Global Information Assurance Certification Paper

Boiling the Ocean: Security Operations and Log Analysis

GIAC (GCIH) Gold Certification

Author: Colin Chisholm (chisholm.colin@gmail.com)
Advisor: Hamed Khiabani, Ph.D.
Accepted: March 24th 2016

Abstract

Incident handlers are expected to provide timely and efficient detection, analysis and response to incidents. They have at their disposal a seemingly endless supply of events, typically in the form of log data from a variety of systems. Unfortunately, the volume of this data can be difficult to capture and analyze, hindering the incident handling process. Specialized software can automate the collection and dying of log data, helping separate the "noise" of events from the "signal" of incidents. This paper will detail a framework and procedures to establish a security operations program that leverages log analysis tools.

1. Introduction

Incident handling is a difficult and challenging job. One of the many challenges of incident response, and the root of this paper, is obtaining access to the data needed to identify an incident. Of the six primary phases of incident handling, Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned (Skoudis, 2010), this paper is focused on the first two, Preparation and Identification. Another fundamental challenge is closing the gap between an ever-increasing amount of available log data and the limited human resources to identify, analyze and act upon that data.

We will discuss the role of security operations in more detail and the value of log data in relation to incident response. The role and benefit of security operations within the organization will be addressed as well as advice and guidance on how to build and maintain the security operations program. There will be a technical demonstration of log analysis from a system that has been attacked with an analysis of the target system's logs to simulate the incident response process. We will close a conclusion with some final thoughts.

The primary audience of this paper is security professionals seeking to establish, enhance or modify a security operations program utilizing log analysis tools to assist with incident response. The secondary audience for this paper are executive and management stakeholders who are responsible for security operations, or who have responsibilities that involve security operations (e.g. Chief Information Security Officer, Chief Information Officer or respective subordinates).

The scope of this paper is limited the establishment of a framework for said security operations program, and establishing processes for log analysis utilizing tools to assist with incident response.

Given that enterprise environments can contain near-infinite configurations, the technical demonstration portion of the paper will be limited to a single attack system, a single victim and automatic forwarding of log data into our analysis tool, in-line with an incident handling process. Information security policies, the "aggregate of directives, regulations, and practices that prescribes how an organization manages, protects, and distributes information," (Kissel, 2013) related to incident response, log collection and

analysis will be addressed, but not in detail. The scope of this paper does not extended to IT operations related to the transmission, storage, retention, backup, or destruction of log data.

Although the technical portion of this paper discusses Kali Linux, Metasploitable Linux and Splunk Light, they are representative technologies for illustrative purposes only. This paper does not function as a 'how-to' on the setup, configuration and use of these products beyond their use in service of this paper's stated intent.

2. Security Operations

The fundamental role of a security operations program is to articulate the organization's security posture for business, executive, management and technical stakeholders. Security posture is defined as "the security status of an enterprise's networks, information, and systems based in IA (information assurance) resources (e.g. people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes" (Kissel, 2013). Quantifying the organization's security posture in language that these stakeholders understand empowers them to make educated, short and long-term decisions about budget, planning and strategy in alignment with the business' needs. More specifically, the responsibility of a security operations program is to continuously monitor, detect, analyze, report and advise on events and incidents.

An **event** is any observable occurrence in a system or network (Cichonski, Millar, Grance & Scarfone, 2012). Events can either be experienced directly or shown to have occurred. Evidence for events is typically captured in log files (technical), human created logs, or other reporting mechanisms such as email, ticketing systems, phone calls, voice mails, etc.

An **incident (**or adverse event) is an occurrence that "actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits" or "that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies" (Cichonski et al., 2012). Incidents are typically detected as deviations from the

normal state of the network and systems. Effectively, an incident indicates harm or the attempt to harm.

In analyzing events, the incident handler should be capable of separating regular events that constitute baseline of activity from adverse events, or incidents. *Events* that indicate significant risk that are classified as *incidents* should be documented and escalated to appropriate stakeholders. Event and incident information should be retained beyond the immediate incident handling time window to meet audit, compliance and contractual requirements (as appropriate for the organization).

