Monitoring d'un Honeypot TPOT avec Wazuh

Jean-Marc Pouchoulon

octobre 2023

Les honeypots comme TPOT permettent d'avoir une idée de la menace qui pèse sur vos réseaux. TPOT est composé de multiples Honeypot packagés sous forme de containers Docker. Il est important de les surveiller et de les analyser afin de comprendre les attaques et de pouvoir les contrer.

Wazuh est un SIEM, qui dans ce TP va avoir pour missions de surveiller le TPOT: il pourrait être une cible pour les attaquants.

Le daemon "auditd" sous Linux permet de recueillir des informations sur les fichiers et les processus à l'instar de sysmon sous Windows.

Sysmon c'est aussi sous Linux et c'est un outil de surveillance complémentaires à auditd.

Suricata est embarqué par défaut dans TPOT et permet de détecter des attaques réseaux.

1 Installation de l'Honeypot TPOT

Vous installerez "TPOT" (voir `https://github.com/telekom-security/tpotce`) sur une VM avec l'Hyperviseur Kvm de préférence. 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.

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]

Sur l'honeypot TPOT installez:

- OSquery voir `https://osquery.readthedocs.io/en/stable/installation/install-linux/`
- Le daemon auditd (installation par package) en utilisant la configuration de l'ANSSI. L'article suivant vous aidera à configurer auditd et à en vérifier son bon fonctionnement. La configuration d'auditd par l'ANSSI est disponible dans le document suivant ici.
- Installez l'agent Wazuh sur la VM TPOT `https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html`

1. User Admin password Admin

— Vérifiez que la conformité et les évènements de sécurité apparaissent bien sur la console Wazuh.
— Faites de même avec un VM windows (installez l'agent via "chocolatey")

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


# 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
```

3 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