

Projet Reconnaissance Réseau - Semaine 2

Contexte du projet

Ce projet s'inscrit dans le cadre d'une semaine dédiée à la **reconnaissance réseau** dans un cursus en cybersécurité / réseaux.

L'objectif est d'apprendre à utiliser différents outils de scan et d'énumération pour analyser des systèmes cibles — ici une machine virtuelle vulnérable **Metasploitable** et une machine d'entreprise **Windows 10**.

Objectifs pédagogiques

- Maîtriser les techniques de reconnaissance réseau essentielles pour un audit de sécurité.
 - Apprendre à effectuer des scans TCP et UDP avancés avec **Nmap**.
 - Découvrir la détection du système d'exploitation distant grâce à Nmap.
 - Utiliser des outils complémentaires comme **enum4linux**, **WhatWeb** et **Nikto** pour approfondir la collecte d'informations.
 - Savoir organiser, documenter et rapporter ses résultats efficacement.
-

Outils utilisés

- **Nmap** : scanner réseau multifonction permettant la découverte d'hôtes, la détection de ports ouverts, versions de services et OS.
 - **enum4linux** : outil d'énumération SMB pour collecter informations utilisateurs, partages, etc.
 - **WhatWeb** : identification des technologies utilisées par les sites web cibles.
 - **Nikto** : scanner de vulnérabilités web.
-

Organisation des dossiers

Les résultats sont classés par outil dans des sous-dossiers, chacun contenant plusieurs sous-catégories :

VM_Metasploitable/

```
|— 01-NMAP/
| |— 01-brut/
| |  └─ README.md
| |— 02-rapports/
| |  └─ README.md
| |— 03-pdf/
| |  └─ README.md
| |— 04-Doc/
| |  └─ README.md
| |— 05-outils/
| |  └─ README.md
| └─ README.md
```

```
|— 02-enum4linux/  
|— 03-whatweb/  
|— 04-nikto/  
└— README.md
```

VM_Windows/

```
|— 01-NMAP/  
|— 02-enum4linux/  
|— 03-whatweb/  
|— 04-nikto/  
└— README.md
```

...

D'autres VM peuvent être ajoutées ici, en suivant cette même structure

D'autres VM peuvent être ajoutées ici, en suivant cette même structure

Livrable attendu

Un audit complet des machines **Metasploitable** et **Windows 10** réalisé avec les outils cités, comprenant :

- Les fichiers de sortie bruts.
- Des rapports clairs et détaillés au format Markdown.
- Des rapports PDF prêts à être remis.
- Une documentation expliquant les méthodes, commandes et observations.
- Les scripts et autres outils utilisés.