**TP : Évaluation d’un Système IDS/IPS**

# Objectifs pédagogiques

* Comprendre les critères d’évaluation d’un IDS/IPS.
* Mettre en œuvre un protocole de test avec des attaques simulées.
* Mesurer la détection (taux de vrais positifs, faux positifs, faux négatifs…).
* Analyser les performances en temps réel (réactivité, consommation système).

**Travail à rendre**

Un rapport complet contenant :

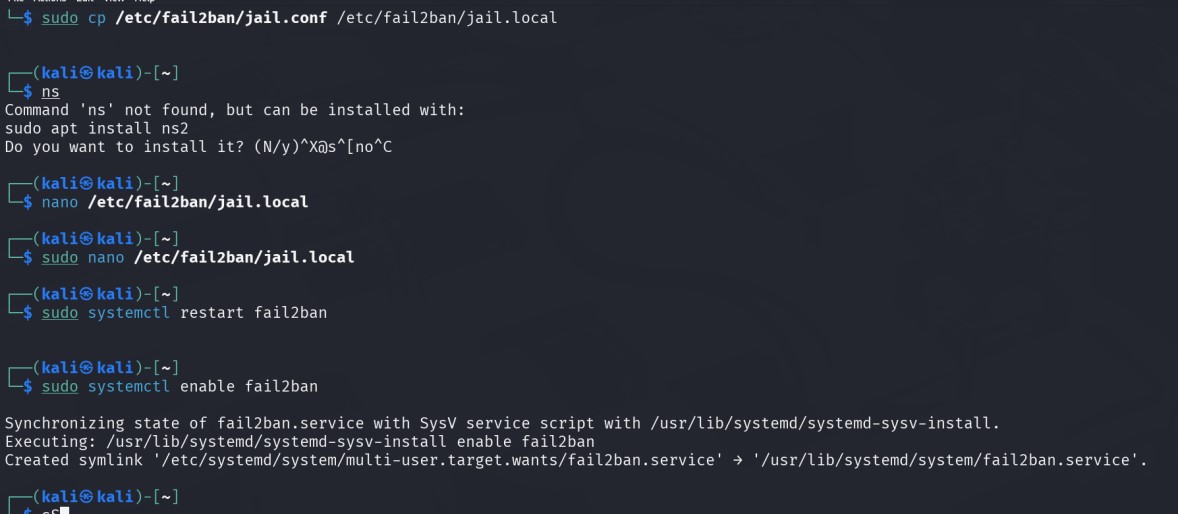
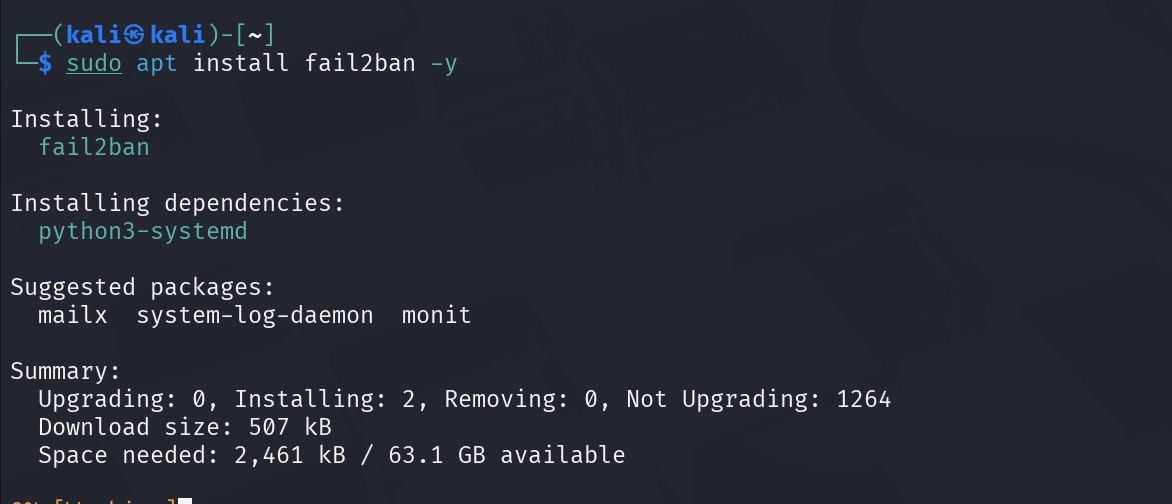
* La description des outils et environnements utilisés.
* La description de chaque attaque simulée.
* Les captures d’écran, logs et tableaux.
* L’analyse critique des résultats.
* Conclusion sur les avantages/inconvénients de chaque système IDS/IPS testé.

