John Gavigan
IST 451
Professor Meky
03/26/2023

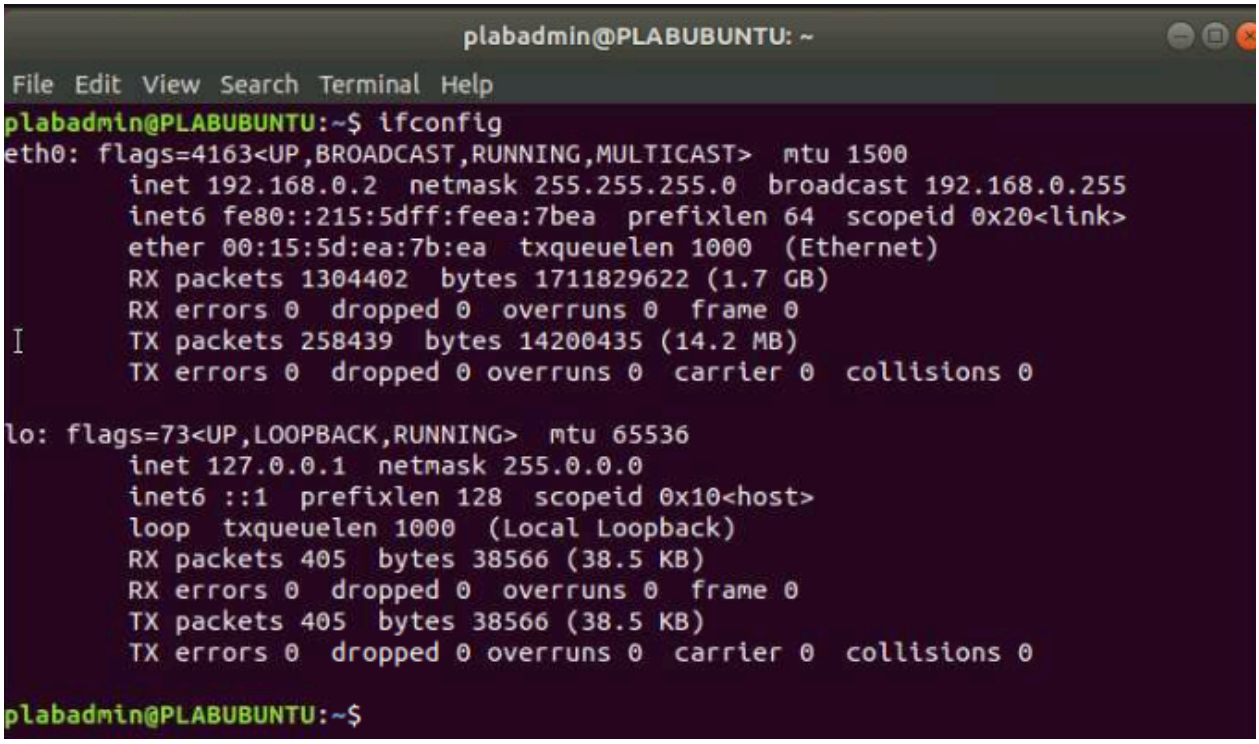
Intrusion Detection Lab

Exercise 1 - Snort

Task 0 - Start Up

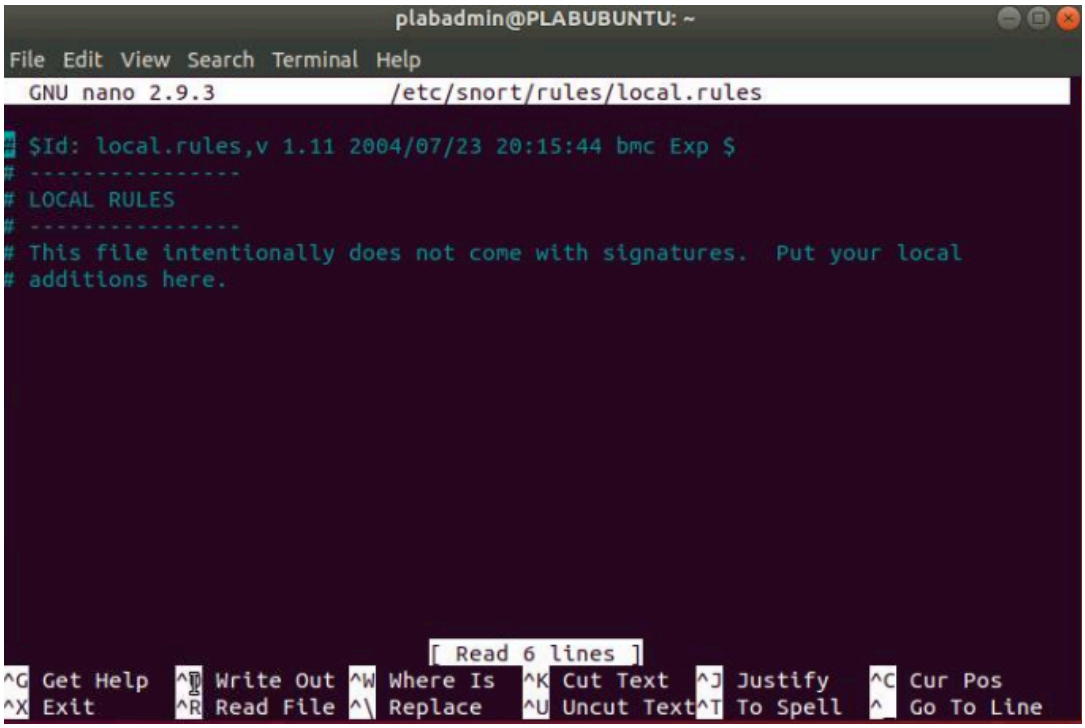
Task 1 - Ping Detection

1. Open terminal
2. VM IP address: **192.168.0.2**

