Introduction to Security Onion

Ross Heenan*
*0705974@abertay.ac.uk

Naghmeh Moradpoor
n.moradpoor@napier.ac.uk

*School of Arts, Media and Computer Games (AMG)
Abertay University
DUNDEE, DD1 1HG, UK

***Abstract* – Security Onion is a Network Security Manager (NSM) platform that provides multiple Intrusion Detection Systems (IDS) including Host IDS (HIDS) and Network IDS (NIDS). Many types of data can be acquired using Security Onion for analysis. This includes data related to: Host, Network, Session, Asset, Alert and Protocols. Security Onion can be implemented as a standalone deployment with server and sensor included or with a master server and multiple sensors allowing for the system to be scaled as required. Many interfaces and tools are available for management of the system and analysis of data such as Sguil, Snorby, Squert and Enterprise Log Search and Archive (ELSA). These interfaces can be used for analysis of alerts and captured events and then can be further exported for analysis in Network Forensic Analysis Tools (NFAT) such as NetworkMiner, CapME or Xplico. The Security Onion platform also provides various methods of management such as Secure SHell (SSH) for management of server and sensors and Web client remote access. All of this with the ability to replay and analyse example malicious traffic makes the Security Onion a suitable low cost alternative for Network Security Management. In this paper, we have a feature and functionality review for the Security Onion in terms of: types of data, configuration, interface, tools and system management.**

Keywords: Security Onion, Intrusion Detection Systems (IDS), Host-based IDS (HIDS), Netwrok-based IDS (NIDS), Network Forensic Analysis Tools (NFAT), Network Security Management (NSM)

I. INTRODUCTION

Providing an efficient security strategy for protecting a computer network is increasingly important in today's networking environment with the rising use of web applications provided to users supplying critical functions. The critical functions include: online banking, healthcare facilities, datacenters, Cloud, SCADA services and remote management. This means that there is a critical need to protect the networks, systems, applications and data that are concerned with these from intrusion and exploitation.

Intrusion Detection Systems (IDS) are a powerful tool available for alerting to and controlling of traffic passing through a network. They can use various methods such as signature based, anomaly based or other machine learning or specification based methods. Many types of IDS are also available. This includes: Host-based IDS (HIDS) to monitor host activity or Network-based IDS (NIDS) to monitor network activity for intrusion and also Hybrid approaches which can contain both.

Host-based IDS (HIDS) use methods of detection such as checking integrity of the concerned file system, registry and memory in use. Tripwire [16], OSSEC [10] and Samhain [15] are three examples for open source HIDS. Network-based IDS (NIDS) use methods such as signature based approaches for intrusion detections. Snort [8], Bro [17] and Suricata [18] are three examples for open source NIDS. Machine Learning (ML) methods commonly used for IDS detection include Genetic Algorithms (GA), Support Vector Machine (SVM), Artificial Neural Network (ANN), and Decision Tree (DT) among others. ML techniques use pattern matching methods and algorithms for detection along with datasets of known behavior or patterns to train them with to detect anomaly behavior. Issues still exist with IDS that allow an attacker to be able to use measures such as encryption, fragmentation or obfuscation of the attack or sending the attack payload over multiple routes, commonly known as Distributed Deny of Service (DDoS), to bypass, fool or evade the IDS rules or filters [19].

A more centralized Network Security Management System (NSM) is needed to provide a more manageable solution to network and system security to allow for more efficient analysis and reporting capabilities and overall control of the network being monitored. In order to provide a more efficient method of managing network security, acceptable user policies, and development and optimization of networking and security approaches other tools such as Databases, packet inspection tools, GUI interfaces and log management facilities are all required to assist the management of an IDS solution. Security Onion [5-6] is a Linux based Open-Source platform that provides multiple HIDS/NIDS Intrusion Detection Systems that provide graphical interface for management and also many other tools to assist analysis and reporting or captured traffic and events.

In this paper, we provide an overview and explore the use of Security Onion and its functionalities. The remainder of this paper is structured as follows. In Section II and III, an overview of the Security Onion regarding its abilities and functionalities as well as the related work are provided respectively. In Section IV, method of use in terms of types of data, configuration, interfaces & tools as well as system management are discussed which is then followed by conclusions of the work in Section V and references.