2.1 Security Operations Goals

A security operations program should endeavor to achieve the following goals:

- To monitor, report, escalate and advise on security incidents.
- To collaborate with stakeholders across the organization and empower stakeholders with relevant data.
- To utilize standard, enterprise-level security solutions across the organization.
- To collect and retain relevant data for security operations, investigations and audit purposes.
- To perform periodic security control review based on quantifiable security operations data.
- To establish a cadence of monitoring, reporting and escalating security incidents as a reactive security service.
- To establish the foundations of a threat intelligence operations as a proactive security service.

2.2 Key Performance Indicators

Establishing key performance indicators (KPIs) is an important practice for security operations. Key Performance Indicators are "quantifiable measurements, agreed to beforehand, that reflect the critical success factors of an organization" (Rey, 2015). These permit the security operations team to document their performance and the security posture of the organization through the use of metrics. Metrics are "tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data." Although

metrics may be unfamiliar to technical IT and security professionals, these practices are essential to communicating with business and executive stakeholders in a language the stakeholders understand. This communication is essential to proving the team's value to the organization and quantifying the case to additional budget for staff, tools and services.

A sample of key performance indicators may include (but is not limited to):

- Number of security events logged.
- Number of security incidents escalated and ticketed.
- Number of server and infrastructure systems monitored.
- Number of endpoint systems monitored.
- Number of user and service accounts monitored.
- Number of user groups (local and central) monitored.
- Number of security controls monitored, reviewed and revised.
- Number of security policies, procedures, standards and guidelines reviewed per security operations activity.

2.3 Team Types – Blue, Red and Purple

Derived from military and intelligence practices, the information security industry has adopted the concept of defence ("Blue Team") and offence ("Red Team") to define and segregate roles and responsibilities.

The Blue Team "identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture" (Kissel, 2013). Blue Teams typically perform three primary tasks, "detect, mitigate and prevent" (Melcalf, 2015) through automated, machine-driven processes and tools. The SOC (Security Operations Center) is typically constituted of Blue Team members.

Due to the type and range of event data that this team has access to, there may be policy, contractual, or third-party compliance restrictions that determine if off-shore or

third-parties can have access to this data. The security operations staff may also be subject to specialized data privacy training.

In contrast, the Red Team is "a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment." (Kissel, 2013). Red Team actions of "recon, escalate, and persist" (Melcalf, 2015) are achieved through manual, human-driven processes.

Purple Teams are a more recent term for activities on which both Blue Teams and Red Teams collaborate. Knowledge of the organization's security is taken from the Blue Team, knowledge of the organization's weaknesses is taken from the Red team and combined (Kikta, 2013). Management should ensure that the collaboration of blue and red teams takes advantage of their respective areas of expertise (defence and offence). After the engagement, both teams should collaborate to discuss the strengths and weaknesses of their efforts, lessons learned, and any proposed changes to technical controls and processes.

2.4 Event and Incident Workflow

A typical workflow for security operations and incident response would involve two primary teams; the SOC (Analysts) and CIRT (Incident Handlers). The SOC is responsible for collecting and analyzing the events, the CIRT is responsible to taking action and performing additional investigations. This workflow permits a segregation of duties in which one team (SOC) is responsible for the collection, retention and analysis of log data (events), but a separate team (CIRT) is responsible for actions based on the analysis of said event data (incidents).

- Event collection.
- Event analysis by Security Operations team (SOC).

- Classification of an event as an incident, either via automation and/or manually via human-driven analysis by the SOC.
- Logging of the incident in a centralized system available to stakeholders and the CIRT (Incident Handler) team (e.g. ticketing system, mailing list).
- Assignation of the incident to the CIRT and/or other appropriate stakeholders for additional investigation and/or action.
- Lessons learned, documentation, process and/or technical control changes after the incident (as appropriate).

2.5 Security Operations Framework and Procedures

The steps below are included to assist with establishing a framework for security operations and log analysis.

Step 1 - Classify Data

Prioritizing the data most valuable to the organization is absolutely critical and should be considered the first step for any security operations program. This exercise will direct the SOC where to focus their attention, both with technical solutions and human-driven analysis of events. Based on the nature of the business, this focus may be on credit card data, health care information, intellectual property, personally identifiable information (PII) or a combination of these and other data types. Third-party compliance requirements can dictate required monitoring and security controls for some data types (e.g. credit card data under PCI-DSS). In order of priority, third-party compliance requirements must be addressed first, then contractual requirements with business partners, then internal policies and standards. This outside-to-inside model is designed to prioritize requirements that are dictated by third-parties and pose the most immediate risk to the organization's ability to operate. Violations of internal security policies and standards are important, but these issues can likely be handled within the organization at a different priority than those visible outside the organization.

