Snort Configuration and Analysis Project Report

This report documents the steps taken to configure, run, and analyze Snort IDS/IPS on a network environment,
along with screenshots for validation of each step. The primary objective was to configure Snort for intrusion detection, log
alerts, and analyze malicious activity, specifically identifying a malicious User-Agent string.

1. Environment Setup

The Snort IDS/IPS environment was set up with the following topology:

- Desktop: 192.168.6.1

- Firewall: External (192.168.6.4), Internal (192.168.10.254)

- Server: 192.168.10.2

The firewall routed all traffic between the desktop and server, providing an ideal location to deploy Snort for traffic monitoring.

2. Snort Configuration

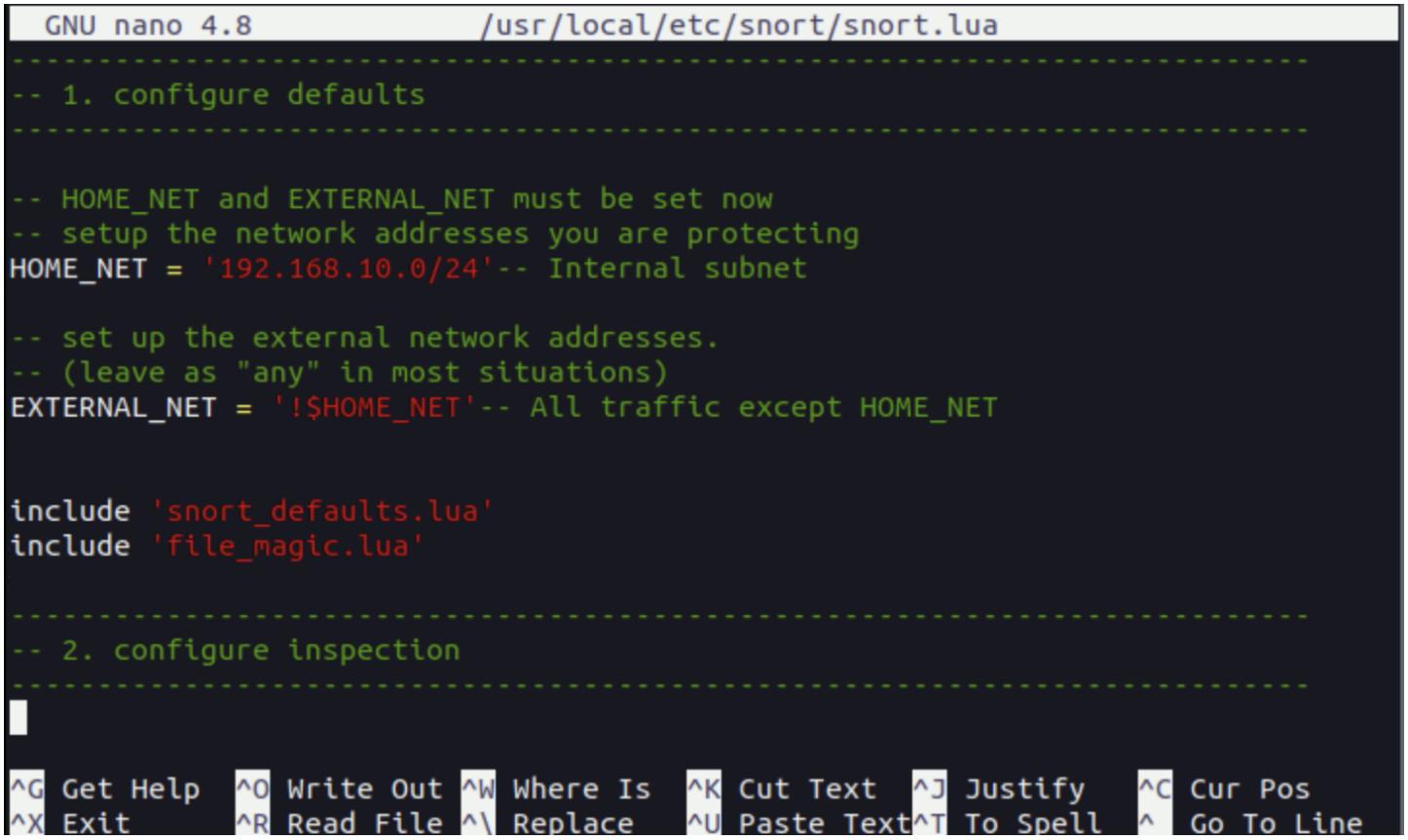
To configure Snort, the following steps were taken:

