Interested in learning more about security?

SANS Institute InfoSec Reading Room

ISE6100 GIAC Enterprises Final Lessons Learned

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.

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: April 23rd, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Doha 2018	OnlineQA	Apr 28, 2018 - May 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced