TP CrowdSec

Objectifs pédagogiques

- Comprendre le rôle de CrowdSec pour renforcer un pare-feu pfSense
- Utiliser une VM Kali (VMware) pour simuler des attaques contrôlées
- Générer des logs détectables par CrowdSec et analyser les décisions
- Rédiger un rapport professionnel et proposer des améliorations

Consignes de sécurité (LECTURE OBLIGATOIRE)

1. **N'effectuez les attaques que dans un environnement de laboratoire** pour lequel vous avez une autorisation explicite
2. **Toute tentative contre des cibles externes ou non autorisées est interdite et illégale**
3. Limitez la vitesse des scans (options `-T3`, `--rate` basse)
4. Prenez des snapshots avant toute manipulation (pfSense ET Kali)
5. Documentez précisément chaque action avec horodatage

📋 Prérequis et Topologie

Équipement nécessaire

- pfSense (VM ou appliance) avec CrowdSec opérationnel
- Machine Kali Linux sous VMware (VM)
- Outils sur Kali : nmap, masscan, hydra, tcpdump, wireshark
- VMware Workstation ou VMware Player

🌐 Topologie Réseau Recommandée

pfSense (VM/Appliance) ↔ Réseau de test ↔ Kali Linux (VM)

Mode : Bridged ou réseau interne VMware

📝 Adresse IP cible (WAN pfSense) : _____ (à compléter)

🔧 Préparation de la VM Kali sous VMware

Étape 1 : Téléchargement et vérification

1. Télécharger l'ISO officiel depuis https://www.kali.org/get-kali/
2. Vérifier l'intégrité avec la somme SHA256

Étape 2 : Création de la VM dans VMware

1. VMware Workstation/Player → **Créer une nouvelle machine virtuelle**
2. Sélectionner **Typical** → Installer depuis image ISO
3. Configuration :
    - Système invité : **Linux / Debian 64-bit**
    - RAM : **2-4 GB**
    - vCPU : **2 cœurs**
    - Disque : **20-50 GB**

Étape 3 : Configuration réseau

Option A (recommandée) : Mode `Bridged` pour que Kali obtienne une IP sur le même réseau que pfSense WAN/Test

Option B : Mode `Host-only` ou `Custom` pour un réseau isolé

Étape 4 : Installation du système

1. Démarrer la VM → Choisir **Graphical install**
2. Suivre l'assistant (partitionnement guidé OK en VM)
3. Créer un utilisateur non-root (ou utiliser root selon politique du lab)

Étape 5 : Mise à jour et installation des outils

```
# Mise à jour du système
sudo apt update && sudo apt full-upgrade -y

# Installation des outils nécessaires
sudo apt install -y nmap masscan hping3 hydra \
  tcpdump wireshark openssh-server seclists
```

Snapshots VMware

Avant d'attaquer : Créer un snapshot de la VM Kali ET de la VM pfSense

Note : Si VMware Player (sans snapshot), conservez une copie clonée des VMs

🎯 Séquence du TP — Exercices Pratiques

Étape 0 — Vérifications préliminaires OBLIGATOIRE

```
# Vérifier l'adresse IP de Kali
ip a

# Vérifier la connectivité avec pfSense
ping <ip_pfSense_wan>

# Créer un snapshot avant de commencer
# (Interface VMware)
```

Exercice 1 — Scan léger (ports standards) OBLIGATOIRE

Objectif : Générer des entrées SYN/scan pour déclencher CrowdSec

```
nmap -sS -sV -Pn -p22,80,443 <ip_pfSense_wan> -oN scan1.txt
```

Exercice 2 — Scan multi-ports progressif OBLIGATOIRE

```
nmap -p1-1000 -sS -T3 <ip_pfSense_wan> -oN scan2.txt
```

Exercice 3 — Scan UDP OPTIONNEL

```
sudo nmap -sU -p1-2000 --top-ports 100 <ip_pfSense_wan> -oN scan_udp.txt
```

Exercice 4 — Scan contrôlé avec masscan AVANCÉ

Note : Réduire `--rate` si saturation réseau

```
sudo masscan <ip_pfSense_wan> -p1-65535 --rate 500 -oL masscan_output.txt
```

Exercice 5 — Tentatives d'authentification SSH OBLIGATOIRE

Méthode A : Avec Hydra (créer `passwords.txt` avec 10 mots de passe)

```
hydra -l testlab -P passwords.txt -t 4 -w 10 -s 22 -f <ip_target> ssh
```

Méthode B : Boucle SSH pour provoquer des échecs

```
for i in {1..20}; do
  ssh -o ConnectTimeout=5 testlab@<ip_target> false || true
done
```

🔍 Vérifications côté pfSense / CrowdSec

Commandes CrowdSec (SSH / console pfSense)

```
# Lister les alertes
sudo cscli alerts list

# Lister les décisions (bans)
sudo cscli decisions list

# Afficher les métriques
sudo cscli metrics
```

Vérification des logs pfSense

```
# Logs du firewall
tail -n 200 /var/log/filter.log

# Logs système
tail -n 200 /var/log/system.log
```

Interface Web pfSense

Accéder à : **Services** → **CrowdSec**

Vérifier : Status, Bouncers, Scenarios actifs

Consignes de Rendu

Livrables à remettre

- `commands.txt` : Liste exacte des commandes exécutées avec timestamps
- `scan1.txt`, `scan2.txt`, `masscan_output.txt` : Fichiers de sortie
- `capture.pcap` : Capture réseau (si tcpdump utilisé)
- Captures d'écran de l'interface CrowdSec (Status / Decisions)
- `rapport.pdf` : Analyse détaillée (1-2 pages)

Contenu du rapport

- Quel(s) scénario(s) CrowdSec ont été déclenchés ?
- Durée du ban appliqué
- Analyse de l'efficacité de la protection
- Recommandations d'amélioration
- Difficultés rencontrées et solutions apportées

Annexes — Commandes de référence rapide

Kali (attaquant)

```
# Informations réseau
ip a
ping <target>

# Scans Nmap
nmap -sS -sV -Pn -p22,80,443 <target> -oN scan1.txt
nmap -p1-1000 -sS -T3 <target> -oN scan2.txt

# Masscan
sudo masscan <target> -p1-65535 --rate 500 -oL masscan_output.txt

# Capture réseau
sudo tcpdump -i eth0 host <target> -w /tmp/capture.pcap

# Brute-force SSH
hydra -l testlab -P passwords.txt -t 4 -s 22 -f <target> ssh
```

pfSense (administrateur)

```
# CrowdSec
sudo cscli alerts list
sudo cscli decisions list
sudo cscli metrics

# Logs pfSense
tail -n 200 /var/log/filter.log
tail -n 200 /var/log/system.log
```

Remarques Finales

Points importants

- **Blocage accidentel** : Si vous bloquez une machine légitime, restaurez les snapshots
- **Documentation temporelle** : Documentez précisément l'heure/date de chaque attaque pour la corrélation avec les logs
- **Pour aller plus loin** : Configurer un reverse-proxy ou HAProxy et analyser ses logs avec CrowdSec

---