

Final Group Project Task Breakdown

General Project Management (Juliana Garza)

1. Develop GitHub repository:

- [] Create main folders: /docs, /scans, /presentation, /images.
- [] Create hierarchy within main folders

2. Initialize README.md:

- [] Write an intro paragraph explaining the project goals and scope.
- [] List each team member's role and responsibilities.
- [] Include links to each major section (docs, scans, final report).

3. Set up GitHub Project Kanban Board:

- [] Add columns: "To Do," "In Progress," "Done."
 - [] Create cards for each task (as listed below) and assign to appropriate members.
-

Initial Endpoint Setup (Juliana Garza)

1. Install and configure the OS on the VM:

- [] Download and install chosen OS (e.g., Windows/Linux) on a virtual machine.
- [] Configure basic settings (hostname, user account, password policies).
- [] Screenshot each step and save to /docs/initial-setup/screenshots/.

2. Document initial OS setup steps:

- [] Write step-by-step instructions in docs/initial-setup/os-setup.md.
- [] Detail any system settings changes (e.g., disabling guest accounts, enabling firewalls).

3. Install and list standard applications:

- **[]** Install standard tools (e.g., browsers, productivity software).
- **[]** List each tool, version, and purpose in docs/initial-setup/software-list.md.
- **[]** Include commands for installation if on Linux or detailed steps for Windows.

4. **Document initial configurations:**

- **[]** List initial configuration settings
- **[]** Save details to docs/initial-setup/configuration.md for reference.

5. **Research and select vulnerability scanning tools:**

- **[]** Compare popular tools (e.g., Nessus, OpenVAS) and record findings in docs/research-tools.md.
- **[]** Justify chosen tool(s) based on features and applicability.

Initial Vulnerability Assessment (Sunwook Kang)

1. Introduce Known Vulnerabilities on the VM:

- **Outdated Software:**
 - **[]** Install an outdated version of critical software such as Apache.
 - **[]** Document the version and installation process in /docs/initial-setup/vulnerabilities.md.
- **Weak Passwords:**
 - **[]** Create a new user with a weak password (password123).
 - **[]** Document user details and password strength.
- **Disabled Firewall:**
 - **[]** Disable the firewall with `sudo ufw disable`.
 - **[]** Document the command used and save output.
- **Insecure Permissions:**
 - **[]** Modify permissions on sensitive files (e.g., /etc/passwd).
 - **[]** Document commands and files affected.

- **Install Vulnerable FTP Server (vsftpd):**

- ☐ Install vsftpd with anonymous access and write permissions.
- ☐ Configure settings in /etc/vsftpd.conf and save the final configuration in /docs/initial-setup/vulnerabilities.md.

2. Run vulnerability scans:

- ☐ Install and configure the selected scanning tool on the VM.
- ☐ Perform a full scan, saving results as .txt or .pdf in /scans/baseline-scan/.
- ☐ Take screenshots of key findings and save in /docs/initial-scan/screenshots/.

3. Document vulnerabilities found:

- ☐ Summarize high, medium, and low-severity vulnerabilities in docs/initial-scan/scan-summary.md.
- ☐ Include CVE numbers and brief descriptions of each vulnerability.

4. Create a visual summary of high-severity issues:

- ☐ Take close-up screenshots of the top 3-5 critical vulnerabilities.
- ☐ Label each screenshot and save to /docs/initial-scan/screenshots/.

5. Review and prioritize vulnerabilities:

- ☐ Study initial scan results and identify vulnerabilities to address.
- ☐ Record top priorities in docs/hardening-priorities.md with justification.

System Hardening and Security Policy Implementation (Joshua Orozco)

1. Implement OS hardening techniques:

- ☐ Disable unnecessary services and take screenshots at each step.
- ☐ Document steps (e.g., registry changes, disabling guest accounts) in docs/hardening/os-hardening.md.

2. Apply network security configurations:

- ☐ Set up firewall rules to block unneeded ports and services.

