Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash

Installation, Configuration & Simulations

Réalisé par :

- Diaby Aboubacar Sidik

- Edi aka ovo samira

- Traore Lopongsi Thierry Kevin

Encadré par:

Dr Diako

SOMMAIRE

1) Prérequis :
   - Serveur principal : Ubuntu Server 24.04 – 8 Go de RAM, 4 processeurs
   - Poste client Linux : Ubuntu Desktop (agents : Filebeat, Auditbeat, Packetbeat)
   - Poste client Windows : Windows 10 (agent : Winlogbeat)
   - Poste d'attaque : Kali Linux (pour tester Packetbeat via des attaques réseau)
2) Étape 1 : Installation et configuration d'Elasticsearch
   - Ajout de la liste des sources de paquets Elastic.

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch |sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg

   - Ensuite, l'ajout de la liste des sources Elastic au sources.list.drépertoire, où APT recherchera de nouvelles sources :

echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

   - Mise à jour des paquets

sudo apt update

   - Installation Elasticsearch

sudo apt install elasticsearch

   - Modifier le fichier de configuration principal d'Elasticsearch. ***elasticsearch.yml***

sudo nano /etc/elasticsearch/elasticsearch.yml

```
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 192.168.145.131
discovery.type: single-node
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
```

   - Démarrez le service Elasticsearch avec systemctl

sudo systemctl start elasticsearch

- pour permettre à Elasticsearch de démarrer à chaque démarrage de notre serveur

sudo systemctl enable elasticsearch

- Envoie de requête http pour voir si Elasticsearch fonctionne

curl -X GET "192.168.145.131:9200"

3) Étape 2 : Installation et configuration de kibana
   - Installer de Kibana

sudo apt install kibana

- activez et démarrez le service Kibana

sudo systemctl enable kibana

sudo systemctl start kibana

- Commande suivante créera l'utilisateur et le mot de passe d'administration Kibana et les enregistrera dans le htpasswd.users (Installer nginx au préalable)

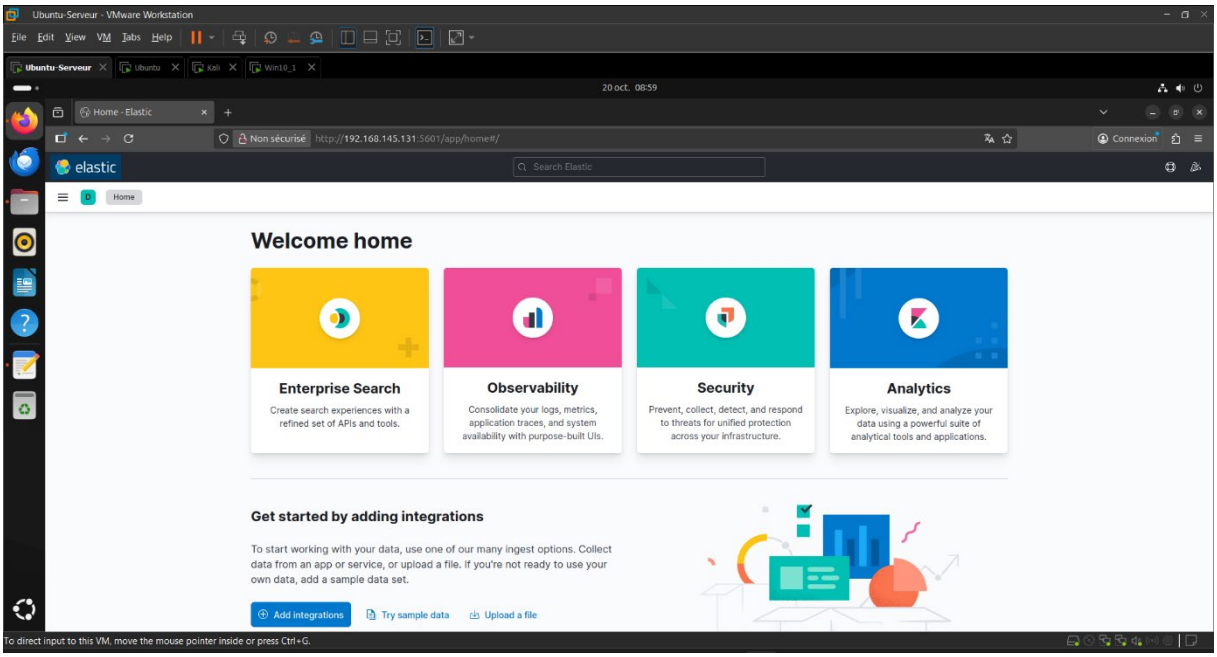
echo "kibanaadmin:`openssl passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users

- Fichier de config de kibana kibana.yml

Sudo nano /etc/kibana/kibana.yml

```
# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name.  This is used for display purposes.
server.name: "your-hostname"
server.host: "192.168.145.131"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.145.131:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"
```

