

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**

```
plabadmin@PLABUBUNTU:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.2 netmask 255.255.255.0 broadcast 192.168.0.255
              inet6 fe80::215:5dff:feea:7bea prefixlen 64 scopeid 0x20<link>
                ether 00:15:5d:ea:7b:ea txqueuelen 1000 (Ethernet)
                  RX packets 1304402 bytes 1711829622 (1.7 GB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  I    TX packets 258439 bytes 14200435 (14.2 MB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

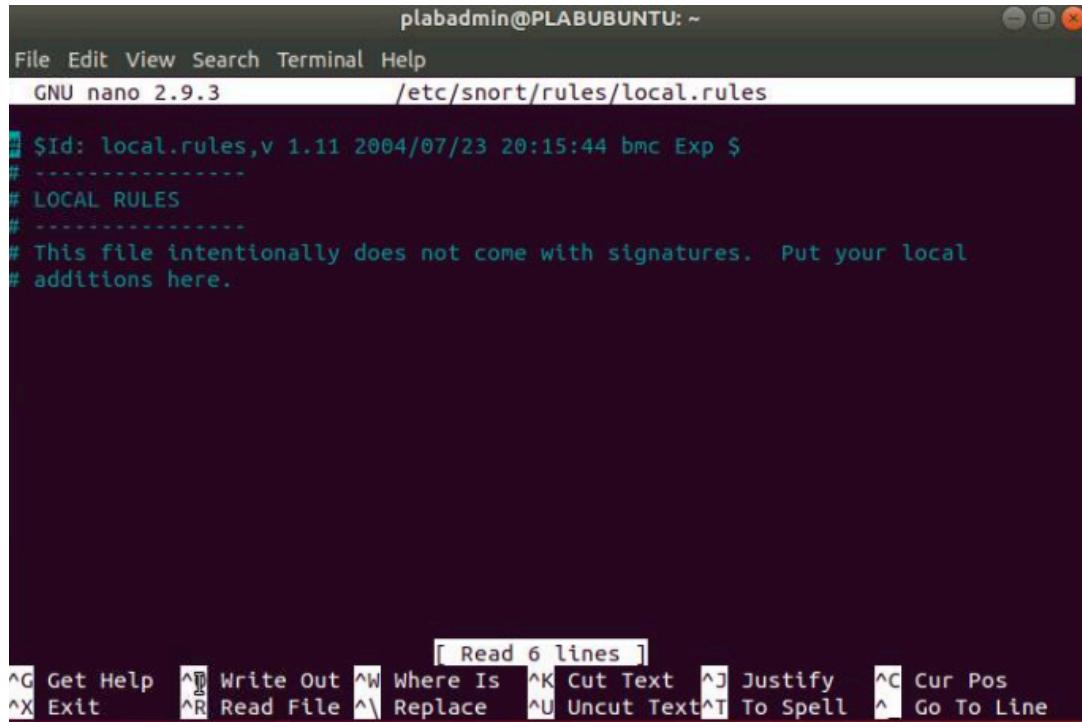
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                loop txqueuelen 1000 (Local Loopback)
                  RX packets 405 bytes 38566 (38.5 KB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 405 bytes 38566 (38.5 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

plabadmin@PLABUBUNTU:~$
```

A terminal window titled "plabadmin@PLABUBUNTU: ~". The window contains the output of the "ifconfig" command. It shows two interfaces: "eth0" and "lo". The "eth0" interface is connected to the network with an IP of 192.168.0.2, a netmask of 255.255.255.0, and a broadcast address of 192.168.0.255. It has received 1.7 GB of data and transmitted 14.2 MB. The "lo" interface is the loopback interface with an IP of 127.0.0.1 and a netmask of 255.0.0.0. Both interfaces have 0 errors and 0 collisions.

