

# Les 5 phases d'un test d'intrusion



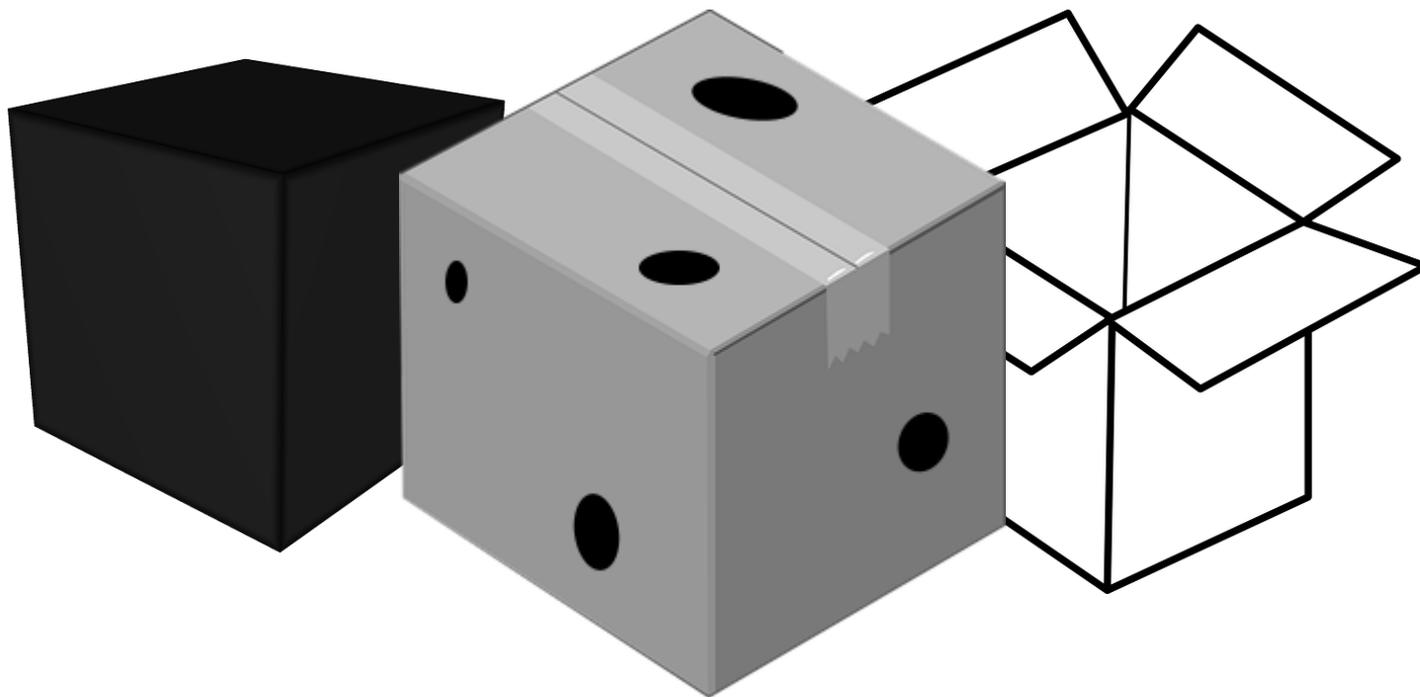


## Pourquoi faire un **test d'intrusion**

- ◉ Tester les **identifiants**
- ◉ Tester un **nouveau service**
- ◉ Tester le **personnel**
- ◉ Sécuriser son système / Vérifier la conformité à une norme
- ◉ Différents **types** : application web, réseau, mobile...etc

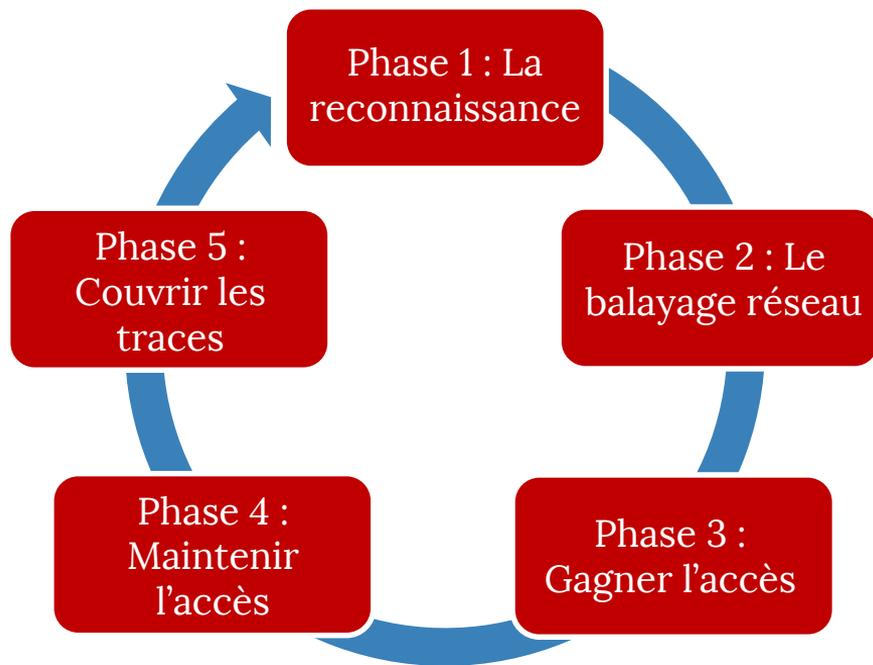


## Les 3 types de **tests d'intrusion**





## Les 5 Phases d'un test d'intrusion



1

# **Phase 1 : la reconnaissance**



## Phase 1 – **La reconnaissance**

- ⦿ Active ou passive
- ⦿ Récupérer des informations **avant de passer à l'attaque**
- ⦿ Étape la plus facile, mais la plus longue

2

## **Phase 2 : le balayage réseau**



## Phase 2 – **Le balayage réseau**

- ⦿ Récupérer des **détails précis** sur les systèmes
- ⦿ Ports ouverts
- ⦿ Vulnérabilité(s) présente(s)

3

## **Phase 3 : Gagner l'accès**



## Phase 3 – Gagner l'accès

- ⦿ On accède au système
- ⦿ Faiblesse(s) exploitée(s)

4

## **Phase 4 : Maintenir l'accès**



## Phase 4 – **Maintenir l'accès**

- ⦿ On se facilite un accès futur
- ⦿ Le cas des **backdoors**

5

## **Phase 5 : Couvrir les traces**



## Phase 5 – **Couvrir les traces**

- ◉ Destruction des preuves
- ◉ Suppression des fichiers **logs**