Détection des processus non autorisés avec Wazuh

La fonctionnalité de surveillance des commandes **Wazuh** permet d'exécuter des commandes sur un point de terminaison et de surveiller les résultats.

I – Configuration du point de terminaison Linux

1. On ajoute le bloc de configuration suivant au fichier **/var/ossec/etc/ossec.conf** de l'agent **Wazuh** pour obtenir périodiquement une liste des processus en cours d'exécution :

```
<ossec_config>
  <localfile>
    <log_format>full_command</log_format>
    <alias>process list</alias>
    <command>ps -e -o pid,uname,command</command>
    <frequency>30</frequency>
  </localfile>
</ossec_config>
```

2. On redémarre l'agent **Wazuh** pour appliquer les modifications :

```
systemctl restart wazuh-agent
```

II – Configuration du serveur Wazuh

1. On ajoute les règles suivantes au fichier **/var/ossec/etc/rules/local_rules.xml** sur le serveur **Wazuh** :

```
<group name="ossec,">
  <rule id="100050" level="0">
    <if_sid>530</if_sid>
    <match>^ossec: output: 'process list'</match>
    <description>Liste des processus en cours d'exécution.</description>
    <group>process_monitor,</group>
  </rule>

  <rule id="100051" level="7" ignore="900">
    <if_sid>100050</if_sid>
    <match>nc -l</match>
    <description>Netcat à l'écoute de connexions entrantes.</description>
    <group>process_monitor,</group>
  </rule>
</group>
```

2. On redémarre le gestionnaire **Wazuh** pour appliquer les modifications :

```
.sudo systemctl restart wazuh-manager
```

Test : Émulation d'Attaque

1. Sur le point de terminaison **Linux** surveillé, on exécute la commande suivante pendant 30 secondes :

```
nc -l 8000
```

2. On visualise les données d'alerte dans le tableau de bord **Wazuh** en accédant au module « **Security Events** ».

Détection des processus non autorisés avec Wazuh

27 mars 2024 à 16:21:44.076 netcat écoute les connexions entrantes. 7 100051

Document développé Afficher les documents environnants Afficher un seul document

Tableau JSON

t _indice	wazuh-alerts-4.x-2024.03.27
t agent.id	009
t agent.ip	192.168.4.42
t nom d'agent	test1-wazuh-agent
t décodeur.nom	ossec
t journal_complet	ossec : sortie : 'liste de processus' : COMMANDE UTILISATEUR PID 1 racine /sbin/init 2 racine [kthreadd] 3 racine [rcu_gp] 4 racine [rcu_par_gp] 5 racine [slub_flushwq] 6 racine [netns] 10 racine [mm_percpu_wq] 11 racine [rcu_tasks_kthread] 12 racine [rcu_tasks_rude_kthread] 13 racine [rcu_tasks_trace_kthread] 14 racine [ksoftirqd/0] 15 racine [rcu_preempt] 16 racine [migration/0] 18 racine [cpuhp/0] 20 racine [kdevtmpfs] 21 racine [inet_frag_wq] 22 racine [kauditd] 23 racine [khungtaskd] 24 racine [oom_reaper] 27 racine [writeback] 28 racine [kcompactd0] 29 racine [ksmd] 30 racine [khugepaged] 31 racine [kintegrityd] 32 racine [kblockd] 33 racine [blkcg_punt_bio] 34 racine [tpm_dev_wq] 35 racine [edac-poller] 36 racine [devfreq_wq] 37 racine [kworker/0:1H-kblockd] 38 racine [kswapd0] 44 racine [kthro
t identifiant	1711552904.2892498
t type d'entrée	enregistrer
t emplacement	liste des processus
t manager.nom	serveur wazuh
t règle.description	netcat écoute les connexions entrantes.