A Review on Security Onion Tools for Intrusion Detection

MAHAWISH, MOBEEN, BUSHRA, MISBAH PERVEEN, SOOMAL FATIMA, MAHAM*

Dept. of Software Engineering Bahria University Karachi Campus
*Dept. of Software Engineering Bahria University Karachi Campus

***Abstract*—**

Intrusion detection has always been the area of interest for network analysts as well as the research community. Especially with the adoption of sophisticated techniques employed by malicious adversaries, it is becoming more difficult to detect and block the malware and threat activities within a Cyber-Physical System (CPS). To better perform security jobs and acquiring network monitoring data, the Security Operations analyst focuses on the tools advantageous for Network Security Monitoring (NSM) which collects, maintains, process, and present the data helpful for detection of intrusions. The Security Onion (SO) is a proper low-cost solution for NSM, It is a Linux based distribution for managing logs, security, and provides multiple tools for intrusion detections including Network IDS and Host IDS.

This paper presents a review of Security Onion tools used for analyzing & inspecting network packets helpful for security analysts to protect a CPS. We have also reviewed the feature and functionalities of SO in terms of tools used for Host and Network visibilities, Analyst tools, architecture, NSM data types, and performed analysis upon the usage of different IDS tools in the literature.

Keywords—Intrusion Detection, Security Onion,Network Security Monitoring (NSM)

I. INTRODUCTION

The internet has become an essential part of human lives and the use of web applications such as online banking, health care facilities, cloud, online shopping, and data centers, require an efficient security mechanism for computer networks. This means that the internet is a big concern and there is a need to protect data from intrusion and exploitation against vulnerabilities.

An IDS (Intrusion Detection System) is a security management tool used to scan malicious traffic for computer networks [1]. IDS protectsa CPS by providing three major security functions including monitor, detect, and respond to unauthorized and illegal activities [2][3].

Typically, an IDS is divided into two categories including Host-Based (HIDS) and Network-Based (NIDS). The HIDS is responsible for monitoring a particular host or system [2] and avoids intruders to compromise system security policies. HIDS collects data of network events, file systems, and system calls to check whether any inconvenient action has been encountered or not. Detection in intrusion is examined by file system integrity and memory usage [4]. Tripwire [5], USSEC [6] and Samhain [7] are on shelf HIDS

NIDS are deployed to monitor the traffic between all the devices on the network. NIDS works like a bodyguard that monitor both inside and outside of property [2]. It monitors packets, matches patterns from already existing signature attacks, or sometimes statistical analysis to detect unusual behavior. Snort [8], Zeek [9], and Suricata [30] are the instances of open-source network IDS. ML-based methodologies (i.e., Genetic Algorithm, SVM [10], and Artificial Neural Networks [11]) are used to detect zero-day attacks.Similarly, Deep Learning approaches are often used to enhance the performance of anomaly-based IDS using a mimetic classifier [12].

Issues still exist, DDoS (Distributed Denial of Service attack), bypass the IDS filters and attack computer networks [13].

To handle security issues, a more organized and central approach is needed to proactively hunt for malicious threats on the networks. SO [13, 14] is a Linux-based distribution that provides a set of tools that offer log management, network security monitoring, and IDS capabilities for multiple types of HIDS and NIDS.

In this paper, we aim to achieve a cavernous understanding of the functionalities, deployment modes and tools included in the SOdistribution, which consequently makes the detection process more robust and effective.
The rest of the paper is segmented as follows. Section II presents a brief background of security onion.A critical review of existing work is presented in section III.. Section IVdiscusses the deployment methods and types of data, configuration, Host, Network, and Analyst tools.Section V,asimplified SO architecture has been discussed. Lastly, section VI concludes the paper.

II. BACKGROUND

In the Security Onion solution, host security is maintained by OSSEC [6], it performs real-time network analysis by performing functionalities includingsystem Logs, file integrity, and monitoring the policies of network endpoints.

IDS logs and Zeek tool, provide full packet capture, which gives a daunting amount of data to analysts. To handle this extensive amount of data SOintegrates Sguil, Squert, and ELSA.

Sguil Provides Graphical User Interface (GUI) [27],GUI is written in TCL/TK whose main function is to view alerts of Snort or Suricata, OSSEC, Zeek HTTP events, and PRADS alerts [29].

