Cycle Ingénieur (BAC+4)

Module : Sécurité des Systèmes et Réseaux

# SÉCURITÉ OFFENSIVE ET DÉFENSIVE

## Séance 1 : Reconnaissance et Cartographie

*Red Team Methodology*

Cas d'étude : Nexus-Industry S.A.

Professeur : Lahcen AITIBOUREK

Createur : RACHID BOUSELAMA

# PARTIE I : Support de Cours Théorique

*Fondamentaux de la reconnaissance réseau et méthodologie d'attaque*

## 1. Introduction et Contexte

Dans le cadre du cas d'étude Nexus-Industry S.A., cette première séance se concentre sur la phase initiale de tout test d'intrusion : la reconnaissance. Cette étape constitue la fondation même de tout audit de sécurité sérieux. Sans une cartographie précise du réseau cible, il devient impossible d'identifier les vulnérabilités exploitables et de planifier une stratégie d'attaque efficace.

La reconnaissance représente la phase la plus critique d'un test d'intrusion. Une erreur à ce stade compromet l'ensemble de l'audit, car toutes les phases ultérieures dépendent de la qualité et de l'exhaustivité des informations collectées. La patience et la méthodologie sont donc essentielles pour mener à bien cette étape cruciale.

### 1.1 Cadre Juridique Marocain

Ce cours enseigne des techniques de sécurité offensive dans un but strictement pédagogique. Il est impératif de comprendre et respecter le cadre légal encadrant ces pratiques au Maroc :

| Article | Sanctions |
|---|---|
| Article 607-3 | Accès frauduleux : 1-3 mois de prison + 2.000-10.000 DH |
| Article 607-5 | Entrave volontaire : 1-3 ans de prison + 10.000-200.000 DH |

*Tableau 1 : Cadre juridique marocain des infractions informatiques*

**Engagement éthique :** En tant qu'étudiant, vous vous engagez à n'utiliser ces outils que sur l'environnement de laboratoire dédié (VMware Host-Only). Toute tentative d'attaque sur un réseau tiers sans autorisation écrite préalable constitue un délit pénal passible de sanctions sévères.

## 2. Méthodologie : La Kill Chain (Standard PTES)

Le standard PTES (Penetration Testing Execution Standard) définit une méthodologie structurée pour les tests d'intrusion. La phase de reconnaissance se divise en deux approches complémentaires, chacune offrant des avantages spécifiques selon le contexte de l'audit.

| Reconnaissance Passive (OSINT) | Reconnaissance Active |
|---|---|
| Collecte d'informations sans interaction directe avec la cible.<br>• Google Dorks<br>• LinkedIn et réseaux sociaux<br>• Whois et registres DNS | Interaction directe avec les paquets réseaux pour cartographier.<br>• Scan de ports<br>• Fingerprinting<br>• Énumération de services |
| ✓ Indétectable par la cible | ⚠ Détectable par IDS/IPS |

*Tableau 2 : Comparaison des approches de reconnaissance*

**Focus de cette séance :** Nous nous concentrons sur les phases 1 et 2 de la Kill Chain (Reconnaissance et Scanning) en utilisant des techniques actives avec Nmap. Ces compétences constituent le socle fondamental de tout pentester.

## 3. Scan de Ports : Fonctionnement TCP

Le scan de port permet de déterminer l'état d'un service sur une machine cible. Pour comprendre le fonctionnement des scans, il est essentiel de maîtriser d'abord le mécanisme d'établissement d'une connexion TCP normale, connu sous le nom de "Three-Way Handshake" (poignée de main en trois étapes).

### 3.1 Le Three-Way Handshake

Le Three-Way Handshake est le processus par lequel une connexion TCP fiable s'établit entre un client et un serveur. Ce mécanisme garantit que les deux parties sont prêtes à échanger des données avant le début de la communication effective.


