GROUP 1

SNORT INTEGRATION WITH SPLUNK

GROUP MEMBERS:

ADWAITH S

ADISH RK

ABEL THOMAS

ALEX VARGHESE

ARUN SANGEETH

ASHIK RASHEED

ASWIN A

Splunk Integrated with Snort for Network Intrusion Detection

This project demonstrates the integration of Snort, a network-based Intrusion Detection System (IDS), with Splunk, a centralized Security Information and Event Management (SIEM) platform. Snort is deployed as the primary network monitoring tool, where it inspects live network traffic and detects suspicious activities using rule-based detection mechanisms. Custom rules were created to identify common network threats such as port scanning, ICMP flooding attacks, and unauthorized access attempts to FTP and SSH services.

Once Snort detects these events, the alert logs are generated in real time and forwarded to Splunk using the Splunk Universal Forwarder. Splunk acts as the analysis layer, where these logs are indexed, visualized, and analyzed using search queries and dashboards. Through Splunk, security events become easier to interpret, helping identify attack patterns, source IP addresses, and frequency of suspicious activity over time.

The main goal of this project is to simulate a real-world Security Operations Center (SOC) environment, where network intrusions are not only detected but also analyzed and monitored from a centralized platform. By integrating Snort with Splunk, this system demonstrates how raw network alerts can be converted into meaningful security intelligence. The project highlights the importance of visibility, monitoring, and correlation in modern cybersecurity environments and provides a foundation for building more advanced detection and prevention systems in the future.

1. INTRODUCTION

With the rapid growth of the internet and digital technologies, organizations and individuals are increasingly dependent on computer networks for communication, data storage, and business operations. As network usage increases, cyber threats such as hacking attempts, malware, denial-of-service attacks, and unauthorized access also increase. These attacks can result in data loss, financial damage, and system disruption. Therefore, network security has become one of the most important aspects of modern computing systems.

Traditional security mechanisms such as firewalls mainly focus on allowing or blocking traffic based on predefined rules. However, attackers continuously develop new techniques to bypass basic protections. This is where advanced security monitoring tools like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) platforms become essential. They not only detect suspicious activities but also provide visibility into what is happening inside the network.

1.1 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security tool designed to monitor network traffic and detect unauthorized access, misuse, and abnormal activity. IDS systems analyze incoming and outgoing network packets and compare them against known attack signatures or suspicious behavior patterns. When an anomaly or known threat is detected, the IDS generates alerts for further investigation.

- IDS can be categorized into two types:
- Network-based IDS (NIDS): Monitors network traffic.
- Host-based IDS (HIDS): Monitors logs and files on individual systems.

In this project, Snort is used as a Network-based IDS (NIDS). Snort captures network packets in real time and checks them against predefined rule sets that identify threats such as port scanning, denial-of-service attempts, and unauthorized service access. Snort is widely used in security environments because it is open-source, reliable, and customizable.

1.2 Importance of Network Security

Cybersecurity is no longer optional due to the increasing number of cyber attacks worldwide. Organizations face threats like:

- Data theft
- Denial-of-Service (DoS) attacks
- Malware infections
- Password attacks
- Network scanning and reconnaissance

These attacks can disrupt business operations and compromise user data. Therefore, continuous monitoring and real-time alerting mechanisms are necessary to detect threats early and minimize damage.

- Network security focuses on:
- Monitoring traffic patterns
- Detecting anomalies
- Preventing unauthorized access
- Responding to security incidents

A successful security system not only detects problems but also provides meaningful insights into attack behavior, enabling administrators to take fast and correct actions.

1.3 Purpose of This Project

The purpose of this project is to integrate Snort with Splunk to simulate a real-world Security Operations Center environment. Snort is responsible for the detection layer, while Splunk acts as the analysis and visualization platform.

- This integration allows:
- Centralized visibility of all alerts
- Faster detection of suspicious activities
- Real-time analysis through dashboards
- Improved understanding of attack trends

By implementing this setup, the project demonstrates how network-level security monitoring can be effectively combined with SIEM capabilities to enhance security operations.

