Université Ibn Zohr
Faculté des Sciences d'Agadir
Département d'Informatique

Filière SMI6
Module : Sécurité des réseaux informatiques
Année Universitaire 2022/2023

Atelier 3: Test de pénétration

Objectif :

L'objectif de cet atelier est d'apprendre à tester la sécurité d'un système d'information contre les stratégies d'attaques courantes.

Remarque :

Il est important de noter que l'utilisation de ces outils de test sans autorisation est illégale et peut entraîner des conséquences graves. Il est fortement recommandé d'utiliser ces outils uniquement à des fins éducatives et de test dans un environnement contrôlé.

Afin d'améliorer le niveau de sécurité, une société a décidé de réaliser un test de pénétration pour son système d'information, afin de se prémunir contre les stratégies d'attaques courantes selon le cahier de charge suivant :

a. Tester la sécurité des systèmes d'exploitation et des routeurs contre les attaques par mots de passe,
b. Tester la sécurité de l'ensemble du système contre les attaques de type "homme du milieu".
c. Tester le niveau de sécurité du site web de la société.

1. Citez les fameuses stratégies d'attaques qui peuvent menacer:
   - ✓ Les systèmes d'exploitation
   - ✓ Les routeurs
   - ✓ Les sites web

2. Donner quelques outils de test de pénétration qui peuvent être utilisés pour répondre aux exigences du cahier des charges ci-dessus ?

Si l'on considère que la société utilise deux systèmes d'exploitation, Linux et Windows, et que vous souhaitez effectuer un test de pénétration préparatoire sur un laboratoire virtuel sur votre machine.

a. Tester la solidité des mots de passe des systèmes d'exploitation utilisés supposons que les hachages sont :
   - ✓ Unix : « 2DC69A0B846B3ABC779AD5AA4728AC120A7C056A »
   - ✓ Windows : « 445CD2FD3273962BDF09425109A2D09F7170E837 »

b. Tester la sécurité du réseau virtuel contre les stratégies d'attaques suivantes :
   - ✓ **Ping of death**
   - ✓ **Attaque par dictionnaire**
   - ✓ **ARP poisoning**
   - ✓ **Déni de service (Dos)**