ISE6100 GIAC Enterprises Final Lessons Learned

Introduction

The following is Lessons Learned from the ISE 6100 project which commenced on March 22nd 2016. The objective of this project was to evaluate, select, and implement an open source Security Information and Event Management (SIEM) solution for the fictional corporation known as GIAC Enterprises. GIAC Enterprises is in the business of collecting fortunes from direct employees and contractors. These fortunes are GIAC Enterprises intellectual property. The ideal SIEM will enhance the detective capacity of GIAC Enterprises.

The following assumptions were made in carrying out this assignment:

- The mobile application would submit fortunes to a web service/application for processing.
- The web service/application would forward submissions to a database for permanent storage.
- The database server would be properly segmented and protected.

What choices were made and why?

The first choice that the team made was selection of a suitable open source SIEM product. To make this decision easier, the team constructed a feature matrix containing the following characteristics:

- Linux Support
- Windows Support
- Active Directory Integration
- Role Based Access Control
- Log Correlation
- Host Intrusion Detection Support
- Network Intrusion Detection Support
- Long Term Log Storage
- Real-Time Search
- Tagged Elements
- Active Development
- Community Support
- Threat Intelligence Feeds
- Reporting Dashboard Support
- Commercial Upgrade Path

Support for each of these features was evaluated for each of the products under consideration. At the outset of evaluation, OSSIM was by far the most capable and well-supported open source SIEM product in the group. The evaluated products included:

- OSSEC
- ELK
- ELSA
- Graylog
- OpenSOC
- Prelude
- Security Onion
- FIDO
- LOGalyze

In addition, to the basic features of a SIEM product, the team considered two absolutely necessary for an open source initiative. First, the product must be under active development and have a solid user base. Second, it would be very attractive if the product had a commercial upgrade path. These characteristics set OSSIM apart from many of the others. In fact, official documentation for OSSIM as a product does not exist. This is because the experience with OSSIM is so close to AlienVault's USM commercial product that they don't feel it necessary to produce alternate documentation. ELSA, a part of the fully-featured Security Onion Linux distribution was another obvious choice, but its use has already been well-documented in the 2013 Richard Bejtlich book "The Practice of Network Security Monitoring".

After selection of the SIEM product, the next challenge was collaborative development of the solution. Fortunately, one team member had an AWS account which could be used to host the fictional corporation's assets. Once AWS was identified as the platform for deployment, the team created the project plan and moved ahead with installation.

Challenges

During deployment of the GIAC Enterprises infrastructure, the first challenge was AWS support for OSSIM. Since there was no AMI image for the OSSIM distro, one had to be created using VMWare Workstation and then converted using the VMWare OVF tool. This caused some logistics challenges as the resulting OVA file had to be uploaded and imported into AWS. Upload and import took several hours to complete. Basic installation of the sensor had to be completed in advance as well. This meant that address schemes had to be known up-front.

In addition, after the OSSIM sensor had been imported into AWS, some challenges arose due to difficulties with addressing. When the OSSIM instance was initially provisioned in AWS an IP address other than the original setup IP was assigned to the instance. This caused difficulty in

accessing the sensor. Consequently, the OSSIM sensor instance had to be destroyed and re-provisioned with the IP address used during setup to resolve the issue.

After the OSSIM sensor was completely operational in the virtual environment attention was turned to the servers and infrastructure operating all within AWS. A public-facing Wordpress server was configured with a backend MySQL database in a protected network, to simulate GIAC's fortune cookie infrastructure. Windows servers running Server 2008 and Server 2012 were deployed to simulate the Active Directory infrastructure supporting the GIAC office environment. Deployment of the OSSEC HIDS agent to the Windows environment took a number of tries, with issues in the AWS Security Group configuration and Windows Firewall due to the change of IP address described above, as well as changes to the User Account Control and Group Policy for NTLM session security.

The AMI Linux distribution did not natively support rsyslog communication over UDP. As a result, the team researched solutions and found that the OSSIM sensor configuration could be altered to support rsyslog over TCP. This appeared to be the best solution since it was also a first step toward rsyslog over TLS. Due to the nature of the configuration change, the OSSIM sensor "Jailbreak" shell access had to be used. The rsyslog and iptables configurations were updated to support this configuration.

