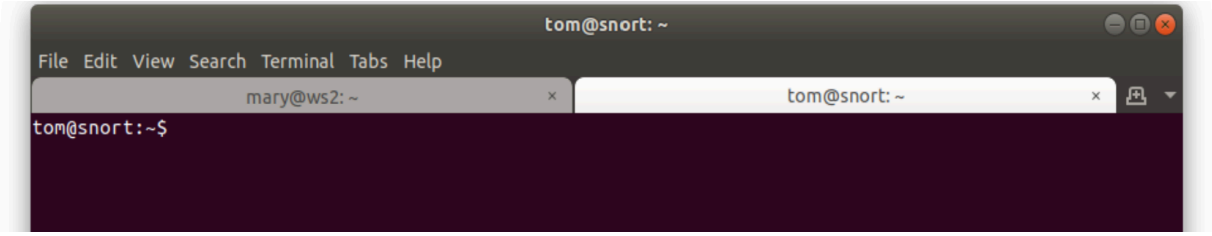
Cat /etc/snort/rules/local.rules inside the tom,

Hit clear to clear the screen.

Then start the script, inside the tom

./start_snort.sh and enter,

This does not show any alert

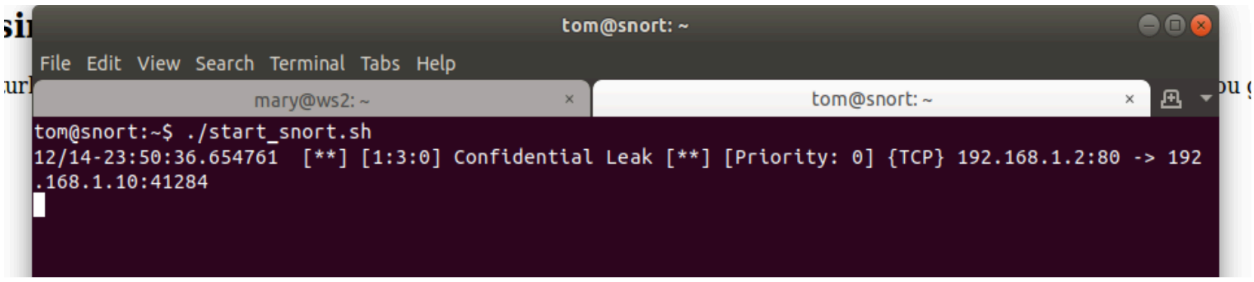


Then go to the firefox and clear all history with all the checkmarks.

Refresh the page of www.example.com

Now rewrite the address bar in firefox as, example.com/plan.html

Now tom will show a confidential leak alert



That is because payload data has confidential in it

Now again clear the history with all the checkmarks

Next edit the address bar as, https://www.example.com/plan.html, then load the page

This will show message that connection is not secure, but we proceed, by add exception and click the confirm security exception.

Now we dont see any alert because when using https we are using ssl or tls protocol and it is encrypted.

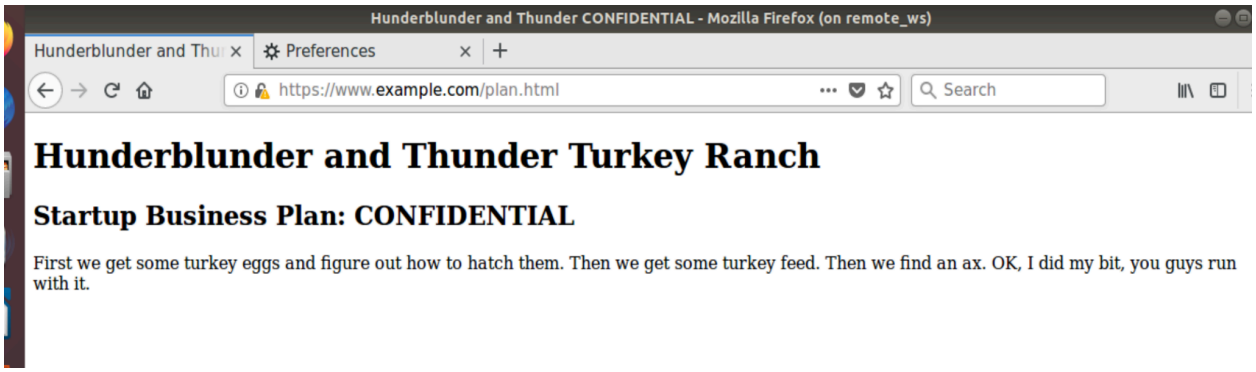
One of the solution is reverse proxy, which will handle encryption aspect and everything between proxy and actual web server wiil be in plaintext.