*Figure 1 : Le Three-Way Handshake TCP*

**Les trois étapes du processus sont les suivantes :**

1. **SYN (Synchronize) :** Le client envoie un paquet SYN au serveur pour initier la connexion. Ce paquet contient un numéro de séquence initial qui sera utilisé pour le suivi de la communication.
2. **SYN-ACK (Synchronize-Acknowledge) :** Si le port est ouvert et le service disponible, le serveur répond par un paquet SYN-ACK, confirmant la réception de la demande et proposant son propre numéro de séquence.
3. **ACK (Acknowledge) :** Le client confirme avec un paquet ACK final. La connexion est alors établie et les données peuvent transiter dans les deux sens.

### 3.2 États des Ports

Lors d'un scan, chaque port peut présenter trois états distincts, chacun révélant des informations différentes sur la configuration de la cible :

| État | Description |
|---|---|
| **Ouvert (Open)** | Une application écoute activement sur ce port et accepte les connexions entrantes. C'est un point d'entrée potentiel. |
| **Fermé (Closed)** | Aucune application n'écoute sur ce port. Le système répond explicitement que le port est inaccessible. |
| **Filtré (Filtered)** | Un pare-feu bloque les requêtes. Aucune réponse n'est renvoyée, ce qui rend l'état du port incertain. |

*Tableau 3 : États possibles d'un port lors d'un scan*

***Analogie simple :*** *Imaginez frapper à une porte. Un port **ouvert** signifie que quelqu'un répond "Entrez !". Un port **fermé** indique qu'on vous dit "Partez, personne ici !". Un port **filtré** correspond à un silence total : personne ne répond, peut-être que la porte existe, peut-être pas.*

## 4. Le Scan SYN (Stealth Scan)

Le Scan SYN (option -sS) est le scan par défaut de Nmap lorsqu'il est exécuté avec les privilèges root. Il est à la fois plus rapide et plus discret qu'un scan TCP complet, ce qui en fait l'outil de choix pour les tests d'intrusion professionnels.

