Issa Odeh

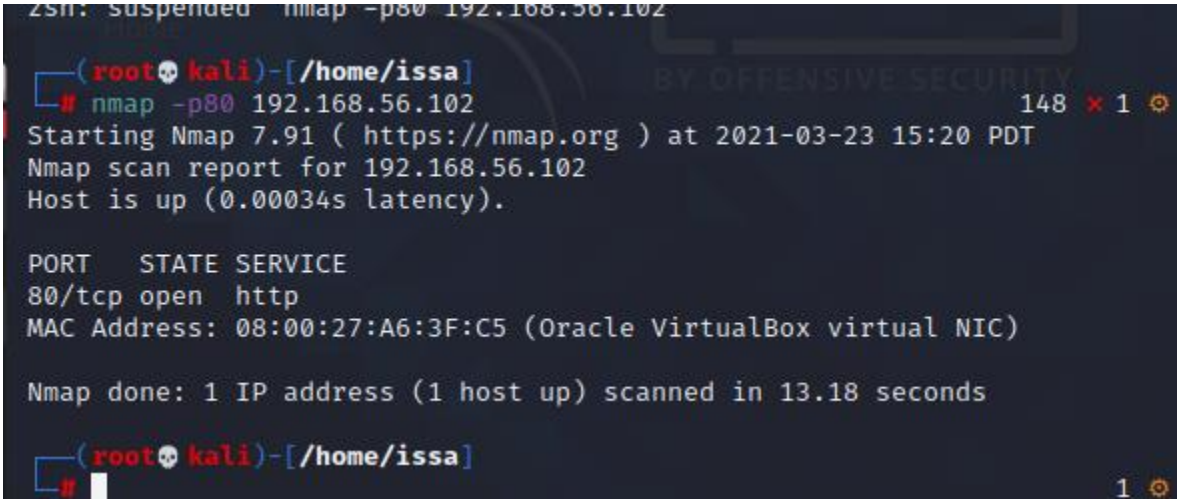
CS 445

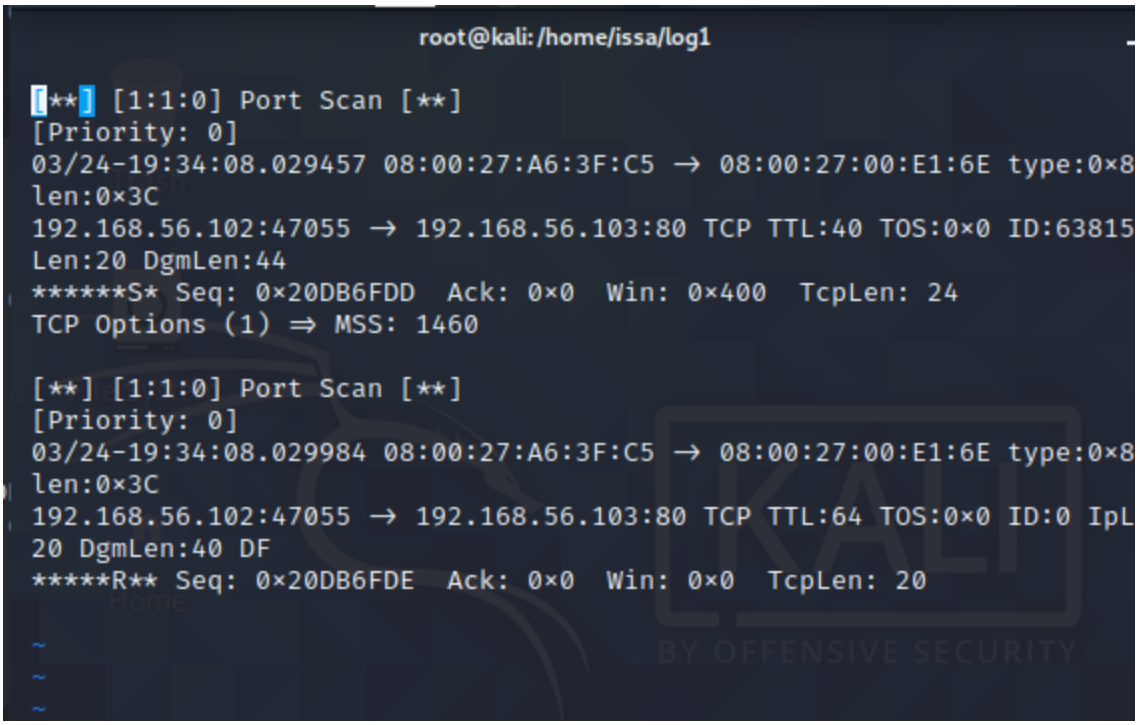
Homework 3

March 24,2021

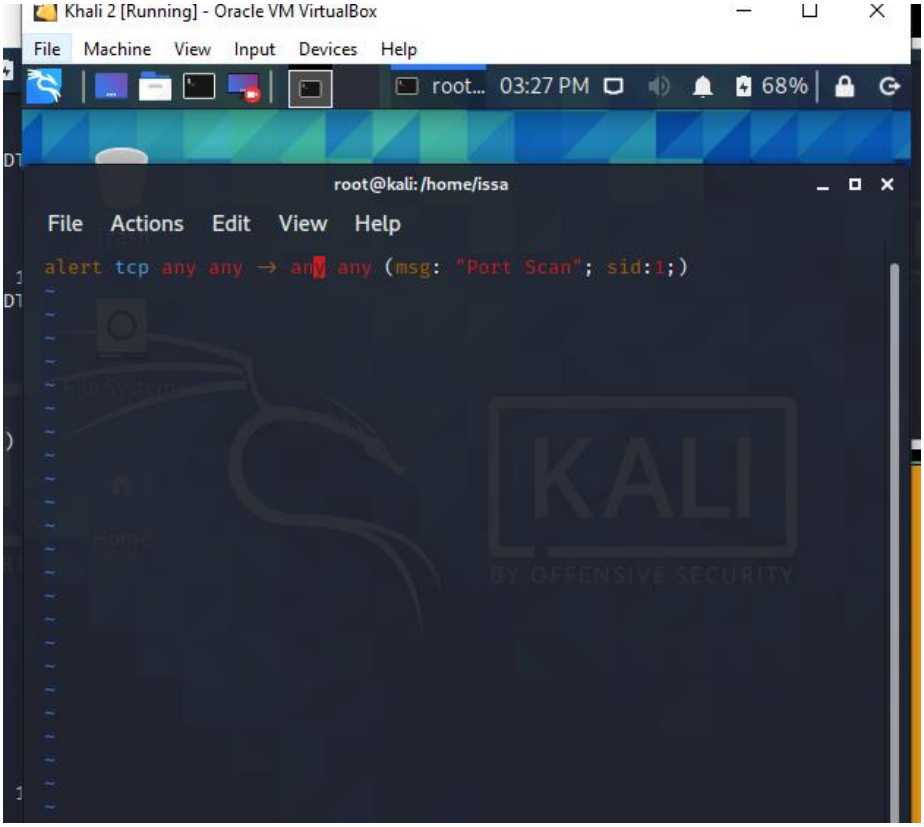
Part 1: Using sort

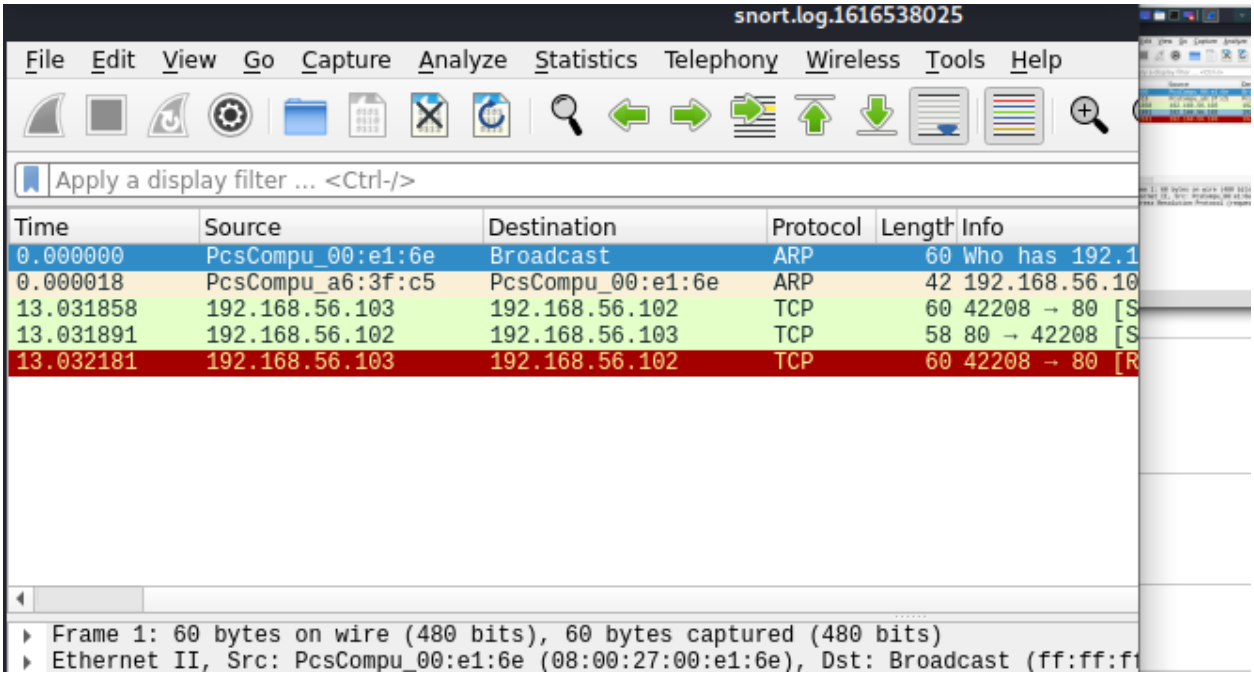
Nmap scan on port 80