3. Open snort rules

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

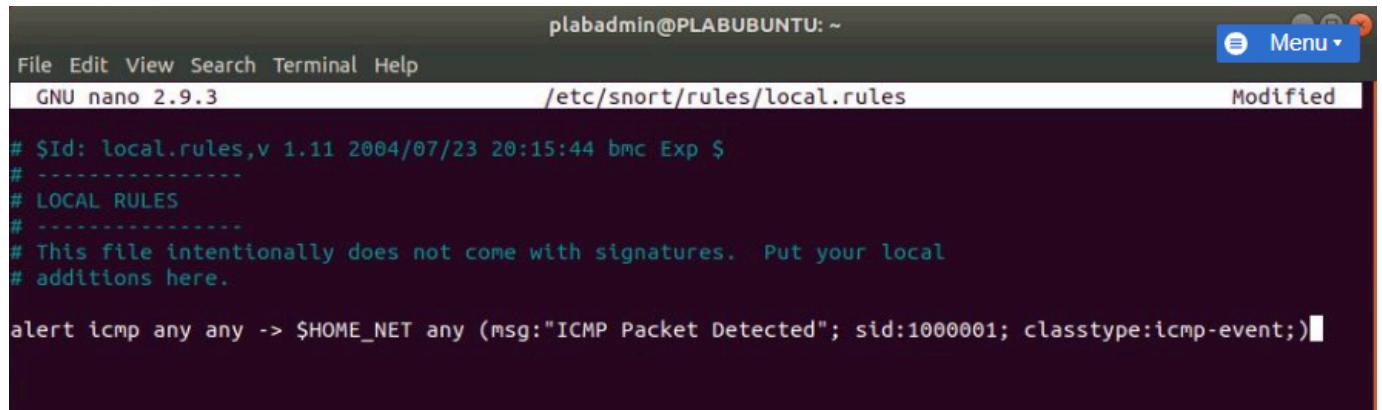


```
plabadmin@PLABUBUNTU: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/snort/rules/local.rules

$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 your local
# additions here.

[ Read 6 lines ]
^G Get Help  ^W Write Out  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text  ^T To Spell  ^L Go To Line
```

4. Create ping detection rule



```
plabadmin@PLABUBUNTU: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/snort/rules/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 your local
# additions here.

alert icmp any any -> $HOME_NET any (msg:"ICMP Packet Detected"; sid:1000001; classtype:icmp-event;)
```

```
plabadmin@PLABUBUNTU:~
```

```
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 0 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 2 809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 811 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 344 43:34444 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 ===-
```

```
o",'_~  --> 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

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

03/26-20:11:30.945560  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49873 -> 192.168.255.13:8080
03/26-20:11:31.659709  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49874 -> 192.168.255.13:8080
03/26-20:11:41.191646  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49875 -> 192.168.255.13:8080
03/26-20:11:43.451853  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49876 -> 192.168.255.13:8080
03/26-20:11:58.148806  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49878 -> 192.168.255.13:8080
03/26-20:12:46.094193  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49883 -> 192.168.255.13:8080
```

6. Ping

```
Command Prompt
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

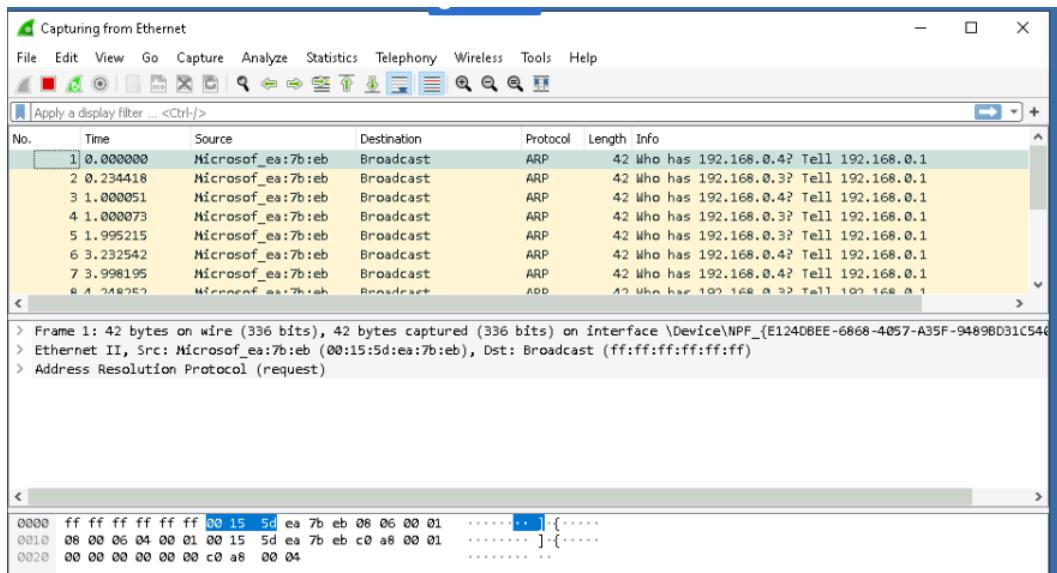
C:\Users\admin>
```

