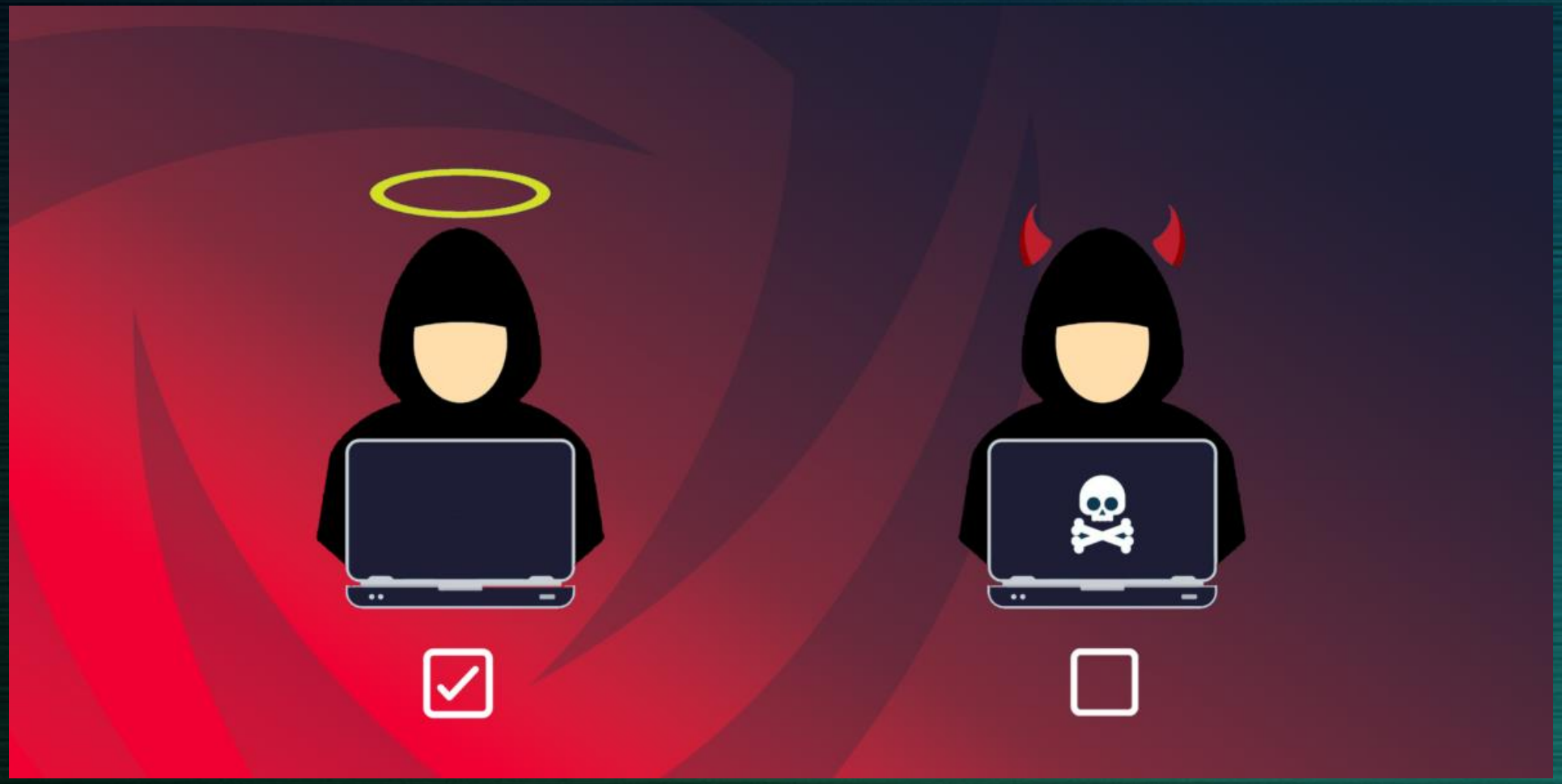
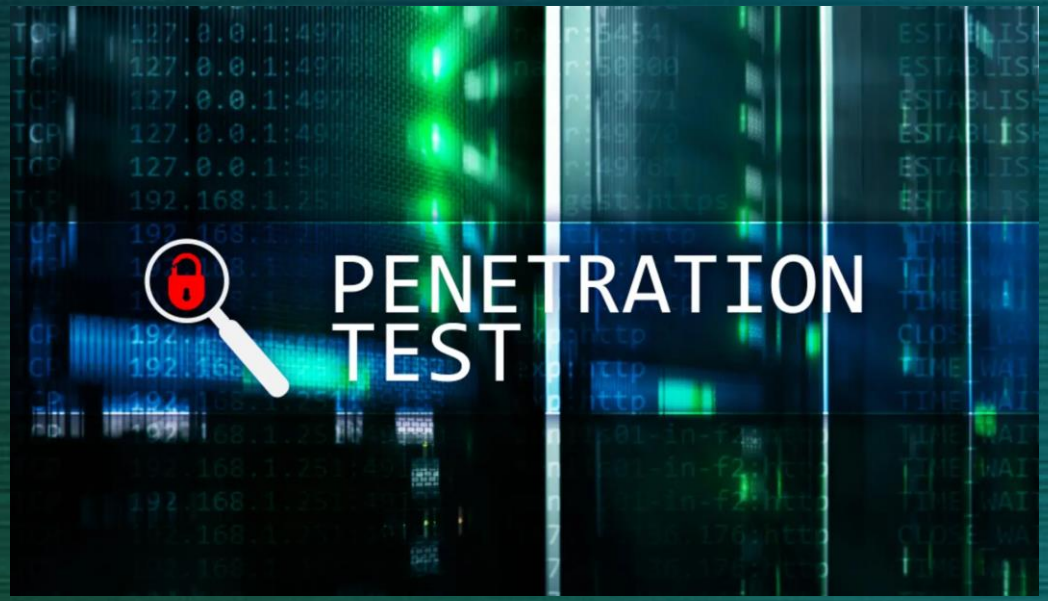
Méthodologies des tests d'intrusion