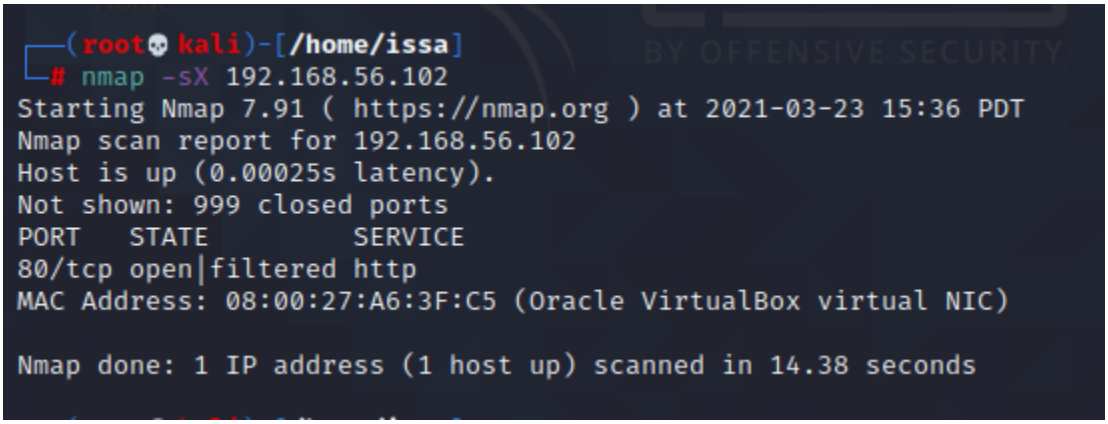
Snort does indeed detect the port scans. The signature id in this case would be 1 as it is showing in the first line. The signature is important because it will tell us If the scan was detected or not. SID is used to uniquely identify snort rules, and it allows the user identify which rule is triggered.


Khali 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root... 03:27 PM 68%
root@kali: /home/issa
File Actions Edit View Help
alert tcp any any → any any (msg: "Port Scan"; sid:1;)
KALI
BY OFFENSIVE SECURITY

