Project Execution Phase

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

Team Members:

1. Dhanraj Pawar
2. Kaushal chougule
3. Balaji Patil
4. Atharv Pawar

Project Execution Phase Overview

The Project Execution Phase is where the project is actively implemented. This involves executing planned tasks, monitoring progress, and ensuring the project remains on schedule.

Objectives:

- Implement the system as per the project design and plan.
- Track progress and address any arising issues.
- Ensure timely completion of project deliverables.

Execution Plan

The project will be executed in three sprints, each lasting seven days. Below is the detailed execution plan:

Sprint 1: Vulnerability Assessment

- **Duration:** 7 days (17 Feb 2025 - 24 Feb 2025)
- **Tasks:**
  - **Task 1:** Install and configure Nessus for vulnerability scanning. *(Assigned to: Aditya Dange)*
  - **Task 2:** Conduct a vulnerability scan on the target system. *(Assigned to: Aditya Dange)*
  - **Task 3:** Analyze scan results and prioritize vulnerabilities. *(Assigned to: Kshitij Patil)*
  - **Task 4:** Generate and share the scan report with stakeholders. *(Assigned to: Athrav Katkar)*
- **Deliverables:**
  - Nessus installed and configured.
  - Vulnerability scan completed.
  - Scan report generated and shared.

Sprint 2: Threat Hunting

- **Duration:** 7 days (25 Feb 2025 - 4 March 2025)
- **Tasks:**
  - **Task 1:** Set up Splunk for SIEM and log monitoring. *(Assigned to: Kshitij Patil)*
  - **Task 2:** Monitor SIEM logs for suspicious activity. *(Assigned to: Kshitij Patil)*
  - **Task 3:** Investigate potential threats and escalate if necessary. *(Assigned to: Athrav Katkar)*
  - **Task 4:** Document findings in an incident report. *(Assigned to: Aditya Dange)*
- **Deliverables:**
  - Splunk installed and configured.
  - SIEM logs monitored and analyzed.
  - Incident report generated.

Sprint 3: Incident Response

- **Duration:** 7 days (5 March 2025 - 11 March 2025)
- **Tasks:**
  - **Task 1:** Analyze phishing emails for indicators of compromise (IOCs). *(Assigned to: Athrav Katkar)*
  - **Task 2:** Create an incident report with remediation suggestions. *(Assigned to: Aditya Dange)*
  - **Task 3:** Share the report with the incident response team. *(Assigned to: Kshitij Patil)*
  - **Task 4:** Conduct a post-incident review and document lessons learned. *(Assigned to: Athrav Katkar)*
- **Deliverables:**
  - Phishing emails analyzed.
  - Incident report generated and shared.
  - Post-incident review completed.

Task Execution Details

Sprint 1: Vulnerability Assessment

1. **Install and configure Nessus:**
   - Set up Nessus on a virtual machine.
   - Configure Nessus to scan the target system.
2. **Perform vulnerability scan:**
   - Run a full vulnerability scan.
   - Monitor the scan progress and ensure successful completion.
3. **Analyze scan results:**
   - Review and prioritize vulnerabilities based on severity (e.g., critical, high, medium, low).
4. **Generate scan report:**
   - Prepare a detailed report including an executive summary, vulnerability details, and recommendations.

Sprint 2: Threat Hunting

1. **Set up Splunk:**
   - Install and configure Splunk for log monitoring.
   - Integrate Splunk with the target system.
2. **Monitor SIEM logs:**
   - Analyze logs for unusual login attempts, failed logins, or unauthorized access.
   - Identify patterns indicating potential threats.

3. **Investigate potential threats:**
    - Investigate suspicious activities identified in logs.
    - Escalate issues to the incident response team if needed.
4. **Document findings:**
    - Compile an incident report detailing suspicious activities and recommendations.

Sprint 3: Incident Response

1. **Analyze phishing emails:**
    - Collect phishing emails from spam folders or a simulated campaign.
    - Examine email headers and content for phishing indicators.
2. **Create an incident report:**
    - Document details of the phishing attack, including IOCs and suggested remediation steps.
3. **Share the report:**
    - Distribute the incident report to the incident response team and stakeholders.
4. **Conduct a post-incident review:**
    - Evaluate the incident response process to identify improvement areas.
    - Document lessons learned.

Monitoring and Tracking

To ensure the project remains on track, the following monitoring and tracking tools will be utilized:

1. **Jira:** For task management and progress tracking.
2. **Daily Stand-ups:** Short daily meetings to discuss progress, address issues, and plan tasks.
3. **Burndown Charts:** To visualize sprint progress and workload.

Deliverables

1. **Nessus Setup and Scan Report:**
    - Nessus installed and configured.
    - Vulnerability scan completed, and report generated.
2. **Splunk Setup and Incident Report:**
    - Splunk installed and configured.
    - SIEM logs monitored and incident report generated.
3. **Phishing Analysis and Incident Report:**
    - Phishing emails analyzed, and incident report generated.
    - Post-incident review completed.

Next Steps

1. **Functional and Performance Testing:**
    - Validate system functionality and performance.
2. **Documentation and Demo:**
    - Prepare documentation and a final demo for project presentation.