Additionally, Sguil permits ananalyst to query all packets to hunt malicious activity. The Sguildatabase based web application interface is supported by the squert tool. It allows to query Sguil database and provides numerous data visualization such as time series representation, logical and weighted group result sets, and geo-IPP mapping. ELSA is a centralized Syslog framework [37] that provides an asynchronous web-based query interface that normalized logs, and also include tools to show logs, email alerts, organized queries, and graphing.

This section describes the basics of SO, its usage, configuration, and management.

A. Using Security Onion

Gonzales et al. [16] on the behalf of The National University Information Security Lab Environment (ISLE) provides an overview of the virtual testing environment for cybersecurity training assignments. They provide examples of attacks including malware, botnet, and honeypot traffic, etc. The tool used in the proposed framework provides insight and also allow to share of practices adopted in industries. The goal of the paper is to propose a framework for national and academic cyber defense using security onion.

B. Configuring Security Onion

Ashely et al. [18] discussed how to block attacks including SQL Injection (SQLi), Cross-Site Scripting (XSS), and web application attacks using SO. This paper gives several labs that test for various Web application vulnerabilities includes Cross XSS, SQL injection, and OS injections, against a well-known attacks Web application virtual machine called DVWA. The study performed on the behalf of SANS shows the capabilities of SO tools and services to protect an environment.

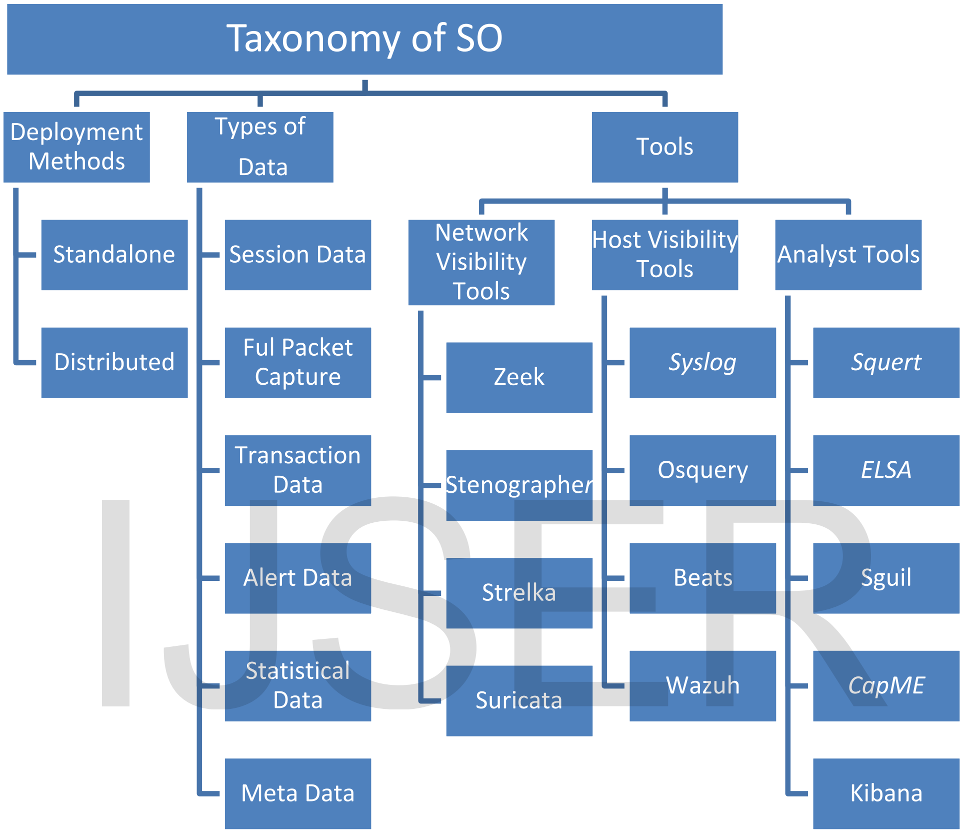
C. Monitoring and Logging

Roger Meyer [19] on behalf of the SANS Institute of InfoSec detects attacks on web applications from log files it allows us to view the detailed analysis of a user’s actions. HTTP files have a complete log of user’s request and response record, by having a record of these logs well-known attacks can be recognized and block against exploitations.

