Cyber Security Incident Response Report

“Investigating of PCAP File using SNORT”

1. Introduction

In this report, we investigate network traffic captured in a PCAP file named "mx-1" using Snort, an open-source network intrusion detection system (NIDS). The PCAP file was obtained from the TryHackMe SNORT room, Task 8. The analysis aims to identify potential threats, anomalies, or malicious activities within the captured traffic. The primary objective is to evaluate the security posture of the network and provide actionable recommendations based on the findings.

The analysis was conducted on Ubuntu 20.04.2 LTS, a popular and secure Linux-based operating system known for its stability and reliability, particularly in the fields of cybersecurity and network analysis.

Snort is a widely-used NIDS that monitors network traffic in real-time, identifying potential threats, anomalies, or malicious activities. It operates by inspecting packets against predefined rule sets, allowing analysts to detect suspicious behavior and take appropriate action. The primary objective of this report is to evaluate the security posture of the network captured in the PCAP file and provide actionable recommendations based on the findings.

2. Methodology

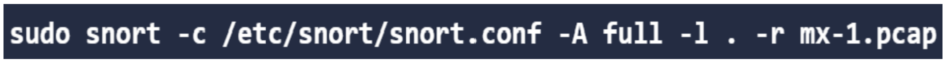
The analysis was conducted on Ubuntu using SNORT. The following steps outline the process:

1. **Environment Setup**:

    - **Operating System**: Ubuntu 20.04.2 LTS
    - **Snort Version**: 2.9.7.0 GRE (Build 149)
    - **The default Snort configuration file** located at “`/etc/snort/snort.conf`” was utilized without any modifications.
    - **Default community rules** were used for detecting potential threats.

2. PCAP File Analysis:

- The PCAP file "mx-1.pcap" was analyzed with the following command:



```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-1.pcap
```

- Snort's output included an `alert` file, summarizing detected threats, and a `log` file with packet details.
- The `alert` file was used to identify key threats, while the `log` file was reviewed for detailed packet information.

3. Incident Detection:

- The analysis focused on identifying ICMP-related threats, protocol anomalies, and possible reconnaissance behavior.

---

3. Findings

The following threats and anomalies were detected using the default Snort ruleset:

Incident 1: ICMP Ping Behavior

- **Alert Type**: ICMP Echo Requests and Replies
- **Source IP**: 192.168.175.129
- **Destination IPs**:
  - 142.250.187.110
  - 172.67.27.10
- **Protocol**: ICMP (Internet Control Message Protocol)
- **Summary**: The captured traffic showed multiple ICMP Echo Requests from `192.168.175.129` to the destination IPs. These requests were followed by ICMP Echo Replies, indicating successful communication exchanges.
- **Significance**: Such ICMP behavior is indicative of network reconnaissance, potentially a **ping sweep** to map active hosts within a network.
- **Recommendation**: Implement IP filtering for suspicious IPs, limit ICMP traffic where necessary, and monitor for unusual ICMP activity.

Incident 2: Pattern of ICMP Traffic

- **Alert Type**: Repeated ICMP Sequences
- **Source IP**: 192.168.175.129
- **Destination IPs**:
  - 142.250.187.110
  - 172.67.27.10
- **Protocol**: ICMP
- **Summary**: A pattern of sequential ICMP requests and responses was detected, showing identical payload sizes and regular timing intervals. This type of traffic is often used for network discovery and mapping.
- **Significance**: The observed traffic suggests automated tools may have been used for reconnaissance.
- **Recommendation**: Disable unnecessary ICMP responses, and use Snort custom rules to detect more sophisticated ICMP-based reconnaissance.

---

4. Conclusion

The investigation of the captured network traffic using Snort's default configuration highlighted several key reconnaissance patterns involving ICMP communication. The behavior suggests potential attempts to identify active hosts within the network, which could serve as a precursor to more targeted attacks.

While the incidents detected are of low severity (Priority 3), they are crucial in understanding the initial steps of an attacker’s reconnaissance phase. Strengthening the network’s defenses with stricter ICMP filtering and enhanced monitoring can mitigate these types of reconnaissance activities.

Recommendations:

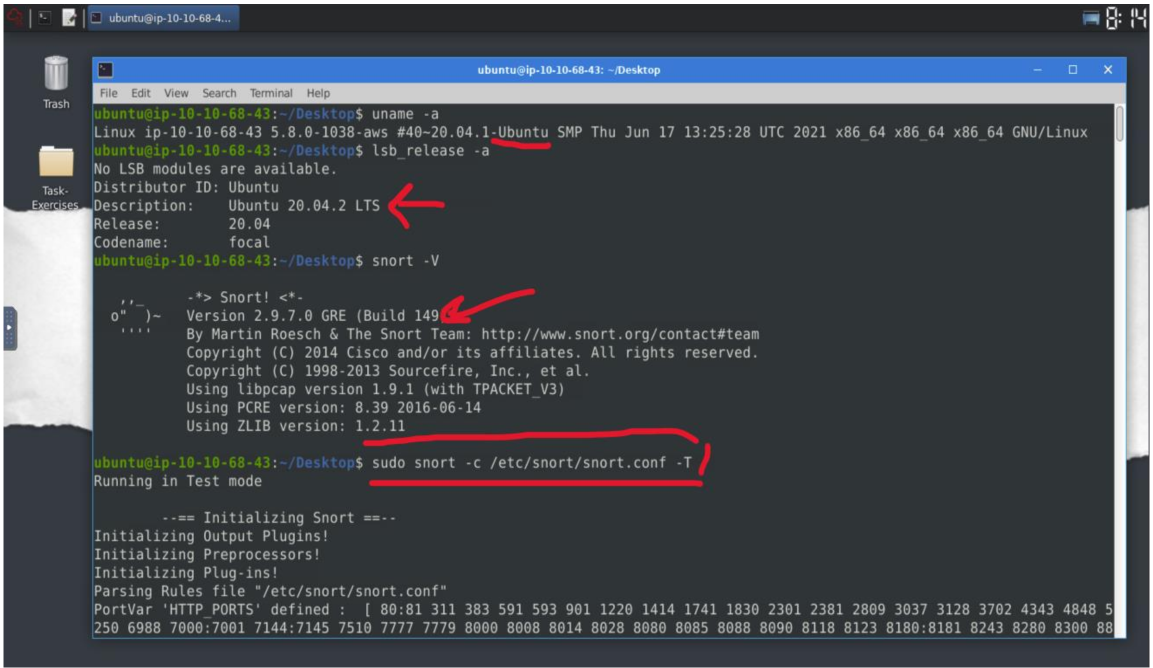
- **Implement IP Filtering**: Block or monitor repeated ICMP traffic from unknown sources.
- **Limit ICMP Traffic**: Restrict ICMP communication to necessary systems only.
- **Enhanced Monitoring**: Use advanced Snort rules tailored to your network to detect more complex attack patterns.