7. Detect

```
File Edit View Search Terminal Help
03/26-20:14:05.969696  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49895 -> 192.168.255.13:8080
03/26-20:14:06.131400  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:49897 -> 192.168.255.13:8080
03/26-20:14:33.450677  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:33.450677  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:33.450677  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:33.450706  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.0.2 -> 192.168.0.1
03/26-20:14:33.450706  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.2 -> 192.168.0.1
03/26-20:14:34.459787  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:34.459787  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:34.459787  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:34.459813  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.0.2 -> 192.168.0.1
03/26-20:14:34.459813  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.2 -> 192.168.0.1
03/26-20:14:35.465008  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:35.465008  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:35.465008  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:35.465034  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.0.2 -> 192.168.0.1
03/26-20:14:35.465034  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.2 -> 192.168.0.1
03/26-20:14:36.479082  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -> 192.168.0.2
03/26-20:14:36.479082  [**] [1:1000001:0] ICMP Packet Detected [**] [Classification: Generic ICMP event]
```

Task 2 - FIN Scan Detection

1. Start wireshark



2. Zenmap

The screenshot shows the Zenmap interface. At the top, there's a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu is a toolbar with 'Target' set to '192.168.0.2', 'Profile' dropdown, and 'Scan' and 'Cancel' buttons. A command line input field contains 'nmap -T4 -A -v 192.168.0.2 -sF'. The main window has tabs for 'Hosts' (selected), 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab displays the following log:

```
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

The screenshot shows the Wireshark interface capturing traffic from the Ethernet interface. The packet list pane shows several TCP retransmissions between 192.168.0.2 and 192.168.0.1. A detailed view of a specific connection is expanded, showing the Transmission Control Protocol (TCP) header fields. The 'Flags' section is highlighted, showing the binary representation of the flags and their meanings. The bottom status bar indicates a live capture is in progress.

