CS 4400 System Administration

Project 7: Create Centralized Logging

Description:

A system administrator has so many logs to check that they might feel like a lumberjack! You can spend your whole day logging into each server and workstation checking each log, or you can forward all the logs to a centralized area. (Hint: you'll want to do the second thing.)

To assist with this process, you should investigate centralized logging software using your Linux server with the free syslog-ng and the free Solarwinds Event Log Forwarder for Windows.

- Syslog-ng: https://www.syslog-ng.com/products/open-source-log-management/
- SolarWinds Event Log Forwarder for Windows: https://www.solarwinds.com/free-tools/event-log-forwarder-for-windows

First, set up syslog-ng on your Linux server and forward Linux-based logs to it. Next, set up the event forwarder for all your Windows computers (servers plus workstations) and forward as many logs as possible to it. Finally, attempt to forward your firewall logs. Once you have done this, please create in a Google doc in your folder:

- A description of what you had to do to set up the logging server
- A list of logs from all servers, workstations, and firewalls you are forwarding to the server
- If you cannot forward some logs to the server, you've just created more work for yourself. Write a rationale for why some logs couldn't/shouldn't be forwarded to the server. Be prepared for me to ask about some missing logs.
- Many pretty pictures of the logs in the centralized location. (The text kind, not the forest kind.)
- Any other resources that helped.

Resources:

- What Linux logs are important?
  - https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/
  - https://stackify.com/linux-logs/
- What Windows logs are important?
  - https://www.loggly.com/ultimate-guide/windows-logging-basics/
- Good rationale for why we need logs.
  - https://geekflare.com/open-source-centralized-logging/
- Official documentation for setting up the free version of syslog-ng: https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.22/administration-guide/12