Checklist pour un test d'intrusion

Table des matières

[Pré-test 3](#_Toc155694097)

[Test 3](#_Toc155694098)

[Post-test 3](#_Toc155694099)

[Détails de chaque étape 4](#_Toc155694100)

[Pré-test 4](#_Toc155694101)

[Test 4](#_Toc155694102)

[Post-test 5](#_Toc155694103)

[Conclusion 5](#_Toc155694104)

# Pré-test

* Réunion de lancement avec le client
  + Définition des objectifs du test
  + Identification des actifs à tester
  + Détermination du périmètre du test
  + Fixation des dates et des horaires du test
* Collecte d'informations sur les actifs à tester
  + Architecture du système d'information
  + Politiques et procédures de sécurité
  + Logiciels et applications utilisés
  + Vulnérabilités connues
* Préparation de l'environnement de test
  + Installation des outils et des logiciels nécessaires
  + Mise en place d'un environnement de test sécurisé

# Test

* Reconnaissance
  + Identification des points d'entrée potentiels
  + Recherche de vulnérabilités
* Exploitation
  + Attaque des vulnérabilités identifiées
  + Exploitation des failles de sécurité
* Post-exploitation
  + Maintien de l'accès obtenu
  + Collecte d'informations sensibles

# Post-test

* Rapport de test
  + Liste des vulnérabilités identifiées
  + Niveau de risque associé
  + Plan d'actions correctives
* Recommandations
  + Mise en œuvre de mesures de sécurité correctives
  + Formation des utilisateurs aux bonnes pratiques de sécurité

# Détails de chaque étape

## Pré-test

* Réunion de lancement avec le client
  + Cette réunion est essentielle pour définir les objectifs du test, identifier les actifs à tester, déterminer le périmètre du test, fixer les dates et les horaires du test.
  + Il est important de bien comprendre les besoins du client et de s'assurer que les objectifs du test sont alignés avec les objectifs de sécurité du client.
* Collecte d'informations sur les actifs à tester
  + Cette étape permet de collecter des informations sur les actifs à tester, telles que l'architecture du système d'information, les politiques et procédures de sécurité, les logiciels et applications utilisés, les vulnérabilités connues.
  + Ces informations sont essentielles pour la phase de reconnaissance, qui permet d'identifier les points d'entrée potentiels et les vulnérabilités connues.
* Préparation de l'environnement de test
  + Cette étape permet de préparer l'environnement de test, en installant les outils et les logiciels nécessaires, et en mettant en place un environnement de test sécurisé.
  + Il est important de s'assurer que l'environnement de test est isolé du système d'information réel, afin d'éviter toute contamination.

## Test

* Reconnaissance
  + Cette étape consiste à identifier les points d'entrée potentiels et les vulnérabilités connues.
  + Les techniques de reconnaissance peuvent inclure le scan des ports, le balayage des vulnérabilités, l'analyse des logs, etc.
* Exploitation
  + Cette étape consiste à exploiter les vulnérabilités identifiées.
  + Les techniques d'exploitation peuvent inclure des attaques par force brute, des attaques par injection SQL, des attaques par déni de service, etc.
* Post-exploitation
  + Cette étape consiste à maintenir l'accès obtenu et à collecter des informations sensibles.
  + Les techniques de post-exploitation peuvent inclure l'installation de logiciels malveillants, le vol de données, la modification de données, etc.

## Post-test

* Rapport de test
  + Le rapport de test doit contenir une liste des vulnérabilités identifiées, le niveau de risque associé, et un plan d'actions correctives.
  + Le rapport de test doit être clair et concis, et il doit être adapté aux besoins du client.
* Recommandations
  + En plus du rapport de test, il est important de fournir des recommandations pour mettre en œuvre des mesures de sécurité correctives.
  + Ces recommandations doivent être adaptées aux besoins et aux objectifs du client.

# Conclusion

Cette checklist est un guide général pour mener à bien un test d'intrusion. Il est important de l'adapter aux besoins spécifiques du client et du périmètre du test.