

Sprint Planning Meeting Minutes:

Attendees: Jonathan Nava-Arenas, Reynaldo Rodriguez, Luisa Faria Novy E Silva, Anthony Whiteman, Rickoy Cunningham

Start time: 7:00PM

End time: 8:00PM

After discussion, the velocity of the team was estimated to be one story per member per sprint.

The product owner chose the following user stories to be done during the next sprint. They are ordered based on their priority.

1. Lab & Scan Setup
 - As a cybersecurity analyst, I want to set up a virtual lab with multiple VMs and run a vulnerability scan using Nessus so that I can identify potential risks in a controlled environment. This includes configuring the VMs to simulate real-world systems and creating another VM running DVWA, which will be used as the target for scanning and vulnerability testing.
2. Data Analysis
 - As a cybersecurity analyst, I want to systematically organize, categorize, and filter the vulnerability scan results to prioritize the most critical threats. This will allow me to focus on addressing the high-risk vulnerabilities that could have the most severe impact on the organization's systems, data, and operations.
3. Incident Response
 - As an Incident Response Analyst, I want to create and maintain incident response playbooks so that we have clear, repeatable procedures to detect, contain, and remediate security incidents effectively.
4. Automation Tool
 - As a cybersecurity analyst, I want to automate the process of mapping vulnerabilities to risk scores so that prioritization is consistent and less prone to human error.
5. Report & Presentation
 - As a cybersecurity analyst, I want to compile the results, risk matrix, and remediation plan into a professional report and presentation so that stakeholders clearly understand the findings.

The team members indicated their willingness to work on the following user stories.

- Reynaldo Rodriguez
 - #1 (Lab & Scan Setup)
 - As a cybersecurity analyst, I want to set up a virtual lab with multiple VMs and run a vulnerability scan using Nessus so that I can identify potential risks in a controlled environment. This includes configuring the VMs to simulate real-world systems and creating another VM running DVWA, which will be used as the target for scanning and vulnerability testing.
- Luisa Faria Novy E Silva
 - #2 (Data Analysis)
 - As a cybersecurity analyst, I want to systematically organize, categorize, and filter the vulnerability scan results to prioritize the most critical threats. This will allow me to focus on addressing the high-risk vulnerabilities that could have the most severe impact on the organization's systems, data, and operations.
- Anthony Whiteman
 - #3 (Risk and Mitigation Analyst)
 - As an Incident Response Analyst, I want to create and maintain incident response playbooks so that we have clear, repeatable procedures to detect, contain, and remediate security incidents effectively.
- Jonathan Nava-Arenas
 - #4 (Automation Tool)
 - As a cybersecurity analyst, I want to automate the process of mapping vulnerabilities to risk scores so that prioritization is consistent and less prone to human error.
- Rickoy Cunningham
 - #5 (Report & Presentation)
 - As a cybersecurity analyst, I want to compile the results, risk matrix, and remediation plan into a professional report and presentation so that stakeholders clearly understand the findings.

