CYBERSECURITY MONITORING & THREAT DETECTION LAB

Leslie Grint

Network Security

Executive Summary

This project involved building a self-contained, virtualised SOC lab replicating a small enterprise network. Using tools like Security Onion, Splunk, pfSense, and Wireshark, the environment was used to simulate, detect, and respond to both controlled and unexpected cyber threats.

Simulated attack vectors (e.g., Kerberos brute-force, port scanning, ICMP sweeps) were detected and triaged in real time, enabling hands-on testing of alerting, packet capture, log correlation, and forensic investigation.

The environment also successfully responded to a real-world external intrusion, resulting in firewall lockdown, user privilege revocation, and PCAP-based analysis—mirroring real SOC workflows.

This project demonstrates my ability to build operational defensive infrastructure, perform incident response, and translate theoretical security principles into practical solutions.

Introduction

This report presents a self-initiated Security Operations Centre (SOC) lab designed to replicate a small enterprise network and test end-to-end **blue team** operations. The primary goal was to simulate real-world attack scenarios and evaluate the effectiveness of industry-standard monitoring, detection, and response tools, including **Splunk**, **Security Onion**, **Suricata**, and **Kibana**.

By designing and deploying a virtualised enterprise environment, this project provided hands-on experience with critical **defensive cybersecurity techniques**, including SIEM configuration, threat hunting, alert analysis, log correlation, and incident response. Simulated attacks such as **ping sweeps**, **port scanning**, and **brute-force logins** were launched from an attacker machine (Kali Linux), and the lab infrastructure was tasked with identifying, analysing, and responding to these threats in real time.

Most notably, the lab also detected and recorded a **genuine external intrusion** attempt. This real-world event triggered alerts in both Security Onion and Splunk, allowing for a full investigation and response cycle — including containment, privilege revocation, and firewall lockdown — mirroring professional SOC protocols.

This project validates not only the functionality of open-source security tools but also the value of **blue team skillsets** in detecting and mitigating both simulated and live threats. The environment reinforces foundational concepts in **threat intelligence**, **incident detection**, and **response coordination**, all essential to defending modern networks against evolving cyber threats.

Lab Setup

To replicate a realistic small-to-medium enterprise network, a fully virtualised SOC lab was developed using **VMware Workstation Pro**. The environment consisted of multiple interconnected virtual machines (VMs), each configured to represent key components of enterprise infrastructure. The lab provided a dedicated platform for testing blue team capabilities such as **log aggregation**, **network-based threat detection**, and **incident response workflows**.

Lab Components

- **Windows Server 2019**
  Configured as the **Domain Controller (DC)** running **Active Directory (AD)** and **DNS** services. This machine served as the backbone of the internal network, managing authentication, user and group policies, and name resolution. Its intentionally weakened security posture provided opportunities for attacker simulation and privilege escalation.

- **Windows 11 Pro**
  A **domain-joined client machine** used to represent an average employee workstation. It was configured for log forwarding and monitored for suspicious activity. It also served as a pivot point for detecting lateral movement and endpoint compromise.

- **Ubuntu Server (with Splunk Enterprise)**
  This server hosted **Splunk Enterprise**, an enterprise-grade **Security Information and Event Management (SIEM)** platform.
  Splunk was configured to:

    - Collect and index logs from key infrastructure (e.g., Windows Server, pfSense, and endpoints)
    - Perform keyword and pattern-based searches across large datasets
    - Detect brute-force attacks, account lockouts, and privilege escalation attempts
    - Correlate multi-source data into actionable security alerts
      Splunk's advanced search and visualisation capabilities made it a central tool for blue team operations, enabling efficient incident detection, investigation, and response.

- **Security Onion**
  Security Onion is a **Linux-based network security monitoring (NSM) and intrusion detection system (IDS)** platform. It aggregates a powerful suite of open-source tools to deliver deep packet inspection, threat detection, and forensic analysis capabilities. In this lab, Security Onion operated in conjunction with:

    - **Suricata** – A high-performance **network IDS/IPS engine** that scans packet data in real time, detecting anomalies and known attack signatures (e.g., port scans, Nmap activity, brute-force attempts).
    - **Kibana** – A **data visualisation and dashboard tool** built on top of Elasticsearch. It was used to visualise alerts and threat intelligence data collected by Suricata and other sensors.

Security Onion provided the **network-centric visibility** to complement Splunk's log-based approach, giving the blue team a more complete picture of attack paths and behaviours.

- **pfSense Firewall**
  Deployed as the **network perimeter device**, **pfSense** managed IP addressing and enforced firewall policies. It was configured to:

    - Act as a **DHCP server** for non-critical machines
    - Route all internal traffic
    - Simulate realistic network segmentation between internal and external zones.
- **Kali Linux**
  A dedicated **attacker machine** used to simulate internal threat actors or compromised insiders. Kali was used to:
    - Conduct **reconnaissance** (e.g., ping sweeps, Nmap scans)
    - Perform **brute-force attacks** on login portals and SMB services
    - Test detection rules and response mechanisms in place within the SOC
- **Metasploitable 2**
  A **vulnerable-by-design virtual machine** that mimics legacy or misconfigured enterprise systems. It served as a target for the Kali Linux attacks, allowing:
    - Testing of exploit payloads
    - Monitoring of attack paths
    - Validation of detection alerts in both Splunk and Security Onion

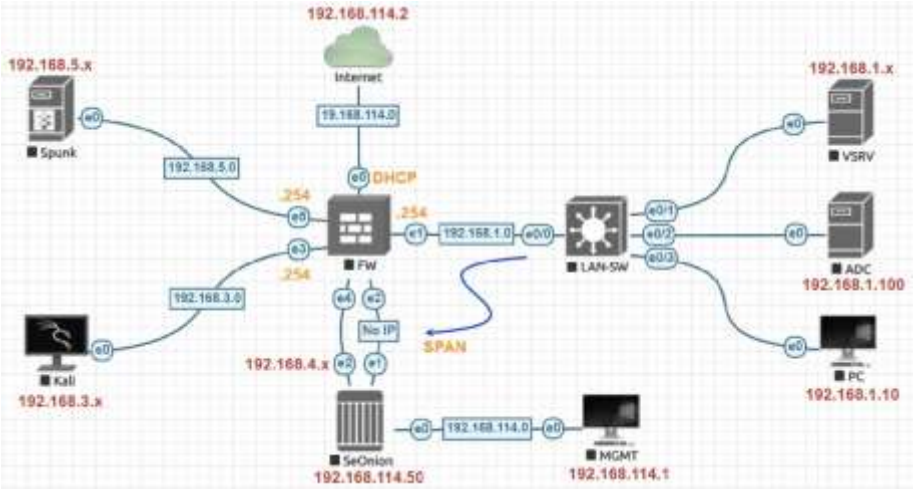
Network Design & Configuration

The lab network was logically structured to mirror segmented enterprise zones (e.g., internal LAN, DMZ, external access). Static IP addresses were configured for:

- **Windows Server 2019** (Domain Controller)
- **Ubuntu Server** (Splunk Enterprise)
- **Security Onion**

All other machines were assigned IP addresses via **pfSense's DHCP service**. This hybrid configuration allowed for reliable log forwarding and rule-based monitoring on critical infrastructure, while preserving flexibility for endpoint testing and attacker simulation.

Traffic from all VMs was routed through **pfSense**, providing visibility into internal and external traffic patterns. Both **Splunk** and **Security Onion** were configured to receive logs and traffic data from various endpoints, enabling complete SOC visibility across the environment.



Network Topology

Simulated Attacks

To rigorously assess the lab's threat detection and monitoring capabilities, a series of realistic cyber-attack techniques were executed from the **Kali Linux** attacker VM. These attacks were carefully selected to simulate common adversary tactics during the early stages of a cyber intrusion, specifically the **reconnaissance** and **initial access** phases of the cyber kill chain.

ICMP Ping Sweep

Using the ping utility, a network-wide ICMP echo request sweep was performed to identify active hosts within the enterprise subnet. This reconnaissance technique mimics an attacker mapping the network to discover potential targets. The sweep generated a burst of ICMP traffic, which was expected to trigger alerts in network-based intrusion detection systems.

Nmap Scanning

Building upon the initial host discovery, the attacker conducted detailed port scanning and service enumeration using **Nmap**. This included TCP SYN scans, OS fingerprinting, and version detection to identify running services and potential vulnerabilities on targeted machines, such as the Windows Server and Metasploitable 2 hosts. Nmap's probing generates characteristic network patterns that can be detected and flagged by IDS signatures and anomaly detection rules.

Kerbrute Brute Force Password Attack

To simulate credential-based attacks aimed at gaining unauthorised access, **Kerbrute** was used to perform a brute force attack against the **Kerberos** authentication service of the Windows Server 2019 domain controller. Kerbrute targets the Kerberos protocol by attempting password

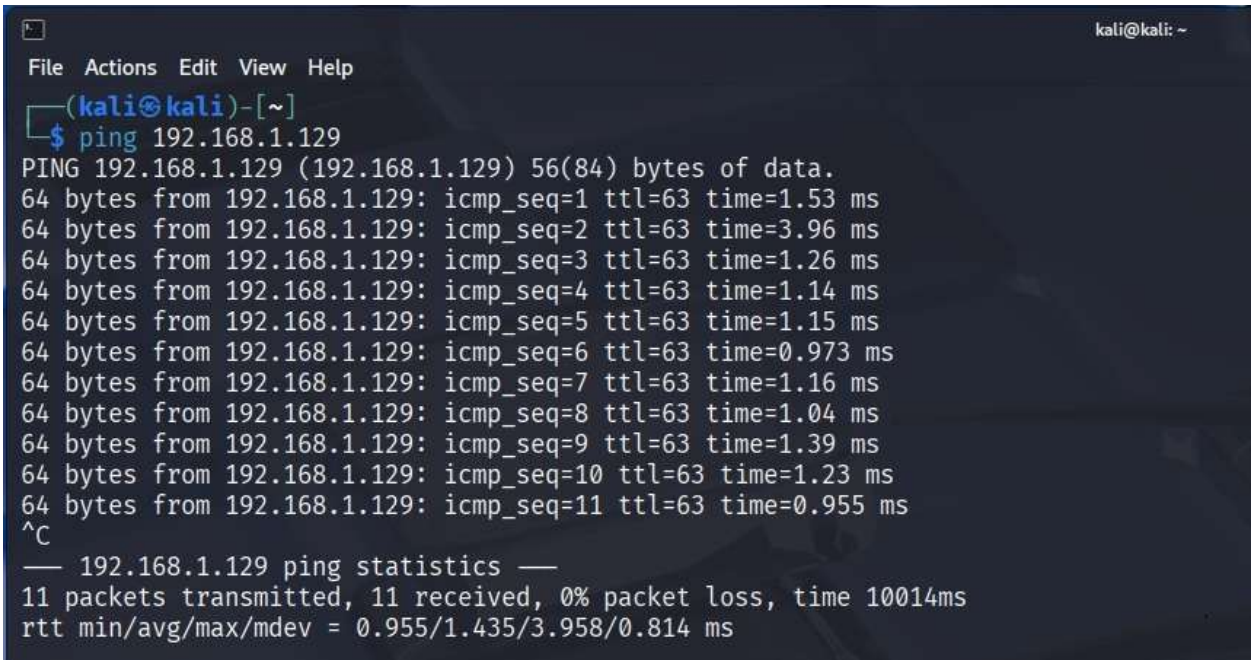
guessing against user accounts, enabling testing of domain credential security and brute force detection mechanisms.

Purpose and Blue Team Relevance

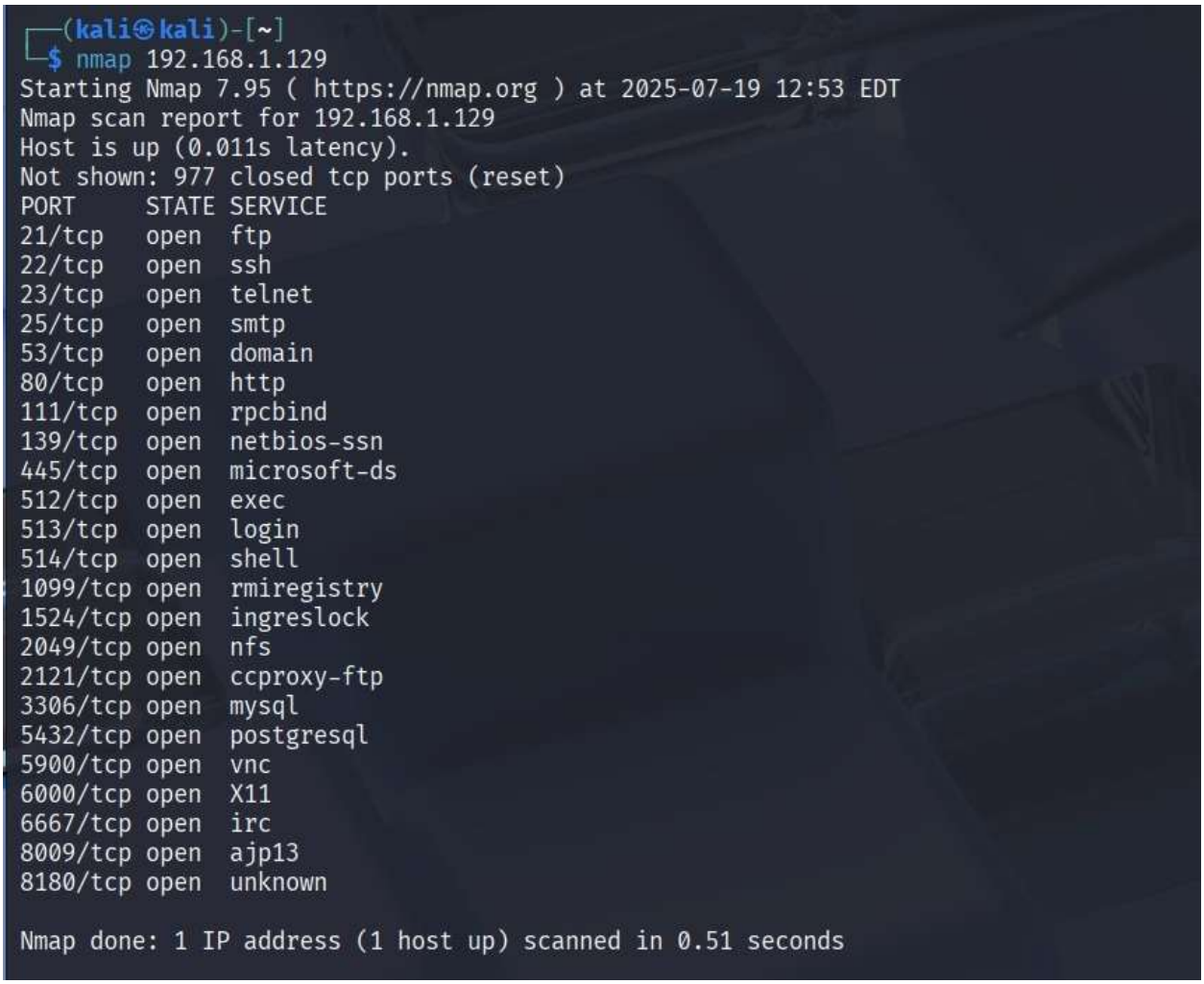
These simulated attacks were integral for validating the lab's **blue team defensive posture**. Each attack generated distinct network and system artefacts, allowing SIEM platforms like **Splunk** and **Security Onion** to:

- Detect anomalous network activity such as scanning and host discovery
- Generate real-time alerts for suspicious authentication attempts via Kerberos
- Log detailed event data to support forensic analysis and incident response
- Correlate multiple sources of data to build a comprehensive picture of attack progression

The comprehensive logging and alerting facilitated the evaluation of detection rules, tuning of signatures, and response workflows in a controlled, realistic setting.



Kali Linux ICMP Ping Sweep



Kali Linux Nmap Port Scanning

Threat Detection and Response

The lab's detection and response capability was centred around two enterprise-grade SIEM platforms—**Security Onion** and **Splunk**—which were deployed to provide layered visibility into network traffic and endpoint behaviour. This section details how each tool detected, processed, and responded to both simulated attack traffic and a real-world external intrusion, simulating how a real SOC team would triage, investigate, and contain threats.

Security Onion Response

Security Onion served as the lab's **Network Security Monitoring (NSM)** platform, built with a suite of integrated tools including **Suricata** (IDS/IPS), **Zeek** (network analysis), **Kibana** (visualisation), and **The Hive** (case management).

🛡️ Simulated Threat Detection

- **Ping Sweep (ICMP reconnaissance)**
  Suricata generated signature-based alerts for high volumes of ICMP echo requests originating from the Kali Linux VM. The alerts contained metadata such as source/destination IPs, ICMP types, and timestamps.
- **Nmap Scanning (Service Enumeration)**
  SYN-based and aggressive Nmap scans triggered Suricata's scan detection rules. Alerts indicated targeted TCP ports, scan techniques (e.g., -sS, -sV), and service fingerprints.
- **Suricata Alert Contextualisation**
  Using **Security Onion Console (SOC)** and **Kibana**, these events were reviewed in chronological order, revealing the attacker's kill chain progression—initial probing, service mapping, and potential targeting.
- **Hunt Interface & PCAP Analysis**
  Using the Hunt interface, analysts drilled into alert sessions and retrieved correlated **Zeek logs** (e.g., conn.log, notice.log, dns.log) to enrich the event timeline. PCAPs were exported and examined in **Wireshark** to perform deep packet inspection and validate the attack vectors (e.g., TCP handshakes).

⚠️ Real-World Intrusion Detection

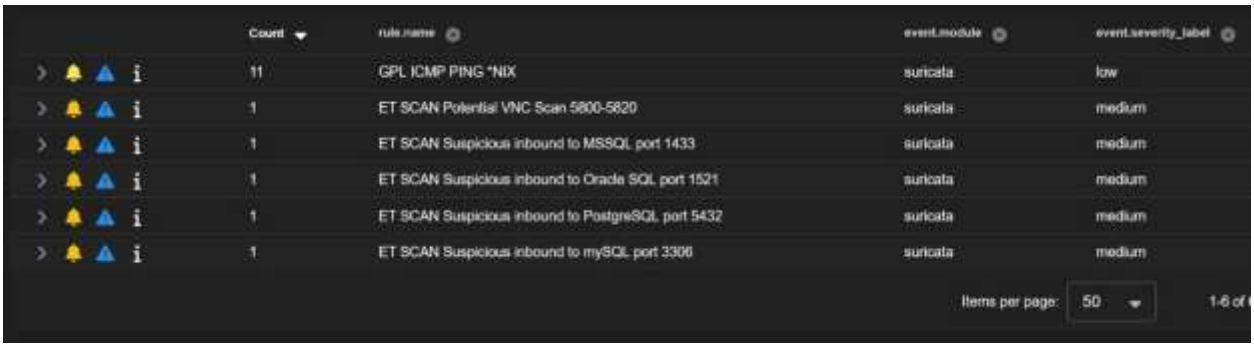
Unexpectedly, Suricata detected suspicious connections originating from an **external IP**—unrelated to internal attack traffic. The attacker initiated:

- **Scanning of exposed vulnerable systems** (e.g., Metasploitable 2, Windows Server)
- **Exploitation attempts** suggesting lateral movement and possible service enumeration

🧩 Incident Response Measures

The detection of the real-world attack was triaged and escalated through Security Onion's case management system. A standard response playbook was executed:

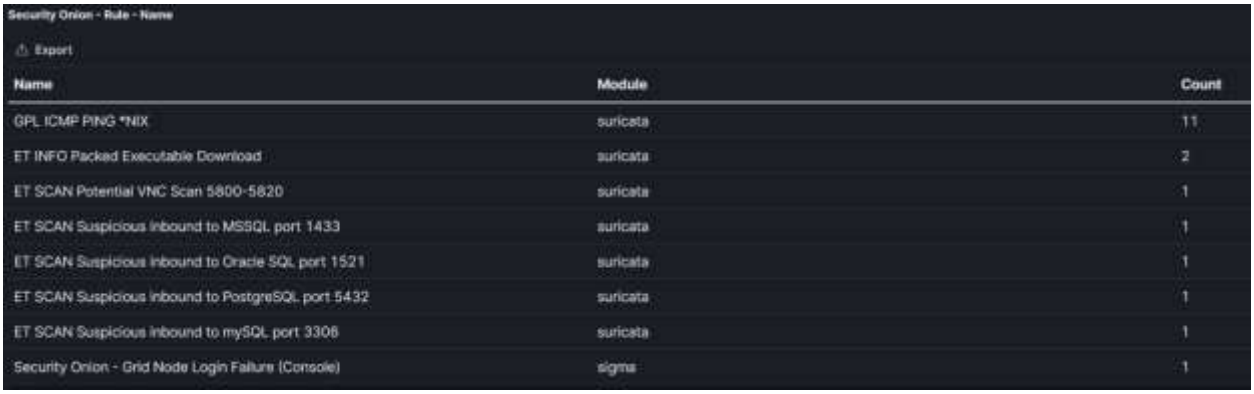
- **Isolated vulnerable assets** from the virtual switch to stop external communication
- **Revoked AD privileges** for user accounts possibly compromised
- **Updated PfSense firewall rules** to restrict all incoming external traffic except whitelisted admin IPs
- **Retained PCAPs and logs** for forensic analysis, preserving evidence chain



	Count	rule.name	event.module	event.severity_label
>	11	GPL ICMP PING *NIX	suricata	low
>	1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium
>	1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
>	1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
>	1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
>	1	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium

Items per page: 50 1-6 of

Security Onion ICMP Ping Sweep and Nmap Port Scan Alert



Security Onion - Rule - Name

Export

Name	Module	Count
GPL ICMP PING *NIX	suricata	11
ET INFO Packed Executable Download	suricata	2
ET SCAN Potential VNC Scan 5800-5820	suricata	1
ET SCAN Suspicious inbound to MSSQL port 1433	suricata	1
ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	1
ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	1
ET SCAN Suspicious inbound to mySQL port 3306	suricata	1
Security Onion - Grid Node Login Failure (Console)	sigma	1

Kibana and Suricata ICMP Ping Sweep and Nmap Port Scan Alert

Security Onion - Source IPs

Export

Source IP	Count
192.168.3.1	16
81.134.116.100	1
81.134.117.168	1

Kibana and Suricata External IP Address Source

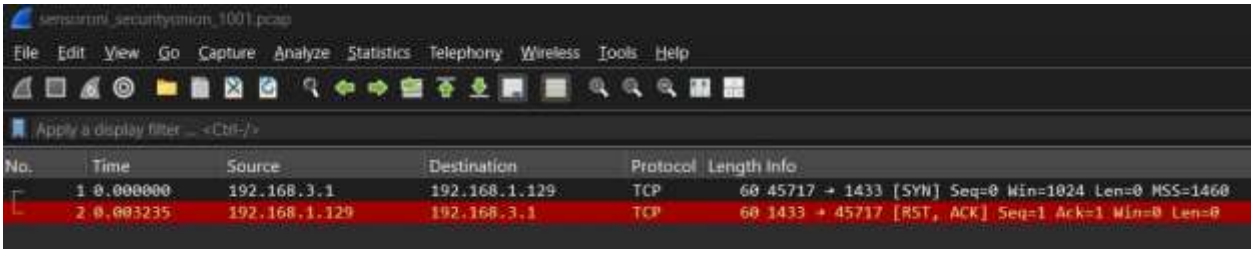
0 2025-07-19 17:53:58.415 +01:00 TCP 192.168.3.1

```
0000  00 0C 29 E8 D9 EF 00 0C  29 68 F0 5D 08 00 45 00   ..).....)h.]..E.
0016  00 2C 73 3F 00 00 32 06  BF BA C0 A8 03 01 C0 A8   .,s?..2.........
0032  01 81 82 95 05 90 DF 17  FE 78 00 00 00 00 60 02   .........x....`.
0048  04 00 78 94 00 00 02 04  05 B4 00 00              ..x.........
```

1 2025-07-19 17:53:58.418 +01:00 TCP 192.168.1.129

```
0000  00 0C 29 68 F0 5D 00 0C  29 E8 D9 EF 08 00 45 00   ..)h.]..).....E.
0016  00 28 00 00 40 00 40 06  B4 FD C0 A8 01 81 C0 A8   .(..@.@.........
0032  03 01 05 99 82 95 00 00  00 00 DF 17 FE 79 50 14   .............yP.
0048  00 00 94 3D 00 00 00 00  00 00 00 00              ...=........
```

Security Onion Pcap (Before Export)



Wire Shark Pcap (Imported from Security Onion)

Splunk Response

While Security Onion focused on network telemetry, **Splunk Enterprise**, running on Ubuntu Server, was configured as the **host-level SIEM** for log aggregation and behaviour analysis. Logs were ingested from **Windows Server 2019** via the **Splunk Universal Forwarder**, offering deep insights into domain authentication, group policy events, and system logs.

🦹 Simulated Attack Detection

- **Kerbrute Password Spray Detection**
    - The brute-force attack using Kerbrute targeted the **Kerberos authentication service** on the Windows Server DC.
    - Splunk parsed and indexed Windows Event ID **4625** (failed logon).
    - By correlating spikes in logon failures from a single IP, Splunk identified the spray pattern.
- **Search Filtering with SPL (Search Processing Language)**
    - Custom SPL queries were crafted to isolate and visualise brute-force attack.

i	Time	Event
>	7/20/25 4:11:19.000 PM	07/20/2025 05:11:19 PM ... 24 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-SRV-2019 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	7/20/25 4:11:10.000 PM	07/20/2025 05:11:10 PM ... 24 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-SRV-2019 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	7/20/25 4:11:08.000 PM	07/20/2025 05:11:08 PM ... 24 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-SRV-2019 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	7/20/25 4:11:05.000 PM	07/20/2025 05:11:05 PM ... 24 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-SRV-2019 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	7/20/25 4:11:03.000 PM	07/20/2025 05:11:03 PM ... 24 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-SRV-2019 source = WinEventLog:Security sourcetype = WinEventLog:Security

Splunk Brute-Force Pattern Detection

Tools and Technologies Used

This SOC lab employed a comprehensive set of tools that reflect those used in professional enterprise environments. The selection spans across security monitoring, attack simulation, infrastructure, and forensic analysis. These tools were integrated to simulate a full defensive security stack, enabling threat detection, log correlation, and incident response workflows.

SIEM & Monitoring

Tool	Description
Security Onion	An open-source, enterprise-grade Linux distribution for intrusion detection, network security monitoring, and log management. Security Onion was used to capture and analyse network traffic in real time. It provided deep packet inspection and threat detection using Suricata along with integrated case management.
Suricata	A powerful network IDS/IPS and network security monitoring engine built into Security Onion. Suricata generated detailed alerts for all malicious traffic including ICMP scans, Nmap SYN scans, and suspicious communications from external IPs.
Kibana	Kibana, part of the Elastic Stack, was used to visualise Suricata-generated alerts and logs. It enabled real-time dashboards, time-based filtering, and pattern recognition, helping to investigate both simulated and real-world threats.
Splunk Enterprise	A commercial SIEM platform used for log collection, indexing, and advanced correlation. Installed on Ubuntu Server, it ingested logs from Windows Server via the Universal Forwarder. Splunk was configured to track user login behaviour, brute-force attempts, and privilege escalation, offering host-level visibility.