Méthodologies des tests d'intrusion

- Ils peuvent avoir une grande variété d'objectifs
- Aucun test d'intrusion n'est identique
- Pas de cas unique quant à la façon dont un pentester devrait l'aborder

Les mesures prises doivent être pertinentes pour la situation actuelle.



Etapes générales

Etapes	Description
1. Collecte d'informations	Collecter autant d'informations que possible sur une cible
2. Enumération	Découvrir des applications et services exécutés sur le système
3. Exploitation	Exploiter les vulnérabilités découvertes
4. Escalade de privilèges	Tenter d'étendre l'accès au système horizontalement et verticalement
5. Post-exploitation	1. Voir quels autres hébergeurs peuvent être ciblés (pivot) 2. Recueillir des informations supplémentaires après l'élévation de privilèges 3. Couvrir nos traces 4. Rapports

OSSTMM (le manuel de méthodologie de test de sécurité open-source)

Fournit un cadre détaillé de stratégies de test pour les systèmes, les logiciels, les applications, les communications et l'aspect humain de la cybersécurité

Il se concentre principalement sur la façon dont ces systèmes communiquent :

- Télécommunications
- Réseaux filaires
- Communications sans fil

Lien du manuel :
https://www.isecom.org/OSSTMM.3.pdf

Avantages

- Couvre en profondeurs diverses stratégies de test
- Comprend des stratégies de test pour des cibles spécifiques
- Flexible en fonction des besoins de l'organisation

Inconvénients

- Le manuel très détaillé est difficile à comprendre et a tendance à utiliser des définitions uniques

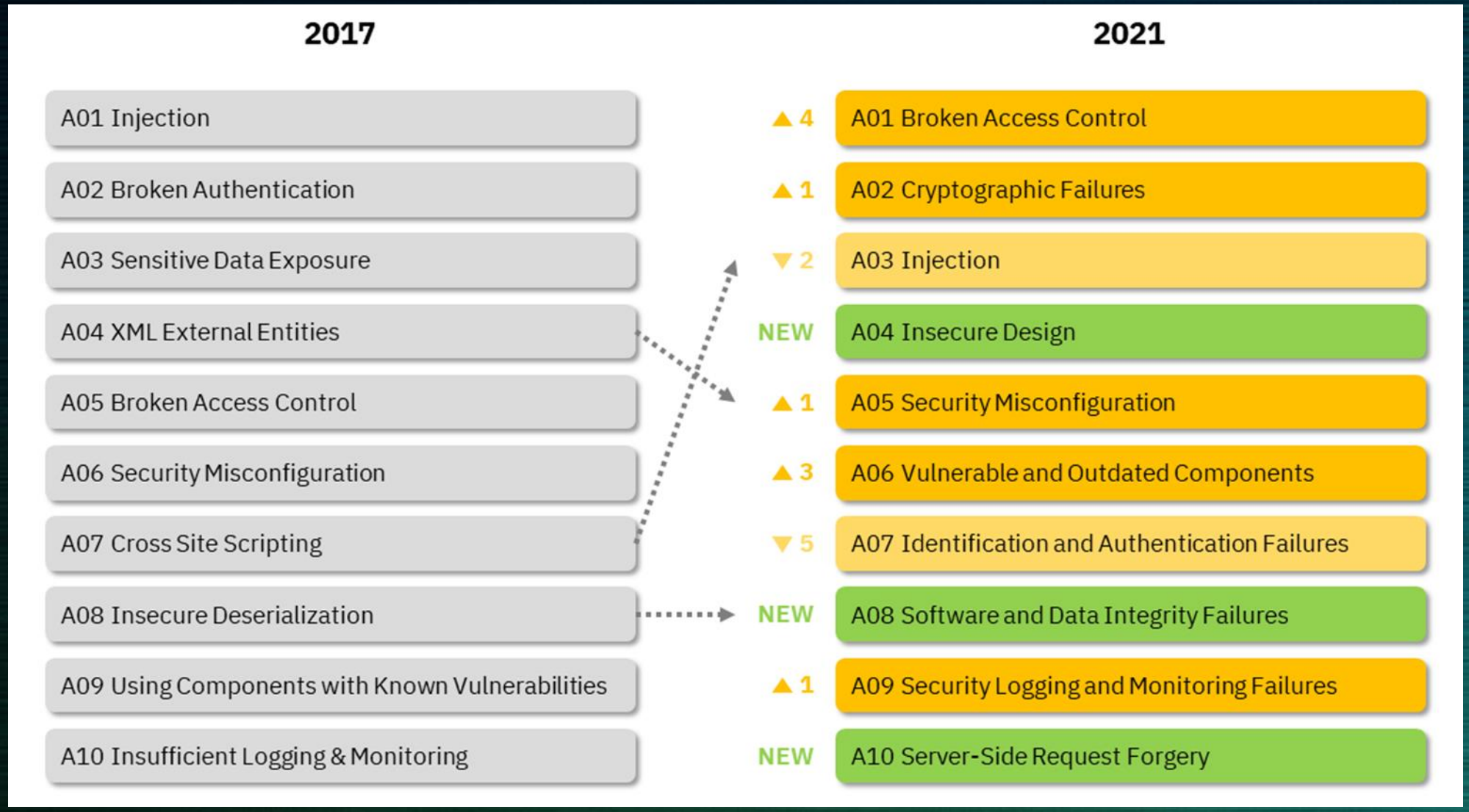
OWASP (Open Web Application Security Project)