II. BACKGROUND

Security Onion [5-6] is an Ubuntu based intrusion detection orientated platform containing multiple IDS both Host (HIDS) and Network (NIDS) based. It provide Host based detection in the form of OSSEC HIDS, and Network based detection with the choice of Snort, Suricata and Bro NIDS. Security Onion can be configured in a master server with multiple sensors or as a standalone or hybrid deployment so is extremely adaptable. As seen in the Figure 1 the platform can be deployed with a master server that can control multiple sensors distributed across the network. The data captured by Security Onion is stored in log files and in a Sguil [12] database that provides a user interface for analysis, reporting and management.

Security Onion provides full packet capture by using PF_RING [20] which is a network socket capable of 10Gbit network speed among other functions and netsniff-ng [21] which is a toolkit for network analysis that provides a zero-copy ability for traffic capture at full speed.

It also uses tools such as Passive Real-time Asset Detection engine (PRADS) [14] for detecting data on assets on the network and HTTP Agent and Audit Record Generation and Usage System (ARGUS) for acquiring and auditing network data. These assist the performance of the IDS and overall system.

Capture and Alert data can also be accessed through the graphical interface (GUI) clients provided Enterprise Log Search and Archive (ELSA), Squert [13] and Snorby [11]. These offer many options for viewing, filtering and querying the data acquired such as by source, destination, service, port, type of threat and many others. Further analysis of the captured traffic can be carried out from exporting entries from Sguil, ELSA or Squert into many of the Network Forensic Analysis (NFAT) tools available included in the platform. NFAT tools available for further analysis of alerts and captured traffic include: CapME, NetworkMiner [22], Xplico [9] and Wireshark [7].

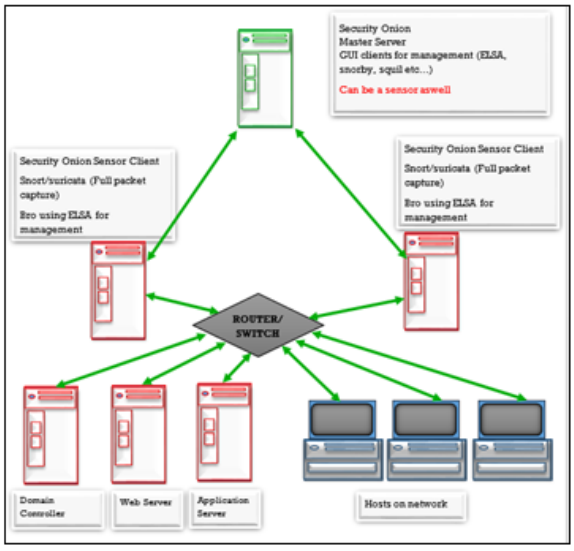

Fig. 1. Security Onion Server/Sensor deployment

These tools allows for filtering analysis and reporting of data for alerts, events, hosts, correlated events and many other options.

Other facilities that can be used in Security Onion for management of the system include the of SOSTAT module for providing analysis and system statistics summaries, SSH connections to the sensors/server for management or configuration or Web client access to the management GUI's ELSA, Squert and Snorby. It also uses SALT which is a management and maintenance tools that allows for tasks such as checking of services status, and configuring of sensors.

With the combination of multiple IDS for both Host and Network based detection (HIDS and NIDS) in conjunction with the User interfaces and NFAT tools provided for further analysis, Security Onion can provide a more vast range of data that can be used for analysis to provide a better monitoring capability to the analyst. This should in turn allow for more secure systems to be developed and more control of the network.

The aim of Security Onion is to provide a more centralised system for Network Security Management by incorporating full capture speed ability, multiple detection methods and also many analysis and management tools to interrogate acquired data. As it is open source it is cost effective in terms or alternatives and is relatively simple to deploy. The tools and interfaces included allow analysis with much more ease than a standard IDS and provides more range of data such as session, alert, network and host to do so. All of this will assist in aiding the overall ability of the monitoring capacity of the IDS and Security Onion system deployed to protect the network and its systems and also allow for better logs, rules and alert managements.

Considerations that need to be assessed before deploying a Security Onion system include the available budget for implementation in terms of staff training, data storage and capture speed abilities depending on the size and estimated usage of the network. For example, a network with a 50Mb connection speed can estimate a 16TB data capture over the space of 30 days. Other considerations are ensuring that a spanning port is available to allow separate ports for monitoring and management and also to allow for full capture speed of traffic.

III. RELATED WORK

This section will provide a review of related work in the field of Security Onion such as its use, configuration and management.

