Vérifier si la sortie a changé

Dans ce cas d'utilisation, la sortie de la commande **netstat** sur un point de terminaison **Linux** est surveillée pour détecter tout changement dans les ports **TCP** écoutés. Pour ce faire, des règles sont configurées dans **Wazuh** pour générer des alertes en cas de modification détectée.

I - Vérification des changements dans la sortie de netstat

Configuration des points de terminaison Linux :

1. **Installation de netstat :** On s'assure que **netstat** est installé sur les points de terminaison **Linux** en exécutant la commande :

```
sudo apt install net-tools
```

2. **Ajout de la Configuration à ossec.conf :**
   - On accède au fichier de configuration de l'agent **Wazuh** :

```
sudo nano /var/ossec/etc/ossec.conf
```

   - On ajoute la configuration suivante dans la section **<ossec_config>** :

```
<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\
+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 == \3 == \4 \5/' | sort -k 4 -g | sed 's/ == \(.*\) ==/:\1/' | sed
1,2d</command>
  <alias>netstat listening ports</alias>
  <frequency>360</frequency>
</localfile>
```

Cette configuration convertit la sortie de **netstat** en un format lisible par **Wazuh** pour la surveillance.

3. **Redémarrage de l'Agent Wazuh :** Une fois la configuration ajoutée, on redémarre le service de l'agent **Wazuh** pour appliquer les modifications :

```
sudo systemctl restart wazuh-agent
```

II – Configuration du Serveur Wazuh

Règle Prête à l'Emploi : Wazuh propose une règle prête à l'emploi avec l'ID 533 pour générer des alertes en cas de changement dans les ports écoutés de **netstat**. La règle est déjà disponible dans **Wazuh**.

III – Test de configuration

Pour tester la configuration et déclencher une alerte :

1. **Modification du fichier ssh_config:**
   - On édite le fichier de configuration **ssh_config** sur un des points de terminaison **Linux** :

```
sudo nano /etc/ssh/ssh_config
```

   - On ajoute le port 2021 comme nouveau port SSH :

```
#Port 22
Port 2021
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

2. **Redémarrage du Service SSH :** Après avoir modifié le fichier, on redémarre le service SSH pour appliquer les changements :

```
sudo systemctl restart ssh
```

Vérifier si la sortie a changé

Visualisation des Alertes :

On accède à l'onglet « **Modules** » > « **Security Events** » sur le tableau de bord **Wazuh** pour visualiser l'alerte montrant les changements dans le réseau.