- **Regular Rule Updates**: Keep Snort's rule set updated to ensure detection of the latest threats.

---

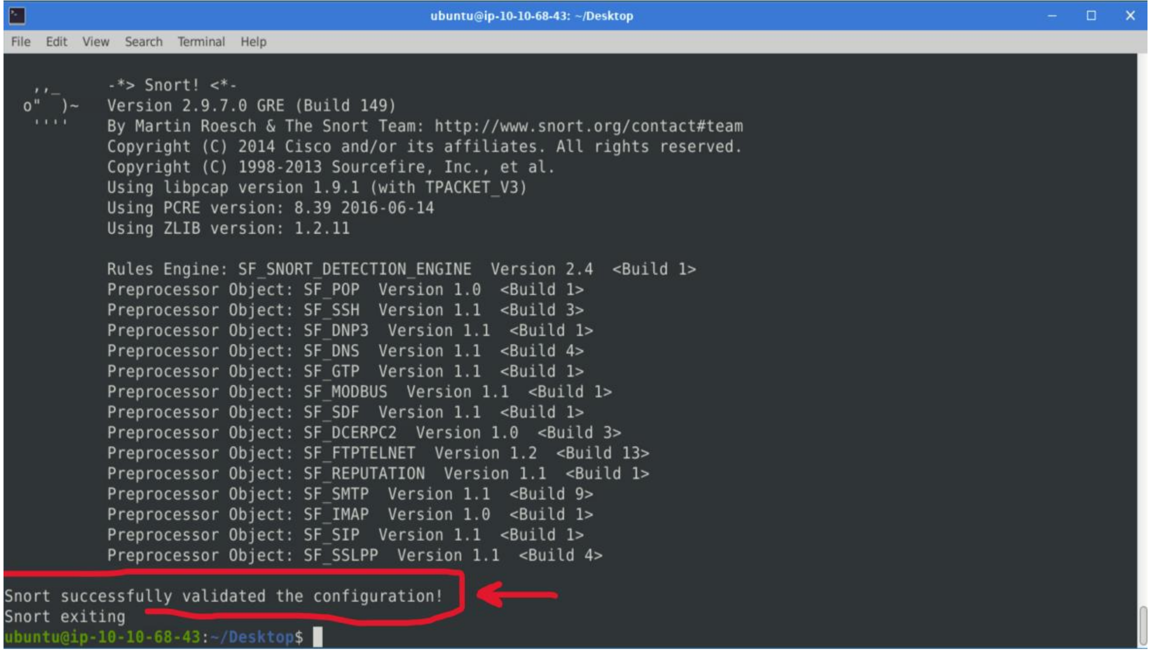
5. Screenshots and Logs

- **For Environment Setup:**



ubuntu@ip-10-10-68-4...
Trash
Task-Exercises
ubuntu@ip-10-10-68-43: ~/Desktop
File Edit View Search Terminal Help

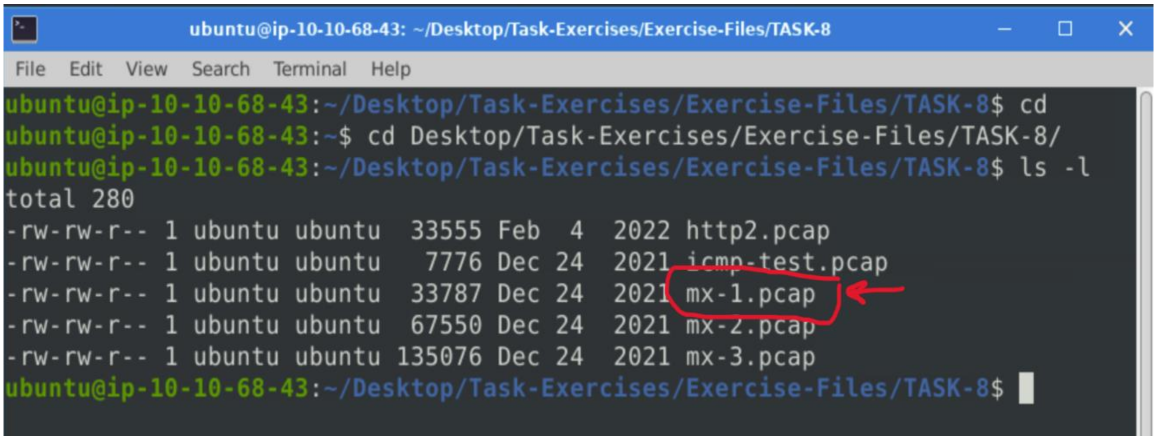
```
ubuntu@ip-10-10-68-43:~/Desktop$ uname -a
Linux ip-10-10-68-43 5.8.0-1038-aws #40~20.04.1-Ubuntu SMP Thu Jun 17 13:25:28 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
ubuntu@ip-10-10-68-43:~/Desktop$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.2 LTS
Release:        20.04
Codename:       focal
ubuntu@ip-10-10-68-43:~/Desktop$ snort -V

   ,,_     -*> 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 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

ubuntu@ip-10-10-68-43:~/Desktop$ sudo snort -c /etc/snort/snort.conf -T
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 5
250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 88
```



ubuntu@ip-10-10-68-43: ~/Desktop
File Edit View Search Terminal Help

```
   ,,_     -*> 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 1.9.1 (with TPACKET_V3)
           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_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
ubuntu@ip-10-10-68-43:~/Desktop$
```