A. Using Security Onion

A paper by Gonzales et al [1] on behalf of the National University which is a department of Homeland Security Center of Excellence provides an overview of created cyber security testing labs using Security Onion. They used the system with its included example traffic capture file that include malware, honeypot and botnet example traffic. These were

replayed and analysis carried with the NFAT tools and interfaces included to provide an insight to students in to common practices used in industry and better prepare them for dealing with them but using an open-source platform. The aim of the units created was to incorporate them in to a framework for National Center of Academic Excellence in Information Assurance/Cyber Defense which shows the regarded abilities of the Security Onion by these and many researchers.

B. *Configuring Security Onion*

A paper by Ashley Deuble [2] on behalf of SANS Institute use Security Onion to explore detection and prevention of Web application attacks. The paper overviews a set of labs that test various Web application vulnerabilities against a known vulnerable Web application virtual machine called Damn Vulnerable Web App (DVWA). Web application vulnerabilities tested included Cross Site Scripting (XSS), SQL injection and Operating System (OS) injection. This study again shows the regarded capability of the Security Onion platform and what it can provide to a researcher.

C. *Monitoring and Loggging*

A further paper provided by Sunil Gupta [3] on behalf of the SANS Institute InfoSec reading room explores the use of Security Onion for effective logging and monitoring for network exploitations. They use known rulesets and explore the analysis and reporting functionality of tools provided in Security Onion to suggest an alerting, logging and monitoring framework to be used to ensure requirements are being met in terms of security, service levels and legislation compliance. This paper provides the obvious suggestion that Security Onion is a suitable solution for individuals or organization that do not have a large security budget and again highlight the obvious power and benefit it provides to the security analyst.

D. *Managing Security*

A study provided by the Forum of Incident Response and Security Teams (FIRST) [4] again looks at the use of Security Onion for analysis of suspected network or system intrusion events using the tool provided in it. It explores various different exploit and again shows it capturing and analysis capability and it growing popularity with researchers.

IV. METHOD OF USE

As specified previously Security Onion can be deployed in various configurations. It can be set up as a standalone deployment with Server and Sensor components built in together (Fig.2), as a master server with multiple distributed sensors across the network being monitored or as a Hybrid set up.

When setting up Security Onion there are two options provided by the setup wizard, Quick and Advanced. The quick mode is used when setting up a standalone Security Onion platform. The advanced mode is used when a more complex deployment is set up such as a Master Server with multiple Sensors, this allows for choice of IDS, rulesets, interface configuration and choice of what tools to enable and disable.

A. *Typess of Data*

The full packet capture ability provided by using Security Onion allows many types of data to be acquired including Alert data generated form the HIDS and NIDS sensors, Asset data from PRADS and Bro, Session data from Argus, PRADS and Bro logs for protocol specific transaction data.

B. *Configuration*

Three important areas in the configuration and use of Security Onion are the management of configuration, logs and rules files. Important locations for configuration files for IDS, tools and other services in the filesystem are “/opt/bro” and “/etc/nsm”. From these many of the tools can be configured as required. The Security Onion system will only be as effective as the rules implemented for it to use. These files can be found in “/etc/nsm/rules”. Important files include: “local.rules”, “downloaded.rules” and also the “whitelist.rules” and “blacklist.rules” files. Log files for network activity for DHCP, DNS, SNMP SSL and various other connections can be found in “/nsm/bro/current” and allow for analysis of traffic captured. This can also be done through the many interfaces provided such as ELSA, Sguil (Fig .1), Squert and Snorby.

C. *Interfaces and tools*

Sguil is an analysis tool that provides an SQL database backend and a GUI front end seen in Figure 2 to allow for analysis from data stored in it. It provides access to generated alerts, events correlated events and data from packets can be viewed in Hex or ASCII or exported for further analysis to tools such as Wireshark, NetworkMiner or Xplico. It also provides the ability to generate a transcript from an alert to reassemble the packet stream for more high level analysis. The database can be managed from the command line by using commands such as sguil-db-purge for example to clear it.

ELSA also provides a user interface that can be used for analysis of traffic and filtering of it by IP, port, service, connection duration and many others. It provides access to asset, session and transaction data and data can also be searched using Bro queries

Fig. 2. Sguil interface

Such as class-Bro_CONN "-" groupby:srcip for grouping results by IP address. Statistical data can also be generated from ELSA to overview statistical performance of the network being monitored. Snorby is a Ruby on Rails based User interface front end that allows access to data captured and logged from the Snort or Suricata IDS. It also provides many abilities of filtering, analysis and reporting of logged data. Squert is a front end GUI that allows access and analysis of data stored in the Sguil database. Events can be accessed and packet data viewed or exported to other tools. Further analysis can be carried out also by exporting data from the Sguil database or interfaces into one of the many Network Forensic Tools (NFAT) available including NetworkMiner, CapME, Wireshark and Xplico.