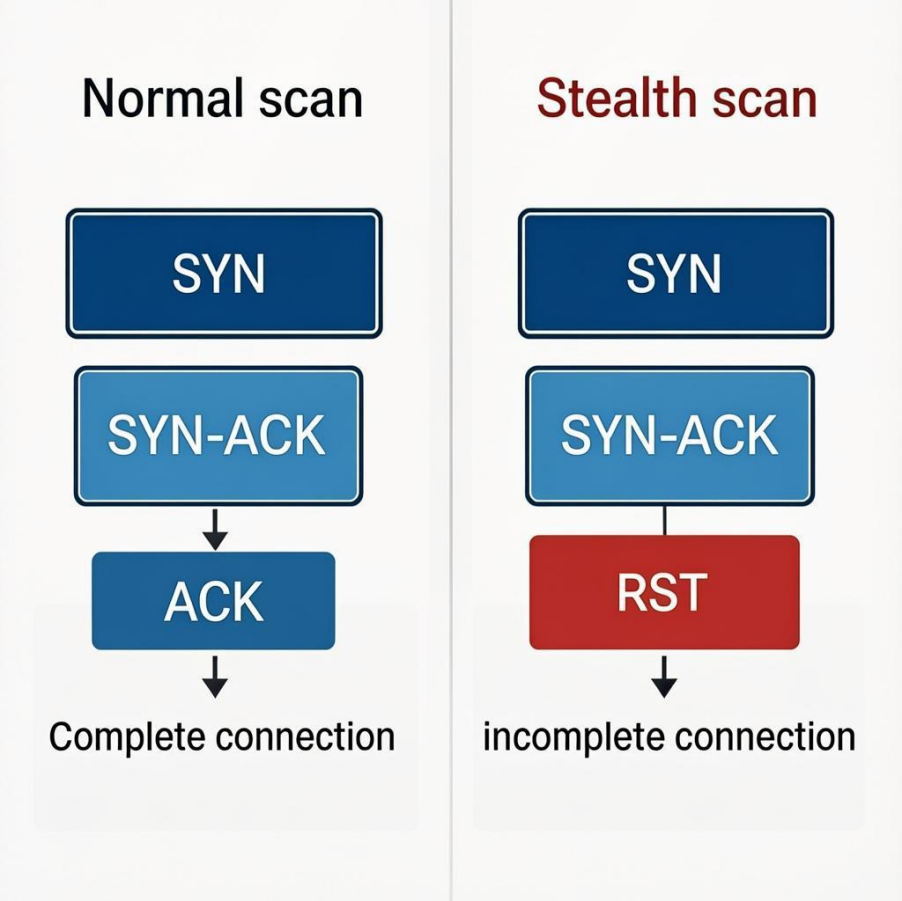



*Figure 2 : Comparaison Scan TCP Normal vs Scan SYN (Stealth)*

### 4.1 Fonctionnement du Scan SYN

La technique du Scan SYN exploite une subtilité du protocole TCP pour déterminer l'état des ports sans compléter la connexion :

1. **L'attaquant envoie SYN :** Une demande de connexion initiale est envoyée au port cible, exactement comme un client légitime le ferait.
2. **La cible répond SYN/ACK :** Si le port est ouvert, le serveur répond positivement, indiquant qu'il est prêt à établir la connexion.
3. **L'attaquant envoie RST :** Au lieu de finaliser avec ACK, l'attaquant envoie RST (Reset) pour annuler la connexion avant qu'elle ne soit établie.

### 4.2 Avantages et Limitations

| Avantages | Limitations |
|---|---|
| • Rapidité : pas de handshake complet<br>• Discrétion : souvent non journalisé<br>• Efficace contre les systèmes legacy | • Nécessite les privilèges root<br>• Détectable par pare-feux modernes<br>• IDS/IPS peuvent le bloquer |

*Tableau 4 : Avantages et limitations du Scan SYN*

**Commande Nmap :** `sudo nmap -sS [cible]` (nécessite les privilèges root)

## 5. Nmap : Network Mapper

Nmap (Network Mapper) est l'outil de cartographie réseau le plus utilisé au monde. Ce scanner de ports open-source permet de découvrir les hôtes et les services sur un réseau informatique. Il constitue un standard de l'industrie utilisé par les professionnels de la sécurité pour auditer les réseaux et identifier les vulnérabilités potentielles.

