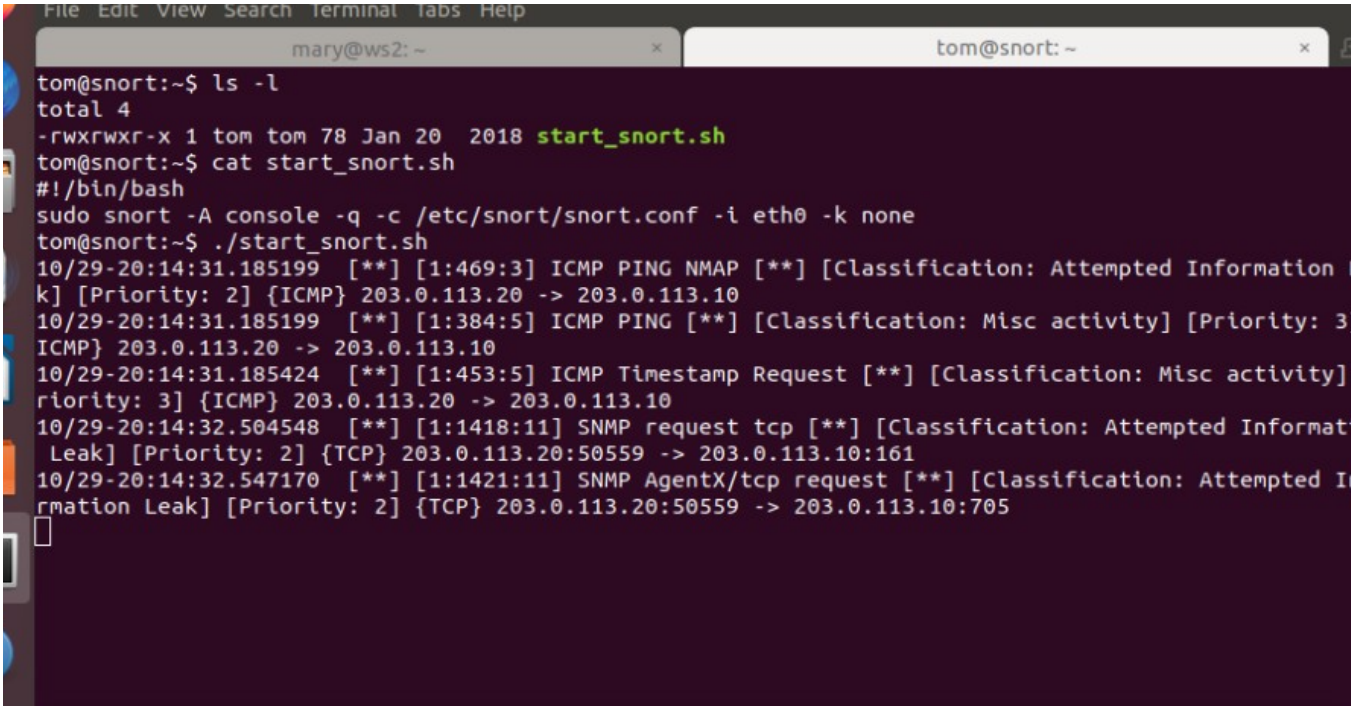
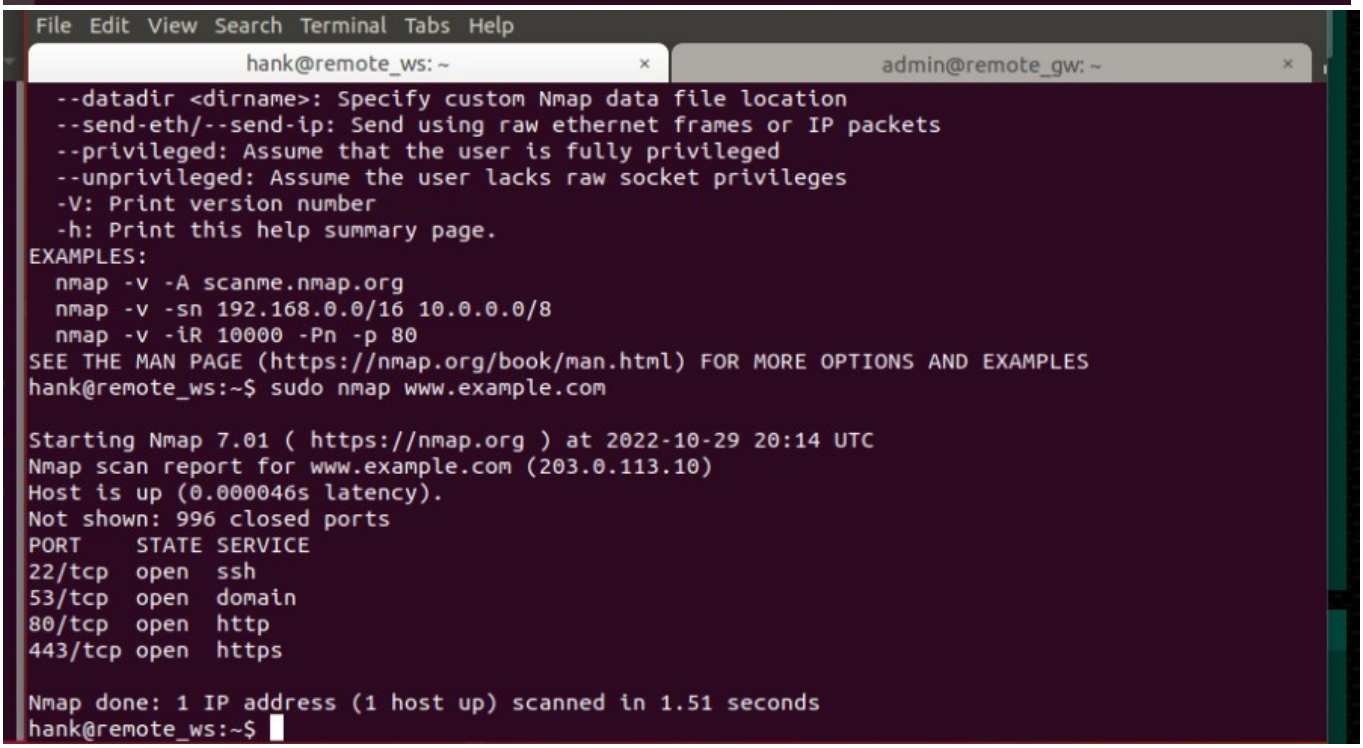
Homework 5 – Snort

