ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR

Membre de HONORIS UNITED UNIVERSITIES

Sécurité des systèmes d'information

Zineb MACHROUH

2024/2025

Chapitres

1. Introduction
2. Vulnérabilités des systèmes
3. Fonctions de la sécurité
4. Mécanismes de sécurité
5. Normes de gestion de la cybersécurité
6. Techniques de cybersécurité avancées

Chapitre 6: Techniques de cybersécurité avancées

Introduction Aux Tests De Pénétration

Les tests de pénétration (Pentesting) simulent des attaques réelles pour évaluer la sécurité des systèmes d'information, il visent à identifier et exploiter les vulnérabilités d'un système ou d'une application pour vérifier la robustesse de la sécurité et trouver les failles avant que les attaquants ne puissent les exploiter.

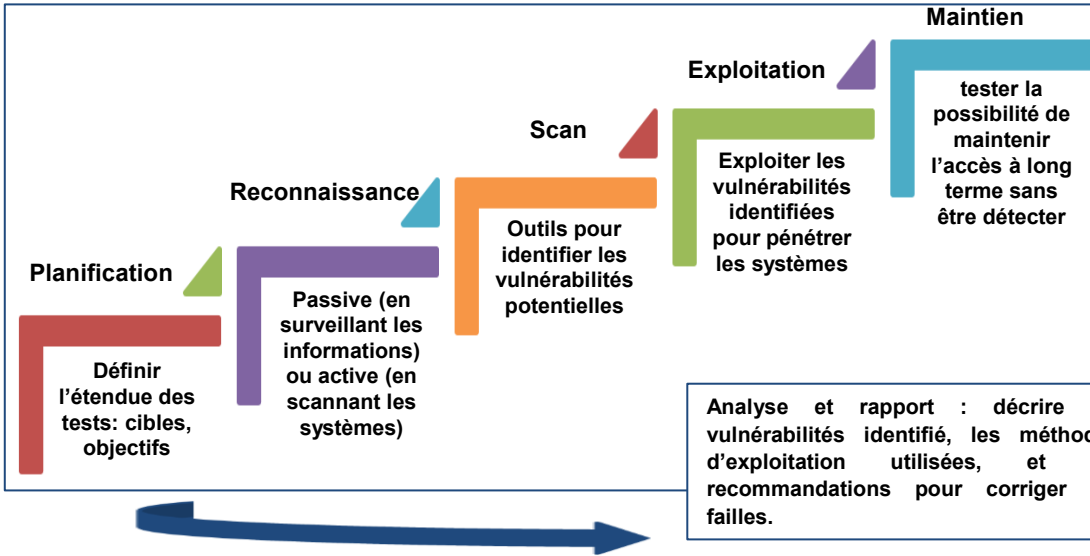
Objectifs des tests de pénétration

- Identifier les vulnérabilités
- Évaluer l'impact des vulnérabilités
- Renforcer la sécurité
- Respecter la conformité

Types de tests de pénétration

- **Tests internes :** il faut avoir un accès au réseau interne, ce qui permet de simuler des attaques venant de l'intérieur.
- **Tests externes :** L'attaquant est supposé être externe, sans accès préalable à l'infrastructure de l'organisation. Ce type de test se concentre souvent sur les services accessibles depuis Internet.
- **Tests d'applications web :** tester les applications web pour détecter des failles comme les injections SQL, les failles XSS, XSRF, ou les problèmes de gestion des sessions.
- **Tests d'ingénierie sociale :** utiliser des techniques comme le phishing contre les employés pour obtenir les informations sensibles ou les informations d'authentification.

Phases d'un test de pénétration



Analyse et rapport : décrire les vulnérabilités identifié, les méthodes d'exploitation utilisées, et les recommandations pour corriger les failles.

