# Snort: Open-Source Intrusion Detection and Prevention

Check GitHub for helpful DevOps tools:

Michael Robotics

Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats information overload by adhering to the set of principles: simplify, prioritize, and execute.

https://github.com/MichaelRobotics

Ask Personal AI Document assistant to learn interactively (FASTER)!

1 Download PDF

2 Go to website

3 Browse file

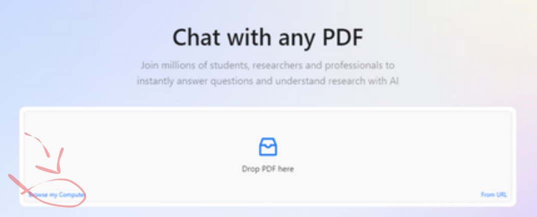
4 Chat with Document

1 https://github.com/MichaelRobotics/DevOpsTools/blob/main/Snort.pdf

Click there to go to ChatPdf website

2

3



Chat with any PDF

Join millions of students, researchers and professionals to instantly answer questions and understand research with AI

Ask questions about document! 4

## Complety new to Linux?

Essential for this PDF is a thorough knowledge of networking. I highly recommend the HTB platform's networking module, which offers extensive information to help build a comprehensive understanding.

HTB - Your Cyber Performance Center

We provide a human-first platform creating and maintaining high performing cybersecurity individuals and organizations.

https://www.hackthebox.com/

## What is Snort?

Snort is an open-source Intrusion Detection and Prevention System (IDS/IPS) that analyzes network traffic to detect and mitigate potential security threats. It uses a rule-based engine to identify malicious activities such as attacks, vulnerabilities, and policy violations.

## How Snort works?

Snort captures and inspects network packets in real-time, comparing them against predefined rules to identify suspicious behavior. When a match is found, it can log, alert, or block the traffic, depending on the configured mode.

## Snort: Why and When

Use Snort to enhance your network security by detecting threats like malware, brute-force attacks, or unauthorized access attempts. It's ideal for both small and large networks seeking a cost-effective, customizable security solution.

Typical Use Case:
A network administrator deploys Snort to monitor traffic for potential malware attacks on a corporate network, automatically blocking harmful packets before they cause damage.

## System Requirements

- 8 gb ram
- 20 free gb storage
- ubuntu 22.04

**If you want to install it on a different Linux distro, ask in the comments and I will write an Ansible playbook or bash script.**