Ryan Foster -CIS 480

Task 1. Start and stop Snort (sec 4.1 & 4.2)

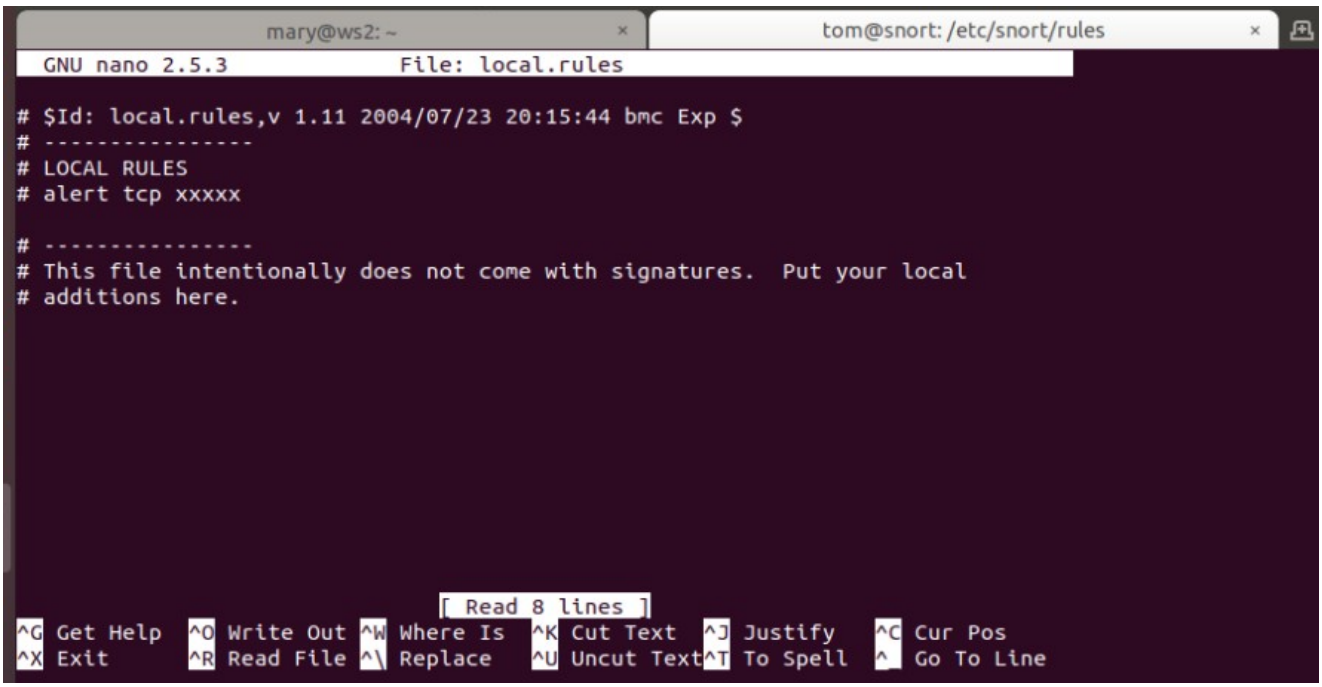
- Follow the instructions in sec 4.2 and perform an nmap scan of www.example.com from the remote workstation. Take a screenshot of the ouput *on the snort terminal*.