- ☐ Save all firewall configuration details to docs/hardening/network-config.md.
- 3. Screenshot each major hardening action:**
- ☐ Take screenshots showing firewall rules, user account permissions, and other major changes.
 - ☐ Save to docs/hardening/screenshots/.
- 4. Implement security settings for applications:**
- ☐ Adjust application-specific settings (e.g., secure browser settings).
 - ☐ List settings changed in docs/hardening/applications.md.
- 5. Configure encryption for data at rest and in transit:**
- ☐ Enable disk encryption or secure storage methods.
 - ☐ Document these settings in docs/hardening/encryption.md (include screenshots).
- 6. Export updated VM:**
- ☐ Export the VM to share with teammates, or document steps for replicating changes.
-

Post-Hardening Vulnerability Assessment (Joseph Montez)

- 1. Test encryption and application security settings:**
- ☐ Conduct basic tests to confirm settings work as expected.
 - ☐ Record any issues and successful configurations in docs/hardening/test-results.md.
- 2. Capture screenshots of critical configurations:**
- ☐ Screenshot any encryption settings or application security settings and save to /docs/hardening/screenshots/.
- 3. Re-run vulnerability scans:**
- ☐ Conduct a full scan using the same tool(s) as in the initial scan.
 - ☐ Save results to /scans/post-hardening/.

4. Analyze differences in vulnerability counts:

- **[]** Compare baseline and post-hardening scan results.
- **[]** Summarize changes in docs/post-hardening-analysis.md.

5. Document remaining vulnerabilities:

- **[]** List unresolved vulnerabilities with explanations for each in docs/post-hardening/remaining-vulnerabilities.md.

6. Capture screenshots of post-hardening scan results:

- **[]** Take screenshots of the final scan results and save to /docs/post-hardening/screenshots/.

Final PowerPoint Creation

Initial PowerPoint Layout and Sharing (Juliana Garza)

1. [] Outline Presentation Structure:

- **[]** Define the main sections: Introduction, Methodology, Findings, Conclusion, and Recommendations.
- **[]** List key slides needed for each section, including title slide and reference slide.
- **[]** Create placeholders for each slide with basic headings to guide content creation.

2. [] Create PowerPoint Template:

- **[]** Choose a cohesive color scheme and font style.
- **[]** Set up consistent formatting (e.g., headers, footers, page numbers).
- **[]** Apply layout to all placeholder slides.

3. [] Save and Share Initial Layout:

- **[]** Save the initial PowerPoint layout as initial-presentation-layout.pptx.

Slide Content Creation (Juliana Garza, Sunwook Kang, Joseph Orozco, Joseph Montez)

Content Creation (Juliana Garza- Project Introduction & Initial Setup)

1. **[] Complete slides for project goals and objectives.**
2. **[] Complete slides covering the initial setup steps:**
 - **[]** Include screenshots or visuals, if available.
 - **[]** Briefly describe the baseline configuration and any challenges faced.
3. **[] Add bullet points, images, and speaker notes for clarity.**

Content Creation (Sunwook Kang- Initial Scanning)

1. **[] Complete slides covering the initial scanning steps:**
 - a. **[]** Include screenshots or visuals, if available.
 - b. **[]** Briefly describe the baseline configuration and any challenges faced.

Content Creation (Joshua Orozco - Hardening Process)

1. **[] Create slides detailing the hardening process:**
 - **[]** Describe changes made to improve security (e.g., firewall rules, OS hardening).
2. **[] Create slides for security settings and encryption**
3. **[] Add bullet points, images, and speaker notes.**

Content Creation (Joseph Montez – Post-Hardening, Conclusion & Recommendations)

1. **[] Complete slides for the post-hardening vulnerability assessments:**
 - **[]** Summarize key vulnerabilities identified.
 - **[]** Use visuals like charts or screenshots of scan results.
1. **[] Complete slides for findings and comparison of pre- and post-hardening scans.**
 - **[]** Summarize the impact of hardening efforts on vulnerabilities.
2. **[] Create conclusion and recommendations slides:**
 - **[]** Offer key takeaways and suggest any future improvements.
3. **[] Add bullet points, images, and speaker notes.**