Use Of Security Onion As A Source Of Alerts

Security Onion is an open-source suite of Network Security Monitoring (NSM) tools that run on an Ubuntu Linux distribution. Security Onion tools provide three core functions for the cybersecurity analyst: full packet capture and data types, network-based and host-based intrusion detection systems, and alert analyst tools.
Security Onion can be installed as a standalone installation or as a sensor and server platform. Some components of Security Onion are owned and maintained by corporations, such as Cisco and Riverbend Technologies, but are made available as open-source.

For more information, and to obtain Security Onion, search the internet for the Security Onion website.
Note: In some resources, you may see Security Onion abbreviated as SO. In this course, we will use Security Onion.

Detection Tools for Collecting Alert Data

Security Onion contains many components. It is an integrated environment that is designed to simplify the deployment of a comprehensive NSM solution. The figure illustrates a simplified view of the way in which some of the components of the Security Onion work together.
The graphic displays a three-level architecture for Security Onion. The bottom level is labelled data. It includes the following elements; pcaps, content data transaction data, session data, host logs, alert data, Syslog data, and metadata. The middle layer is labelled detection. It includes the following elements; CapME, Snort, Bro, OSSEC, and Suricata. The top-level is labelled Analysis. It includes Sguil with Wireshark and ELSA supporting Sguil.

A Security Onion Architecture

This is a web application that allows viewing of pcap transcripts rendered with the tcpflow or Zeek tools. CapME can be accessed from the Enterprise Log Search and Archive (ELSA) tool. CapME provides the cybersecurity analyst with an easy-to-read means of viewing an entire

Layer 4 session. CapME acts as a plugin to ELSA and provides access to relevant pcap files that can be opened in Wireshark.

Analysis Tools

Security Onion integrates these various types of data and Intrusion Detection System (IDS) logs into a single platform through the following tools:

- **Sguil** – This provides a high-level console for investigating security alerts from a wide variety of sources. Sguil serves as a starting point in the investigation of security alerts. A wide variety of data sources are available to the cybersecurity analyst by pivoting directly from Sguil to other tools.
- **Kibana** – Kibana is an interactive dashboard interface to Elasticsearch data. It allows querying of NSM data and provides flexible visualizations of that data. It provides data exploration and machine learning data analysis features. It is possible to pivot from Sguil directly into Kibana to see contextualized displays based on the source and destination IP addresses that are associated with an alert. Search the internet and visit the elastic.co website to learn more about the many features of Kibana.
- **Wireshark** – This is a packet capture application that is integrated into the Security Onion suite. It can be opened directly from other tools and will display full packet captures relevant to the analysis.
- **Zeek** – This is a network traffic analyzer that serves as a security monitor. Zeek inspects all traffic on a network segment and enables in-depth analysis of that data. Pivoting from Sguil into Zeek provides access to very accurate transaction logs, file content, and customized output.

Note: Other Security Onion tools that are not shown in the figure are beyond the scope of this course. A full description of the Security Onion and its components can be found on the Security Onion website.

Alert Generation

Security alerts are notification messages that are generated by NSM tools, systems, and security devices. Alerts can come in many forms depending on the source. For example, Syslog provides support for severity ratings which can be used to alert cybersecurity analysts regarding events that require attention.
In Security Onion, Sguil provides a console that integrates alerts from multiple sources into a

