Cybersecurity Insights

Le marché et les enjeux autour des scanners de vulnérabilités

Côme **BERNE**
Stagiaire Cyber Tech & Transformation

FAILLES DE SÉCURITÉ : DES POINTS D'ENTRÉE VARIÉS, DES RISQUES ACCRUS

Dans le paysage numérique actuel, les systèmes d'information et les réseaux informatiques sont constamment **exposés** à une multitude de **failles de sécurité**. Qu'elles soient d'origine logicielle, matérielle ou humaine, elles représentent des vulnérabilités potentielles pouvant être exploitées par des **acteurs malveillants**. Ces failles englobent un large spectre, allant des **erreurs de configuration aux bugs logiciels**, en passant par les faiblesses des protocoles de communication et **des stratégies de sécurité inadéquates**.
Voici les grandes familles de failles ainsi que quelques exemples concernant ces dernières :

FAILLES RÉSEAU

- Protocoles réseaux vulnérables
- Protocoles non sécurisés (Telnet/SSH)
- Faiblesse dans le chiffrement
- Faiblesse dans la configuration

FAILLES SYSTÈME

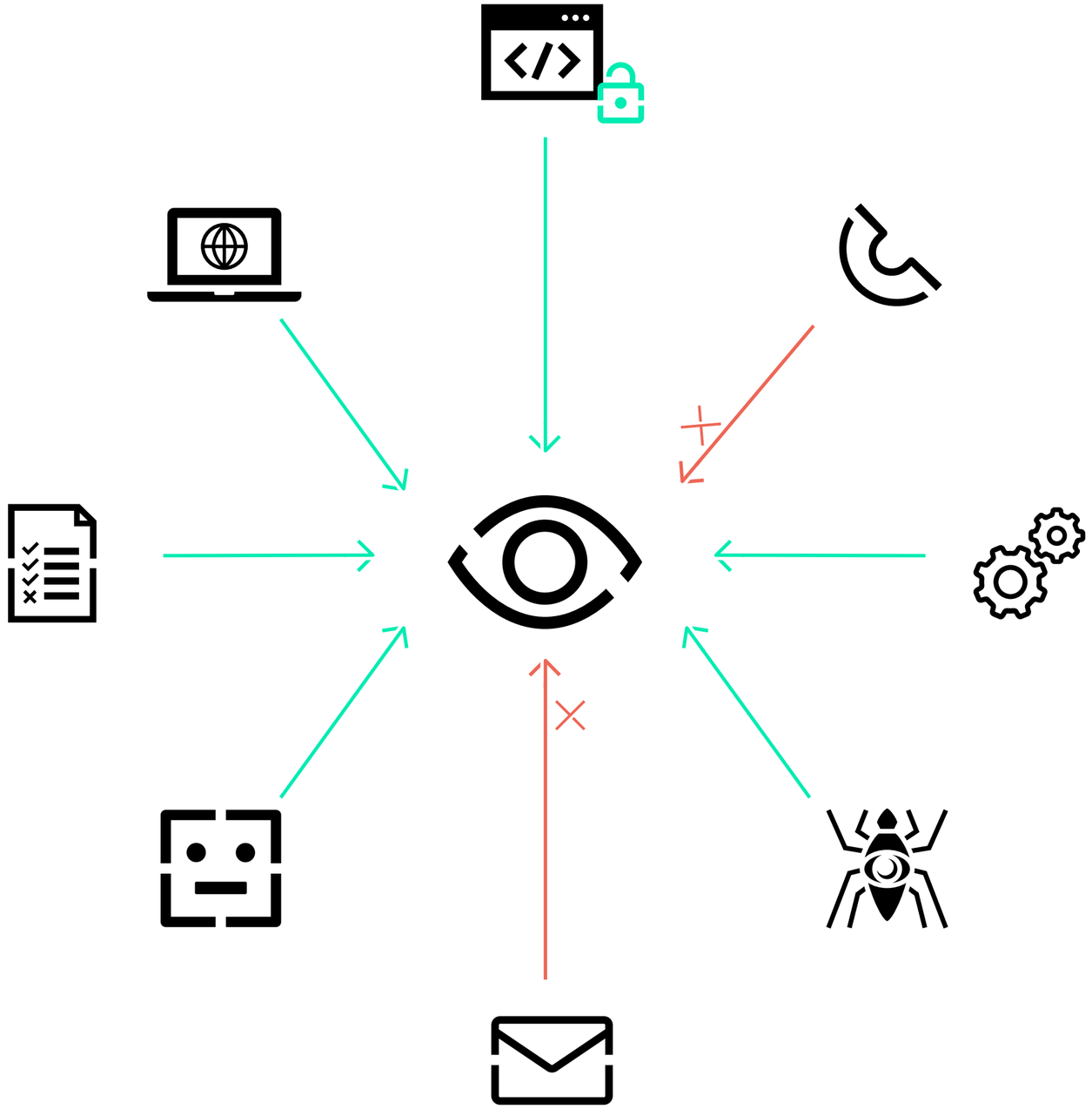
- Dépassement de mémoire
- Faiblesses dans le noyau même
- Race condition

