Our project centers around hardening Linux based web servers or other Linux hosts exposed to the internet.

There are many best practices when it comes to hardening a web server. For example:

1. Keeping your operating system patched and otherwise up-to-date

2. Disabling remote access via root

3. Restricting remote access to certain IP addresses

4. Forcing key-based authentication via SSH

5. Disabling all services except those absolutely necessary for the server to perform its function.

6. Enabling SELINUX

7. Enable a packet filter such as Firewalld and configure it with a default-deny stance.

Despite these and other defensive steps, a web server is inherently exposed as you must allow inbound connections from TCP ports 80 and 443 from all hosts on the internet.

See our wiki page: http://csci-6651.noyage.com for more details.

Also Github : https://github.com/akona1/CSCI6651\_Final\_Project