**SIEM Implimentation(Wazuh + ELK)**

**Objective**

The objective of this report is to explore the implementation of a SIEM (Security Information and Event Management) system by integrating ELK (Elasticsearch, Logstash, and Kibana) with Wazuh for enhanced security monitoring. The report details the setup of the SIEM environment, the execution of a DoS attack using hping3, and the analysis of security events captured in the Wazuh event dashboard. This project aims to demonstrate the effectiveness of SIEM solutions in detecting and responding to cybersecurity threats in real time.

**Introduction**

In today's evolving cybersecurity landscape, organizations face constant threats, including Denial-of-Service (DoS) attacks, which can disrupt services and cause significant downtime. SIEM solutions play a crucial role in real-time threat detection, log management, and incident response.

This report focuses on implementing a SIEM solution using Wazuh integrated with ELK to monitor security events effectively. Wazuh serves as an open-source security platform that collects and analyzes logs, while ELK provides log storage, processing, and visualization. To evaluate the effectiveness of this setup, a DoS attack will be conducted using hping3 on a monitored Windows system, and security logs will be analyzed in Wazuh’s event dashboard to detect the attack.

**What is SIEM?**

**SIEM (Security Information and Event Management)** is a **cybersecurity tool** that helps organizations **collect, analyze, and respond** to security threats in real-time. It works like a **smart security system** that monitors all activities happening in a network and alerts security teams if something suspicious happens.

**SIEM has two main functions:**

**Security Information Management (SIM)** – Stores and analyzes security logs for reports.  
 **Security Event Management (SEM)** – Detects threats, correlates data, and sends alerts.

**Purpose of SIEM**

SIEM gathers data from **firewalls, servers, endpoints, and cloud systems** and looks for signs of cyber threats.

1. **Collects logs** from different devices.
2. **Finds suspicious patterns** by analyzing events.
3. **Sends alerts** when a potential attack is detected.
4. **Helps investigate** security incidents.
5. **Ensures compliance** with laws like GDPR, PCI-DSS, HIPAA

**Understanding DoS Attacks and Their Impact**

A Denial-of-Service (DoS) attack is a cyber threat that aims to disrupt the availability of a target system, service, or network by overwhelming it with an excessive amount of requests. Unlike Distributed Denial-of-Service (DDoS) attacks, which involve multiple compromised systems, a DoS attack typically originates from a single source.

**The impact of a DoS attack includes:**

* Service Disruption: Legitimate users are unable to access the target system.
* High Resource Consumption: CPU, memory, and bandwidth may be exhausted, causing slowdowns or system crashes.
* Potential Financial and Reputational Loss: Businesses relying on online services suffer revenue loss and customer trust issues.

**What is ELK?**

ELK stands for **Elasticsearch, Logstash, and Kibana**—a free and open-source tool used to collect, store, and analyze security logs. Many organizations use ELK as a **SIEM (Security Information and Event Management) solution** to detect and investigate cyber threats.

**ELK Components in SIEM:**

**Elasticsearch** – A powerful search engine that stores security logs.

**Logstash** – A tool that collects logs from different sources (firewalls, IDS, servers) and processes them.

**Kibana** – A dashboard that lets you visualize and analyze logs using charts and graphs.

**What is Wazuh?**

Wazuh is an **open-source security platform** designed for **threat detection, incident response, and compliance monitoring**. It integrates **host-based intrusion detection (HIDS), log analysis, file integrity monitoring (FIM), vulnerability detection, and SIEM** capabilities.

**How Wazuh Works**

1. **Agents** – Installed on endpoints (Windows, Linux, macOS) to collect security events.
2. **Manager** – Processes and analyzes logs received from agents.
3. **Elasticsearch & Kibana** – Stores and visualizes security data.
4. **Rules & Decoders** – Detect anomalies, threats, and attacks.

**ELK Integration with Wazuh**

Integrating Wazuh with ELK (Elasticsearch, Logstash, and Kibana) provides a comprehensive security monitoring solution by combining log analysis, threat detection, and visualization.

1. Overview of Integration

* Wazuh: An open-source security platform that provides log analysis, threat detection, intrusion detection (HIDS), and compliance monitoring.
* ELK Stack: A log management and visualization platform composed of:
  + Elasticsearch: Stores and indexes logs efficiently.
  + Logstash: Collects, processes, and forwards logs from different sources.
  + Kibana: Visualizes security events with dashboards and analytics.

By integrating Wazuh with ELK, security teams can centralize and analyze logs from multiple endpoints, detect anomalous activities, and respond to security incidents in real-time.