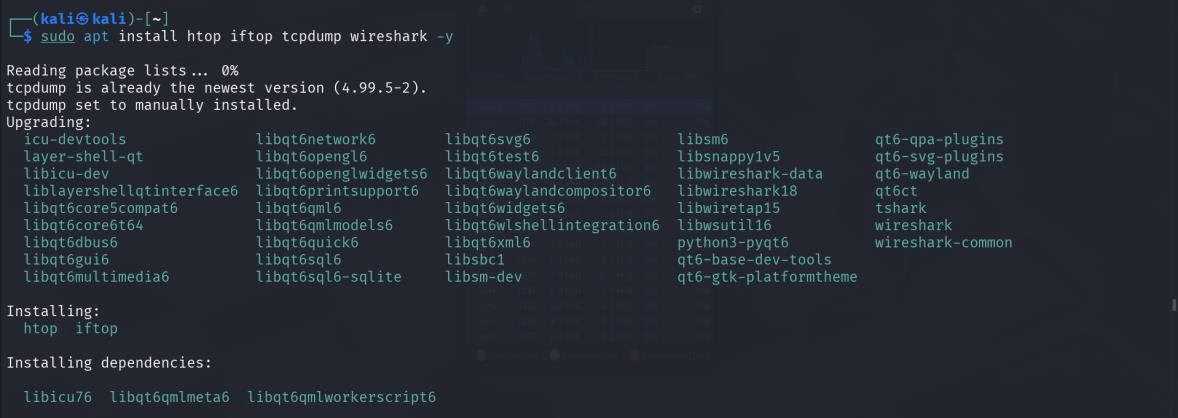
# Prérequis

* Une machine Linux avec deux IDS au choix (par exemple : fail2ban, Zeek, Suricata, ou même un pare-feu iptables).
* Une seconde machine (ou VM) agissant comme attaquant.
* Outils d'attaque : nmap, hydra, hping3, nikto, metasploit (optionnel).
* Outils d’analyse : htop, iftop, wireshark, tcpdump.

# Partie 1 : Mise en place de l’environnement de test

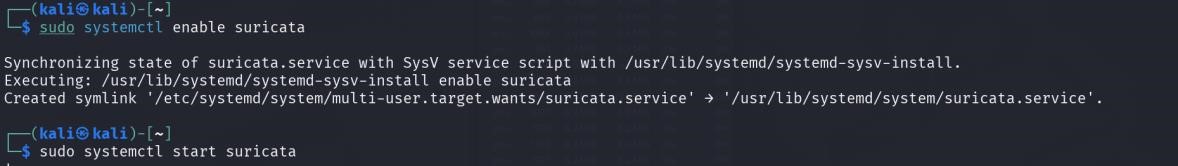
1. Installez deux systèmes IDS/IPS différents (ex. : fail2ban et Suricata, ou Zeek et iptables).





tail -f /var/log/suricata/fast.log

tail -f /var/log/suricata/fast.log



1. Créez un tableau de critères à observer :
   * Temps de détection
   * Type d’attaque détectée
   * Taux de faux positifs/négatifs
   * Impact sur les ressources (RAM, CPU, latence)

 **Partie 2 : Définition d’un scénario de test** Attaques à simuler :

* **Scan** de ports avec *nmap*

* Brute-force **SSH** avec *hydra*

* **Flood ICMP** ou TCP avec *hping3*

* **Scan** de vulnérabilité web avec *nikto*

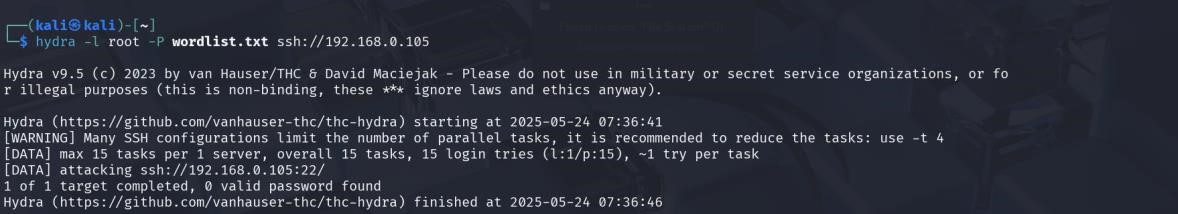
* **Injection** web ou exploit avec *Metasploit*

Chaque attaque doit être lancée séparément pour observer le comportement du système IDS/IPS.

