**PR07 :Déploiement**

**d’une solution de**

**détection d’intrusion**

**Une image contenant Graphique, Police, logo, graphisme

Le contenu généré par l’IA peut être incorrect.Une image contenant conception

Description générée automatiquement avec une confiance faible**

**Table des matières**

[**Cahier des charges** 3](#_Toc192507686)

[**Installation et configuration de Suricata** 4](#_Toc192507687)

[**Configuration de règles** 4](#_Toc192507688)

[**Test d’efficacité de la règle** 6](#_Toc192507689)

# **Cahier des charges**

-Installation de Suricata

-Configuration de Suricata

- Créer des règles de filtrage pour :

* Détection de ping vers le serveur
* Détection de connexion FTP/SFTP
* Détection de tentative de connexion FTP/SFTP

Une image contenant texte, capture d’écran, diagramme, Police

Description générée automatiquement

Architecture réseau

# **Installation et configuration de Suricata**

Il faut en premier temps, installer Suricata et les dépendances annexes.

****

En parallèle, on vérifie le nom de la carte réseau du serveur à observer, ici « ens33 ».

Cette information nous permet de modifier correctement le fichier de configuration

« af-packet ».

Une image contenant texte, Police, capture d’écran, blanc

Description générée automatiquement

La configuration de base est terminée, il faut maintenant configurer des règles en fonction des besoins.

# **Configuration de règles**

* Détection de ping vers le serveur



Explication de la règle :

1. **alert** : Ce mot-clé indique que cette règle générera une alerte si les conditions spécifiées sont remplies.
2. **icmp** : Cela spécifie le protocole réseau concerné par cette règle.
3. **any any** : Le premier any indique que la règle s'applique à n'importe quelle adresse IP source. Le second any signifie que la règle s'applique à n'importe quel port source.
4. **->** : Cette flèche indique la direction du trafic.
5. **192.168.10.251 any** : Cela spécifie l'adresse IP de destination et le port de destination. 192.168.10.251 est l'adresse IP du serveur Web, et any signifie que la règle s'applique à n'importe quel port de destination.
6. **(msg:"Ping détecté vers le serveur Web";** : Ce champ contient le message qui sera enregistré dans les logs lorsque la règle est déclenchée.
7. **itype:8;** : Ce champ spécifie le type de message ICMP. Le type 8 correspond à une requête echo (ping).
8. **sid:1000001;** : C'est l'identifiant unique de la règle (Signature ID).
9. **rev:1;)** : Ce champ indique la révision de la règle.

* Détection de connexion FTP/SFTP



Explications de la règle FTP :

1. **alert** : Ce mot-clé indique que la règle générera une alerte si les conditions spécifiées sont remplies.
2. **tcp** : Cela spécifie que la règle concerne le protocole TCP.
3. **any any** : Le premier any indique que la règle s'applique à n'importe quelle adresse IP source. Le second any signifie que la règle s'applique à n'importe quel port source.
4. **->** : Cette flèche indique la direction du trafic.
5. **any 21** : Cela spécifie que la règle s'applique à n'importe quelle adresse IP de destination, mais uniquement sur le port 21, qui est le port standard pour FTP.
6. **(msg:"Connexion FTP détectée";** : Ce champ contient le message qui sera enregistré dans les logs lorsque la règle est déclenchée.
7. **flow:to\_server,established;** : Ce champ spécifie que la règle ne doit déclencher une alerte que pour les paquets TCP établis et dirigés vers le serveur.
8. **content:"serveur";** : Ce champ spécifie que la règle doit rechercher la chaîne de caractères "serveur" dans le contenu du paquet. Si cette chaîne est trouvée, la règle sera déclenchée.
9. **nocase;** : Ce champ indique que la recherche de la chaîne de caractères "serveur" ne doit pas être sensible à la casse.
10. **sid:2000001;** : C'est l'identifiant unique de la règle (Signature ID).
11. **rev:1;)** : Ce champ indique la révision de la règle.



