Evènements de sécurité

Jean-Marc Pouchoulon

novembre 2025

Lorsqu'une intrusion a lieu il est essentiel de pouvoir en analyser les causes. Il faut donc s'assurer que des outils pré-deployés sur vos serveurs permettent de tracer les actions des attaquants. Les agents installés et remontant les informations sur les SIEM peuvent se nourrir des événements de sécurité générés par les outils de détection et de réponse déployés sur vos systèmes. Ebpf est une technologie du kernel Linux récente qui permet de tracer les actions des utilisateurs et des processus en profondeur. Sous Linux, les outils les plus courants sont: *auditd, sysmon, kunai, falco* Pour Windows *Sysmon* est l'outil de référence mais il n'est pas supporté par Microsoft et il est fait ici abstraction des EDR (Endpoint Detection and Response) commerciaux.

Vous travaillerez avec une machine Debian et une machine Windows >= 10.

1 Installation d'auditd

Installer auditd

- Le daemon "auditd" sous Linux qui permet de recueillir des informations sur les fichiers et les processus.
- Sysmon qui est aussi disponible sous Linux et qui est un outil de surveillance complémentaire à auditd.
- Suricata qui est embarqué par défaut dans TPOT et permet de détecter des attaques réseaux.

Docker limite le nombre de pull d'images. Vous pourriez être bloqué lors de l'installation. Si c'est le cas éditez le fichier .env sous la directory /home/tsec/tpotce et remplacez la ligne suivante:

TPOT_REPO=dtagdevsec par TPOT_REPO=ghcr.io/telekom-security

afin d'utiliser le registry de deutch-telekom plutôt que le registry de la société "Docker".

Relancez l'installation.

2 Installation et utilisation du SIEM Wazuh

2.1 Configuration de Wazuh et de son agent sur la machine TPOT

Récupérez et lancez la VM de Wazuh récupérable ici. [1]

1. User Admin password Admin

Wazuh se protège des attaques par dictionnaire en utilisant fail2ban sur son service SSH.

Si vous êtes bloqué par fail2ban, vous pouvez modifier le fichier /etc/fail2ban/jail.d/tpot.conf afin de vous "white-lister". Relancez ensuite le service fail2ban.

2.2 Configuration de Suricata dans TPOT

Suricata fonctionne d'office dans TPOT. C'est un container accessible via les commandes suivantes:

```
# connexion au tpot avec le compte tsec avec le "vrai ssh" :
ssh -p 64295 tsec@IP_TPOT
# connexion au container suricata
docker exec -it suricata sh
```

Ses logs sont partagés avec le système hôte dans le répertoire data/suricata/log.

Une fois connecté dans le container vous pouvez charger les règles de détection de Suricata avec les commandes suivantes:

```
# maj des listes
suricata-update list-sources
suricata-update update-sources
suricata-update list-enabled-sources
suricata-update enable-source oisf/trafficid
suricata-update enable-source etnetera/aggressive
suricata-update enable-source sslbl/ssl-fp-blacklist
suricata-update enable-source et/open
suricata-update enable-source tgreen/hunting
suricata-update enable-source sslbl/ja3-fingerprints
suricata-update enable-source ptresearch/attackdetection
suricata-update --no-test


# les règles sont stockées dans  /usr/share/suricata/rules/ mais lues dans Loading rule file: /var/lib/suricata/rules/suricata.rules

# reload
suricatasc -c reload-rules
```

2.3 installez un agents wazuh sur la machine TPOT ainsi que sur une machine Windows

3 Génération d'évènements de sécurité

Après avoir fait valider votre installation par l'enseignant, vous lancerez des attaques sur les ports 22, 23, 25, 21, 80 et vous en vérifierez l'impact sur les tableaux de bord du honeypot en particulier sur le "dashboard" de Suricata.

Vous ferez constater à l'enseignant le résultat en mettant en rapport attaques et logs et vous en ferez un compte-rendu.

4 Wazuh et active response

Utilisez "active-response" `https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force.html` afin de générer des règles Netfilter sur la machine Linux monitorée.

C'est un exemple d'automatisation de réponse à une attaque (SOAR).