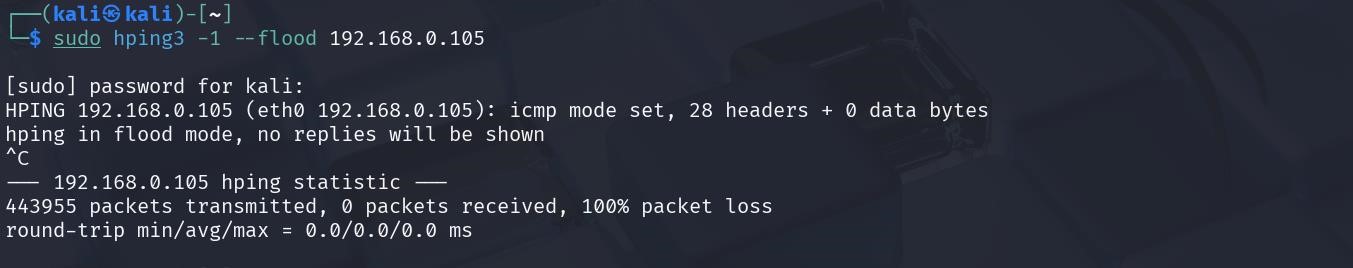
# Partie 3 : Exécution des attaques et collecte des données