# Snort: Main components & packages

sudo apt-get install snort

# Snort Setup

### 1) Install snort

```
$ sudo apt install snort
```

### 2) check Ip and interface

Check ip of your network. Chose one on which attack machine will be available

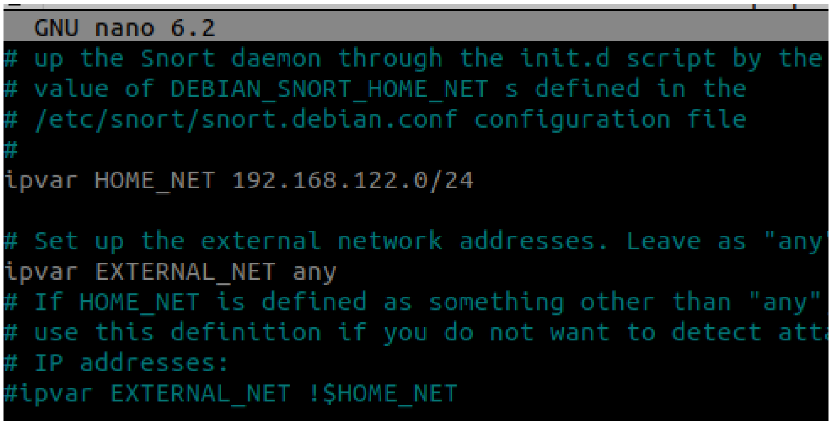
```
$ ifconfig
```

my interface is wlp3s0 and network 192.168.122.0/24

### 3) configure snort config

```
$ sudo nano /etc/snort/snort.conf
```

Add your network to ipvar HOME_NET



```
  GNU nano 6.2
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.122.0/24

# Set up the external network addresses. Leave as "any'
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any"
# use this definition if you do not want to detect att
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

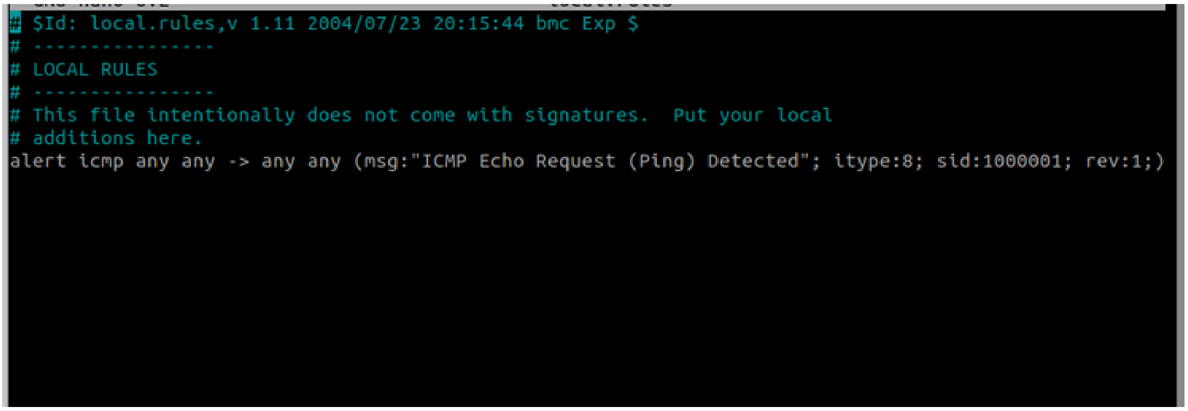
### 4) set snort rules

We will set up a rule to monitor and detect ping requests.

```
$ sudo nano /etc/snort/rules/local.rules
```

Add rule:

```
$ alert icmp any any -> any any (msg:"ICMP Echo Request (Ping) Detected"; itype:8; sid:1000001; rev:1;)
```



```
# $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 -> any any (msg:"ICMP Echo Request (Ping) Detected"; itype:8; sid:1000001; rev:1;)
```

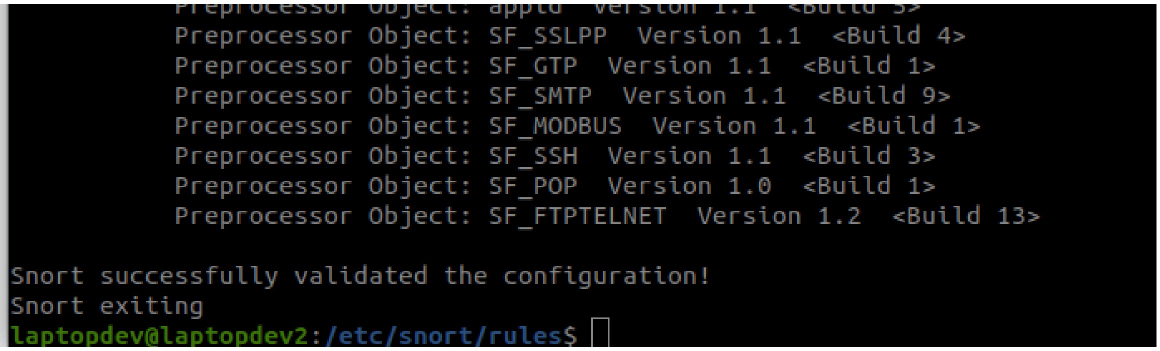
Explanation of Rule Components:

- alert: Action to perform when the rule matches (generate an alert).
- icmp: Protocol to inspect.
- any any -> any any: Source and destination IPs and ports. any indicates all.
- msg:"...": Custom message for the alert.
- itype:8 / itype:0: ICMP type. 8 is Echo Request, and 0 is Echo Reply.
- sid:1000001 / sid:1000002: Unique Snort ID for the rule. Use IDs above 1000000 for local rules to avoid conflicts.
- rev:1: Revision number of the rule.

# Snort test

### 1) Test validity of created configuration