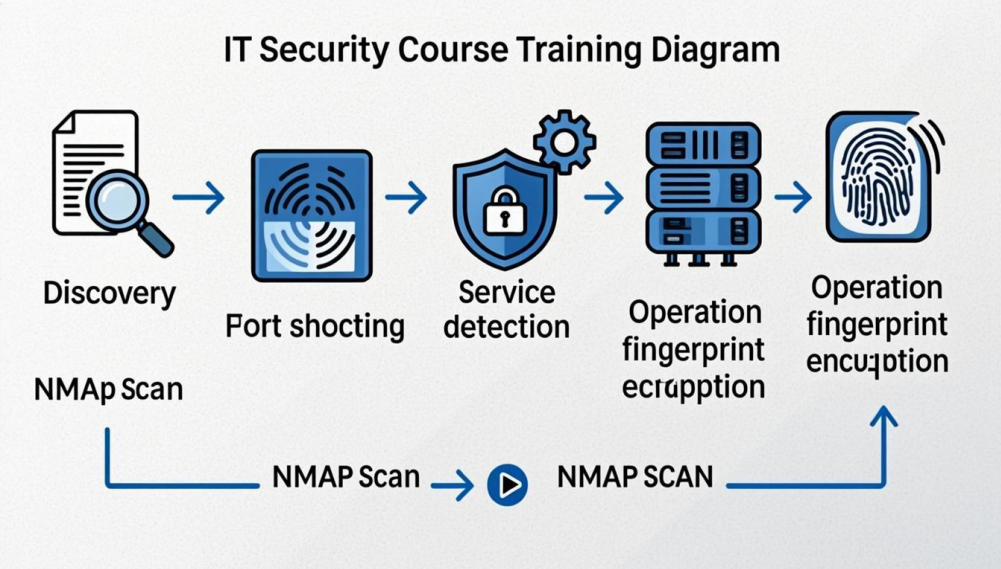



*Figure 3 : Workflow de scan Nmap*

### 5.1 Options Principales

| Option | Privilèges | Description |
|---|---|---|
| `-sS` | Root requis | TCP SYN Scan (Stealth) - le scan le plus populaire |
| `-sV` | Non requis | Détection de version des services en écoute |
| `-O` | Root requis | Détection du système d'exploitation (OS Fingerprinting) |
| `-p-` | Non requis | Scan de tous les 65535 ports (plus lent) |
| `-A` | Root requis | Mode agressif (Version + OS + Scripts + Traceroute) |
| `--script` | Variable | Utilisation des scripts NSE (Nmap Scripting Engine) |

*Tableau 5 : Options principales de Nmap*

**Astuce professionnelle :** Combinez les options pour des scans complets. Exemple : `sudo nmap -sS -sV -O [cible]` permet d'obtenir simultanément les ports ouverts, les versions des services et le système d'exploitation.

## 6. Nmap Scripting Engine (NSE)

Nmap Scripting Engine (NSE) est l'une des fonctionnalités les plus puissantes de Nmap. Elle permet d'utiliser des scripts écrits en langage Lua pour automatiser la détection de vulnérabilités et effectuer des tâches avancées qui dépassent le simple scan de ports. Avec plus de 600 scripts disponibles, NSE couvre une large gamme de services et de cas d'utilisation.

**Syntaxe de base :**

```
nmap --script [nom-du-script] [cible]
```

**Exemple - Test FTP anonyme :**

```
sudo nmap -p 21 --script ftp-anon [cible]
```

Ce script teste si le serveur FTP autorise les connexions anonymes, une vulnérabilité courante qui peut permettre l'accès non autorisé aux fichiers du serveur.

**Commande complète recommandée pour un audit complet :** `sudo nmap -sS -sV -O -p- [cible]`

# PARTIE II : Fiche de Travaux Pratiques

*Scénario : Cartographier le serveur Legacy (Metasploitable2)*

## 1. Prérequis et Environnement

Vous êtes consultant junior pour Nexus-Industry. On vous demande de cartographier le serveur "Legacy" (Metasploitable2) dont la documentation a été perdue, afin d'identifier les services exposés et d'évaluer la surface d'attaque potentielle.

| Élément | Machine Attaquant | Machine Cible |
|---|---|---|
| **Système** | Kali Linux | Metasploitable2 |
| **Identifiants** | kali / kali | msfadmin / msfadmin |
| **Rôle** | Effectuer les scans | Cible des tests |

*Tableau 6 : Configuration de l'environnement de laboratoire*

**Configuration réseau :** VMware en mode Host-Only (VMnet1). Pas d'accès Internet pour la cible. Les deux VMs doivent être sur le même réseau isolé pour des raisons de sécurité et pour simuler un environnement de test réaliste.

## 2. Étape 1 : Découverte du Réseau (Network Discovery)

Avant de scanner la cible, nous devons identifier sa présence sur le réseau et connaître notre propre configuration réseau. Cette étape est cruciale pour éviter de scanner les mauvaises machines.

### Étape 1.1 : Identifier votre adresse IP

Ouvrez un terminal sur Kali Linux et exécutez la commande suivante :

```
$ ip a
```

Cette commande affiche toutes les interfaces réseau. Notez votre adresse IP et le masque de sous-réseau (exemple : 192.168.146.128/24). Recherchez l'interface "eth0" ou "ens33" qui correspond à votre connexion réseau VMware.