2. SYSTEM ARCHITECTURE

This section explains the architecture of the system developed in this project, which integrates Snort with Splunk to build a real-time Intrusion Detection and Monitoring system.

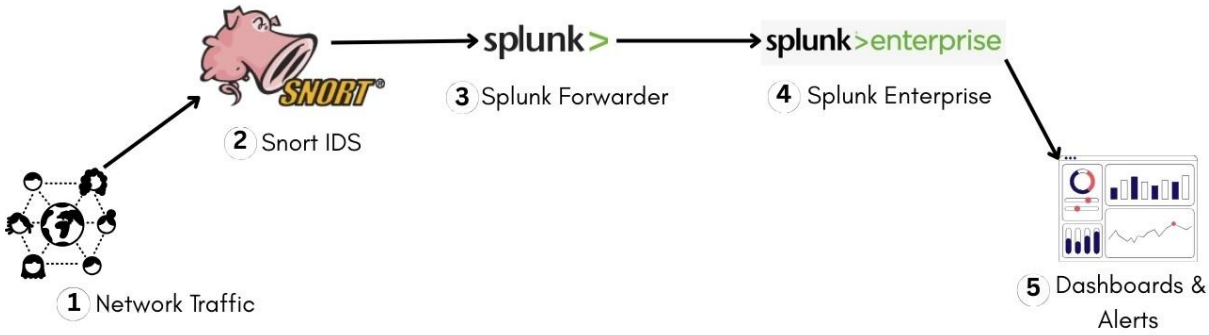
The architecture follows a layered design where traffic is captured, analyzed, forwarded, and visualized in a structured pipeline. Each tool in the system plays a specific role in ensuring intrusion detection and security visibility.

2.1 Architecture Overview

The architecture consists of four major components:

1. Network Traffic Source
2. Snort IDS (Detection Engine)
3. Splunk Universal Forwarder
4. Splunk Enterprise (SIEM Platform)

The overall data flow of the system is:



This design models a simplified version of a real-world Security Operations Center (SOC).

2.2 Components Description

2.2.1. Network Traffic

This layer represents all communication occurring on the system, including legitimate user activity and simulated attacks such as port scanning and ICMP flooding. The traffic is generated from different devices in the network or test tools used during demonstration.

2.2.2. Snort IDS

Snort is deployed as a Network Intrusion Detection System (NIDS) that listens to the live network interface.

- Functions of Snort:
- Captures network packets
- Matches packets against detection rules
- Generates alerts when suspicious activity is detected
- Logs alerts into log files

Custom detection rules were implemented to identify:

- Port scanning activity
- ICMP flooding
- FTP access
- SSH access

Snort works as the detection layer of the system.

2.2.3. Splunk Universal Forwarder

The Splunk Universal Forwarder is installed on the same machine as Snort. Its role is to monitor the Snort log file and securely forward detection logs to Splunk Enterprise.

Functions:

- Reads Snort logs from file system
- Sends logs to Splunk in real-time
- Maintains secure data transmission
- Forwarder ensures:
- No alert is lost
- Logs appear live in Splunk

2.2.4. Splunk Enterprise

Splunk Enterprise is used as the SIEM platform for:

- Storing logs
- Indexing data
- Searching events
- Displaying dashboards
- Performing correlation

Splunk converts raw output from Snort into clear charts, graphs, and searches that allow analysts to quickly identify:

- Attack patterns
- Source IP addresses
- Traffic spikes
- Time of events

Splunk acts as the analysis and visualization layer.

2.3 Data Flow Explanation

1. Network packets are captured by Snort.
2. Each packet is checked against detection rules.
3. When suspicious activity is found, Snort generates an alert.
4. The alert is written to a log file.
5. Splunk Forwarder reads the file and forwards the logs.
6. Splunk Enterprise indexes the log data.
7. The security analyst views the results in dashboards.

2.4 Advantages of This Architecture

- Real-time detection: Alerts are generated immediately.
- Centralized monitoring: All logs are analyzed in Splunk.
- Scalable design: Easy to add more systems.
- Better visibility: Dashboards simplify analysis.
- Professional model: Similar to real SOC environments.