Again clearing the history

Close the firefox window.

Task 4.5:Effects of encription

Screenshot

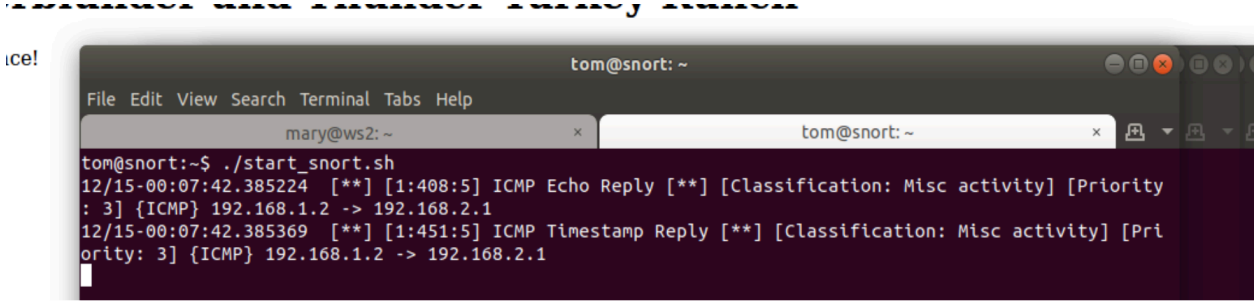


There is no alert because when we are using https then , we are using ssl or tls protocol then it should be encrypted and therefore we dont see the confidential plaintext as a payload.if we can see them then it means the encryption is failing and that is not happening there.

Task and observation

Task 4.6: Pre - Watching internal traffic

Screenshot



All the traffic that is going in from the internal network is also in routed to the snort. Workstation 2 is connected with gateway and gateway is connected to the snort.

Task and observation
Marry is inside the corporation or network, so she is working in ws2

Since she is not an it or security person she should not run a nmap scan

Lets imagine mary run this command below

sudo nmap www.example.com

This will create a snort alert containng ICMP echo reply which is a default rules but we dont see any nmap rule. But this snort allert did not create a nmap alert which will help us to detect insider threat.

So to fix that ,

We can go to the ubuntu@gateway and run this command

ll /etc/rc.local

This will show us a file is exist there

Then we run a another command

cat /etc/rc.local

This will result some pre configured information

Press clear to clean the screen

Then we run this command

sudo vi /etc/rc.local

This will help us to edit the table

We add this line into the table that contains #mirror incoming wan traffic to snort

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

Hit Alt+shift+colon+wq to save file

Then relaunch the file using this command

Sudo /etc/rc.local

Go to the tom and clear the screen

Then start a snort in tom using this comand

./start_snort.sh

Go to marys terminal, clear the screen and run this command

sudo nmap www.example.com

We can see an alert on tom

Press this command from mary

sudo nmap www.example.com

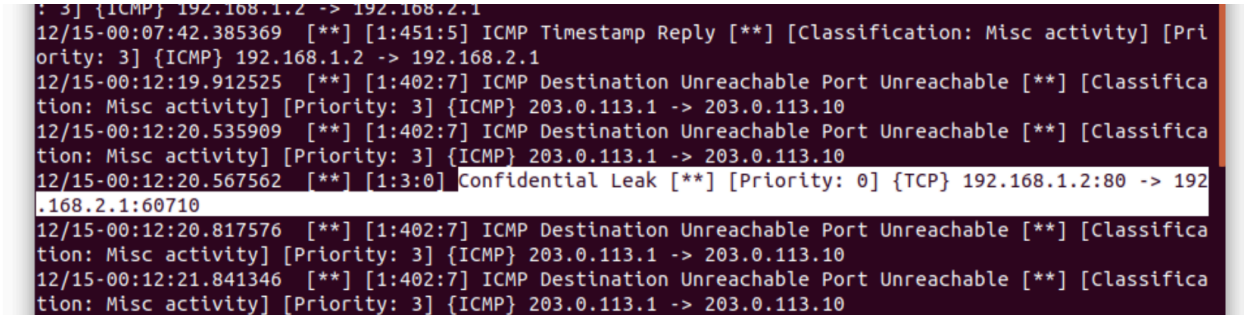
This will create an alert on tom

From the diagram , All the traffic that is going from internal network is also inrouted to snort , so if something that is internal network which is w2 that is connected to a gateway and gateway sends back to the snort.

