Syslog Servers

Bridgette Chapman

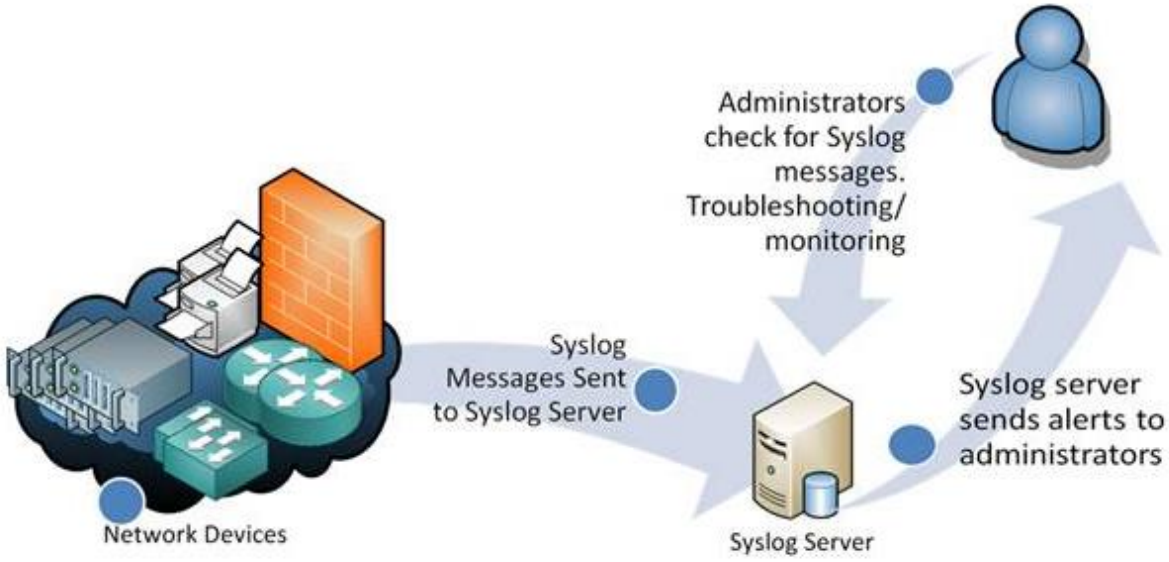
ODU

Reflection Number 5

Syslog Servers

Day 21, the attention was paid to the syslog servers involved in the CSN project. This entailed securing and deploying servers for consolidating log data over the physical layer of the organization's network. Implementation of this central logging mechanism will be beneficial for live analysis, diagnosing some issues, and corporate security policies' adherence. It is something that involved a lot of work and precise approach in order to make sure that all the logs were grouped properly and could be accessed for the analysis.

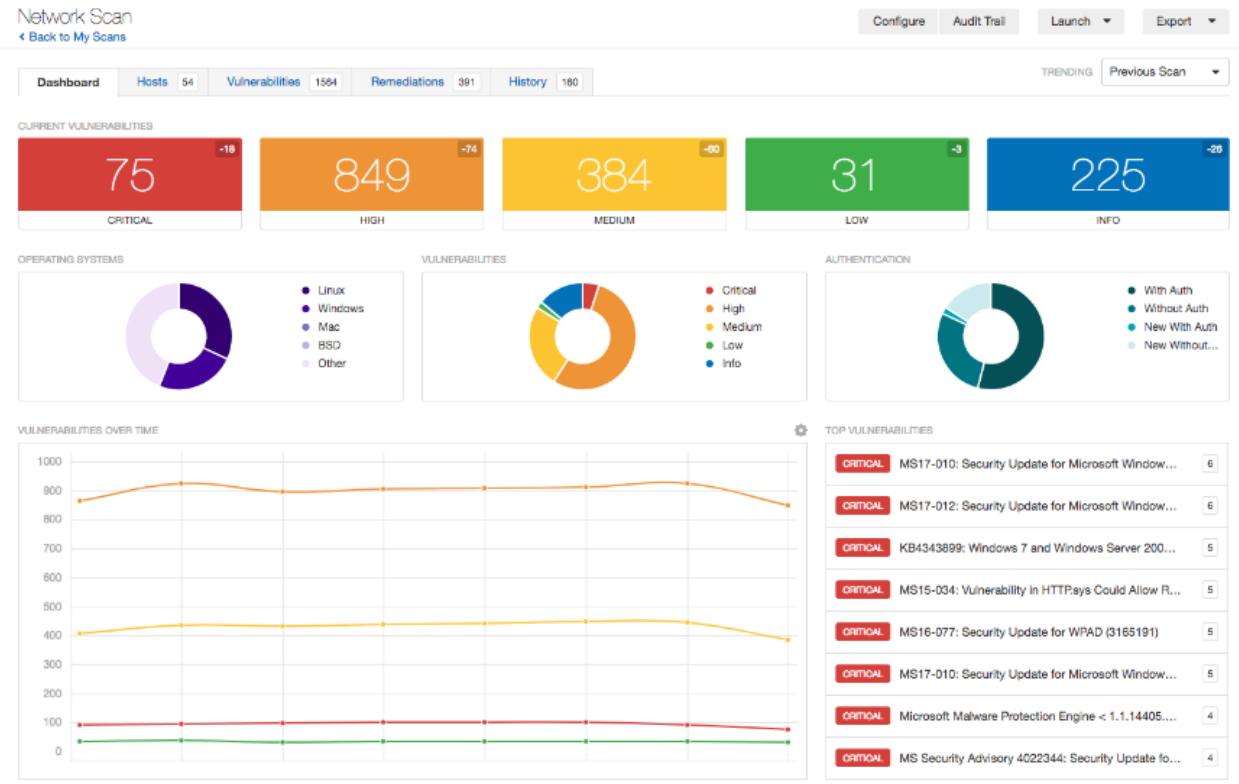
Figure 1: syslog server setup configuration



The next day concerned setting of the OTMP in this case entailing the following activities: scanning of the systems where 13 were identified. These scans were very useful in the process of search for host, backup and in general to find potential weak spot or outdated settings in the system. Day 23 was spent cleansing the system after the scans had been made. On updating the system, I concentrated on fixing the operating system, updating the applications,

and improving the security by installing Symantec for end-of-level protection. The next day was a holiday which enabled me to relax and think about the week's activities.

Figure 2: Nessus vulnerability scan results dashboard



After not repeating the OTMP activities for a while, on Day 25, I configured WSUS and Hyper-V environments. To be more precise, I focused on Windows servers which had to be updated; all of them had to have the latest patches and security updates. Once I was done with the updates I used commands to both report and scan for update compliance on all systems proving their status compliant.

Reflection

All of those activities helped me to gain the insights in the field of system administration, protecting the network from the unauthorized access or cyber threats, and the necessity of the systematic approach to the networks maintaining.

Reference.

Zhang, S., Liu, Y., Meng, W., Bu, J., Yang, S., Sun, Y., ... & Zhang, M. (2020). Efficient and robust syslog parsing for network devices in datacenter networks. *IEEE access*, *8*, 30245-30261.