



Test d'Intrusion



Plan

- Préparation d'un test d'intrusion
- Différents types d'audit
- Déroulement d'un audit
- Rapport de test

Préparation d'un test d'intrusion





Différents types d'audit

Informations disponibles :

- Boîte noire : aucune information
- Boîte grise : avec des comptes utilisateurs / documentation
- Boîte blanche : accès au code source

Méthode:

- Audit de configuration
- Audit d'architecture
- Test d'intrusion
 - Interne
 - Externe
- Audit de code



Cadrer le pentest

- Définir le périmètre de l'audit
 - Application web
 - Réseau Interne
- Demander les technologies utilisées
 - Réviser avant l'audit
 - Étudier la faisabilité
- Estimer la charge
 - En fonction du nombre de machines, et de la complexité
 - Test d'intrusion web : 4-5 jours
 - Réseau interne : ~ 10 jours



Prérequis

- Toujours essayer de faire les tests en environnement de **pré-production**
 - Minimiser le risque de perte de données / disponibilité
- Comptes de test sur l'application
 - comptes admin (test élévation privilèges)
 - comptes de test (contrôle d'accès horizontal)
- (Sauvegarde des données)
- Demander la documentation
 - ex: dossier d'architecture



Lettre d'autorisation de tests

Se protéger légalement :

- Lister les IPs concernées
- Liste des tests autorisés
- Accord du propriétaire
- Accord de l'hébergeur

Déroulement d'un audit





Réunion de lancement de l'audit

- S'assurer que tout le monde est à la page
- Vérification des prérequis
- Optionnelle



Pendant l'audit

- On peut prévoir des points réguliers avec le client
- Tenir au courant des découvertes (notamment vuln critique)
- Demander la permission avant une action pouvant avoir des effets de bord
- Contacter en cas de blocage, pré-requis non fournis.



Restitution

- Clot l'audit
- Présente les résultats
- Échange et réponse aux question
 - du commanditaire
 - des équipes techniques

Le but d'un audit est d'évaluer la
sécurité d'un système, pas d'obtenir
un shell.





Rapport d'audit

- Liste les vulnérabilités découvertes, et indique une remédiation
- “Executive Summary” au début, pour résumer les vulnérabilités
- Ni trop court, ni trop long
- Utiliser des captures d'écran
- Souvent accompagner d'un Excel qui reprend les vulnérabilités




Rapport d'audit

<https://www.offensive-security.com/pwk-online/PWK-Example-Report-v1.pdf>

<https://github.com/juliocesarfort/public-pentesting-reports/>

- Randori Sec
- Cure 53



Test d'intrusion Web



Réalisation des tests

Tests d'infrastructure :

1. Scan de port
2. Scanner de vulnérabilités
3. Vérification des version, recherche de vulnérabilités
4. Test d'exploit si applicable
5. Recherche d'erreur de configuration

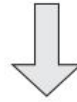
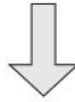
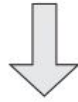
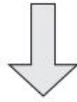
Web :

6. Énumération du contenu
7. Scan de vulnérabilités
8. Test approfondi des fonctionnalités web