ASBL dédiée à permettre aux organisations de développer, acheter et maintenir des applications et des API fiables.

Cette communauté publie régulièrement des rapports indiquant les 10 principales vulnérabilités qu'une application WEB peut avoir

Lien du site WEB officiel :
https://owasp.org/

OWASP (Open Web Application Security Project)



Black box, grey box et white box

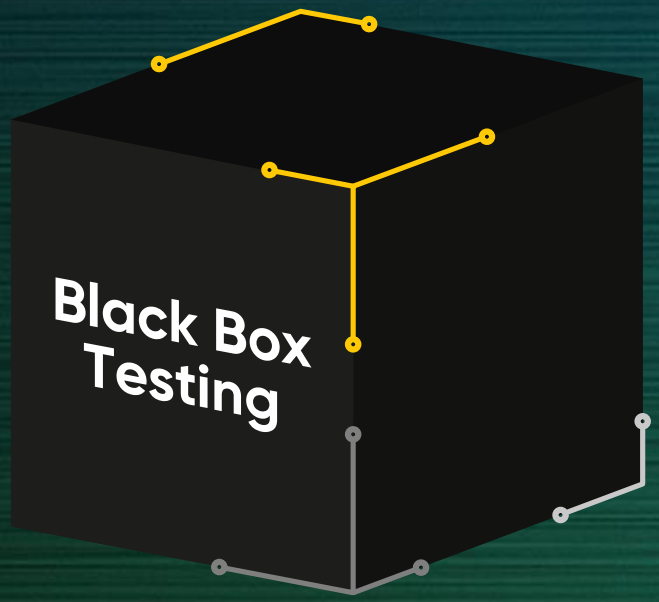
Trois approches sont possibles lors d'un audit de sécurité. Elles correspondent à différents niveaux d'information et d'accès fournis aux pentesters

Le choix de l'approche d'un test d'intrusion dépend des objectifs :

- Quel niveau de profondeur ?
- Tester l'attaque interne ou externe ?

Black box

- Audit de sécurité réalisé dans les conditions les plus proches d'une attaque externe
- Analyse du système sans connaitre son fonctionnement interne
- Les pentesters connaissent uniquement le nom de l'entreprise et souvent une IP ou une URL



White box

- Audit de sécurité où un maximum d'informations est transmis aux pentesters
- Les pentesters connaissent le fonctionnement de la cible
- Accès à des documents d'architecture, des accès admin à des serveurs, l'accès au code source,…
- Analyse de sécurité plus poussée qu'un test d'intrusion
- Permet de découvrir des vulnérabilités non visibles lors d'un pentest

Grey box

- Audit de sécurité réalisé en ayant quelques informations sur la cible
- Permet de réaliser des tests plus approfondis, en ayant une meilleure connaissance du contexte
- Périmètre d'attaque défini pour permettre de concentrer les tests sur des éléments déjà identifiés

En résumé…

- Black box : tests d'intrusion du point de vue d'un attaquant externe, niveau minimal d'informations mises à disposition des pentesters

- Grey box : tests du point de vue d'un utilisateur standard, niveau intermédiaire d'informations partagées aux pentesters

- White box : tests sécurité du point de vue d'un administrateur, niveau maximal d'informations transmises

Merci de m'avoir écouté !

PEN TESTER

CORE SECURITY
A HelpSystems Company

What my friends think I do

What my mom thinks I do

What society thinks I do

What hackers think I do

What I think I do

What I actually do