

## Rapport de tests de pénétration

### Objectif du test de pénétration

Le but de ce test de pénétration était de vérifier la sécurité du réseau cible (192.168.1.1) en exécutant des tests de pénétration.

### Objectifs non atteints

L'exécution des commandes suivantes n'a pas réussi à fournir les résultats attendus :

1. `nmap -T4 -O -p- report.xml` : Aucun hôte n'a été sélectionné pour l'énumération.
2. `nmap -T4 -O -p80,443,8080,3306,22 report.xml` : Le fichier XML n'a pas été résolu par nmap, ce qui a entraîné une erreur.
3. `nmap -T4 -O -p80,443,8080,3306,22 report.xml` : Le résultat de l'analyse a indiqué que nmap n'a pas pu générer de résultats.

### Résultats obtenus

Après l'exécution de la commande `nmap -T4 -O -p`, des résultats ont été obtenus pour les ports 80, 443, 8080 et 3306.

### Analyses et recommandations

1. Port 80 (HTTP) : Ouvert : Le port 80 est ouvert, ce qui signifie qu'il est possible de tester des requêtes HTTP.
2. Port 443 (HTTPS) : Ouvert : Le port 443 est ouvert, ce qui signifie qu'il est possible de tester des requêtes HTTPS.
3. Port 8080 : Ouvert : Le port 8080 est ouvert, ce qui signifie qu'il est possible de tester des requêtes HTTP.
4. Port 3306 (MySQL) : Fermé : Le port 3306 est fermé, ce qui signifie qu'il n'est pas possible d'envisager d'attaquer MySQL.

### Conclusion

Ce test de pénétration a révélé que le système cible offre des points d'entrée pour les attaques en provenance de l'extérieur.