D. System Management

Many tools are also available for managing Security Onion including the use of SSH connections for remote analysis and configuration or SALT which provides system management through the command line. Sensor and Server service can be controlled and checked among other functions. The previously mentioned tools in this section provide powerful analysis and management abilities for log, rule and alert files and assist the overall configuration and performance of the system. Another tool provided in Security Onion is "SOSTAT" which is a tool to provide statistical data in the command line for analysis or exporting to email.

Remote and local GUI access is possible through a web client using something like "http://localhost/application" or to access remotely "http://serverIPaddress/applicaiton".

Updating of the platform is recommended to be carried out using either "sudo soup" in the terminal or the script below. Rules for the IDS can also be update using sudo rule-update.

V. DISCUSSION & CONCLUSION

The full packet capture ability of Security Onion provides powerful monitoring, analysis and management capability to the Security Analyst by giving access to Host, Session and Network data. It provides the tools to allow for centralized management of logs and alerts. Alert data is provided by the HIDS/NIDS sensors, Asset data from PRADS and bro, Host data from OSSEC and Session data from Argus, PRADS and Bro. Many tools are available to export data into for further analysis such as NetworkMiner, CapME, or Xplico among many others. Other benefits of Security Onion include it adaptability in deployment as can be deployed in a standalone or server/sensor distribution. Security Onion can be configured as required depending on the production networks needs using chosen IDS and detection methods and it is scalable and provides secure remote access and management methods. Also, it is a useful research platform as it provides example malicious traffic captures that can be replayed and investigated providing a mock lab environment. It is Linux based so presents opportunities for development and it is open-source so should have considerably lower in cost to implement that other alternatives. In summary, Security Onion is an extremely powerful NSM platform with many tools available for analysis to provide power capability to the user. It is scalable, adaptable and highly configurable to needs and provides a good education platform and development community for researchers.

REFERENCES

[1] Gonzales, Ronald; Watkins, Alan; Simpson, Chris. (2015). Using Security Onion for Hands-On Cybersecurity Labs. Proceedings of the 2015 American Society for Engineering Education/Pacific South West Conference Copyright © 2015, American Society for Engineering Education. p1-6.

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

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

[4] Hjelmvik, Erik . (2015). Hands on network forensics. Swedish Armed Forces CERT FIRST 2015, Berlin. - (-), p1-93.

[5] Security Onion. Available: https://github.com/Security-Onion-Solutions/security-onion. Last accessed 1st Apr 2016.

[6] Security Onion blog. Available: http://blog.securityonion.net/. Last accessed 1st Apr 2016.

[7] Wireshark Available: https://www.wireshark.org. Last accessed 29th Apr 2016

[8] Snort. Available: http://www.snort.org. Last accessed 1st Apr 2016. Last accessed 29th Apr 2016

[9] Xplico Available:http://www.xplico.org. Last accessed 29th Apr 2016

[10] OSSEC. Available: http://www.ossec.net. Last accessed 1st Apr 2016.

[11] Snorby. Available: https://github.com/snorby/snorby. Last accessed 1st Apr 2016.

[12] Sguil. Available: http://sguil.sourceforge.net/. Last accessed 1st Apr 2016.

[13] Squert. Available: http://www.squertproject.org/. Last accessed 1st Apr 2016.

[14] PRADS. Available: http://gamelinux.github.io/prads/. Last accessed 1st Apr 2016.

[15] Samhain Available: http://www.la-samhna.de/samhain. Last accessed 29th Apr 2016

[16] Tripwire Available: http://www.tripwire.com. Last accessed 29th Apr 2016

[17] Bro Available: https://www.bro.org. Last accessed 29th Apr 2016

[18] Suricata Available: https://suricata-ids.org. Last accessed 29th Apr 2016

[19] Tsung-Huan Cheng ; Ying-Dar Lin ; Yuan-Cheng Lai ; Po-Ching Lin. Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems, EEE Communications Surveys & Tutorials, (Volume:14 , Issue: 4

[20] PF_RING Available: http://www.ntop.org. Last accessed 29th Apr 2016

[21] netsniff-ng Available: http://netsniff-ng.org. Last accessed 29th Apr 2016

[22] NetworkMiner Available: http://www.netresec.com/?page=NetworkMiner. Last accessed 29th Apr 2016.