PROJET 1 : PLATEFORME DE PRIORISATION DES VULNÉRABILITÉS IOT

Annonce: Semaine 2 --- **Remise et présentation:** Semaine 9

Contexte

La popularité croissante des objets connectés (caméras IP, routeurs, assistants, capteurs, passerelles IIoT) accroît les risques lorsque les mises à jour ne sont pas appliquées, que les configurations restent par défaut ou que l'exposition du réseau n'est pas maîtrisée. Dans les tendances récentes, de nombreuses campagnes exploitent rapidement des vulnérabilités publiées et ciblent des équipements "edge". Ce projet vise à renforcer la capacité à surveiller, comprendre et prioriser ces vulnérabilités afin de réduire le risque.

But du projet

Concevoir et réaliser une plateforme web qui se met à jour automatiquement à partir de sources ouvertes et gratuites, afin d'informer les utilisateurs sur les vulnérabilités pertinentes aux objets connectés, de prioriser celles qui représentent le plus grand risque, et de proposer des mesures de mitigation concrètes.

Périmètre

Chaque équipe choisit soit une famille d'objets IoT (par exemple caméras IP, routeurs domestiques/PME, systèmes domotiques, passerelles industrielles), soit un écosystème/vendeur. Le travail se base uniquement sur des données publiques. Il n'est pas nécessaire d'acheter un appareil ni de réaliser des tests intrusifs.

Objectifs attendus

La plateforme doit collecter automatiquement des informations de vulnérabilités (identifiants CVE), enrichir ces informations avec des données de scoring et de contexte, identifier si une vulnérabilité est activement exploitée, puis fournir une priorisation du risque. La priorisation ne doit pas se limiter au CVSS (Common Vulnerability Scoring System - système d'évaluation de sévérité) : elle doit au minimum combiner l'impact (CVSS), l'exploitation réelle (KEV - Known Exploited Vulnerabilities - vulnérabilités connues en cours d'exploitation) et une estimation de probabilité d'exploitation (EPSS - Exploit Prediction Scoring System - système de prédiction du risque d'exploitation).

Fonctionnalités minimales (MVP)

La solution doit inclure un module de collecte automatique (script planifié, worker, ou tâche cron), un stockage documenté (base locale ou fichiers structurés), une interface web de consultation (recherche, filtres, tri, détail), un module de priorisation explicite, et une section de recommandations (patching, configuration, segmentation, désactivation de services, bonnes pratiques).

Contraintes et règles

Le projet doit rester strictement défensif. Il est interdit de scanner Internet, d'attaquer des systèmes réels ou de publier des contenus opérationnels d'exploitation. Les données utilisées doivent être open-source et gratuites. Toutes les sources doivent être référencées (URL et date d'accès).

Livrables (Semaine 6)

Un rapport de 8 à 12 pages décrivant l'architecture, le pipeline de collecte, le modèle de données, la méthode de priorisation, les limites et les recommandations; une présentation de 20 minutes incluant une démonstration; et un code reproductible avec un README (dépendances, commandes d'exécution, et exemples de données).

Évaluation (recommandation /100)

Collecte et qualité des données (25) | Priorisation du risque et justification (20) | Interface et clarté de la restitution (15) | Analyse et recommandations incluant des aspects de confidentialité (25) | Qualité du rapport et de la présentation (15)

Sources et liens open-source à utiliser

NVD (NIST) - base de vulnérabilités: https://nvd.nist.gov/
NVD API - documentation développeurs: https://nvd.nist.gov/developers/vulnerabilities
CISA KEV - catalogue des vulnérabilités exploitées: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
CISA KEV - ressources (fichiers, schéma): https://www.cisa.gov/resources-tools/resources/kev-catalog
EPSS (FIRST) - score de probabilité d'exploitation: https://www.first.org/epss/
EPSS API: https://www.first.org/epss/api
CVE Program - identifiants CVE: https://www.cve.org/
CWE (MITRE) - catégories de faiblesses: https://cwe.mitre.org/
ETSI EN 303 645 v3.1.3 - baseline IoT: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259a.pdf
NISTIR 8259B - IoT Non-Technical Supporting Capability Core Baseline: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259B.pdf

Outils gratuits suggérés

Backend : Python (Flask/FastAPI) ou Node.js (Express) | Stockage : SQLite ou fichiers JSON/CSV | Frontend : React/Vue ou pages HTML simples | Déploiement : local; Docker optionnel