Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configure Snort IDS to forward logs to EventTracker

Publication Date:

June 17, 2022

Abstract

This guide provides instructions to retrieve Snort events based on the rules defined in the Snort configuration file and then forward the logs to EventTracker from the syslog extension.

Scope

The configuration details in this guide are consistent with Snort 2.9 or later and EventTracker version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Snort IDS events to forward logs to EventTracker.

Table of Contents

1 Overview

Snort IDS is an open-source intrusion detection system that analyze network traffics in real-time and provides data packet logging. It detects potentially malicious activities by employing a rule-based language that integrates anomaly, protocol, and signature inspection methods.

Netsurion monitors Snort events retrieved via syslog. Dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking possible attacks, suspicious activities, or any other threat based on rules defined in the Snort configuration file.

2 Prerequisites

- A Linux user with root admin privilege.
- Snort 2.9 or later must be configured.
- Rsyslog must be enabled (for Linux).

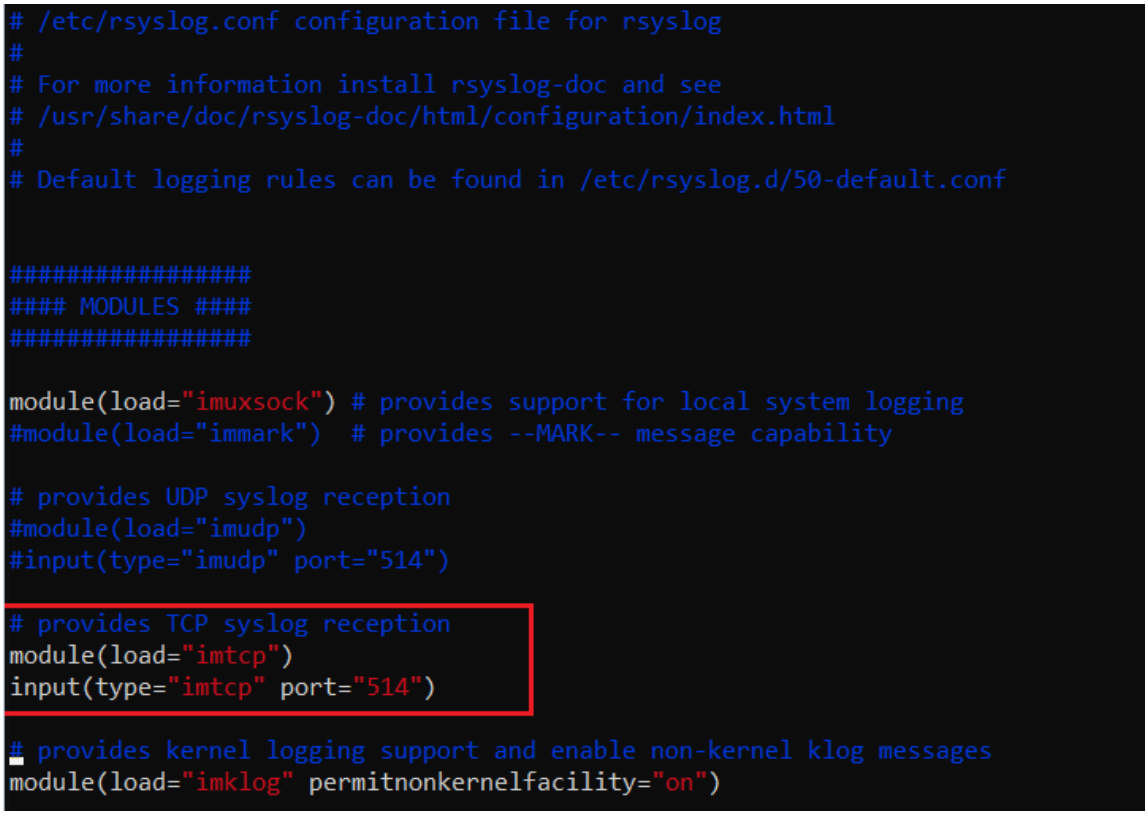
3 Configure Snort IDS to send logs via syslog

Perform the following steps to configure Snort IDS to send logs to EventTracker.

1. Log in to the server or system where you have installed and configured Snort.
2. Edit the rsyslog.conf file using the command: `sudo vi /etc/rsyslog.conf`

> **Note:**
>
> You must have sudoers permission to access the rsyslog configuration file.