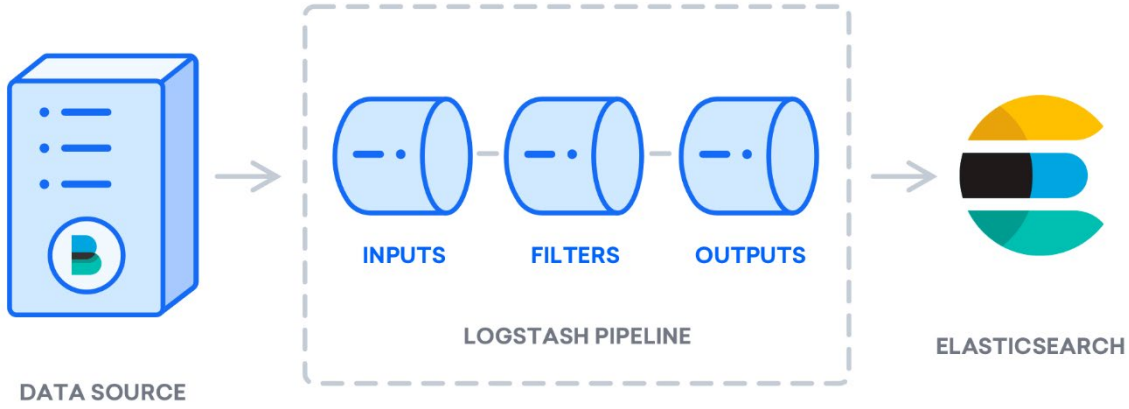
Accéder à Kibana : http://192.168.145.131:5601



4) Étape 3 : Installation et configuration de Logstash

- Installez Logstash avec cette commande :

sudo apt install logstash



- Fichier de configuration des Beats 02-beats-input.conf

sudo nano /etc/logstash/conf.d/02-beats-input.conf

```
input {
  beats {
    port => 5044
  }
}

filter {
  if [winlog] {
    if [winlog][event_id] == 4625 {
      mutate {
        add_tag => ["failed_login", "security"]
      }
    }
  }

  if [fileset][module] == "system" and [fileset][name] == "auth" {
    if "failure" in [message] or "failed" in [message] {
      mutate {
        add_tag => ["failed_login", "security"]
      }
    }
  }

  if [fileset][module] == "packetbeat" {
    mutate {
      add_tag => ["network", "packetbeat"]
    }
  }
```

```
  if [fileset][module] == "auditbeat" {
    mutate {
      add_tag => ["audit", "security"]
    }
  }

  if [source][ip] {
    geoip {
      source => "source.ip"
      target => "geoip"
      add_field => ["[geoip][coordinates]", "%{[geoip][longitude]}"]
    }
  }
}

output {
  elasticsearch {
    hosts => ["http://192.168.145.131:9200"]
    index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
  }

  stdout {
    codec => rubydebug
  }
}
```

- Demarrez logstash

sudo systemctl start logstash

sudo systemctl enable logstash

5) Étape 4 : Installation et configuration des beats

- Installation

La suite Elastic utilise plusieurs outils de transfert de données légers appelés Beats pour collecter des données provenant de diverses sources et les transférer vers Logstash ou Elasticsearch. Voici les Beats actuellement disponibles chez Elastic :

- Filebeat : collecte et expédie les fichiers journaux.
- Metricbeat : collecte les métriques de vos systèmes et services.
- Packetbeat : collecte et analyse les données du réseau.
- Winlogbeat : collecte les journaux d'événements Windows.
- Auditbeat : collecte les données du framework d'audit Linux et surveille l'intégrité des fichiers.
- Heartbeat : surveille la disponibilité des services avec un sondage actif.

Dans notre cas, nous utiliserons :

- Filebeat, Auditbeat et Packetbeat sur Ubuntu Desktop
- Winlogbeat sur Windows 10

- Installation des Beats (Ubuntu)

sudo apt install filebeat auditbeat packetbeat -y

- Installation de Winlogbeat (Windows 10)

Télécharger l'archive ZIP

Extraire le contenu dans : `C:\Program Files\Winlogbeat`

- Fichier de configuration de chaque agent beats :