3. SYSTEM REQUIREMENTS & INSTALLATION

3.1 System Requirements

The following requirements were used for implementing this project:

Hardware Requirements

- Minimum 8 GB RAM
- 2 Core CPU
- 40 GB Storage

Software Requirements

- Ubuntu Linux (Snort & Forwarder machine)
- Splunk Enterprise (SIEM Server)
- Splunk Universal Forwarder
- Snort IDS
- Nmap (for testing)
- Internet connection

Network Requirements

- Static IP for Splunk Server
- Port 9997 open for receiving logs
- Same network or reachable network for Snort and Splunk

3.2 Installation of Snort on Ubuntu

Step 1: Update system packages

- sudo apt update && sudo apt upgrade -y

Step 2: Install Snort

- sudo apt install snort -y

During installation:

- Enter HOME_NET = your local subnet

  Example:

  192.168.29.0/24

Step 3: Check Snort version

- snort –version

```
dedmxd@dedmxd:~$ snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3
```

3.3 Configuration of Custom Snort Rules

Edit local rule file:

- sudo nano /etc/snort/rules/local.rules

Add custom rules:

```
# $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 tcp any any -> any 22 (msg:"SSH ACCESS DETECTED"; sid:100001; rev:1;)

alert tcp any any -> any 21 (msg:"FTP ACCESS DETECTED"; sid:100002; rev:1;)

alert icmp any any -> any any (msg:"ICMP FLOOD / DOS DETECTED"; sid:100003; rev:1;)

alert tcp any any -> any any (flags:S; threshold:type both, track by_src, count 10, seconds 5; msg:"PORT SCAN DETECTED"; sid:100004; rev:1;)
```

Save file.