Third-party compliance requirements may be limited to a very small portion of the organization's data, systems and assets, but the security practices established to meet those requirements engage executive, management and technical stakeholders. That

engagement can be leveraged to widen security practices across the organization if they are perceived to have value.

Step 2 – Establish Documentation

Security operations is too complicated and variable to fit into a how-to document, but establishing, developing and maintaining baseline documentation is invaluable. At a minimum, detail what tools are in-scope for security operations, relevant stakeholders in the organization, and a workflow for regular and escalated response. More detail can be incorporated as the team and operations mature, but this baseline document should serve as a reference so the security operations analyst understands what resources they have, and to whom they can turn for assistance or escalation.

Step 3 – Identify and Implement Training

Security operations will engage the use of multiple tools on a daily basis. In addition to log collection and analysis tools, these can include IPS/IDS, vulnerability management, endpoint protection, and ticketing systems. The SOC analysts should be provided with, at a minimum, baseline training on the tools which they will access to conduct investigations. Additional, in-depth training with key solutions will empower the security operations staff to implement efficiencies with the tools and processes. Vendor-specific certifications and training with these tools can provide a uniform baseline of knowledge and provide transferrable career benefits for the security operations staff.

Step 4 - Ensure Access to Log Data

The security operations team should be provided with read-only access to as much log data as possible. The basis of this effort should be the data classification exercise conducted as step one of this guide. Obtaining access to this data will require establishing and maintaining relationships with technical stakeholders within the organization. The more log data that can be collected and analyzed from as wide a variety of systems, the more likely that incidents can be detected. However, simply having access to this much log data is not a solution, it is the first step in providing the security operations team with what they require.

Step 5 – Monitor Events Regularly, Establish Baselines

The most effective way to understand the difference between events and incidents in an environment is to perform continuous monitoring and regular analysis of events.

Performing these activities regularly (preferably daily) enables the security operations team to gain an understanding of regular, baseline activity in the environment. This baseline activity will likely constitute the majority of events that will be monitored and analyzed. A significant caveat is that "because it can take considerable effort to understand the significance of log entries, the initial days, weeks, or even months of performing the log analysis process are the most challenging and time-consuming" (Kent & Souppaya, 2016). This time-consuming effort will pay off over time, as the security operations team is able to perform more focused analysis once they have a good day-to-day understanding of what occurs regularly in the environment.

Step 6 - Automation, Automation, Automation

Another benefit to understanding the baseline events in an environment is to leverage the power of automation. The security operations team should be able to implement automated filtering of events to both report effectively on "status quo" and to create alerts and dashboards for events that may be classified as incidents.

To borrow a concept from audio engineering, the difference between events and incidents is analogous to a signal-to-noise radio. A non-technical definition is that this radio "compares the level of a desired signal (such as music) to the level of background noise" (Sengpiel, 2016). In our case, events are the noise and incidents are the signal.

An appropriate log collection and analysis tool will assist with three significant challenges related to log management; "Many Log Sources", "Inconsistent Log Content" and "Inconsistent Timestamps" (Kent & Souppaya, 2016).

Step 7 – Log Analysis

The procedures and processes for log analysis will vary from organization to organization and even team to team based on a wide range of variables. These variables can include the ratio of events to security operations staff, the tools employed by those teams, and the teams's required turnaround for addressing incidents per Service Level Agreements (SLAs). That said, there are some fundamental procedures that should be followed, regardless of these variables:

- Monitor events regularly and consistently. The frequency of monitoring can vary based on the tools involved, the degree of automation and the number of security operations analysts available. For example, one tool may provide incident data

for the prior 24 hours which creates a consistent timeframe from which to respond to a "snapshot" of the organization's security posture. In conjunction, another tool, such as endpoint protection, may provide near real-time incident data that would be analyzed and escalated to stakeholders immediately.

- Move incidents into a centralized database or ticketing system as quickly in the analysis workflow as possible. This will initiate an incident timeline that other stakeholders engage with based on their level of involvement. This system may be as complex as a ticketing system, or as simple as a shared mailbox. This also creates a central audit point to reconstruct the incident response as part of a lessons learned session (as appropriate).
- Don't re-invent the wheel. Leverage your internal help desk, knowledge base, and trusted stakeholders in the organization when analyzing incidents. These resources can assist with determining application owners, system owners and data types.