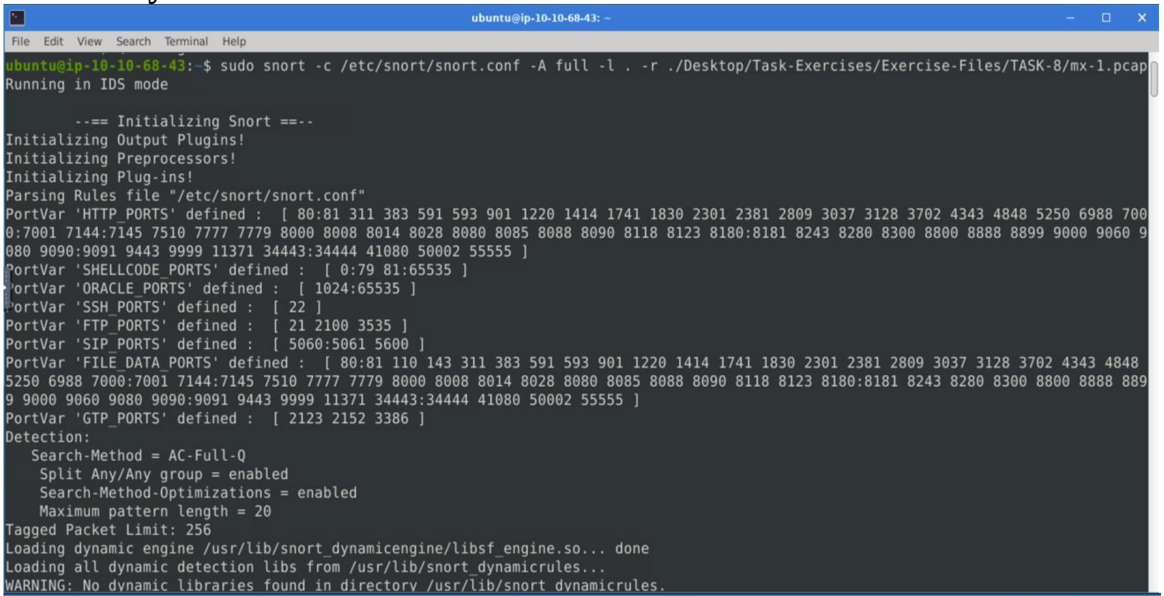
- **For PCAP Files:**



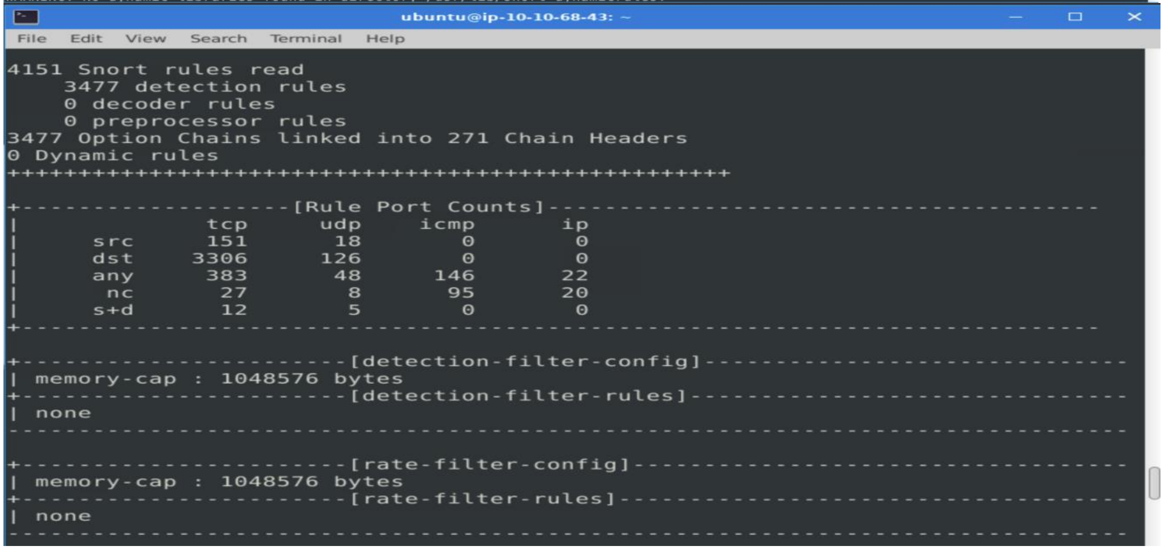
ubuntu@ip-10-10-68-43: ~/Desktop/Task-Exercises/Exercise-Files/TASK-8
File Edit View Search Terminal Help

```
ubuntu@ip-10-10-68-43:~/Desktop/Task-Exercises/Exercise-Files/TASK-8$ cd
ubuntu@ip-10-10-68-43:~$ cd Desktop/Task-Exercises/Exercise-Files/TASK-8/
ubuntu@ip-10-10-68-43:~/Desktop/Task-Exercises/Exercise-Files/TASK-8$ ls -l
total 280
-rw-rw-r-- 1 ubuntu ubuntu  33555 Feb  4  2022 http2.pcap
-rw-rw-r-- 1 ubuntu ubuntu   7776 Dec 24  2021 icmp-test.pcap
-rw-rw-r-- 1 ubuntu ubuntu  33787 Dec 24  2021 mx-1.pcap
-rw-rw-r-- 1 ubuntu ubuntu  67550 Dec 24  2021 mx-2.pcap
-rw-rw-r-- 1 ubuntu ubuntu 135076 Dec 24  2021 mx-3.pcap
ubuntu@ip-10-10-68-43:~/Desktop/Task-Exercises/Exercise-Files/TASK-8$ 
```

