IDS Mod 2 Assignment

Audrey Long

206/06/2020

Objective

Given our case study on insider threat in Module 1,

- What type of host-based IDS would you use and how would you deploy this across the enterprise?
- Discuss any risks and challenges you would have in deploying your HIDS solution across an enterprise.
- Describe at least one attack that is best detected using HIDS
- Explain how the HIDS would be deployed in an enterprise environment to detect the attack.

Scenario

A Host Intrusion Detection System has three main parts containing sensors on the local host to create a data stream, a classifier which identifies suspicious events, and reporting either locally or network based logging. The HIDS generally collects and audits logs within the system such as operating system logs, system logs, application logs, and contains target based monitoring, for example sensor checking with a baseline to see if anything has changed or checking a checksum in the filesystem.

After doing some internet research it seems some of the top host based intrusion detection systems include: SolarWinds Security Event Manager, Papertrail, ManageEngine Event Log Analyzer, OSSEC, Sagan, and Splunk. I decided to choose Splunk as its a host based intrusion detection system complete with an enterprise edition which includes network based methods which can be installed on Windows, Linux, Mac, and contains a cloud based version.

Splunk comes with an intrusion detection and prevention system which can compare inbound and outbound network traffic against known signatures which cross references known signatures and behaviors known in the Splunk database. The tool then generates a report which collects data on unauthorized wireless access points found on the network and provides summarized behavior involving assets on the PCI domain. This report can be used as a tool to identify and remediate attack trends and behaviors that could lead to a significant threat. This intrusion detection tool can be configured to alert you to stop the intrusion attempt caught by the intrusion detection system.

Since Splunk is already a widely used tool there are many online documents that can step by step walk you through how to properly deploy this tool on the network. The first thing to do would be to collect information on the network and operating system which Splunk would be deployed on. Ensuring the hardware and virtual machines used for the deployment are correctly sized is also important to ensure the package installation will be used. The next step in implementing a Splunk HIDS is to get some automated detection. A HIDS will search through log messages for specific events that look like they may have recorded malicious activity. This is the core of a HIDS tool and the detection method that specifies which records to retrieve is set by policies and a rule base.

Distributed Splunk deployment is generally the way other enterprises install the software which consists of different systems using Splunk, the network would need to be set up in such a way where a head node contains all of the licenses and releases those licenses whenever an asset asks for one. A lot of information will need to be setup, in general a system administrator would be the best person for the job to set up the LDAP, and ensure the configuration files are all properly setup for the deployment, ensure the Splunk user has all of the appropriate permissions and access that it needs along with setting up a connection to the Splunk database. Figure 1 below demonstrates a way to deploy distributed splunk on a network using AWS along with various steps to setup the network properly for the deployment. Other

methods for deployment are viable but this deployment is interesting since we are connecting to the cloud server and we can easily and quickly access the Splunk database.