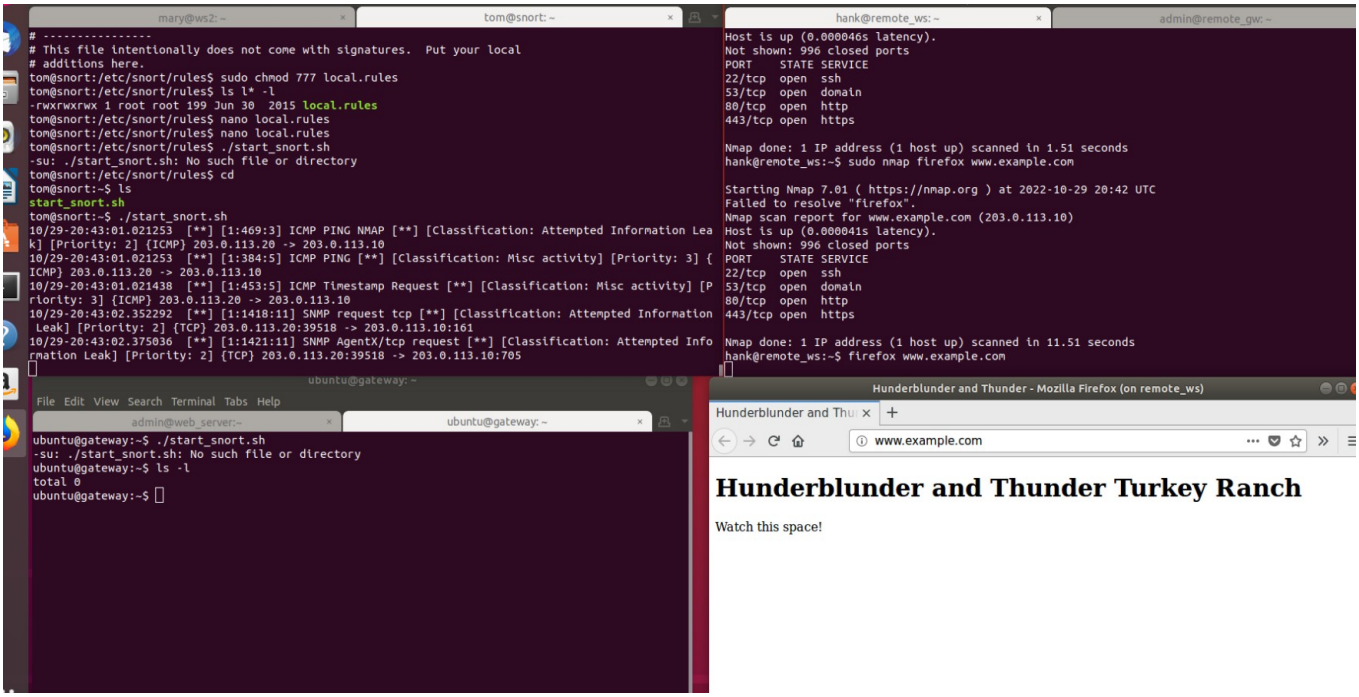


Task 2. Write a sample bad rule (sec 4.3)

