Ulysses Palomar, Mike Stoj, Caleb Fager

Objective:

The goal of this portion of the project is to set up a firewall for our machines and conduct penetration testing to ensure the security of our network, set up network file system and load balancing on the network, and finally a performance monitoring tool suite to assist admins in monitoring, managing, adjusting and tweaking the individual performance metrics on the system to ensure peak efficiency.

Tasks:

Firewall:

1. Research and Select a Firewall Solution:
   1. Research various firewall solutions to determine which one best fits our needs.
   2. Select the firewall solution that best meets our requirements.
   3. Install and configure the firewall on all machines in our network.
2. Develop Firewall Rules:
   1. Develop a set of firewall rules that provide a baseline level of security for our network.
   2. Customize the firewall rules to meet the specific needs of our network.
   3. Test the firewall rules to ensure that they are effective
3. Conduct Pentesting:
   1. Determine the scope of the pentesting, including the types of attacks that will be simulated and the machines that will be targeted.
   2. Use a variety of pentesting tools and techniques to simulate attacks and attempt to gain unauthorized access to our network.
   3. Identify and document any vulnerabilities or weaknesses in our network.
   4. Make recommendations for improving the security of our network based on the results of the pentesting.
4. Implement Recommendations:
   1. Use the results of the pentesting to develop a plan for improving the security of our network.
   2. Implement the recommendations from the pentesting plan.
   3. Test the changes to ensure that they have improved the security of our network.

NFS and Load Balancing::

1. Research and Select NFS and load balancing:
   1. Research the different NFS server software options available and choose the one that best fits your requirements.
   2. Research the different load balancing algorithms and choose the one that is appropriate for your resources.
   3. Research the different load balancer software and hardware options and choose the one that best fits your requirements.
   4. Research security best practices for NFS file systems and load balancers and ensure that you follow them.
2. Tasks:
   1. Set up the NFS server: Install the NFS server software on the server and configure the file system that you want to export.. Start the NFS server service on the server.
   2. Set up the NFS client: Install the NFS client software on the client and mount the NFS file system.
   3. Set up the load balancer: Choose a load balancer software or hardware appliance that can be implemented. Configure the load balancer by specifying the resources to be load balanced, the algorithm to use, and any health checks or other settings that are required.
   4. Test the NFS and load balancing setup: Verify that the NFS file system is accessible from the client and that the load balancer is distributing traffic to the resources as expected.
   5. Monitor and maintain the NFS and load balancing setup: Monitor the performance of the NFS file system and load balancer to ensure that they are functioning properly and meeting your requirements.
3. Documentation:
   1. Develop a plan for setting up the NFS file system and load balancer, including a timeline, a list of required resources, and a list of tasks to be performed.
   2. Develop documentation for the NFS file system and load balancer, including configuration details, security settings, and maintenance procedures.
   3. Create a disaster recovery plan for the NFS file system and load balancer, including backup and restore procedures and failover procedures in case of a hardware or software failure.
   4. Develop a plan for scaling the NFS file system and load balancer as needed to handle increased load or additional resources.

Performance Monitoring:

1. Research required dependencies and perform installation:
   1. Before installing Zabbix, ensure that the necessary dependencies are installed. This includes Apache web server, PHP, and MySQL.
   2. Download the latest version of Zabbix from the official website and install it on the server. Follow the installation guide provided by Zabbix to complete the installation process.
   3. Create a new MySQL database and user for Zabbix. Then configure Zabbix to use this database by providing the database details in the configuration file.
   4. Once the installation is complete, set up the web interface for Zabbix by configuring Apache to serve the Zabbix web files.
2. Maintenance and daily use
   1. Database backup: Regularly backup the Zabbix database to prevent data loss in case of a disaster.
   2. Monitor server performance: Monitor the performance of the server running Zabbix to ensure that it is running optimally.
   3. Software updates: Regularly update Zabbix to the latest version to benefit from bug fixes and new features.
   4. Clean up old data: Remove old data from the Zabbix database to free up space and improve performance.
3. Document, collect data, and adapt settings
   1. Determine the scope of the documentation project and identify the specific systems and components that need to be documented.
   2. Collect all relevant information about the systems and components that need to be documented.
   3. Once all relevant data has been collected, create detailed documentation for each system and component.
   4. Review the settings of the systems and components being documented and determine if any changes need to be made to improve performance, security, or efficiency.
   5. Review the documentation regularly to ensure that it remains accurate and up-to-date. Update the documentation as needed to reflect any changes to the systems or components being documented.

Roles:

The individual responsible for this portion of the project will be in charge of:

Firewall:

* Researching and selecting a firewall solution.
* Developing firewall rules.
* Conducting pentesting.
* Implementing recommendations.
* Documenting all findings and recommendations.

NFS and Load Balancing:

* Research and select tools.
* Setup the tools needed.
* Monitor and maintain.
* Write a performance report.
* Troubleshooting and diagnostic information.

Performance Monitoring:

* Installing, configuring, and maintaining Zabbix.
* Setting up Zabbix agents on network devices and configuring network monitoring.
* Configuring security monitoring and alerts in Zabbix.
* Monitoring and troubleshooting issues reported by users.

Deliverables:

The deliverables for this portion of the project will include:

Firewall:

* A report outlining the selected firewall solution, the firewall rules, and the results of the pentesting.
* A list of recommendations for improving the security of our network, along with an implementation plan.
* Documentation of all findings and recommendations.

NFS and Load Balancing::

* Configuration documentation: This should include the configuration settings for the NFS server, NFS client, and load balancer.
* Testing documentation: This should include the results of the testing that was performed on the NFS file system and load balancer.
* Maintenance documentation: This should include the procedures for ongoing maintenance, such as software updates and security patches, as well as any monitoring and management procedures.
* Disaster recovery plan: This should include the procedures for backing up the NFS file system and load balancer
* Training documentation: This should include any training materials that are required to help users understand how to access the NFS file system and how to use the load balancer.
* Final report: This should summarize the project, including the goals, scope, and objectives, as well as any issues or challenges that were encountered during the project.

Performance Monitoring:

* A detailed guide on how to install Zabbix.
* Initial guide on how to maintain and optimize Zabbix.
* Document a user manual on how to use Zabbix monitoring system.
* Report outlining the network and server performance metrics collected by Zabbix.
* A security report detailing the security monitoring metrics collected by Zabbix.
* Troubleshooting and diagnostic information report: A report outlining the steps taken to troubleshoot and diagnose issues with Zabbix.