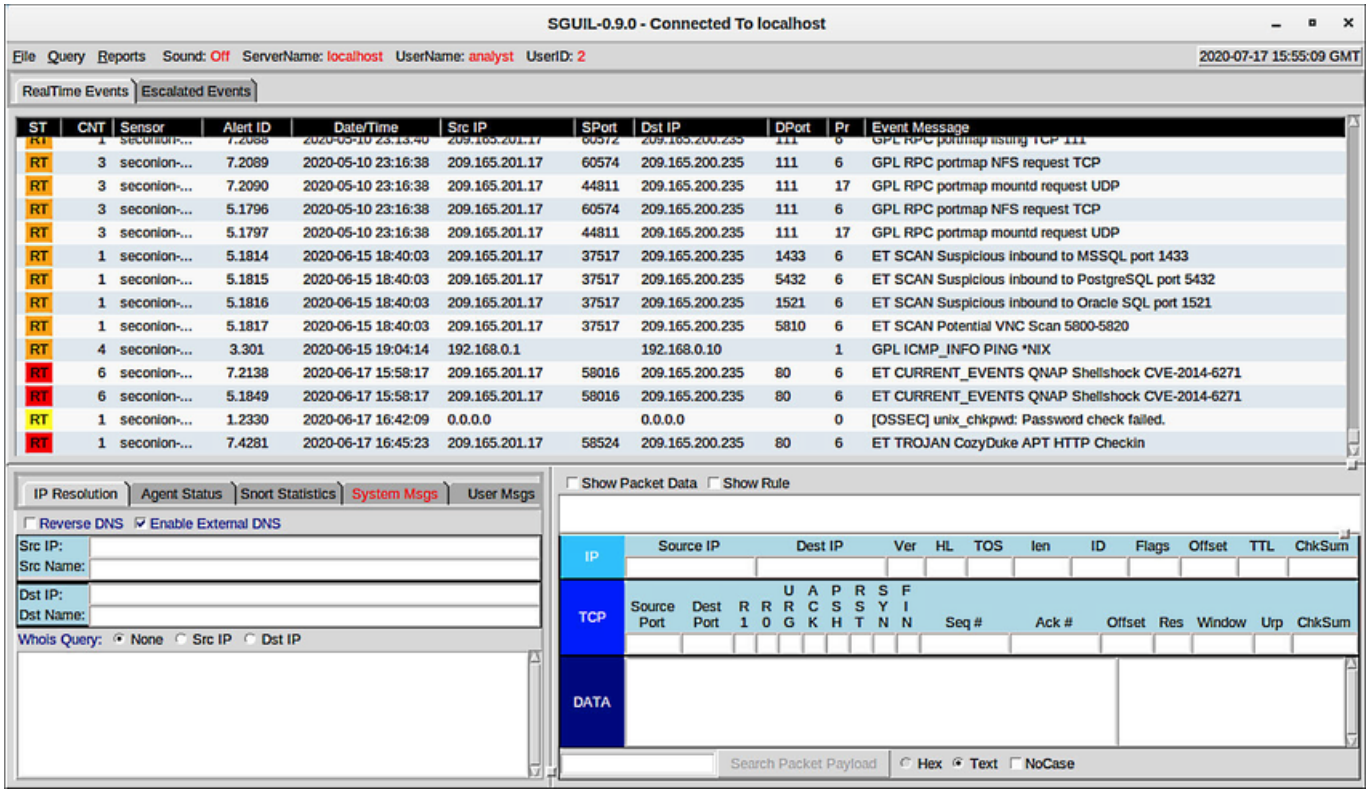
timestamped queue. A cybersecurity analyst can work through the security queue investigating, classifying, escalating, or retiring alerts. Instead of using a dedicated workflow management system such as Request Tracker for Incident Response (RTIR), a cybersecurity analyst would use the output of an application like Sguil to orchestrate an NSM investigation. Alerts will generally include five-tuples information when available, as well as timestamps and information identifying which device or system generated the alert. Recall that the five tuples include the following information for tracking a conversation between a source and destination application:

- **SrcIP** – the source IP address for the event.
- **SPort** – the source (local) Layer 4 port for the event.
- **DstIP** – the destination IP for the event.
- **DPort** – the destination Layer 4 port for the event.
- **Pr** – the IP protocol number for the event.

Additional information could be whether a permit or deny decision was applied to the traffic, some captured data from the packet payload, or a hash value for a downloaded file, or any of a variety of data.

