Travaux pratiques – Tout savoir sur les attaques Lab (version de l'instructeur)

**Remarque à l'intention de l'instructeur**: le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

1. Objectifs

Rechercher et analyser les vulnérabilités des applications IoT

1. 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. Les experts estiment que d'ici 2020, on dénombrera près de 50 milliards d'appareils IoT actifs. 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.

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet

1. 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. Voici quelques ressources que nous vous conseillons de consulter pour démarrer votre recherche :

[Ressources Cisco sur l'IoT](http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html)

[Règles de sécurité concernant l'IoT](https://iotsecurityfoundation.org/)

[Business Insider - Menaces de sécurité IoT](http://www.businessinsider.com/iot-cyber-security-hacking-problems-internet-of-things-2016-3)

**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 :

* + 1. En quoi consiste la vulnérabilité ?

**La vulnérabilité identifiée concerne les dispositifs médicaux IoT utilisés dans les hôpitaux. Certains de ces dispositifs ne chiffrent pas correctement les données qu'ils transmettent, rendant les informations médicales sensibles vulnérables aux interceptions non autorisées.**

Les réponses varient selon la vulnérabilité choisie.

* + 1. Qui pourrait l'exploiter ? Expliquez votre réponse.

**Des hackers malveillants pourraient exploiter cette vulnérabilité pour intercepter et accéder aux données médicales sensibles des patients. Cela pourrait être motivé par des intentions malveillantes telles que le vol d'identité ou la demande de rançon.**

Les réponses varient selon la vulnérabilité choisie.

* + 1. Quelle est l'origine de la vulnérabilité ?

**L'origine de la vulnérabilité réside souvent dans la conception des dispositifs médicaux IoT, qui ne mettent pas en œuvre de manière adéquate les protocoles de sécurité pour le chiffrement des données. Les mises à jour de sécurité sont également souvent négligées.**

Les réponses varient selon la vulnérabilité choisie.

* + 1. Que pourrait-on faire pour limiter la vulnérabilité ?

**Pour limiter cette vulnérabilité, les fabricants de dispositifs médicaux devraient mettre en place un chiffrement robuste des données lors de la transmission. Les hôpitaux devraient également s'assurer que les dispositifs médicaux sont régulièrement mis à jour avec les derniers correctifs de sécurité.**

Les réponses varient selon la vulnérabilité choisie.