Step 8 – Reporting

In addition to metrics and key performance indicators, a valuable tool that the security operations team can utilize is effective reporting to executive, management and technical stakeholders. The security operations team is in a unique position of having access to more comprehensive data on the activities and security posture of the organization than any other department. Over time, this data can be used to generate valuable reports for stakeholders that indicate trends, user behavior and efficiencies or deficiencies related to IT and security controls. This may fall outside the typical portfolio of security operations, but the cross-pollination of this data into other areas of the organization can improve executive support of the team and associated technologies.

Step 9 – Care and Feeding (The Human Factor)

The security operations team may encounter resistance from executive and management stakeholders regarding the staff hours and resources required to build this baseline. The short-term view would be to only observe, analyze and react to incidents. However, this reactionary approach, while applicable in a live incident scenario, poses risks to the integrity and stability of the security operations team. The process of manually viewing, analyzing and reacting to incidents is time-consuming and prone to

human-error. Initially, this proves to be a challenging job. Over time, familiarity with the tools, processes and environment can result in a repetitious and unfulfilling job. This will work against the organization, in that highly knowledgeable and technical staff can lose interest, "burn out" and leave. In this scenario, the organization will lose valuable personnel and hands-on skill to handle security operations.

Personnel management is outside the scope of this paper, but utilizing automation will help the security operations team focus their energies on relevant and interesting tasks, instead of grinding through repetitive and time-consuming events. True incidents will engage the team, provide them with an opportunity to contribute to the overall security program and help them develop and maintain technical skills of value to the organization and their individual careers.

The prior guidelines that we have discussed (prioritize data, daily monitoring, baselines and automation) lead us to the most important element in your security operation and incident handling program; your staff. Engagement with stakeholders can assist with defining scope. Tools, software and automation can present relevant events and incidents based on the aforementioned scope. But the success or failure of any security operations program will rest on the shoulders of your analysts, those responsible for applying their knowledge and skills to the data presented to them. Dashboards, emails and alerts are all important tools, but the responsiveness, insight and actions of your staff are crucial.

Step 10 - Empower Stakeholders

Now that you've convinced stakeholders from different areas around the organization to provide you with their log data, return the favor. Provide stakeholders with access to their own data through the viewfinder of your security tools (e.g. Splunk Light) as search queries, alerts and dashboards. They will likely find value in seeing their data in a different light as part of their regular operations, and you will benefit from their engagement during an incident if they already have access to the same data as you.

Step 11 - Maintain Key Relationships

We've identified that one of the goals of the security operations team is to monitor, report, escalate and advise on security incidents. The obvious next question should be "who acts on these results?" A wide range of stakeholders may be involved,

including "architecture, audit/compliance, infrastructure engineers, development, contract management and IT leadership" (Woods, 2012). These stakeholders, directly or indirectly, affect the remediation, enforcement, maintenance, funding and support of your security operations. Individual communication with these stakeholders on events and incidents that concern them, with sensitivity to their existing workload can help establish trust and support.

3. Technical Demonstration

The test environment for this technical demonstration consists of two systems; a Metasploitable Linux system and a Kali Linux 2.0 system. Both systems have been configured as virtual machines on the same subnet with access to the internet. The Metasploitable Linux system is "an intentionally vulnerable Linux virtual machine, typically used to conduct security training, test security tools, and practice common penetration testing techniques" (Metasploitable, 2012). This target system has been selected to present the greatest number of events and incidents in the shortest time possible for illustrative purposes. The Kali Linux 2.0 system is a standard distribution, updated as of February 2016.

The log analysis tool for this demonstration is Splunk Light, a log search and analysis tool intended for small IT environments, with a default limit of 500mb/day of log data. Splunk Light has been selected for illustrative purposes, given the product's feature set, cross-platform support and cost (free per the software license agreement (Splunk, Software License Agreement, 2016). No explicit recommendation or advertisement of Splunk (the corporation) or their products is intended.

The attack methodology for this test entails using reconnaissance tools and exploitation tools included in the standard Kali Linux 2.0 distribution against the Metasploitable Linux system. Exploitation of the system will be dependent on the information gathered during the reconnaissance phase.

It is anticipated that event and incident data will include reconnaissance efforts as represented by log data on the Metasploitable Linux system. Efforts to query and exploit network services and unusual user activity involving user accounts should also be recorded.