- 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.
-

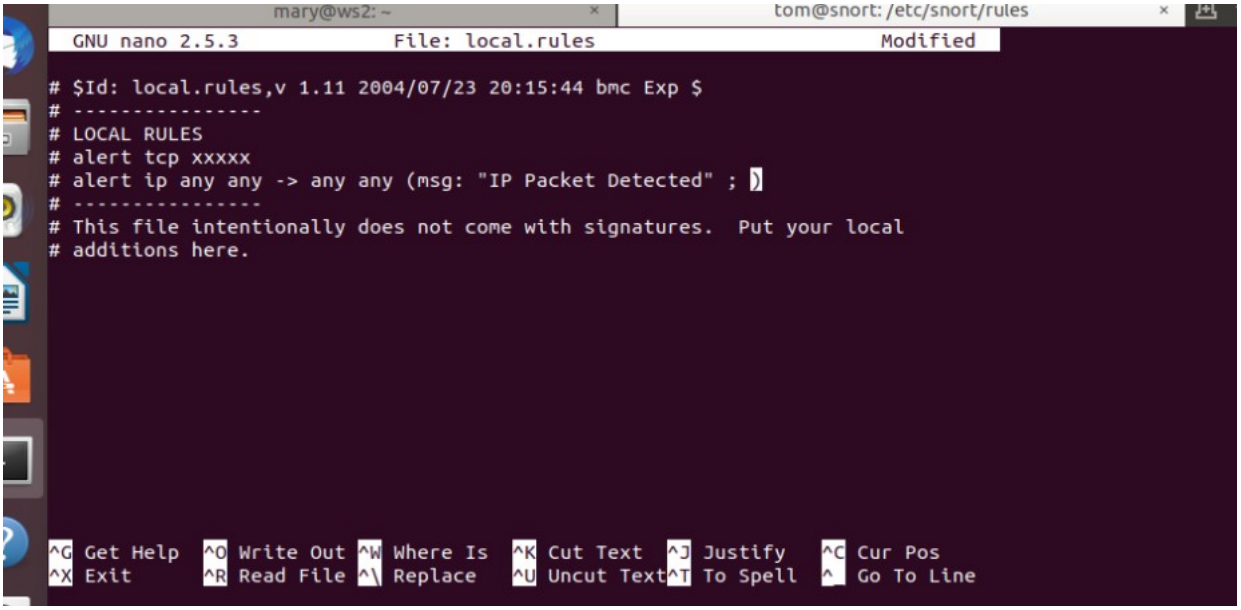


- Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.
-

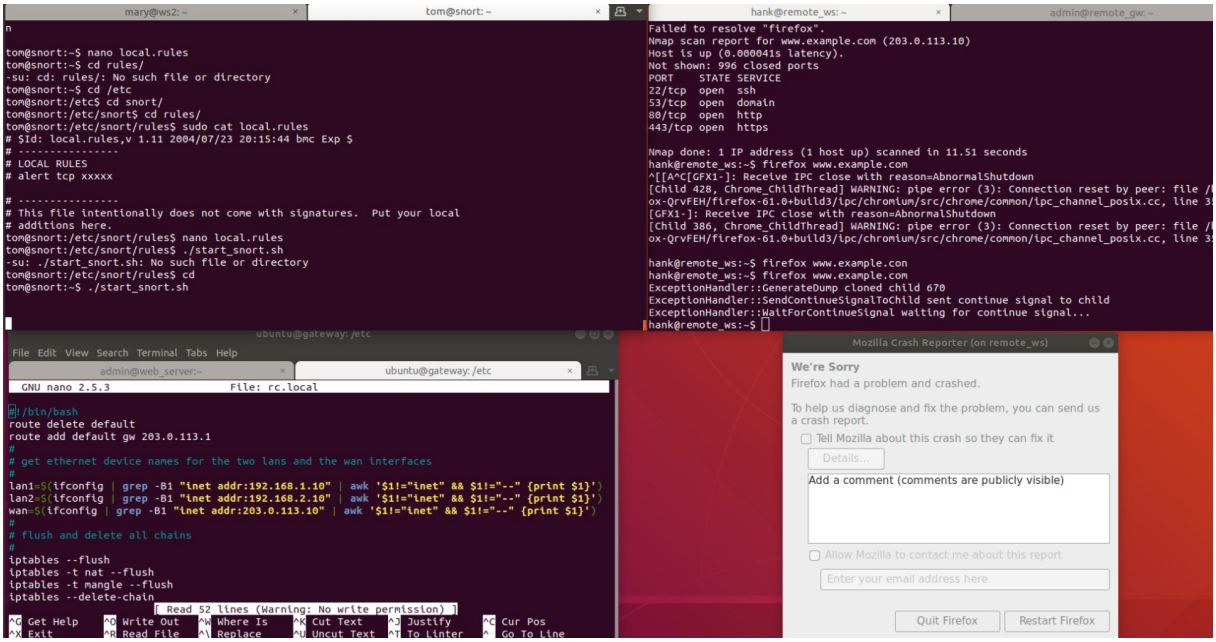


Task 3. Create a custom rule for confidential traffic (sec 4.4)

