Travaux pratiques - Apprendre les détails des attaques

# Objectifs

Rechercher et analyser les vulnérabilités des applications IoT

Partie 1: Rechercher les vulnérabilités des applications IoT

# Contexte/scénario

L'internet des objets (IoT) fait référence aux appareils numériques connectés qui relient tous les aspects de notre vie, y compris notre maison, notre bureau, notre voiture et même notre corps, à Internet. Avec la démocratisation du protocole IPv6 et le déploiement quasi universel des réseaux Wi-Fi, l'IoT connaît une croissance exponentielle. Selon Statista, les experts de l'industrie estiment que d'ici 2030, le nombre des appareils IoT actifs approchera les 50 milliards.

Cependant, les appareils IoT sont particulièrement vulnérables aux menaces, car le facteur sécurité n'a pas toujours été pris en compte dans la conception de ces appareils. De plus, ces appareils connectés intègrent souvent des logiciels et des systèmes d'exploitation obsolètes et non corrigés.

# Ressources requises

* Ordinateur ou terminal mobile avec accès Internet

# Instructions

## Rechercher les vulnérabilités des applications IoT

À l'aide de votre moteur de recherche favori, effectuez une recherche sur les vulnérabilités de l'Internet des objets. Lors de votre recherche, trouvez un exemple de vulnérabilité IoT pour chacun des secteurs d'activité concernés : industrie, systèmes électriques, santé et administration. Soyez prêt à expliquer qui pourrait exploiter cette vulnérabilité et pourquoi, quelle est l'origine de la vulnérabilité et comment elle pourrait être limitée.

**Remarque**: Vous pouvez utiliser le navigateur sur la machine virtuelle installée lors d'un TP précédent pour lancer votre recherche sur les problèmes de sécurité. En utilisant la machine virtuelle, vous évitez d'infecter votre ordinateur avec des malwares.

À partir des résultats de votre recherche, choisissez une vulnérabilité IoT et répondez aux questions suivantes :

**Sources : https://iotindustriel.com/cybersecurite/cyberattaques-iot-top-6-des-vulnerabilites/**

### **Dispositif médical piraté**

Cette cyberattaque contre St. Jude Medical est un exemple terrifiant de violation de la sécurité de l’IoT dans le secteur de la santé.

En octobre 2016, un groupe de pirates informatiques connu sous le nom de « Shadow Brokers » a annoncé qu’il avait volé à St. Jude Medical des documents contenant des informations sur les dispositifs médicaux de l’entreprise

L’attaque contre St. Jude Medical a mis en évidence la vulnérabilité des dispositifs médicaux aux cyberattaques et a suscité des inquiétudes quant à la sécurité des patients qui utilisent ces dispositifs.

### Questions :

* + 1. En quoi consiste la vulnérabilité ?
    2. La vulnérabilité détermine une faille de sécurité exposant à une potentielle attaque
    3. Qui pourrait l'exploiter ? Expliquez votre réponse.
    4. Quelle est l'origine de la vulnérabilité ?
    5. Que pourrait-on faire pour limiter la vulnérabilité ?

### **Mots de passe non sécurisés**

La mauvaise sécurité des mots de passe est l’un des plus grands défis de la cybersécurité des dispositifs IoT.

Malheureusement, peu d’appareils IoT sont protégés par mot de passe, et même lorsqu’ils le sont, les utilisateurs ont généralement tendance à utiliser des mots de passe par défaut, ce qui rend ces appareils vulnérables aux violations.

De plus, de nombreux appareils IoT, tels que les montres connectées, s’appuient sur la vérification d’identité à l’aide de systèmes biométriques. Bien que ceux-ci puissent être plus sécurisés que l’utilisation de mots de passe faciles à deviner, les données de vérification doivent être stockées et gérées de manière plus sécurisée.

Comme la plupart des appareils personnels, les appareils IoT sont livrés avec des paramètres par défaut codés en dur pour une configuration simple. Ces paramètres deviennent prévisibles au fil du temps et sont très peu sûrs.

* + 1. En quoi consiste la vulnérabilité ?
    2. La vulnérabilité détermine une faille de sécurité exposant à une potentielle attaque, ici les vulnérabilités sont les mots de passe par défauts et le peu d’appareils non protégé par mots de pass.
    3. Qui pourrait l'exploiter ? Expliquez votre réponse.
    4. Quelle est l'origine de la vulnérabilité ?
    5. Que pourrait-on faire pour limiter la vulnérabilité ?