Transmission Control Protocol, Src Port: 8080, Dst Port: 50160, Seq: 1, Ack: 1, Len: 0

Source Port: 8080
Destination Port: 50160
[Stream index: 1059]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2560723530
[Next sequence number: 2 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 3053360528
0101 = Header Length: 20 bytes (5)

Flags: 0x011 (FIN, ACK)

000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
....0.. = ECN-Echo: Not set
....0.... = Urgent: Not set
....1.... = Acknowledgment: Set
....0... = Push: Not set
....0.. = Reset: Not set
....0.. = Syn: Not set
....1 = Fin: Set
[TCP Flags:A...F]
Window size value: 501

4. Edit snort rules again

The screenshot shows a terminal window on a BUBUNTU desktop environment. The user is editing the file /etc/snort/rules/local.rules using the nano text editor. The terminal window title is "Terminal". The file content includes a header and two specific alert 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 your local
# additions here.

alert icmp any any -> $HOME_NET any (msg:"ICMP Packet Detected"; sid:1000001; classtype:icmp-event;)
alert tcp any any -> $HOME_NET any (msg:"FIN Scan Detected"; flags:AF; sid:1000002;)
```

```
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

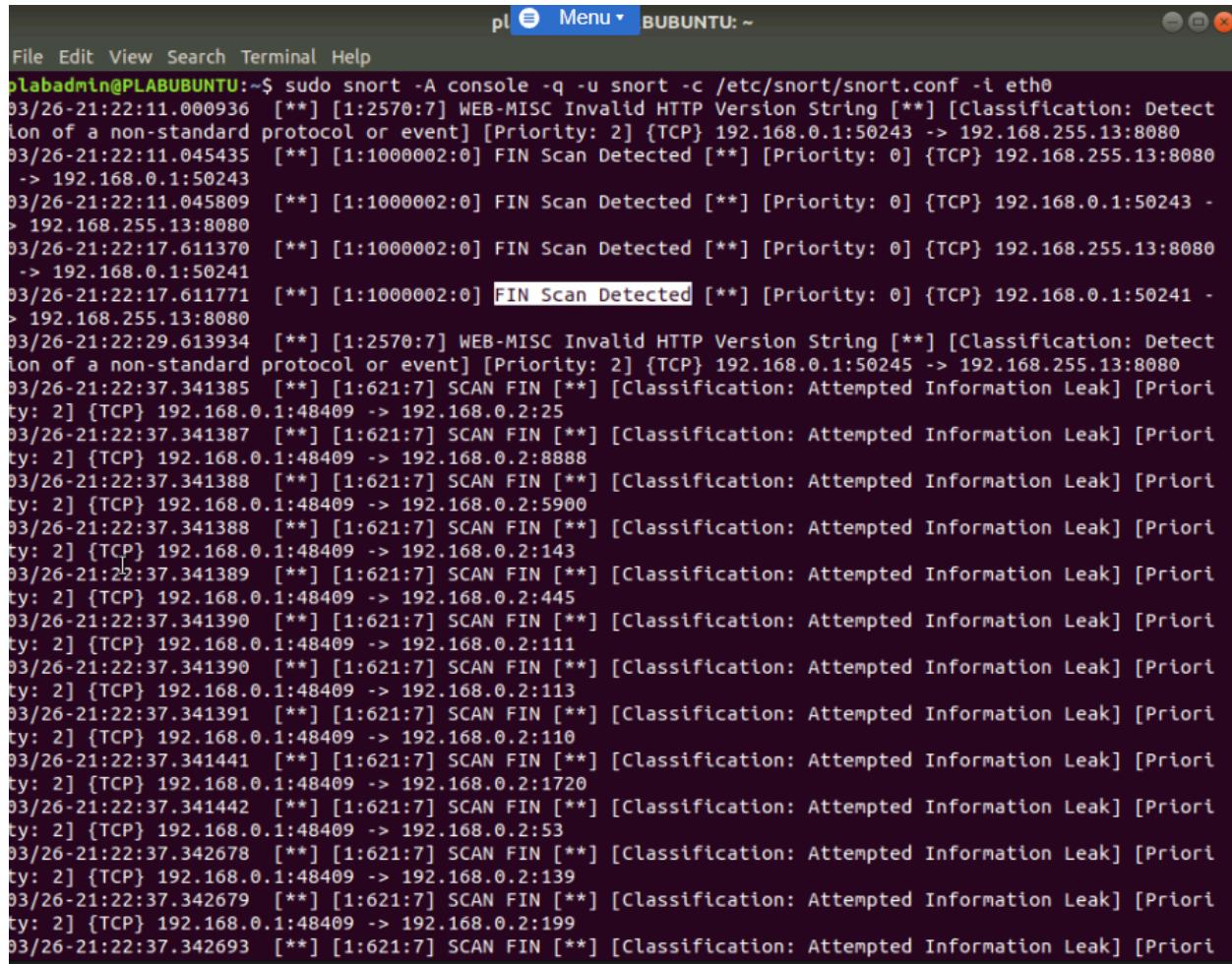
| Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
| Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
| Preprocessor Object: SF_SDF Version 1.1 <Build 1>
| Preprocessor Object: SF_POP Version 1.0 <Build 1>
| Preprocessor Object: SF_SSH Version 1.1 <Build 3>
| Preprocessor Object: SF_SSLPP 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

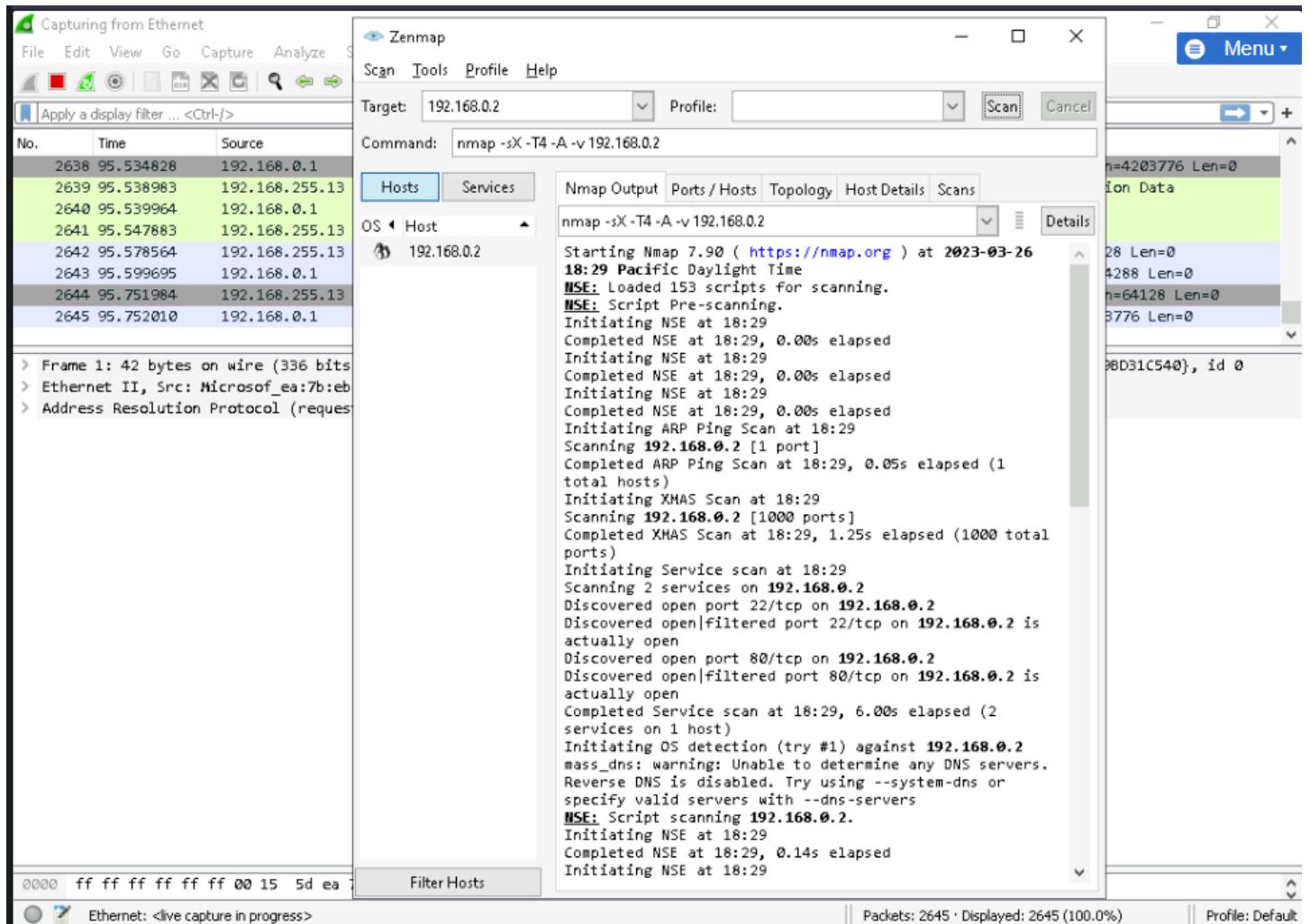


The screenshot shows a terminal window titled 'BUBUNTU: ~' with the command 'sudo snort -A console -q -u snort -c /etc/snort/snort.conf -i eth0' running. The log output displays numerous alerts from March 26, 2021, at various times between 22:11:00 and 22:37:34. The alerts are primarily related to 'FIN Scan Detected' and 'SCAN FIN' events, often categorized as 'Attempted Information Leak' with priority 0. The source IP for these scans is 192.168.0.1:50241, and the destination IP is 192.168.0.2. The logs also mention 'WEB-MISC Invalid HTTP Version String' and 'Detection of a non-standard protocol or event'.