**2. How Wazuh Integrates with ELK**

* Wazuh Agents are installed on monitored endpoints (Windows/Linux), collecting logs and security events.
* Wazuh Manager processes logs, detects threats, and forwards data to Elasticsearch via Filebeat.
* Logstash parses and enriches logs before storing them in Elasticsearch.
* Kibana (Wazuh Plugin) provides a user-friendly dashboard to visualize alerts, analyze security events, and monitor threats effectively.

**3. Benefits of ELK Integration with Wazuh**

* Real-time Threat Detection: Detects anomalies, malware, DoS attacks, and security breaches.
* Log Centralization & Correlation: Gathers logs from multiple sources for enhanced visibility.
* Compliance Monitoring: Helps meet regulatory requirements (PCI DSS, GDPR, HIPAA, etc.).
* Automated Alerting & Response: Generates alerts and supports incident investigation using dashboards.

**Role of Wazuh in Detecting DoS Attacks**

Wazuh, an open-source Security Information and Event Management (SIEM) tool, helps in monitoring, analyzing, and detecting security threats in real time. When integrated with the ELK (Elasticsearch, Logstash, Kibana) stack, Wazuh enhances visibility into system logs and network activity, making it an effective solution for detecting and responding to DoS attacks.

**How Wazuh Detects DoS Attacks:**

* Log Monitoring: Wazuh collects and analyzes system, application, and network logs to detect unusual activity.
* Behavioral Analysis: It can identify anomalies such as excessive requests from a single IP, which may indicate a DoS attempt.
* Real-time Alerts: Wazuh generates alerts for abnormal network traffic, helping security teams take action.

**Objective of This Report**

The purpose of this report is to:

1. Perform a DoS attack on a Windows machine running the Wazuh agent.
2. Monitor logs and network activity using Wazuh integrated with ELK.
3. Detect the attack by analyzing Wazuh alerts and logs.
4. Provide mitigation strategies to prevent and respond to such attacks.

By following this approach, we aim to demonstrate how security teams can detect, analyze, and mitigate DoS attacks using Wazuh and ELK.

**Lab Setup**

This section outlines the environment setup required to simulate a DoS attack, monitor system logs, and detect the attack using Wazuh integrated with ELK.

**Installing prerequisites**

Some extra packages are needed for the installation, such as curl or unzip, which will be used in further steps. However, this step can be skipped if curl and unzip are already installed on the server.

Command >apt-get install apt-transport-https zip unzip lsb-release curl gnupg

**Installing Elasticsearch**

Elasticsearch is a highly scalable full-text search and analytics engine.

**Install the GPG key:**

> curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/elasticsearch.gpg --import && chmod 644 /usr/share/keyrings/elasticsearch.gpg

**Add the repository:**

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

**Update the package information:**

> apt-get update

**Install the Elasticsearch package:**

> apt-get install elasticsearch=7.17.13

**Download the configuration file /etc/elasticsearch/elasticsearch.yml as follows:**

**>** curl -so /etc/elasticsearch/elasticsearch.yml <https://packages.wazuh.com/4.5/tpl/elastic-basic/elasticsearch_all_in_one.yml>

**Certificates creation and deployment**

**Download the configuration file for creating the certificates:**

**>** curl -so /usr/share/elasticsearch/instances.yml https://packages.wazuh.com/4.5/tpl/elastic-basic/instances\_aio.yml

In the following steps, a file that contains a folder named after the instance defined here will be created. This folder will contain the certificates and the keys necessary to communicate with the Elasticsearch node using SSL.

**The certificates can be created using the elasticsearch-certutil tool:**

**>** /usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem --in instances.yml --keep-ca-key --out ~/certs.zip

**Extract the generated /usr/share/elasticsearch/certs.zip file from the previous step.**

**>** unzip ~/certs.zip -d ~/certs

**The next step is to create the directory /etc/elasticsearch/certs, and then copy the CA file, the certificate and the key there:**

**>** mkdir /etc/elasticsearch/certs/ca -p

> cp -R ~/certs/ca/ ~/certs/elasticsearch/\* /etc/elasticsearch/certs/

> chown -R elasticsearch: /etc/elasticsearch/certs

> chmod -R 500 /etc/elasticsearch/certs

> chmod 400 /etc/elasticsearch/certs/ca/ca.\* /etc/elasticsearch/certs/elasticsearch.\*

