Atividade ponderada em grupo

1 - Realizar uma análise do seu projeto para identificar as vulnerabilidades (pontos fracos) e possíveis ataques (pelo menos dois ataques diferentes). (2 pontos)

Vulnerabilidades:

- Credenciais do wifi e do servidor mqtt expostos no código
- Necessidade de energia constante (pilha)

Possíveis ataques:

- Denial of Service Attack - Um milhão de requisições ao servidor ao mesmo tempo que o torna inoperável.
- Brute force - não temos limitação no número de tentativas de login.
- Ataque bruto ao hardware - alguém arrancar o localizador

2 - Consolidar as análises e resultados em um relatório técnico, organizando os itens solicitados. (1 ponto)

Vulnerabilidade/Ataque	**Consequência**	**Como resolver?**
Credenciais do wifi e do servidor mqtt expostos no código	Acesso não autorizado à redes Wi-Fi de parceiros e da Prodesp; Comprometimento do broker MQTT com mensagens irreais; Interceptação de dados; Sobrecarga do broker;	Criptografia e proteção no código com uso de bibliotecas específicas.
Necessidade de energia constante (pilha)	Interrupção do funcionamento do dispositivo; Perda de dados, ou seja, não envio dos pings e, consequentemente, o ativo vai para perdido depois de 3 meses, mesmo que não esteja; Substituição dos componentes do TrackFi, ou seja, necessidade de manutenção quando a pilha acabar; Ineficiência operacional; Risco de ataques por vulnerabilidade.	Desenvolvimento de um código que alerta sobre a baixa energia na bateria e possibilita a troca de bateria antes que o dispositivo fique inoperável.
Denial of Service Attack	Servidor para de funcionar devido ao overload de	Identificar esses ataques e bloquear essas requisições

	dados	
Brute force	A mesma pessoa (Hacker) pode ter tentativas infinitas para fazer login e acertar as credenciais, assim, tendo acesso total a aplicação	Implementar um limite de tentativas de login por aparelho em determinado tempo definido
Ataque bruto ao hardware	Total destruição do aparelho causando na perda do Track-Fi e de seus dados de localização	Fazer com que a case seja muito bem presa aos ativos de forma que não seja possível arrancá-la

3 - Todos os grupos devem elaborar uma tabela consolidada dos ataques e ordenar os ataques desta tabela de forma decrescente (do maior risco para o menor risco). Cada ataque deve ter um título representativo, e a tabela deve conter o título do ataque, o nível impacto caso ocorresse (baixo, médio, alto) e o nível de risco (baixo, médio, alto) como colunas. (2 pontos)

Título do Ataque	**Impacto Caso Ocorresse**	**Nível de Risco**
Denial of Service Attack	Alto	Alto
Brute Force	Médio	Médio
Ataque bruto ao hardware	Alto	Médio

Justificativa da ordem:

1. **Denial of Service Attack**: Esse ataque tem alto impacto por tornar o sistema inoperável, impedindo o uso dos serviços.
2. **Brute Force**: Embora o impacto seja médio, a ausência de limitação no número de tentativas de login aumenta o risco de acesso não autorizado.
3. **Ataque bruto ao hardware**: Apesar de ter impacto alto (se alguém fisicamente comprometer o localizador), a probabilidade é menor comparada a ataques cibernéticos, devido à necessidade de acesso físico.