```
pl  Menu  BUBUNTU: ~
File Edit View Search Terminal Help
plabadmin@PLABUBUNTU:~$ sudo snort -A console -q -u snort -c /etc/snort/snort.conf -i eth0
03/26-21:22:11.000936  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:50243 -> 192.168.255.13:8080
03/26-21:22:11.045435  [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.255.13:8080 -> 192.168.0.1:50243
03/26-21:22:11.045809  [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:50243 -> 192.168.255.13:8080
03/26-21:22:17.611370  [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.255.13:8080 -> 192.168.0.1:50241
03/26-21:22:17.611771  [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:50241 -> 192.168.255.13:8080
03/26-21:22:29.613934  [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:50245 -> 192.168.255.13:8080
03/26-21:22:37.341385  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:25
03/26-21:22:37.341387  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:8888
03/26-21:22:37.341388  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:5900
03/26-21:22:37.341388  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:143
03/26-21:22:37.341389  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:445
03/26-21:22:37.341390  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:111
03/26-21:22:37.341390  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:113
03/26-21:22:37.341391  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:110
03/26-21:22:37.341441  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:1720
03/26-21:22:37.341442  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:53
03/26-21:22:37.342678  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:139
03/26-21:22:37.342679  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.1:48409 -> 192.168.0.2:199
03/26-21:22:37.342693  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority:
```

Task 3 - XMAS Scan Detection

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



2. Identify flags in wireshark and make new snort rule

The screenshot shows a Wireshark capture window for interface "Ethernet". A single packet is selected, with its details pane expanded. The selected packet is a TCP segment with Source Port 42362 and Destination Port 22. The Flags section shows the binary value 0x02b, which is expanded to show the individual flags: Reserved (Not set), Nonce (Not set), Congestion Window Reduced (CWR) (Not set), ECN-Echo (Not set), Urgent (Set), Acknowledgment (Not set), Push (Set), and Reset (Not set).