### Étape 1.2 : Scanner le réseau pour découvrir les hôtes

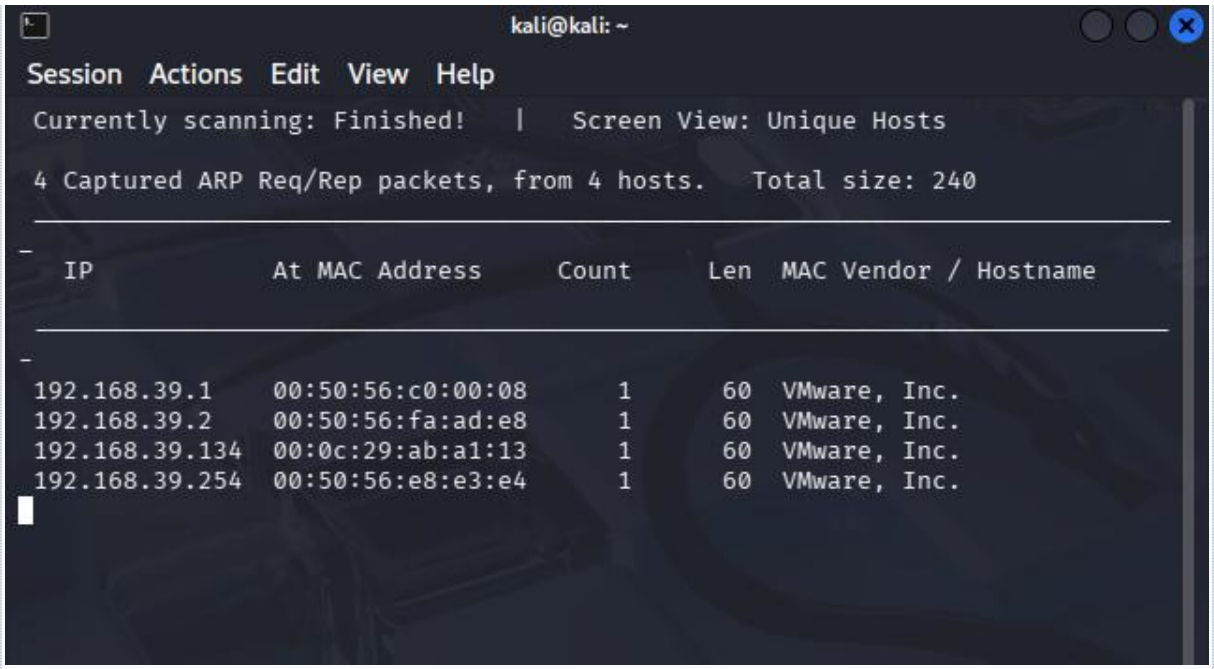
Utilisez netdiscover pour identifier toutes les machines actives sur votre réseau local :

```
$ sudo netdiscover -r 192.168.146.0/24
```

Remplacez 192.168.146.0/24 par votre propre réseau. Cette commande utilise le protocole ARP pour découvrir les machines actives.

**Points importants à noter :**

- Netdiscover fonctionne en scan ARP passif/actif
- Il affiche les adresses IP, MAC et les vendeurs des cartes réseau
- La cible Metasploitable2 sera visible dans la liste des hôtes découverts




*la capture du résultat de netdiscover*

**Action requise :** Notez l'adresse IP de la cible Metasploitable2 (exemple : 192.168.146.130) pour les étapes suivantes.

## 3. Étape 2 : Scan de Ports Basique

Réalisez un scan rapide des 1000 ports les plus communs pour identifier les services exposés. Ce scan initial vous donnera une première vue d'ensemble de la surface d'attaque.

**Commande à exécuter :**

```
$ sudo nmap -sS 192.168.146.130
```

Remplacez 192.168.146.130 par l'adresse IP de votre cible Metasploitable2.

**Explication des paramètres :**

- `-sS` : Scan SYN (Stealth) - rapide et discret
- `192.168.146.130` : Adresse IP de la cible


*Note : Le port 23 correspond généralement au service Telnet, un protocole non sécurisé qui transmet les données en clair (y compris les mots de passe).*

## 4. Étape 3 : Cartographie Avancée (Service & OS)

Nous devons connaître les versions exactes des services et le système d'exploitation pour rechercher des vulnérabilités (CVE) connues. Cette étape est essentielle pour l'analyse de risque.