Operating Systems & Infrastructure

Tool	Description
Windows Server 2019	Configured as the Domain Controller (DC), running Active Directory and DNS. The DC served as a key target for attack simulations and generated valuable security logs for analysis. Security configurations were deliberately weakened to test defensive detection strategies.

Tool	Description
Windows 11 Pro	Acted as a domain-joined endpoint simulating a typical employee workstation. This machine could access the internal network and SOC dashboards.
Ubuntu Server	Hosted Splunk Enterprise SIEM. Also used to centralise and visualise log data from Windows hosts. The server's static IP configuration ensured reliable connectivity for log forwarding and SOC operations.

Attack Simulation & Vulnerable Targets

Tool	Description
Kali Linux	Used as the red team attacker node. Launched internal reconnaissance and password attacks (ICMP sweeps, Nmap scanning, Kerberos-based brute-forcing). Enabled practical demonstration of the Cyber Kill Chain stages including reconnaissance and initial access.
Kerbrute	A Kerberos brute forcing tool used to perform password spraying attacks against domain accounts via AS-REQ packets. Chosen specifically to test blue team detection of authentication anomalies.
Nmap	Used for host discovery, OS fingerprinting, and open port enumeration. Generated scan traffic that triggered IDS alerts in Suricata and was captured in PCAPs.
Metasploitable 2	An intentionally vulnerable Linux VM that served as an easy-to-exploit endpoint. Used to simulate exploitable assets inside the network, helping test lateral movement visibility.

Firewall & Network Control

Tool	Description
PfSense	An open-source firewall/router software deployed as the central network gateway. Configured with NAT, DHCP (for most hosts), and segmentation rules. Played a critical role in isolating compromised systems and blocking external intrusion once detected. Also logged blocked and allowed connections.

🔍 Forensic Analysis & PCAP Inspection

Tool	Description
Wireshark	Used to open and inspect PCAP files exported from Security Onion. Enabled byte-level analysis of suspicious packets (e.g., Nmap SYN scans, brute-force traffic, and the unexpected external intrusion). This tool was vital for verifying alert accuracy and understanding protocol misuse.

📄 Log Collection & Forwarding

Tool	Description
Splunk Universal Forwarder	Installed on Windows Server 2019 to forward event logs to Splunk Enterprise over a secure channel. Enabled near real-time ingestion of authentication logs, group policy changes, and system events, all of which were used to detect lateral movement and unauthorised activity.

This tooling environment provided full lifecycle coverage for the **blue team**, from log ingestion and correlation to alerting, case management, and packet-level validation. It allowed for hands-on experience with professional SOC workflows, including threat triage, incident response, and forensic analysis.

Conclusion

This self-initiated SOC lab successfully demonstrated the design, deployment, and operation of a simulated enterprise security environment capable of detecting and responding to both simulated and real-world cyber threats. By integrating open-source and enterprise-grade tools—including Splunk, Security Onion, Suricata, Kibana, and pfSense—the lab replicated core functions of a modern Security Operations Centre.

Attack Simulation & Detection Validation

Through the execution of structured attack simulations such as ICMP reconnaissance, Nmap scanning, and Kerberos password brute-forcing (via Kerbrute), the lab validated its detection and monitoring capabilities across both network and host layers. Security Onion effectively flagged reconnaissance and scanning activity in real time, while Splunk correlated authentication failures and identified brute-force attempts through Windows event logs. The combined use of PCAP analysis, SIEM dashboards, and event correlation techniques reinforced the importance of layered visibility in threat detection.

Real-World Intrusion & Incident Response

Significantly, the detection and containment of an unexpected external intrusion showcased the real-world applicability of the lab setup. The ability to triage, investigate, and respond using professional tooling—mirroring industry-standard incident response workflows—further showcasing the operational readiness of the defensive configurations in place.

Blue Team Skills Development

This project not only highlighted the efficacy of open-source defensive technologies but also reinforced critical blue team skills, including log analysis, alert tuning, forensic investigation, and network monitoring. The hands-on experience gained through this lab builds a strong foundation for real-world SOC roles, bridging the gap between theoretical knowledge and practical application in cyber defence.

Personal Capability & Employability

This project showcases my ability to independently design, configure, and operate a comprehensive cybersecurity lab simulating real-world enterprise threats and defences. From initial architecture to final incident response, every component of this environment was planned and implemented autonomously.

In addition to technical proficiency across SIEM platforms, IDS/IPS tools, log correlation, and forensic analysis, this project reflects a deep understanding of blue team workflows and security operations lifecycle. It also demonstrates the self-motivation, curiosity, and discipline necessary to learn complex systems outside of a formal setting.

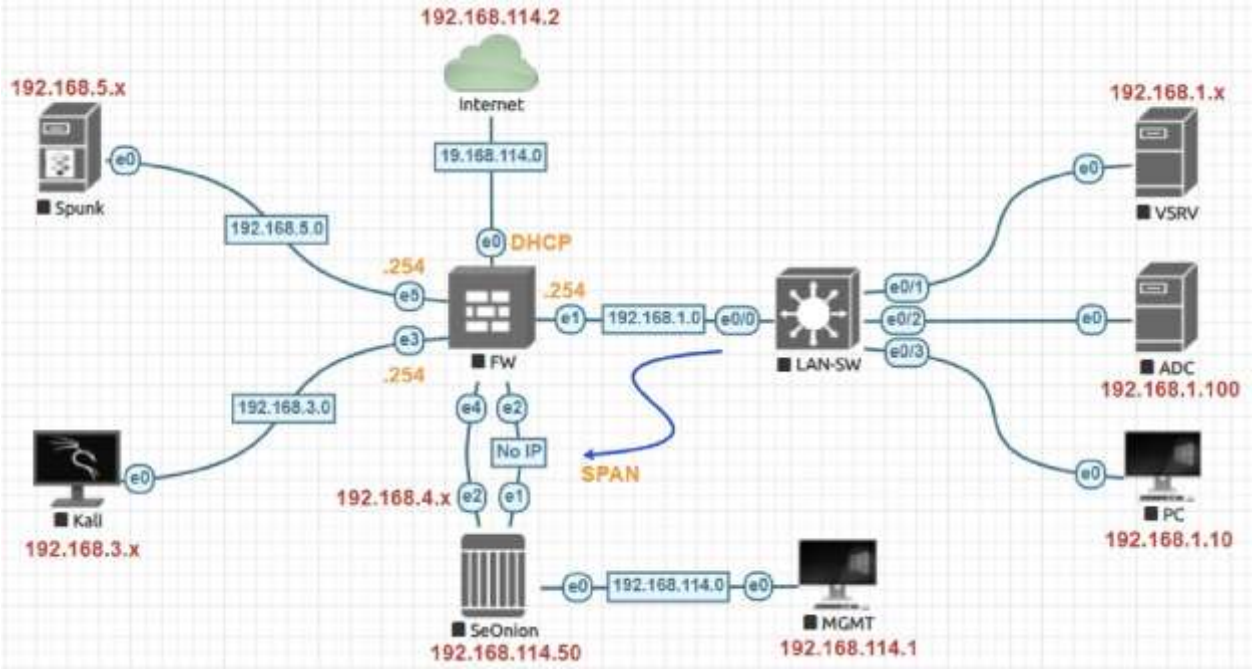
Whether in a junior SOC role or an entry-level cybersecurity position, I bring practical experience, a strong analytical mindset, and a hands-on approach to cyber defence that translates directly into value for any security team.

Final Thoughts

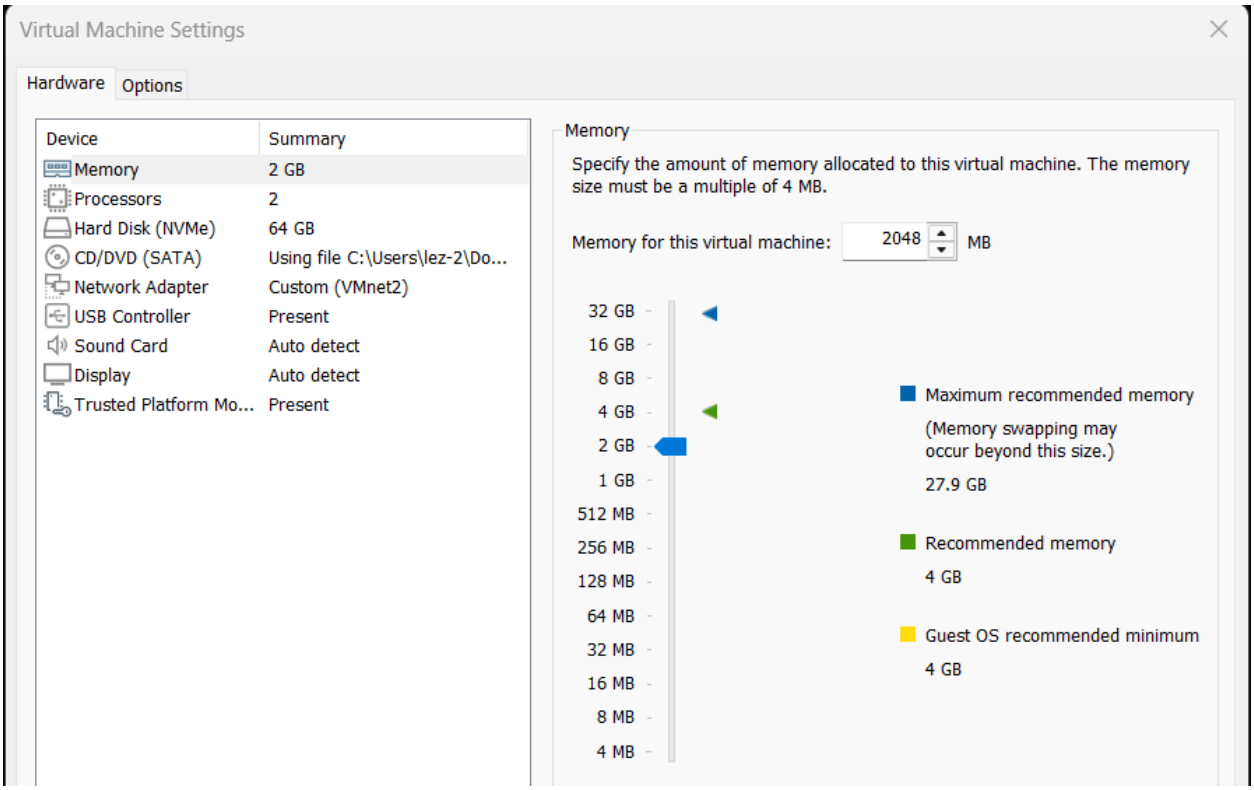
Ultimately, this SOC lab serves as a scalable blueprint for developing cybersecurity operations capabilities—whether for training, research, or operational testing—and affirms the importance of proactive defence in today’s threat landscape.