Colin Chisholm, chisholm.colin@gmail.com

3.1 Executing the Attack

A series of attacks were performed against the target system (Metasploitable) from the source system (Kali Linux). The primary tool used for the attack was Armitage, a graphical front-end interface for the Metasploit penetration testing solution. Armitage was used to perform nmap and MSF scans of the target system, the resulting data from which was used to create and execute attack against which the Metasploitable system was vulnerable. Additionally, a flood of attacks (**Attacks > Hail Mary**) were executed against the target system. The total window for these attacks was approximately eight hours.

3.2 Validating the Data

The hostname for the target system is "metasploitable." Querying Splunk Light for this hostname (host=metasploitable) for the date and time range of the attack (02/05/2016 08:30 through 02/05/2016 14:00) discloses a total of 75,491 events.

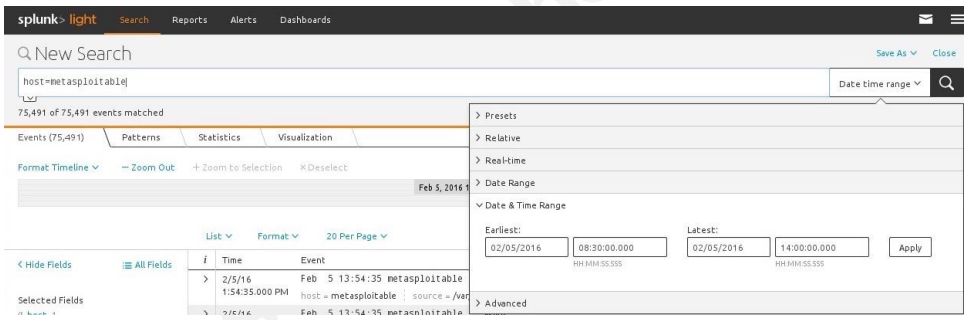


***Figure 1**: Host query with data/time range*

3.3 Creating the Dashboard

In addition to the ability to query "raw" log data to which it has access, Splunk Light provides add-ons that provide pre-built inputs for specific monitoring items. In this instance the 'Splunk Add-on for *Nix' has been installed (**Administrator > Data > Add-Ons > Splunk Add-on for *Nix**) to analyze the event data more efficiently. A full list of the pre-built data inputs provided by this add-on is provided in **Appendix B – Splunk Data Inputs**. The complete list of event types can be accessed within the Splunk administrative menu at **Knowledge > Event types**.

A dashboard has been created in Splunk Light utilizing the supplied data inputs and event types to highlight a range of events on a unix system that may initiate an

incident investigation. The complete list of the queries used for this dashboard is provided in **Appendix A – Dashboard Queries.**

Table 1: Event Types and Actions Monitored

Event Type	Monitored Action
Account Management	groupadd, groupdel, linux-password-change, linux-password-change-failed, useradd, userdel
Anomalies	useraccounts_anomalies
Authentication	pam_unix_authentication, failed login
Privileged Access	su_root_session, su_session
SSH	ssh_check_pass, ssh_close, ssh_open, ssh_authentication
System Performance	nix_process_kill, nix_runlevel_change

3.4 Analysis

Assuming the role of a security operations analyst, reviewing our dashboard will show several events that require further attention.

3.4.1 SSH (ssh_authentication) Dashboard Panel

SSH (ssh_authentication)

i	Time	Event
>	2/5/16 9:23:19.000 AM	Feb 5 09:23:19 metasploitable sshd[9099]: Failed password for invalid user support from 10.0.1.156 port 39201 ssh2
>	2/5/16 9:23:17.000 AM	Feb 5 09:23:17 metasploitable sshd[9099]: Invalid user support from 10.0.1.156
>	2/5/16 9:23:00.000 AM	Feb 5 09:23:00 metasploitable sshd[8980]: Failed password for invalid user sysadmin from 10.0.1.156 port 45847 ssh2
>	2/5/16 9:22:58.000 AM	Feb 5 09:22:58 metasploitable sshd[8980]: Invalid user sysadmin from 10.0.1.156
>	2/5/16 9:22:48.000 AM	Feb 5 09:22:48 metasploitable sshd[8960]: Invalid user mateidu from 10.0.1.156

***Figure 2**: ssh_authentication failure events*

The **SSH (sshd_authentication)** panel is reporting five (5) SSH authentication failures, using individual user name in less than two (2) minutes. The attempted user names are those of typical privileged users (e.g. sysadmin, support). The authentication attempts also originate from rotating source ports (e.g. 39201, 45847).