FAILLES WEB

- Injection de code et de commandes malveillantes
- Authentification faible
- Faiblesse de configuration

Certains types de failles ne sont pas détectables par un scanner de vulnérabilités du fait de leurs **spécificités** (failles concernant les attaques par canaux auxiliaires par exemple) ou de leur aspect inhérent à la **complexité du comportement humain** (phishing ou toute attaque par ingénierie social) car ce sont des aspects qui ne sont pas mesurables tangiblement.

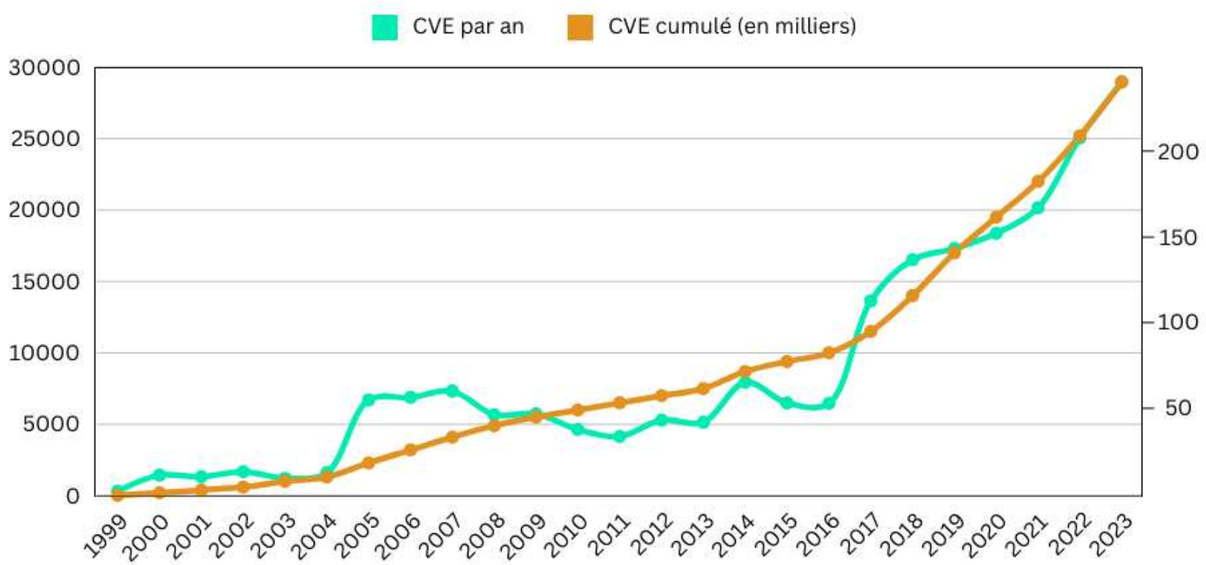
Finalement, un scanner de vulnérabilités analyse en détail les **contraintes techniques** d'un système pour évaluer sa **vulnérabilité**, en utilisant une base de données comme référence et en se concentrant uniquement sur le **contenu de ce système**.



UN REGARD HISTORIQUE : DE SATAN À L'ÈRE DE LA SÉCURITÉ AUTOMATISÉE ET DES NORMES PCI DSS

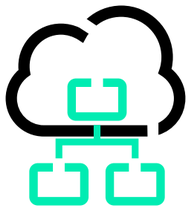
Historique

- Le premier scanner historique, SATAN (Security Administrator Tool for Analizing Networks) voit le jour en 1995.
- La croissance exponentielle du nombre de vulnérabilités au début des années 2000 a rendu la détection à la main impossible, une solution automatisée a donc été nécessaire à la bonne réalisation de cette mission.
- Augmentation du nombre de scanners avec les nouvelles normes de sécurité (PCI DSS en 2004) qui sont adoptées en tant qu'exigence et de meilleurs pratiques.