Appendix A – Network and Virtual Machine Configurations

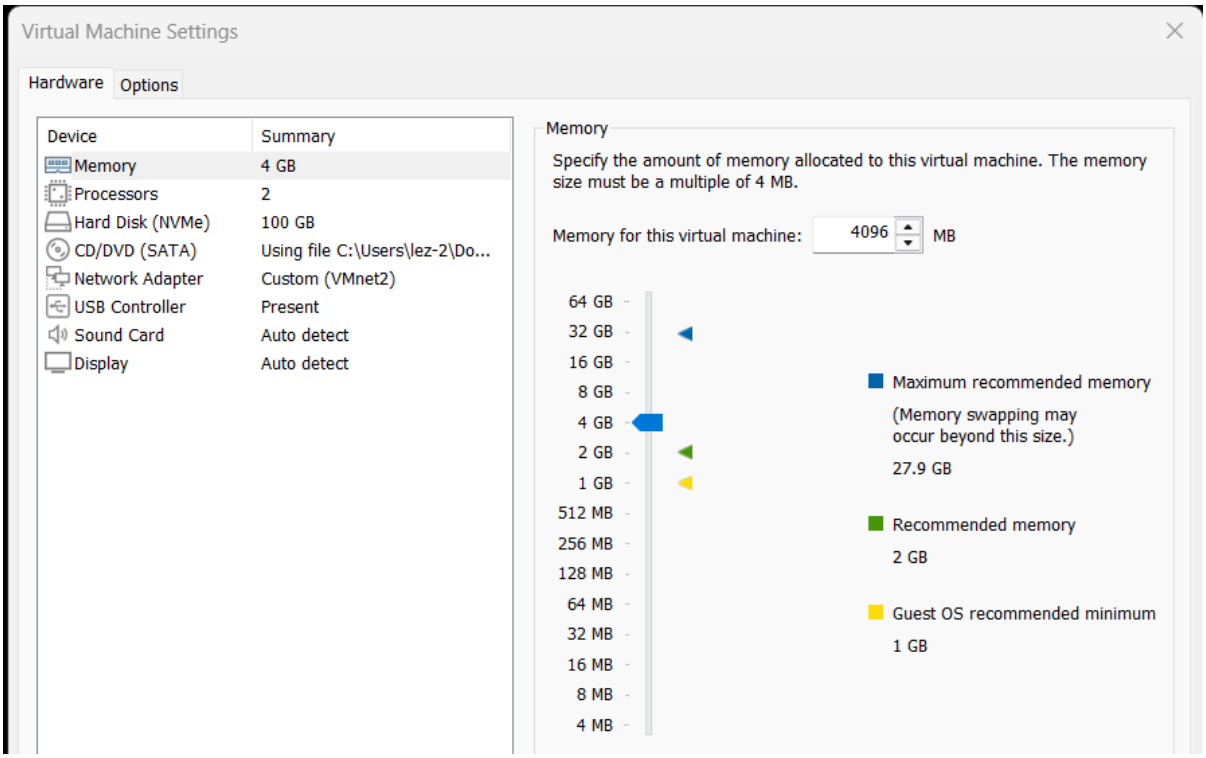
Network Topology



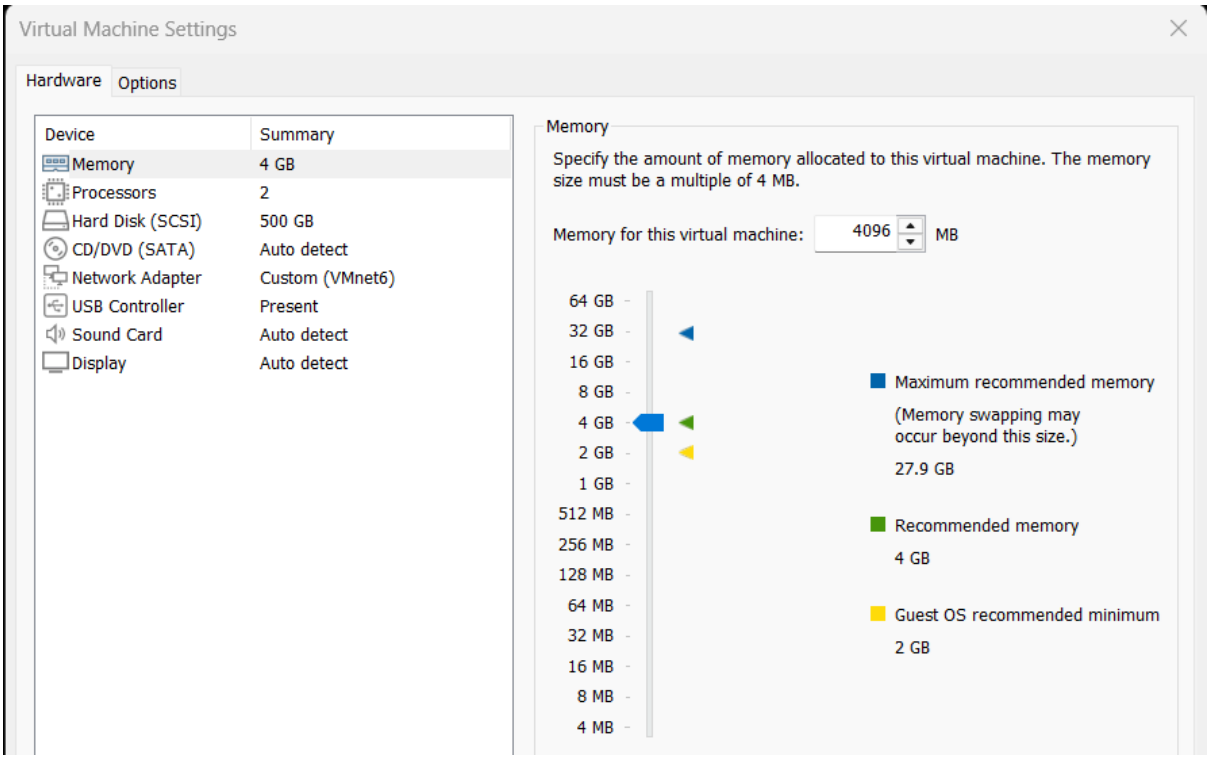
Windows 11 VM Configuration



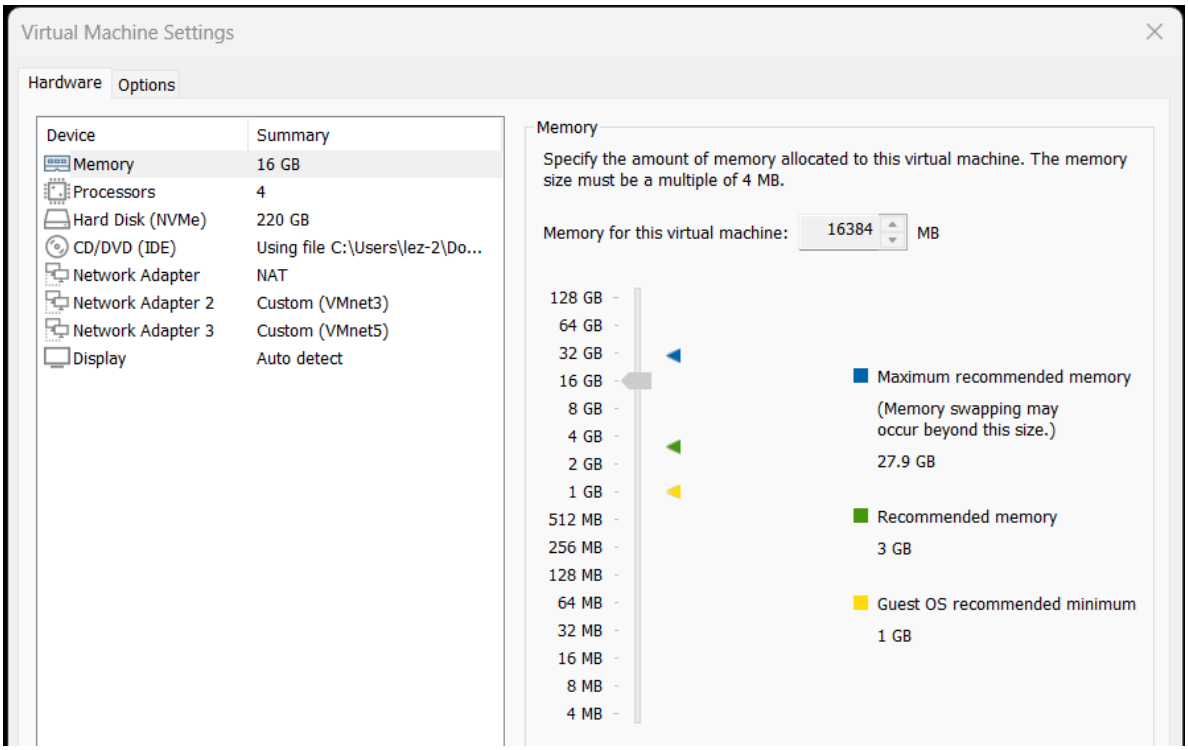
Windows Server 2019 VM Configuration



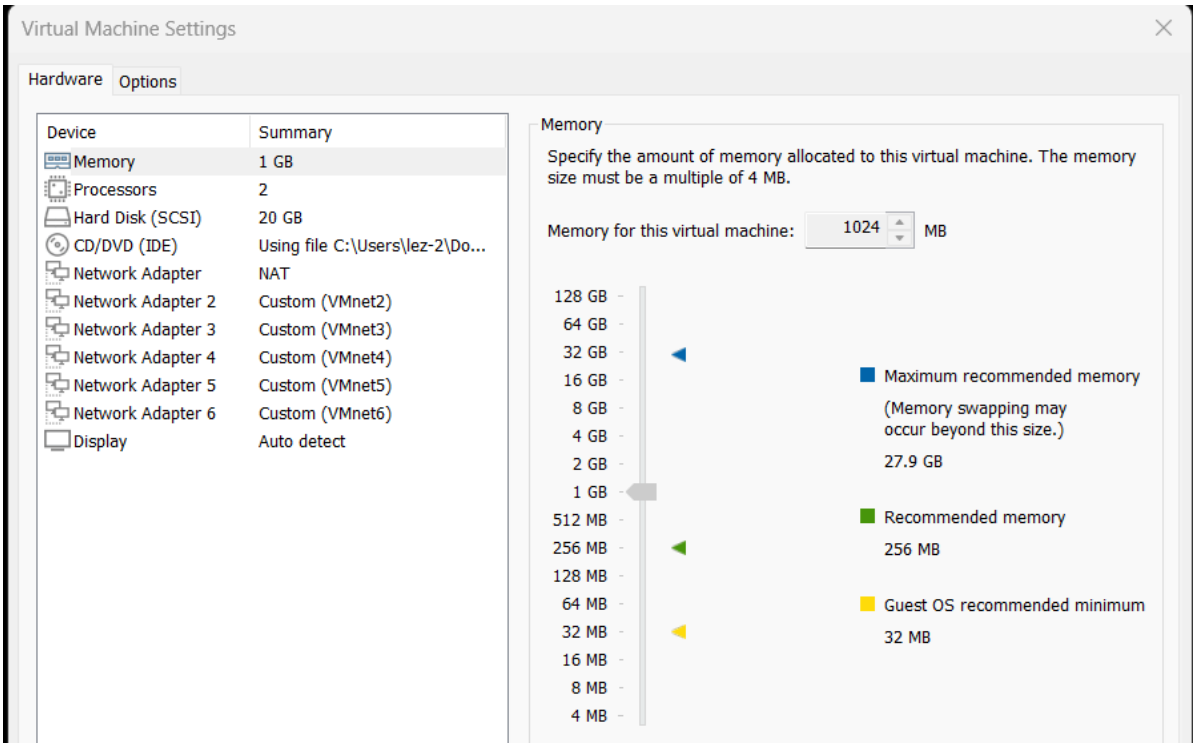
Ubuntu Server VM Configuration



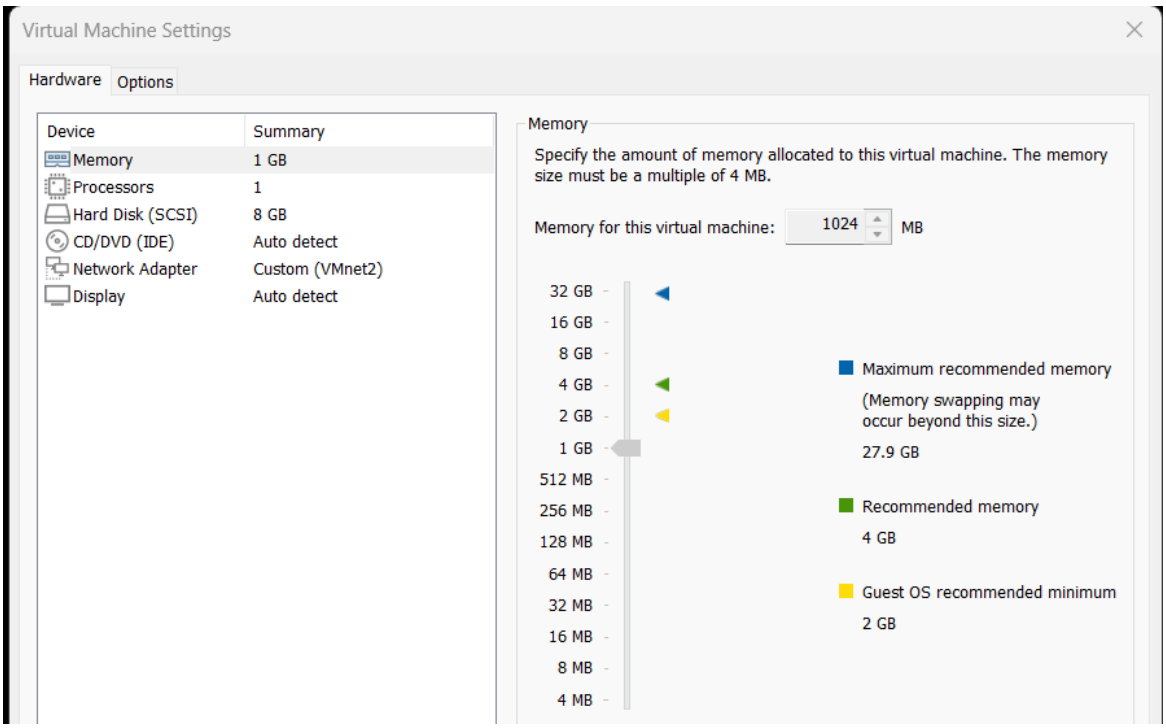
Security Onion VM Configuration



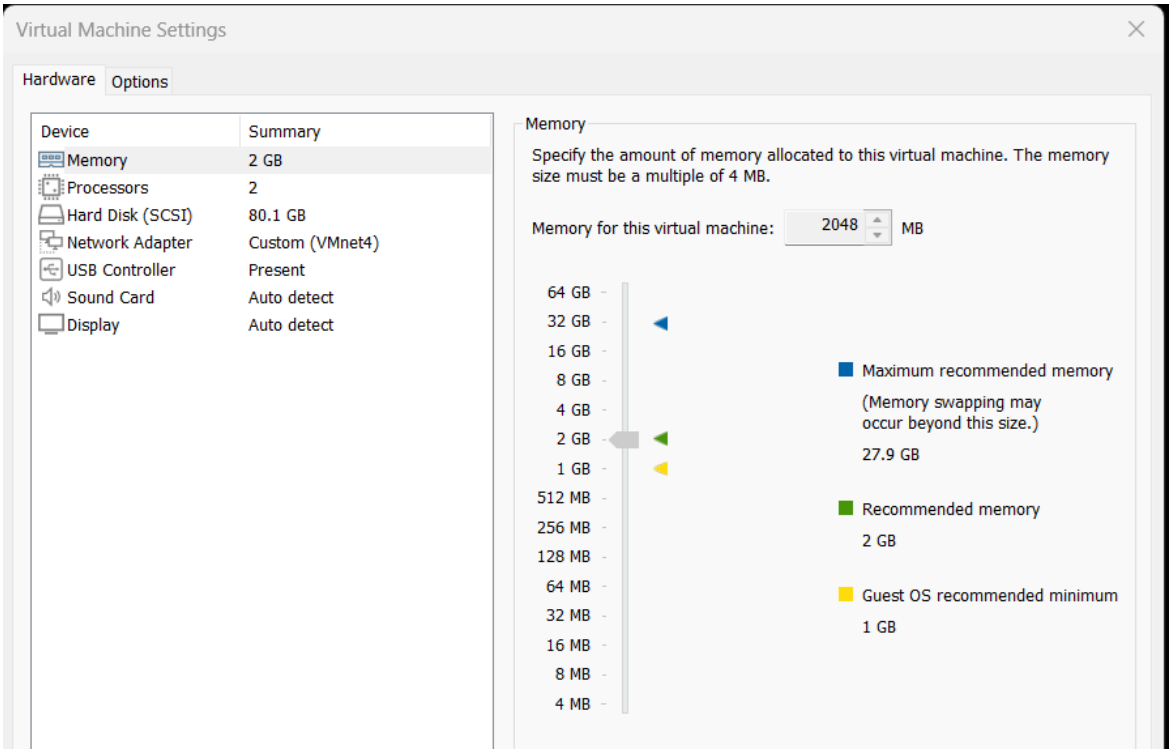
Pfsense VM Configuration



Matasploitable 2 VM Configuration

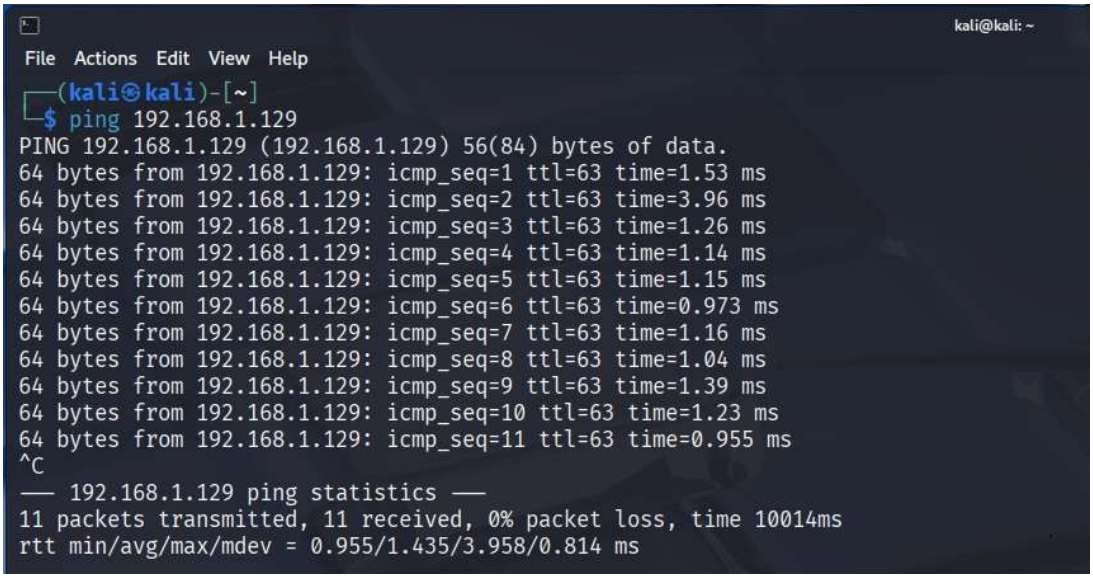


Kali Linux VM Configuration

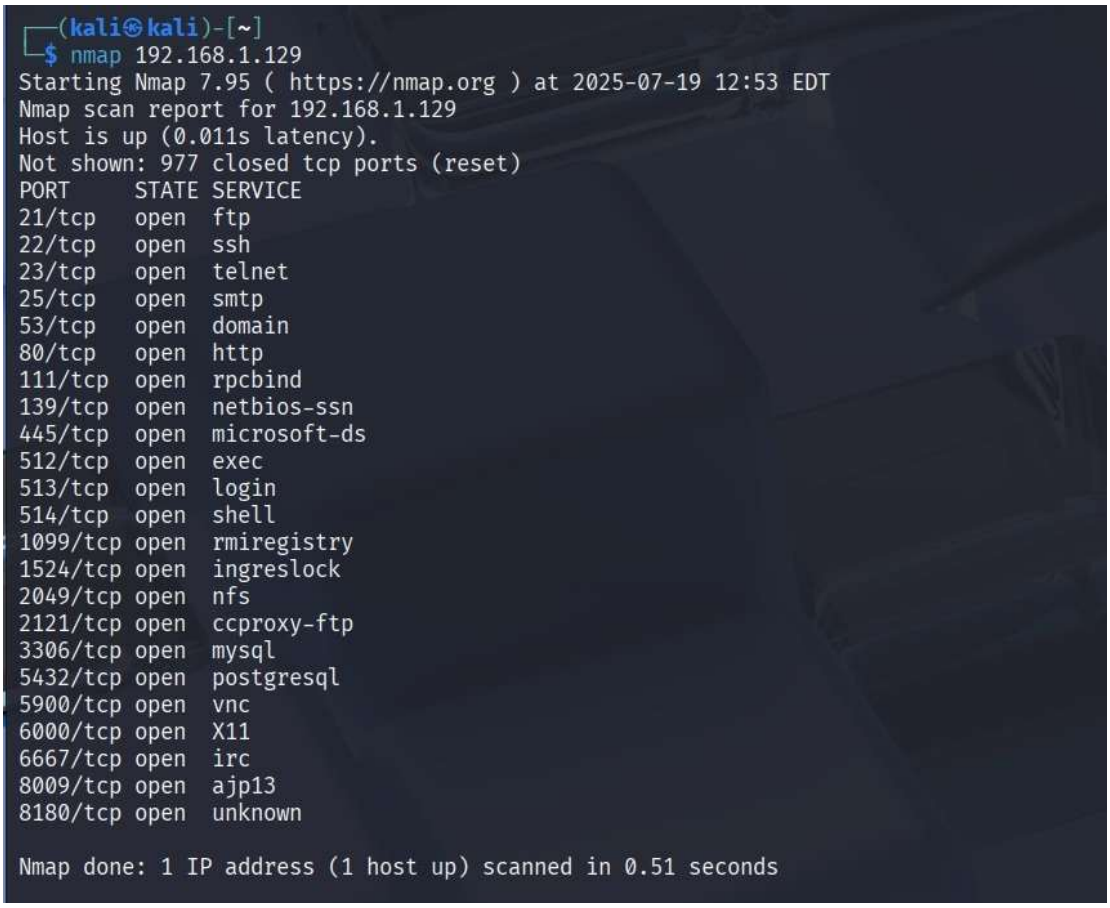