Step 4: Start Snort in IDS mode

- sudo snort -c /etc/snort/snort.conf -i enp0s3

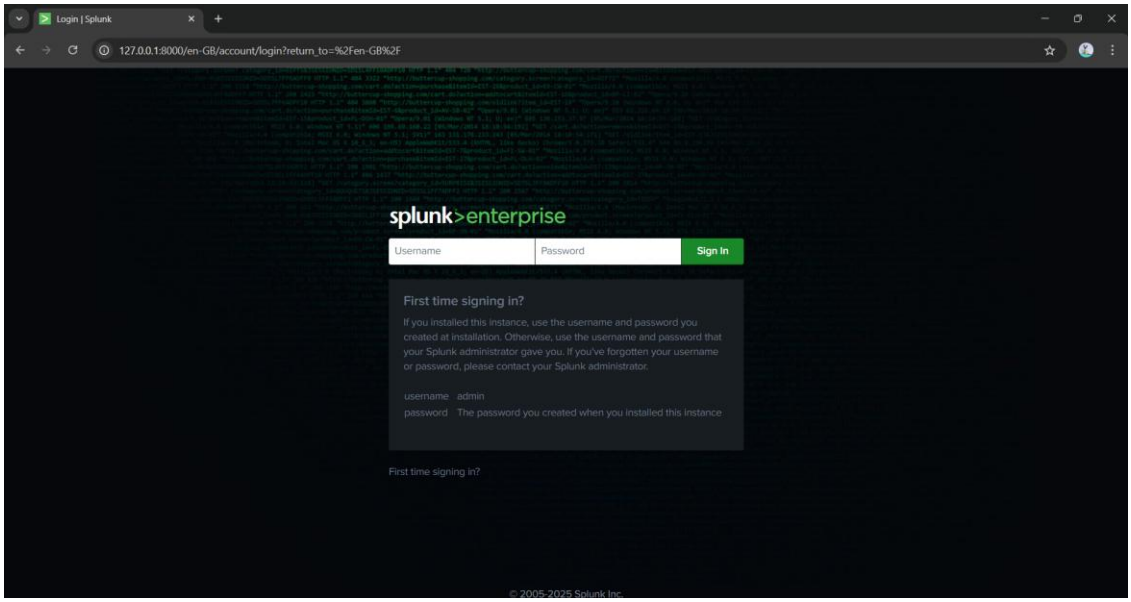
3.4 Installation of Splunk Enterprise

- https://www.splunk.com

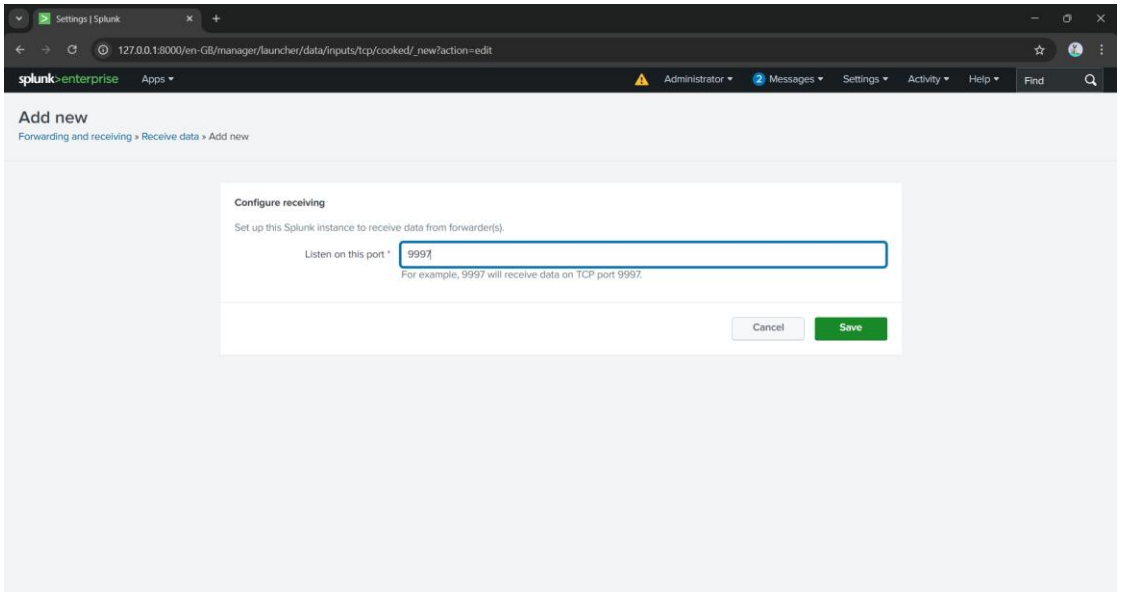
Steps:

- Install Splunk Enterprise
- Create admin username and password
- Access Web Interface:

  http://<Splunk-IP>:8000



3.5 Enable Receiving Port in Splunk



In Splunk Enterprise:

- Settings → Forwarding and Receiving → Configure Receiving → Add Port 9997

3.6 Installation of Splunk Universal Forwarder (Ubuntu)

Place .deb or .tgz file in directory.

Install:

- sudo dpkg -i splunkforwarder-*.deb

or if tgz:

- sudo tar -xvf splunkforwarder.tgz -C /opt

Enable Forwarding

- sudo /opt/splunkforwarder/bin/splunk start
- sudo /opt/splunkforwarder/bin/splunk enable boot-start