Another Paper provided by Sunil Gupta [20] for the SANS Institute of InfoSec describes the use of SO to detect the network exploitations for effective logging and monitoring. In this paper,the author provided the SO with an appropriate solution for individual entities or groups with minimum. budget and this paper also highlight the advantages provided to security analyst

Hjelmvik Erik [21] also describes the usage of SO for the analysis of network and system intrusions using the provided tool. It explores many activities that gain growing attractiveness with researchers.

D. *Managing Security*



III. TAXONOMY OF SECURITY ONION

This section presents a taxonomy of security onion for understanding its overall architecture that consequently helps in devising a deployment methodology of the SIEM solution in accordance with the needs of a particular cyber-physical system.The taxonomy is broadly based on three main categories including deployment methods, types of data and tools.

A. *Deployment Methods*

The Security Onioncan be deployed in many scenarios such as evaluation and production mode [21] which gives the following deployment options as discussed below:

1) *Standalone*

In this mode, it runs on a single physical machine that has multiple interfaces monitoring different network segments. Easy to use and convenient to monitor single location networks.

2) *Distributed*

It runs on single server machine running components related to a server, the client machines forward queries to the server, all sent queries disseminated to the suitable sensors with the information requested back to the client. All the traffic between client and server is encrypted.

Table 1: Comparison of deployment methods

Deployment Mode	**Scalable**	**Perform- -ance**	**Through put**	**Cost**
Standalone	No	Low	Low	Low
Distribute	Yes	High	High	High

The above table show the comparison of SO deployment methods in terms of scalability, performance, throughput and cost.

A. *Types of NSM data*

NSM tool is software that collects, maintains, processes, and presents NSM data. Network security monitoring data may be classified into the following [34].

1) Session Data

Session data is the summary data that is associated with network conversation. It is based upon the source and destination IPs, ports, and transport layer protocol.

2) Full Packet Capture

Full packet capture or full content data records all network traffic and details exactly what was communicated. The data is written to disk, commonly in PCAP format.

3) Transaction Data

Transaction data lies between session data and full packet capture. It captures the details associated with requests and responses.

4) Alert Data

Alert data is produced by intrusion prevention systems (IPS). Alerts are produced when network traffic matches certainconditions for which IPS are configured to respond.

5) Statistical Data

Alert data can be processed to produce statistical data. e.g.; how many requests per second does this webserver normally receive? How many DNS requests per second are made from inside? How often does a user log into that system?

Are there cycles in data patterns based on time of the day, day of the week, on the day of the month?

6) Meta Data

Metadata is used to augment the NSM data. It is directly collected by Geo-location, reputation scores, and ownerships that are associated with IP addresses.

Each type of data provides unique values to the analyst. Correlation is key to the analysts' ability to use all the NSM data types. The analyst uses a correlation between different NSM data sets to relate events in different data slots.

B. *Tools and Configuration*

Security Onion offers a variety of tools that can capture session data, including Zeek, Argus, and PRADS. This section describes the aforementioned tools along with their abilities.

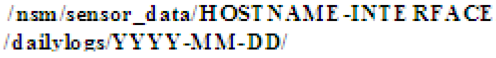
a) Network Visibility Tools

1) Zeek

Zeek is a network analysis [9] framework written in a specialized scripting language. Zeek can produce much more than session data, the SO administrator commonly chooses to implement Zeek because the analyst can configure it to produce session data, transaction data, extract content, statistical data, metadata, and alert data. The default Zeek installation provides several NSM functions. It provides audit records of every network session that is seen on the wire. It also provides audit records at the application layer. For example, all HTTP sessions are tracked with the requested URIs, MIME types, and server responses. The Zeek scripting language provides analyzers for many commonly used protocols that can be used for semantic analysis at the application layer.

2) Stenographer

Stenographer works as an open-source networking tool [32]. SO uses Stenographer to assemble full packet capture in the form of pcap files. The main factor that is influenced by it is an increment in the performance that reaches by zero-copy mechanisms, on packet receiving and transmission the kernel does not necessarily require to copy packets from kernel space to user space and vice versa. It writes full-packet capture in form of pcap file as given below:

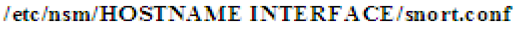


```
/nsm/sensor_data/HOSTNAME-INTERFACE
/dailylogs/YYYY-MM-DD/
```

(HOSTNAME represents real hostname, INTERFACE represents real sniffing interface and YYYY-MM-DD is the year, month, and date).

3) Snort

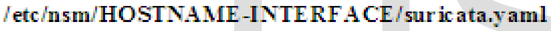
In SO, the Snort [8] is a NIDS. Snort generates ID alerts and works for the sniffing in network traffic. It is commonly compiled with PF_RING to allow handling more network traffic. It is configured via snort.confas given below:


/etc/nsm/HOSTNAME INTERFACE/snort.conf

(HOSTNAME represents actual hostname to be used and INTERFACE represents real sniffing interface).

4) Suricata

Suricata works as a robust network threat detector and fast open-source and fast open-source Network [30]. It examines the network traffic using an extensively powerful rule and has Lua scripting to help detect complex threats. Suricata is combined with PF_RING to allow you to spin up several workers to handle additional traffic. It can be configured via Suricata.yaml as given below:


/etc/nsm/HOSTNAME-INTERFACE/suricata.yaml

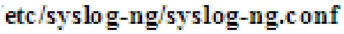
(HOSTNAME represents your real hostname and INTERFACE represents your real sniffing interface).

b) Host Visibility Tools

1) Syslog-ng

Syslog-ng provides the facility to flexibly collect [34], parse, classify, and correlate logs from the infrastructure and supply or route them to log analysis tools. Syslog-ng is used by SO to use it as a primary Syslog collector and sender of logs to ELSA.

Syslog-ng's configuration file is positioned at:


etc/syslog-ng/syslog-ng.conf

2) Ossec

OSSEC monitors all activities of the system including file integrity, log, process, and root check monitoring [5]. SO uses OSSEC as a HIDS. OSSEC also works as monitoring and defending SO and you can add its agents to monitor other hosts working on the network.

To Configure OSSEC to direct email notification(s) is given as Send OSSEC logs to an external Syslog collector.

c) Analyst Tools

1) Squert

Squert works as a web application tool [28] used for query and views IDS alert data stored in the form oftheSguil database. Squert is a graphical tool that provides a supplementary framework to events through the use of logically collected results, metadata, and time series representations. Squert offers access to the data types, e.g. NIDS alerts, HIDS alerts, Asset data from PRADS, HTTP logs from Zeek. Squert can pivot to CapMe for full packet capture. To do this, drill into an event and click on the Event the alert pane consists of several columns, such as SC source alerts, DC as destination alerts, PROTO as event alerts and etc.

2) Enterprise Log Search and Archive (ELSA)

It is a three-tier tool for log receiver, archiver, indexer, and web frontend for received Syslog [36]. It controls Syslog-ng's pattern-db parser for efficient log normalization and Sphinx full-text indexing for log searching. It is very fast, scalable. Each sensor has its own Mysql database and sphinx index. When you query the ELSA web interface, it queries all ELSA databases in parallel and then gives you the aggregate results. ELSA can pivot to CapME to access full packet capture. For any log relating to TCP traffic that has timestamp; source and destination IPs; source and destination ports. A user can get Info by providing credentials. CapMe!will retrieve the pcap files and render them as an ASCII transcript.

3) Sguil

Sguil is used as a network analyst tool [30]. The main component in Sguil is its GUI through which real-time events, session data, and raw packets can be accessed. NSM and event-driven analysis are captured through NIDS alert.

4) CapME

CapME works as a web interface [36]. It helps in view the pcap transcripts and also helps users in reducing these files with tcpdump.CapMEallows users to pivot from a

NIDS alert in Squert or from any log in ELSA that has a timestamp, source,and destination IPs; source, and destination ports.

5) Kibana

Kibana can perform all advanced data analysis. It also helps in visualize user's data in the form of a chart, maps, and tables. Different data types like HTTP, DNP3 is generated by SO [38].