```
$ sudo snort -T -c /etc/snort/snort.conf -i wlp3s0
```

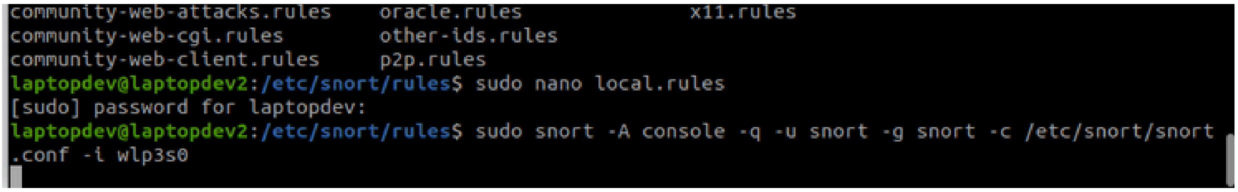


```
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>

Snort successfully validated the configuration!
Snort exiting
laptopdev@laptopdev2:/etc/snort/rules$
```

### 2) Run snort

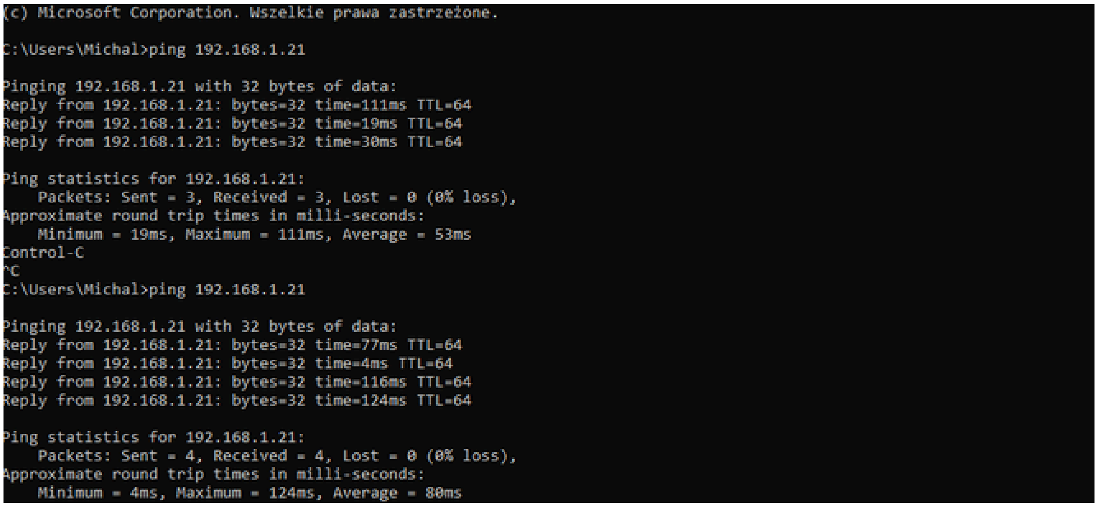
```
$ sudo snort -A console -q -c /etc/snort/snort.conf -i <interface_name>
```

In my case, <interface_name> is wlp3s0



```
community-web-attacks.rules    oracle.rules              x11.rules
community-web-cgi.rules        other-ids.rules
community-web-client.rules     p2p.rules
laptopdev@laptopdev2:/etc/snort/rules$ sudo nano local.rules
[sudo] password for laptopdev:
laptopdev@laptopdev2:/etc/snort/rules$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort
.conf -i wlp3s0
```

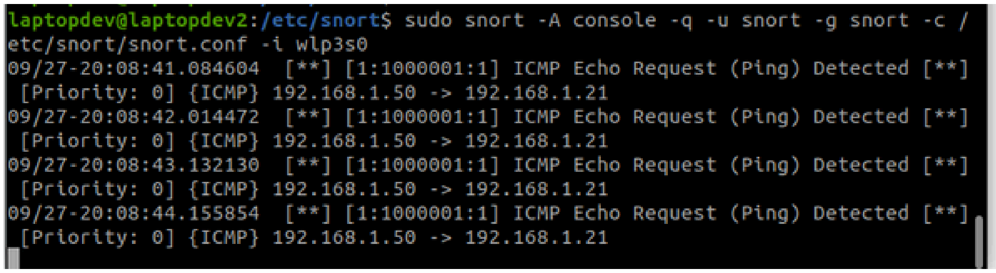
## 3) Ping the machine running Snort from another device connected to the same network.