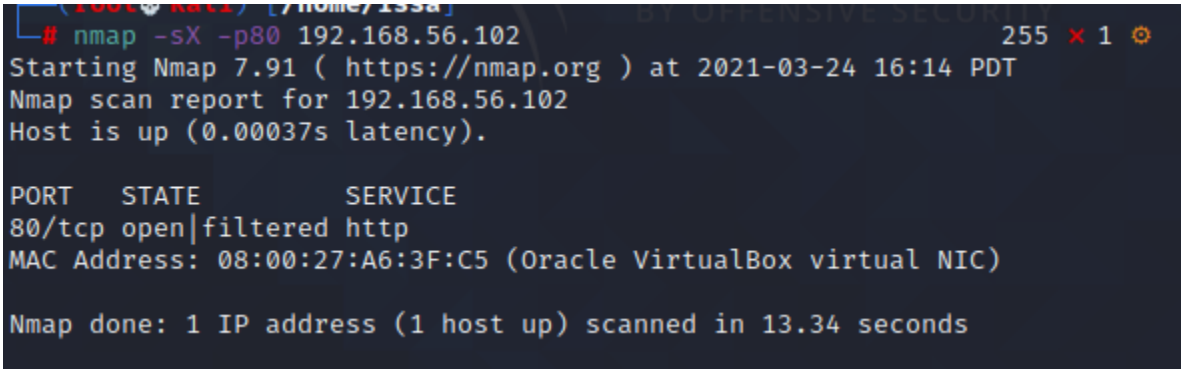

snort.log.1616538025
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
0.000000 PcsCompu_00:e1:6e Broadcast ARP 60 Who has 192.1
0.000018 PcsCompu_a6:3f:c5 PcsCompu_00:e1:6e ARP 42 192.168.56.10
13.031858 192.168.56.103 192.168.56.102 TCP 60 42208 → 80 [S
13.031891 192.168.56.102 192.168.56.103 TCP 58 80 → 42208 [S
13.032181 192.168.56.103 192.168.56.102 TCP 60 42208 → 80 [R
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: PcsCompu_00:e1:6e (08:00:27:00:e1:6e), Dst: Broadcast (ff:ff:f

3.

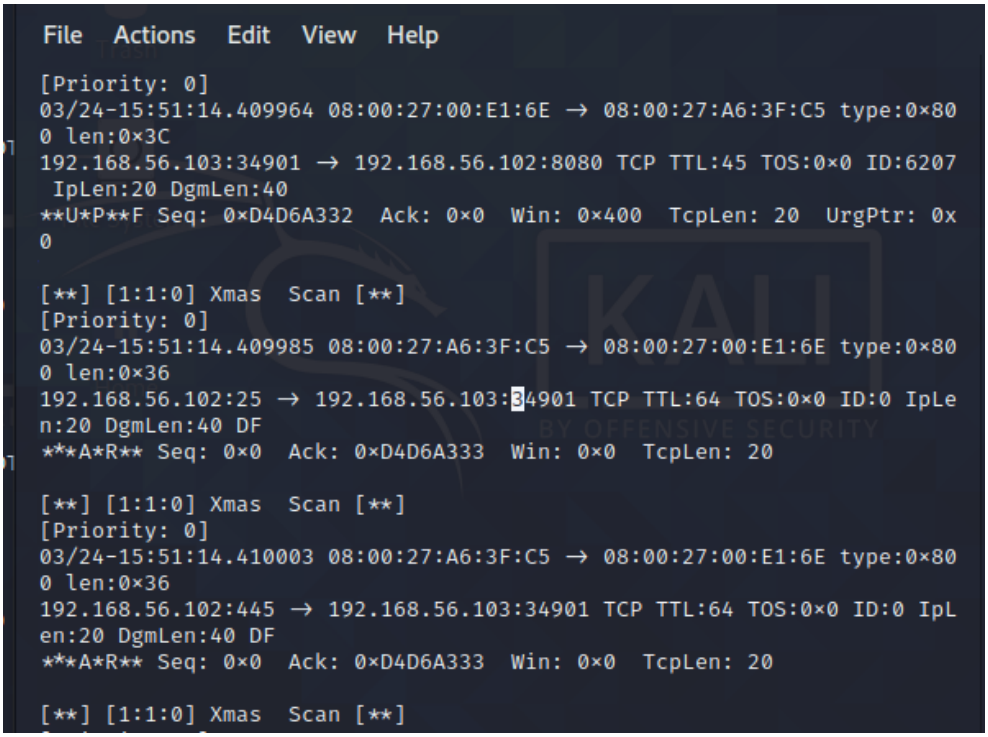
Nmap Xmas stealthy scan



I did two scans. One above is on all ports and one below is just at port 80.

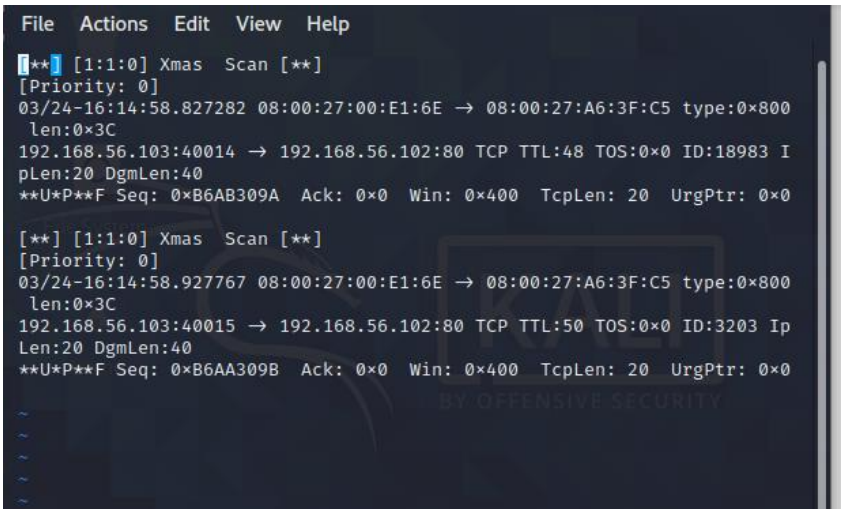


Alert for this screenshot on all ports.

