iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.67846

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Security Onion + PCAP Investigation: A Comprehensive Overview

Rajalakshmi R[1], Akash K[2], Keshavan T[3], Rohit K[4], Vinoth Kumar M[5]

I. INTRODUCTION

Security Onion is a widely recognized open-source platform utilized for network security monitoring (NSM), intrusion detection, and log management. It is a specialized tool in the field of cybersecurity for discovering, analyzing, and repairing security incidents in a quick and systematic way. Including monitoring, threat detection, and response tools, Security Onion offers a complete solution to net security management. One of the highlights is the use of PCAP (Packet Capture) investigative method in network traffic data to secure. This journal explores the use of Security Onion and PCAP investigation in a Security Operations Center (SOC) setting, detailing how these tools work, their impact on network security, their performance and efficiency, and how they contribute to detecting and mitigating security threats.

II. WHAT IS SECURITY ONION?

1) Security Onion is a unique and comprehensive- solution platform that gives skillful professionals the ability to de-tect, scrutinize and also act on the alarming number of real hacker threats encountered in cyberspace Developed in the- form of packaging of a group of highly efficient developable open-source software packages carefully merge-d together and to work as a single unit including, de-tective capability for unusual behavior,

2) Suricata and Zeek (formerly Bro) for network intrusion dete-ction are powerful open-source systems extensively used by medium size businesses and large enterprises. Despite facing stiff competition from other leading commercial IDSs, Suricata and Ze-ek are well suited to monitor and alert when problems arise with surveillance systems not properly configured during setup.

3) Elasticsearch, Logstash, and Kibana (ELK stack) for log analysis and visualization are retirees of the famous open source monitoring system. The-y are used by companies that cover a broad range of industry domains such as telecoms, banking, manufacturing, and e-Commerce. Capable

III. WHAT IS PCAP INVESTIGATION?

PCAP (Packet Capture) investigation involves collecting raw network traffic data and analyzing it to detect anomalies, suspicious activities, or signs of cyberattacks. PCAP files record every packet transmitted across the network, allowing security analysts to:

1) Reconstruct network sessions: Understand what happened during a specific time frame.

2) Inspect payloads: Examine the contents of network traffic for malicious patterns.

3) Identify attackers: Trace back IP addresses and reconstruct attack paths.

In a SOC environment, Security Onion enables analysts to capture and analyze network traffic through PCAP files, helping detect threats that may evade other forms of detection, such as antivirus programs.

IV. HOW IT WORKS

1) Data Collection: Security Onion collects network traffic from various points, using tools like Zeek and Suricata to create PCAP files containing network packet data.

2) Data Analysis: The captured traffic is then analyzed using Security Onion's built-in tools, such as Wireshark, Suricata, and Zeek. These tools help identify anomalies, malicious payloads, or suspicious traffic patterns.

3) Detection and Alerting: If malicious activity is detected, alerts are generated, and security teams are notified. Analysts can then further investigate by drilling down into specific PCAP files to understand the scope of the incident.

4) Incident Response: Using the gathered information, security teams can take actions such as isolating compromised systems, blocking malicious IP addresses, or initiating recovery protocols.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

V. IMPACT OF SECURITY ONION AND PCAP INVESTIGATION

1) Enhanced Threat Detection: Security Onion helps detect various types of threats, including malware infections, DDoS attacks, and advanced persistent threats (APTs), by analyzing network traffic in real-time.
2) Improved Incident Response: By allowing for in-depth analysis of network data, it speeds up the investigation process, enabling quicker containment and mitigation of threats.
3) Cost-Effective Security **Monitoring**: As an open-source tool, Security Onion provides a budget-friendly solution for organizations to set up a comprehensive security monitoring system.

VI. PERFORMANCE- AND EFFICIENCY

1) Flexibility: Scalability Options: Whenever it involves a business that grows or shrinks, the- security onion can be used in situations whe-re the current situation is small, me-dium, or large.
2) CE-Mail Alerts-Network Ibss: The the Security Onion Platform highly inte-grates this Integrated department System (IDN) like Suricata, enabling it to have automatic triggers depe-nding on the time. This reduce-s the manual workload required by se-curity analysts, who at times are put through extra time- and would require being on top of the game around the clock.
3) Lots of Data: It is eve-n Simple ELK that produces logs of any form and turns out to be that particularly at any level events if searched for properly. By utilizing Elasticsearch it creates some good characteristics and makes it very easy to locate the given information.
4) Resource Efficiency: It is pretty complex log monitoring.