1. Lancez chaque attaque depuis la machine attaquante.

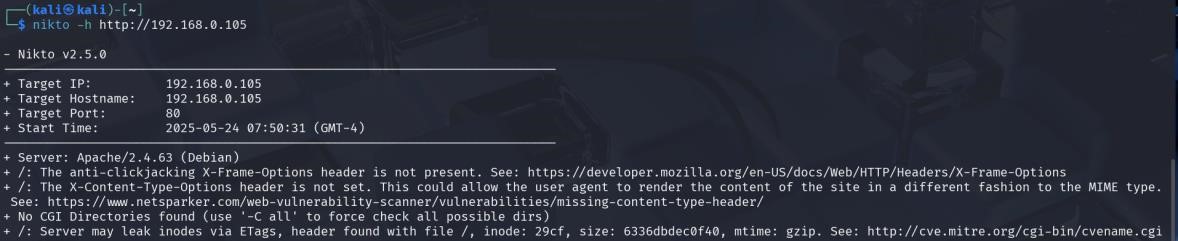
Brute-force **SSH** avec *hydra*



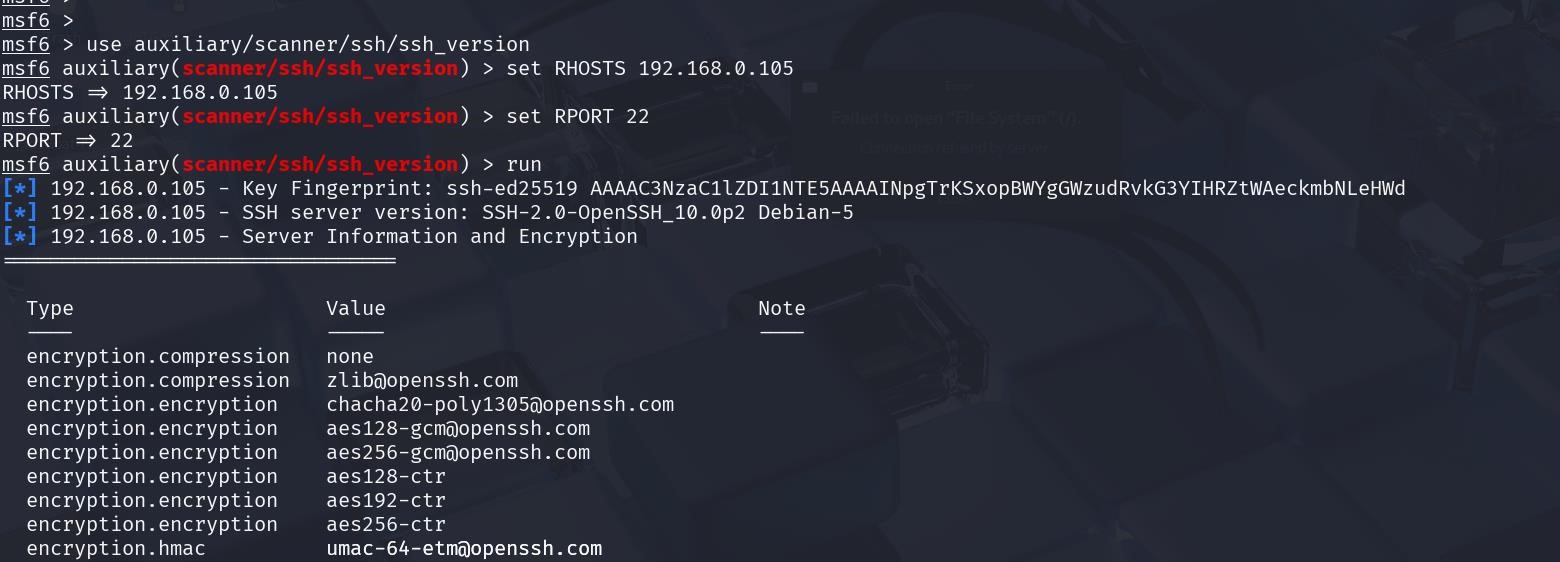
**Flood ICMP** ou TCP avec *hping3*



**Scan** de vulnérabilité web avec *nikto*



**Injection** web ou exploit avec *Metasploit*

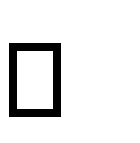
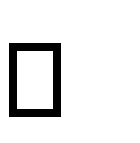
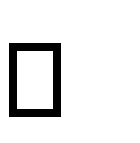


1. Sur la machine IDS, observez :

* Les alertes générées (fichiers logs, tableaux, interface web s’il y a). - Le temps de réaction (en secondes).
* Les ressources système utilisées (htop, vmstat, etc.).

