6 bis. Tests de durcissement et analyse de la sécurité SSH

6.1 Objectif des tests

L'objectif était d'évaluer l'impact réel des paramètres de sécurité SSH sur la résistance du serveur face aux attaques par force brute, en particulier celles menées à l'aide d'outils automatisés.

Les tests ont été réalisés dans un laboratoire personnel, sur un serveur volontairement exposé à des tentatives de connexion contrôlées.

6.2 Méthodologie adoptée

Configuration d'un serveur SSH durci :

Accès root désactivé

Utilisateurs autorisés explicitement définis

Nombre maximal de tentatives limité

Nombre maximal de sessions limité

Pare-feu actif

Fail2Ban activé

Mise en place d'un compte utilisateur avec :

Mot de passe volontairement faible

Permissions limitées

Lancement d'attaques par force brute depuis une machine Kali Linux à l'aide de Hydra.

6.3 Approche expérimentale

Afin de comprendre précisément à quel niveau de configuration les attaques deviennent efficaces :

Le durcissement SSH a été progressivement allégé

Certains paramètres ont été modifiés un par un :

Nombre d'essais autorisés

Méthode d'authentification

Règles Fail2Ban

Les effets ont été observés à chaque étape

6.4 Résultats observés

Avec une configuration stricte, Hydra n’a pas réussi à identifier le mot de passe

Les tentatives ont été bloquées automatiquement

Les adresses IP ont été bannies par Fail2Ban

Après affaiblissement progressif de la configuration, l’attaque est devenue efficace

6.5 Conclusion sécurité

Ces tests ont permis de démontrer que :

La sécurité SSH repose avant tout sur une bonne configuration

La réduction des privilèges est essentielle

Les mots de passe faibles restent une vulnérabilité majeure

Les outils d’attaque ne sont efficaces que lorsque la configuration est négligée

Une défense efficace combine :

configuration stricte

pare-feu

mécanismes de détection et de blocage