Appendix B – Kali Linux

Ping Sweep

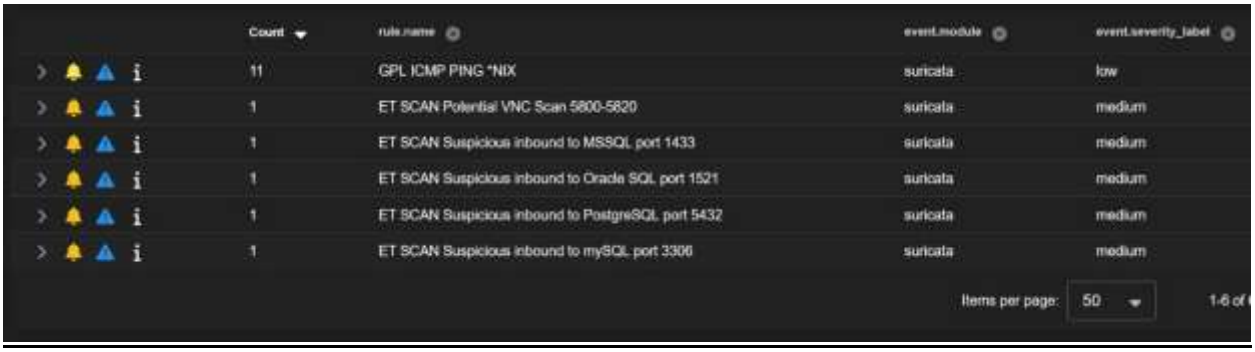


Nmap Scan



Appendix C – Security Onion

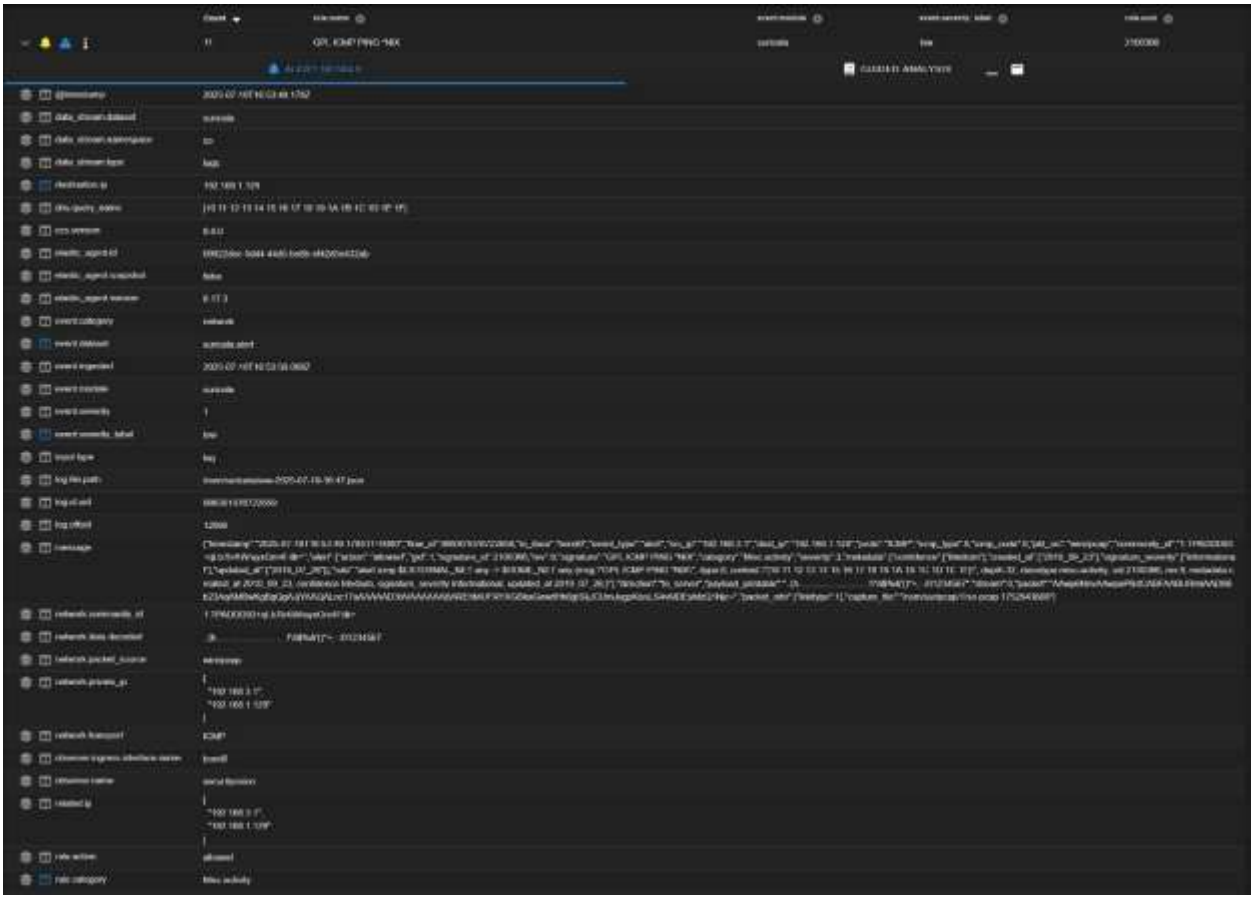
Ping and Nmap Scan Alerts



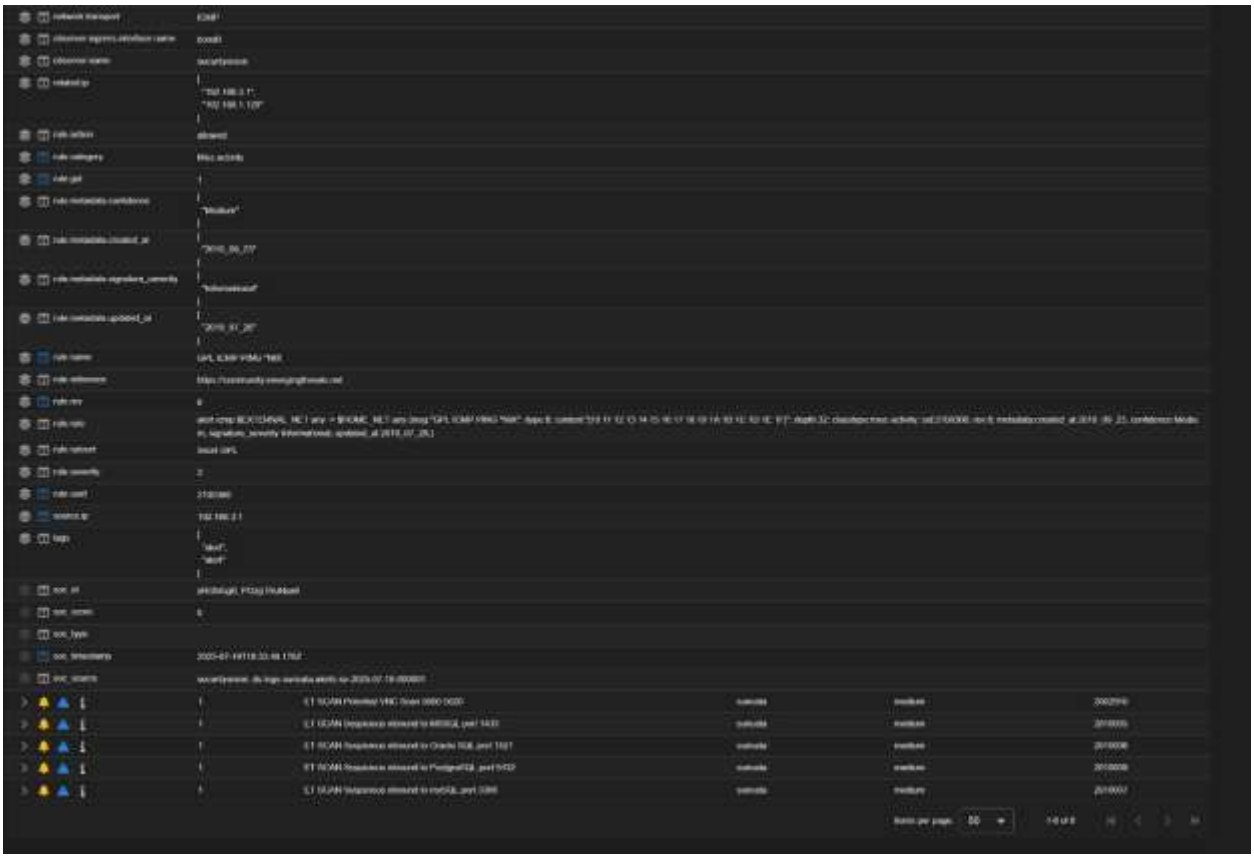
	Count	rule.name	event.module	event.severity_label
>	11	GPL ICMP PING *NIX	suricata	low
>	1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium
>	1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
>	1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
>	1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
>	1	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium

Items per page: 50 1-6 of

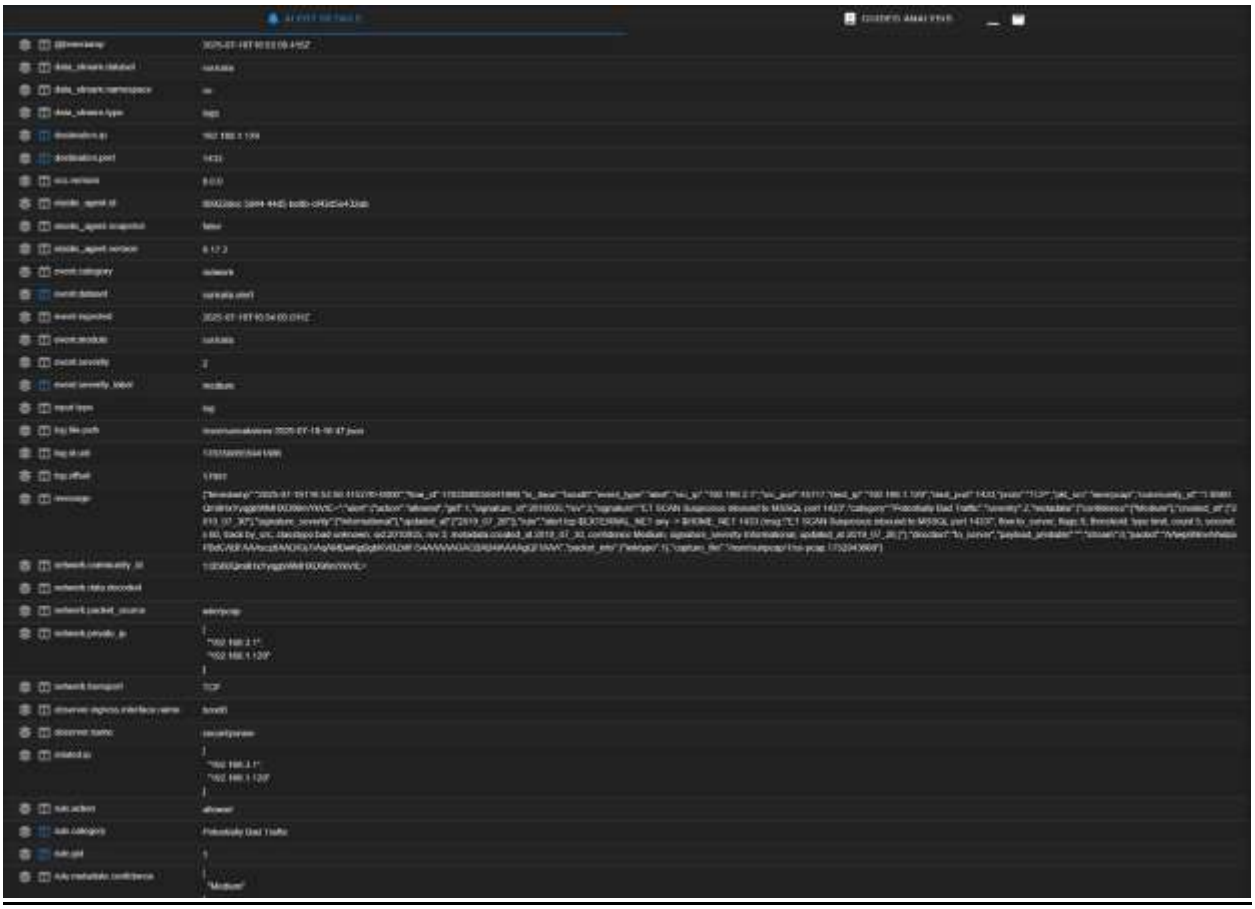
Ping Scan Info 1



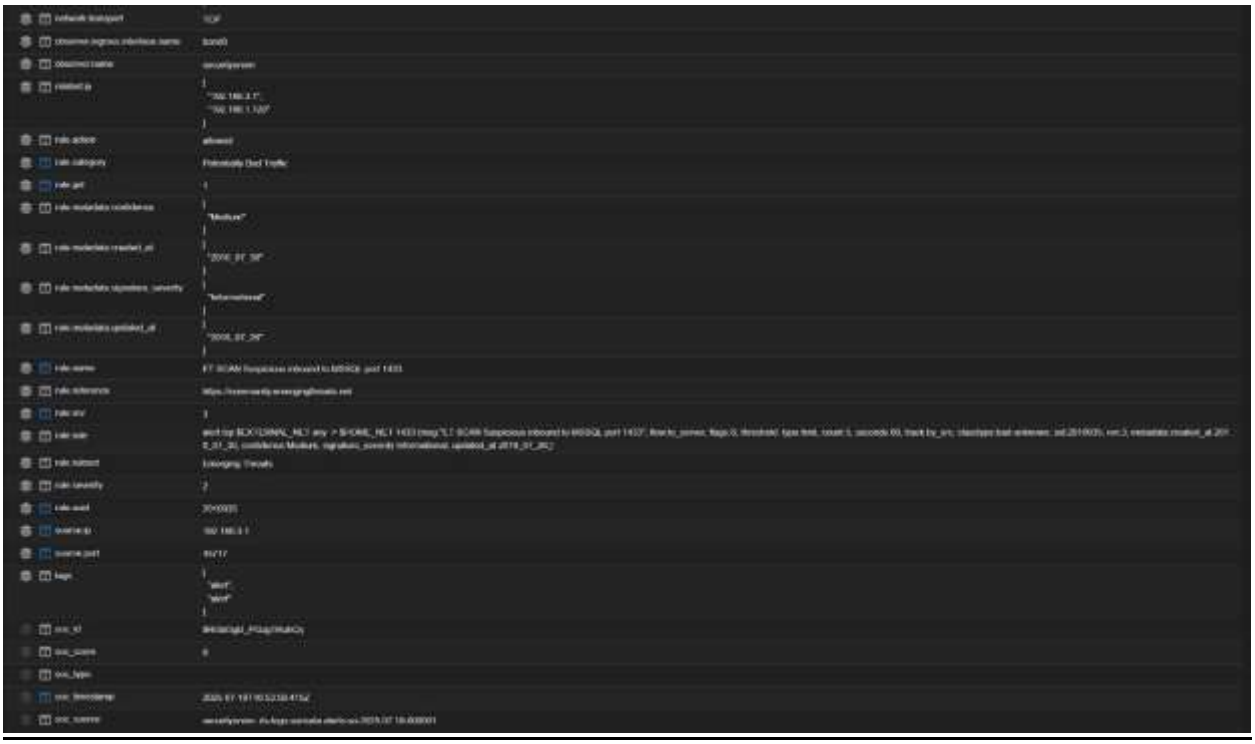
Ping Scan Info 2



Nmap Scan Info 1

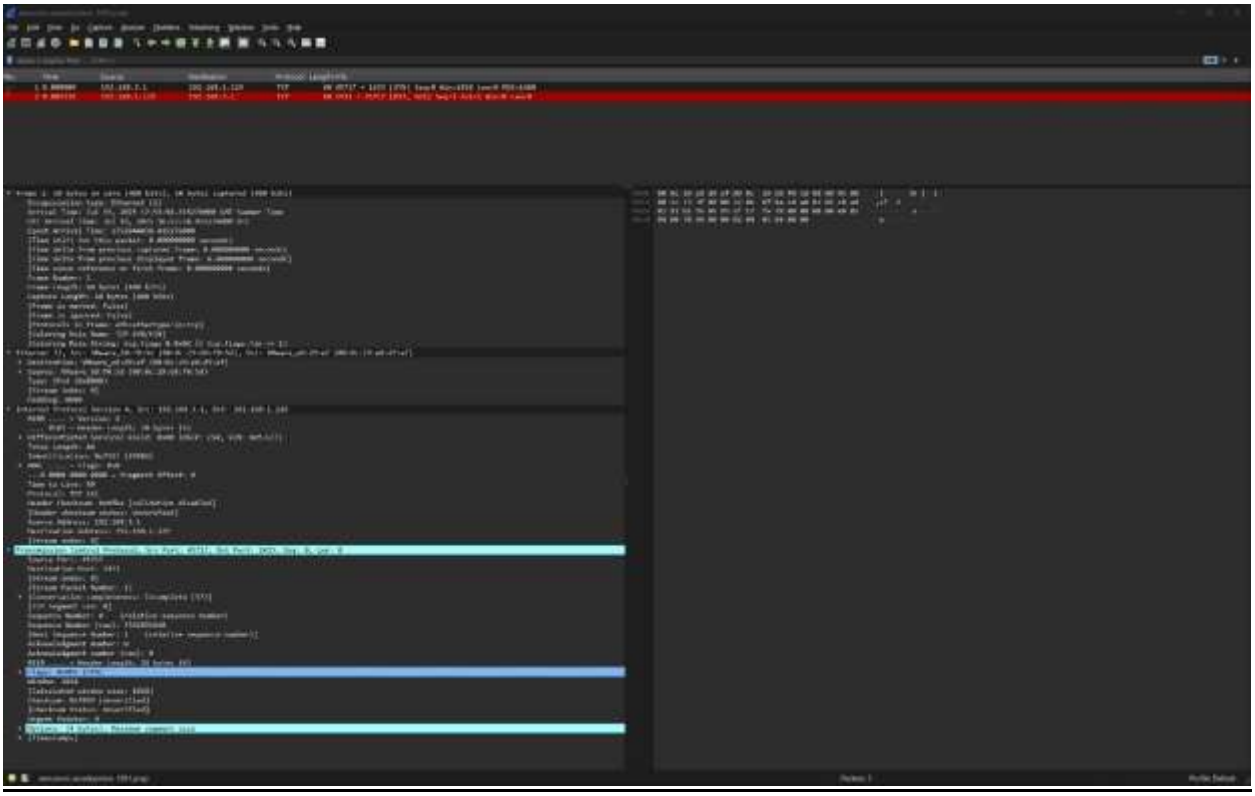


Nmap Scan Info 2

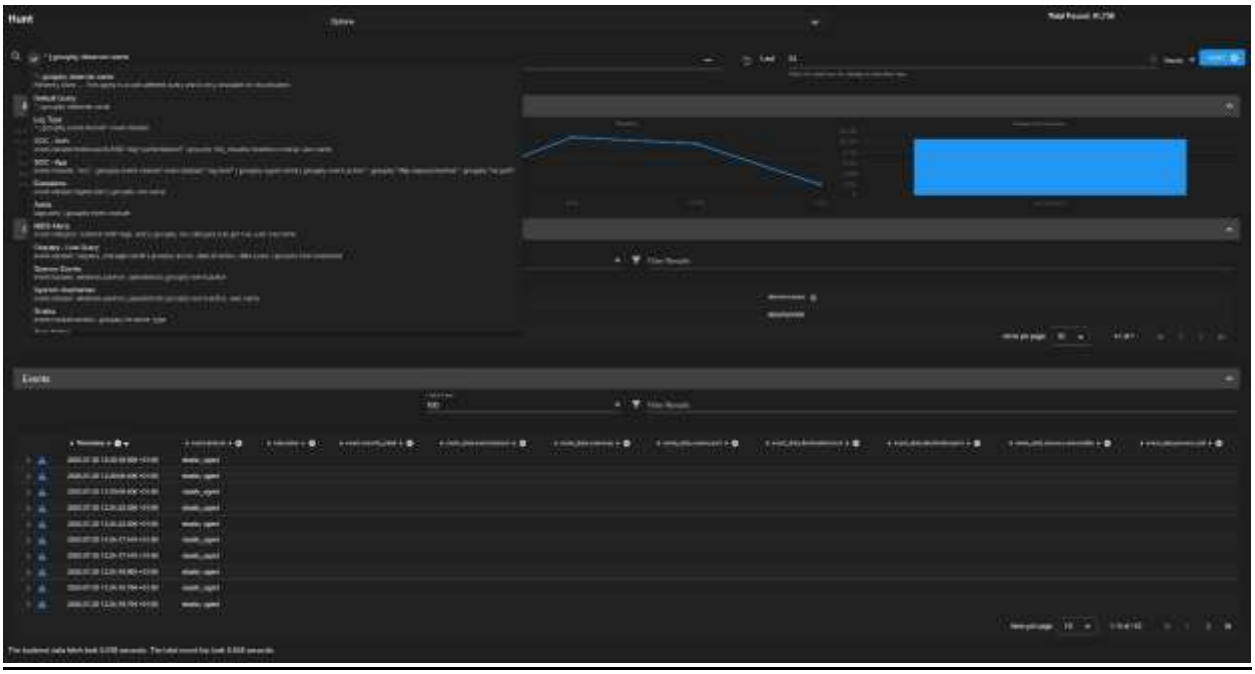


Security Onion Investigation - Pcap

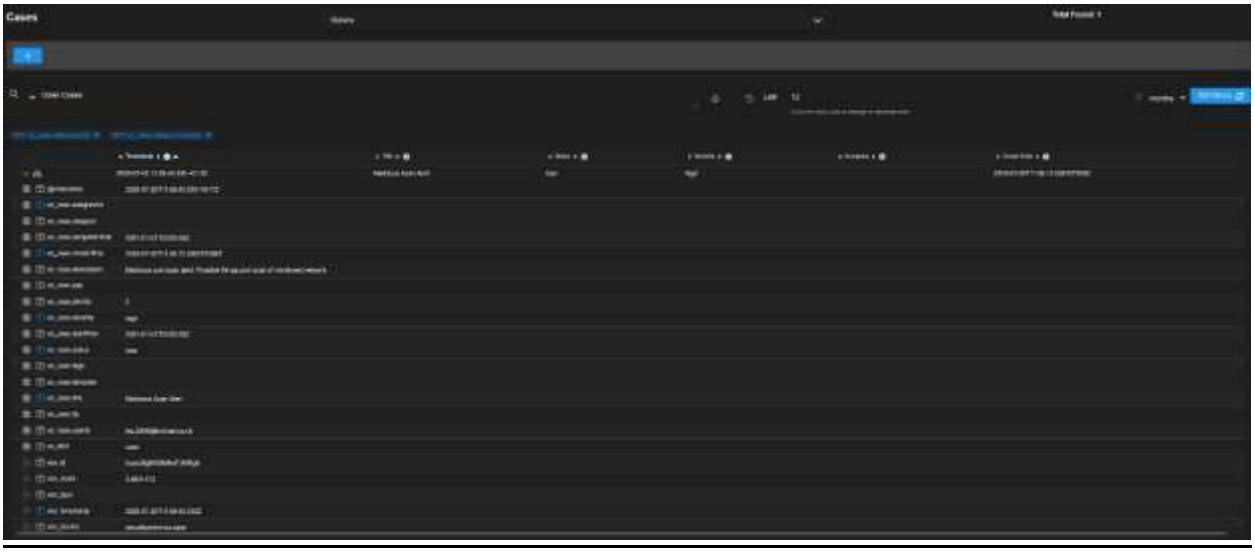
Security Onion Investigation - Pcap - Wireshark