/etc/filebeat/filebeat.yml

```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.145.131:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

/etc/auditbeat/auditbeat.yml

/etc/packetbeat/packetbeat.yml

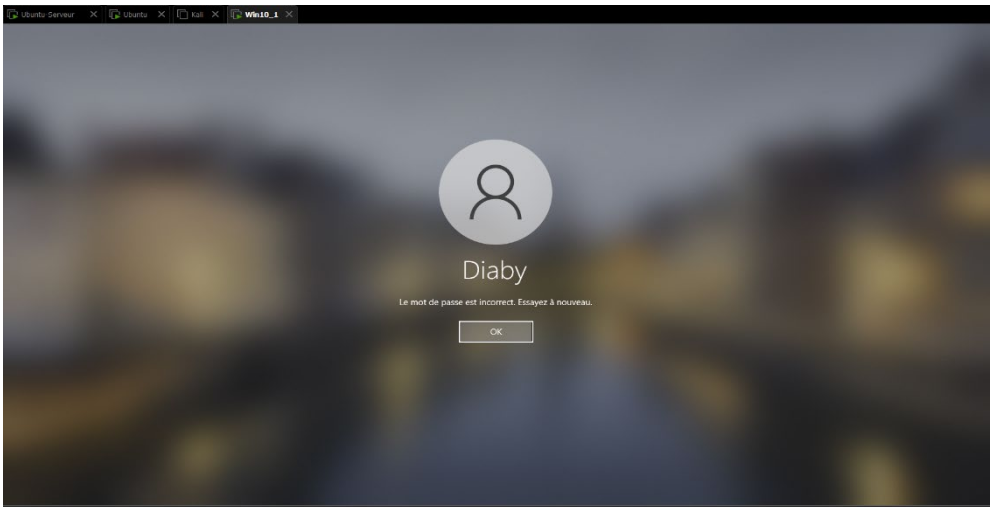
C:\Program Files\Winlogbeat\winlogbeat.yml

6) Etape 5 : Simulations (tests et vérifications)

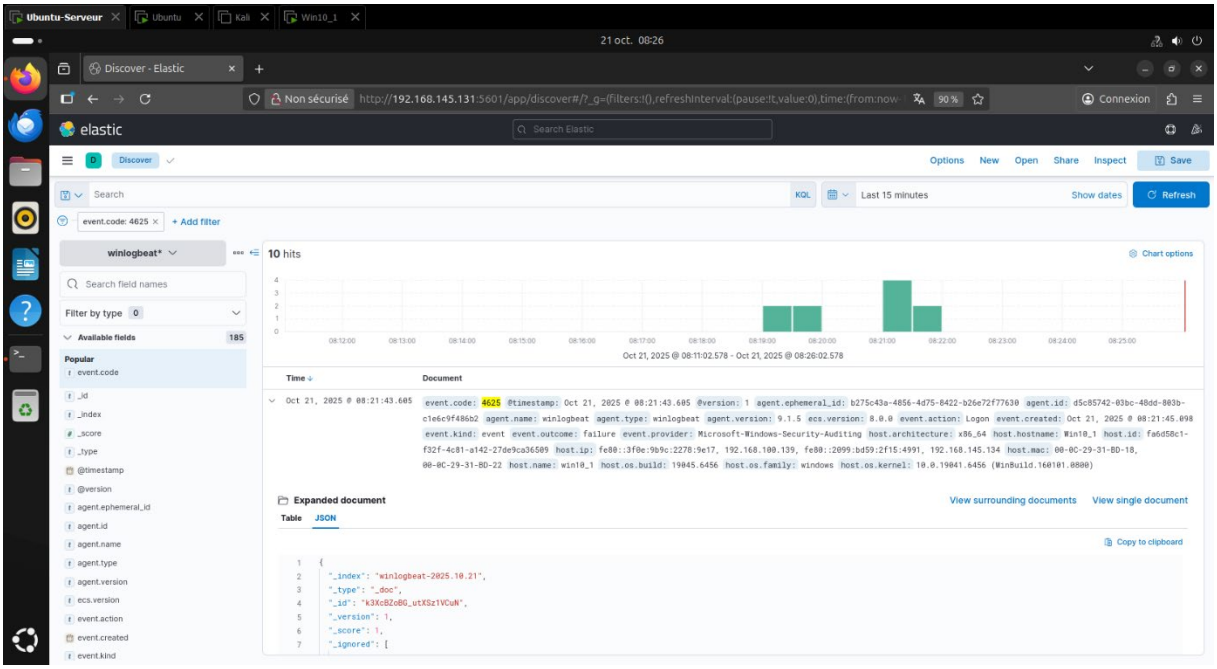
