**PROJECT SPECIFICATION**

**Navigating a Cyber Security Incident**

**Understanding Threats**

| CRITERIA | MEETS SPECIFICATIONS |
| --- | --- |
| Create the basic component of a threat assessment in order to prioritize assets and actions. | The project includes the basic component of a threat assessment in order to navigate the incident by:   * Correctly summarizing the threat scenario of what occurred in Hospital X and other hospitals. * Discussing correct assets * Focusing on impact of resources |
| Identify the relevant cyber security threat. | The project includes identification of threat actors, motivations, and capabilities by:   * Discussing both internal and external threat actors * Identifying the correct threat actor motivations * Listing out the correct tactics discussed [here](https://attack.mitre.org/groups/G0085/) |

**Conducting Vulnerability Scanning and Penetration Testing**

| CRITERIA | MEETS SPECIFICATIONS |
| --- | --- |
| Successfully conduct vulnerability scan. | The project includes a successful vulnerability scan by attaching a screenshot that illustrates:   * The scan configuration and the plug-in window * The correct results produced * The screenshot of results should be included in the final report. |
| Successfully attempted password cracking. | * Successfully cracked at least 1 weak password, and makes adequate recommendations for addressing this risk. * The screenshot of the password cracking results was added to the final report. |
| Prioritize remediation plan to address vulnerabilities. | * Correctly prioritized vulnerability scan findings based on the risk level. * Any critical findings should be illustrated as a top priority, unless justification is provided that explains otherwise. |

**Incident Response**

| CRITERIA | MEETS SPECIFICATIONS |
| --- | --- |
| List recommended actions for incident response. | * Complete the actions of the IR checklist based on the project information provided. * Illustrates the realistic severity of the scenario and makes valid recommendations for navigating the incident. * Includes thoughtful recommendations to improve the incident response process and also prevents a similar incident from happening again in the future. |

**Suggestions to Make Your Project Stand Out!**

* Brainstorm beyond obvious threat motivations and attack methods to create a more robust list of theories.
* Crack more than 10 passwords.