3.4.2 SSH (ssh_check_pass) Dashboard Panel

SSH (ssh_check_pass)

i	Time	Event
>	2/5/16 9:23:17.000 AM	Feb 5 09:23:17 metasploitable sshd[9099]: pam_unix(sshd:auth): check pass; user unknown
>	2/5/16 9:22:58.000 AM	Feb 5 09:22:58 metasploitable sshd[8980]: pam_unix(sshd:auth): check pass; user unknown

***Figure 3**: "ssh_check_pass" events*

The **SSH (ssh_check_pass)** panel is reporting two SSH authentication attempts using unknown user logins. These events occurred within two minutes of each other from two, separate source ports.

3.4.3 Authentication (Failed Login) Dashboard Panel

Authentication (Failed Login)

i	Time	Event
>	2/5/16 11:52:33.000 AM	Feb 5 11:52:33 kali gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
>	2/5/16 9:23:19.000 AM	Feb 5 09:23:19 metasploitable sshd[9099]: Failed password for invalid user support from 10.0.1.156 port 39201 ssh2
>	2/5/16 9:23:17.000 AM	Feb 5 09:23:17 metasploitable sshd[9099]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.156
>	2/5/16 9:23:00.000 AM	Feb 5 09:23:00 metasploitable sshd[8980]: Failed password for invalid user sysadmin from 10.0.1.156 port 45847 ssh2
>	2/5/16 9:22:58.000 AM	Feb 5 09:22:58 metasploitable sshd[8980]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.156

***Figure 4**: Authentication and Password Failure events*

The **Authentication – Failed Login** panel is reporting five (5) authentication failures of various types. The first four of which occur within two minutes and match the **ssh_authentication** event data detailed above.

3.4.4 Authentication (pam_unix_authentication) Dashboard Panel

Authentication (pam_unix_authentication)

i	Time	Event
>	2/5/16 11:52:33.000 AM	Feb 5 11:52:33 kali gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root host = kali source = /var/log/auth.log sourcetype = auth-4

***Figure 5**: pam_unix_authentication events*

The **Authentication (pam_unix_authentication)** panel is reporting a single, failed instance of authentication failure of the root account. This matches the failed login failure reported in the **failed login** event data above.

3.5 Analysis Conclusion and Next Steps

The event data reported in the Splunk Light dashboards strongly suggests a scripted or automated attack against the monitored system (metasploitable). The data indicates that the attack has originated from a single source IP address (10.0.1.156) and has attempted to authenticate to the system using privileged accounts in rapid succession while rotating source ports.

These events qualify as an **incident** and necessitate escalation. The system owner should be notified (preferably via a central ticketing system) with the recommendation that the system be inspected. Any indication of unauthorized changes or activity on this system would likely require removal from the network.

In this demonstration, we have demonstrated how a log collection and analysis solution has collected and classified event data on a single system. This event data has been made available to the security operations analyst in a single location, with the convenience of showing questionable activity using different monitoring criteria. Rather than hunting through individual system logs, this solution and configuration has reduced the time between incident, analysis and escalation.

4. Conclusion

As stated earlier in this paper, the security operations team is in a unique position, having access to a wide range of log data from a variety of systems. This width and breadth of data is unlikely to be held by any other department within the organization. The data, tools and skills utilized by the security operations team on a daily basis to investigate events and handle incidents can benefit the organization in both immediate and long-term ways. The immediate benefit of day-to-day analysis results in awareness of the organization's technical operations, security posture and the ability to escalate incidents further investigation or remediation.

Colin Chisholm, chisholm.colin@gmail.com

The longer-term benefit of the security operations team can transcend day-to-day security operations. Using metrics and key performance indicators, it is possible to quantify the success and failure of your security and IT departments. This view can influence strategic planning, the selection and use of tools and solutions in the organization and even staffing. In addition, retaining log data in a single location can prove invaluable to meet compliance requirements and to assist audit efforts.

To revisit the major security operations guidelines from earlier; work with executive, business and technical stakeholders to classify your organization's data. This will assist your team with understanding where to focus their efforts. Establish and develop documentation so your team understands the tools at their disposal, the standard processes they should follow and the stakeholders across the organization they can engage as needed. Ensure that your team has appropriate training and support. Leverage automation as much as possible to separate the "signal" from the "noise" and concentrate your efforts on those assets most valuable to your organization, per your data classification efforts.