Outils courants utilisés pour les tests de pénétration

- **Kali Linux :** Une distribution Linux spécialisée qui regroupe une multitude d'outils de pentesting.
- **Nmap :** Un outil de scan de réseau utilisé pour découvrir les services et les machines sur un réseau.
- **OpenVAS :** **U**n logiciel composé de plusieurs services et outils pour l'analyse et la gestion des vulnérabilités.
- **Metasploit :** Un framework d'exploitation de vulnérabilités permettant de tester les failles de sécurité.
- **Burp Suite :** Un ensemble d'outils pour tester la sécurité des applications web.
- **Wireshark :** Un analyseur de paquets qui permet d'observer le trafic réseau.



Les normes et cadres des tests de pénétration

Les tests de pénétration sont souvent réalisés pour répondre à des exigences spécifiques en matière de sécurité. Parmi les normes utilisés dans le domaine du pentesting :

OWASP	Une liste des 10 vulnérabilités les plus critiques pour les applications web
PCI-DSS	Une norme de sécurité pour les entreprises traitant des cartes de paiement.
ISO 27001	Une norme qui spécifie les exigences pour SMSI
NIST SP 800-115	Un guide de test de pénétration

Exercice

1. Quel est l'objectif principal des tests de pénétration ?
A) Créer des vulnérabilités logicielles.
B) Identifier et exploiter les faiblesses de sécurité.
C) Développer de nouveaux protocoles de sécurité.
D) Former les employés à la sensibilisation à la sécurité.

2. À quoi sert l'ingénierie sociale dans le contexte des tests de pénétration ?
A) Tester la sécurité physique d'un bâtiment.
B) Manipuler des individus pour obtenir des informations confidentielles.
C) Analyser le trafic réseau pour détecter les vulnérabilités.
D) Écrire du code pour exploiter les vulnérabilités logicielles.

3. Lequel des outils suivants est couramment utilisé pour les tests de pénétration réseau ?
A) Unix.
B) Nmap.
C) GNS3.
D) Access.

Exercice

4. Quel est le but d'une analyse de vulnérabilité dans les tests de pénétration ?
A) Exploiter les vulnérabilités.
B) Identifier les faiblesses potentielles de sécurité.
C) Créer un rapport pour la direction.
D) Former le personnel aux protocoles de sécurité.

5. Quelle phase des tests de pénétration implique la collecte d'informations sur la cible ?
A) Exploitation.
B) Rapports.
C) Analyse.
D) Reconnaissance.

6. Qu'est-ce qu'une vulnérabilité zero-day ?
A) Une vulnérabilité qui a été divulguée publiquement.
B) Une vulnérabilité qui est connue mais pas encore corrigée.
C) Une vulnérabilité qui est exploitée le jour même de sa découverte.
D) Une vulnérabilité qui est corrigée avant de pouvoir être exploitée.

Exercice

7. Lequel des éléments suivants est un cadre commun utilisé pour les tests de pénétration ?
A) OWASP.
B) ISO 27001.
C) ITIL.
D) COBIT.

8. Quelle est la différence entre un test de pénétration white box et un test black box ?
A) Les tests white box n'ont aucune connaissance du système, contrairement aux black box.
B) Les tests white box ont une connaissance complète du système, contrairement aux black box.
C) Les tests white box sont externes, alors que les tests black box sont internes.
D) Il n'y a aucune différence.

9. Quel est le résultat final d'un test de pénétration ?
A) Une liste de tous les mots de passe.
B) Un rapport détaillé des résultats et des recommandations.
C) Une présentation à l'équipe informatique.
D) Un correctif logiciel.

Réponses

1 -- B) Identifier et exploiter les faiblesses de sécurité
2 -- B) Manipuler des individus pour obtenir des informations confidentielles
3 -- B) Nmap
4 -- B) Identifier les faiblesses potentielles de sécurité
5 -- D) Reconnaissance
6 -- C) Une vulnérabilité qui est exploitée le jour même de sa découverte
7 -- A) OWASP et ISO27001
8 -- B) Les tests white box ont une connaissance complète du système, contrairement aux black box
9 --B) Un rapport détaillé des résultats et des recommandations