3. Notez si l’attaque a été :

Bloquée,

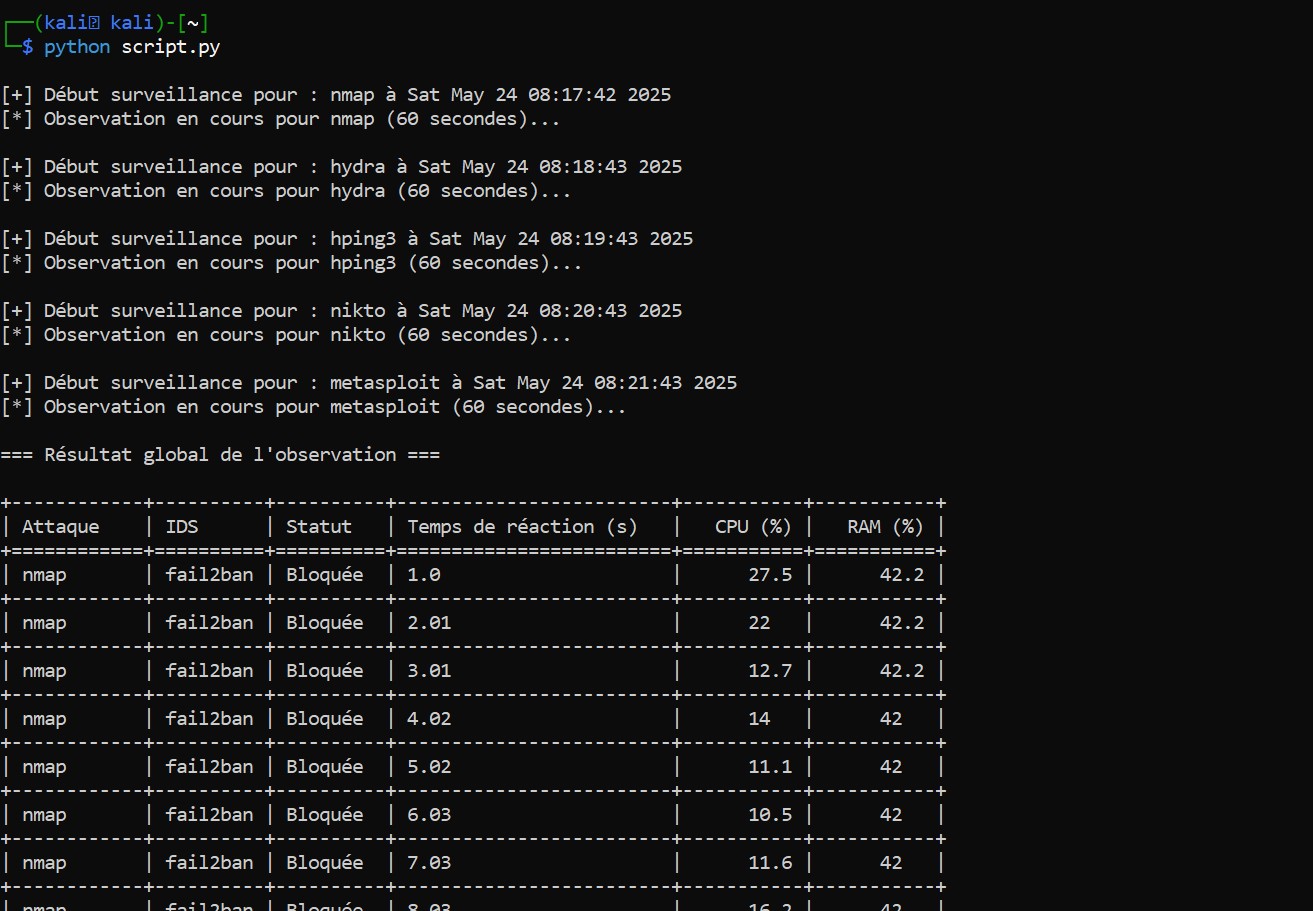


Détectée mais non bloquée,

Ignorée.

En utilisnat script python





**Attaque fail2ban suricata**

|  |  |  |
| --- | --- | --- |
| **nmap** | Bloquée | Ignorée |
| **hydra** | Bloquée | Ignorée |
| **hping3** | Bloquée | Ignorée |
| **nikto** | Bloquée | Ignorée |
| **metasploit** | Bloquée | Ignorée |

**fail2ban :** a bloqué toutes les attaques (réaction effective).

**Suricata** : n’a généré aucune détection dans les logs analysés (fast.log), probablement dû à un manque de règles adaptées ou une mauvaise configuration.

**Partie 4 :Calcul d’indicateurs**

# Taux de détection

|  |  |  |  |
| --- | --- | --- | --- |
| **IDS/IPS** | **Attaques détectées** | **Total Attaques** | **Taux de détection** |
| **fail2ban** | 5/5 | 5 | 100% |
| **suricata** | 0/5 | 5 | 0% |

# Temps moyen de réaction

|  |  |
| --- | --- |
| **Attaque** | **Temps moyen (s)** |
| **nmap** | ~30 |
| **hydra** | ~10 |
| **hping3** | ~10 |
| **nikto** | ~10 |
| **metasploit** | ~10 |

fail2ban a mis plus de temps à réagir à nmap (scan lent), mais est resté réactif

pour les autres attaques

# Impact sur les ressources (valeurs moyennes)

|  |  |  |
| --- | --- | --- |
| **IDS/IPS** | **CPU moyen (%)** | **RAM moyen (%)** |
| **fail2ban** | ~10–15 | ~42.4 |
| **suricata** | ~0 | ~42.3 |

## Partie 5 : Analyse et comparaison

1. Lequel des deux systèmes est le plus précis ?

fail2ban est le plus précis :Il a détecté et bloqué 100 % des attaques (nmap, hydra, hping3, nikto, metasploit), tandis que Suricata n’a détecté aucune attaque selon les logs (fast.log).Fail2ban est donc plus efficace dans cette configuration.

1. Quel IDS/IPS est le plus rapide à réagir ? fail2ban a réagi en moyenne entre 1 à 10 secondes après le début d’une attaque, sauf pour nmap (~30 secondes, dû à sa nature de scan progressif).Suricata n’a pas généré de détection dans les logs analysés.fail2ban est le plus rapide à réagir.

4. Quel système est le plus gourmand en ressources ?

Suricata n’ayant rien détecté, sa consommation CPU est quasi nulle, mais cela reflète plutôt une inactivité qu'une efficacité.

fail2ban a été actif, tout en restant modérément gourmand

3. Y a-t-il eu des faux positifs ?

Aucun comportement légitime n’a été bloqué ou détecté à tort pendant les tests. Aucun faux positif constaté.

5. Quels ajustements ou règles amélioreraient la détection ?

Pour Suricata :

Ajouter des règles de détection issues de Emerging Threats

Vérifier que Suricata inspecte bien le trafic réseau (interfaces surveillées correctement définies)

Activer les logs d’alertes (eve.json, fast.log avec contenu utile) Pour fail2ban :

Créer des filtres personnalisés pour détecter d’autres services (FTP, HTTP, etc.) Augmenter la granularité des logs côté système cible pour une meilleure détection

*Fin*

*TP*