Add receiving server

- sudo /opt/splunkforwarder/bin/splunk add forward-server <Splunk-IP>:9997

Monitor Snort Logs

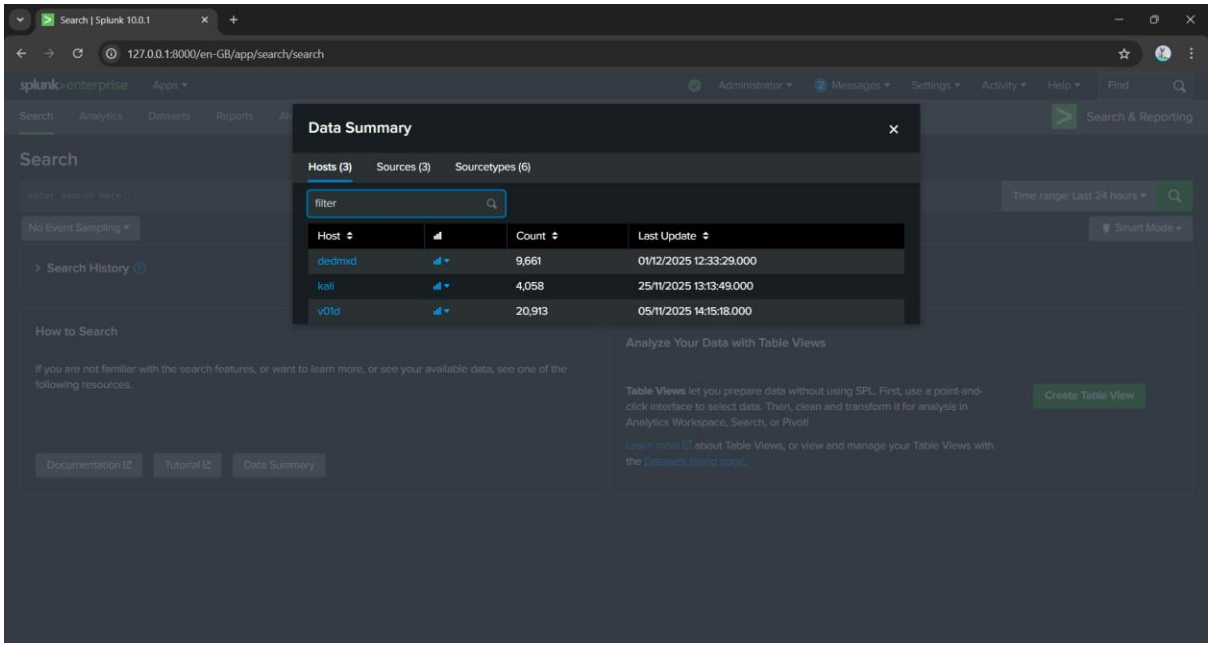
- sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/snort/snort.alert.fast

Verification Commands

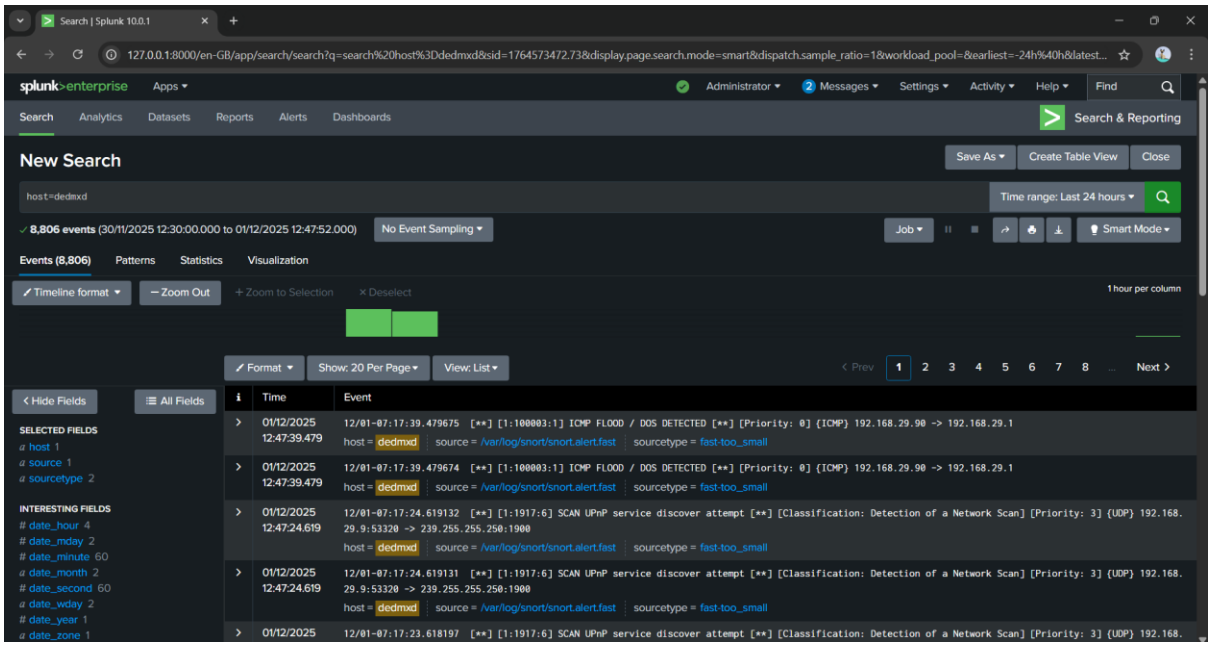
- sudo /opt/splunkforwarder/bin/splunk list forward-server
- sudo /opt/splunkforwarder/bin/splunk list monitor
- sudo /opt/splunkforwarder/bin/splunk status