Source : https://www.cvedetails.com/vulnerabilities-by-types.php

UN PÉRIMÈTRE DE COUVERTURE ÉTENDU ET UN DÉPLOIEMENT FLEXIBLE

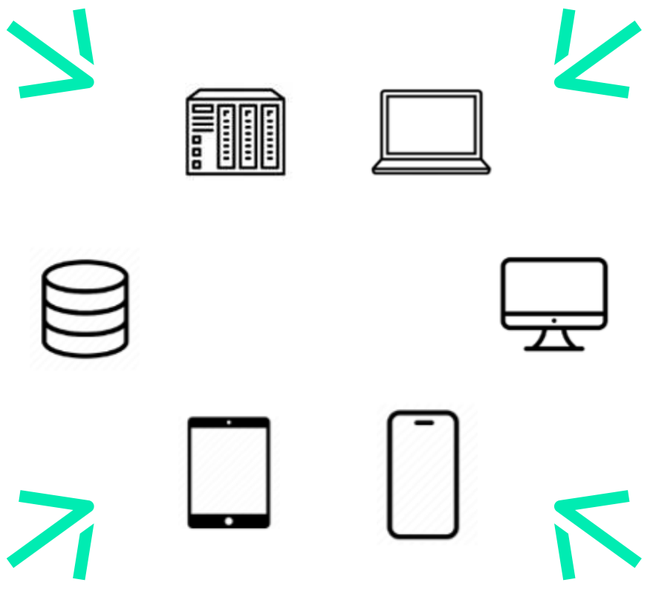


Saas

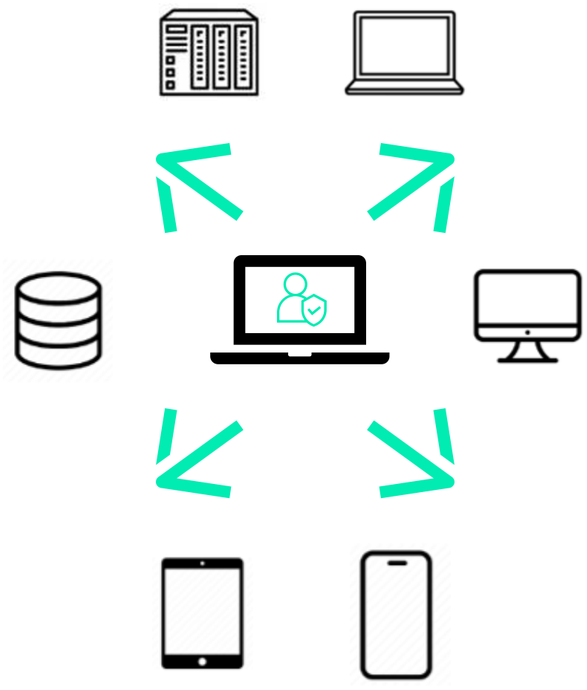
Machine virtuelle

Hébergé

SCAN DE VULNÉRABILITÉ EXTERNE



SCAN DE VULNÉRABILITÉ INTERNE



Cible et architecture

- Le scanner a pour cible toute machine générique possédant une IP.
- Il peut être déployé dans le cloud (solution SaaS, software as a service), sur une machine virtuelle ou directement sur une machine faisant l'objet du scan.
- Plusieurs types de scans existent : en dehors du réseau cible (scan externe) ou à l'intérieur (scan interne) auxquels on peut ajouter des identifiants pour avoir accès directement à la machine (scan authentifié).

DE LA DÉTECTION À L'ANALYSE

La majorité des scanners fonctionnent de la manière suivante :

01.

Host Discovery avec les protocoles ARP, IMP et TCP/UDP

02.

Scan des ports TCP/UDP

03.

Comparaison en fonction des labels à une base de données de vulnérabilités

04.

Modules plus spécifiques (malware, applications web, mot de passe par défaut...)

05.

Scan authentifié éventuellement (escalade de privilège, gestion des accès...)

06.

Rédaction automatique d'un rapport

AVANTAGES ET LIMITES

Finalement on peut distinguer plusieurs avantages et inconvénients inhérents aux scanners de vulnérabilités :

	Rapidité et efficacité	Portée et flexibilité	Facilité d'utilisation	Autres
Avantages	• Automatisés donc rapides	• Large éventail de services testés • Personnalisables	• Faciles à utiliser	• Support technique
Inconvénients	• Reste moins précis qu'un test d'intrusion • Faux positifs et faux négatifs fréquents	• Ne convient cependant pas pour des services précis (Active Directory, systèmes industriels, services maison...) • Ne traitent pas les failles d'ingénierie sociales	• Peuvent nécessiter des compétences pour le déploiement et l'interprétation des résultats	• Infos brutes donc manque de visibilité sur certains points notamment l'exposition et le risque business

