Parfait, merci pour la précision. Vu que tu **n’as pas encore de serveur web**, je vais t’expliquer comment :

1. 📦 Créer les fichiers factices .exe, .zip, .rar, .dll sur Kali
2. 🌐 Mettre en place un mini **serveur web HTTP avec Python** (sur Kali, simple et rapide)
3. 🌍 Télécharger ces fichiers depuis la machine Windows ou Ubuntu pour déclencher les règles Suricata

**✅ 1. Créer les fichiers factices**

Sur Kali, exécute ceci :

bash

Copier le code

mkdir ~/malwares

cd ~/malwares

# Créer un faux fichier .exe

echo "fake exe" > test.exe

# Créer un faux fichier .zip

echo "fake zip" > test.zip

# Créer un faux fichier .rar

echo "fake rar" > test.rar

# Créer un faux fichier .dll

echo "fake dll" > test.dll

Tu auras donc dans ~/malwares :

python

Copier le code

test.exe

test.zip

test.rar

test.dll

**🚀 2. Lancer un serveur web temporaire avec Python**

Toujours dans le dossier ~/malwares :

bash

Copier le code

cd ~/malwares

python3 -m http.server 8080

Cela lancera un serveur web HTTP sur le port **8080**

Vérifie l’IP de Kali avec :

bash

Copier le code

ip a

Supposons que c’est 192.168.60.10

**🌍 3. Depuis Windows (ou Ubuntu), télécharger les fichiers**

Sur Windows (dans un navigateur ou curl si installé) :

* Ouvre :  
  http://192.168.60.10:8080/test.exe  
  http://192.168.60.10:8080/test.zip  
  etc.

Sinon, sur Ubuntu (si tu as curl ou wget) :

bash

Copier le code

curl http://192.168.60.10:8080/test.exe -O

curl http://192.168.60.10:8080/test.zip -O

curl http://192.168.60.10:8080/test.rar -O

curl http://192.168.60.10:8080/test.dll -O

**🔍 4. Voir les alertes sur la machine Suricata (Ubuntu)**

bash

Copier le code

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

Tu devrais voir apparaître :

log

Copier le code

[\*\*] [1:100001:1] Téléchargement fichier EXE détecté - possible malware [\*\*]

[\*\*] [1:100004:1] Téléchargement fichier ZIP détecté [\*\*]

...

Souhaites-tu que je t’aide à configurer un serveur web plus permanent (Apache/Nginx) ou restons sur ce serveur Python simple ?

Demander à ChatGPT

**Vous avez dit :**

test.rar et test.zip sont en rouge

**ChatGPT a dit :**

Les noms des fichiers en **rouge** dans un terminal Linux (comme sur Kali) indiquent souvent que ces fichiers **n’ont pas les droits de lecture** ou que leurs **permissions sont spéciales**, comme "exécutables sans lecture", ou qu’ils sont **liens symboliques cassés** (moins probable ici).

Voici comment corriger ça :

**✅ 1. Vérifie les permissions**

Dans ton dossier ~/malwares, tape :

bash

Copier le code

ls -l

Tu verras un résultat comme :

bash

Copier le code

-rw-r--r-- 1 kali kali 9 Aug 8 12:05 test.dll

-rw-r--r-- 1 kali kali 9 Aug 8 12:05 test.exe

-rw------- 1 kali kali 9 Aug 8 12:05 test.rar

-rw------- 1 kali kali 9 Aug 8 12:05 test.zip

Ici, on voit que .rar et .zip ont des droits rw------- → seuls lisibles par le propriétaire.

**🔧 2. Corrige les permissions**

Pour donner les bons droits de lecture pour que le serveur web (Python HTTP) les serve :

bash

Copier le code

chmod 644 test.\*

Cela donne :

* Lecture/écriture pour le propriétaire
* Lecture pour les autres

**🔁 3. Vérifie à nouveau**

bash

Copier le code

ls --color

Les fichiers ne devraient plus être en rouge.

Tu peux aussi tester depuis un navigateur (Windows ou Ubuntu) :

arduino

Copier le code

http://192.168.60.10:8080/test.zip

S’il se télécharge, c’est bon 👍

Souhaites-tu que je t’aide à créer de vrais fichiers .zip et .rar compressés avec des fichiers internes (pas juste du texte) ?

**Vous avez dit :**

**ChatGPT a dit :**

Merci pour la capture.

Tes fichiers ont bien les **droits en lecture (rw-r--r--)**, donc tout est correct. Le fait que .rar et .zip apparaissent encore en **rouge** est probablement dû à la configuration du **thème de ton terminal**, qui colore certains types de fichiers (comme les archives compressées .zip, .rar) en rouge par défaut — **ce n’est pas une erreur**.

**✅ Tu peux continuer :**

1. Lance le **serveur HTTP** :

bash

Copier le code

cd ~/malwares

python3 -m http.server 8080

1. Depuis **Windows** ou **Ubuntu (avec Suricata)**, fais des tests avec :

bash

Copier le code

curl http://192.168.60.10:8080/test.zip -O

curl http://192.168.60.10:8080/test.rar -O

curl http://192.168.60.10:8080/test.dll -O

curl http://192.168.60.10:8080/test.exe -O

Remplace bien 192.168.60.10 par l’adresse IP de ta machine Kali sur vmnet8 si différente.

**📌 Si tu veux ajouter plus de contenu :**

On peut créer de vrais fichiers .zip ou .rar contenant des documents simulés (ex : fichier .txt, .bat, etc.), pour tester des règles Suricata plus réalistes.

Tu veux qu’on le fasse ?