Table 2 shows the comparison between different analysis tools according to their working and type of IDS supported by them. The comparison shows that most of the IDS are work only for NIDS but the Kibana tool work on both types of IDs (HIDS & NIDS). These are web-based tools, and are used for the query and viewing ID alert along with the normalized data form, SGUIL is the tool which is based on Network security through which real-time events and session data can be managed easily and Kibana is mainly focused on Visual Interfaces through which decision making can be easily done between different given fields.

V. ANALYSIS PERFORMED ON INTRUSION DETECTION TOOLS

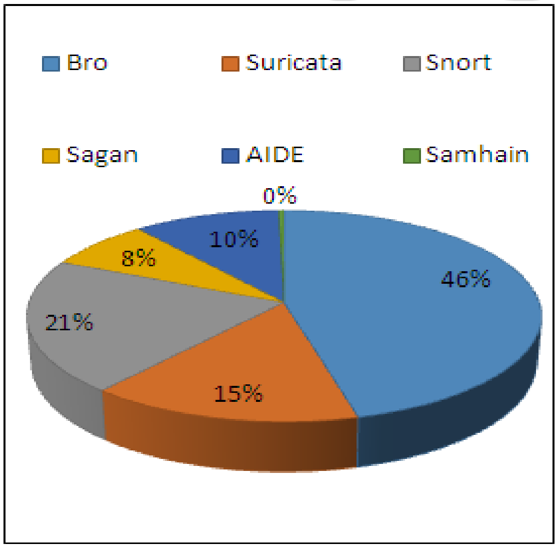


Figure 1 Intrusion Detection Tools

The researchers explore top IDS tools and find that the above tools shown in Fig.1 are the most widely used tools for the IDS,results are collected from the top five databases (i.e., Science Direct, Springer, IEEE, JhonWiley,and ACM).

We wrote the following query to get the result as shown in Fig.1

(((“Intrusion Detection System” OR “IDS”) AND “Zeek”) NOT “Sagan” NOT “AIDE” NOT “Samhain” NOT “Suricata” NOT “Snort”)

Tools	**Type**	**Purpose**
Squert	NIDS	Use to query and View IDS alert data for a web-based application
ELSA	NIDS	It is used for efficient weblog normalization
SGUIL	NIDS	It provides graphical access to real-time events and session data.
CAPME	NIDS	View a pcap transcript rendered with tcpflow
Kibana	NIDS, HIDS	Investigations and decision-making is used to accelerate multiple hyperlinked fields.

Table 02 Comparison of different Network analysis Tools

Zeek is the most used intrusion detection tool which works efficiently in different intrusion detection mechanism. The least used intrusion detection tool isSamhain. After Zeek the second most used tool is Suricata due to its fast open-source network mechanism, then snort which is famous for its IDS alert which can easily detect the intrusion in the network. AIDE has 10% of usage from different tools and lastly Sagan tool with 8% of consumption from different sources.

V. SIMPLIFIED SECURITY ONION ARCHITECTURE

SO can be deployed as a simple standalone system where one NIC is used for management and one or more additional NICs are used for monitoring. SO can also scale using a distributed deployment where one system acts as the master server and the monitoring duties are spread across multiple sensor systems [40].

When it comes to NSM tools, for every function, there are numerous options. For example, SO provides a choice between Snort and Suricata for the NIDS rule-based functionalities, which is a core component of SO. To understand the different types of tools and different types of data that a network security analyst will work with, SO provide a cohesive set of these tools as shown in Figure 2.

The diagram serves to introduce the complexity of and interactions between the NSM tools in SO. The tools in the bottom row are largely dedicated to the collection and production of raw NSM data. The tools in the middle row are associated with the optimization and maintenance of the data, for example, Zeek, OSSEC,and Syslog-ng all produce flat files with one log entry per line. The ELSA system takes this raw data and organizes it into a relational MYSQL database using high-performance Sphinx indexing. The tools that are listed in the top row are responsible for the presentation of the data to the analyst. There are many linkages between the data sets and the tools. For example, the ELSA can display Zeek connection events, providing session data. From any Zeek connection log, ELSA can pivot to the CapME. The tool can extract the PCAP content that is associated with that connection from the Sguil database display and decode it to the analyst. CapME! Pivot to Wireshark for an even more detailed analysis of the associate PCAP data. While one might describeSguil and Squert as Snort alert managers, both offer much more including the presentation of PCAP data, incorporation of metadata such as geo-location, and the ability to pivot other NSM tools.

