

SUPNUM

RSS

TP 1

Énumération Réseau et Audit Web

Sécurité des Réseaux et Systèmes

Mohamed Said M'Bareck
21-11-2025

Objectifs du Travaux Pratiques

Ce TP vise à vous familiariser avec les outils fondamentaux de reconnaissance et d'énumération dans un contexte de test d'intrusion. Vous apprendrez à utiliser Nmap pour la découverte de services, CM-Seek pour l'identification de CMS, Fuzzing pour la recherche de contenu caché, et WPScan pour l'audit de sites WordPress.

Contexte et Préparation

Ce laboratoire est conçu pour être effectué dans un environnement sécurisé via un Réseau Privé Virtuel (VPN). Tous les exercices doivent être réalisés après connexion au réseau 192.168.9.0/24 via Wireguard.

Test de Connexion VPN

Vous devez utiliser le même fichier de configuration Wireguard (/etc/wireguard/wg0.conf) partagé lors des séances de TD. Avant de commencer, vérifiez que vous êtes connecté au réseau VPN en exécutant les commandes suivantes :

```
sudo wg-quick down wg0 && wg-quick up wg0
ifconfig wg0
ping -c 5 192.168.9.1
ping -c 5 app1.rss.lab
```

Listing 1 – Vérification de la connexion Wireguard

Instructions de Rapport

Rapport à Soumettre

Vous devrez soumettre un rapport PDF à la fin du TP contenant vos travaux. Ce rapport DOIT inclure :

- Des captures d'écran de **toutes les commandes exécutées** pour chaque étape.
- Les **résultats complets** (si applicable) de chaque commande.
- Les **réponses claires et concises** à toutes les questions posées dans les exercices.
- Les fichiers de sortie ('outputs'), s'ils sont applicables (ex : **ips.txt**, fichiers Nmap), doivent être joints au rapport ou déposés sur la plateforme d'apprentissage (**Classroom**).

Tâches à Réaliser

1. Découverte des Hôtes et Services avec Nmap

Cet exercice vise à maîtriser les techniques de scan de réseau pour la découverte d'hôtes, de ports et de versions de services.

1. **Découverte d'Hôtes** : Identifier les hôtes actifs sur le réseau 192.168.9.0/24 **sans effectuer de scan de ports** et enregistrer les résultats dans un fichier de format **grepable**.

2. **Liste d'IPs** : Créez un fichier `ips.txt` contenant uniquement les adresses IP trouvées.
 3. **Scan de Ports** : Identifier les ports ouverts sur les hôtes listés dans `ips.txt`, en excluant le Gateway (192.168.9.1). Quel est l'hôte actif ayant le plus de ports ouverts ?
 4. **Identification de Services** : Identifiez les services et leur version pour les ports ouverts sur l'hôte ayant le plus de ports ouverts (en utilisant l'option `-sV`) et enregistrer les résultats dans un fichier de format **normal**.
 5. **Détection d'OS** : Déterminez le système d'exploitation d'un hôte actif (un hôte actif de votre choix).
 6. **Scripts NSE par Défaut** : Identifiez les services et exécutez les scripts NSE par défaut (`-sC`) pour détecter les vulnérabilités sur l'hôte 10.10.7.20.
 7. **Scan Agressif et Formats de Sortie** : Effectuer un scan Agressif (`-A`) sur 10.10.7.20 ou 10.10.7.22 en générant des fichiers de sortie dans différents formats (normal, XML, grepable).
 8. **Scan Silencieux** : Scannez les ports web sur 192.168.9.4 ou 192.168.9.6 sans déclencher d'alertes (pensez aux scans furtifs ou à faible intensité).
-

2. Détection des Systèmes de Gestion de Contenu avec CMSeek

Cet exercice utilise un outil spécialisé pour identifier les technologies web (CMS) utilisées.

1. **Nedevinez pas les options** : Identifier les options de CMSeek
 2. **Scan Rapide de CMS** : Effectuez un scan rapide pour identifier le CMS utilisé par le site web `http://app1.rss.lab`.
 3. **Sous-domaines** : Identifier les sous-domaines du `rss.lab` et enregistrer les sous-domaines trouvés dans un fichier `xxxxx.txt` (où `xxxxx` est votre matricule).
 4. **CMS sur Sous-domaines** : Identifier les CMS utilisés sur chacun des sous-domaines listés.
 5. **Scan Automatique** : Effectuer des scans automatiques sur la même liste de sites web sans interaction manuelle (recherchez l'option adéquate dans CMSeek).
 6. **Sauvegarde Spécifique** : Effectuer le même scan et consultez les résultats du scan dans le répertoire spécifique.
 7. **User Agent Aléatoire** : Effectuer un scan sur `app1.rss.lab` en utilisant un agent utilisateur aléatoire.
-

3. Fuzzing pour découvrir des fichiers et répertoires cachés

Utilisation de l'outil de fuzzing pour trouver des ressources non indexées sur un serveur web.

1. **Téléchargement de Wordlist** : Télécharger la liste de mots du laboratoire de fuzzing :

```
wget http://fuz.rss.lab/wordlist.txt -O wordlist.txt
```

2. **Découverte de Répertoires/Fichiers** : Identifier les répertoires/fichiers cachés sur `http://fuz.rss.lab` en utilisant l'outil de fuzzing de votre choix (ex : `gobuster`, `ffuf`, `dirb`, `wfuzz`). inspectez les résultats dans navigateur.
3. **Recherche de Format Spécifique (.txt)** : Identifier les fichiers cachés de format `.txt`.
4. **Recherche de Format Spécifique (.bak)** : Identifier les fichiers cachés de format `.bak`.
5. **Recherche de Format Spécifique (.html)** : Identifier les fichiers cachés de format `.html`.
6. **Question** : C'est quoi le résultats trouvés le plus pertinente ? Quelle serait la prochaine étape logique de votre audit ?
7. **Scan Avancé et Sortie HTML** : Effectuer un scan avec **70 threads** sur tous les extensions précédentes et afficher uniquement les statuts HTTP **200** et **500**. Enregistrez le résultat dans un fichier de format **html**.
8. **Analyse des Résultats** : Ouvrir ce fichier dans un navigateur et comparer le résultat sous format html et le résultat dans la console.

4. Audit et Exploitation d'une Installation WordPress

Application des techniques d'audit web sur une plateforme CMS spécifique : WordPress, en utilisant `wpscan`.

1. **Scan Basique** : Utilisez `wpscan` pour rechercher les vulnérabilités sur `http://wp.rss.lab`.
2. **Scan Authentifié (API)** : Analysez avec un jeton API (`-api-token`). Vous devez obtenir un jeton gratuitement sur le site : <https://wpscan.com/register>.
3. **Exploitation** : Exploitez **au moins une** des vulnérabilités détectées (par exemple, une faille dans un plugin ou un thème). (*Note : Documentez les étapes de validation/exploitation dans votre rapport*).

Bon courage !