# TP : Identification et Évasion du Fingerprinting d'un OS sur un Réseau Local

## Objectifs du TP

- Mettre en œuvre un scénario pratique de fingerprinting passif et actif.
- Identifier précisément les systèmes d'exploitation cibles à l'aide d'outils spécifiques.
- Expérimenter des techniques d'évasion pour contourner ou brouiller la détection du système d'exploitation.

## Contexte du TP

Vous êtes analyste en sécurité informatique dans une entreprise. Vous suspectez que certains équipements présents sur votre réseau local utilisent des systèmes d'exploitation obsolètes ou non autorisés.

Votre objectif est double :

- Identifier précisément le système d'exploitation de ces machines en analysant discrètement le trafic réseau (**fingerprinting passif** et **fingerprinting actif**).
- Expérimenter des techniques spécifiques pour masquer ou brouiller cette identification (**évasion du fingerprinting**).

## Environnement requis

Pour réaliser ce TP, préparez un environnement virtuel composé d'au moins trois machines distinctes :

- **Machine A** : Windows 10
- **Machine B** : Ubuntu Linux
- **Machine C** : Kali Linux (machine d'analyse)
- Installez les outils suivants sur la machine Kali (analyse) :
  `Wireshark , tcpdump , p0f (v3) , Nmap`

## Partie A : Fingerprinting Passif

### Étape A1 : Capture du trafic réseau

- Configurez Wireshark ou tcpdump en mode *promiscuous* sur votre machine Kali.

- Générez du trafic réseau classique sur les machines Windows et Linux (navigation web, SSH, FTP, etc.).
- Capturez pendant 10 à 15 minutes le trafic réseau généré.

### Étape A2 : Analyse automatique avec p0f

- Lancez l'analyse automatique avec `p0f` :

```
sudo p0f -r capture.pcap
```

- Relevez les résultats obtenus et présentez-les dans un tableau récapitulatif :

| Adresse IP | OS identifié (p0f) | Version OS | Niveau de certitude |
|---|---|---|---|
| Machine A | | | |
| Machine B | | | |

### Étape A3 : Analyse manuelle avec Wireshark

- Ouvrez votre capture réseau avec Wireshark.
- Sélectionnez plusieurs paquets TCP/IP provenant des machines cibles.
- Notez les valeurs suivantes pour chaque machine cible :
  - TTL initial
  - Window size TCP
  - DF bit (Don't Fragment)
  - Options TCP utilisées (MSS, SACK, timestamps, etc.)
- Validez et complétez les résultats de p0f grâce à votre analyse manuelle.

## Partie B : Techniques d'Évasion (Fingerprinting Passif)

### Étape B1 : Modification des caractéristiques TCP/IP (Machine Linux)

- Modifiez explicitement les paramètres suivants :
  - **TTL initial** (`sysctl net.ipv4.ip_default_ttl`)
  - **TCP Window size**
  - Désactivation des **timestamps TCP**

```
sudo sysctl -w net.ipv4.ip_default_ttl=128
sudo sysctl -w net.ipv4.tcp_window_scaling=0
```

```
sudo sysctl -w net.ipv4.tcp_timestamps=0
```

- Capturez à nouveau le trafic réseau similaire à l'étape A1.

### Étape B2 : Évasion par VPN/Proxy (Machine Windows)

- Configurez votre machine Windows pour passer par un VPN ou un proxy transparent.
- Réalisez une nouvelle capture réseau similaire à l'étape A1.

### Étape B3 : Analyse comparative des résultats

- Relancez p0f et l'analyse Wireshark sur les nouvelles captures.
- Comparez clairement les résultats obtenus avant et après les techniques d'évasion :

| Machine cible | Technique appliquée | OS réel | OS identifié avant évasion | OS identifié après évasion | Efficacité |
|---|---|---|---|---|---|
| Linux | Modification TCP/IP | Ubuntu | | | |
| Windows | VPN / Proxy | Win10 | | | |

## Partie C : Fingerprinting Actif avec Nmap

### Étape C1 : Identification active des OS avec Nmap

- Lancez une analyse active avec Nmap sur vos machines cibles :

```
sudo nmap -O -A <IP_MACHINE_CIBLE>
```

- Documentez précisément :
  - L'OS détecté et sa version
  - Le niveau de certitude indiqué par Nmap

| Adresse IP | OS détecté (Nmap) | Version | Niveau de certitude |
|---|---|---|---|
| Machine A | | | |
| Machine B | | | |

### Étape C2 : Comparaison fingerprinting actif / passif

- Réalisez un tableau comparatif clair entre les résultats obtenus par fingerprinting passif (p0f, Wireshark) et actif (Nmap) :

| Machine | OS réel | OS (Passif) | OS (Actif Nmap) | Concordance |
|---|---|---|---|---|
| Windows | Win10 | | | |
| Linux | Ubuntu | | | |

## Partie D (Optionnelle mais recommandée) : Évasion du Fingerprinting Actif

### Étape D1 : Application des techniques d'évasion face à Nmap

- Reprenez les modifications effectuées à l'étape B1 et B2.
- Relancez l'analyse active avec Nmap sur les machines modifiées.

### Étape D2 : Analyse comparative de l'impact sur Nmap

| Machine | Technique d'évasion | OS réel | OS (Nmap avant évasion) | OS (Nmap après évasion) | Impact |
|---|---|---|---|---|---|
| Linux | Modification TCP/IP | Ubuntu | | | |
| Windows | VPN / Proxy | Win10 | | | |

## Questions complémentaires à traiter dans votre rapport final:

- Quelle technique de camouflage est la plus efficace (et pourquoi) ?
- Quelles caractéristiques TCP/IP semblent les plus cruciales pour l'identification des OS ?
- Quelle est la fiabilité du fingerprinting passif face aux méthodes d'évasion utilisées ?
- Quelle stratégie adopteriez-vous en tant qu'administrateur réseau pour détecter des tentatives de fingerprinting actif ?