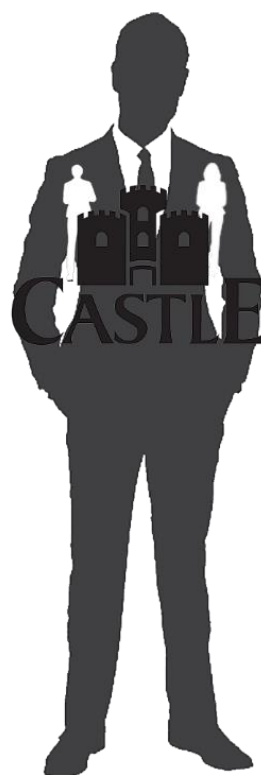


CASTLE

Rapport de benchmarking



En partenariat avec l'ensibs: École d'Ingénieurs
Université Bretagne Sud

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 résutatats ci-dessus, la solution de sécurité offensive dont vous avez besoin est :

Nessus

Rapport de benchmarking des solutions de sécurité *Red team*

Résultats de l'évaluation de nessus

Critère : Mise à jour	Description du critère de notation : Capacité de l'outil à détecter les vulnérabilités les plus récentes.
------------------------------	---

Note attribuée pour ce critère : 0 / 5

L'outil est mis à jour moins d'une fois par an.

Critère : Capacité de détection	Description du critère de notation : Capacité de l'outil à détecter des vulnérabilités.
--	---

Note attribuée pour ce critère : 0 / 5

L'outil a détecté moins de 10% des vulnérabilités.

Critère : Configuration	Description du critère de notation : 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.
--------------------------------	--

Note attribuée pour ce critère : 0 / 5

Le scanner ne propose pas d'options de configuration.

Critère : Rapidité d'exécution	Description du critère de notation : Temps demandé par l'outil pour scanner une cible
---------------------------------------	---

Note attribuée pour ce critère : 0 / 5

Le scanner met plus de 36 heures pour analyser une machine.

Critère : Consommation de ressources	Description du critère de notation : 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.
---	---

Note attribuée pour ce critère : 0 / 5

Le scanner utilise plus de 80% du CPU de la machine hôte.

Critère : Explication de vulnérabilité	Description du critère de notation : Capacité de l'outil à expliquer simplement une vulnérabilité, voire proposer une méthode de correction possible.
---	---

Note attribuée pour ce critère : 0 / 5

Le rapport d'analyse contient seulement le nom de la vulnérabilité.

Critère : Documentation	Description du critère de notation : Volume et pertinence de la documentation officielle de l'outil.
--------------------------------	--

Note attribuée pour ce critère : 0 / 5

La documentation de l'outil est inexistente.

Critère : Scope de scan	Description du critère de notation : Capacité de l'outil à scanner plusieurs machines simultanément.
--------------------------------	--

Note attribuée pour ce critère : 0 / 5

Le scanner pratique une analyse service par service.

Critère : Flexibilité	Description du critère de notation : Capacité de l'outil à s'adapter à ses différents utilisateurs (personnalisation des rapports, des paramètres, ...)
------------------------------	---

Note attribuée pour ce critère : 0 / 5

L'outil ne permet pas la création de règles.

Critère : Communauté	Description du critère de notation : 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.
-----------------------------	--

Note attribuée pour ce critère : 0 / 5

L'outil ne possède pas de communauté présente.

Critère : Compatibilité avec outils externes	Description du critère de notation : 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.
---	---

Note attribuée pour ce critère : 0 / 5

L'outil n'est compatible avec aucun outil externe.

Rapport de benchmarking des solutions de sécurité *Red team*

Résultats de l'évaluation de openvas

Critère : Mise à jour	Description du critère de notation : Capacité de l'outil à détecter les vulnérabilités les plus récentes.
------------------------------	---

Note attribuée pour ce critère : 0 / 5

L'outil est mis à jour moins d'une fois par an.

Critère : Capacité de détection	Description du critère de notation : Capacité de l'outil à détecter des vulnérabilités.
--	---

Note attribuée pour ce critère : 0 / 5

L'outil a détecté moins de 10% des vulnérabilités.

Critère : Configuration	Description du critère de notation : 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.
--------------------------------	--

Note attribuée pour ce critère : 0 / 5

Le scanner ne propose pas d'options de configuration.

Critère : Rapidité d'exécution	Description du critère de notation : Temps demandé par l'outil pour scanner une cible
---------------------------------------	---

Note attribuée pour ce critère : 0 / 5

Le scanner met plus de 36 heures pour analyser une machine.

Critère : Consommation de ressources	Description du critère de notation : 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.
---	---

Note attribuée pour ce critère : 0 / 5

Le scanner utilise plus de 80% du CPU de la machine hôte.

Critère : Explication de vulnérabilité	Description du critère de notation : Capacité de l'outil à expliquer simplement une vulnérabilité, voire proposer une méthode de correction possible.
---	---

Note attribuée pour ce critère : 0 / 5

Le rapport d'analyse contient seulement le nom de la vulnérabilité.

Critère : Documentation	Description du critère de notation : Volume et pertinence de la documentation officielle de l'outil.
--------------------------------	--

Note attribuée pour ce critère : 0 / 5

La documentation de l'outil est inexistente.

Critère : Scope de scan	Description du critère de notation : Capacité de l'outil à scanner plusieurs machines simultanément.
--------------------------------	--

Note attribuée pour ce critère : 0 / 5

Le scanner pratique une analyse service par service.

Critère : Flexibilité	Description du critère de notation : Capacité de l'outil à s'adapter à ses différents utilisateurs (personnalisation des rapports, des paramètres, ...)
------------------------------	---

Note attribuée pour ce critère : 0 / 5

L'outil ne permet pas la création de règles.

Critère : Communauté	Description du critère de notation : 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.
-----------------------------	--

Note attribuée pour ce critère : 0 / 5

L'outil ne possède pas de communauté présente.

Critère : Compatibilité avec outils externes	Description du critère de notation : 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.
---	---

Note attribuée pour ce critère : 0 / 5

L'outil n'est compatible avec aucun outil externe.