[Debian] ELK

Introduction

La suite **ELK** pour **Elastic Logstash et Kibana** est un ensemble d'outil de sécurité qui permettent de collecter, indexer, parser et afficher les logs.

Ces outils sont complémentaires et primordiaux pour la **blue team**.

Sources

- Documentation officielle - Installation Elasticsearch
- Documentation officielle - Installation Logstash
- Documentation officielle - Installation Kibana

Installation

Prérequis

Tout d'abord, il faut importer la **clé GPG** pour être en mesure d'installer les outils de la suite ELK :

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg && apt-get install apt-transport-https && echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-7.x.list && apt-get update
```

Elasticsearch

Voici la commande pour installer **Elasticsearch** :

```
apt install -y elasticsearch
```

Démarrez et activez le service elasticsearch :

```
systemctl enable --now elasticsearch
```

> La configuration globale d'elasticsearch se trouve dans le fichier **/etc/elasticsearch/elasticsearch.yml** .

Ensuite, configurez le mot de passe de l'utilisateur **elastic** grâce à cette commande :

```
/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic -i
```

> Le service est désormais disponible depuis le navigateur en vous rendant sur **https://<IP>:9200** .

Logstash

Voici la commande pour installer **Logstash** :

```
apt install -y logstash
```

> Logstash peut être configuré à travers le fichier **/etc/logstash/conf.d/beats.conf** .

Démarrez et activez le service logstash :

```
systemctl enable --now logstash
```

> Le service est désormais disponible sur le port**5044** .

Filebeat

Voici la commande pour installer **Filebeat** :

```
apt install -y filebeat
```

> Logstash peut être configuré à travers le fichier **/etc/filebeat/filebeat.yml** .

Démarrez et activez le service filebeat :

```
systemctl enable --now filebeat
```

Kibana

Voici la commande pour installer **Kibana** :

```
apt install -y kibana
```

> Kibana peut être configuré à travers le fichier **/etc/kibana/kibana.yml** .

Démarrez et activez le service kibana :

```
systemctl enable --now kibana
```

> Le service est désormais disponible sur l'url **http://<IP>:5601** .

Pour activer Kibana, il vous sera demandé un token d'enrollement qui peut être généré grâce à la commande suivante :

```
/usr/share/kibana/bin/kibana-verification-code
```

Ensuite, un code de vérification vous sera demandé, tapez cette commande pour l'obtenir :

```
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```

Revision #7
Created 28 December 2023 20:05:59 by Elieroc
Updated 29 December 2023 14:29:11 by Elieroc