```

pl@BUBUNTU:~$ nano /etc/snort/rules/local.rules
GNU nano 2.9.3
# $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 your local
# additions here.

alert icmp any any -> $HOME_NET any (msg:"ICMP Packet Detected"; sid:1000001; classtype:icmp-event;)
alert tcp any any -> $HOME_NET any (msg:"FIN Scan Detected"; flags:AF; sid:1000002;)
alert tcp any any -> $HOME_NET any (msg:"XMAS Scan Detected"; flags:FPU; sid:1000003;)

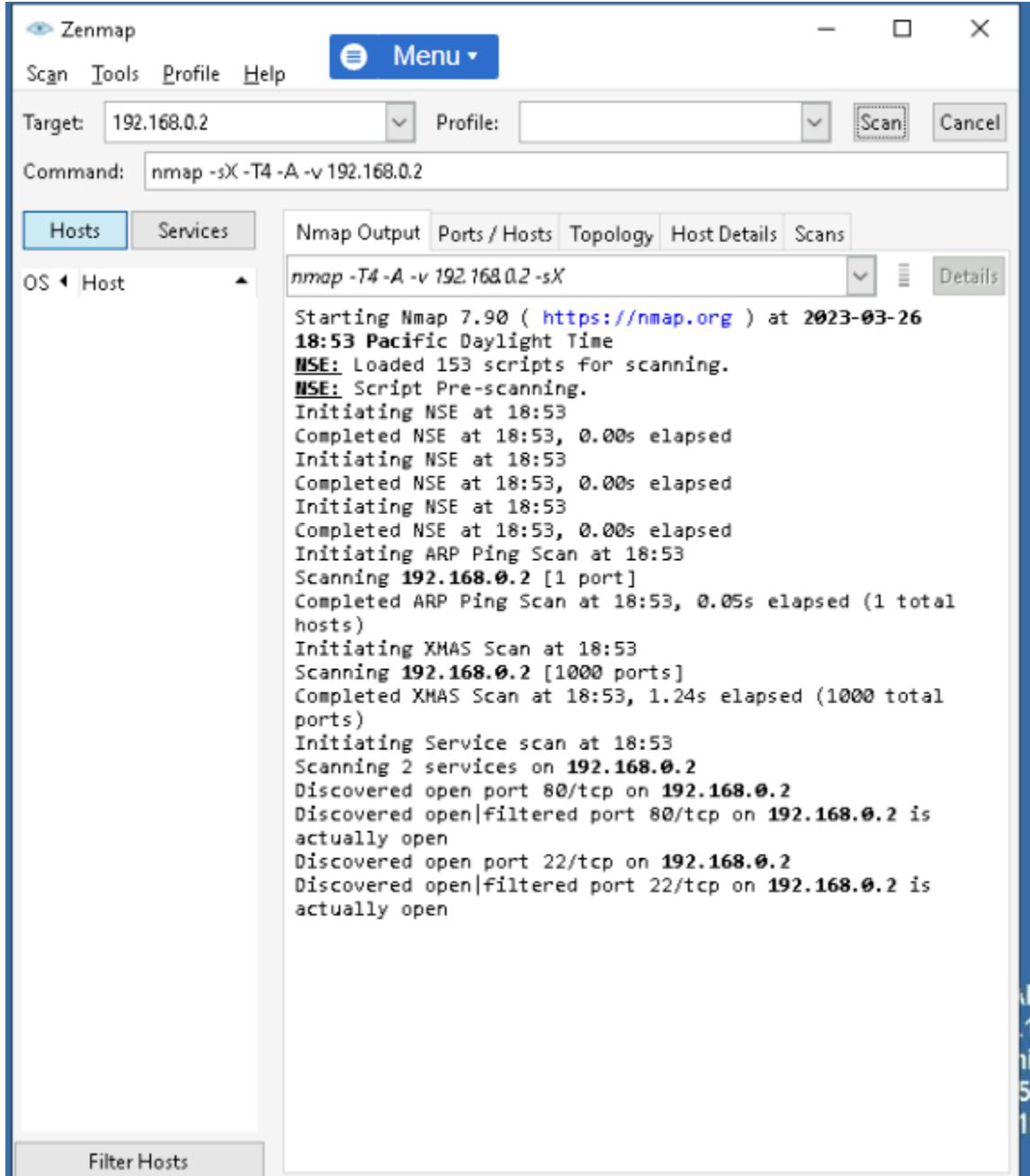
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