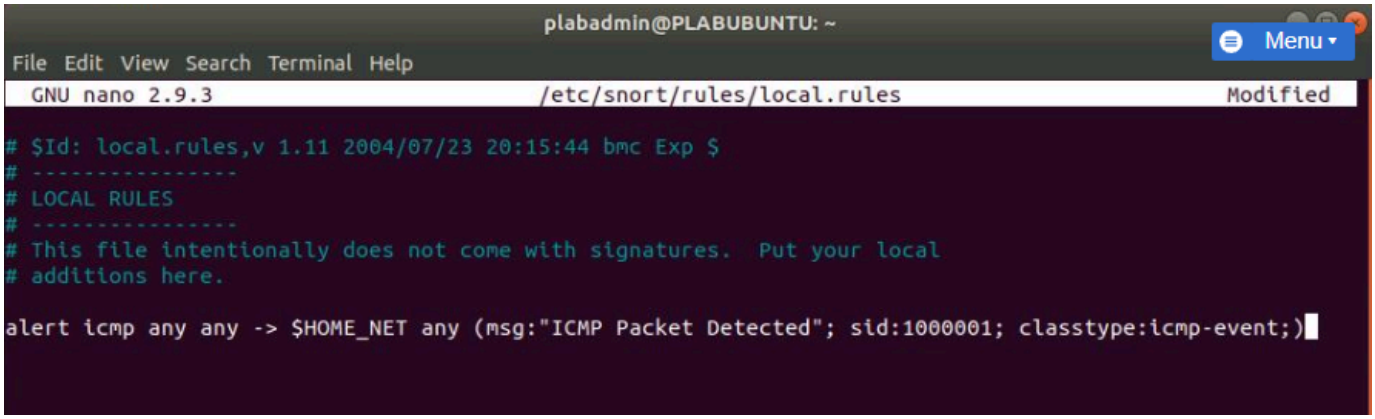


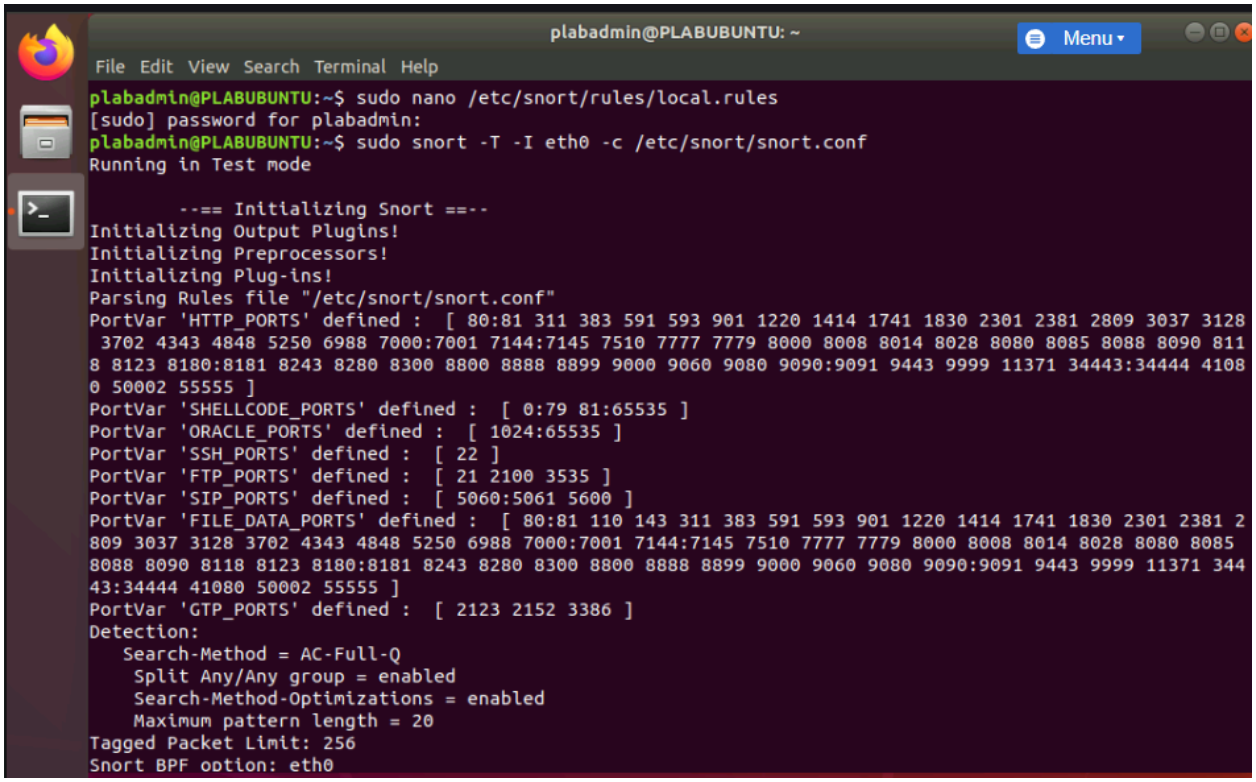
3. Open snort rules

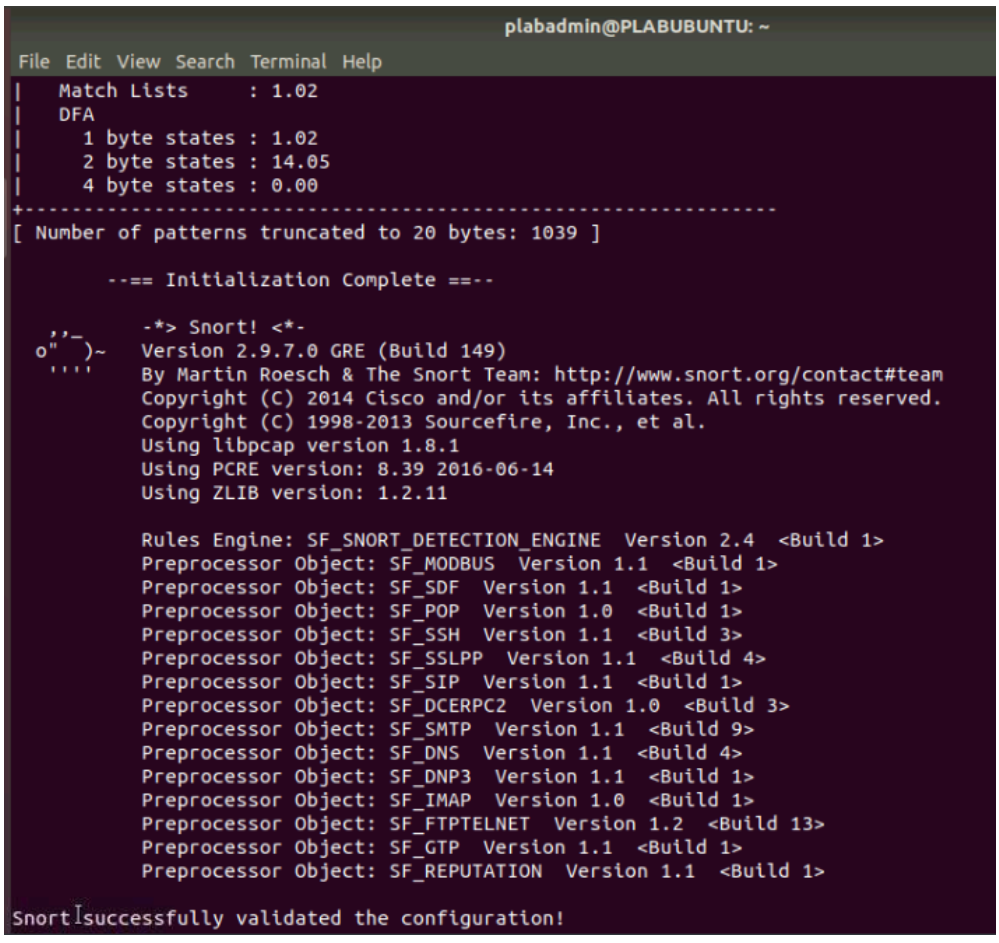
```
plabadmin@PLABUBUNTU:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for plabadmin:
plabadmin@PLABUBUNTU:~$
```