3.7 Firewall Configuration

- sudo ufw allow 9997/tcp
- sudo ufw reload



- click on host



- Go to Ubuntu (Snort machine) → Open terminal
- Run:

  sudo snort -c /etc/snort/snort.conf -i enp0s3

  (Replace enp0s3 if your interface name is different.)

  Snort is now LIVE and monitoring traffic.

4. ATTACK SIMULATION & DETECTION

4.1. ICMP / DOS TEST

- ping <target_ip>

Example:

- ping 192.168.29.90

Press CTRL + C after a few seconds.

4.2. PORT SCAN (NMAP)

On another system or same system:

- nmap <target_ip>

Example:

- nmap 192.168.29.90

4.3. FTP ACCESS

Make sure FTP is running.

Test:

- ftp <target_ip>

4.4. SSH ACCESS

- ssh <target_ip>

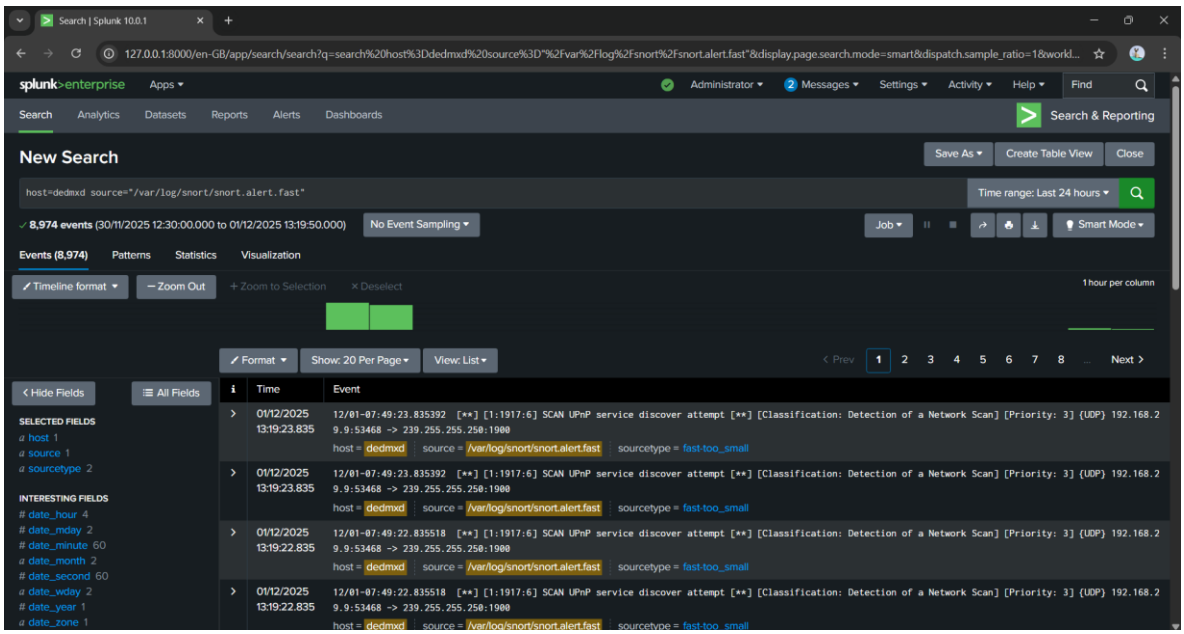
5. RESULTS & OBSERVATIONS

Go to:

- Search & Reporting → Data Summary → click on host

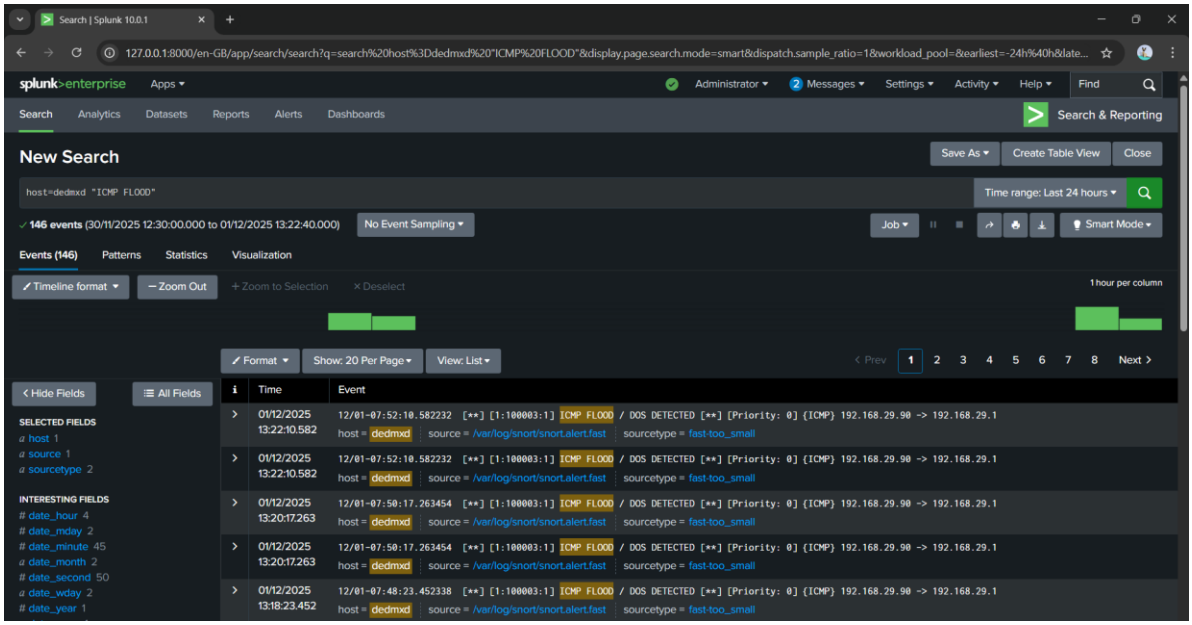
View all Snort logs:

- (host=”host-name” source="/var/log/snort/snort.alert.fast")