An interesting note is that this "Jailbreak" access also allows several security enhancements to be made to the OSSIM sensor. These enhancements include rsyslog over TLS, ssh public key authentication, and stricter firewall configuration.

As an overall project, the team had several discussions regarding scope creep. Eventually the team settled on focusing efforts toward log correlation and analysis, rather than trying to incorporate all of the features available in OSSIM. As a result, ideas that were outside of this scope were abandoned or included in the future development section of the completed paper.

Lessons

In general, the OSSIM installation worked as advertised short of a few performance issues. Many of the challenges encountered were due to the deployment environment. Using AWS to host the services also was convenient, especially in a distributed team environment. However, it

also limited options for configuring information sources within the environment. Other useful sources that would have been realistic given the target scenario would include:

- Web Application Firewall
- Network Firewall
- Network Intrusion Detection System
- Network Infrastructure (routers and switches)
- Mobile Device Management Solution
- Flow Data

These sources would also have allowed further prioritization of resources and stronger correlative evidence. The configuration wouldn't have changed significantly and the basic monitoring premise remains the same. This would have increased the realism of the simulated environment.

Conclusion

While there were certainly challenges in configuration and support of OSSIM there weren't any challenges that couldn't be overcome. Despite these challenges, OSSIM remains the best option among all of those considered due to the supported features and an upgrade path to a commercially supported product. Deployment of the GIAC Enterprises architecture within AWS brought with it some complications and limitations but was suitable for a test instance. Overall, the project was executed without much trouble.

Last Updated: August 9th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Reboot - NOVA 2020	Arlington, VAUS	Aug 10, 2020 - Aug 15, 2020	Live Event
SANS FOR508 Sydney August 2020	Sydney, AU	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Virginia Beach 2020	Virginia Beach, VAUS	Aug 30, 2020 - Sep 04, 2020	Live Event
SANS London September 2020	London, GB	Sep 07, 2020 - Sep 12, 2020	Live Event
SANS Philippines 2020	Manila, PH	Sep 07, 2020 - Sep 19, 2020	Live Event
SANS Baltimore Fall 2020	Baltimore, MDUS	Sep 08, 2020 - Sep 13, 2020	Live Event
SANS Munich September 2020	Munich, DE	Sep 14, 2020 - Sep 19, 2020	Live Event
SANS Network Security 2020	Las Vegas, NVUS	Sep 20, 2020 - Sep 25, 2020	Live Event
SANS Australia Spring 2020	, AU	Sep 21, 2020 - Oct 03, 2020	Live Event
SANS Northern VA - Reston Fall 2020	Reston, VAUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS San Antonio Fall 2020	San Antonio, TXUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS FOR500 Milan 2020 (In Italian)	Milan, IT	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Amsterdam October 2020	Amsterdam, NL	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Brussels October 2020	Brussels, BE	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Prague October 2020	Prague, CZ	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS London October 2020	London, GB	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS Orlando 2020	Orlando, FLUS	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS October Singapore 2020	Singapore, SG	Oct 12, 2020 - Oct 24, 2020	Live Event
SANS Stockholm October 2020	Stockholm, SE	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Dallas Fall 2020	Dallas, TXUS	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Rome October 2020	Rome, IT	Oct 19, 2020 - Oct 24, 2020	Live Event
Cloud & DevOps Security 2020	Denver, COUS	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS SEC504 Rennes 2020 (In French)	Rennes, FR	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Geneva October 2020	Geneva, CH	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS SEC560 Lille 2020 (In French)	Lille, FR	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS San Francisco Fall 2020	San Francisco, CAUS	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS Cologne October 2020	Cologne, DE	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS Krakow November 2020	Krakow, PL	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS London November 2020	London, GB	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Rocky Mountain Fall 2020	Denver, COUS	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS DFIRCON 2020	Miami, FLUS	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Sydney 2020	Sydney, AU	Nov 02, 2020 - Nov 14, 2020	Live Event
SANS OnDemand	OnlineUS	Anytime	Self Paced
SANS SelfStudy	Books & MP3s OnlyUS	Anytime	Self Paced