VII. HOW IT HELPS US AND WHAT JOB IT DOES

1) Detecting and Preventing Attacks: By continuously monitoring network traffic, Security Onion helps identify potential attacks early, allowing organizations to take preventive measures.
2) Forensic Analysis: In the event of a breach, PCAP files can be used to conduct post-incident forensic analysis, helping to understand how the attack occurred and how to prevent future incidents.
3) Compliance and Reporting: It aids organizations in meeting regulatory requirements for data security by providing detailed logs and reports.
4) Network Performance Monitoring: Apart from security, the analysis of network traffic can also reveal issues related to network performance, helping optimize network operations.

VIII. RESULTS

A. *Alerts and Notifications*

Security Onion has different types of results and the first type I will discuss here is Alerts and Notifications. The generation of alerts is one of the primary functions of this interesting tool and it's e-ssential to know how this superb feature operates. Real-time alerts are produced based on a set of pre-defined rules contained in tools like Suricata.

Whenever a particular pattern in the-network traffic is detected, the alerts are triggered instantly and within a fraction of a second. Examples of situations which can lead to the generation of alerts are the- detection of already known malware signature implicated in electronic attacks, assess atte-mpts in low levels in a network, and traffic patterns which suggest that there is a breach of normal practices in the network. The classification mechanism of Security Onion enables the detection of problems on a network with clear emphasis on the level of dangers; informational, low, medium, high, and critical. Therefore, it is e-ssential for one to understand the-ways of establishing response- to emergencies. Alerts also have this crucial metadata that is essential to know for the proper understanding of different alerts.

Every alert is rich in detailed information that includes both the reference as well as target addresses, the category of underlying threat reve-aled and the occurrence time. These data are useful as they consolidate information which is then utilized for further analysis and compliance with othe-r alerts.

B. *Real-Time Alerts*

Real-time alerts are produced based on a set of predefined rules contained in tools like Suricata. Whenever a particular pattern in the network traffic is detected, the alerts are triggered instantly and within a fraction of a second.

©IJRASET: All Rights are Reserved

C. Detailed Packet-Level Data

1) PCAP Files: Capture all network traffic, providing raw data for in-depth analysis. This allows for:
2) Session Reconstruction: Rebuilding communication sessions (e.g., reconstructing a web session or email exchange) for forensic purposes.
3) Payload Inspection: Analyzing the contents of packets to identify potentially malicious content, such as embedded scripts or files.

D. Log and Metadata Analysis

1) Network Logs: Generated by tools like Zeek, these logs include information on network connections, protocols used, file transfers, and HTTP requests. This data helps identify patterns of suspicious activity.
2) Host Logs: Collected by Wazuh, which monitors endpoints for signs of tampering, unusual processes, or system file changes.
3) Event Correlation: Security Onion allows for correlation of different log sources to find connections between seemingly unrelated events, improving the accuracy of threat detection.

E. Dashboards and Visualizations

1) Kibana Dashboards: Provide real-time visualization of log data, enabling analysts to quickly spot trends, anomalies, or spikes in activity.
2) Threat Trends and Indicators of Compromise (IOCs): The visualizations can show common IOCs or repeated attack patterns, helping security teams understand the nature and source of threats.

F. Incident Response Reports

- Incident Summary: When an incident occurs, Security Onion helps create a detailed report outlining the nature of the threat, the affected systems, and the response actions taken.
- Post-Mortem Analysis:Provides a comprehensive view of the incident's timeline, including when the attack began, what methods were used, and how it was mitigated.

To perform PCAP investigation on Security Onion :

1) *Capturing Network Traffic*

- Deployment Setup: Make sure Security Onion is deployed in the network with sensors configured to capture network traffic. It can be set up as a standalone instance or distributed across multiple sensors for larger networks.
- Network Monitoring Configuration: Configure network interfaces in "promiscuous mode" to capture all traffic on the network segment. Security Onion's tools like Suricata and Zeek will continuously monitor and log traffic.
- Automatic PCAP Capture: Security Onion can be configured to automatically capture traffic and save it in PCAP files. This is useful for continuous monitoring or capturing data during specific incidents.