- **Simuler tentatives de connexion échouées (Windows)**

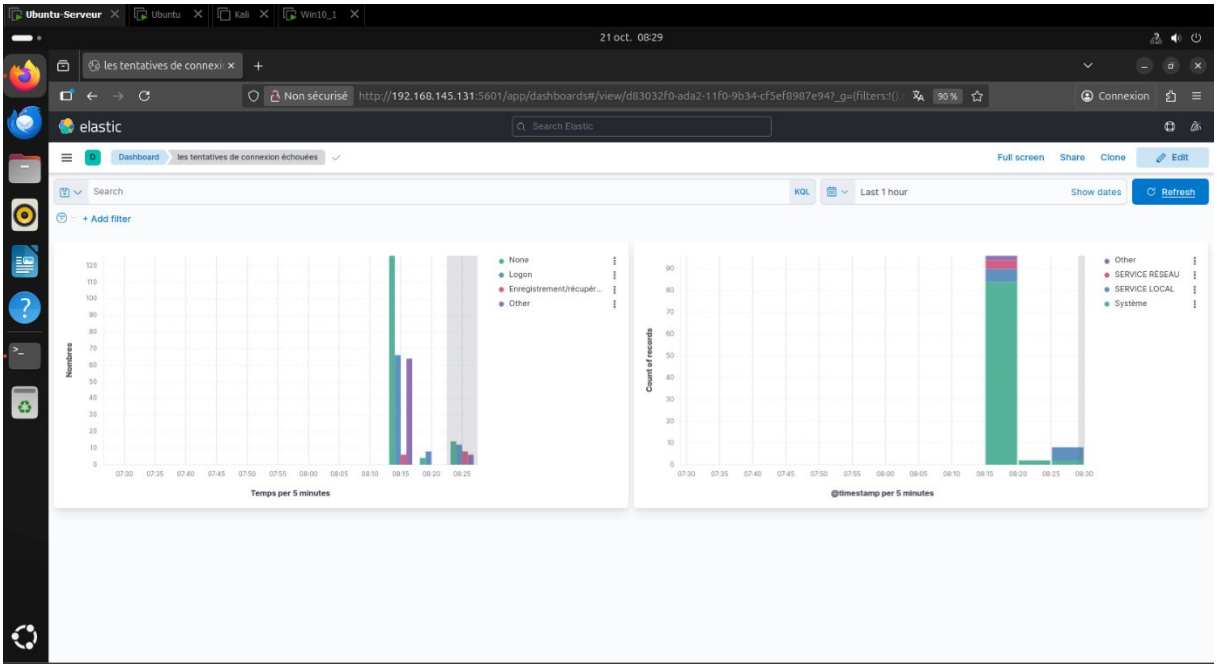
But : générer des **EventID 4625** visibles par **Winlogbeat**

Sur la machine Windows 10 (exécuter plusieurs fois) :



Résultat attendu : événements 4625 listés ; Dashboard “Échecs de connexion“

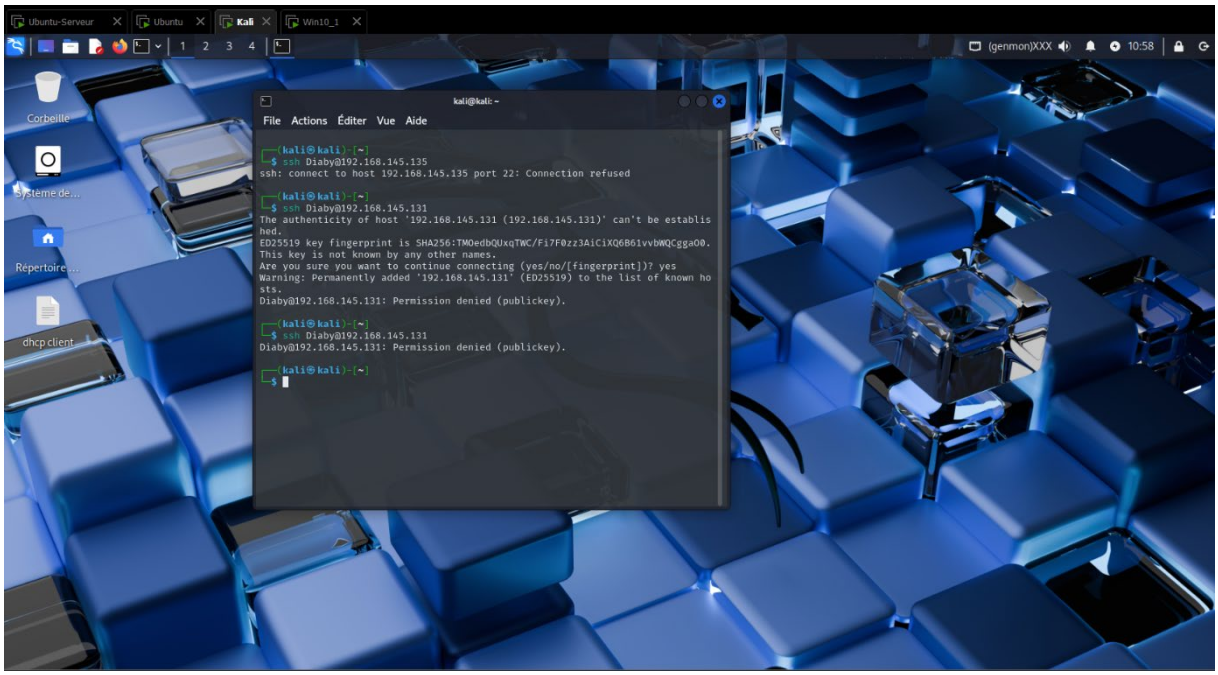




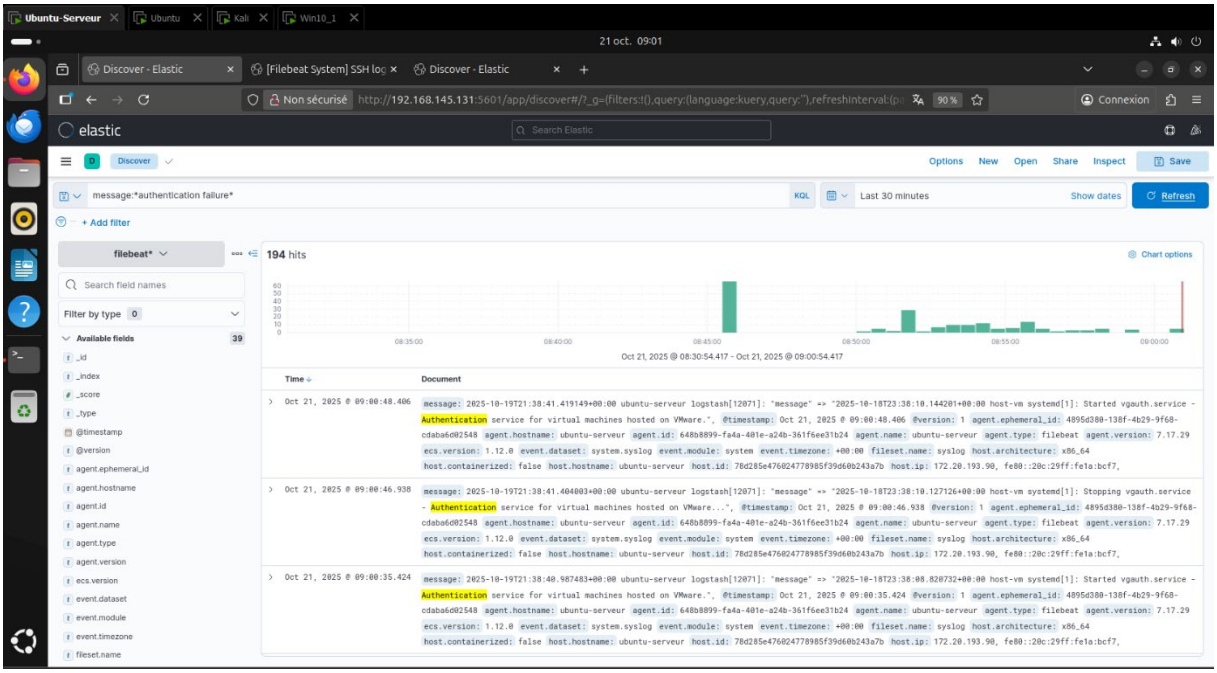