Monitor your systems and tools regularly to act on incidents when they occur and to develop and mature your baseline activity models. Develop reporting (short, medium, and long-term) that meets the needs and interests of your audience; business, technical, management and executive. Collect as much data as possible, engage stakeholders outside of your department, establish and maintain good relationships.

Above all, do not forget that your fundamental role is to articulate the organization's security posture. Capture the data, identify the incidents, report and advise. Engage your team to affect positive change within the organization by communicating in a helpful manner and build trust and value.

Colin Chisholm, chisholm.colin@gmail.com

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). Computer *Security Incident Handling Guide*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., . . . Stine, K. (2011, September). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Kent, K., & Souppaya, M. (2006, September). *Guide to Computer Security Log Management*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006, August). *Guide to Integrating Forensic Techniques into Incident Response*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Kissel, R. (2013, May). *Glossary of Key Information Security Terms*. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Kit, M. (2013). *Seeing Purple: Hybrid Security Teams for the Enterprise - BSides Jackson 2013*. Retrieved from http://www.slideshare.net/beltface/hybrid-talk

Metasploitable Description. (2012). Retrieved from http://sourceforge.net/projects/metasploitable/

Metcalf, S. (2015). *Red vs. Blue: Modern Active Directory Attacks, Detection, & Protection*. Retrieved from https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf

Noise Calculation Calculator. (2016). Retrieved from http://www.sengpielaudio.com/calculator-noise.htm

Rey, J. F. (2015). *Key Performance Indicators (KPI)*. Retrieved from http://management.about.com/cs/generalmanagement/a/keyperfindic.htm

Skoudis, E (2010) *Incident Handling Step-by-Step and Computer Crime Investigation. SEC504: Hacker tools, techniques, exploits and Incident Handling*. Bethesda, MD: SANS Institute.

Colin Chisholm, chisholm.colin@gmail.com

Spunk Software License Agreement. (2016). Retrieved from http://www.splunk.com/en_us/legal/splunk-software-license-agreement.html