The figure shows the Sguil application window with the queue of alerts that are waiting to be investigated in the top portion of the interface.

Sguil Window



The fields available for the real-time events are as follows:

- **ST** – This is the status of the event. RT means real-time. The event is colour-coded by priority. The priorities are based on the category of the alert. There are four priority levels: very low, low, medium, and high. The colours range from light yellow to red as the priority increases.
- **CNT** – This is the count for the number of times this event has been detected for the same source and destination IP address. The system has determined that this set of events is correlated. Rather than reporting each in a potentially long series of correlated events in this window, the event is listed once with the number of times it has been detected in this column. High numbers here can represent a security problem or the need for tuning of the event signatures to limit the number of potentially spurious events that are being reported.
- **Sensor** – This is the agent reporting the event. The available sensors and their identifying numbers can be found in the Agent Status tab of the pane which appears below the events window on the left. These numbers are also used in the Alert ID column. From the Agent Status pane, we can see that OSSEC, pcap, and Snort sensors are reporting to Sguil. In addition, we can see the default hostnames for these sensors, which includes the monitoring interface. Note that each monitoring interface has both

pcap and Snort data associated with it.

- **Alert ID** – This two-part number represents the sensor that has reported the problem and the event number for that sensor. We can see from the figure that the largest number of events that are displayed are from the OSSEC sensor (1). The OSSEC sensor has reported eight sets of correlated events. Of these events, 232 have been reported with event ID 1.24.
- **Date/Time** – This is the timestamp for the event. In the case of correlated events, it is the timestamp for the first event.
- **Event Message** – This is the identifying text for the event. This is configured in the rule that triggered the alert. The associated rule can be viewed in the right-hand pane, just above the packet data. To display the rule, the **Show Rule** checkbox must be selected.

Depending on the security technology, alerts can be generated based on rules, signatures, anomalies, or behaviours. No matter how they are generated, the conditions that trigger an alert must be predefined in some manner.

Rules and Alerts

Alerts can come from a number of sources:

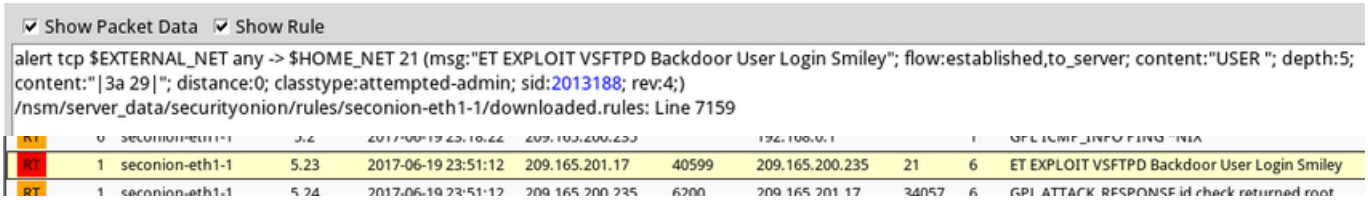
- **NIDS** – Snort, Zeek, and Suricata
- **HIDS** – OSSEC, Wazuh
- **Asset management and monitoring** – Passive Asset Detection System (PADS)
- **HTTP, DNS, and TCP transactions** – Recorded by Zeek and pcaps
- **Syslog messages** – Multiple sources

The information found in the alerts that are displayed in Sguil will differ in message format because they come from different sources.
The Sguil alert in the figure was triggered by a rule that was configured in Snort. It is important for the cybersecurity analyst to be able to interpret what triggered the alert so that the alert can be investigated. For this reason, the cybersecurity analyst should understand the components of Snort rules, which are a major source of alerts in Security Onion.