PANORAMA DES ACTEURS ACTUELS DU MARCHÉ

IKare by ITrust

Qualys

Nessus vulnerability scanner

TRIPWIRE IP360

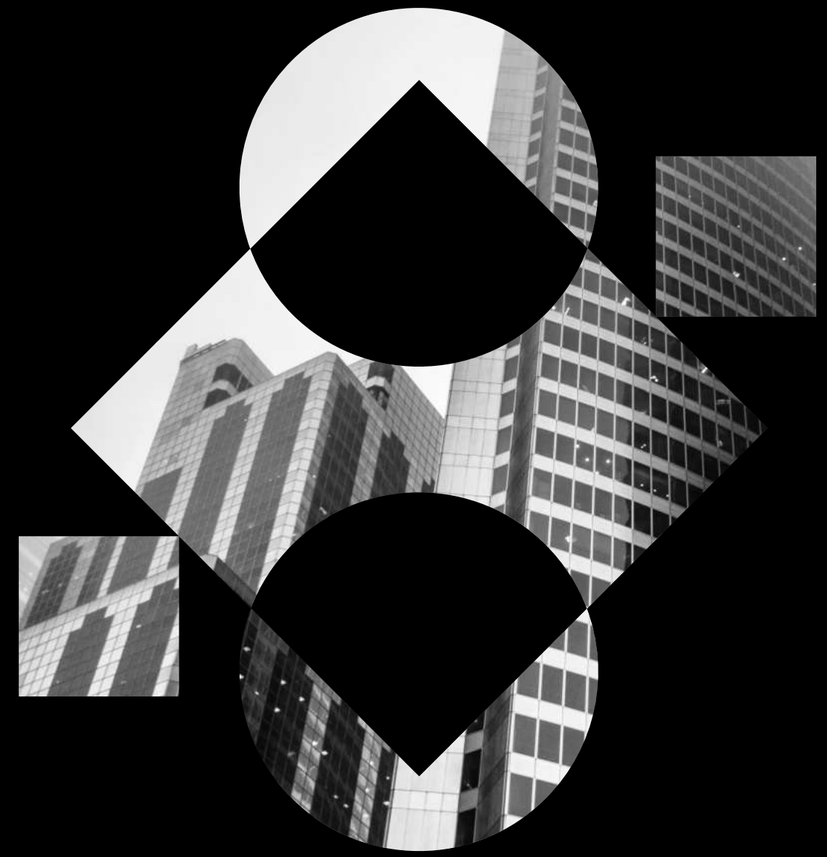
RAPID7 insightVM

VERS UNE APPROCHE COMPLÈTE ET INTELLIGENTE

Actuellement, les éditeurs de solutions de sécurité informatique s'orientent de plus en plus vers des **outils complets**. En effet, en plus du simple scanner de vulnérabilités, plusieurs modules sont ajoutés pour renforcer l'efficacité de ces solutions. Parmi ces modules, on peut citer les évaluations de conformité suivant différents standards, les **scans de cloud** et l'intégration de patching automatisé.

Enfin, ces solutions proposent une variété de **services et d'infrastructures** supportés toujours plus nombreux.

Certains éditeurs commencent également à utiliser **l'intelligence artificielle** dans leurs produits pour obtenir des résultats plus précis. Ces algorithmes d'IA peuvent analyser les vulnérabilités en tenant compte de leur **impact potentiel** sur l'entreprise, de la probabilité **qu'elles soient exploitées** et de leur **gravité globale**. Grâce à cette approche, les entreprises peuvent non seulement identifier les menaces de manière plus fine, mais aussi **prioriser les actions à entreprendre** en fonction de la criticité des failles identifiées, améliorant ainsi leur résilience face aux cyberattaques.



LES ENJEUX DE LA DATA

Pour résumer, un scanner est un **élément essentiel** dans un projet de gestion des vulnérabilités et de l'amélioration de la sécurité des systèmes d'information par **son vaste champ d'action**, **sa facilité d'utilisation et son automatisation.** Le marché des scanners de vulnérabilités est vaste avec des acteurs proposant des solutions similaires mais **différentiables** par plusieurs qualités.
Finalement, voici quelques pistes à suivre pour choisir judicieusement votre scanner de vulnérabilités :

Critères techniques

Qualité et quantité de vulnérabilités — Rapidité de scan

Etendue des équipements pris en compte — Faux positifs et faux négatifs

Bande passante, CPU, mémoire, stockage — Modules additionnels, personnalisation

Fréquence de mise à jour — Facilité d'intégration

Critères utilisateurs et commerciaux

Prix — Facilité d'utilisation

Facilité de mise en place — Support technique

Pertinence dans le classement des vulnérabilités — Certification (ASV PCI-DSS par exemple)