But what if mary have allowed access in this scenario we check this command in marry,

firefox www.example.com/plan.html

Now if we check the snort alert then we can see a lot of alert which is icmp a predefined rules and other rules. But we can see a confidential leak



, which is not a good sign during the internal traffic that means if some employee have access of confidential stuff then it should not give a confidential alert.

Now we can clear the tom and run following command to read rules

sudo vi /etc/snort/rules/local.rules

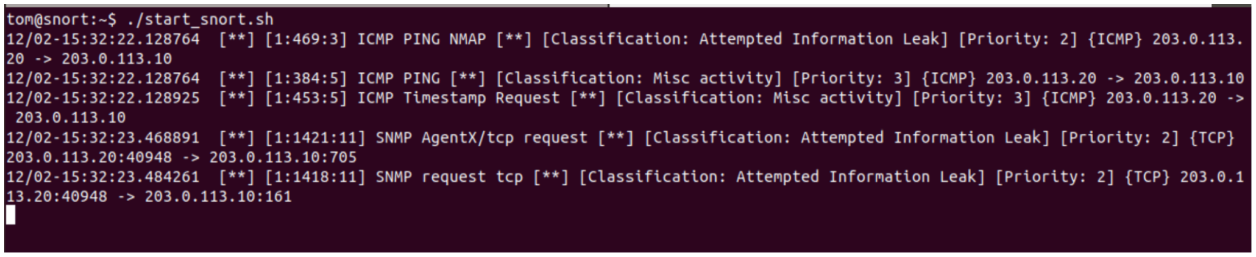
Comment out rules for 4.4

Then we write a new rules for task 4.7

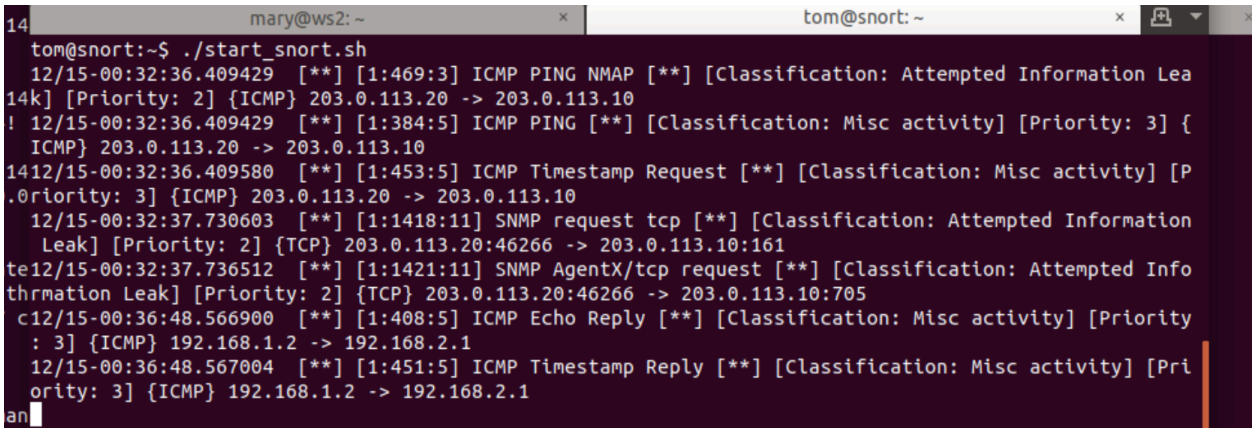
Task 4.7: Distinguishing traffic by address