**Commande à exécuter :**

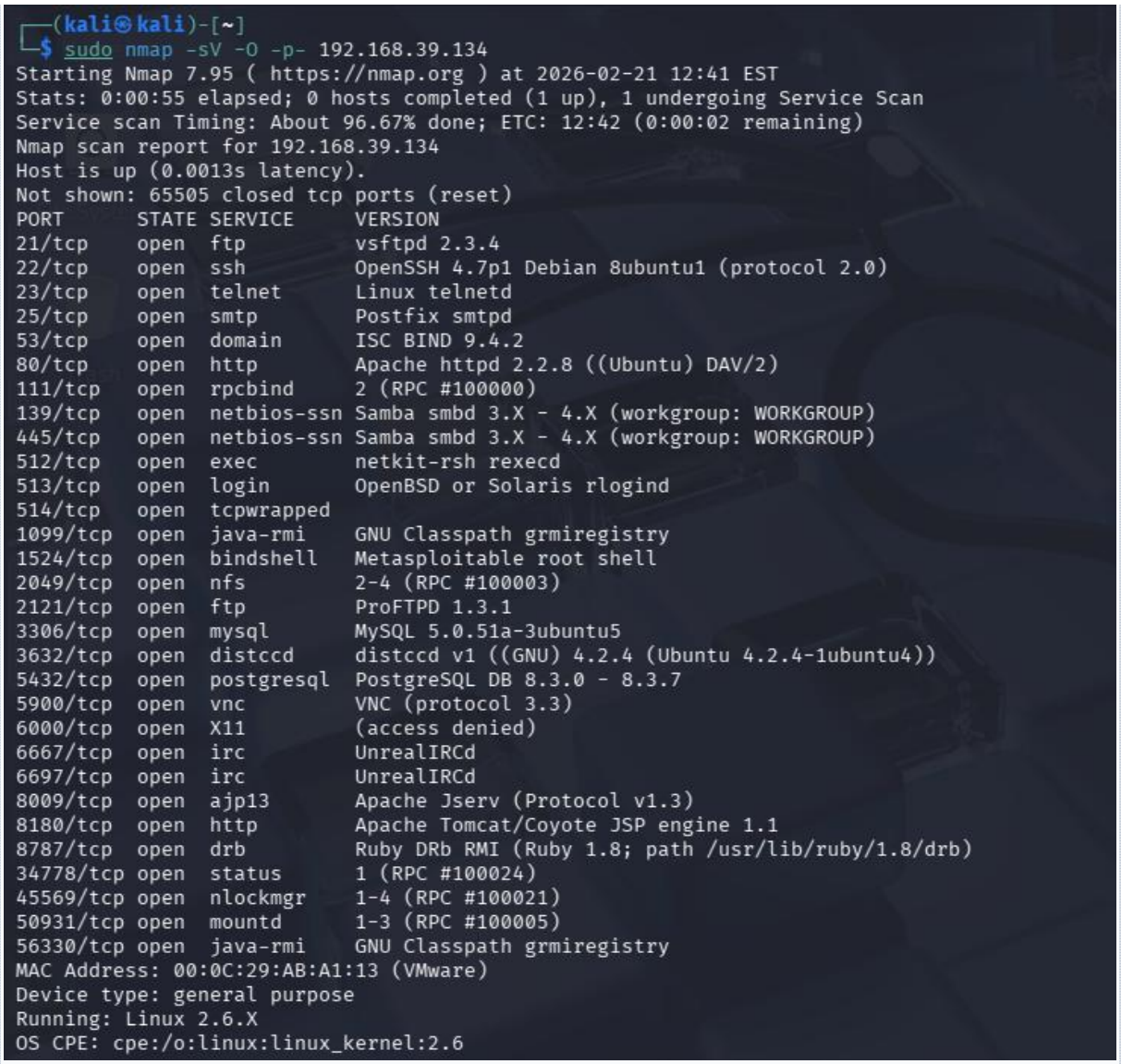
```
$ sudo nmap -sV -O -p- 192.168.146.130
```

**Explication des paramètres :**

- `-p-` : Force le scan de tous les ports (0-65535)
- `-sV` : Interroge les bannières des services pour identifier les versions
- `-O` : Détection du système d'exploitation par analyse des empreintes TCP/IP

