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

Partie 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.

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 :

a. En quoi consiste la vulnérabilité ?

Les vulnérabilités sont des faiblesses ou des failles dans les systèmes informatiques qui peuvent être exploitées par des attaquants pour compromettre la sécurité. Les vulnérabilités peuvent résider dans les logiciels, les systèmes d'exploitation, les applications, les protocoles réseau ou même les erreurs humaines.

b. Qui pourrait l'exploiter ? Expliquez votre réponse.

La vulnérabilité pourrait être exploitée par des hackers, des cybercriminels ou même des employés malveillants ayant des connaissances techniques. Ils pourraient utiliser ces vulnérabilités pour surveiller les activités des installations industrielles, obtenir des informations sensibles, perturber les opérations ou lancer d'autres attaques ciblées.

c. Quelle est l'origine de la vulnérabilité ?

L'origine d'une vulnérabilité peut être attribuée à des pratiques de sécurité insuffisantes lors de la conception et de la configuration des caméras de surveillance. Des mots de passe par défaut non modifiés, des mises à jour de firmware non appliquées et des protocoles de communication non sécurisés sont quelques-unes des causes courantes de cette vulnérabilité.

d. Que pourrait-on faire pour limiter la vulnérabilité ?

Pour limiter les vulnérabilités, plusieurs mesures peuvent être prises :

➔ Changer les mots de passe par défaut et utiliser des mots de passe forts.

➔ Mettre à jour régulièrement le firmware des équipements pour bénéficier des correctifs de sécurité.

➔ Utiliser des protocoles de communication sécurisés, tels que le chiffrement des données.

➔ Mettre en place un contrôle d'accès strict pour restreindre l'accès des équipements aux utilisateurs autorisés uniquement.

➔ Effectuer des tests de vulnérabilité et des audits de sécurité réguliers pour détecter et corriger les vulnérabilités avant qu'elles ne soient exploitées.