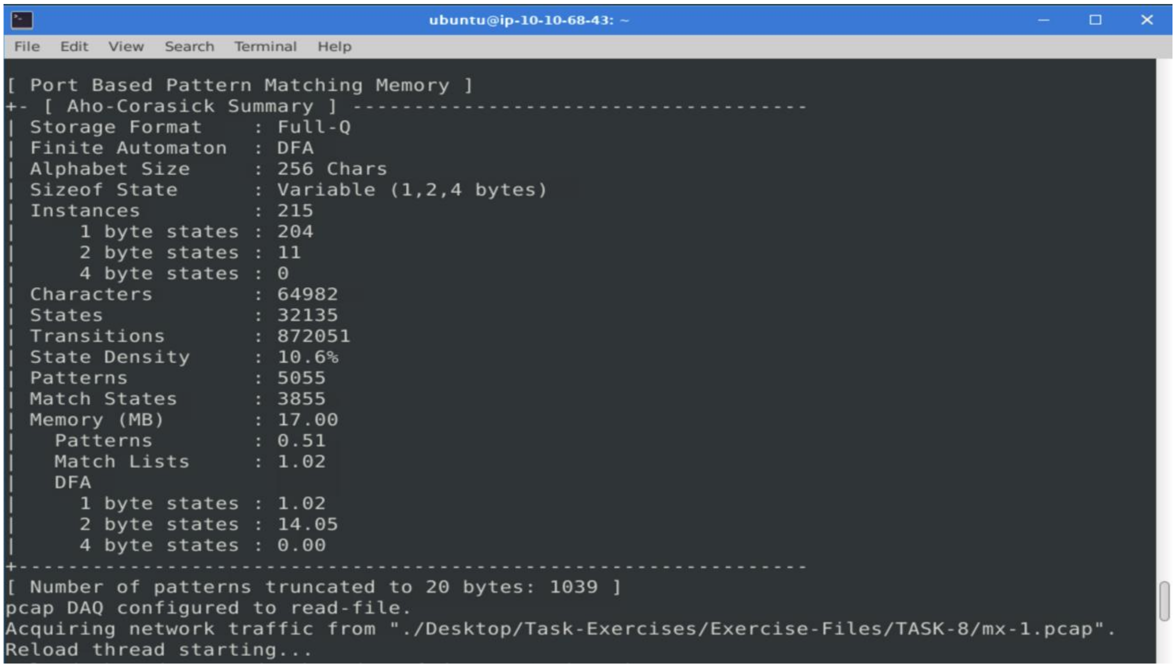
- **For Analysis of PCAP File:**



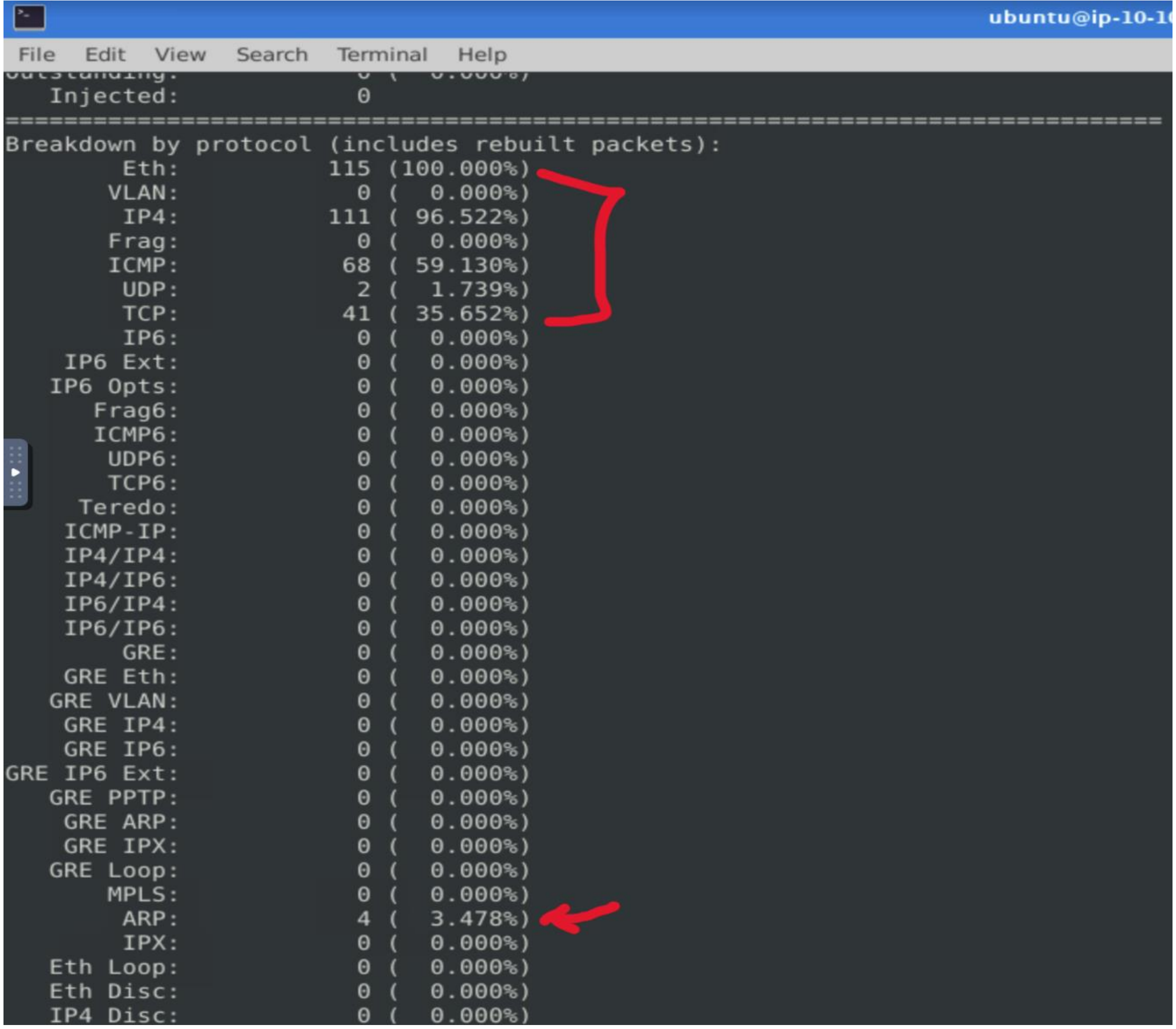
```
ubuntu@ip-10-10-68-43:~$ sudo snort -c /etc/snort/snort.conf -A full -l . -r ./Desktop/Task-Exercises/Exercise-Files/TASK-8/mx-1.pcap
Running in IDS mode

        --== 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 700
0:7001 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 9
080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
ortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
ortVar '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 889
9 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
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
```



```
4151 Snort rules read
    3477 detection rules
    0 decoder rules
    0 preprocessor rules
3477 Option Chains linked into 271 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     151      18       0       0
|     dst    3306     126       0       0
|     any     383      48     146      22
|      nc      27       8      95      20
|     s+d      12       5       0       0
+----------------------------------------------------------------------------

+-----------------------[detection-filter-config]------------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]-------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[rate-filter-config]-----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]------------------------------------
| none
-------------------------------------------------------------------------------
```