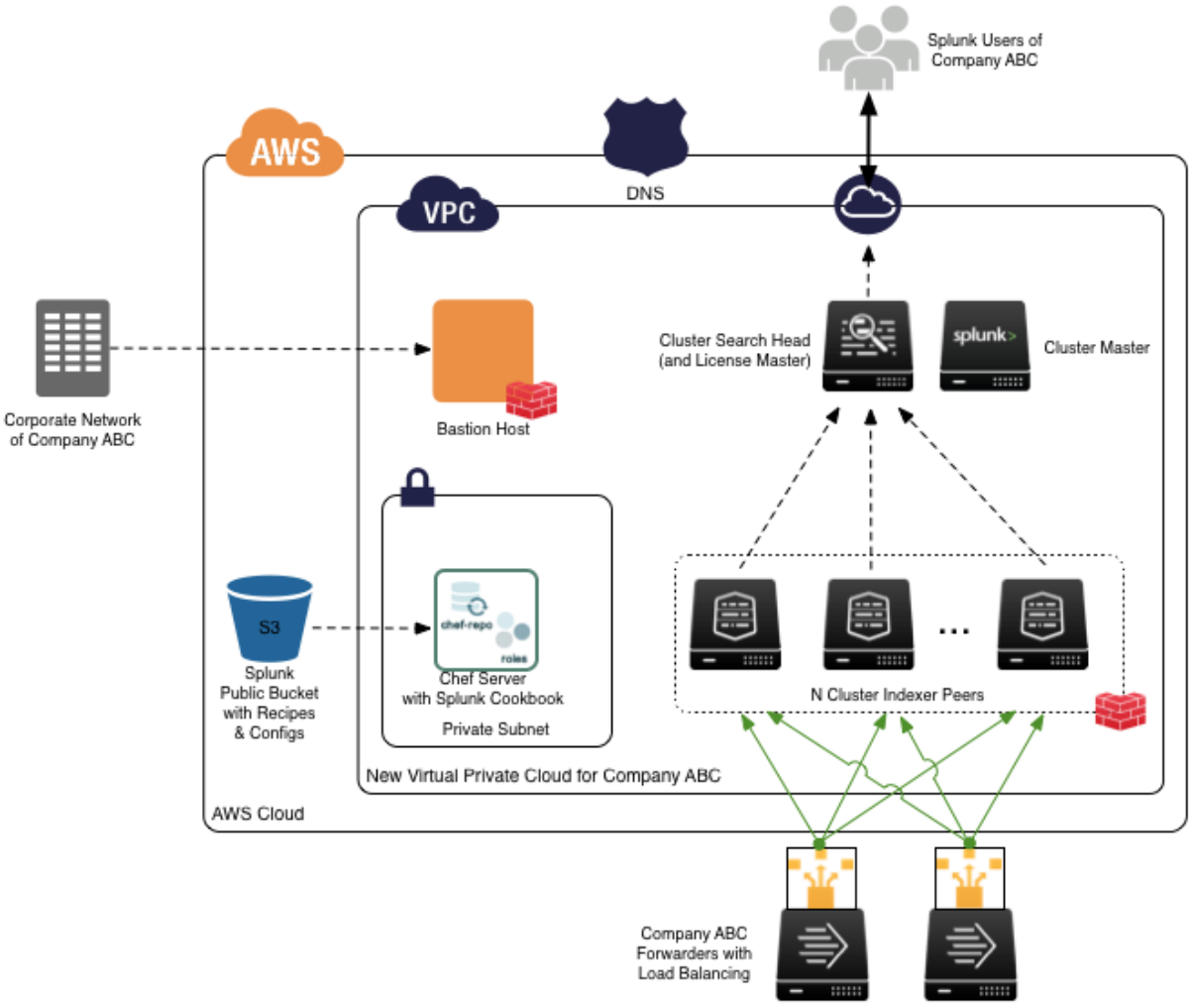

Figure 1: Distributed Splunk Cluster

Some challenges when deploying a HIDS is truly understanding the system as a whole for example which operating system we have access too and where to obtain the log files, which sensors are available on the server and how to create / use APIs to these sensors and creating scripts to write these sensor values to a file to be checked upon.

For Splunk in particular it might be problematic ensuring all of the correct permissions are given to the Splunk user during the process its important to ensure no backdoors were opened along the way for bad actors to break into the network, sometimes blindly installing packages leave open doors just enough for a bad actor to take advantage of a vulnerable network as well. Another important challenge to overcome will be the overwhelming amount of data that will be obtained after the intrusion detection system is setup and consuming data on the network. It will be important for a security analyst to thoroughly parse through the information and correctly determine the false positives away from the true positives. White and Black listing items are going to be the first things the analyst should do to ensure the

data consumption contains threats we are interested in alongside making the analyst less distracted with a potential threat that ends up being fine.

The host based intrusion detection system contains many great features for an enterprise to protect against many network outsider and insider threats. In general if some intrusion threshold has been tripped an alert to notify a security analyst that something needs to be investigated. Lack of intrusion detection allows an attacker to attempt attacks until a successful one is identified. Intrusion detection allows the attack to be identified long before a successful attack is likely.

Some Host based Intrusion Detection attacks clearly identified include operating system sources such as audit logs, security logs, user level activity monitoring, API logs which connect to host based services, and basic security logs such as password guessing, and administer access. Some extreme cases detected by HIDs include rootkits, remote controls and privilege elevation. Misrouting is an attack type I will dive a bit deeper into; Essentially this attack is classified as an API attack where an OS is "hooking" for rootkits, this attack is also known as the man-on-the-side-attack. Essentially this attack is a form of active attack where the attacker only has regular access to the communication channel, which allows him to read the traffic and insert new messages, but not to modify or delete messages sent by other participants. The attacker relies on a timing advantage to make sure that the response he sends to the request of a victim arrives before the legitimate response. Another major attack that can be prevented using a host based intrusion detection system is a trojan horse attack. Essentially having a HIDS installed on the system will detect right away malicious users or files have been added to the network and if any critical files have been tampered with.

References

https://www.comparitech.com/net-admin/hids-tools-software/ [1]
https://docs.splunk.com/Documentation/PCI/4.1.1/Install/IDSIPSAlertActivity [2]
https://wiki.splunk.com/Installing_Splunk_in_the_Enterprise_Step_by_Step [3]
https://www.redscan.com/news/the-key-challenges-of-intrusion-detection-and-how-to-overcome-them/ [4]
https://www.splunk.com/en_us/blog/cloud/deploy-your-own-splunk-cluster-on-aws-in-minutes.html [5]
https://owasp.org/www-community/controls/Intrusion_Detection [6]
https://en.wikipedia.org/wiki/Man-on-the-side_attack [7]