The figure shows two main sections: rule and alert. An arrow goes from the rule section pointing to the alert section. Information in the rule section: enabled show packet data

checkbox and show rule checkbox. Text: alert t c p $EXTERNAL_NET any -> $HOME_NET 21 (msg:ET EXPLOIT VSFTPD backdoor user login smiley; flow:established,to_server; content:USER; depth:5; content:|3a 29|; distance:0; classtype:attempted-admin; sid:2013188; rev:4;) /nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules: Line 7159. Alert highlighted text: R T 1 seconion-eth1-1 5.23 2017-06-19 23:51:12 209 dot 165 dot 201 dot 17 40599 209 dot 165 dot 200 dot 235 21 6 ET EXPLOIT VSFTPD backdoor user login smiley.

Sguil Alert and the Associated Rule



RuleAlert

Snort Rule Structure

Snort rules consist of two sections, as shown in the figure: the rule header and the rule options. The rule header contains the action, protocol, source and destination IP addresses and netmasks, and the source and destination port information. The rule options section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken. Rule Location is sometimes added by Sguil. Rule Location is the path to the file that contains the rule and the line number at which the rule appears so that it can be found and modified, or eliminated if required.
The figure shows text in blue: alert ip any any -> any any, in green: (msg: GPL ATTACK_RESPONSE id check returned root; content: uid=0|28|root|29|; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;), and in purple: /nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692.

Snort Rule Structure and Sguil-supplied Information

alert ip any any -> any any (msg:”GPL ATTACK_RESPONSE id check returned root”; content:”uid=0|28|root|29|”; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692

Component	Example (shortened…)	Explanation
rule header	alert ip any any -> any any	Contains the action to be taken, source and destination addresses and port, and the direction of traffic flow
rule options	(msg:”GPL ATTACK_RESPONSE ID CHECK RETURNED ROOT”;…)	Includes the message to be displayed, details of packet content, alert type, source ID, and additional details, such as a reference for the rule or vulnerability
rule location	/nsm/server_data/securityonion/rules/…	Added by Sguil to indicate the location of the rule in the Security Onion file structure and in the specified rule file

PEOPLE ALSO READ: Comprehensive Guide About Cloud Computing

The Rule Header

The rule header contains the action, protocol, addressing, and port information, as shown in the figure. In addition, the direction of flow that triggered the alert is indicated. The structure of the header portion is consistent with Snort alert rules.

Snort can be configured to use variables to represent internal and external IP addresses. These variables, **$HOME_NET** and **$EXTERNAL_NET** appear in the Snort rules. They simplify the creation of rules by eliminating the need to specify specific addresses and masks for every rule. The values for these variables are configured in the **snort.conf** file. Snort also allows individual IP addresses, blocks of addresses, or lists of either to be specified in rules. Ranges of ports can be specified by separating the upper and lower values of the range with a colon. Other operators are also available.

The figure shows text in blue: alert ip any any -> any any, then text in normal font: (msg: GPL ATTACK_RESPONSE id check returned root; content: uid=0|28|root|29|; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;) /nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692.

Snort Rule Header Structure

Component	Explanation
alert	the action to be taken is to issue an alert, other actions are log and pass
ip	the protocol

Component	Explanation
any any	the specified source is any IP address and any Layer 4 port
->	the direction of flow is from the source to the destination
any any	the specified destination is any IP address and any Layer 4 port

The Rule Options

The structure of the options section of the rule is variable. It is the portion of the rule that is enclosed in parenthesis, as shown in the figure. It contains the text message that identifies the alert. It also contains metadata about the alert, such as a URL that provides reference information for the alert.

Other information can be included, such as the type of rule and a unique numeric identifier for the rule and the rule revision. In addition, features of the packet payload may be specified in the options. The Snort users manual, which can be found on the internet, provides details about rules and how to create them.