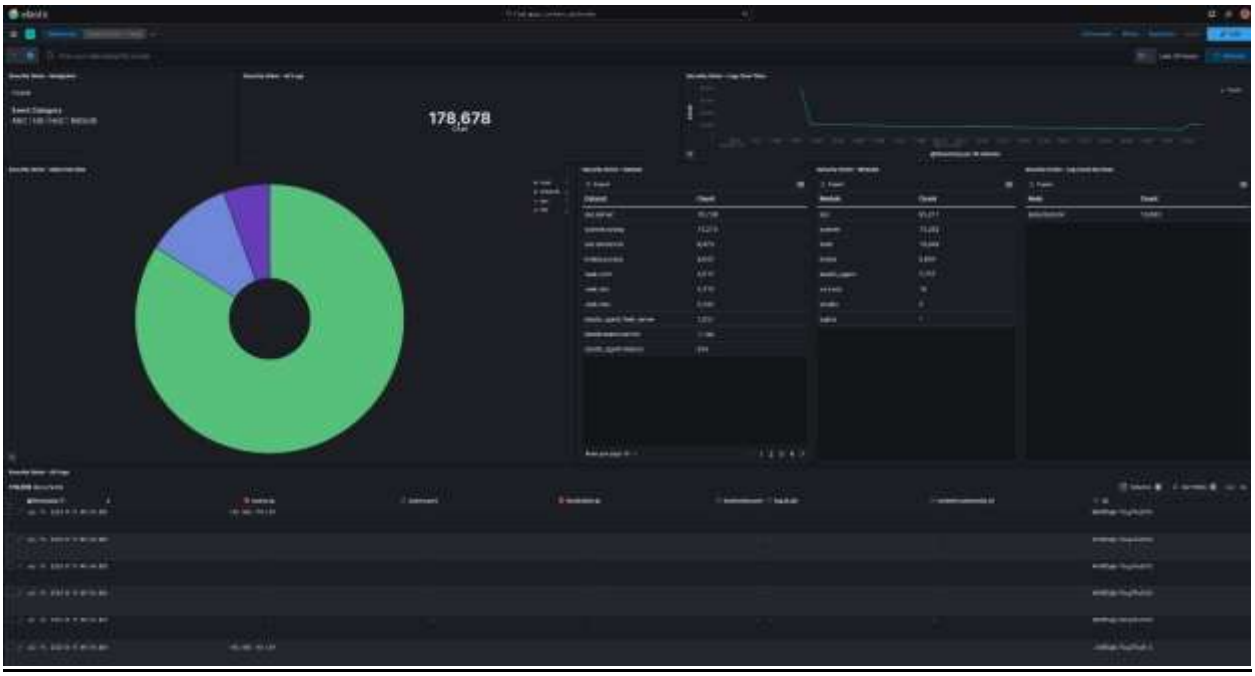
Security Onion Investigation – Hunt



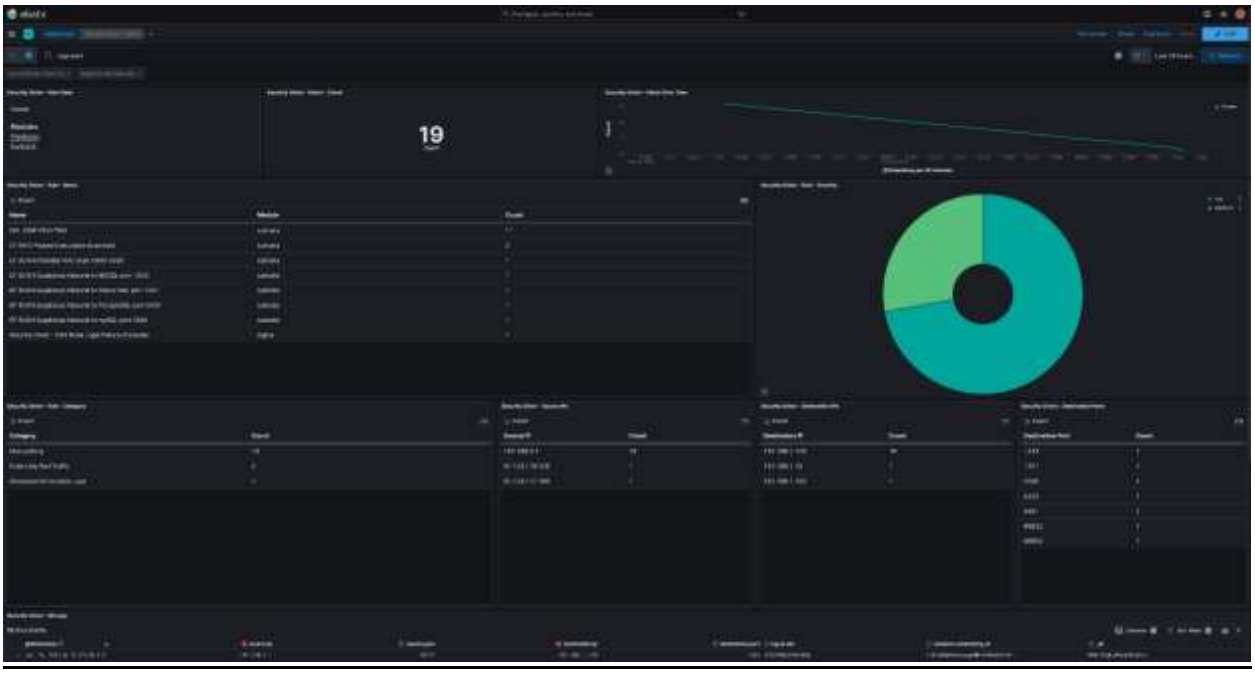
Security Onion Investigation – Case



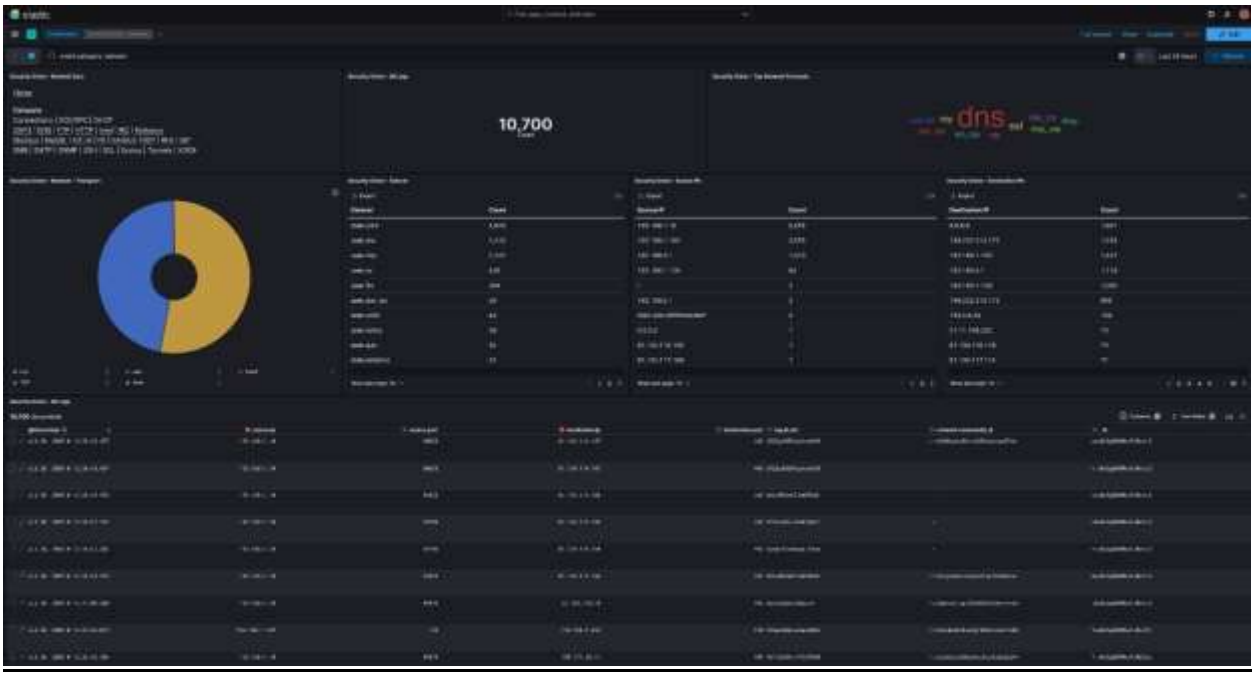
Security Onion – Kibana – Home



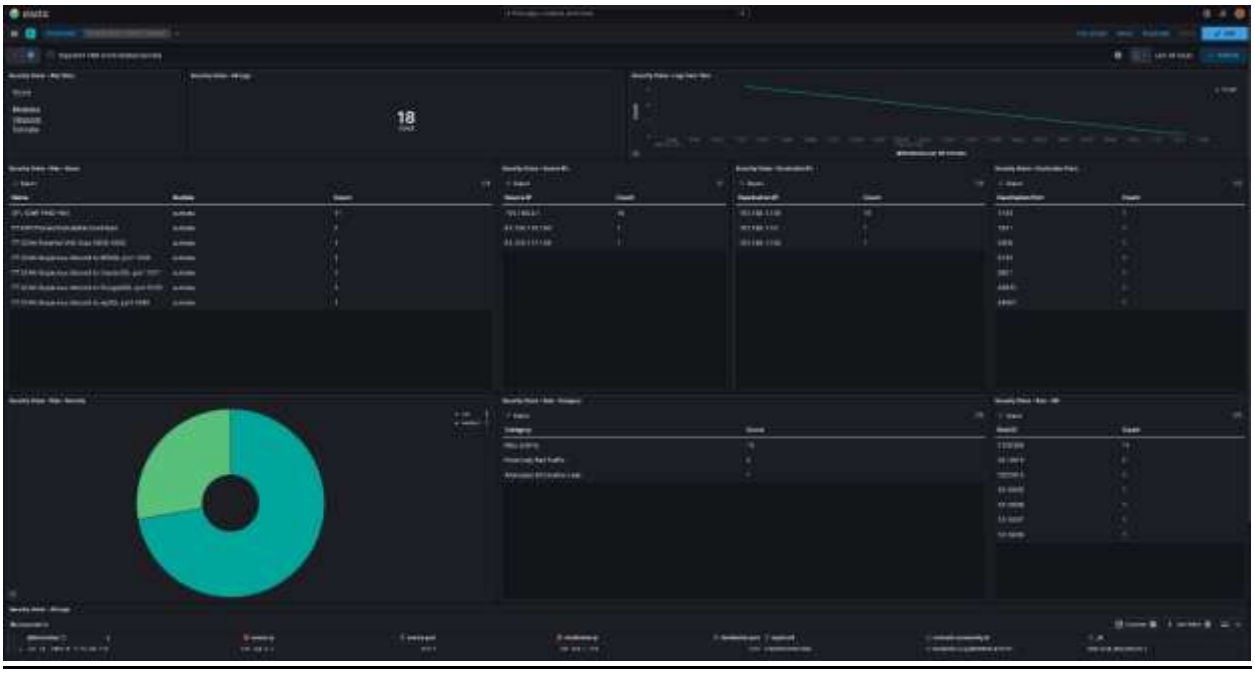
Security Onion – Kibana – Alerts



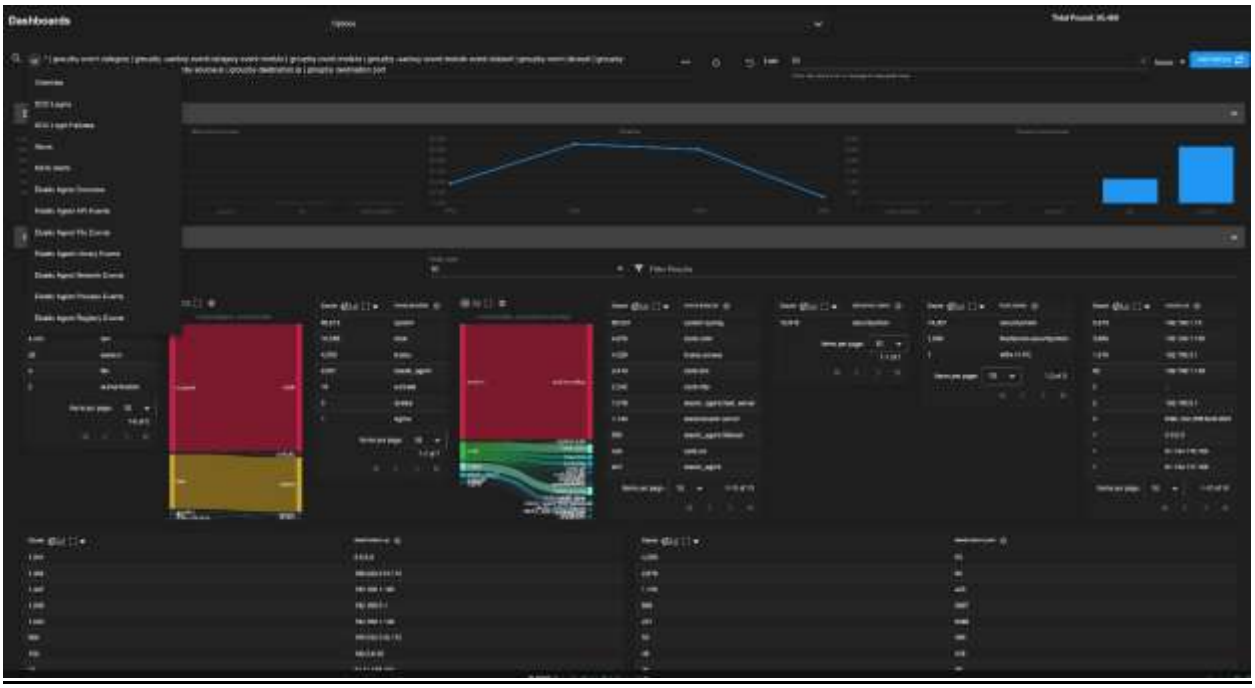
Security Onion – Kibana – Network