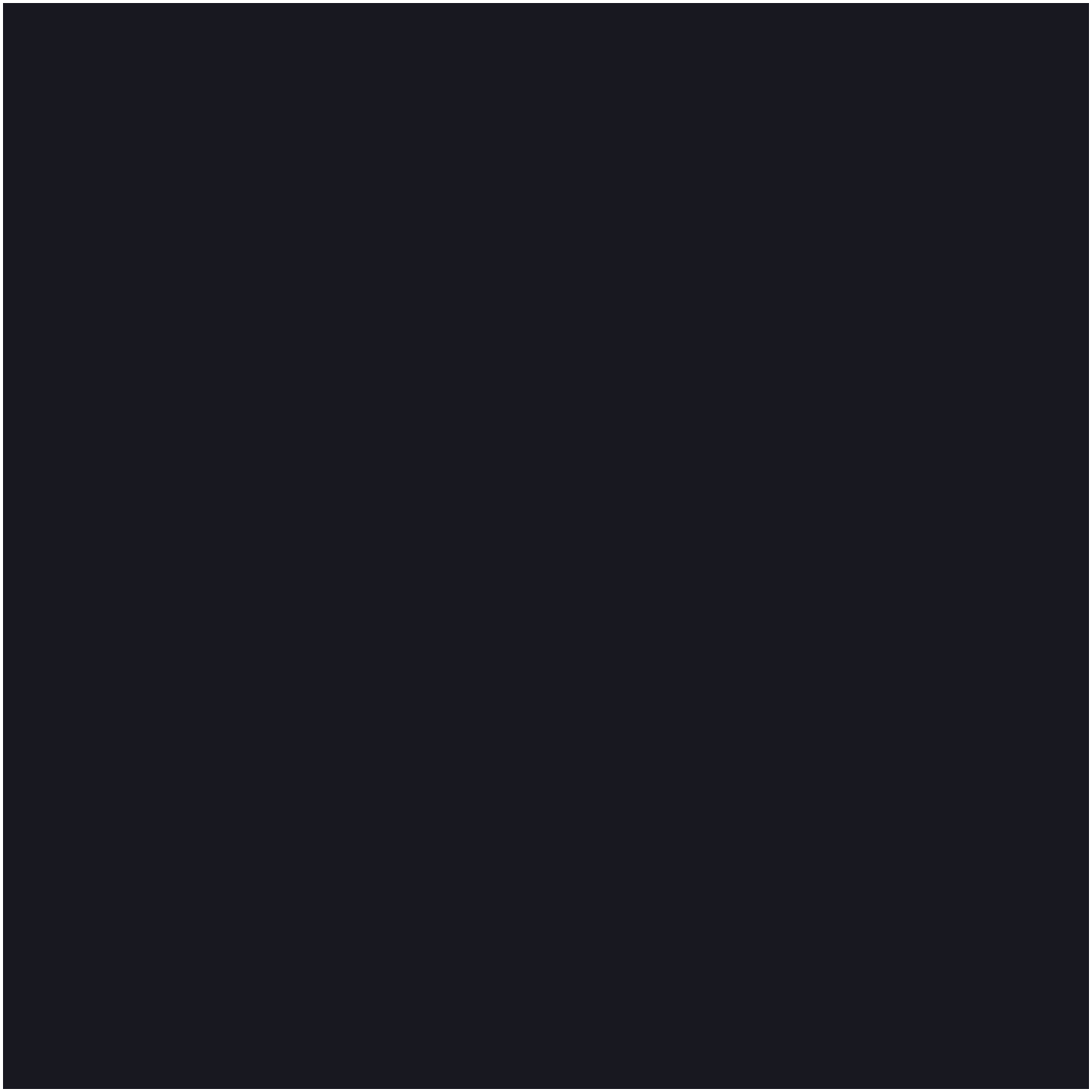
1. Defined the internal and external networks in `/usr/local/etc/snort/snort.lua`.
   - HOME_NET was set to '192.168.10.0/24'.
   - EXTERNAL_NET was set to '!$HOME_NET'.
2. Included the community rules file located at `/usr/local/etc/rules/community.rules`.
3. Enabled file-based logging by adding an `alert_fast` table in the Snort configuration file.
4. Started Snort in daemon mode to log events to `/var/log/snort`.

