Research -  **Ariel, Taj**

a.Conduct research to understand the

significance of network security monitoring and analysis using Syslog.

b.

Explore the key components of

Syslog, including Syslog servers, Syslog messages, and Syslog levels.

c.

Familiarize yourself with the steps

and best practices for implementing Syslog for network security purposes.

Assignment Tasks: **Daniel, Rayon**

a.

Explain the importance of network

security monitoring and analysis using Syslog.

b.

Describe the components of the

Syslog system, including Syslog servers, Syslog messages, and Syslog levels.

c.

Discuss the benefits of implementing

Syslog for network security, such as detecting security incidents, identifying

unauthorized access attempts, and monitoring system health.

d.

Outline the steps involved in

configuring and using Syslog for network security monitoring and analysis.

Practical Configuration: **Sanada**

a.

Using a network simulation tool or a

real network environment, set up a Syslog server and at least one network

device (e.g., router or switch).

b.

Configure the network device to send

Syslog messages to the Syslog server based on your research and the steps

outlined in your assignment.

c.

Validate the configuration by

monitoring and analyzing the Syslog messages received by the Syslog server.

Documentation: **Brandon Danvers**

a.

Document your research findings from

step 1.

b.

Prepare a detailed report that

includes the explanations, steps, and examples outlined in the assignment

tasks.

c.

Include screenshots or

configurations from your practical configuration in step 3.