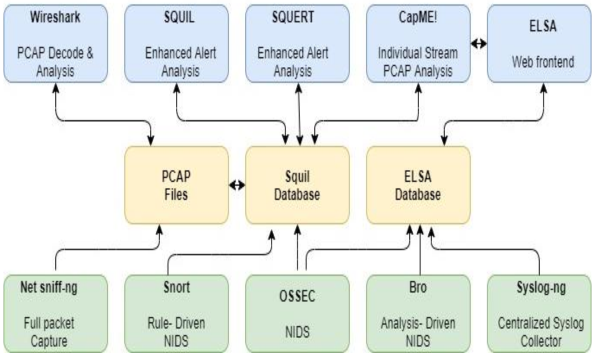


Figure 2: Simplified Security Onion Architecture

VI. DISCUSSION AND CONCLUSION

In this paper, we have discussed two fundamentally different intrusion methods – Host IDS and NIDS and of SO tools handling these Host and Network attacks.Different types of data havealso been discussed which are helpful in security monitoring (NSM) and security analyst use these data types to generate alerts in a network-based environment. SO provides the tools including Zeek, Argus, and PRADS that capture session data. Similarly, HIDS/NIDS sensors deliver Alert data, PRADS, and zeek are responsible for Asset data, and OSSEC for Host data. SO also gives tools including web applications such as Squert to query data kept placed in the Sguil database. Another analyst tools of SO are ELSA and Sguil. The main part is an instinctive GUI that offers access to raw packet captures, real-time events, and session data, and. Many tools are offered such as NetworkMiner, CapME, or Xplico to disseminate data for further analysis.

SO provides secure remote access and management methods to capture the malicious traffic that can be investigated further in research problems. It is a Linux based platform, therefore, lower in implementation cost than the other alternatives. In a summarized way the we can say that, SO is an extremely influential Network Security Management platform which is rapidly developing new tools and authorizing security analysts to configure full monitoring and reporting capability in network intrusion detection environment and giving a good platform for education and the research development community.

REFERENCES

[1] S. Sharma, R. K. Gupta, “Intrusion Detection System: A Review,” International Journal of Security and Its Applications Vol. 9, No. 5 (2015), pp. 69-76 http://dx.doi.org/10.14257/ijsia.2015.9.5.07.

[2] N. Das, T. Sarkar,” Survey on Host and Network Based Intrusion Detection System,” Int. J. Advanced Networking and Applications, Volume: 6 Issue: 2 Pages: 2266-2269 (2014) ISSN : 0975-0290.

[3] Sultana, N., Chilamkurti, N.K., Peng, W., &Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, *12*, 493-501.

[4] Heenan, Ross &Moradpoor, Naghmeh. Introduction to Security Onion. Conference: PGCS: The First Post Graduate Cyber Security Symposium – The Cyber Academy, Edinburgh Napier University, At Edinburgh Napier University, Scotland, Volume: 1, May 2016.

[5] Tripwire Available: http://www.tripwire.com. Last accessed 29thJanuary 2020.

[6] OSSEC. Available: http://www.ossec.net. Last accessed 1st February 2020.

[7] Samhain Available: http://www.la-samhna.de/samhain. Last accessed 20th January 2020.

[8] Snort. Available: http://www.snort.org. Last accessed 24th January 2020.

[9] Zeek Available: https://www.zeek.org. Last accessed 29th January 2020.

[10] S. Lessmann, R. Stahlbock, and S. F. Crone, “Genetic Algorithms for Support Vector Machine Model Selection,” International Joint Conference on Neural Networks, Sheraton Vancouver Wall Centre Hotel, Vancouver, BC, Canada, July 16-21, 2006.

[11] M. S. Mhatre, F. Siddiqui, M. Dongre, P. Thakur, “A Review paper on Artificial Neural Network: A Prediction Technique,” International Journal of Scientific & Engineering Research, Volume 8, Issue 3, March-2017, ISSN 2229-5518.