**Vous avez dit :**

je tape dans ubuntu: curl not found

**ChatGPT a dit :**

Parfait, tu es très proche du test. Si ta machine **Ubuntu** n’a pas curl installé, voici la commande pour l’installer :

**✅ Installation de curl sur Ubuntu :**

bash

Copier le code

sudo apt update

sudo apt install curl -y

Une fois l’installation terminée, tu peux relancer les commandes de téléchargement :

bash

Copier le code

curl http://192.168.60.10:8080/test.zip -O

curl http://192.168.60.10:8080/test.rar -O

curl http://192.168.60.10:8080/test.dll -O

curl http://192.168.60.10:8080/test.exe -O

⚠️ N’oublie pas de remplacer 192.168.60.10 par l’adresse IP réelle de **Kali** si ce n’est pas celle-là.

Tu me dis quand c’est bon ou si tu veux créer un .zip ou .rar plus "réaliste" avec du contenu.

**Vous avez dit :**

**ChatGPT a dit :**

Merci pour la capture : ton système a bien curl installé, mais il est lancé depuis **Snap** et peut avoir un comportement un peu particulier selon les versions.

**✅ Ce que tu peux faire :**

Teste maintenant le téléchargement depuis ta machine **Ubuntu (suricata)** vers ta machine **Kali (serveur HTTP)**.

Par exemple, si tu as lancé le serveur HTTP avec :

bash

Copier le code

sudo python3 -m http.server 8080

Dans le dossier contenant les fichiers .exe, .dll, .rar, .zip, alors, depuis Ubuntu tu tapes (en adaptant l’IP de Kali) :

bash

Copier le code

curl http://192.168.68.101:8080/test.zip -O

curl http://192.168.68.101:8080/test.rar -O

curl http://192.168.68.101:8080/test.dll -O

curl http://192.168.68.101:8080/test.exe -O

Remplace bien 192.168.68.101 par l’adresse IP réelle de Kali sur le réseau.

**🔍 Objectif :**

Ces commandes simulent un téléchargement de **malwares** (ou fichiers suspects) afin que **Suricata** les intercepte **grâce aux règles que tu as créées**, par exemple :

rules

Copier le code

alert http any any -> any any (msg:"Téléchargement de fichier ZIP suspect"; content:".zip"; http\_uri; nocase; sid:3010101;)

alert http any any -> any any (msg:"Téléchargement de fichier RAR suspect"; content:".rar"; http\_uri; nocase; sid:3010102;)

alert http any any -> any any (msg:"Téléchargement de DLL suspecte"; content:".dll"; http\_uri; nocase; sid:3010103;)

alert http any any -> any any (msg:"Téléchargement de fichier EXE suspect"; content:".exe"; http\_uri; nocase; sid:3010104;)

Tu peux maintenant :

✅ Lancer le serveur web Kali  
✅ Lancer les curl sur Ubuntu  
✅ Vérifier dans /var/log/suricata/fast.log si les alertes s’affichent

Tu veux qu’on fasse la version .zip avec un vrai fichier à l’intérieur aussi ?

**Vous avez dit :**

je peux faire le curl dans windows aussi?

**ChatGPT a dit :**

Oui, tu peux tout à fait faire les curl depuis **Windows**, et c’est **même une excellente idée** car :

🔸 **Tu crées du trafic HTTP sortant depuis Windows**, ce qui simule un comportement réel d’un poste client qui télécharge des fichiers suspects (comme un malware .exe, .zip, .dll, etc.).

🔸 **Suricata**, installé sur **Ubuntu** (si tu es en mode af-packet, NFQUEUE ou simplement IDS sur interface), pourra détecter ces téléchargements.

**✅ Étapes pour utiliser curl sur Windows :**

1. **Ouvre PowerShell** ou **CMD**
2. Tape une commande du genre :

powershell

Copier le code

curl http://192.168.68.101:8080/test.zip -OutFile test.zip

curl http://192.168.68.101:8080/test.exe -OutFile test.exe

Remplace 192.168.68.101 par l’IP de ta machine **Kali** (serveur HTTP).

**🔎 Vérifie ensuite dans Suricata :**

Sur Ubuntu, regarde dans :

bash

Copier le code

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

Tu devrais voir des alertes comme :

css

Copier le code

[\*\*] [1:3010101:1] Téléchargement de fichier ZIP suspect [\*\*]

**🟡 Remarques :**

* curl est installé **par défaut sur Windows 10 et 11**, donc tu ne devrais pas avoir besoin d’installation.
* Tu peux tester avec .zip, .rar, .dll, .exe, même si le fichier est vide, ça suffit pour que Suricata détecte via content:".zip"; http\_uri;

Souhaites-tu que je te donne un exemple de mini page HTML ou lien à télécharger pour tester depuis Windows ?

**Vous avez dit :**

C'est bon

**ChatGPT a dit :**

Parfait ! 👍

Tu peux maintenant :

1. Lancer un petit **serveur web** sur ta machine Kali avec :

bash

Copier le code

python3 -m http.server 8080

1. Depuis **Windows**, utilise curl pour télécharger un des fichiers (exemple .exe, .zip, etc.) :

powershell

Copier le code

curl http://192.168.68.XXX:8080/test.exe -OutFile test.exe

(Remplace XXX par l’adresse IP de Kali)

1. Sur **Ubuntu**, observe les logs Suricata en direct :

bash

Copier le code

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

Tu devrais voir l'alerte si ta règle est bien chargée et fonctionne. Si besoin, je peux t’aider à confirmer que ta règle est bien écrite et activée.

N’hésite pas à me dire si tu veux tester un autre type de fichier (PDF, image, etc.) ou un autre protocole (FTP, SMB, etc.).