SPC-Project 2-Part 3

Yue Guan

1. **Summarize the strengths and limitations of each of the security software used in this project (Firewall, IDS/IPS and SIEM).**

Firewall:

From my point of view, I think firewall is effective for detection. It can set special rules basic on protocols, port and IP. And can block or drop the packet to protect the host. However, it is limited on the type of attack. It can't be partially block something by general rules but it's hard to monitor and detection, even alert. Also, it can be a high false positive rate because you just block traffics under a general rule.

The log can only generate the traffic related to the firewall, not all the network traffics here. From my point of view, it just mentions on what we block or drop in the firewall level and for the traffics we let them forwarded, it doesn't show the detail on that.

The scoop of the rules for firewall, it can only detect for IPs, protocols, ports etc. and do whether allow or disallow here. It can be functional in a generic way; however, it couldn't work well if we want to detect for some detailed event which has a deeper information needs to be set in rules. Or, if may set a rule either too tight and restrictive, or loose for ineffective.

IDS/IPS:

IDS/IPS does this very well. It can alert and monitor all the traffics among the host and networks. Also, gather all the traffics information together to monitoring and alert if needed. However, it can't filter the packet as a tunnel, just a monitoring tools we are using now. The false positive or true negative rate depend a lot on the rule setting from protocol to threshold etc.

The IDS/IPS has a detailed log on the alert. It's great to see where and why the traffic has been alerted from the log. However, it just focuses on the alert logs not on the holistic network traffic rules. There may be some situation that we didn't think of before or some case that we forget to set up the rule here. So, the log file may not be that useful. It just shows the result based on the rules that have already been settled.

The scoop of the rules for IDS/IPS depends on the software we used and the rule

management of that IDS/IPS. Based on Snort, there is a community rules that have already been set with some specific alerts respective from various attack. However, it just includes rules based on attacks that has already happened. IDS/IPS need to be improved to detect some unknown attacks using anomaly detection method with more advanced rules.

Security information and event management (SIEM):

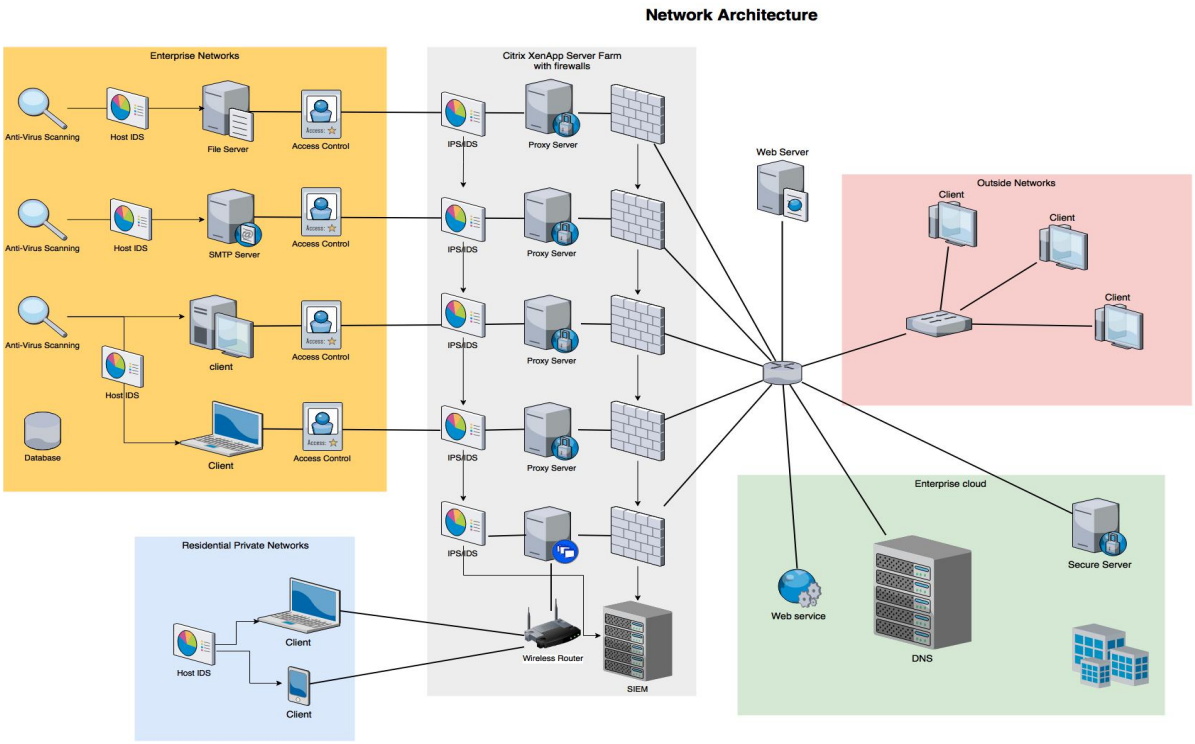
For SIEM, it's great that it can detect all the actions in one platform, from attack to victim, and our monitor status. It's like we can in charge of the entire network and host systems! It includes the data of both security information and events. The relevant data may be in multiple locations, and SIEM gather it. So, it's more efficient to see and view trends and patterns for cybersecurity management. However, the performance of SIEM based on the network devices, like firewall and IPS/IDS we are using for our network. Also, based on SIEM itself functional of log generation methods and analysis functions.

From a SIEM log perspective, it can be real-time monitoring and analysis on all platforms and network devices. It's better and quicker for defense and response based on all the logs from various places. In addition, instead of simple view form one network devices. We can check a sequences of security event from logs in SIEM now. The limitation here is SIEM is a management system, it needs large memory and configuration to establish one.

SIEM rules also based on the capability of the network devices. Plus, we can add some rules in OSSIM from a more comprehensive perspective or evidence from sequences events.

2. **Additionally, please use the network diagram in Figure 5 as a reference and create your own view of how to secure the network using the devices that we have worked with in this project.**

This is the network Architecture based on what we do in project 2. I integrated with firewall, IDS and SIEM in one graphs here. This network architecture is heavily focusing on Enterprise Networks here.



For firewall, I design it as a first level security guard to filter and drop suspicious network traffic. It may not be that restrict, just the very first level to tunnel. Then I would like to introduce a new network device **Proxy Server** here. Instead of receiving the network traffic directly on host, I would like to have a proxy server between host and network to analyze the result of traffic before we receiving that. We can also deploy IDS/IPS on the proxy server. It can analyze the traffic in advance and prevent some malicious actions executed on the host directly. If the traffic is under regulation, then the proxy server will forward it to host.

Before host and some other servers, I apply a new network device **Access Control** on each server as **an IAM (Identify and Access Management)** here. It can help us to filter the traffics which violates the access privilege to our hosts. Some of their actions may not be vulnerable to our hosts, but it should not be happened because they don't have the access to it.

On the host site, I would like to have a **host-based IDS** to check again and monitoring the traffic from host perspective. It is more detailed than network-based IDS. In addition, I will deploy **anti-virus** software to daily scanning or alert before executing hosts on malicious code. It can make host side more secure.

For the extra score, the new devices I introduce here: Proxy Server, Access Control(IAM), Host-based IDS, Anti-Virus.