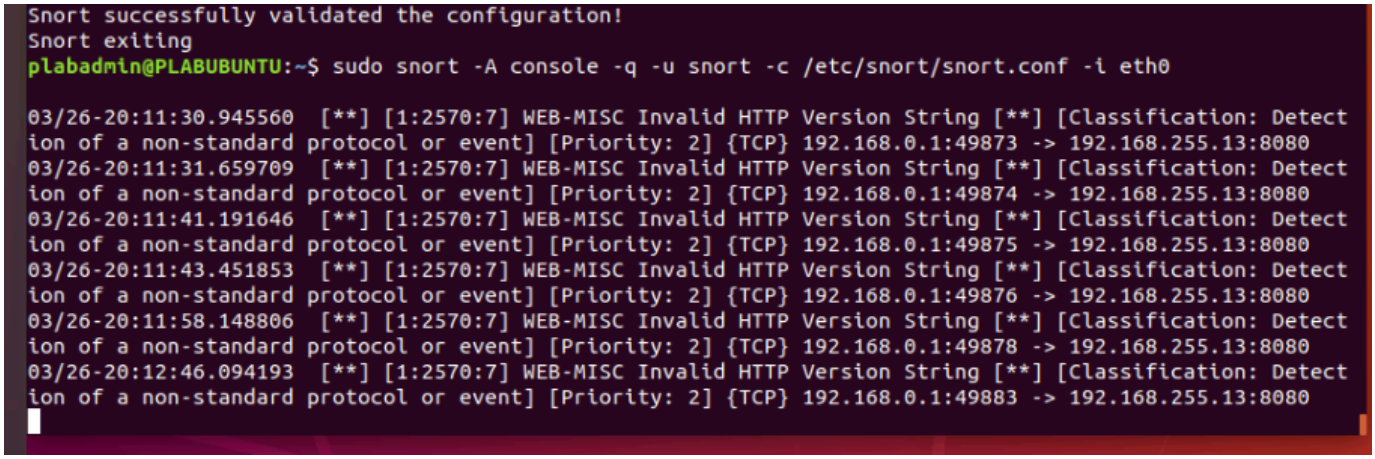
4. Create ping detection rule



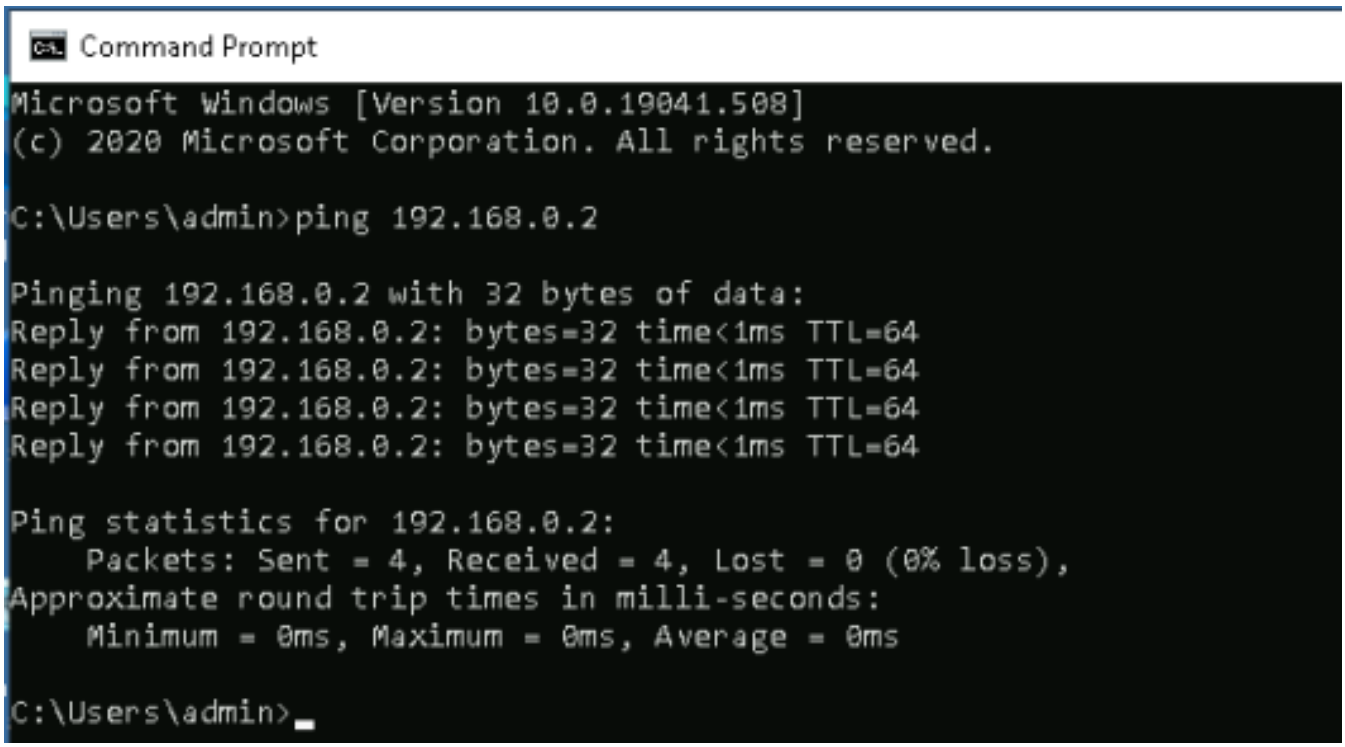

plabadmin@PLABUBUNTU: ~
Menu
File Edit View Search Terminal Help
plabadmin@PLABUBUNTU:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for plabadmin:
plabadmin@PLABUBUNTU:~$ sudo snort -T -I eth0 -c /etc/snort/snort.conf
Running in Test mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555]
PortVar 'SHELLCODE_PORTS' defined : [0:79 81:65535]
PortVar 'ORACLE_PORTS' defined : [1024:65535]
PortVar 'SSH_PORTS' defined : [22]
PortVar 'FTP_PORTS' defined : [21 2100 3535]
PortVar 'SIP_PORTS' defined : [5060:5061 5600]
PortVar 'FILE_DATA_PORTS' defined : [80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555]
PortVar 'GTP_PORTS' defined : [2123 2152 3386]
Detection:
Search-Method = AC-Full-Q
Split Any/Any group = enabled
Search-Method-Optimizations = enabled
Maximum pattern length = 20
Tagged Packet Limit: 256
Snort BPF option: eth0


plabadmin@PLABUBUNTU: ~
File Edit View Search Terminal Help
| Match Lists : 1.02
| DFA
| 1 byte states : 1.02
| 2 byte states : 14.05
| 4 byte states : 0.00
+---
[Number of patterns truncated to 20 bytes: 1039]
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Snort successfully validated the configuration!