Screenshot

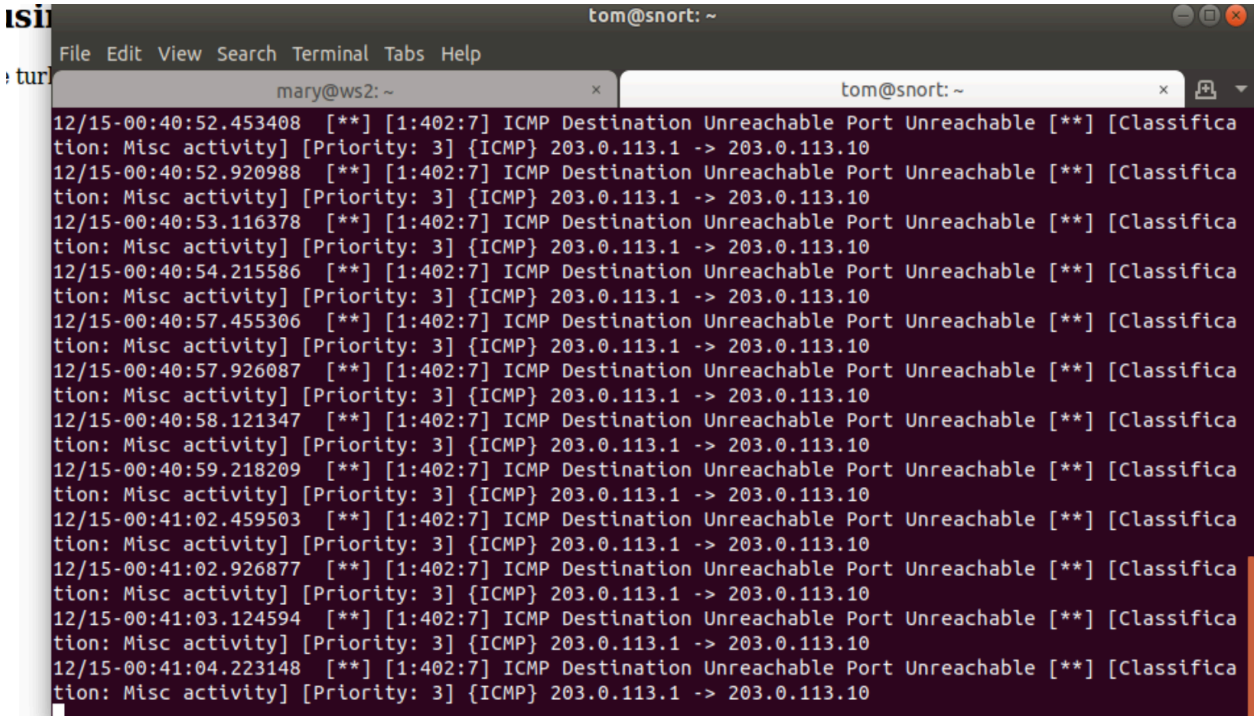
1) External access to the business plan generates an alert



2) internal access



3) external or internal



This will result a icmp alert but no confidential alert, when internal user accessing confidential file.

task and observation

alert tcp any any -> 192.168.1.10 any (msg:”Confidential leak”,content:”CONFIDENTIAL”; sid:00003;)

To save press alt+shift+:+wq

To verify use cat command

Cat /etc/snort/rules/local.rules

This will show us all the rules saved

Clear

Run a snort

./start_snort.sh

Go to hank which is remote terminal and run this command

Firefox www.example.com/plan.html then hit enter

We can see an alert on tom

clear the screen of hank and run that command

sudo nmap www.example.com

Then we can see an alert on tom

In the mary we run a nmap command

sudo nmap www.example.com

This will generate alert in tom containing second piece of icmp alert.

Now we run another command,

firefox www.example.com/plan.html

This will generate lot of alert containing icmp alert but surprisingly no confidential alert.

Close the firefox tabs

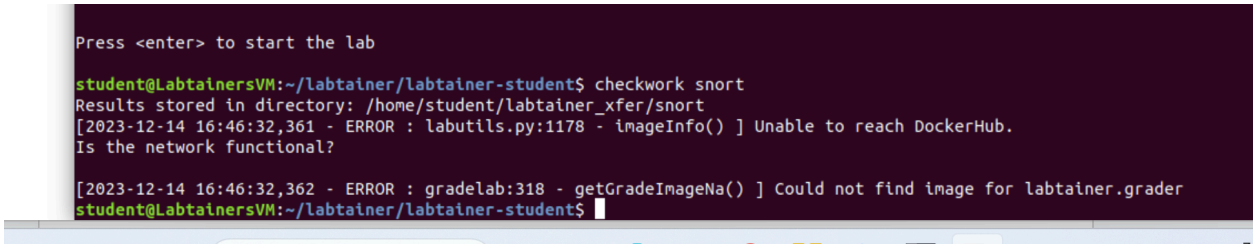
Control c to shut down and

Clear the screen

Check all the work on student by

Checkwork

Screen shot of saving attempt of checkwork


Press <enter> to start the lab
student@LabtainersVM:~/labtainer/labtainer-student$ checkwork snort
Results stored in directory: /home/student/labtainer_xfer/snort
[2023-12-14 16:46:32,361 - ERROR : labutils.py:1178 - imageInfo()] Unable to reach DockerHub.
Is the network functional?
[2023-12-14 16:46:32,362 - ERROR : gradelab:318 - getGradeImageNa()] Could not find image for labtainer.grader
student@LabtainersVM:~/labtainer/labtainer-student$