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

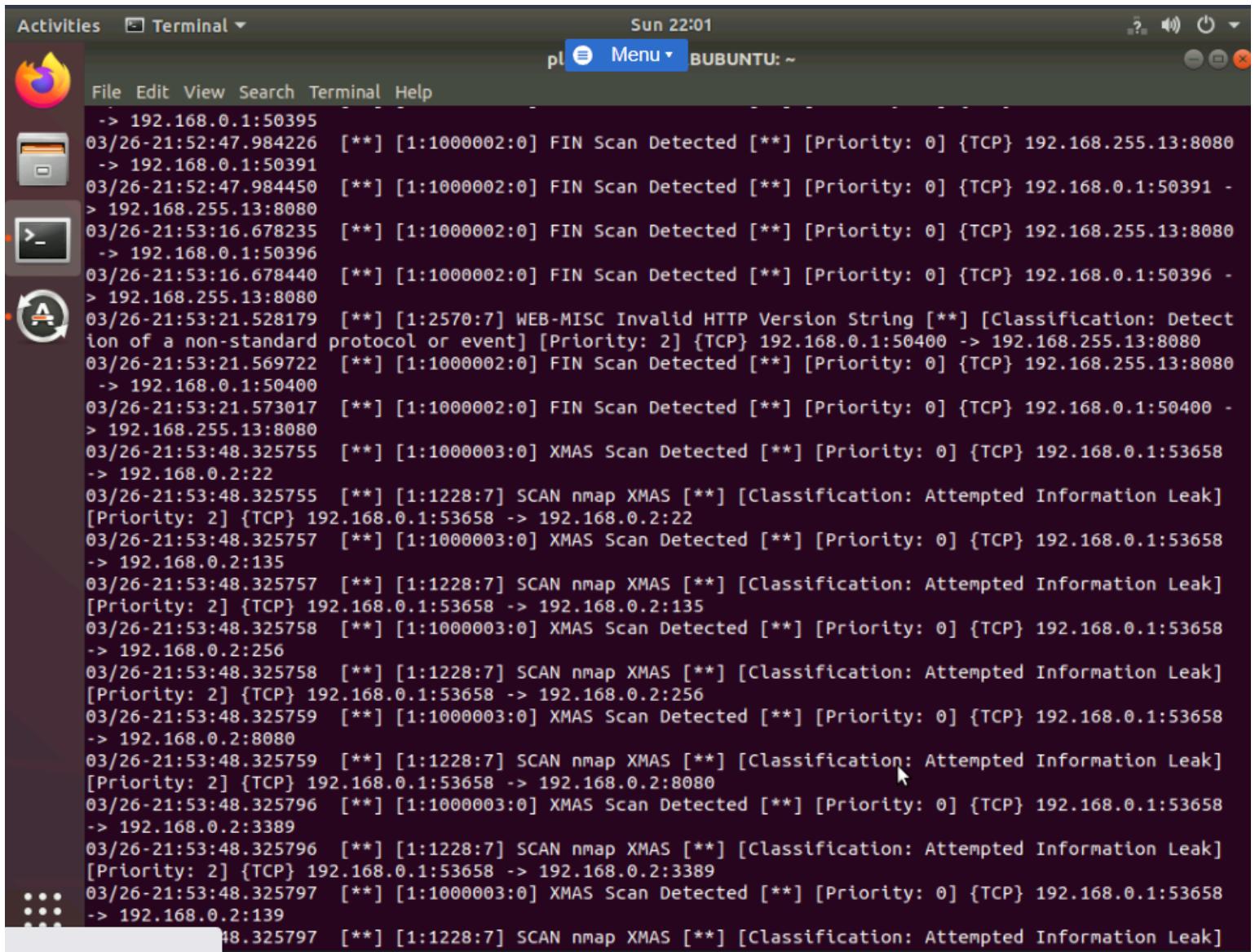
3. Start Snort

```
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



A screenshot of a Linux desktop environment, specifically BUBUNTU, showing a terminal window. The terminal window title is "Terminal". The window contains a log of network traffic alerts. The log shows multiple FIN Scan Detected and XMAS Scan Detected events from various IP addresses (e.g., 192.168.0.1, 192.168.255.13) to port 8080, and one WEB-MISC Invalid HTTP Version String event. The events are timestamped from 03/26/21 at 21:52:47 to 03/26/21 at 21:53:48. The log entries include details like classification (Attempted Information Leak for XMAS scans), priority (0 or 2), and protocol (TCP). The terminal window is part of a desktop interface with other icons visible in the background.