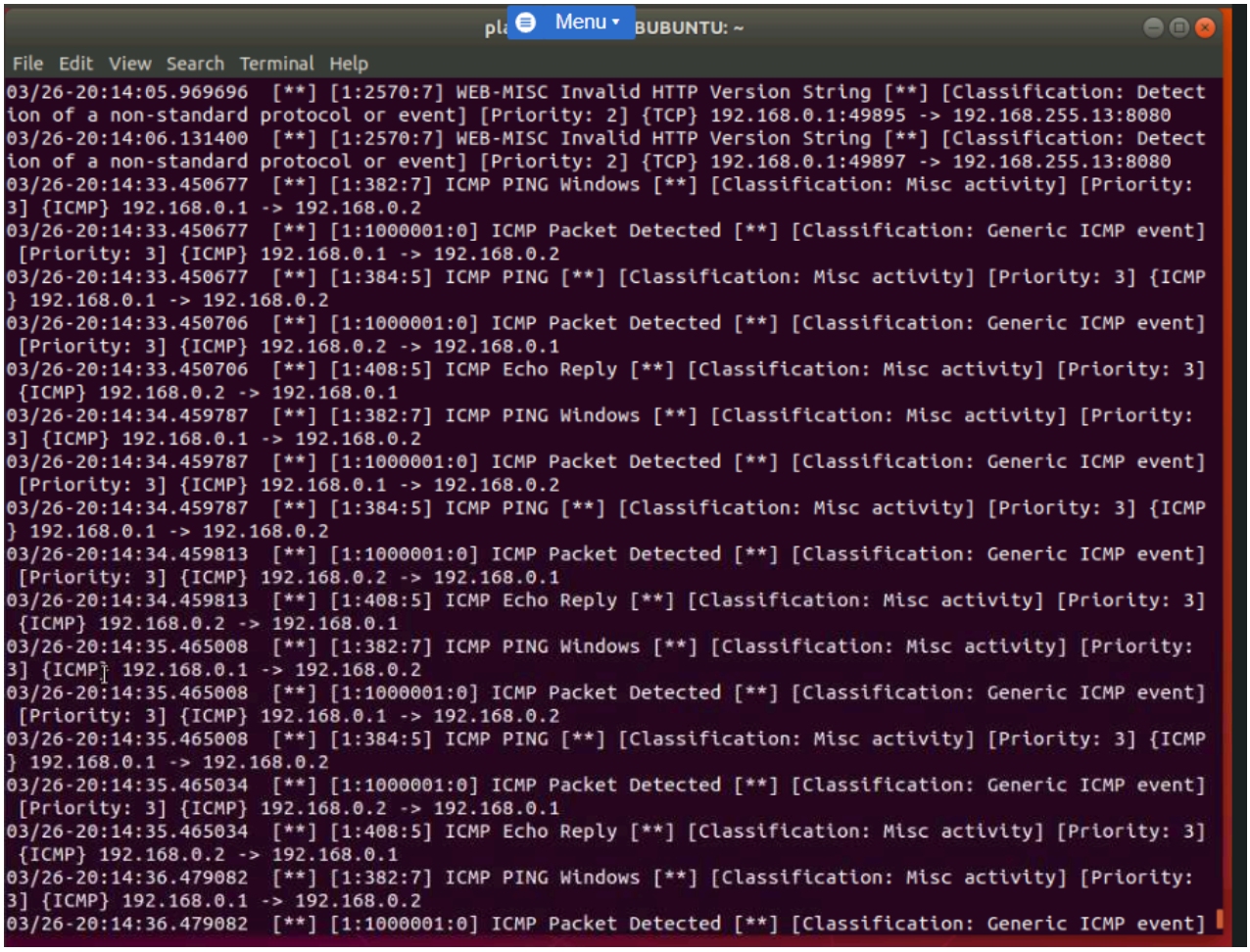
5. Start Snort and detect packages



6. Ping

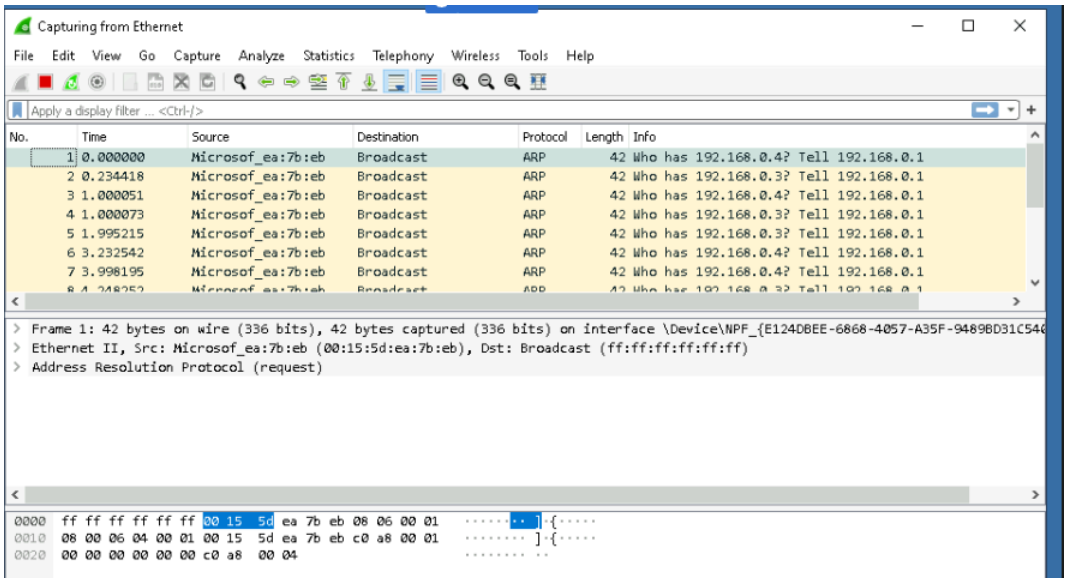


7. Detect

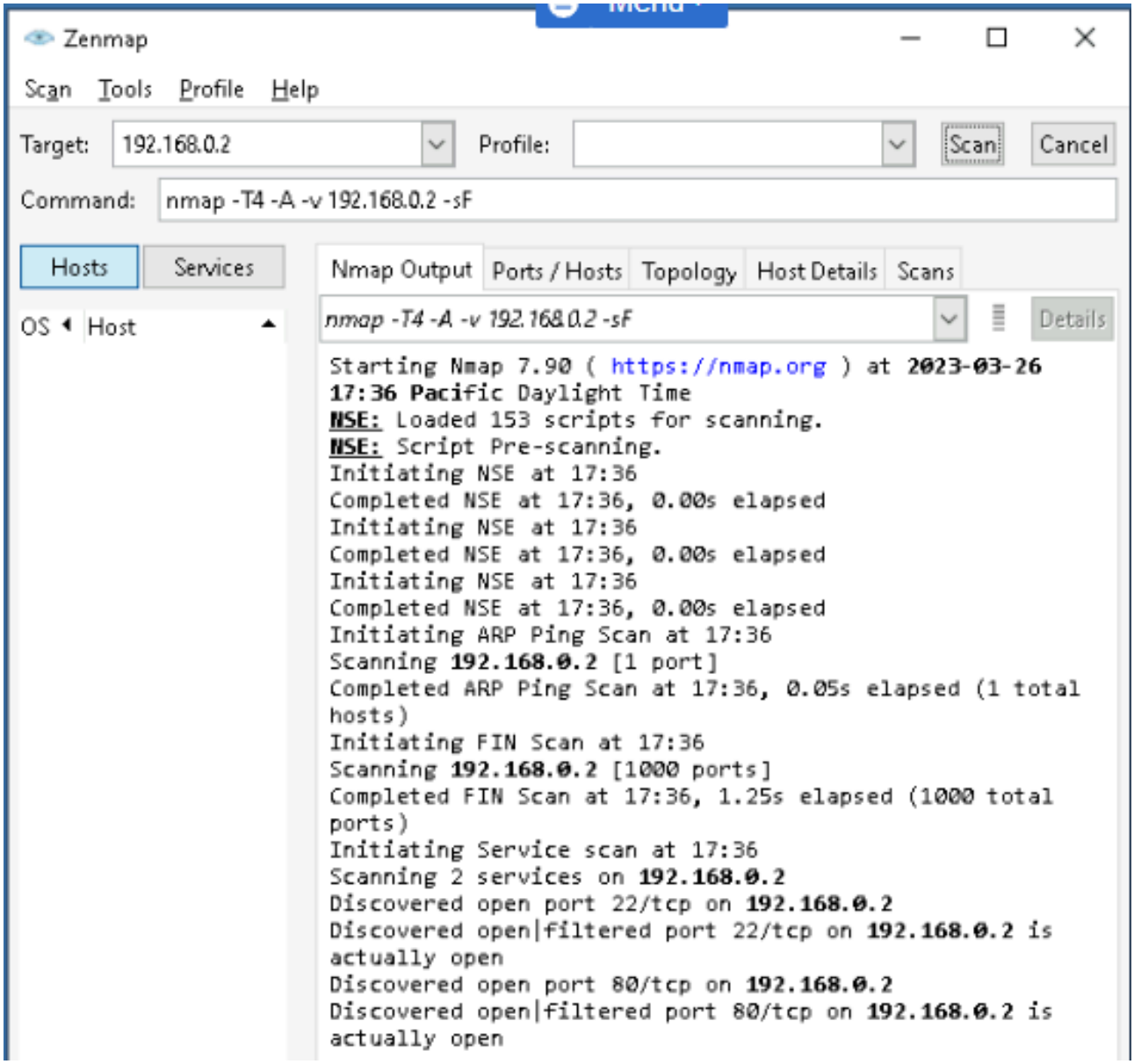


Task 2 - FIN Scan Detection

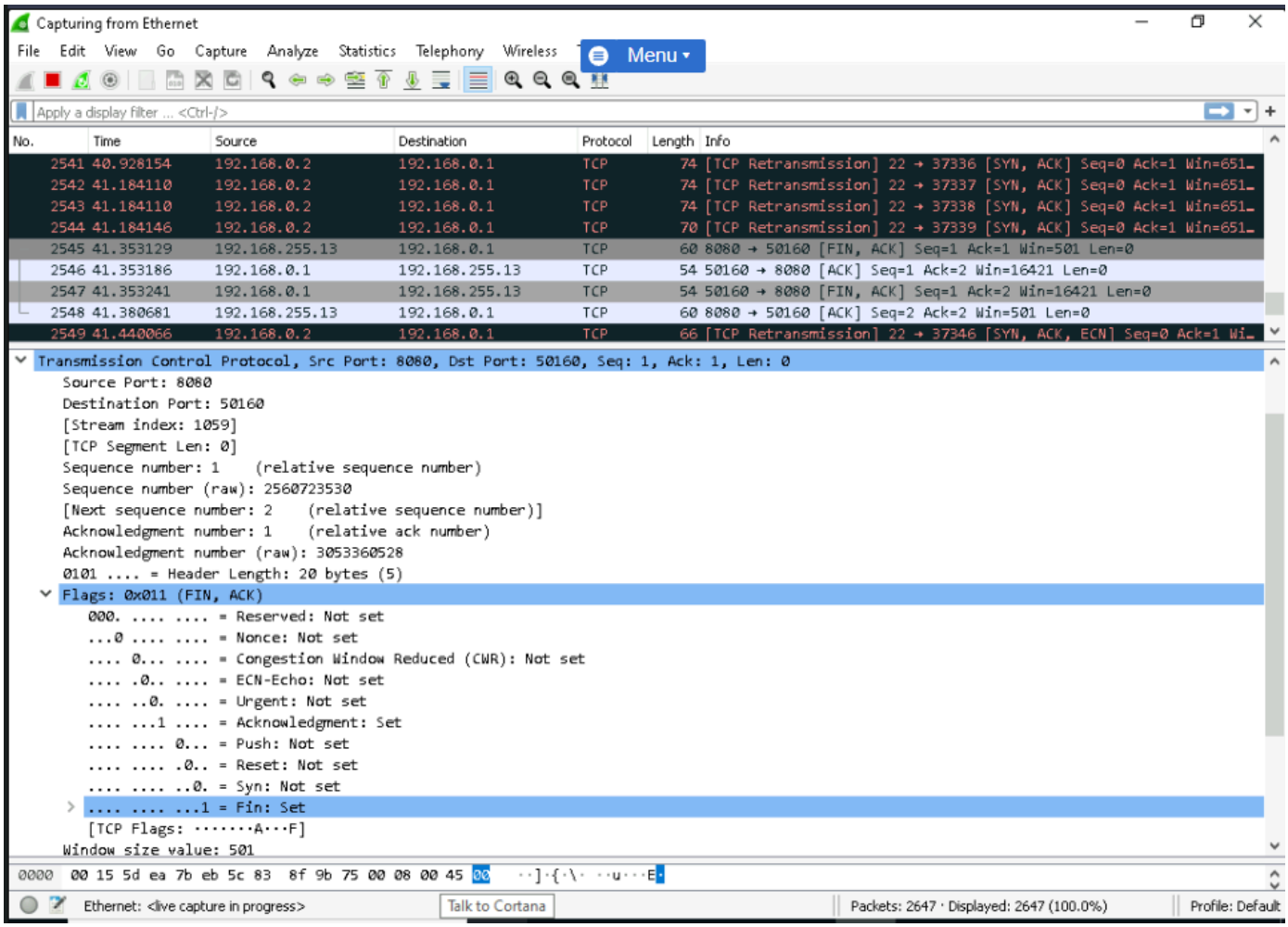
1. Start wireshark



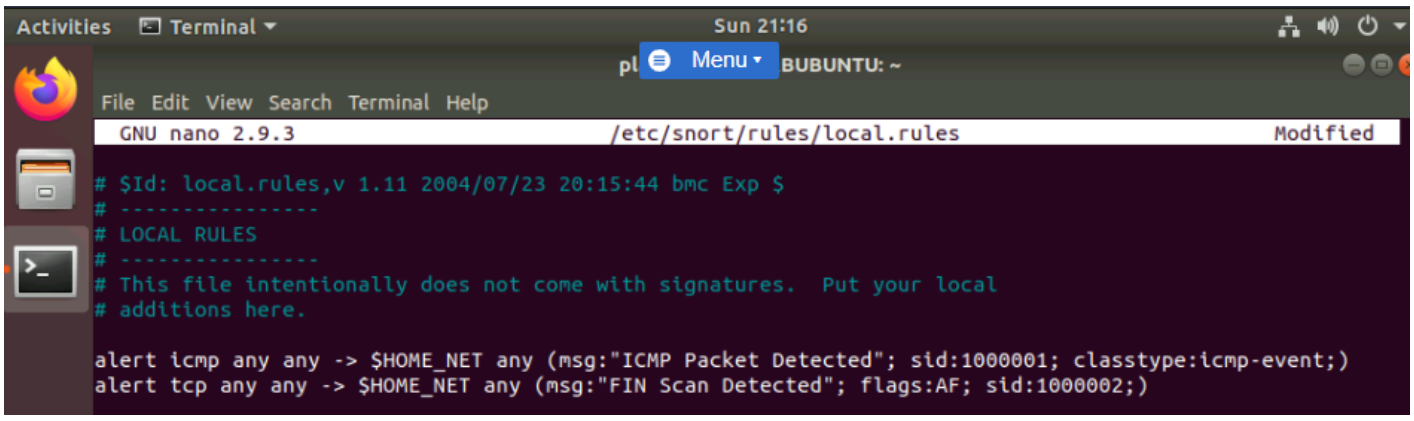
2. Zenmap


Zenmap
Scan Tools Profile Help
Target: 192.168.0.2
Profile:
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.2 -sF
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.0.2 -sF
Details
Starting Nmap 7.90 (https://nmap.org) at 2023-03-26 17:36 Pacific Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating ARP Ping Scan at 17:36
Scanning 192.168.0.2 [1 port]
Completed ARP Ping Scan at 17:36, 0.05s elapsed (1 total hosts)
Initiating FIN Scan at 17:36
Scanning 192.168.0.2 [1000 ports]
Completed FIN Scan at 17:36, 1.25s elapsed (1000 total ports)
Initiating Service scan at 17:36
Scanning 2 services on 192.168.0.2
Discovered open port 22/tcp on 192.168.0.2
Discovered open|filtered port 22/tcp on 192.168.0.2 is actually open
Discovered open port 80/tcp on 192.168.0.2
Discovered open|filtered port 80/tcp on 192.168.0.2 is actually open