- **Simuler tentatives échouées (Linux SSH)**

But : générer des logs d’échec SSH dans /var/log/auth.log et les voir via Filebeat.

Sur la machine attaquante (Kali) :



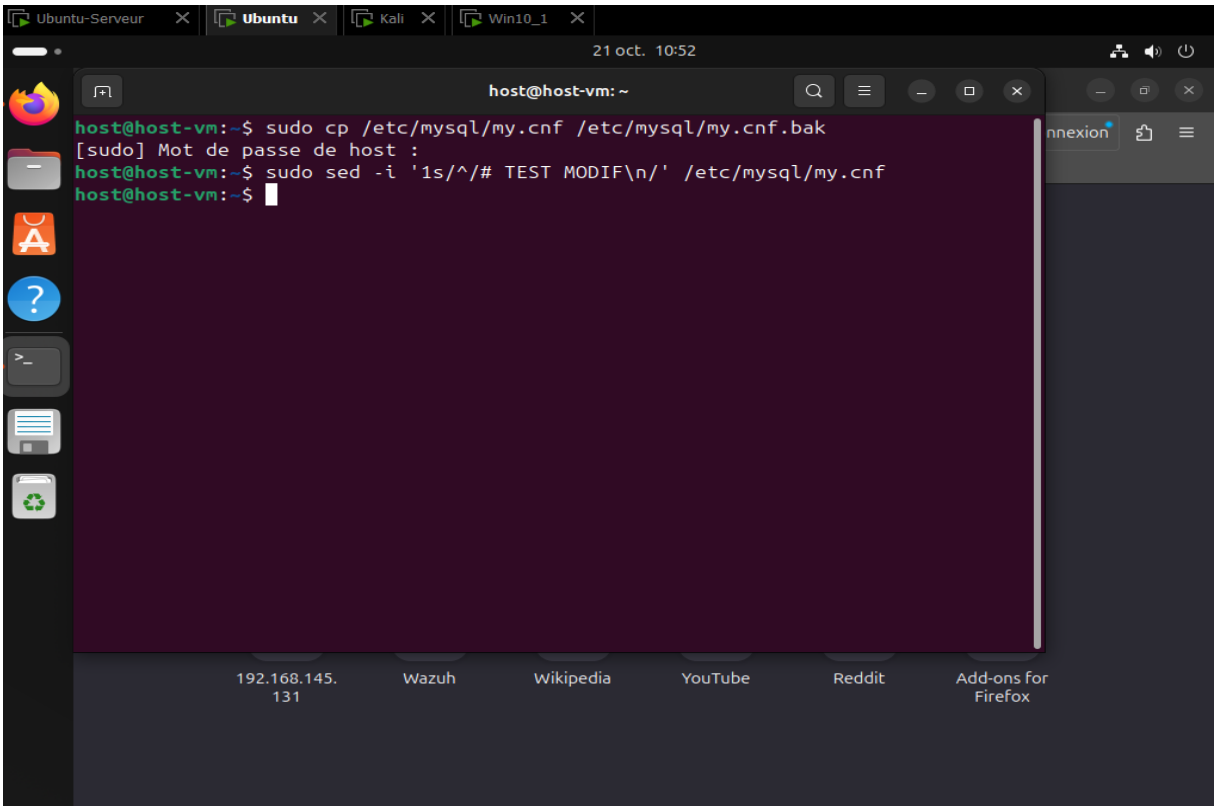
Résultat attendu : événements d'échec SSH visibles (message:*authentication failure*)



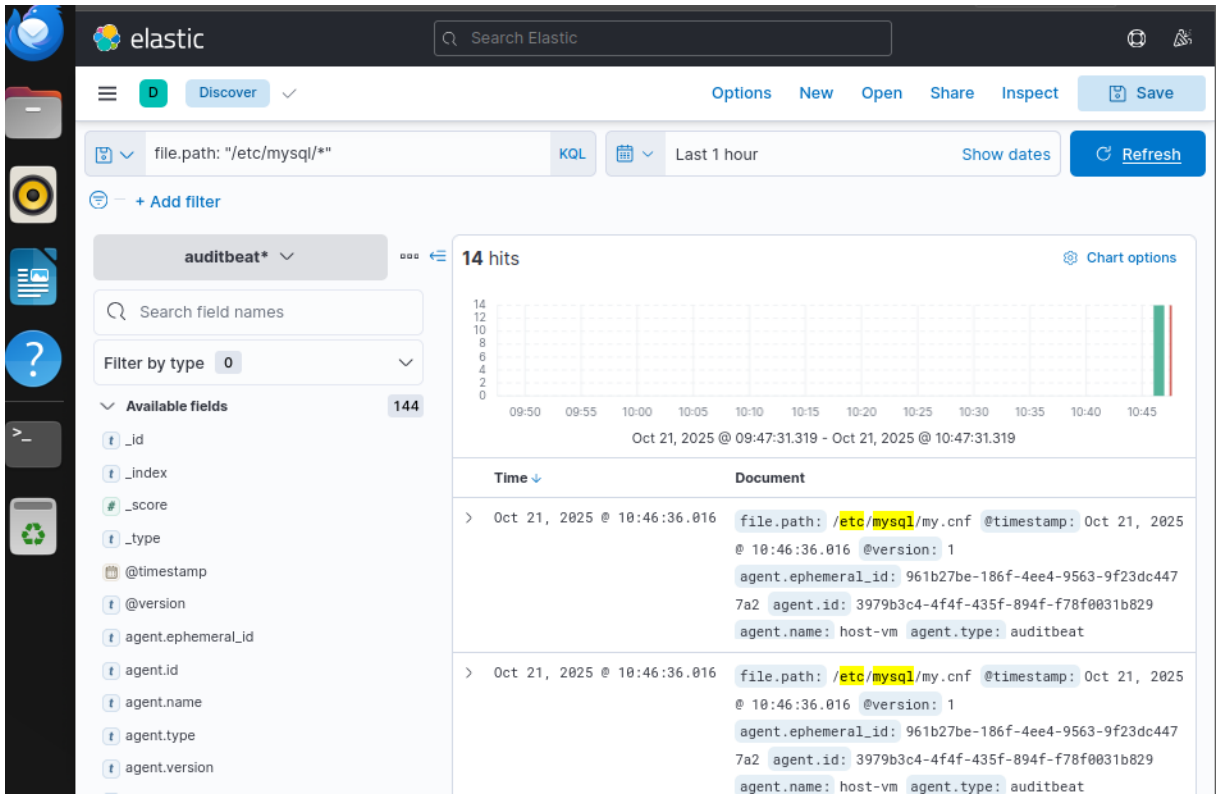
- **Simuler changement de configuration DB**