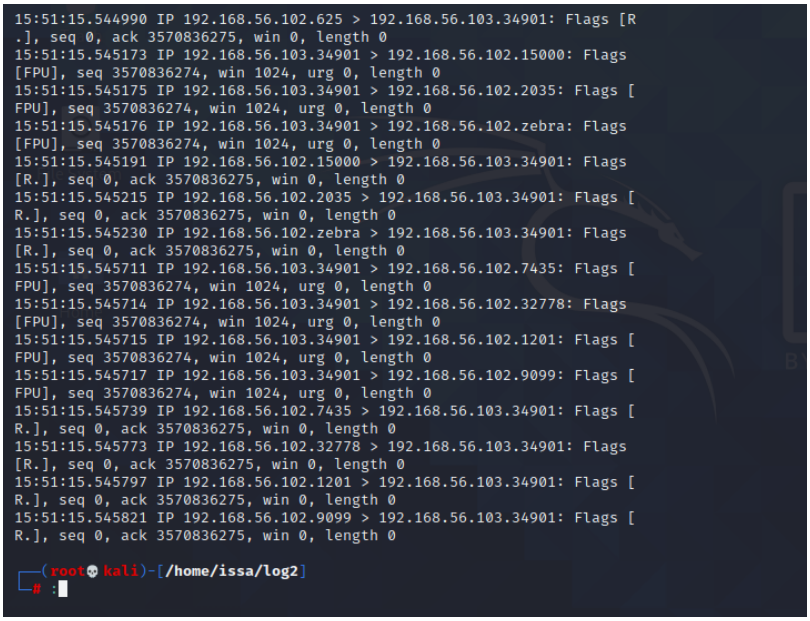


When doing the stealthy xmas scanning there was a flag but there is no response coming in. If a RST packet is received, the port is considered closed, while no response means it is open/filtered. It does not manage to evade snort in this case. The signature identified was 1 and the rev is 0. I can clearly see the flags shown above.

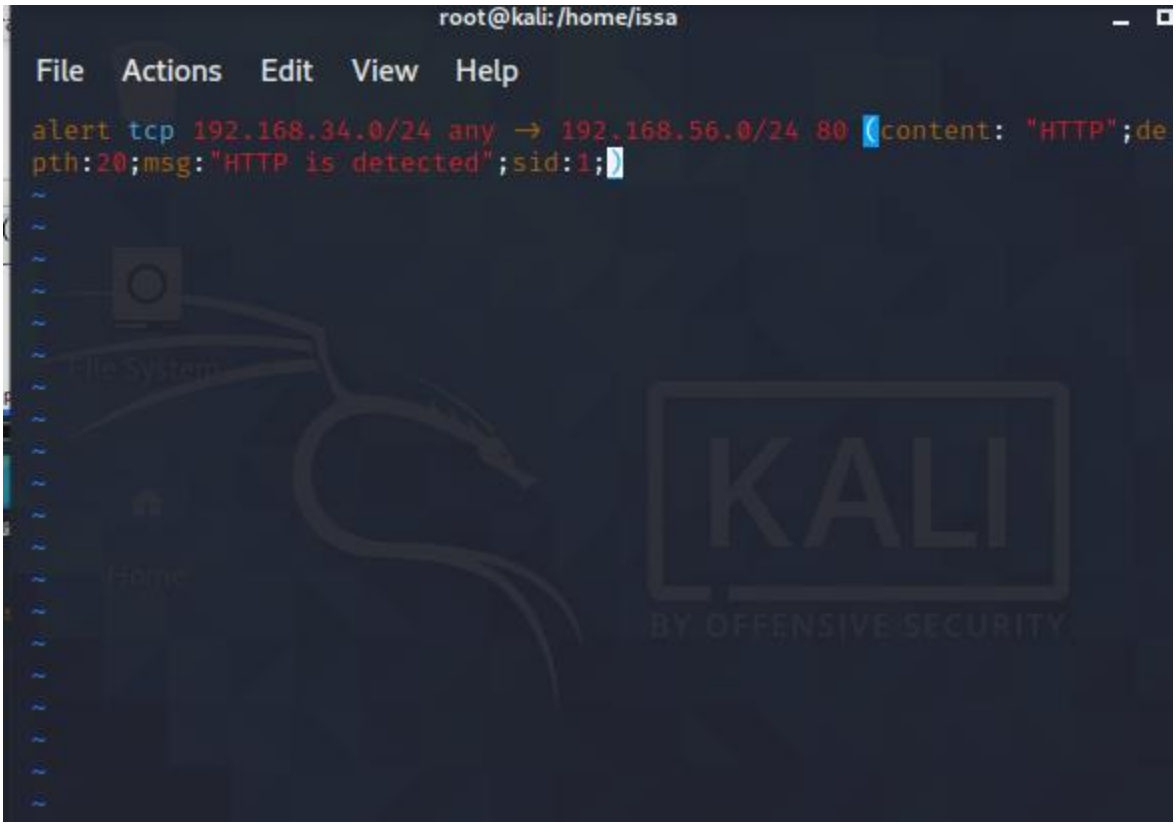
This one I only ran the scan on port 80 and this is the results. Same as above. There is no response.