3. Enable the TCP (or UDP) syslog reception configurations from the rsyslog.conf file.



```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")
```

4. Include the below details at the end of the configuration file in the following format.

Function

`*.* @<EventTracker_Manager_FQDN>:<port>`

Example

`*.* @EventTracker.contoso.com:514`

Parameters	Description
`*.*`	It defines to log all types of alerts (use `*.alert` to log only alerts)
EventTracker.contoso.com	It is the EventTracker Manager FQDN address
`TCP/514`	It is the port on which the syslog server runs

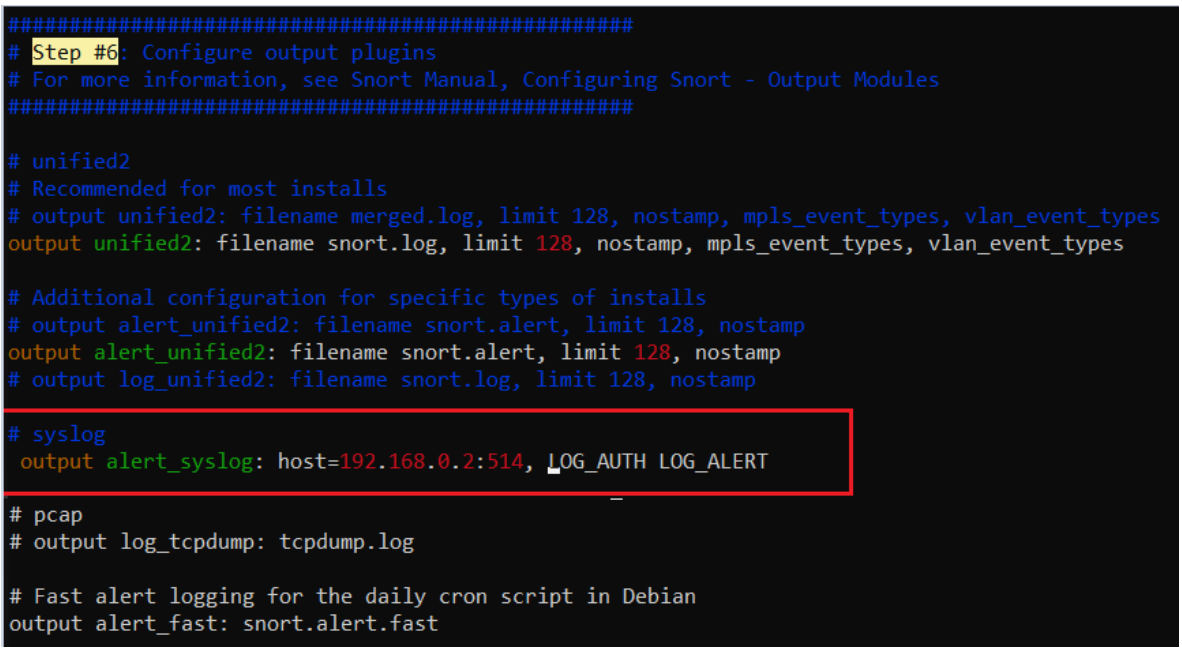
5. After providing the specified details, save and exit the rsyslog.conf file.

6. Then, restart rsyslog.conf file using `sudo /etc/init.d/rsyslog restart`

> **Note:**
>
> The module name may differ in different Linux versions. To enable the module, it is always essential that you remove the hash symbol (#).

> **Note:**
>
> To communicate through the firewall, make sure port 514 (TCP/ UDP depending on your selection) is enabled.

7. Go to the Snort configuration file using `sudo vi /etc/snort/snort.conf` and edit the **syslog** section under **Configure output plugins.**



8. In the syslog section, remove the hash symbol (#) to uncomment the value and provide the following details in the below format.

Function

output alert_syslog: host=<EventTracker_Manager_FQDN>:<syslog_server_port>, LOG_AUTH LOG_ALERT

Example

output alert_syslog: host=EventTracker.contoso.com:514, LOG_AUTH LOG_ALERT

Note:

If you encounter any issues by providing EventTracker Manager FQDN, you can alternatively provide the EventTracker Manager IP address.

9. Start Snort by executing the following command.

Function

```
sudo snort -c /etc/snort/snort.conf -i eth0
```

Parameters	Description
-c	It is used to specify the Snort configuration file
-i	It defines on which interface the Snort must detect the packets

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

Contact Us

Corporate Headquarters
Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support