Snort Alert Analysis using SGUIL via Security Onion

January 14, 2024

Content

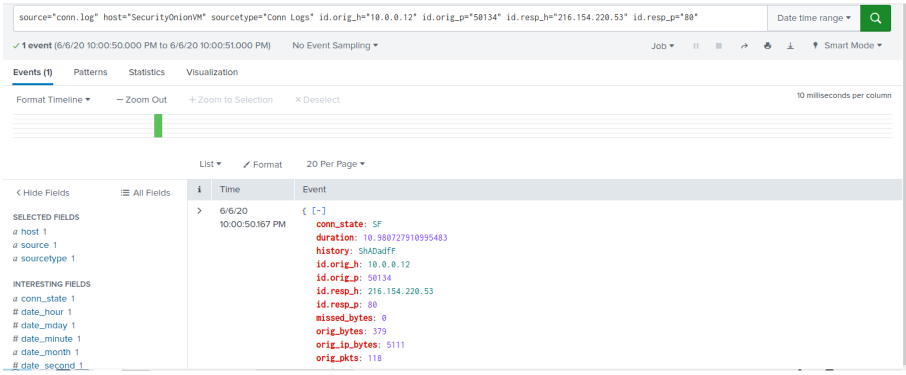
1 Introduction

Network logs are important because network is the most common attack vector. With the exception o DDOS attack, we are usually more interested in what effect an attack has on target host or hosts.

Timestamps are vital for logs and common for every log entry. Unfortunately, timestamps they are not always in the same format across different log types. Normalizing timestamps is one area that tools like Splunk can be helpful. We will be using Splunk to understand the impact of the malicious malware activity on the host.

2 Connection Summaries - Zeek Logs

Looking at connection summaries such as Zeek provide insight into network activity without storing every bit of data.



```
source="conn.log" host="SecurityOnionVM" sourcetype="Conn Logs" id.orig_h="10.0.0.12" id.orig_p="50134" id.resp_h="216.154.220.53" id.resp_p="80"
```

✓ 1 event (6/6/20 10:00:50.000 PM to 6/6/20 10:00:51.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a conn_state 1
- # date_hour 1
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 1

Time	Event
6/6/20 10:00:50.167 PM	{ [-] conn_state: SF duration: 10.980727910995483 history: ShADadfF id.orig_h: 10.0.0.12 id.orig_p: 50134 id.resp_h: 216.154.220.53 id.resp_p: 80 missed_bytes: 0 orig_bytes: 379 orig_ip_bytes: 5111 orig_pkts: 118

Figure 1: Snapshot showing the network connection summary of conn.log file on Splunk

- The first thing to do is to locate the conn.log (Connection Log) - that provides detailed information about network connections observed by Zeek.
- Import the conn.log into Splunk and ”start searching”

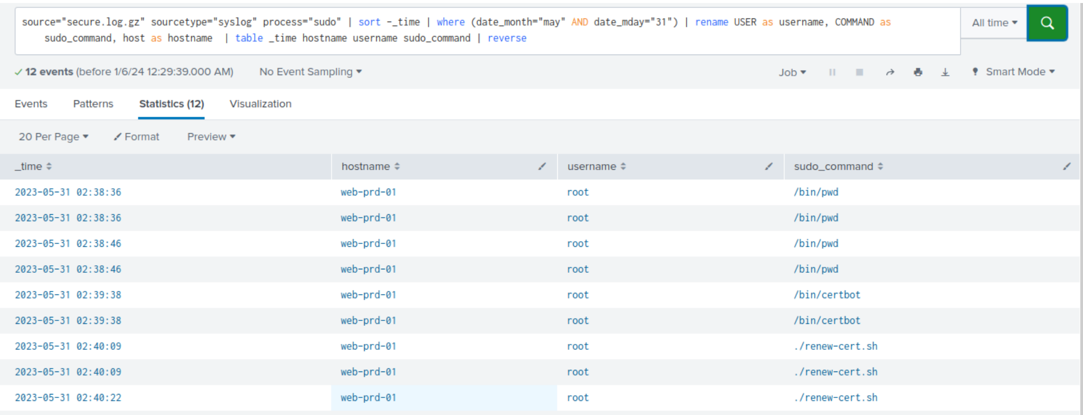
Note conn.log file can be found in the /nsm/import/bro/bro-* directory. It is automatically generated when you run so-import-pcap. FIG. 1 shows that connection summary of the malicious malware activity in Splunk. Each entry in the ”conn.log” corresponds to a connection between two endpoints, including details such as source and destination IP addresses, port numbers, connection duration, and various other attributes.

Privilege Escalation

During privilege escalation, users or system process gains higher-level access or permissions than originally assigned to a it. It involves elevating one’s privileges to access resources, execute commands, or perform actions that are typically restricted.

Privilege escalation is a significant security concern because unauthorized users or malicious software gaining higher privileges can lead to serious security breaches. We want to create a dashboard to identify privilege escalation.

- Identify both users who used sudo and the command or commands they ran.
- The dashboard should contain the following fields: _time, hostname, username, sudo_command.
- The events will be ordered by _time in ascending order (earliest time value first). Update the dashboard to display events from May 31.

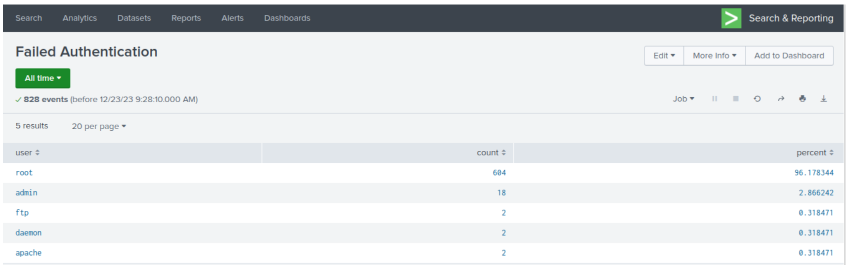


```
source="secure.log.gz" sourcetype="syslog" process="sudo" | sort -_time | where (date_month="may" AND date_mday="31") | rename USER as username, COMMAND as
    sudo_command, host as hostname  | table _time hostname username sudo_command | reverse
```

_time	hostname	username	sudo_command
2023-05-31 02:38:36	web-prd-01	root	/bin/pwd
2023-05-31 02:38:36	web-prd-01	root	/bin/pwd
2023-05-31 02:38:46	web-prd-01	root	/bin/pwd
2023-05-31 02:38:46	web-prd-01	root	/bin/pwd
2023-05-31 02:39:38	web-prd-01	root	/bin/certbot
2023-05-31 02:39:38	web-prd-01	root	/bin/certbot
2023-05-31 02:40:09	web-prd-01	root	./renew-cert.sh
2023-05-31 02:40:09	web-prd-01	root	./renew-cert.sh
2023-05-31 02:40:22	web-prd-01	root	./renew-cert.sh

Figure 2: Screenshot Splunk Dashboard showing Privilege escalation

Failed Authentication



user	count	percent
root	604	96.178344
admin	18	2.866242
ftp	2	0.318471
daemon	2	0.318471
apache	2	0.318471

Figure 3: Failed Authentication by user

To create a report in Splunk to display authentication failures by user from the host-based logs, I used Splunk field extraction property.