**Project Planning Phase**

Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age

Team Members:

1. Dhanraj Pawar
2. Kaushal Chougule
3. Athrav Pawar
4. Balaji Patil

**Project Planning Phase Overview**  
The Project Planning Phase is crucial for outlining the tasks, schedules, and necessary resources for executing the project efficiently. This phase ensures a structured approach, keeping all team members informed about their roles and responsibilities.

**Objectives of this Phase:**

* Decompose the project into achievable tasks.
* Allocate tasks to respective team members.
* Approximate the effort required for each task.
* Develop a timeline for project completion.

**Sprint Plan**

The project will be carried out in three sprints, each spanning 7 days. The breakdown is as follows:

**Sprint 1: Vulnerability Assessment**

* **Duration:** 7 days (17 Feb 2025 - 24 Feb 2025)
* **Tasks:**
  1. **Task 1:** Set up and configure Nessus for vulnerability scanning. *(Assigned to: Dhanraj Pawar)*
  2. **Task 2:** Conduct a vulnerability scan on the target system. *(Assigned to: Dhanraj Pawar)*
  3. **Task 3:** Assess the scan results and rank vulnerabilities. *(Assigned to: Kaushal Chougule)*
  4. **Task 4:** Compile a scan report and distribute it to stakeholders. *(Assigned to: Balaji Patil)*

**Sprint 2: Threat Hunting**

* **Duration:** 7 days (25 Feb 2025 - 4 March 2025)
* **Tasks:**
  1. **Task 1:** Install and configure Splunk for SIEM and log analysis. *(Assigned to: Kaushal Chougule)*
  2. **Task 2:** Track SIEM logs for unusual activities. *(Assigned to: Kaushal Chougule)*
  3. **Task 3:** Examine potential threats and escalate if needed. *(Assigned to: Athrav Pawar)*
  4. **Task 4:** Record observations in an incident report. *(Assigned to: Balaji Patil)*

**Sprint 3: Incident Response**

* **Duration:** 7 days (5 March 2025 - 11 March 2025)
* **Tasks:**
  1. **Task 1:** Inspect phishing emails for signs of compromise (IOCs). *(Assigned to: Athrav Pawar)*
  2. **Task 2:** Generate an incident report with remediation measures. *(Assigned to: Dhanraj Pawar)*
  3. **Task 3:** Distribute the report to the incident response team. *(Assigned to: Kaushal Chougule)*
  4. **Task 4:** Conduct a post-incident evaluation and document key learnings. *(Assigned to: Balaji Patil)*

**Task Breakdown**

**Sprint 1: Vulnerability Assessment**

1. **Task 1:** Set up Nessus.
   * Install Nessus on a virtual environment.
   * Configure Nessus to scan designated systems.
2. **Task 2:** Execute a vulnerability scan.
   * Initiate a full vulnerability scan on the designated system.
   * Monitor the scan to ensure its successful execution.
3. **Task 3:** Evaluate scan outcomes.
   * Examine the Nessus-generated report.
   * Prioritize vulnerabilities based on their severity (e.g., critical, high, medium, low).
4. **Task 4:** Prepare a scan report.
   * Develop a comprehensive report with a summary, vulnerability details, and recommendations.

**Sprint 2: Threat Hunting**

1. **Task 1:** Install and configure Splunk.
   * Set up Splunk for log monitoring.
   * Connect Splunk with target systems for log collection.
2. **Task 2:** Analyze SIEM logs.
   * Identify unusual login attempts, failed authentication, or unauthorized access.
   * Detect patterns signaling potential threats.
3. **Task 3:** Investigate threats.
   * Review any detected anomalies.
   * Escalate threats to the incident response team when necessary.
4. **Task 4:** Document findings.
   * Create a report detailing suspicious activities, key observations, and recommendations.

**Sprint 3: Incident Response**

1. **Task 1:** Examine phishing emails.
   * Retrieve phishing emails from spam folders or a simulated attack.
   * Assess email headers and content for indicators of phishing.
2. **Task 2:** Compile an incident report.
   * Document the phishing attack details, including IOCs and recommended mitigation steps.
3. **Task 3:** Share the report.
   * Distribute the report to the incident response team and relevant stakeholders.
4. **Task 4:** Conduct a post-incident review.
   * Evaluate the incident response process and identify potential improvements.

# Resource Allocation

Below is the resource allocation for the project:

|  |  |  |
| --- | --- | --- |
| Team Member | Tasks | Sprint |
| Dhanraj Pawar | Install and configure Nessus, perform vulnerability scans, generate reports. | Sprint 1, Sprint 3 |
| Kaushal Chougule | Set up Splunk, monitor SIEM logs, analyze scan results. | Sprint 1, Sprint 2 |
| Athrav  Pawar | Investigate threats, analyze phishing emails, document findings. | Sprint 2,  Sprint 3 |

## Timeline

Below is the timeline for the project:

|  |  |  |  |
| --- | --- | --- | --- |
| Sprint | Start Date | End Date | Tasks |
| Sprint 1 | 17 Feb  2025 | 24 Feb  2025 | Vulnerability assessment (Nessus setup, scanning, analysis, reporting). |
| Sprint 2 | 25 Feb  2025 | 4 March  2025 | Threat hunting (Splunk setup, log monitoring, investigation, reporting). |
| Sprint 3 | 5 March  2025 | 11 March  2025 | Incident response (phishing analysis, incident reporting, review). |

## Deliverables

1. Sprint Plan:
   1. A detailed plan for each sprint, including tasks, timelines, and assigned team members.
2. Task Breakdown:
   1. A breakdown of the tasks for each sprint.
3. Resource Allocation:
   1. A table showing the tasks assigned to each team member.
4. Timeline:
   1. A timeline for the project, showing the start and end dates for each sprint.

## Next Steps

1. Project Execution:
   1. Begin implementing the project based on the sprint plan.
2. Monitoring and Tracking:
   1. Monitor progress and track completed tasks using a project management tool (e.g., Jira, Trello).