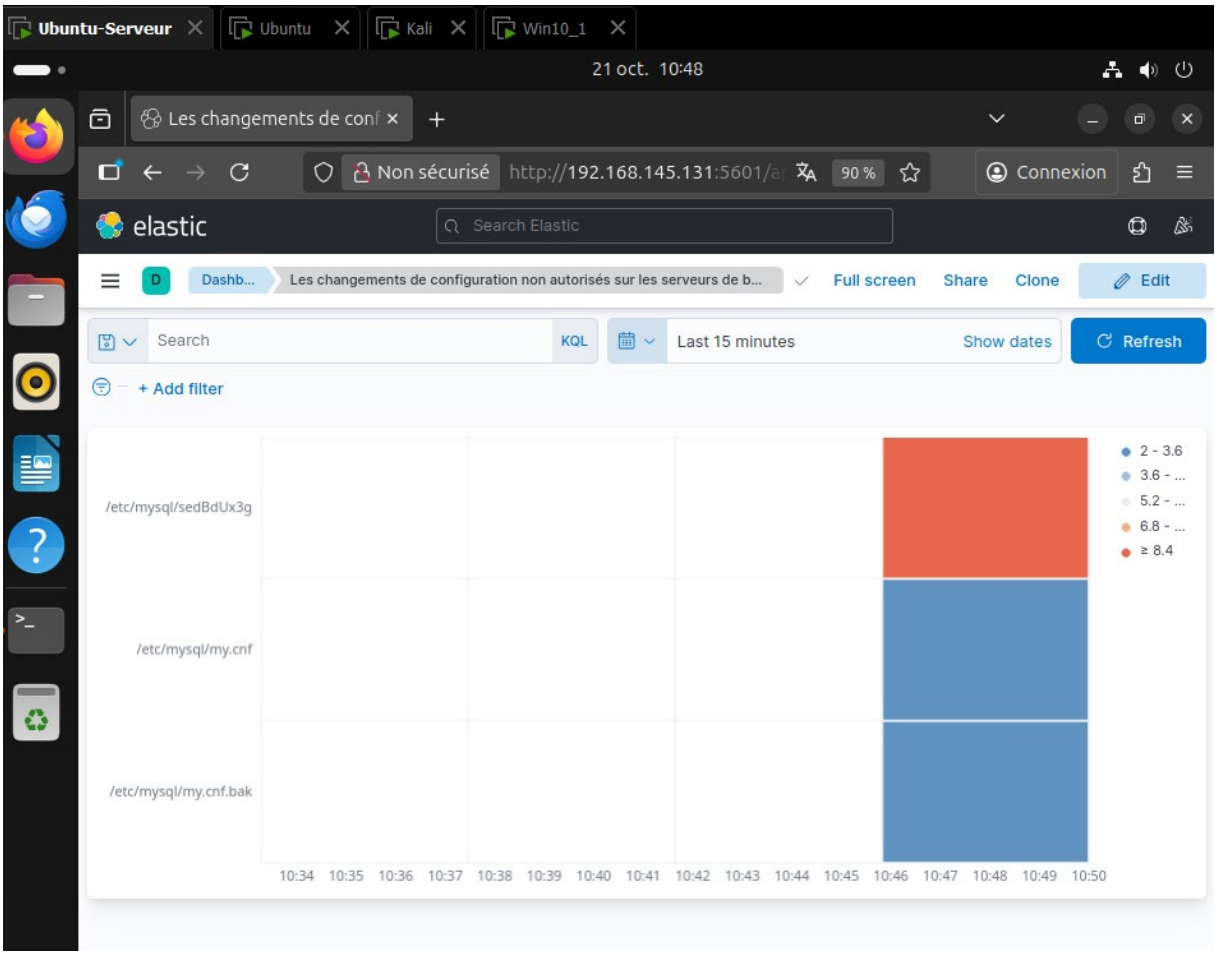
But : produire un événement FIM (File Integrity Monitoring).

Sur la machine DB (Ubuntu) :



Résultat attendu : événement change ou modified listé (file.path: "/etc/mysql/*") ; Dashboard “Changements de configuration non autorisés sur les serveurs de base de données.”

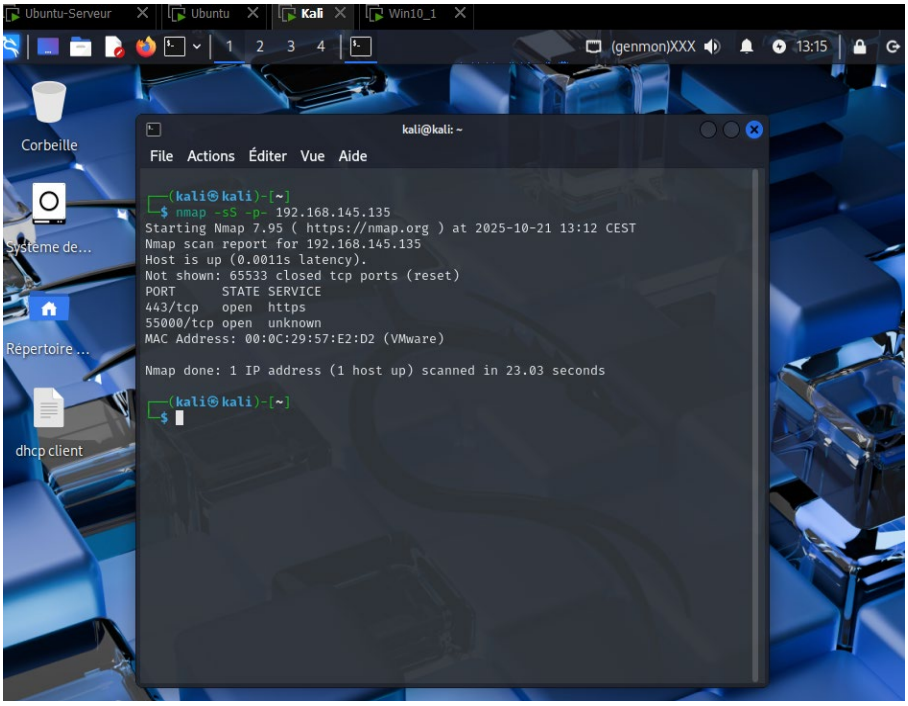




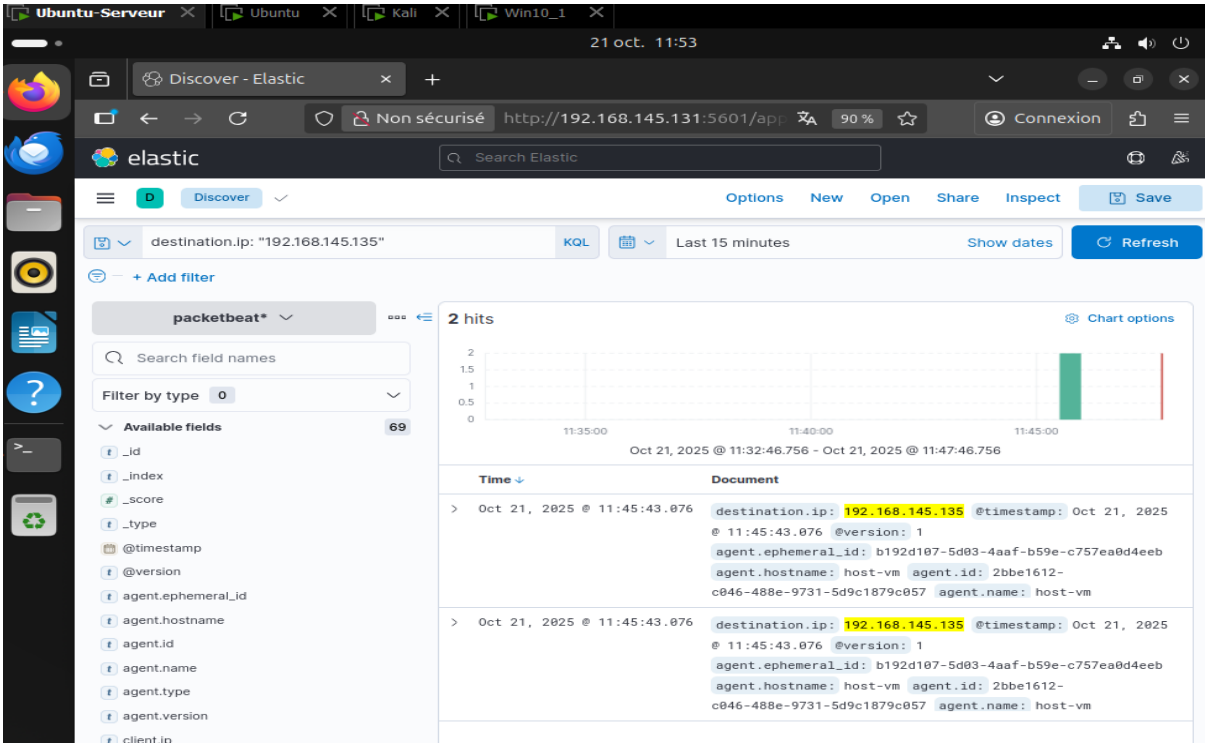
