Collegiate Cyber Defense Competitions

Inject Name	Setup Centralized Logging
Inject ID	TOOL25T

Description	In order to efficiently use the syslog and event log data produced by the servers, we need all the events logged to a central repository. 1. Select a server to host the centralized log. 2. Modify the firewall rules to allow log data to flow between segments. 3. Configure Linux servers to forward their log records to the central repository. 4. Configure Windows servers to forward events to the central repository. 5. Use *eventcreate* on Windows and *logger* on Linux to create a series of test records from each server to verify functionality.
Deliverables	Respond with a business memo that identifies the host which provides the central repository. Identify any software application that you are using. Describe the firewall security policy changes with a screenshot of the changes. Provide a screenshot of configuring forwarding on an example Linux server and Windows server. Provide a screen shot of the test-message records from each server in the central repository.