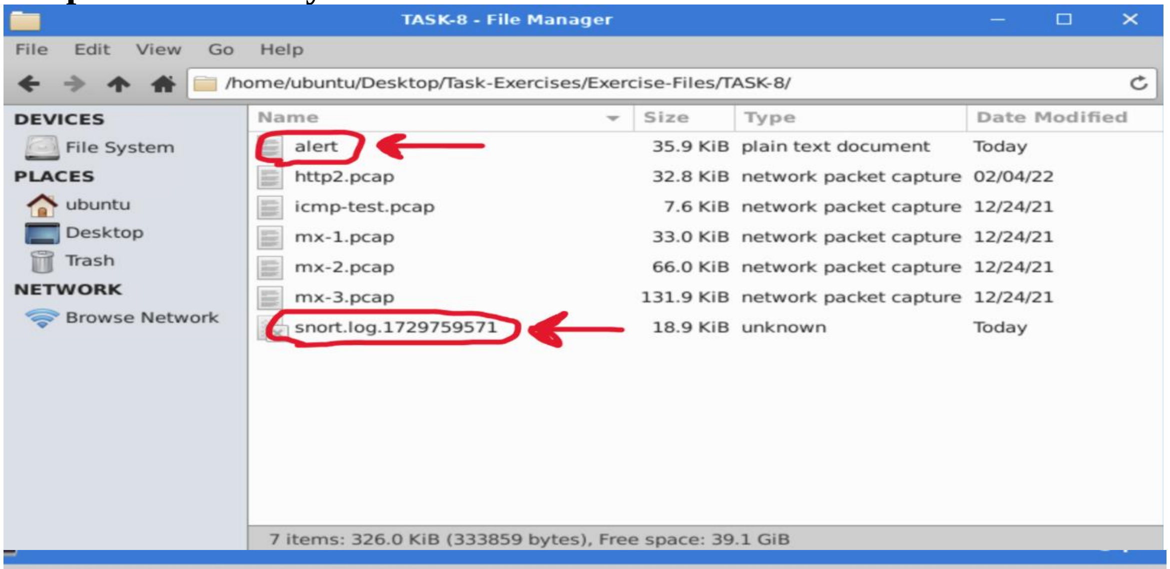


```
[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64982
| States            : 32135
| Transitions       : 872051
| State Density     : 10.6%
| Patterns          : 5055
| Match States      : 3855
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   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 ]
pcap DAQ configured to read-file.
Acquiring network traffic from "./Desktop/Task-Exercises/Exercise-Files/TASK-8/mx-1.pcap".
Reload thread starting...
```



```
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          115 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          111 ( 96.522%)
       Frag:            0 (  0.000%)
       ICMP:           68 ( 59.130%)
        UDP:            2 (  1.739%)
        TCP:           41 ( 35.652%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            4 (  3.478%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
```