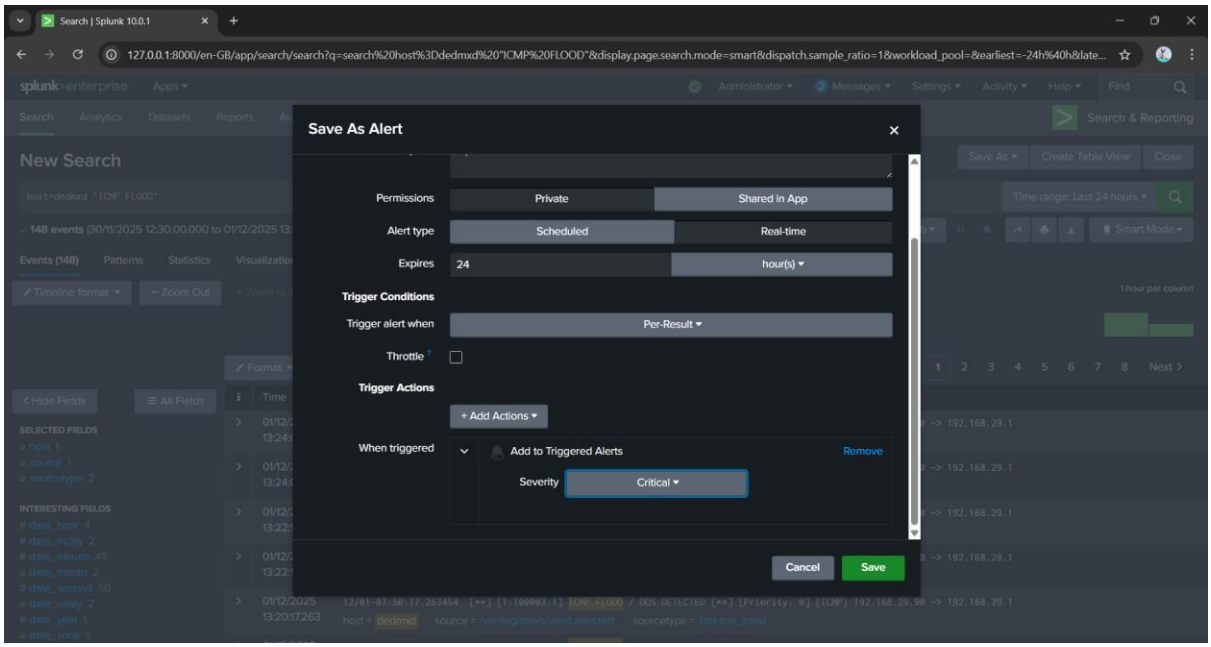


ICMP / DOS TEST

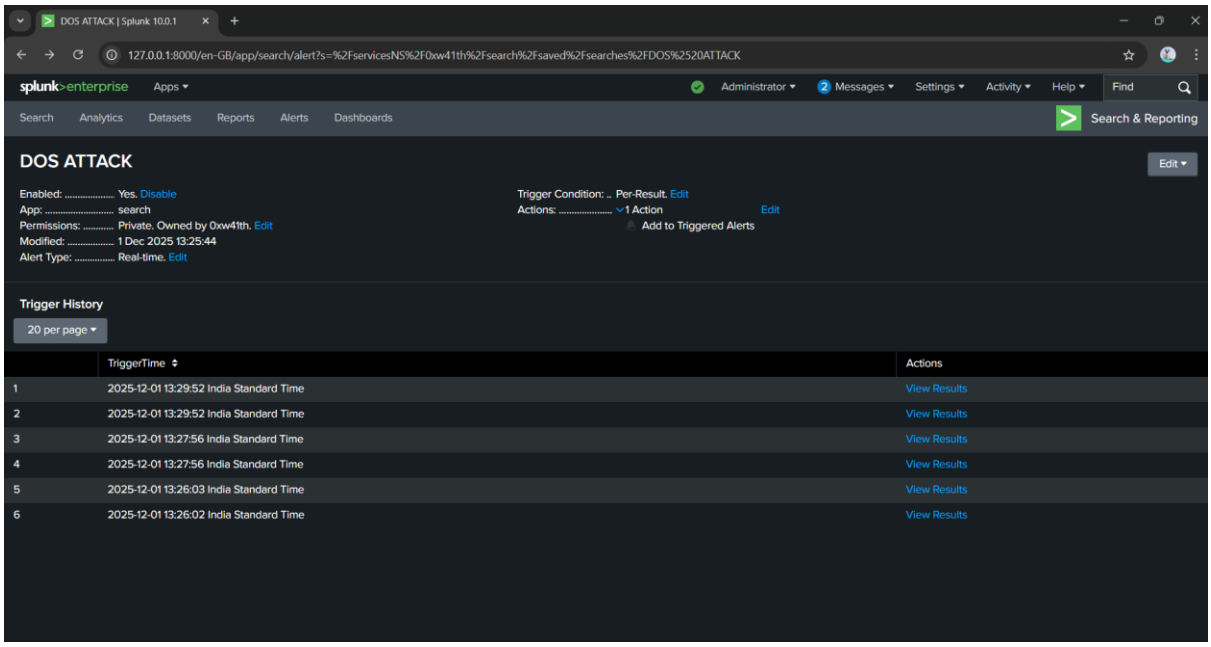
- ping <target ip>



- click on save as alert



- Click on Save → View Alert
- Go to ubuntu machine → open terminal
- Type Command:
- ping <target ip>
- Go to Splunk enterprise → Acitivity → Triggered Alerts



- Click on View Results