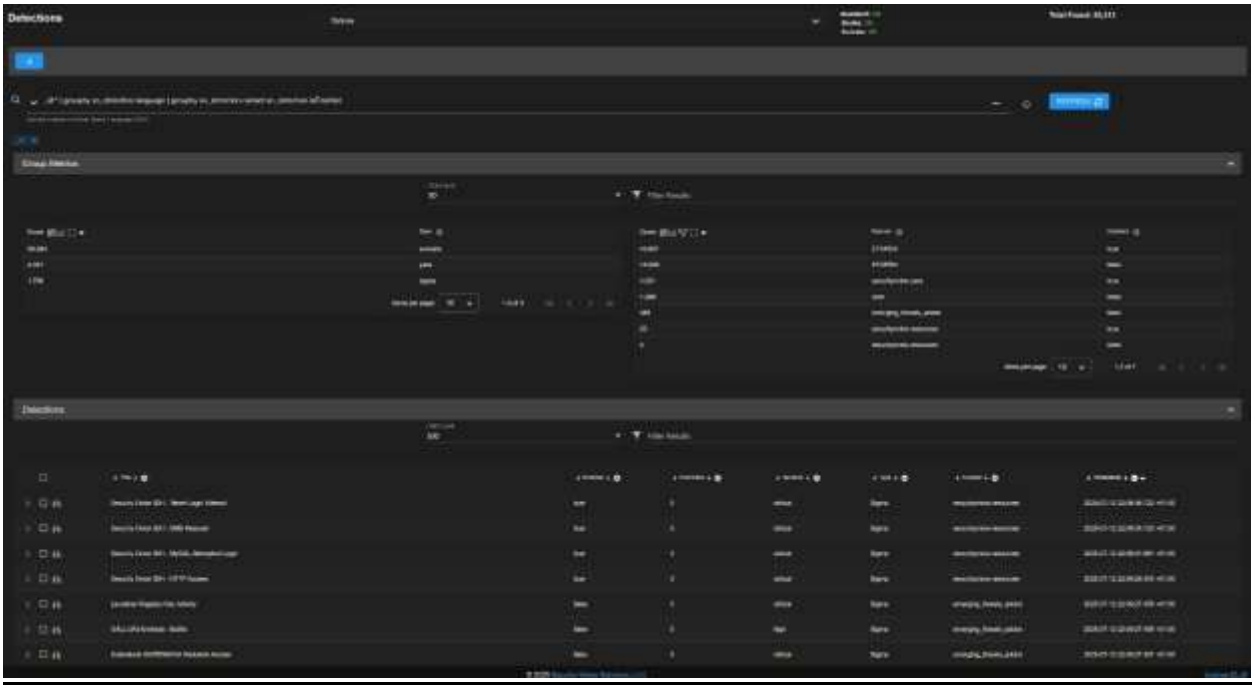
Security Onion – Kibana - Suricata



Security Onion Dashboard

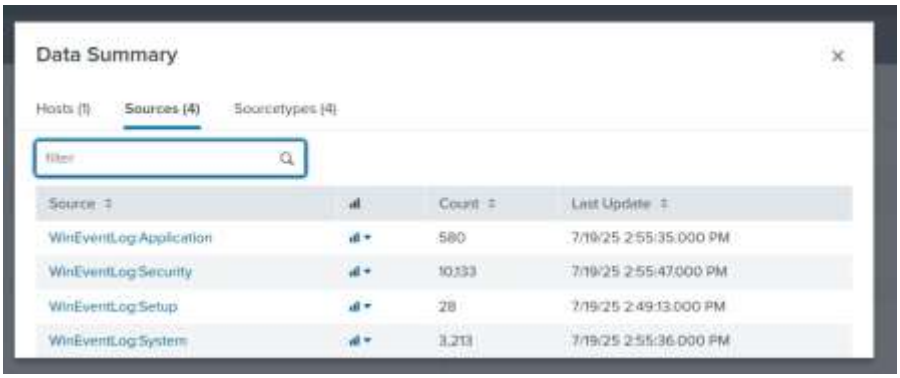


Security Onion Dashboard – Category Filter

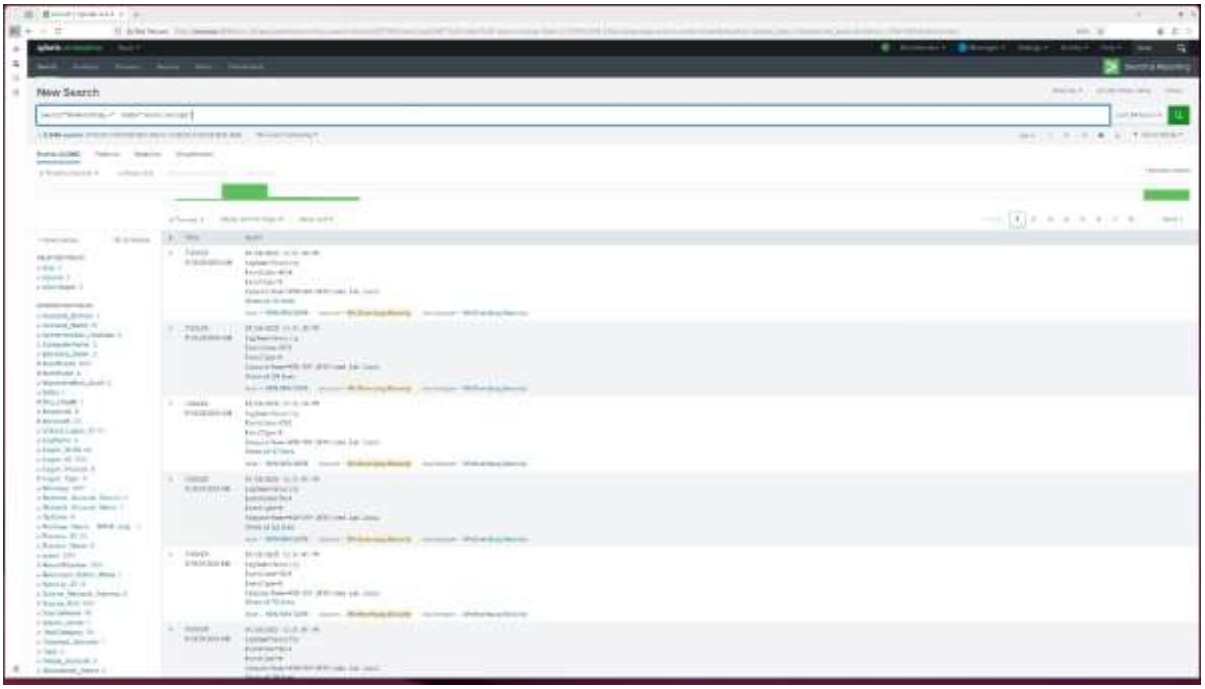


Appendix D – Splunk

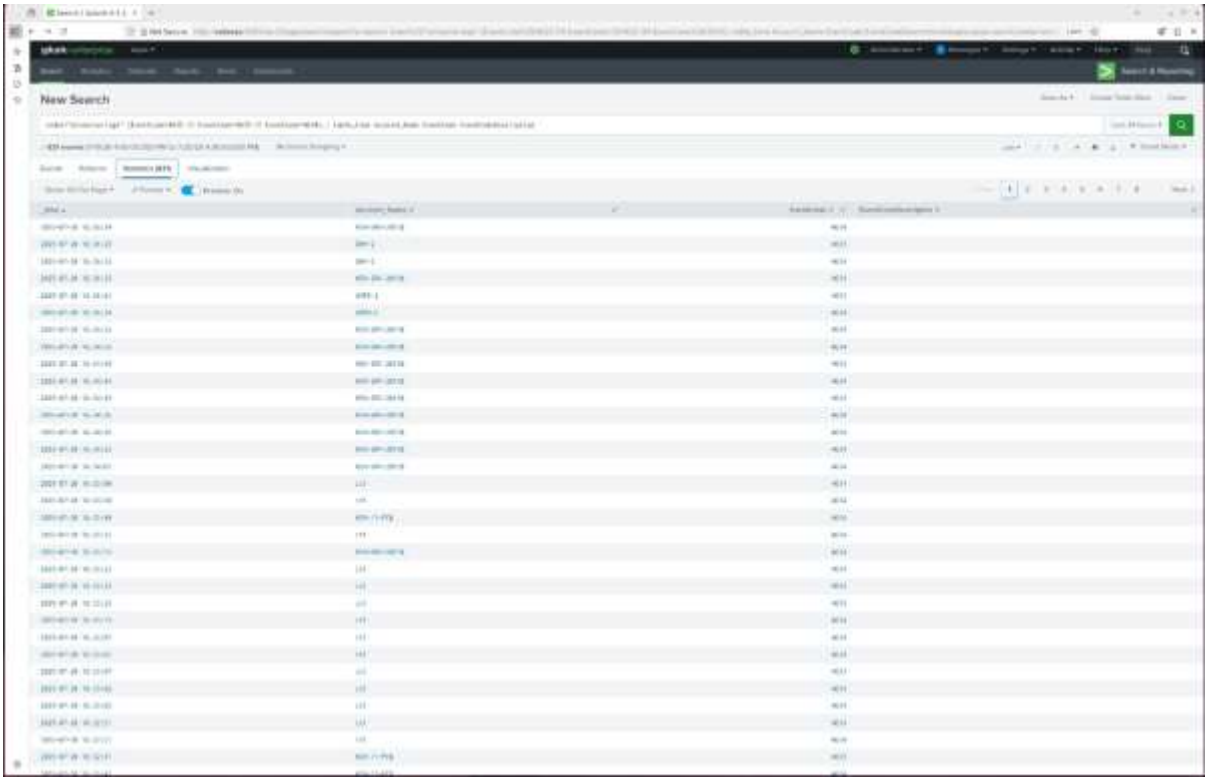
Splunk Log Source Type



Splunk Search Filtering



Splunk Log User Account Access Monitoring



Splunk Log Brute Force Detection