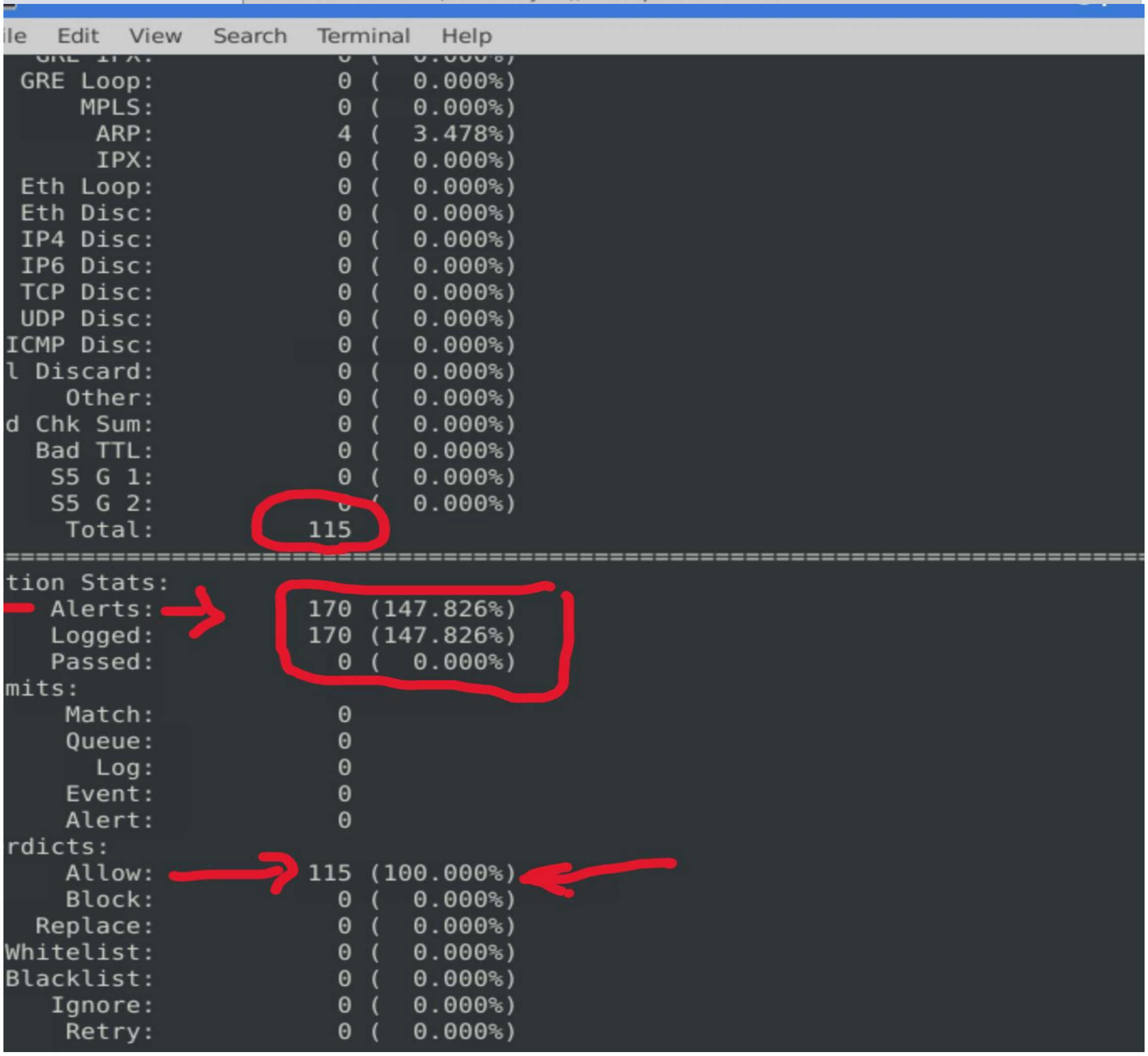
- **Output of the Analysis:**



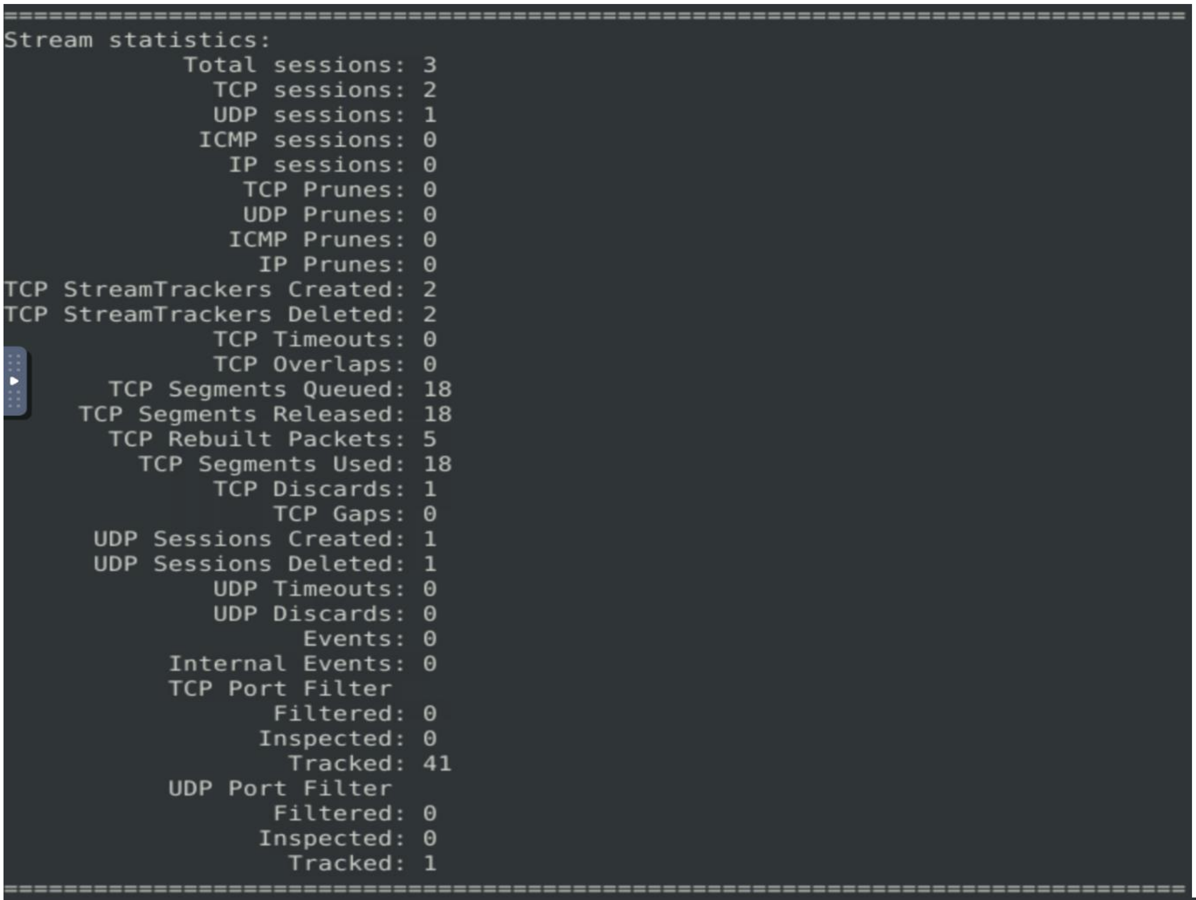
/home/ubuntu/Desktop/Task-Exercises/Exercise-Files/TASK-8/

Name	Size	Type	Date Modified
alert	35.9 KiB	plain text document	Today
http2.pcap	32.8 KiB	network packet capture	02/04/22
icmp-test.pcap	7.6 KiB	network packet capture	12/24/21
mx-1.pcap	33.0 KiB	network packet capture	12/24/21
mx-2.pcap	66.0 KiB	network packet capture	12/24/21
mx-3.pcap	131.9 KiB	network packet capture	12/24/21
snort.log.1729759571	18.9 KiB	unknown	Today

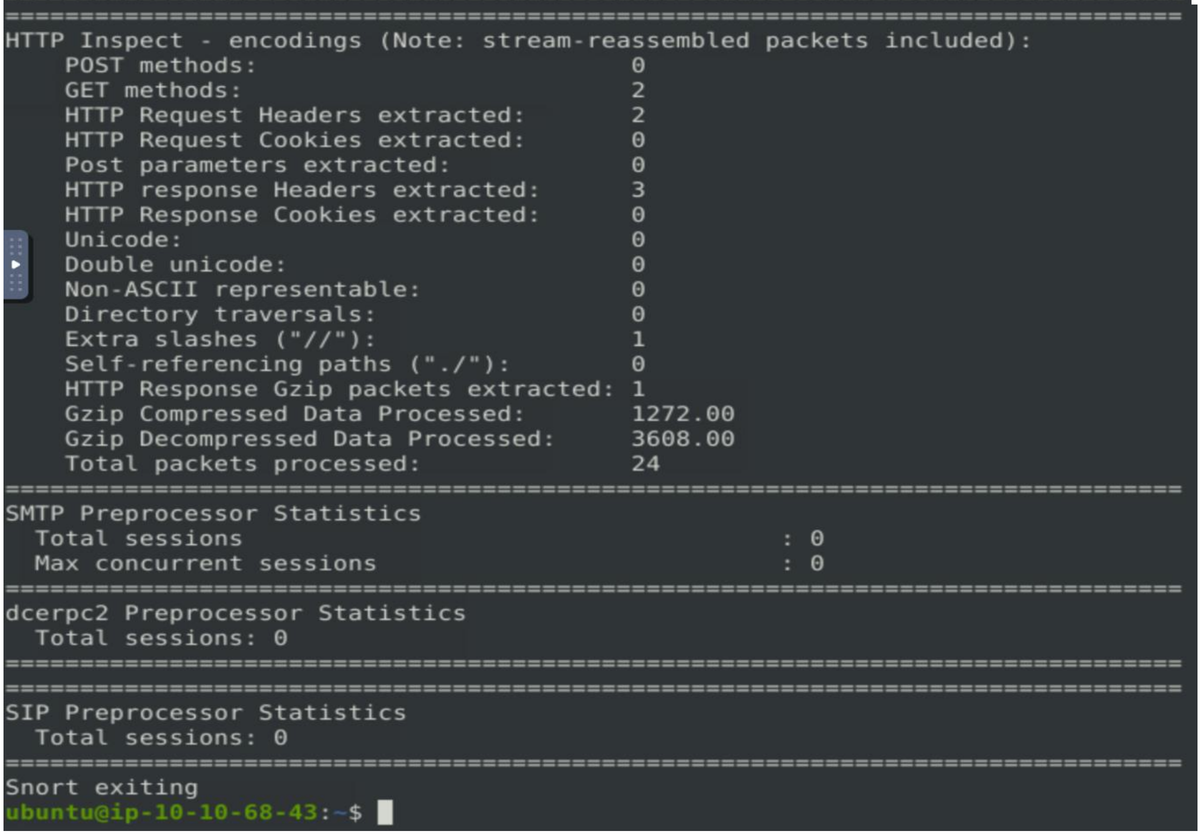
7 items: 326.0 KiB (333859 bytes), Free space: 39.1 GiB



```
 GRE Loop:          0 (  0.000%)
     MPLS:          0 (  0.000%)
      ARP:          4 (  3.478%)
      IPX:          0 (  0.000%)
 Eth Loop:          0 (  0.000%)
 Eth Disc:          0 (  0.000%)
 IP4 Disc:          0 (  0.000%)
 IP6 Disc:          0 (  0.000%)
 TCP Disc:          0 (  0.000%)
 UDP Disc:          0 (  0.000%)
ICMP Disc:          0 (  0.000%)
l Discard:          0 (  0.000%)
    Other:          0 (  0.000%)
d Chk Sum:          0 (  0.000%)
  Bad TTL:          0 (  0.000%)
   S5 G 1:          0 (  0.000%)
   S5 G 2:          0 (  0.000%)
    Total:        115
===========================================================================
tion Stats:
   Alerts:        170 (147.826%)
   Logged:        170 (147.826%)
   Passed:          0 (  0.000%)
mits:
    Match:          0
    Queue:          0
      Log:          0
    Event:          0
    Alert:          0
rdicts:
    Allow:        115 (100.000%)
    Block:          0 (  0.000%)
  Replace:          0 (  0.000%)
Whitelist:          0 (  0.000%)
Blacklist:          0 (  0.000%)
   Ignore:          0 (  0.000%)
    Retry:          0 (  0.000%)
```