- 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.
-

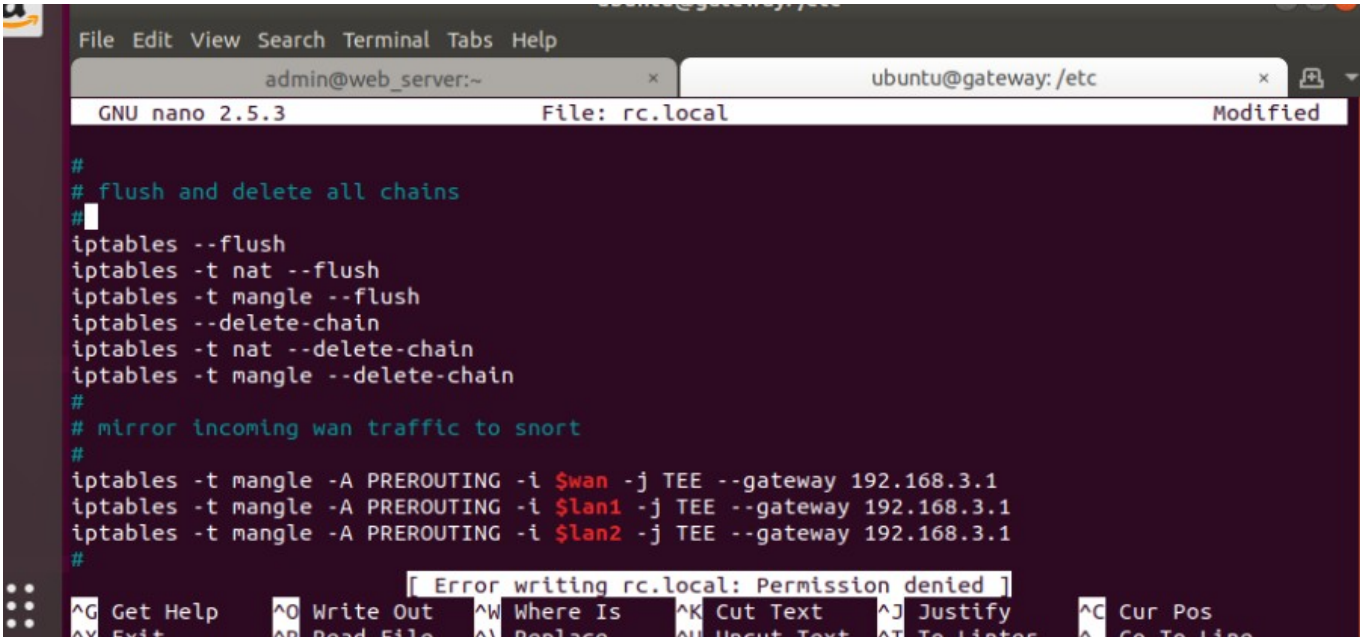


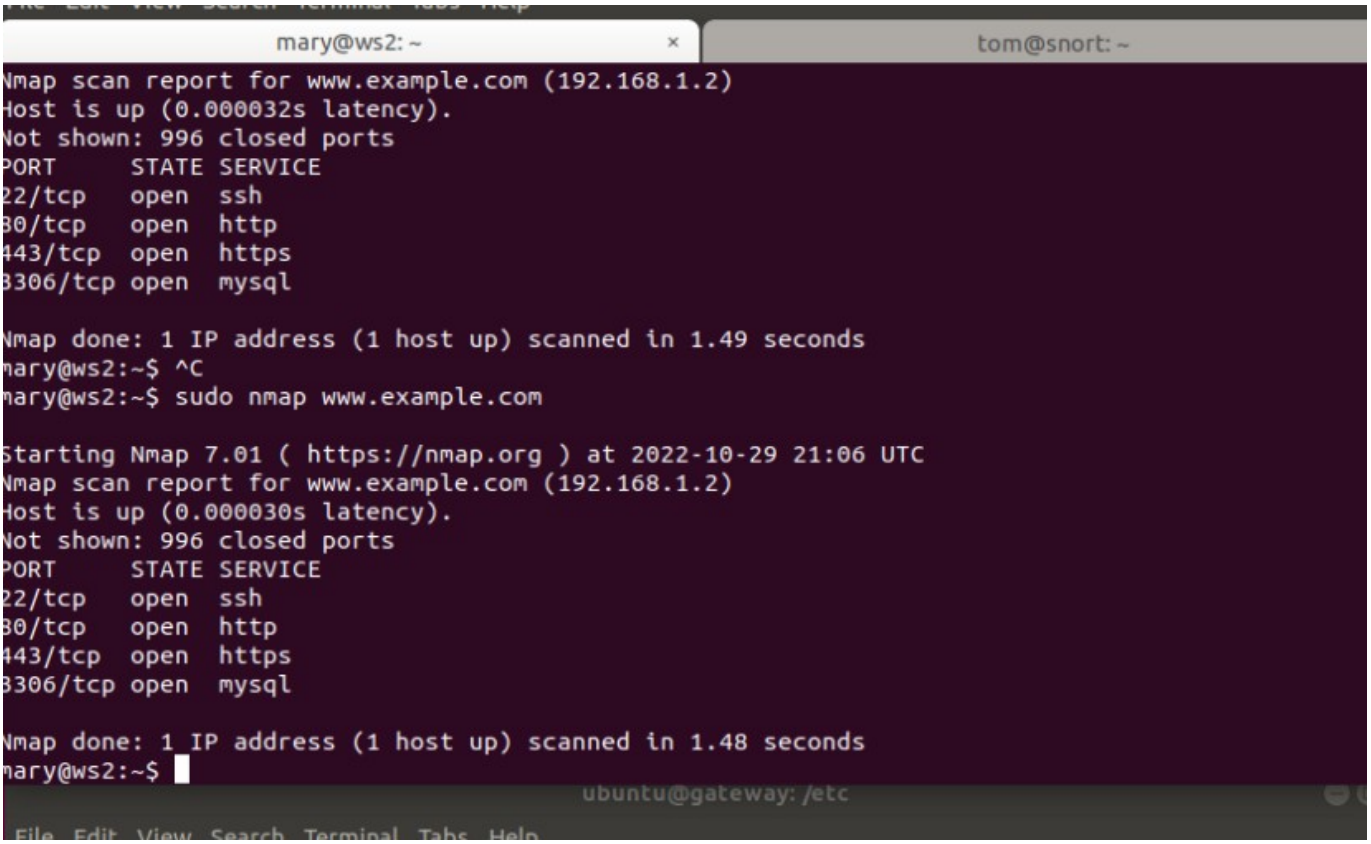
- Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.
-



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.
- 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.
-




mary@ws2: ~
tom@snort: ~
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000032s 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 1.49 seconds
mary@ws2:~$ ^C
mary@ws2:~$ sudo nmap www.example.com
Starting Nmap 7.01 (https://nmap.org) at 2022-10-29 21:06 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000030s 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 1.48 seconds
mary@ws2:~$
ubuntu@gateway: /etc