ESD Cybersecurity Academy
10, rue de Penthièvre
75008 - PARIS

Téléphone : 08 05 62 60 00
Email : contact@esdacademy.eu
Https://esdacademy.eu/

Exemple Rapport Test d'intrusion

[Nom_client]

Test d'intrusion : [Nom_application]

Date : [Date_rapport]

variables rapport :

[Nom_client]
[Nom_application]
[Date_rapport]
[Date_Réunion]
[Durée_test]
[Type-Pentest] (boite blanche, grise, noir)

Rédigé par :		Date de création :	
Validé par :		Date d'application :	
Approuvé par :		Version :	

Table des matières

1. préambule

a. Contexte et note de l'application

[Nom_client] a mandaté la société ESD Cybersecurity Academy pour réaliser un audit de sécurité sur *[Nom_application]*. La réunion de lancement a eu lieu le : [Date_Réunion]
La prestation a été réalisée dans les locaux de la société ESD Cybersecurity Academy sur une durée de [Durée_test]

Ce qui a été réalisé:

- Une évaluation des vulnérabilités présentes.
- Une évaluation de la sécurité des différents modules
- Une appréciation qualité fonctionnelle de la sécurité mise en place (habilitation, intégrité, disponibilité, paramétrage...).
- Des recommandations techniques permettant de remédier aux éventuelles failles et/ou faiblesses décelées au cours de la prestation.
- Un plan d'action permettant d'atteindre le niveau de sécurité requis et d'en assurer la pérennité.
- Une mise en évidence des risques résiduels.

Sur une échelle de 1 à 9, le score de criticité de l'application est de : **000**

Score de vraisemblance	0,00	Score de gravité	0,00
Criticité de l'application (échelle 1 à 9) : 0,00 **(satisfaisant)**, **(à améliorer)**, **(critique)**			

b. Périmètre

La société ESD Cybersecurity Academy intervient sur l'application [Nom_application] avec l'URL suivante: https://xxxxxxxx .
Un compte utilisateur: xxx@xxx.xxx - a été fourni pour mener à bien le test d'intrusion.
Le test d'intrusion est donc de type boîte [Type-Pentest].

Après une recherche, X entrées potentielles (pages, liens, etc) ont été trouvées.
L'arborescence ci-dessous suivante est donc le périmètre de l'application.

image arborescence

c. Méthodologie

Pour effectuer les tests, l'auditeur a utilisé le référentiel de l'OWASP testing guide modifié et EBIOS Risk manager.
L'OWASP (Open Web Application Security Project) est une communauté mondiale ayant pour objectif d'améliorer la sécurité des applications. Pour cela, elle met à disposition gratuitement et librement un ensemble de matériels (normes, outils, ouvrages, projets...) créés et maintenus au sein de la communauté. Structurée sous forme de chapitres locaux dans le monde entier, elle organise également des évènements autour de la Sécurité des Applications Web.

Voici les différentes phases du test:

La méthode OWASP propose de dérouler un test d'intrusion applicatif sous forme de checklist avec différentes catégories:

Phase 1 - Recherche d'informations / prise d'empreintes

Le but est de rechercher de l'information sur l'organisation et ses membres. Des logiciels dits OSINT (open source intelligence) permettent de récupérer de l'information avec un cheminement précis.

Phase 2 - Tests de configuration

Cette phase a pour objectif la recherche de diverses brèches sur le réseau, application web, classifier le degré de criticité des vulnérabilités trouvées.

Phase 3 - Tests applicatifs

En adéquation avec ce qui a été trouvé dans la phase précédente, le testeur tente de pénétrer le serveur web par le biais de différentes injections.

Phase 4 - Reporting

La phase de « reporting » consiste à rassembler les outputs des différents tests et de consolider le rapport autour d'une étude des risques applicatifs.

d. Métriques

Les phases 1, 2, 3 du test d'intrusion terminées. Un listing des vulnérabilités est établie, exemple :

No	Type	Chemin	Vraisemblance	Gravité	Note
1	ex 1	ex1.php	Facilité de détection 7	Perte d'intégrité 7	Critique
2	ex 2	ex2.php	Vulnérabilité connue 6	Perte disponibilité 2	Moyen

Ici, la gravité et la vraisemblance des vulnérabilités sont évaluées par les critères suivants:

Critères d'évaluation de la *vraisemblance* technique (1 à 9)			
Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection

Critères d'évaluation de la *gravité* technique (1 à 9)			
Perte de confidentialité	Perte d'intégrité	Perte de disponibilité	Perte de traçabilité

	Note gravité		
Note vraisemblance	Faible (1, 2, 3)	Moyenne (4, 5, 6)	Haute (7, 8, 9)
Faible (1, 2, 3)	Négligeable	Faible	Moyen
Moyenne (4, 5, 6)	Faible	Moyen	Important
Haute (7, 8, 9)	Moyen	Important	Critique

Une fois toutes les vulnérabilités répertoriées, celles-ci sont évaluées par pondération avec des critères techniques et métiers. Ce qui permet de transformer des vulnérabilités en risque et d'apporter une dimension stratégique au test d'intrusion et éventuellement l'alignement à une analyse de risque SSI (sécurité des systèmes d'information).
À noter, que l'évaluation de la gravité et de la vraisemblance métier sont à renseigner en amont dans les règles d'engagements par le commanditaire du test d'intrusion.
Ci-dessous les matrices d'évaluation des risques de l'application:

Critère de
vraisemblance du risque total pour l'application

Critères d'évaluation de la *vraisemblance technique*			
Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection
Critères d'évaluation de la *vraisemblance métier* (capacité de la source de risque)			
Capacité de l'attaquant	Motivation de l'attaquant	Besoin d'accès et de ressources de l'attaquant	Proximité de l'attaquant
Total = sum(vraisemblance technique / vraisemblance métier) / 8 critères			