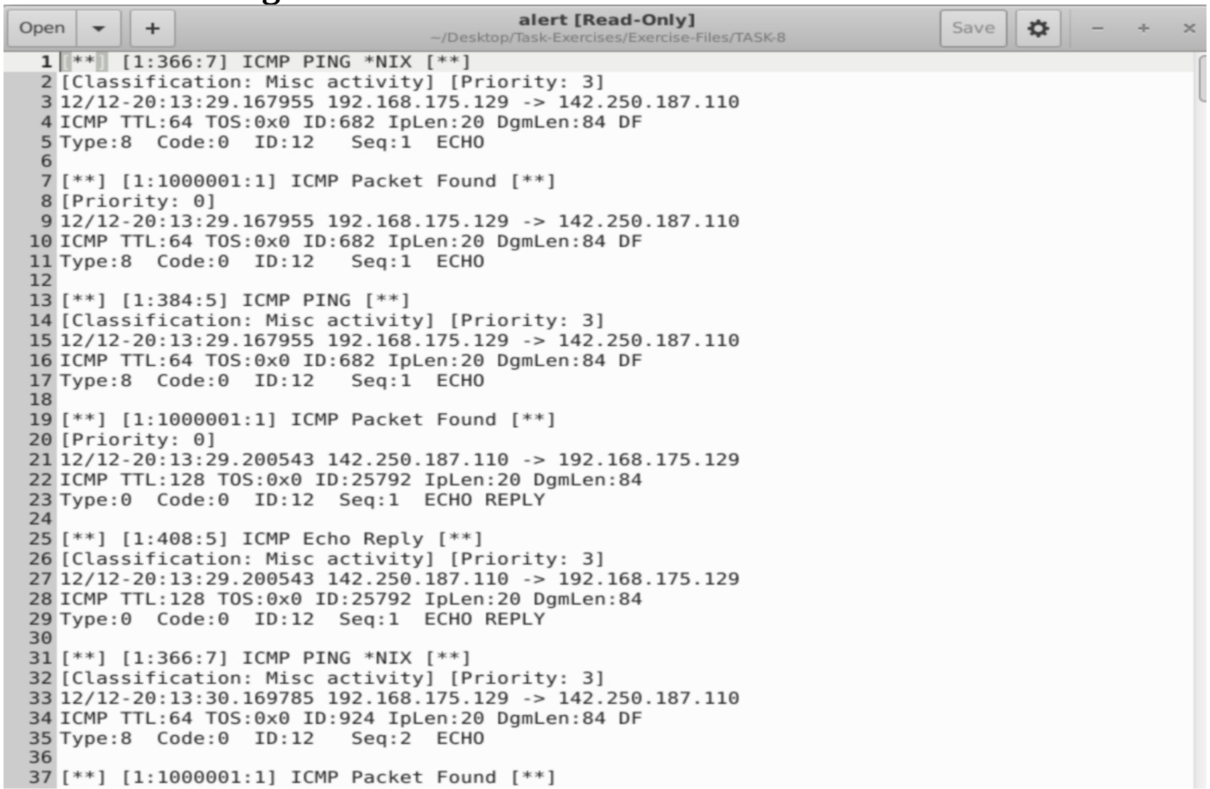


```
===============================================================================
Stream statistics:
            Total sessions: 3
              TCP sessions: 2
              UDP sessions: 1
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
                 IP Prunes: 0
TCP StreamTrackers Created: 2
TCP StreamTrackers Deleted: 2
              TCP Timeouts: 0
              TCP Overlaps: 0
       TCP Segments Queued: 18
     TCP Segments Released: 18
       TCP Rebuilt Packets: 5
         TCP Segments Used: 18
              TCP Discards: 1
                  TCP Gaps: 0
      UDP Sessions Created: 1
      UDP Sessions Deleted: 1
              UDP Timeouts: 0
              UDP Discards: 0
                    Events: 0
           Internal Events: 0
           TCP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 41
           UDP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 1
===============================================================================
```