- **Simuler scan réseau (packetbeat)**

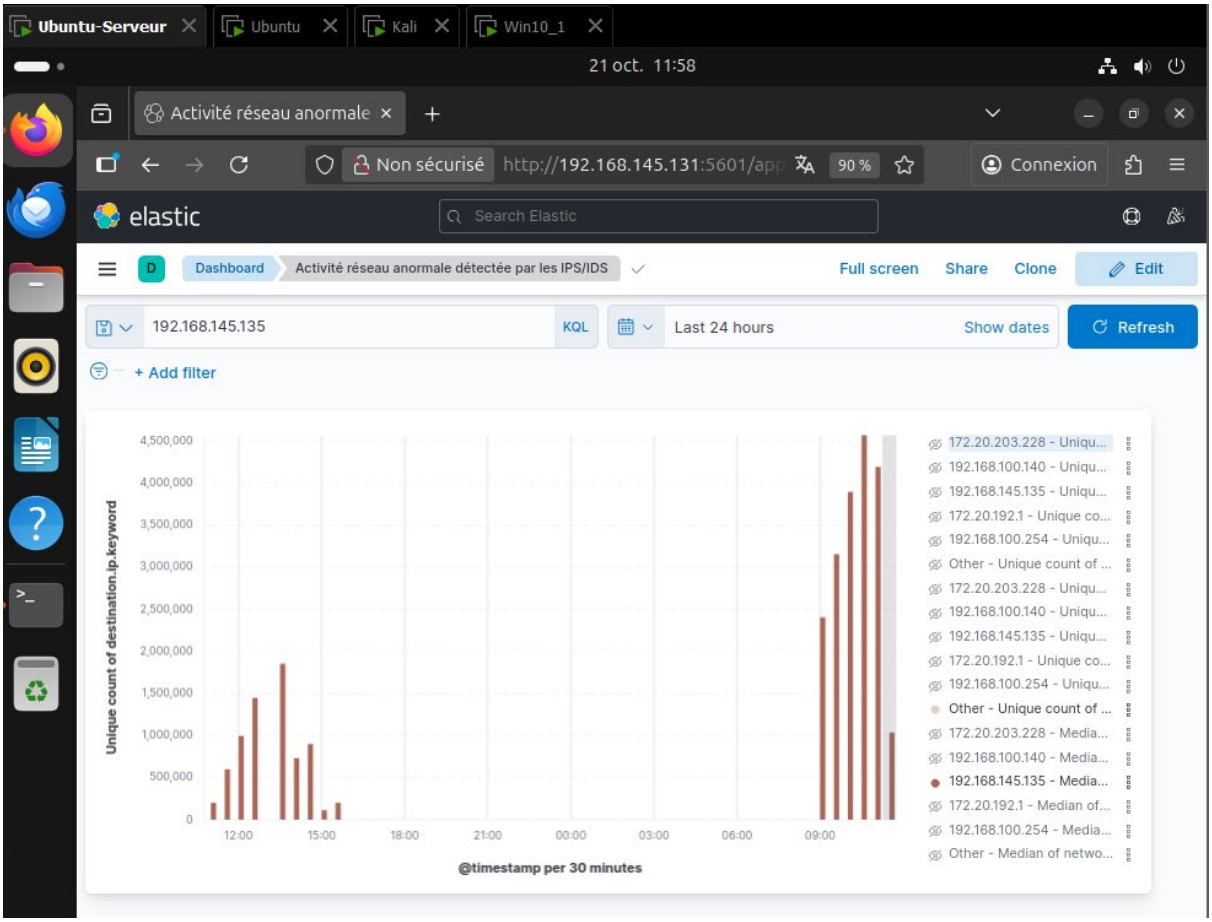
But : détection d'anomalies réseau

Sur une machine attaquante (kali) :



Résultat attendu : Trafic vers la cible (destination.ip: "192.168.145.135") ; dashboard “Activité réseau anormale détectée”





7) Résultats attendus

- Dashboards Kibana :
  - “Échecs de connexion” (EventID 4625 + logs SSH échoués)
  - “Activité réseau anormale détectée” (Packetbeat : scans, trafic suspect)
  - “Changements de configuration non autorisés sur les serveurs de base de données” (Auditbeat FIM)
- Flux de données : Beats → Logstash → Elasticsearch → Kibana
- Alertes/visualisations opérationnelles basées sur les indices et les champs (**event.code**, **destination.ip**, **file.path**, **winlog.event_id**)