

Surveillance de l'exécution de commandes malveillantes

Dans cette configuration, on met en place l'outil **d'audit** natif **d'Ubuntu**, **Auditd**, pour surveiller les commandes exécutées sur un point de terminaison. On utilise **Wazuh** pour alerter sur les activités suspectes détectées par **Auditd**.

I – Configuration du point de terminaison Ubuntu

1. Installation et activation **d'Auditd** :

- On exécute les commandes suivantes pour installer **Auditd** sur le point de terminaison **Ubuntu** :

```
sudo apt -y install auditd
sudo systemctl start auditd
sudo systemctl enable auditd
```

2. On ajoute les règles d'audit dans **/etc/audit/audit.rules** :

```
echo "-a exit,always -F auid=1000 -F egid!=994 -F auid!=-1 -F arch=b32 -S execve -k audit-wazuh-c" >>
/etc/audit/audit.rules
echo "-a exit,always -F auid=1000 -F egid!=994 -F auid!=-1 -F arch=b64 -S execve -k audit-wazuh-c" >>
/etc/audit/audit.rules
```

3. On actualise les règles :

```
sudo auditctl -R /etc/audit/audit.rules
sudo auditctl -l
```

4. On ajoute la configuration ci-dessous dans **/var/ossec/etc/ossec.conf** pour permettre à **Wazuh** de lire les logs **d'Auditd** :

```
<localfile>
  <log_format>audit</log_format>
  <location>/var/log/audit/audit.log</location>
</localfile>
```

5. On redémarre l'agent **Wazuh** :

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

II – Configuration de l'agent Wazuh

1. On examine les paires clé-valeur dans le fichier de recherche **/var/ossec/etc/lists/audit-keys** :

```
cat /var/ossec/etc/lists/audit-keys
```

Résultat attendu :

```
audit-wazuh-w:write
audit-wazuh-r:read
audit-wazuh-a:attribute
audit-wazuh-x:execute
audit-wazuh-c:command
```

Note :

La liste **CDB** est constituée de paires clé-valeur séparées par des deux-points. **Wazuh** permet la gestion de ces listes pour des recherches hautes performances, nécessitant une compilation dans un format binaire spécial. Après création et ajout à la configuration **Wazuh**, les règles peuvent être configurées pour rechercher les champs correspondants dans ces listes lors de la détection d'activités suspectes.

Surveillance de l'exécution de commandes malveillantes

- On édite une nouvelle liste CDB `/var/ossec/etc/lists/suspicious-programs` et on ajoute le contenu suivant :

```
ncat:yellow
nc:red
tcpdump:orange
```

- On ajoute la liste à la section `<ruleset>` du fichier `/var/ossec/etc/ossec.conf` du serveur **Wazuh** :

```
<list>etc/lists/suspicious-programs</list>
```

- On crée une règle de gravité élevée à déclencher lorsqu'un programme « rouge » est exécuté. On ajoute cette nouvelle règle au fichier `/var/ossec/etc/rules/local_rules.xml` sur le serveur **Wazuh**.

```
<group name="audit">
  <rule id="100210" level="12">
    <if_sid>80792</if_sid>
    <list field="audit.command" lookup="match_key_value" check_value="red">etc/lists/suspicious-programs</list>
    <description>Audit: Highly Suspicious Command executed: $(audit.exe)</description>
    <group>audit_command,</group>
  </rule>
</group>
```

- On redémarre le gestionnaire **Wazuh** :

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

III – Émulation de l'attaque

- On installe et exécute le programme **netcat** sur le point de terminaison **Ubuntu** :
 - On utilise la commande ping pour simuler une activité réseau depuis le serveur **Wazuh** :

```
sudo apt -y install netcat
nc -v
```

- On visualise les alertes :
 - On accède au tableau de bord **Wazuh** et consultez les alertes générées dans le module **Security Events** (en utilisant les filtres appropriés = facultatif).

Temps ▾	règle.description	règle.niveau	règle.id
> 28 mars 2024 à 13:30:26.996	Audit : Commande hautement suspecte exécutée : /usr/bin/nc	12	100210
> 28 mars 2024 à 13:29:50.957	Audit : Commande hautement suspecte exécutée : /usr/bin/nc	12	100210
> 28 mars 2024 à 13:29:10.921	Audit : Commande hautement suspecte exécutée : /usr/bin/nc	12	100210
> 28 mars 2024 à 13:26:52.786	Audit : Commande hautement suspecte exécutée : /usr/bin/nc	12	100210

Commandes suspectes exécutées