Colin Chisholm, chisholm.colin@gmail.com

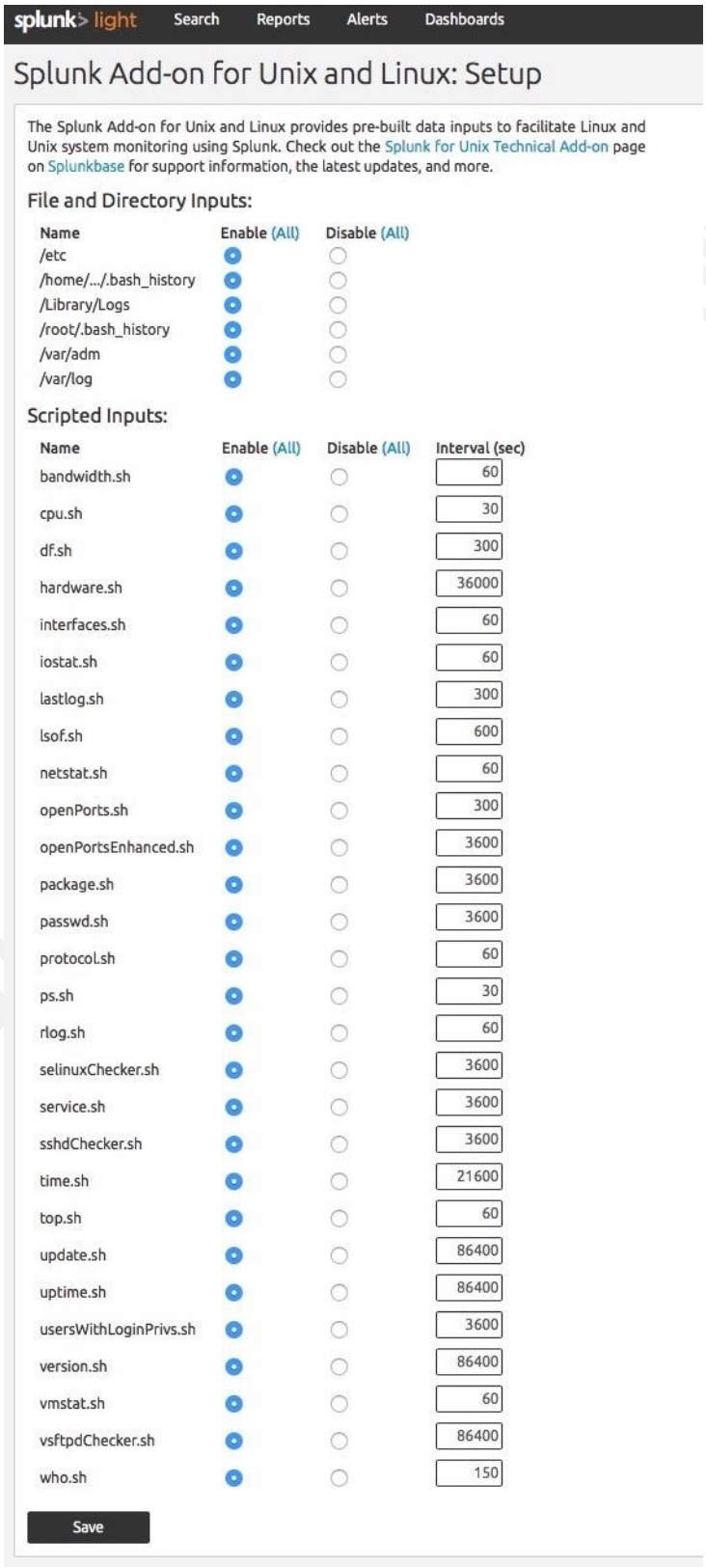
Appendix A – Dashboard Queries

Event Type	Event Title	Query
Account Management	groupadd	(NOT sourcetype=stash) useradd group
Account Management	groupdel	(NOT sourcetype=stash) userdel group
Account Management	linux-password-change	(NOT sourcetype=stash) process=passwd password changed
Account Management	linux-password-change-failed	(NOT sourcetype=stash) process=passwd password change failed
Account Management	useradd	(NOT sourcetype=stash) useradd user
Account Management	userdel	(NOT sourcetype=stash) userdel user
Anomalies	useraccounts_anomalous	sourcetype=*:UserAccounts NOT password=x NOT password=*
Authentication	pam_unix_authentication	(NOT sourcetype=stash) NOT sourcetype=ossec pam_unix (gdm OR sudo OR su) ("authentication failure" OR "session opened")
Authentication	Failed Login	(NOT sourcetype=stash) "failed login" OR "FAILED LOGIN" OR "Authentication failure" OR "Failed to authenticate user" OR "authentication ERROR" OR "Failed password for"
Privileged Access	Failed_SU	(NOT sourcetype=stash) ("failed SU to another user" AND "Agent platform:" AND "linux-x86") OR ("failed SU to another user" AND "authentication failure" AND "for su service") OR ("failed SU to another user" AND logname=*) OR (exe="/bin/su" AND res="failed") OR (FAILED su for) OR (source="/var/adm/sulog" SU "-") OR ("BAD SU ")
Privileged Access	su_root_session	(NOT sourcetype=stash) su: session root
Privileged Access	su_session	(NOT sourcetype=stash) su: session
SSH	ssh_check_pass	(NOT sourcetype=stash) sshd check pass user unknown (punct="__*::__()[]:__;__" OR punct="*__::_*_[]:_(:):__;__")
SSH	ssh_close	(NOT sourcetype=stash) punct="*__::_*_[]:____*..." OR punct="*__::_*_[]:_(:):_____" OR

Colin Chisholm, chisholm.colin@gmail.com

		punct="*__::_*_()[]:_____" sshd (Closing connection to) OR (Connection closed by) OR (session closed)
SSH	ssh_open	(NOT sourcetype=stash) punct="*__::_*_[]:_(:):_____*__(=)" sshd (session opened) OR (connection from)
SSH	sshd_authentication	(NOT sourcetype=stash) NOT sourcetype=ossec sshd (((Accepted OR Failed OR failure OR "Invalid user" OR "authentication error") from) OR "Authorized to" OR "Authentication tried" OR "Login restricted")
System Performance	nix_process_kill	(NOT sourcetype=stash) exiting signal 15
System Performance	nix_runlevel_change	(NOT sourcetype=stash) init: punct="__::_*:_*"

Appendix B – Splunk Data Inputs



Colin Chisholm, chisholm.colin@gmail.com