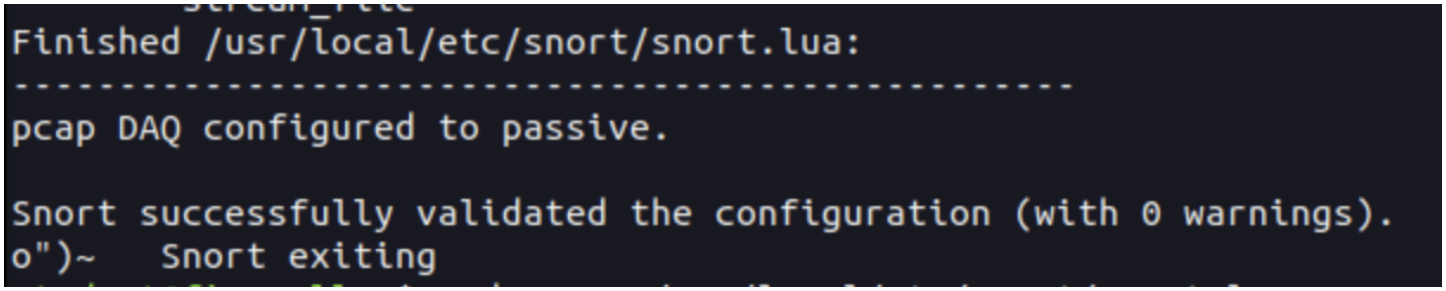
3. Analysis and Results

After configuring Snort and starting it with logging enabled, traffic was monitored, and alerts were logged to

`/var/log/snort/alert_fast.txt`. A malicious User-Agent string, `fortis`, was identified in the logs, classified as a Network Trojan. This validates Snort's ability to detect suspicious traffic using the configured rules.


GNU nano 4.8 /usr/local/etc/snort/snort.lua
-- 1. configure defaults
-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = '192.168.10.0/24'-- Internal subnet
-- set up the external network addresses.
-- (leave as "any" in most situations)
EXTERNAL_NET = '!$HOME_NET'-- All traffic except HOME_NET
include 'snort_defaults.lua'
include 'file_magic.lua'
-- 2. configure inspection
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line




Finished /usr/local/etc/snort/snort.lua:
pcap DAQ configured to passive.
Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting

```
ips =
{
 include = '/usr/local/etc/rules/community.rules',
    variables = default_variables
    -- use this to enable decoder and inspector alerts
    --enable_builtin_rules = true,

    -- use include for rules files; be sure to set your path
    -- note that rules files can include other rules files
    --include = 'snort3-community.rules',

}
```

```
student@firewall:~$ sudo grep "User-Agent" /var/log/snort/alert_fast.txt
01/19-01:34:07.057296 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:58852 -> 1.1.1.1:80
01/19-01:34:12.078393 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:58866 -> 1.1.1.1:80
01/19-01:34:17.100027 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:52346 -> 1.1.1.1:80
01/19-01:34:22.120784 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:52352 -> 1.1.1.1:80
01/19-01:34:27.142211 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:51924 -> 1.1.1.1:80
01/19-01:34:32.162503 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:51932 -> 1.1.1.1:80
01/19-01:34:37.182961 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:55504 -> 1.1.1.1:80
01/19-01:34:42.204209 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:55520 -> 1.1.1.1:80
01/19-01:34:47.224584 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:60216 -> 1.1.1.1:80
01/19-01:34:52.245471 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:60224 -> 1.1.1.1:80
01/19-01:34:57.265332 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:44732 -> 1.1.1.1:80
01/19-01:35:02.286628 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:44742 -> 1.1.1.1:80
01/19-01:35:07.306964 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:46494 -> 1.1.1.1:80
01/19-01:35:12.326789 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:46502 -> 1.1.1.1:80
01/19-01:35:17.346648 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:58946 -> 1.1.1.1:80
01/19-01:35:22.366790 [**] [1:29174:1] "BLACKLIST User-Agent known malicious user-agent string fortis" [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.16
8.10.2:58956 -> 1.1.1.1:80
```