Snort rule messages may include the source of the rule. Three common sources for Snort rules are:

- **GPL** – Older Snort rules that were created by Sourcefire and distributed under a GPLv2. The GPL ruleset is not Cisco Talos certified. It includes Snort SIDs 3464 and below. The GPL ruleset is can be downloaded from the Snort website, and it is included in Security Onion.
- **ET** – Snort rules from Emerging Threats. Emerging Threats is a collection point for Snort rules from multiple sources. ET rules are open source under a BSD license. The ET ruleset contains rules from multiple categories. A set of ET rules is included with Security Onion. Emerging Threats is a division of Proofpoint, Inc.
- **VRT** – These rules are immediately available to subscribers and are released to registered users 30 days after they were created, with some limitations. They are now created and maintained by Cisco Talos.

PEOPLE ALSO READ: Understanding Insider Threat In Network Security

Rules can be downloaded automatically from Snort.org using the PulledPork rule management utility that is included with Security Onion.

Alerts that are not generated by Snort rules are identified by the OSSEC or PADS tags, among others. In addition, custom local rules can be created.

The figure shows text in normal font: alert ip any any -> any any, then text in green: (msg: GPL ATTACK_RESPONSE id check returned root; content: uid=0|28|root|29|; fast_pattern:only;

classtype:bad-unknown; sid:2100498; rev:8;), then text in normal font: /nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692.

Snort Rules Options Structure

alert ip any any -> any any (msg:”GPL ATTACK_RESPONSE id check returned root”; content:”uid=0|28|root|29|”; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692

Component	Explanation
msg:	Text that describes the alert.
content:	Refers to content of the packet. In this case, an alert will be sent if the literal text “uid=0(root)” appears anywhere in the packet data. Values specifying the location of the text in the data payload can be provided.
reference:	This is not shown in the figure. It is often a link to a URL that provides more information on the rule. In this case, the sid is hyperlinked to the source of the rule on the internet.
classtype:	A category for the attack. Snort includes a set of default categories that have one of four priority values.
sid:	A unique numeric identifier for the rule.
rev:	The revision of the rule that is represented by the sid.

Lab – Snort and Firewall Rules

Different security appliances and software perform different functions and record different events. As a consequence, the alerts that are generated by different appliances and software will also vary.
In this lab, to get familiar with firewall rules and IDS signatures you will:

- Perform live monitoring of IDS and events.
- Configure your own customized firewall rule to stop internal hosts from contacting a malware-hosting server.
- Craft a malicious packet and launch it against an internal target.
- Create a customized IDS rule to detect the customized attack and issue an alert based on it.

Action Point
I know you might agree with some of the points that I have raised in this article. You might not agree with some of the issues raised. Let me know your views about the topic discussed. We will appreciate it if you can drop your comment. Thanks in anticipation.

Fact Check Policy

CRMNAIJA is committed to fact-checking in a fair, transparent and non-partisan manner. Therefore, if you've found an error in any of our reports, be it factual, editorial, or an outdated post, please contact us to tell us about it.

Action Point

Get My 66 Page eBook on How to Run Success Ads ON TikTok for 2,000 Naira. Click Here to Buy.

Get my 90 Page ebook on How to Run Ads on Facebook. Click here to buy now.

PS: Are you a Nigerian resident abroad and you need to send money to your loved ones back home? The stress is over now! Send money to Nigeria using the MonieWorld app. It's fast, easy and has great rates! MonieWorld is powered by Moniepoint. Sign up with my link

https://spoo.me/iy8taz

P.S.: If you need private online training on any of the ICT courses I offer here and you are in Nigeria, please send me a DM on my WhatsApp at **+2348103180831.** Please note that the Training will be 100percent online. It will be delivered via Zoom or Google Meet.

PS: I know you might agree with some of the points raised in this article or disagree with

some of the issues raised.

Please share your thoughts on the topic discussed. We would appreciate it if you could drop your comment. Thanks in anticipation.

Sharing Is Caring. If you enjoy this article, help us share with others.

Related posts:

1. The 10x Daughter. How to be The Star Girl of The Family
2. The 10x Whatsapp Group Administrator . Being a Leader With a Difference
3. The 10x Employee. Building Leaders in Our Organisations
4. Building a 10x Career. The Untaken Path to Career Growth