Critère de gravité du risque total pour l'application

Critères d'évaluation de la *gravité* technique (vulnérabilité)			
Perte de confidentialité	¨Perte d'intégrité	Perte de disponibilité	Perte de traçabilité
Critères d'évaluation de la *gravité* (métier)			
Dommage financier	Dommage en réputation	Dommage de non-conformité	Dommage en violation de la vie privée
Total = sum(gravité technique / gravité métier) / 8 critères			

Exemple de notation du risque pour l'application

Score de vraisemblance	0,00	Score de gravité	0,00
Criticité de l'application (échelle 1 à 9) : 0,00 **(satisfaisant)**, **(à améliorer)**, **(critique)**			

1. résumé du test d'intrusion

a. Synthèse du test d'intrusion

Nombre de vulnérabilités identifiées	0
Critère de sécurité *confidentialité*	0
Critère de sécurité intégrité	0
Critère de sécurité *disponibilité*	0
Critère de sécurité *traçabilité*	0
Recommandations	0
Points positifs	0
Niveau critique de l'application (échelle 1 à 9)	0

b. listing des vulnérabilités

id	Vulnérabilité	Score
V01	xxx	0
V02	xxx	0

c. Préconisations

id	Préconisations	Coût	Difficulté
P01	xxx	Faible	Faible
P02	xxx	Faible	Faible
P03	xxx	Faible	Faible
P04	xxx	Faible	Faible

d. Point positif

id	Remarques
REM01	xxx
REM02	xxx
REM03	xxx
REM04	xxx

2. test d'intrusion

a. Infrastructure

i. visibilité

1. enregistrements WHOIS

Description de test

Le WHOIS est un registre contenant les informations sur le propriétaire d'un nom de domaine. Dans
certain cas, des informations sensibles peuvent être présentes dans ce registre.

Observation
xxx

Caractéristique de la vulnérabilité

	Critère vraisemblance				
ID	Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection	Note
V	0	0	0	0	0,00
	Critère gravité				
	Perte de confidentialité	Perte d'intégrité	Perte de disponibilité	Perte de traçabilité	
	0	0	0	0	

Préconisation

id	Préconisations	Coût	Difficulté
P	xxx	Faible	Faible

Point positif

id	Point positif
REM	xxx

2. référencement par les Moteurs de recherche

Description de test
L'indexation de certaines pages non pertinentes n'apporte rien à un utilisateur de l'application. Par contre, celles-ci peuvent fournir quelques informations sur l'application à un attaquant (ex. : pages spécifiques à un module de statistiques de visites, etc.).

Observation
xxx

Caractéristique de la vulnérabilité

	Critère vraisemblance				
ID	Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection	Note
V	0	0	0	0	0,00
	Critère gravité				

	Perte de confidentialité	Perte d'intégrité	Perte de disponibilité	Perte de traçabilité	
	0	0	0	0	

Préconisation

id	Préconisations	Coût	Difficulté
P	xxx	Faible	Faible

Point positif

id	Point positif
REM	xxx

ii. Serveurs

1. Transfert de zone DNS

Description de test

Un transfert de zone DNS, lorsque celui-ci est activé, permet d'obtenir le contenu de la base DNS sur le serveur ayant autorité sur le domaine. L'attaquant peut ainsi obtenir la totalité de la configuration des sous-domaines ainsi que les adresses IP associées.

Observation

xxx

Caractéristique de la vulnérabilité

	Critère vraisemblance				
ID	Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection	Note
V	0	0	0	0	0,00
	Critère gravité				
	Perte de confidentialité	Perte d'intégrité	Perte de disponibilité	Perte de traçabilité	
	0	0	0	0	

Préconisation

id	Préconisations	Coût	Difficulté
P	xxx	Faible	Faible

Point positif

id	Point positif
REM	xxx

2. Version du service DNS

Description de test

Des attaques sont réalisables sur plusieurs versions de de service DNS ne disposant pas des correctifs nécessaires. Ainsi, la connaissance de la version du service DNS utilisé permet à un attaquant d'identifier très rapidement un serveur potentiellement vulnérable. Cette information permet donc à un attaquant de compromettre rapidement un serveur DNS vulnérable. Il est à noter que cette valeur peut être modifiée par l'administrateur et peut donc ne pas refléter la version réelle du logiciel utilisé.

Observation

xxx

Caractéristique de la vulnérabilité

	Critère vraisemblance				
ID	Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection	Note
V	0	0	0	0	0,00
	Critère gravité				
	Perte de confidentialité	Perte d'intégrité	Perte de disponibilité	Perte de traçabilité	
	0	0	0	0	

Préconisation

id	Préconisations	Coût	Difficulté
P	xxx	Faible	Faible

Point positif

id	Point positif
REM	xxx

3. Services accessibles

Description de test

La présence de services augmente la surface d'attaque de la cible : configurations de plusieurs applications à gérer, suivi des correctifs de sécurité d'applications supplémentaires, augmentation du risque de configuration non sécurisée d'une application,

etc. Un attaquant aura donc d'autant plus de possibilités de compromission de la cible que de services non nécessaires accessibles.

Observation
xxx

Caractéristique de la vulnérabilité

	Critère vraisemblance				
ID	Facilité de détection	Facilité d'exploitation	Vulnérabilité connue	Détection	Note
V	0	0	0	0	0,00
	Critère gravité				
	Perte de confidentialité	Perte d'intégrité	Perte de disponibilité	Perte de traçabilité	
	0	0	0	0	

Préconisation

id	Préconisations	Coût	Difficulté
P	xxx	Faible	Faible

Point positif

id	Point positif
REM	xxx