3. Check wireshark



4. Edit snort rules again



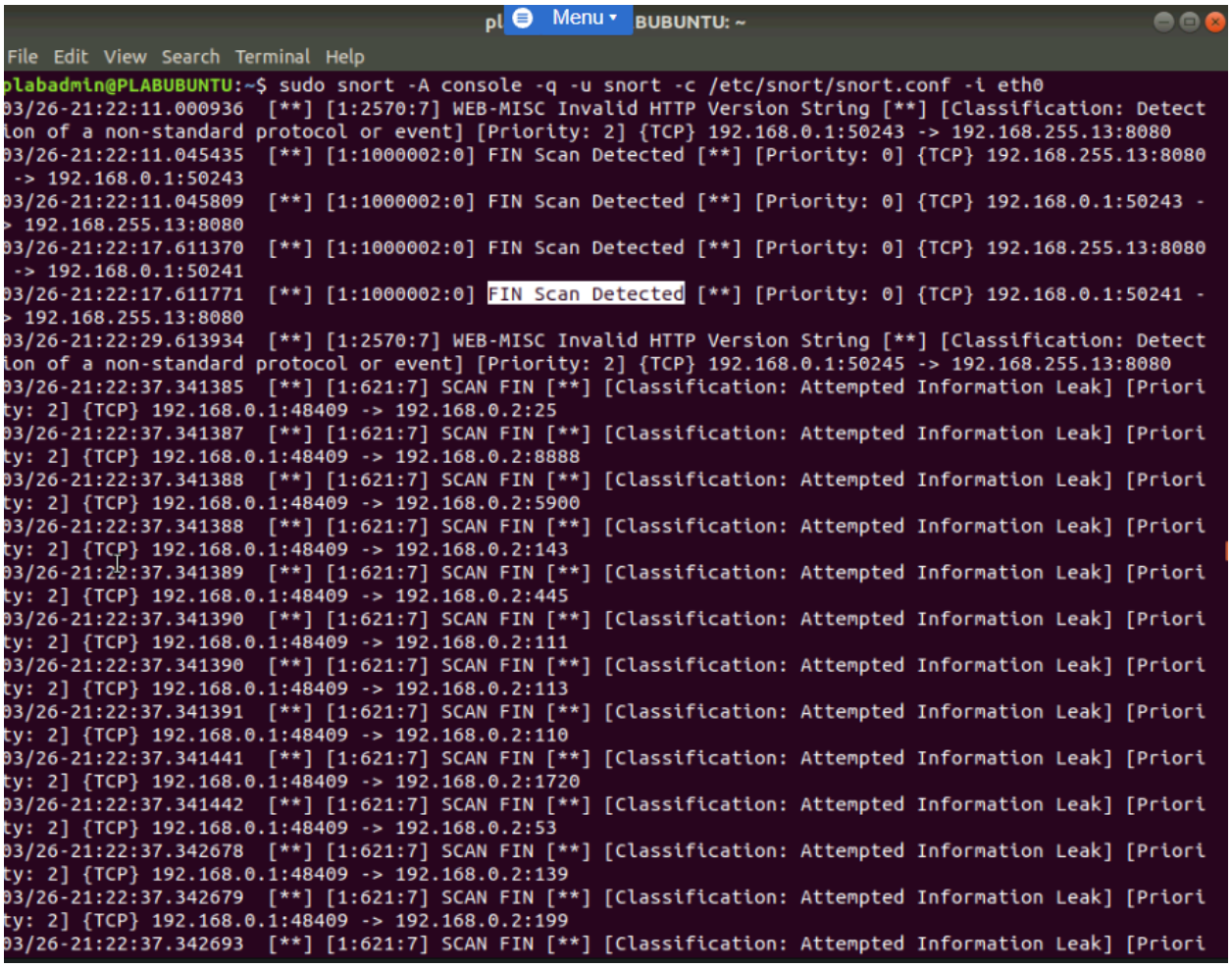
```
File  Edit  View  Search  Terminal  Help
plabadmin@PLABUBUNTU:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for plabadmin:
plabadmin@PLABUBUNTU:~$ sudo snort -T -I eth0 -c /etc/snort/snort.conf
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128
 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 811
8 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 4108
```

```
|   Match Lists      : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+-------------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]

        --== Initialization Complete ==--

   ,,_      -*> Snort! <*-
  o"  )~    Version 2.9.7.0 GRE (Build 149)
   ''''     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
            Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
            Copyright (C) 1998-2013 Sourcefire, Inc., et al.
            Using libpcap version 1.8.1
            Using PCRE version: 8.39 2016-06-14
            Using ZLIB version: 1.2.11

            Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
            Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
            Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
            Preprocessor Object: SF_POP  Version 1.0  <Build 1>
            Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
            Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
            Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
            Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
            Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
            Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
            Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
            Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
            Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
plabadmin@PLABUBUNTU:~$
```