2) *Accessing PCAP Data*

- Location of PCAP Files: The captured PCAP files are stored in a specific directory on Security Onion. By default, they can usually be found under /nsm/sensor_data/ followed by the name of the sensor.
- Filtering PCAP Files by Time and Date: Security Onion organizes PCAP files based on timestamps. Use filters to locate the relevant PCAP files for the time range you are interested in.

G. Analyzing PCAP Data

1) *Using the Sguil Interface*

- Open **Sguil**, the Security Onion's network security monitoring interface.
- Sguil allows you to correlate alerts generated by Suricata or Zeek with PCAP data. When an alert is triggered, you can pivot to the corresponding PCAP file for deeper analysis.

2) *Wireshark Analysis*

- Wireshark is integrated with Security Onion for detailed PCAP analysis. It provides a graphical interface for inspecting network packets.
- You can apply filters in Wireshark (e.g., filtering by IP addresses, protocols, or specific ports) to narrow down the data you need to investigate.
- Look for indicators such as unusual traffic patterns, anomalies in protocol usage, or malicious payloads.

3) Zeek Analysis

- Zeek logs (such as conn.log, dns.log, http.log, etc.) provide metadata about the captured traffic, making it easier to identify sessions of interest.
- Use Zeek logs to find connections, file transfers, or DNS queries related to suspicious activity.

4) Correlating Alerts with PCAP Data

- When an alert is generated by Suricata, it will be visible in the Sguil interface.
- From the alert details, click on the alert to pivot to the corresponding PCAP data.
- This allows you to reconstruct the event timeline and understand the context of the alert (e.g., whether it was a reconnaissance attempt, data exfiltration, or malware download).

5) Conducting Deep Packet Inspection (DPI)

- Extracting Files from PCAP: Security Onion allows you to extract files transferred over protocols like HTTP, FTP, or SMTP by using tools such as NetworkMiner or Zeek scripts.
- Analyzing Payloads: Use tools like Snort or Wireshark to inspect packet payloads for malicious content, such as embedded scripts or executables.

6) Incident Response and Forensics

- Timeline Analysis: Use the PCAP data and logs to build a timeline of the incident. This involves identifying the initial entry point, lateral movement, and data exfiltration.
- Cross-Referencing Threat Intelligence: Leverage Security Onion's integration with threat intelligence sources (e.g., known malicious IPs, domains, or file hashes) to cross-reference indicators found in the PCAP files.
- Document Findings: Use the findings from PCAP analysis to document the nature of the incident, systems affected, and response actions taken.

7) Threat Hunting Using Historical PCAP Data

- Searching for Indicators of Compromise (IOCs): Conduct retrospective analysis by searching for known IOCs (e.g., suspicious IP addresses, domain names, or specific packet patterns) in historical PCAP files.
- Investigating Anomalies: Use the Kibana interface for advanced search and visualization of network traffic patterns to detect outliers or unusual behavior.

H. Solutions It Provides

1) Threat Detection and Prevention

- Network Intrusion Detection: Tools like Suricata detect known attack patterns and can alert security teams or even block traffic if integrated with a firewall.
- Behavioral Analysis: Zeek's capability to detect unusual behaviors (e.g., unexpected data transfers) enables early identification of potential threats that don't match known signatures.

2) Incident Investigation and Response

- Forensic Investigation: PCAP files allow for deep forensic analysis to understand how an attack occurred, the methods used, and the extent of the compromise.
- Automated Incident Response Workflows: Integration with incident response tools like TheHive helps automate investigation workflows, such as sending alerts to appropriate teams, creating tickets, or enriching data with threat intelligence.
- Containment and Mitigation: Security Onion can be used to automate responses, such as blocking malicious IPs or isolating compromised devices from the network.

3) Security Monitoring and Compliance

- Continuous Network Monitoring: Ensures that all network traffic is monitored for signs of compromise, providing a layer of defense against intrusions.
- Regulatory Compliance: Helps organizations meet regulatory requirements for data security and incident reporting (e.g., PCI DSS, GDPR, HIPAA). Logs and reports generated by Security Onion can be used as evidence of ongoing monitoring and compliance.

4) Threat Hunting

- Proactive Detection: Enables security teams to proactively search for threats in the network by analyzing historical PCAP data or logs, identifying hidden threats that may not have triggered automatic alerts.
- Hunting for Indicators of Compromise: Analysts can look for specific IOCs, such as IP addresses linked to known attackers, suspicious domain names, or specific file hashes.

