# CodeAlpha\_Snort\_Intrusion\_\_Detection\_System

This is to expain how to develop a basic\_netwrok instrdiuon dtetction system usin snort tool

//Explanation video is on my LinkedIn page posts (https://www.linkedin.com/in/raghad-al-yatim-0619282a6/)

# Snort Installation

. sudo apt update

. sudo apt install snort

. snort --version //to make sure it was installed successfully

# Snort Cofiguration

sudo nano /etc/snort/snort.lua

//the file included as the snort.lua for better understanding

Here we will will adjust the HOME\_NET our local network range.

And the alerts mode if you not prefer to run it mannually using commands in the terminal.

# Setting Rules

navigating to the local in this case

using command: sudo nano /etc/snort/rules/local.rules

insert the desired rules

example:

alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP Ping Request"; sid:1000001; rev:1;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 80 (msg:"Possible XSS Attack"; content:"<script>"; sid:1000002; rev:1;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 21 (msg:"FTP Login Attempt"; sid:1000003; rev:1;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 22 (msg:"SSH Connection Attempt"; sid:1000004; rev:1;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any (flags:S; msg:"Possible SYN Flood"; sid:1000005; rev:1;)

Then you will save the rules and include them in the snrot.lua as :

ips = {

rules = [[

include /etc/snort/rules/local.rules

]],

variables = default\_variables

}

//be carefule with the syntax

# Creating logfile (alert\_fast.filename) for output of alerts

make sure to have the diectory in /var/log/snort and that it has permission to access and write in the file

possible steps:

alert\_fast = {

file = true,

}

// insert in the configuration section in the snort.lua section

sudo mkdir -p /var/log/snort/

sudo chmod 755 /var/log/snort/

sudo chown -R snort:snort /var/log/snort

//then you create the file inside it and change mode the persmission too

touch alert\_fast.txt // this file will conatin all the alerts when testing the snort after creating some network traffic using ping/nmap tools

// in the /var/log/snort/ directory

# Running Snort

sudo snort -A fast -c /etc/snort/snort.lua -R /etc/snort/rules/local.rules -i eth0 -l /var/log/snort/

Overview of Command Behavior: Track Real-Time Traffic

Snort listens for packets on eth0.

Process Rules:

Snort compares the rules specified in /etc/snort/rules/local.rules to the traffic that has been captured.

Create Alerts:

Alerts in the fast format are triggered by matches with rules.

Log Alerts:

Logs and alerts are stored in the /var/log/snort/ directory.

# Simulating Attacks to test your rules using (ping/nmap)

commands example;

nmap -sS [with network ip]

ping -c 5 [with network ip]

finally you will be able to see all results and outputs in the logging directory file we created earlier (alert\_fast.txt ) which can then be used by Wireshark or Splunk for further analysis