5. Start Snort again

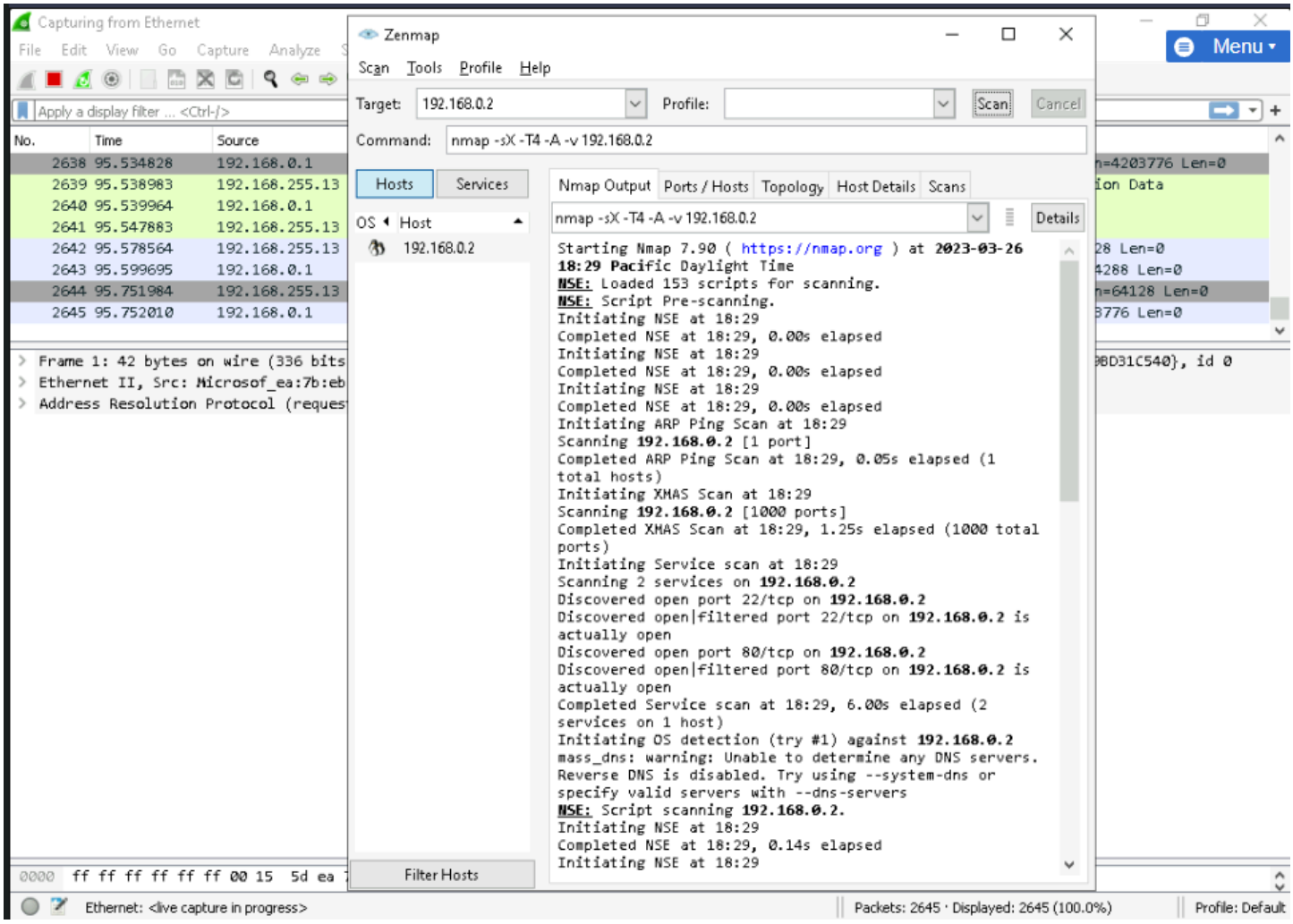
New snort displayed in next image

6. Check victim machine

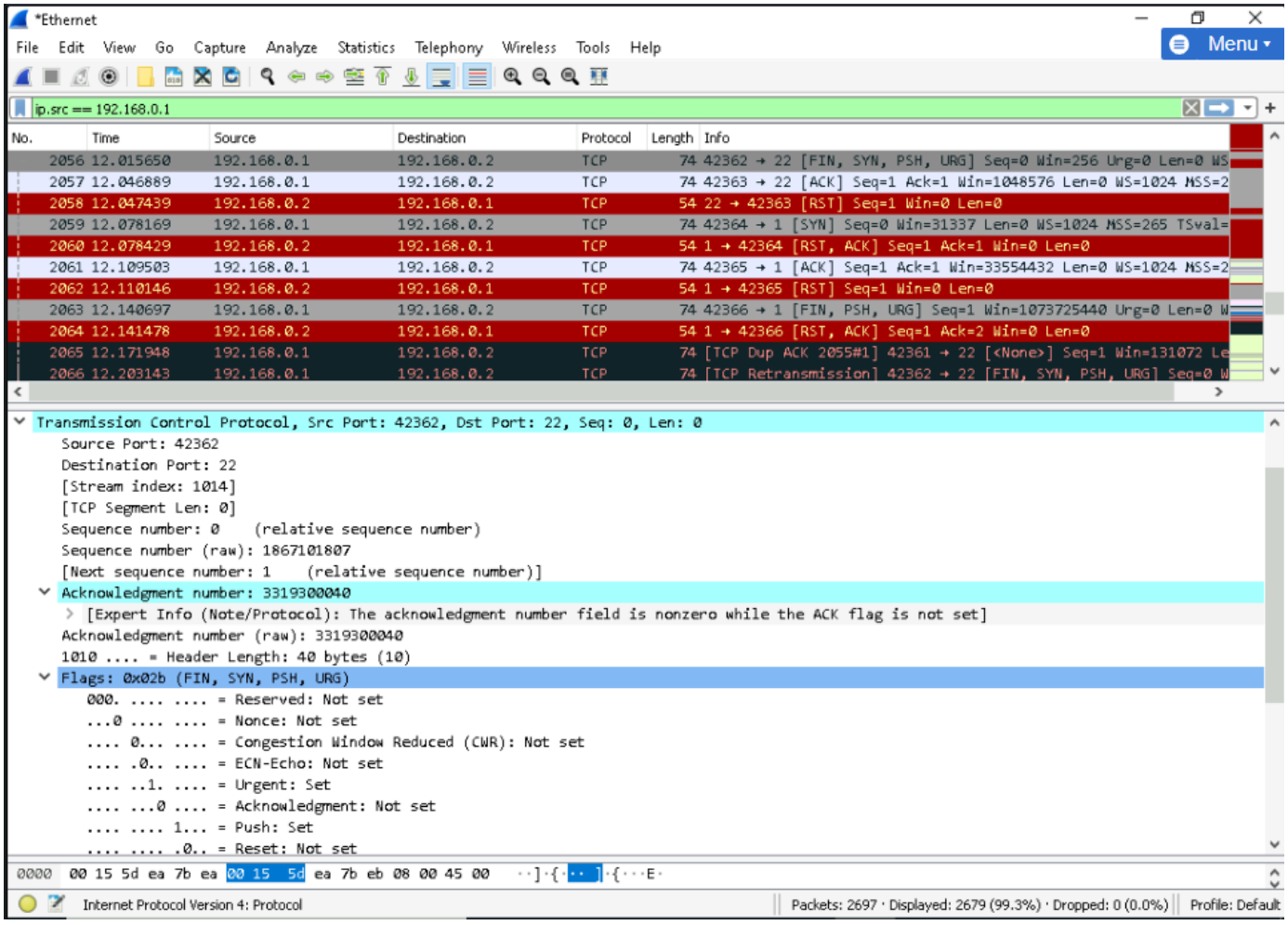


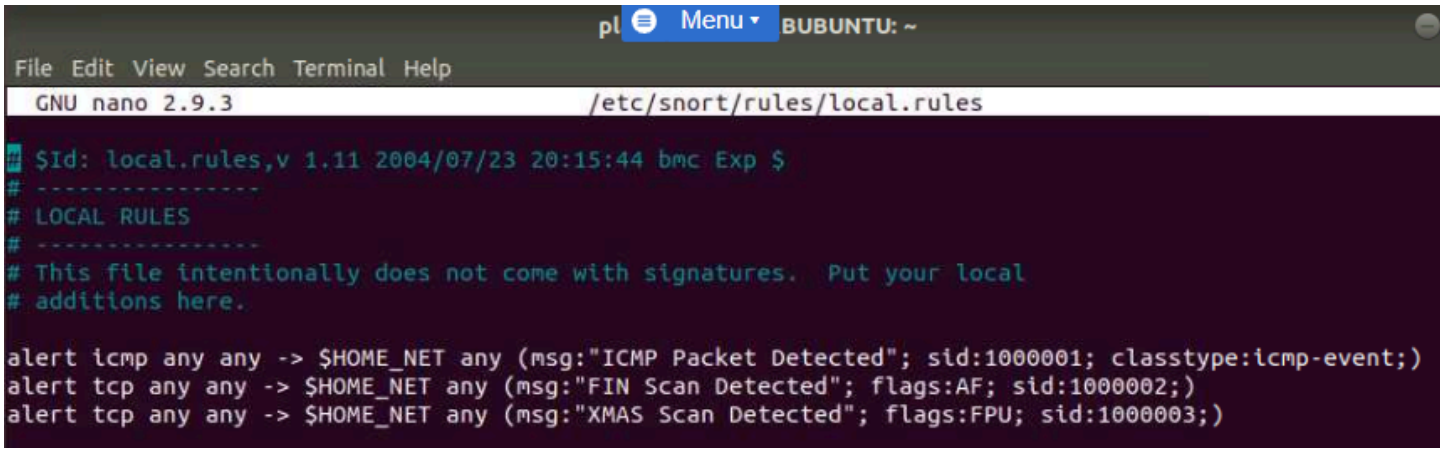
Task 3 - XMAS Scan Detection

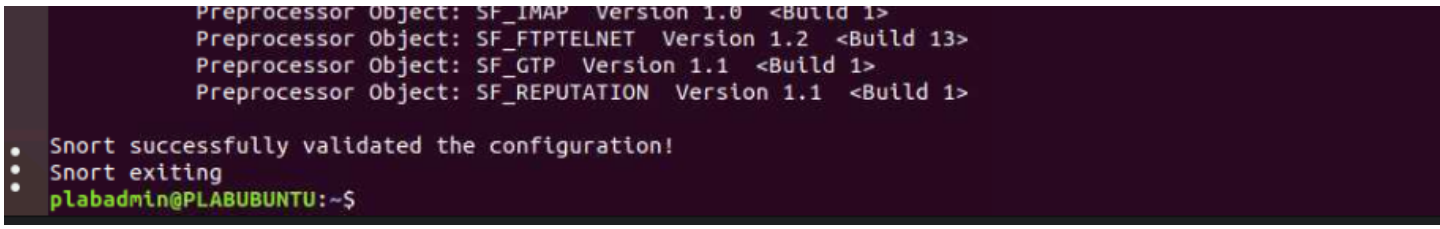
1. Begin wireshark capture and generate XMAS scan (continued below)