[12] S. Mohammadi, A. Namadchian, “A New Deep Learning Approach for Anomaly Base IDS using Memetic Classifier,” International journal of computers communications & control issn 1841-9836, 12(5), 677-688, October 2017.

[13] T.S. Cheng, Y.D. Lin, Y.C. Lai, P.C. Lin, "Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems", *IEEE Commun. Surveys Tutorials*, vol. 14, no. 4, pp. 1011-1020, 2012.

[14] Security Onion. Available: https://github.com/Security-OnionSolutions/security-onion. Last accessed 1st January 2020.

[15] Security Onion blog. Available: http://blog.securityonion.net/. Last accessed 1st January 2020.

[16] Gonzales, Ronald; Watkins, Alan; Simpson, Chris. “Using Security Onion for Hands-On Cybersecurity” Proceedings of the 2015 American Society for Engineering Education/Pacific South West Conference.

[17] Carey, M. J., Oyeniyi, T. U.S. Patent No. 10,395,040. Washington, DC: U.S. Patent and Trademark Office. 2019.

[18] Deuble, Ashley; Shinberg, David. “Using and Configuring Security Onion to detect and prevent Web Application Attacks.” SANS Institute InfoSec Reading Room. p1-35. 2012.

[19] Roger Meyer, “Detecting Attacks on Web Applications from Log Files.” As part of the Information Security Reading Room, © SANS Institute 2008.

[20] Gupta, Sunil; Luene, DrKees. Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment. SANS Institute InfoSec Reading Room. p1-44. 2012

[21] Hjelmvik, Erik. “Hands on network forensics. Swedish Armed Forces CERT

FIRST, Berlin., p1-93. 2015.

[22] Coleman Kane, ”Network Security Monitoring,” Cyber Defense Overview, September 24, 2014.

[23] S. Anwar et al., "From intrusion detection to an intrusion response system: Fundamentals requirements and future directions", *MDPI Algorithms*, vol. 10, no. 2, pp. 1-24, Mar. 2017.

[24] A. A. Sayar, S. N. Pawar, V. Mane, *A Review of Intrusion Detection System in Computer Network*, vol. 3, no. 2, pp. 700-703, 2014.

[25] Techniques in Network Intrusion Detection System,” International .S.Subrahmanyam., “A Review of Anomaly Detection Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 11, November 2014.

[26] Wireshark Available: https://www.wireshark.org. Last accessed 27th February 2020.

[27] XplicoAvailable:http://www.xplico.org. Last accessed 30th December 2019.

[28] Sguil. Available: http://sguil.sourceforge.net/. Last accessed 1st January 2020.

[29] Squert. Available: http://www.squertproject.org/. Last accessed 10th February 2020.

[30] PRADS. Available: http://gamelinux.github.io/prads/. Last accessed 15th January 2020.

[31] Suricata Available: https://suricata-ids.org. Last accessed 29th November 2019.

[32] PF_RING Available: http://www.ntop.org. Last accessed 29th December 2017. netsniff-ng Available: http://netsniff-ng.org. Last accessed 12th March 2020.

[33] NetworkMinerAvailable:http://www.netresec.com/?page=NetworkMine r. Last accessed 29th January 2020.

[34] Book, Richard Bejtlich, “The Practice of Network Security Monitoring: Understanding Incident Detection and Response,” Paperback, 376 pages, Published August 2nd 2013 by No Starch Press, ISBN 1593275099 (ISBN13: 9781593275099).

[35] Syslog Available: https://github.com/Security-Onion-Solutions/security-onion/wiki/Syslog. Last accessed 12th January 2020.

[36] CapME! Available: http:// securityonion.net/2014/01/new-capme-package-allows-you-to.html. Last accessed 25th March 2020.

[37] ELSA Available: https://github.com/Security-Onion-Solutions/security- onion/wiki/ELSA. Last accessed25th December 2019.

[38] Proffitt T. How Can You Build and Leverage SNORT IDS Metrics to Reduce Risk. The SANS (SysAdmin, Audit, Networking, and Security) Institute, Boston, MA. 2013.

[39] Perez, Steven. "Practical SIEM tools for SCADA environment." (2018).

[40] Mikail, A., &Pranggono, B. (2019). Securing Infrastructure-as-a-Service Public Clouds Using Security Onion. Applied System Innovation. 2019.