Recon and analysis

1. Map application content

2. Analyze the application



Application logic

3. Test client-side controls

9. Test for logic flaws

Access handling

4. Test authentication

5. Test session management

6. Test access controls

Input handling

7. Fuzz all parameters

8. Test for issues with specific functionality

Application hosting

10. Test for shared hosting issues

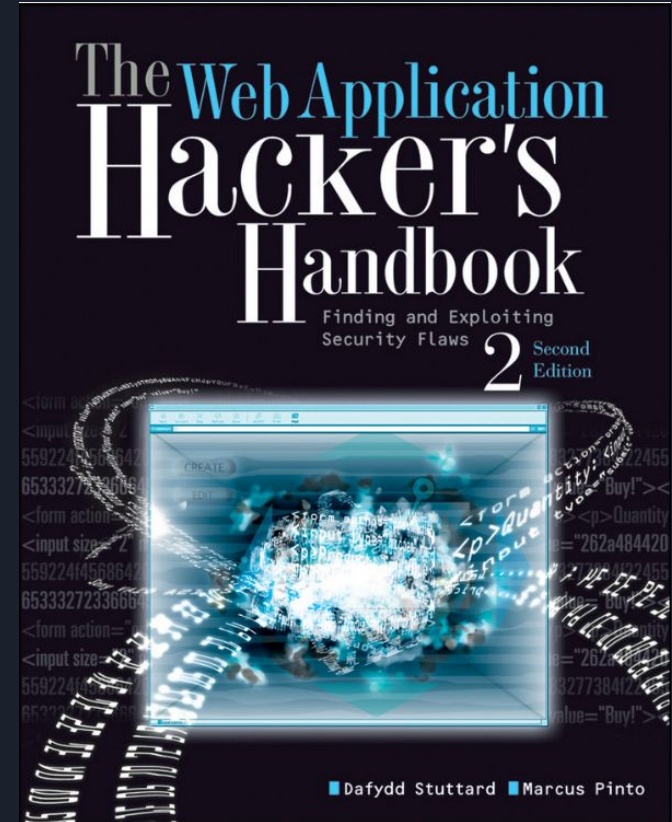
11. Test the web server

12. Miscellaneous Checks

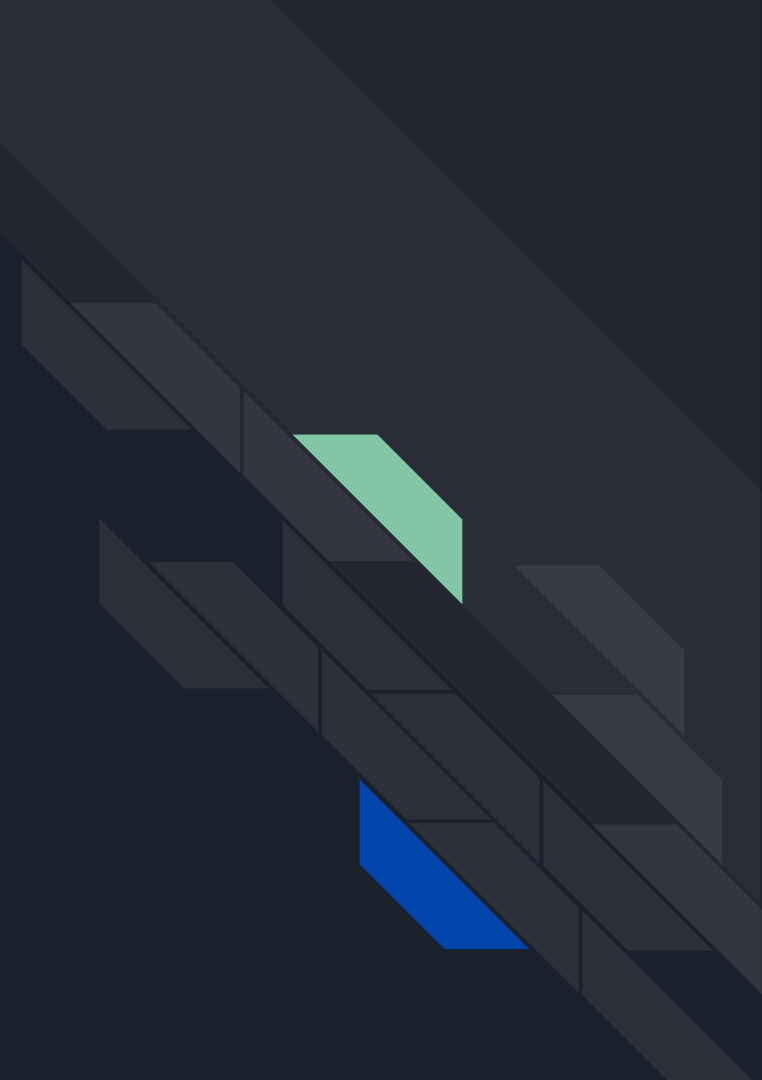
13. Information Leakage

Méthodologies

- Web Application Hacker Handbook
- OWASP Testing Guide
- Penest : tests en temps contraints
- différent de conformité à une liste d'exigences



