

Rapport de benchmarking des solutions de sécurité *Red team*

Synthèse des notations et pondérations

Critère	Nessus		OpenVAS	
	Note	Poids	Note	Poids
Mise à jour	0	5	0	5
Capacité de détection	0	5	0	5
Configuration	0	4	0	4
Rapidité d'exécution	0	4	0	4
Consommation de ressources	0	4	0	4
Explication de vulnérabilité	0	4	0	4
Documentation	0	4	0	4
Scope de scan	0	3	0	3
Flexibilité	0	3	0	3
Communauté	0	2	0	2
Compatibilité avec outils externes	0	3	0	3
Note finale	0		0	

Appréciation

D'après les résutats ci-dessus, la solution de sécurité offensive dont vous avez besoin est :

Nessus

Résultats de l'évaluation de Suricata

Critère : Mise à jour	Description : Capacité de l'outil à détecter les vulnérabilités les plus récentes.
Critère : Capacité de détection	Description : Capacité de l'outil a déceler des vulnérabilités.
Critère : Configuration	Description : Pertinence des options de configuration des scans proposées par l'outil. Les options de configuration sont importantes pour s'adapter à certaines architectures peu communes, mais trop d'options peuvent perdre l'utilisateur.
Critère : Rapidité d'exécution	Description : Temps demandé par l'outil pour scanner une cible
Critère : Consommation de ressources	Description : Quantité de ressources demandées par l'outil. Un scanner consommant trop de ressources peut être handicapant pour l'entreprise car il faudrait allouer une machine puissante uniquement pour le scanner.
Critère : Explication de vulnérabilité	Description : Capacité de l'outil à expliquer simplement une vulnérabilité, voire proposer une méthode de correction possible.
Critère : Documentation	Description : Volume et pertinence de la documentation officielle de l'outil.
Critère : Scope de scan	Description : Capacité de l'outil à scanner plusieurs machines simultanément.
Critère : Flexibilité	Description : Capacité de l'outil à s'adapter à ses différents utilisateurs (personnalisation des rapports, des paramètres, ...)
Critère : Communauté	Description : Présence d'une communauté active autour de l'outil. Une communauté active sur un projet permet de faire avancer le projet dans la bonne direction et de remonter les bugs ou problèmes rapidement aux développeurs.

Critère : Compatibilité
avec outils externes

Description :

Compatibilité de l'outil avec des applications tierces permettant d'effectuer des scans (Nmap, par exemple). Cette fonctionnalité n'est pas forcément importante mais peut être appréciée.