```
Sun 22:01
pl Menu ~ BUBUNTU: ~

File Edit View Search Terminal Help
-> 192.168.0.1:50395
03/26-21:52:47.984226 [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.255.13:8080
-> 192.168.0.1:50391
03/26-21:52:47.984450 [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:50391 -
> 192.168.255.13:8080
03/26-21:53:16.678235 [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.255.13:8080
-> 192.168.0.1:50396
03/26-21:53:16.678440 [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:50396 -
> 192.168.255.13:8080
03/26-21:53:21.528179 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP} 192.168.0.1:50400 -> 192.168.255.13:8080
03/26-21:53:21.569722 [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.255.13:8080
-> 192.168.0.1:50400
03/26-21:53:21.573017 [**] [1:1000002:0] FIN Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:50400 -
> 192.168.255.13:8080
03/26-21:53:48.325755 [**] [1:1000003:0] XMAS Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:53658
-> 192.168.0.2:22
03/26-21:53:48.325755 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.0.1:53658 -> 192.168.0.2:22
03/26-21:53:48.325757 [**] [1:1000003:0] XMAS Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:53658
-> 192.168.0.2:135
03/26-21:53:48.325757 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.0.1:53658 -> 192.168.0.2:135
03/26-21:53:48.325758 [**] [1:1000003:0] XMAS Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:53658
-> 192.168.0.2:256
03/26-21:53:48.325758 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.0.1:53658 -> 192.168.0.2:256
03/26-21:53:48.325759 [**] [1:1000003:0] XMAS Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:53658
-> 192.168.0.2:8080
03/26-21:53:48.325759 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.0.1:53658 -> 192.168.0.2:8080
03/26-21:53:48.325796 [**] [1:1000003:0] XMAS Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:53658
-> 192.168.0.2:3389
03/26-21:53:48.325796 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.0.1:53658 -> 192.168.0.2:3389
03/26-21:53:48.325797 [**] [1:1000003:0] XMAS Scan Detected [**] [Priority: 0] {TCP} 192.168.0.1:53658
-> 192.168.0.2:139
48.325797 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak]
```