```
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Michal>ping 192.168.1.21

Pinging 192.168.1.21 with 32 bytes of data:
Reply from 192.168.1.21: bytes=32 time=111ms TTL=64
Reply from 192.168.1.21: bytes=32 time=19ms TTL=64
Reply from 192.168.1.21: bytes=32 time=30ms TTL=64

Ping statistics for 192.168.1.21:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 111ms, Average = 53ms
Control-C
^C
C:\Users\Michal>ping 192.168.1.21

Pinging 192.168.1.21 with 32 bytes of data:
Reply from 192.168.1.21: bytes=32 time=77ms TTL=64
Reply from 192.168.1.21: bytes=32 time=4ms TTL=64
Reply from 192.168.1.21: bytes=32 time=116ms TTL=64
Reply from 192.168.1.21: bytes=32 time=124ms TTL=64

Ping statistics for 192.168.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 124ms, Average = 80ms
```

## 4) Review Snort logs for intrusion detection activity

Snort detected ping command and works correctly!



```
laptopdev@laptopdev2:/etc/snort$ sudo snort -A console -q -u snort -g snort -c /
etc/snort/snort.conf -i wlp3s0
09/27-20:08:41.084604  [**] [1:1000001:1] ICMP Echo Request (Ping) Detected [**]
 [Priority: 0] {ICMP} 192.168.1.50 -> 192.168.1.21
09/27-20:08:42.014472  [**] [1:1000001:1] ICMP Echo Request (Ping) Detected [**]
 [Priority: 0] {ICMP} 192.168.1.50 -> 192.168.1.21
09/27-20:08:43.132130  [**] [1:1000001:1] ICMP Echo Request (Ping) Detected [**]
 [Priority: 0] {ICMP} 192.168.1.50 -> 192.168.1.21
09/27-20:08:44.155854  [**] [1:1000001:1] ICMP Echo Request (Ping) Detected [**]
 [Priority: 0] {ICMP} 192.168.1.50 -> 192.168.1.21
```

# Common troubleshooting

**1) Snort Fails to Start**

Ensure that all necessary rule files are included in snort.conf.

**2) Snort Not Generating Alerts**

Disable Unnecessary Rules: Comment out rules that are not relevant to your environment.

**3) High CPU or Memory Usage**

Run Snort in Debug Mode and Isolate Rules: Disable custom rules and re-enable them one by one to identify the culprit.

**4) Check the snort man page**

**5) If everything is a complete mess**

Remove the bridge and revert the configuration to its previous state.

# Snort: How to remove

### 1) Stop and Disable the Services:

```
sudo systemctl stop snort
```

### 2) Remove the packages

```
sudo apt remove snort
sudo apt purge snort
```

### 3) Remove directories

```
sudo apt autoremove
```

### 4) Check if removed

```
snort -V
```

## Learn more about Snort

### Check Snort website, they have great docs

What is Snort?

Snort is the foremost Open Source Intrusion Prevention System

https://www.snort.org/

# Share, comment, DM and check GitHub for scripts & playbooks created to automate process.

### Check my GitHub

Michael Robotics

Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats skill information overload by adhering to the set of principles: simplify, prioritize, and execute.

https://github.com/MichaelRobotics

*PS.*

*If you need a playbook or bash script to manage KVM on a specific Linux distribution, feel free to ask me in the comments or send a direct message!*