Capturing from Ethernet
File Edit View Go Capture Analyze
Apply a display filter ... <Ctrl-/>
No. Time Source
2638 95.534828 192.168.0.1
2639 95.538983 192.168.255.13
2640 95.539964 192.168.0.1
2641 95.547883 192.168.255.13
2642 95.578564 192.168.255.13
2643 95.599695 192.168.0.1
2644 95.751984 192.168.255.13
2645 95.752010 192.168.0.1
Frame 1: 42 bytes on wire (336 bits
Ethernet II, Src: Microsof_ea:7b:eb
Address Resolution Protocol (reques
0000 ff ff ff ff ff ff 00 15 5d ea
Ethernet: <live capture in progress>
Zenmap
Scan Tools Profile Help
Target: 192.168.0.2
Profile:
Scan
Cancel
Command: nmap -sX -T4 -A -v 192.168.0.2
Hosts
Services
OS Host
192.168.0.2
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sX -T4 -A -v 192.168.0.2
Details
Starting Nmap 7.90 (https://nmap.org) at 2023-03-26 18:29 Pacific Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:29
Completed NSE at 18:29, 0.00s elapsed
Initiating NSE at 18:29
Completed NSE at 18:29, 0.00s elapsed
Initiating NSE at 18:29
Completed NSE at 18:29, 0.00s elapsed
Initiating ARP Ping Scan at 18:29
Scanning 192.168.0.2 [1 port]
Completed ARP Ping Scan at 18:29, 0.05s elapsed (1 total hosts)
Initiating XMAS Scan at 18:29
Scanning 192.168.0.2 [1000 ports]
Completed XMAS Scan at 18:29, 1.25s elapsed (1000 total ports)
Initiating Service scan at 18:29
Scanning 2 services on 192.168.0.2
Discovered open port 22/tcp on 192.168.0.2
Discovered open|filtered port 22/tcp on 192.168.0.2 is actually open
Discovered open port 80/tcp on 192.168.0.2
Discovered open|filtered port 80/tcp on 192.168.0.2 is actually open
Completed Service scan at 18:29, 6.00s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.2
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
NSE: Script scanning 192.168.0.2.
Initiating NSE at 18:29
Completed NSE at 18:29, 0.14s elapsed
Initiating NSE at 18:29
Menu
Packets: 2645 · Displayed: 2645 (100.0%)
Profile: Default

2. Identify flags in wireshark and make new snort rule



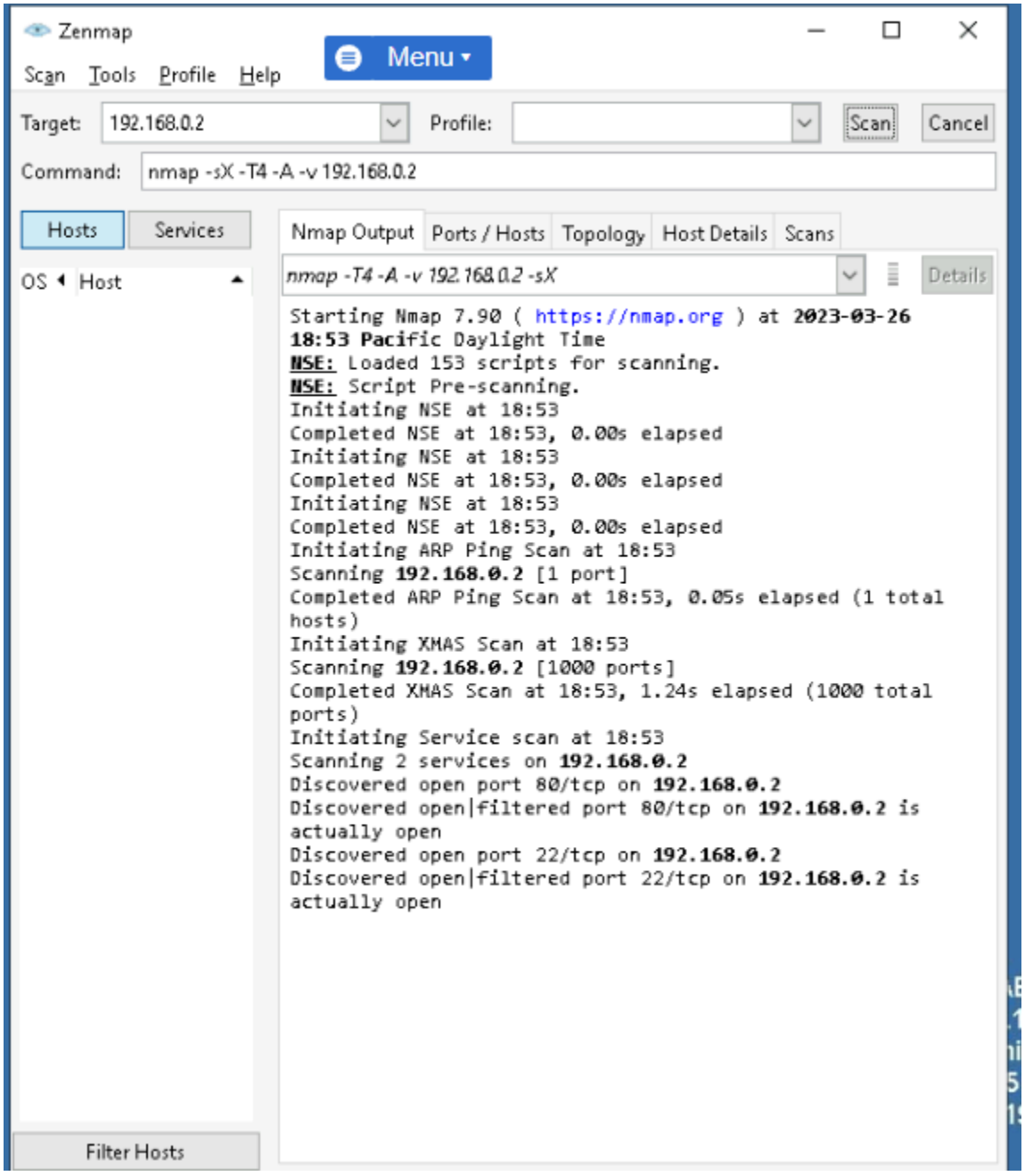




3. Start Snort

```
Snort successfully validated the configuration!
Snort exiting
plabadmin@PLABUBUNTU:~$ sudo snort -A console -q -u snort -c /etc/snort/snort.conf -i eth0
```

4. Generate new XMAS scan



5. Check alert terminal