Test d'intrusion Interne

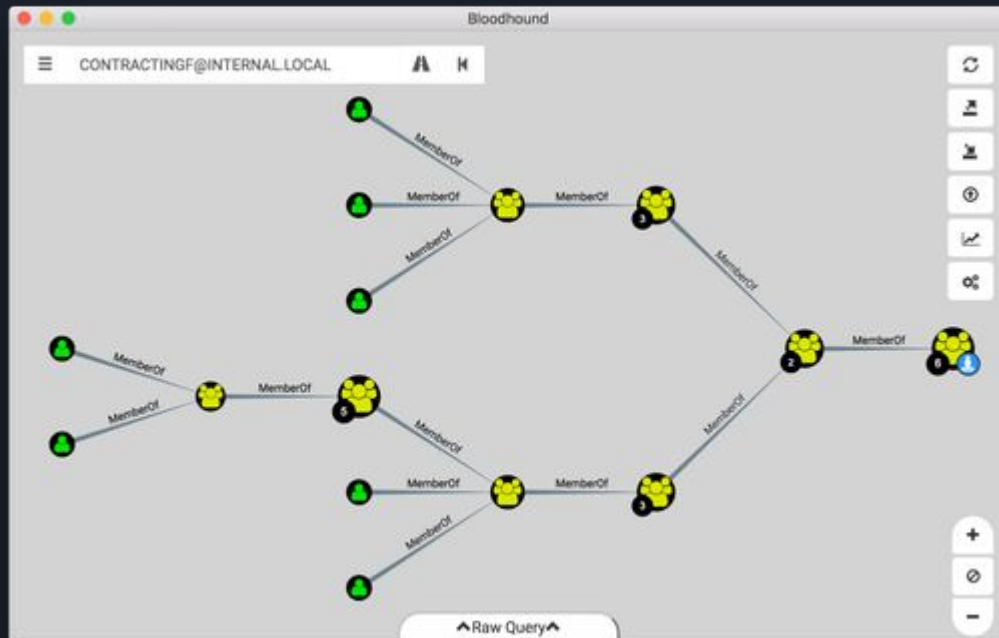




Test d'intrusion Interne

- Scan du réseau interne
- Scan de vulnérabilités (Nessus ou OpenVAS)
- Exploiter les vulnérabilités Critiques
- Utilisation de Bloodhound pour trouver un chemin d'accès
- Erreurs de configuration d'AD
- Réutilisation de mot de passe
- Si possible devenir administrateur de domaine

BloodHound



Audit de configuration





Audit de configuration

Comparer la configuration avec un référentiel

- Guide de l'ANSSI
- Guides du CIS

Audit de code





Audit de code

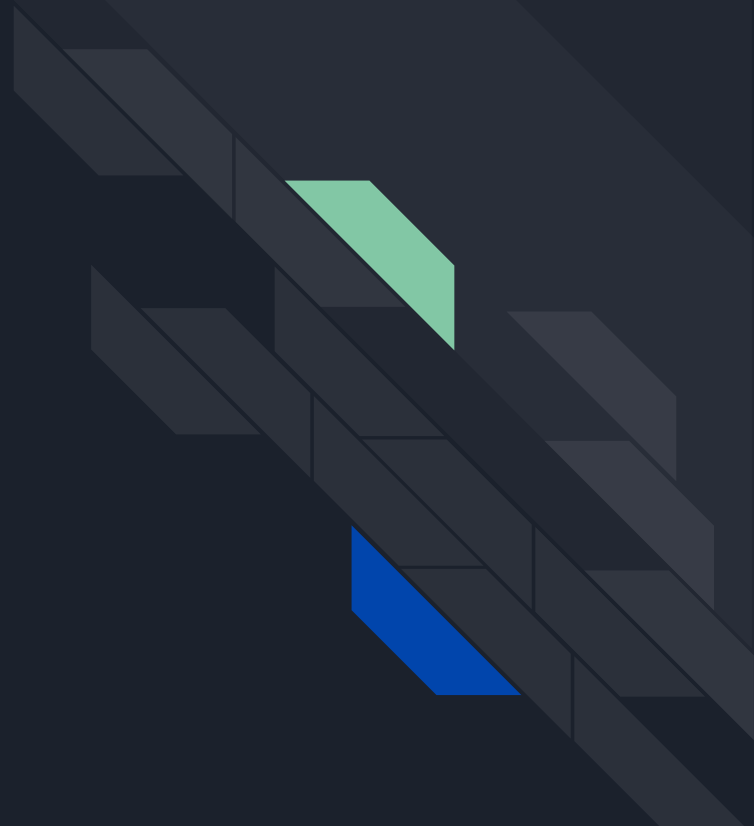
Méthodologie assez spécifique :

<https://www.pentesterlab.com/exercises/codereview/course>

Idéalement va combiner :

- Des scans automatiques
- Analyse des entrées utilisateur
- Vérification de la logique
- Du fuzzing

Ressources pour
progresser





Ressources

Test d'intrusion, exploitation de vulnérabilités :

- [Hackthebox](#)
- [Pentesterlab](#)

Sécurité Web :

- [PortSwigger Web Security](#)
- [The Web Application Hacker Handbook](#)

Autres :

- [Live Overflow](#)
- [CTFs & Internet](#)