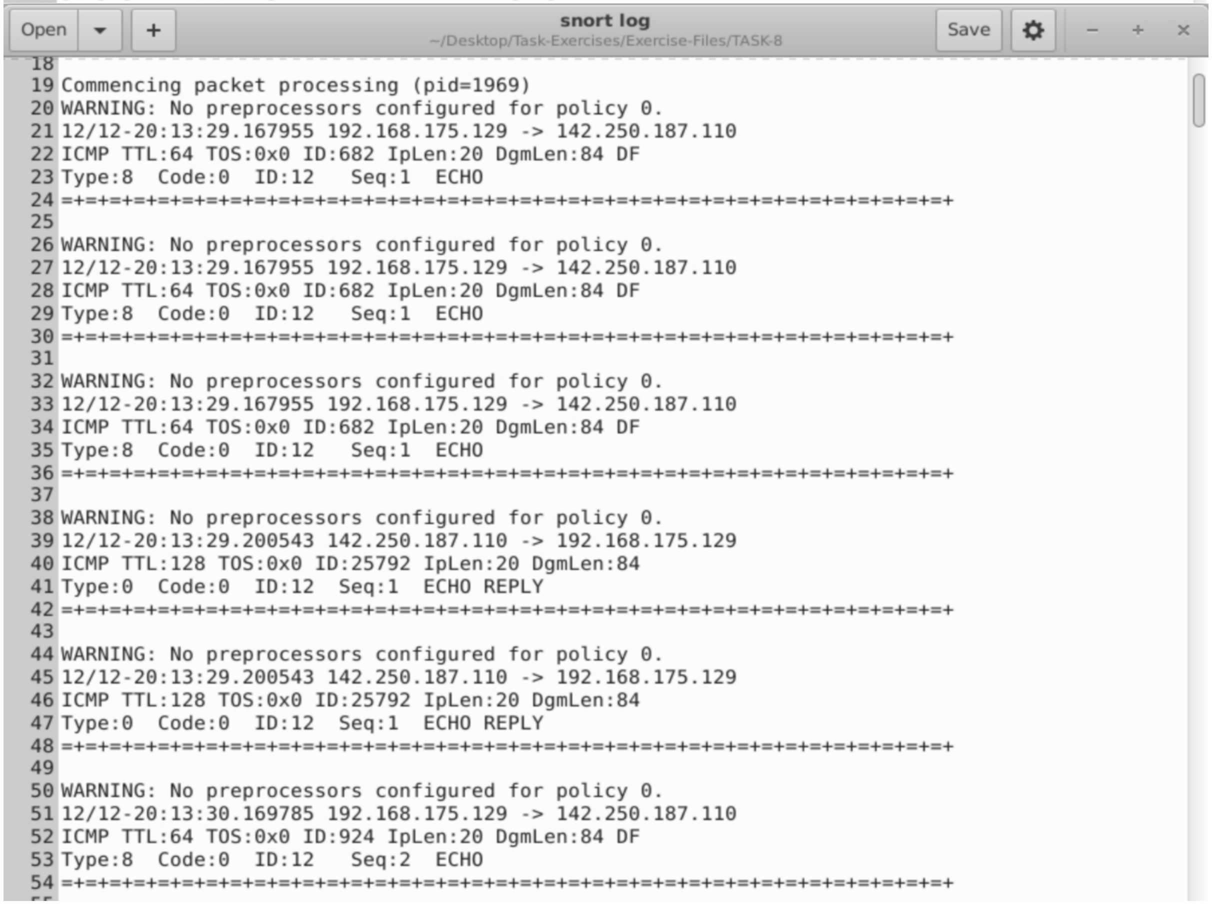


```
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         0
    GET methods:                          2
    HTTP Request Headers extracted:       2
    HTTP Request Cookies extracted:       0
    Post parameters extracted:            0
    HTTP response Headers extracted:      3
    HTTP Response Cookies extracted:      0
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 1
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 1
    Gzip Compressed Data Processed:       1272.00
    Gzip Decompressed Data Processed:     3608.00
    Total packets processed:              24
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Snort exiting
ubuntu@ip-10-10-68-43:~$ 
```

- **For Alerts & Logs:**



```
[**] [1:366:7] ICMP PING *NIX [**]
[Classification: Misc activity] [Priority: 3]
12/12-20:13:29.167955 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:682 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:1  ECHO

[**] [1:1000001:1] ICMP Packet Found [**]
[Priority: 0]
12/12-20:13:29.167955 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:682 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:1  ECHO

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
12/12-20:13:29.167955 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:682 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:1  ECHO

[**] [1:1000001:1] ICMP Packet Found [**]
[Priority: 0]
12/12-20:13:29.200543 142.250.187.110 -> 192.168.175.129
ICMP TTL:128 TOS:0x0 ID:25792 IpLen:20 DgmLen:84
Type:0  Code:0  ID:12  Seq:1  ECHO REPLY

[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
12/12-20:13:29.200543 142.250.187.110 -> 192.168.175.129
ICMP TTL:128 TOS:0x0 ID:25792 IpLen:20 DgmLen:84
Type:0  Code:0  ID:12  Seq:1  ECHO REPLY

[**] [1:366:7] ICMP PING *NIX [**]
[Classification: Misc activity] [Priority: 3]
12/12-20:13:30.169785 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:924 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:2  ECHO

[**] [1:1000001:1] ICMP Packet Found [**]
```



```
Commencing packet processing (pid=1969)
WARNING: No preprocessors configured for policy 0.
12/12-20:13:29.167955 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:682 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:1  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/12-20:13:29.167955 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:682 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:1  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/12-20:13:29.167955 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:682 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:1  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/12-20:13:29.200543 142.250.187.110 -> 192.168.175.129
ICMP TTL:128 TOS:0x0 ID:25792 IpLen:20 DgmLen:84
Type:0  Code:0  ID:12  Seq:1  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/12-20:13:29.200543 142.250.187.110 -> 192.168.175.129
ICMP TTL:128 TOS:0x0 ID:25792 IpLen:20 DgmLen:84
Type:0  Code:0  ID:12  Seq:1  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/12-20:13:30.169785 192.168.175.129 -> 142.250.187.110
ICMP TTL:64 TOS:0x0 ID:924 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12   Seq:2  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

6. References

- Snort Official Documentation: https://www.snort.org/documents
- Snort Community Rules: https://www.snort.org/downloads
- TryHackMe SNORT Room: https://tryhackme.com
- Understanding ICMP Traffic: https://www.cisco.com
- Network Security Best Practices: https://nvlpubs.nist.gov