> rm -rf ~/certs/ ~/certs.zip

**Enable and start the Elasticsearch service:**

> systemctl daemon-reload

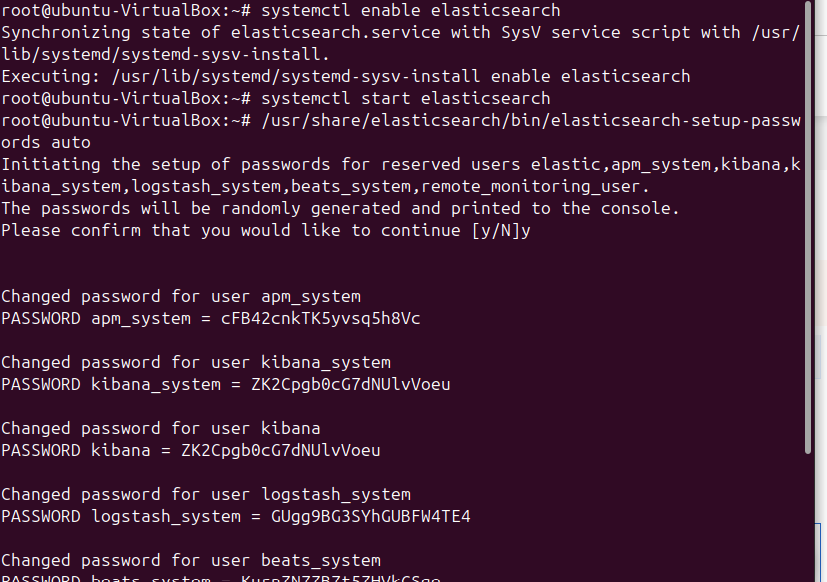
> systemctl enable elasticsearch

> systemctl start elasticsearch

**Generate credentials for all the Elastic Stack pre-built roles and users:**

> /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto

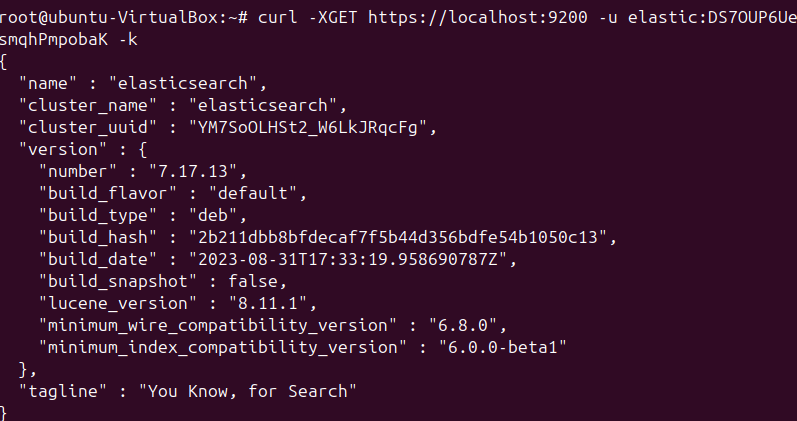
The command above will prompt an output like this. Save the password of the elastic user for further steps:



**To check that the installation was made successfully, run the following command replacing <elastic\_password> with the password generated in the previous step for elastic user:**

> curl -XGET https://localhost:9200 -u elastic:<elastic\_password> -k

This command should have an output like this:



**Installing Wazuh server**

The Wazuh server collects and analyzes data from deployed agents. It runs the Wazuh manager, the Wazuh API and Filebeat. The first step in setting up Wazuh is to add the Wazuh repository to the server. Alternatively, the Wazuh manager package can be downloaded directly, and compatible versions can be checked [here](https://documentation.wazuh.com/4.5/installation-guide/packages-list.html).

**Adding the Wazuh repository**

**Install the GPG key:**

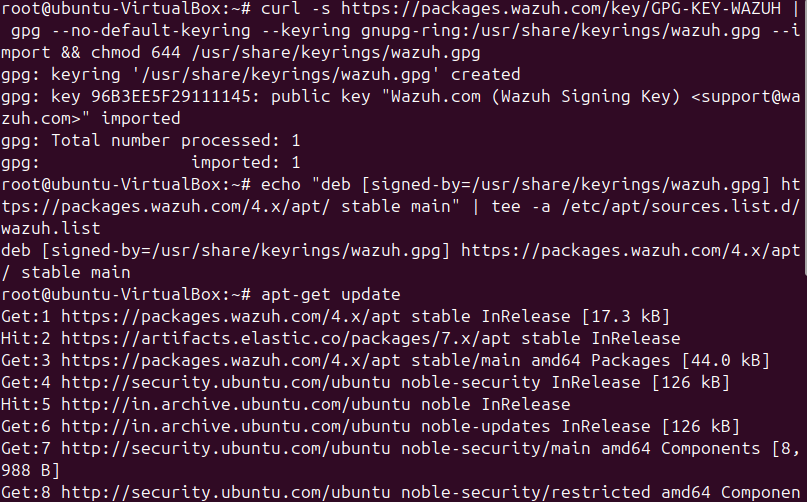
> curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg