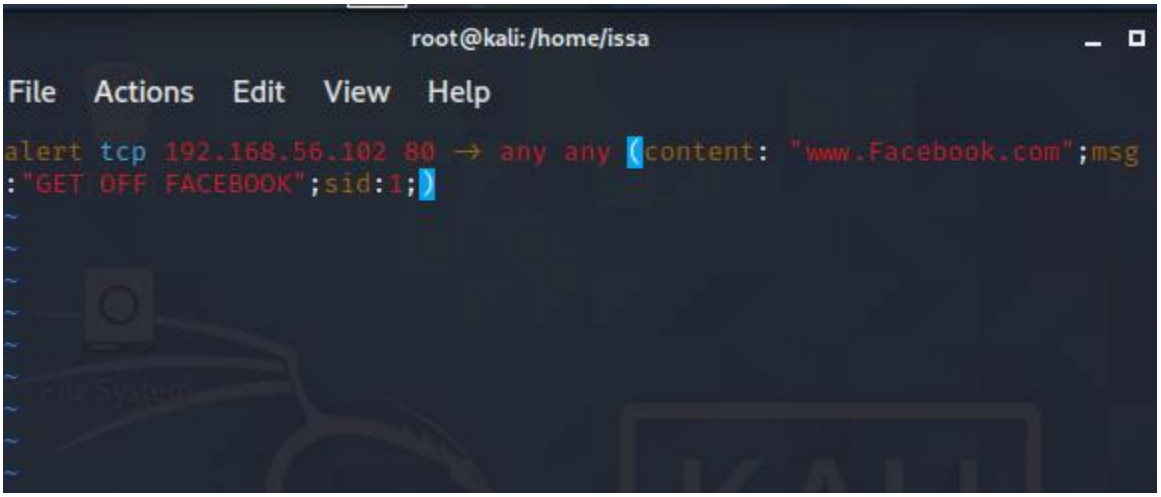
Used tcp dumb for this screenshot



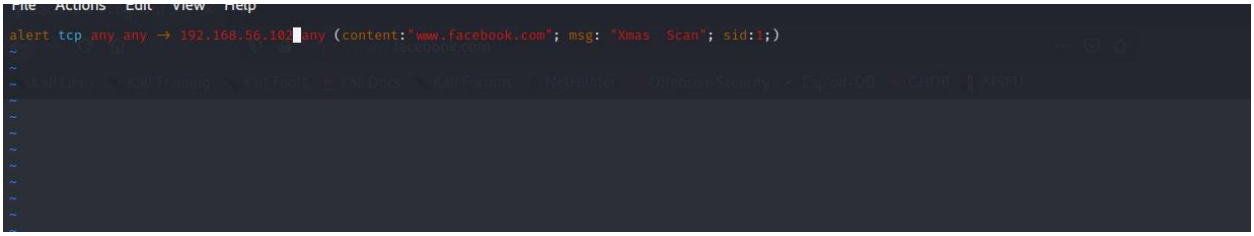
Part 2:



I tried to use this alert and the one below. This one didn't quite work.



This alert worked when I opened Facebook browser.



Used tcpdump to open information. Was not quite sure where else I can get the message. I tried wireshark but my computer did not have the best time running it.