Explications de la règle SFTP :

1. **alert** : Ce mot-clé indique que la règle générera une alerte si les conditions spécifiées sont remplies.
2. **tcp** : Cela spécifie que la règle concerne le protocole TCP, qui est utilisé pour les connexions SFTP via SSH.
3. **any any** : Le premier any indique que la règle s'applique à n'importe quelle adresse IP source. Le second any signifie que la règle s'applique à n'importe quel port source.
4. **->** : Cette flèche indique la direction du trafic, allant de la source vers la destination.
5. **any 22** : Cela spécifie que la règle s'applique à n'importe quelle adresse IP de destination, mais uniquement sur le port 22, qui est le port standard pour SSH (et donc SFTP).
6. **(msg:"Connexion SFTP détectée (via SSH)";** : Ce champ contient le message qui sera enregistré dans les logs lorsque la règle est déclenchée.+
7. **flow:to\_server,established;** : Ce champ spécifie que la règle ne doit déclencher une alerte que pour les paquets TCP établis et dirigés vers le serveur.
8. **sid:3000003;** : C'est l'identifiant unique de la règle (Signature ID). Il est utilisé pour référencer cette règle spécifique dans les logs et les rapports.
9. **rev:1;)** : Ce champ indique la révision de la règle. La révision 1 signifie que c'est la première version de cette règle.

* Détection de tentative de connexion FTP/SFTP



v

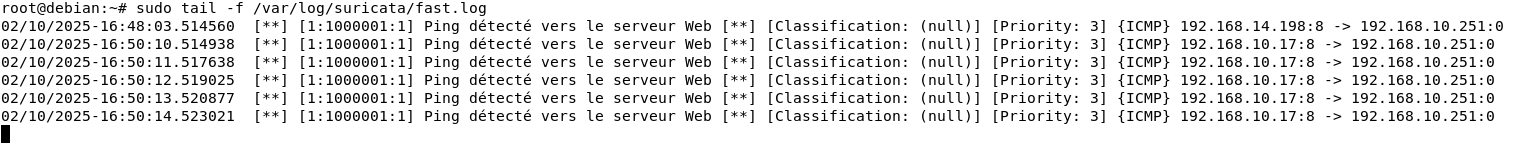
1. **alert** : Ce mot-clé indique que la règle générera une alerte si les conditions spécifiées sont remplies.
2. **tcp** : Cela spécifie que la règle concerne le protocole TCP, qui est utilisé pour les connexions FTP.
3. **any any** : Le premier any indique que la règle s'applique à n'importe quelle adresse IP source.
4. **->** : Cette flèche indique la direction du trafic, allant de la source vers la destination.
5. **192.168.10.251 21** : Cela spécifie que la règle s'applique à l'adresse IP de destination 192.168.10.251 sur le port 21, qui est le port standard pour FTP.
6. **(msg:"Tentative de connexion FTP";** : Ce champ contient le message qui sera enregistré dans les logs lorsque la règle est déclenchée.
7. **flow:to\_server,established;** : Ce champ spécifie que la règle ne doit déclencher une alerte que pour les paquets TCP établis et dirigés vers le serveur.
8. **sid:1000003;** : C'est l'identifiant unique de la règle (Signature ID).
9. **rev:1;)** : Ce champ indique la révision de la règle. La révision 1 signifie que c'est la première version de cette règle.

# **Test d’efficacité de la règle**

Test regle ping



test réalisé sur la machine test.  
En allant dans les logs de suricata, nous pouvons voir les alertes de ping !



Test de connexion FTP

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

test réalisé sur la machine test

et en allant sur les logs nous observons les alertes de connexion FTP:

Test de connexion SFTP

Une image contenant texte, capture d’écran, Police, ligne

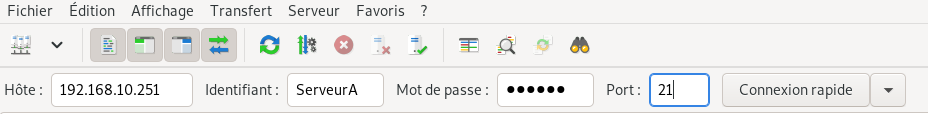
Description générée automatiquement

test réalisé sur la machine test

et en allant sur les logs nous observons les alertes de connexion SFTP:



Test de tentative infructueuse de connexion FTP



test réalisé sur la machine test

et en allant sur les logs nous observons les tentatives infructueuses de connexion FTP