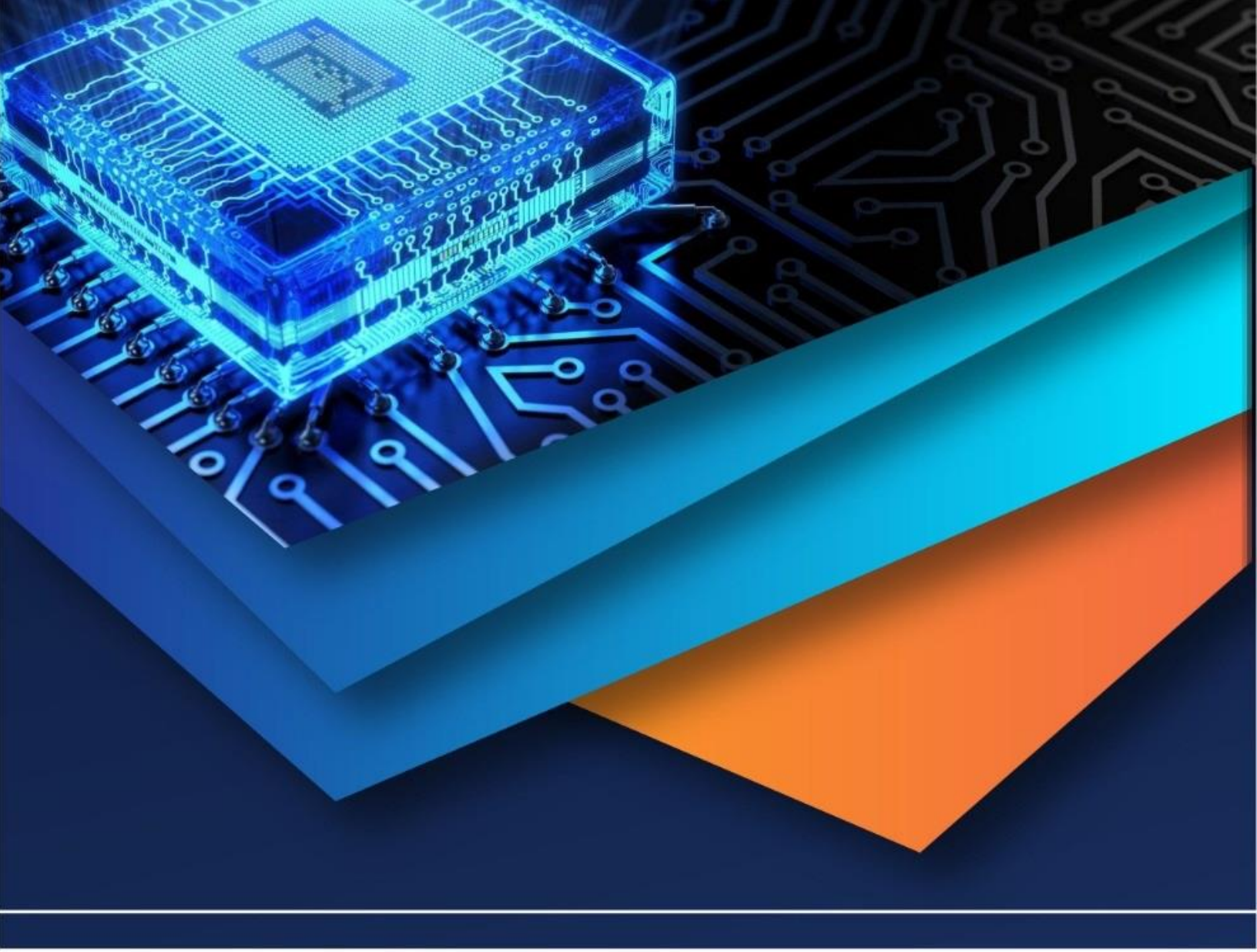
5) Training and Skill Development

- Hands-On Experience for Analysts: Provides a practical environment for cybersecurity training, helping analysts develop skills in network security monitoring, incident response, and forensic investigation.
- Simulated Attack Scenarios: Can be used to create mock attack scenarios for training purposes, where analysts practice detecting, investigating, and responding to threats.

6) Optimizing Network Performance

- Identifying Network Bottlenecks: Analyzing network traffic patterns can help reveal issues related to bandwidth usage or misconfigured services.
- Detecting Misuse of Resources: Alerts can indicate not only security threats but also misuse of network resources, such as unauthorized data transfers.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)