**Informations attendues :**

1. **Liste complète des ports :** Tous les ports ouverts avec leurs services associés
2. **Versions des services :** Exemples : Apache 2.2.8, OpenSSH 4.7p1, vsftpd 2.3.4
3. **Système d'exploitation :** Type et version de l'OS détecté (ex: Linux 2.6.9 - 2.6.33)




*résultat du scan avancé*

*Attention : Cette commande peut être longue (plusieurs minutes) car elle scanne tous les 65535 ports et effectue des tests approfondis.*

## 5. Étape 4 : Nmap Scripting Engine (NSE)

Nmap possède des scripts Lua pour automatiser la détection de vulnérabilités basiques. Testons si le service FTP autorise la connexion anonyme, une vulnérabilité courante qui peut exposer des données sensibles.

**Commande à exécuter :**

```
$ sudo nmap -p 21 --script ftp-anon 192.168.146.130
```

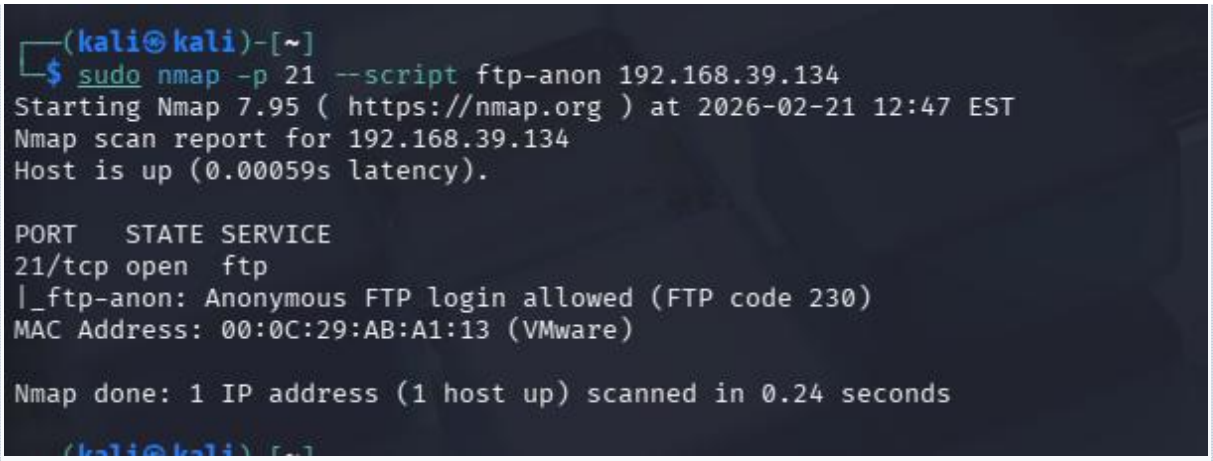
**Explication des paramètres :**

- `-p 21` : Cible uniquement le port FTP (21)
- `--script ftp-anon` : Teste si l'accès FTP anonyme est autorisé

### Vulnérabilité FTP Anonyme :

L'accès FTP anonyme est une vulnérabilité courante qui permet à n'importe qui de se connecter sans authentification. Les impacts potentiels incluent :

- Lecture de fichiers sensibles
- Téléchargement de données confidentielles
- Reconnaissance du système de fichiers




*la capture du résultat du script ftp-anon*

*Autres scripts NSE utiles : http-title, smtp-enum-users, ssh-hostkey, smb-enum-shares*

### 1. Tableau des Ports

Liste complète des ports ouverts et des services associés avec leurs versions. Utilisez le format suivant :

| Port | Protocole | Service | Version |
|---|---|---|---|
| 21 | tcp | ftp | vsftpd 2.3.4 |
| 22 | tcp | ssh | OpenSSH 4.7p1 |
| ... | ... | ... | ... |

*Tableau 7 : Format du tableau des ports à inclure dans le rapport*

| Dépôt | Plateforme LMS |
|---|---|
| Nom du fichier | [Nom]_[Prénom]_TP1_Sécurité.pdf |

*Tableau 8 : Format du rapport à déposer*

-