**Add the repository:**

> echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

**Update the package information:**

> apt-get update



**Installing the Wazuh manager**

**Install the Wazuh manager package:**

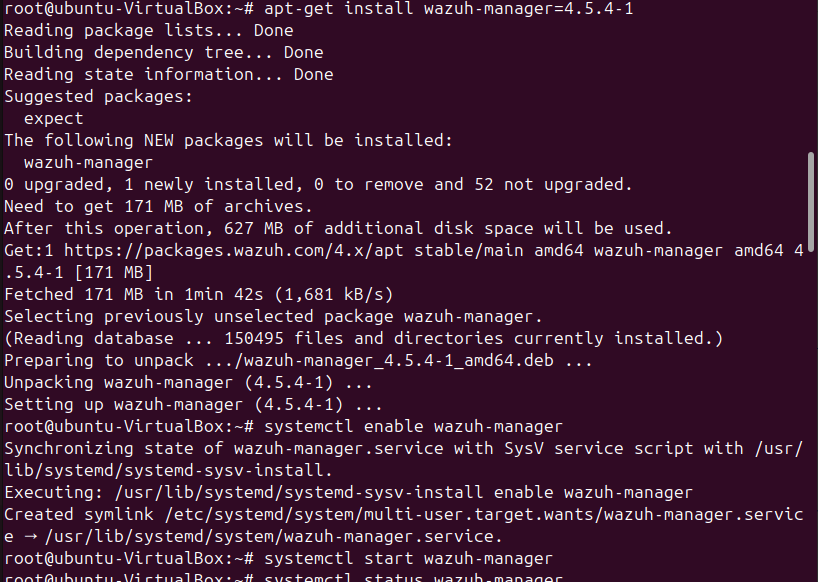
> apt-get install wazuh-manager=4.5.4-1

**Enable and start the Wazuh manager service:**

> systemctl daemon-reload

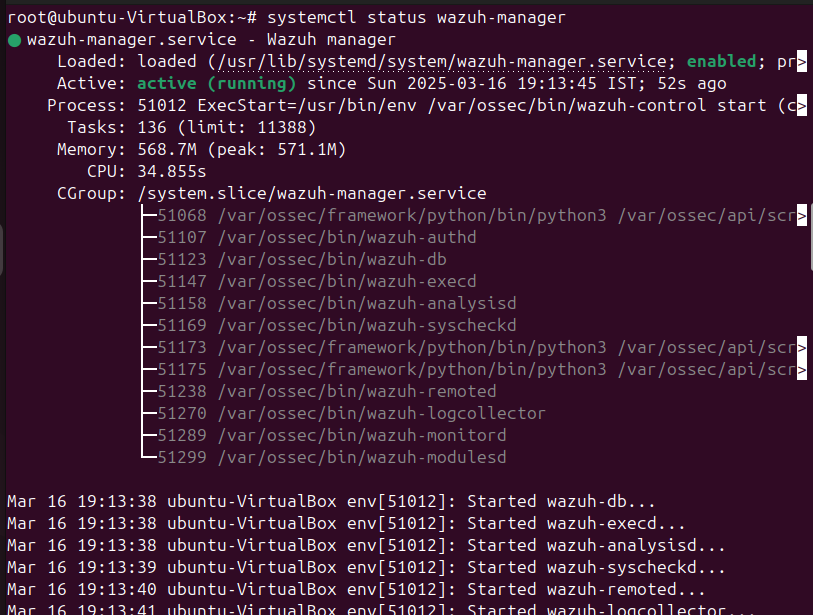
> systemctl enable wazuh-manager

> systemctl start wazuh-manager



**Run the following command to check if the Wazuh manager is active:**

**>** systemctl status wazuh-manager



**Installing Filebeat**

Filebeat is the tool on the Wazuh server that securely forwards alerts and archived events to Elasticsearch.

**Filebeat installation and configuration**

**Install the Filebeat package:**

**>** apt-get install filebeat=7.17.13

**Download the pre-configured Filebeat config file used to forward Wazuh alerts to Elasticsearch:**

**>** curl -so /etc/filebeat/filebeat.yml <https://packages.wazuh.com/4.5/tpl/elastic-basic/filebeat_all_in_one.yml>

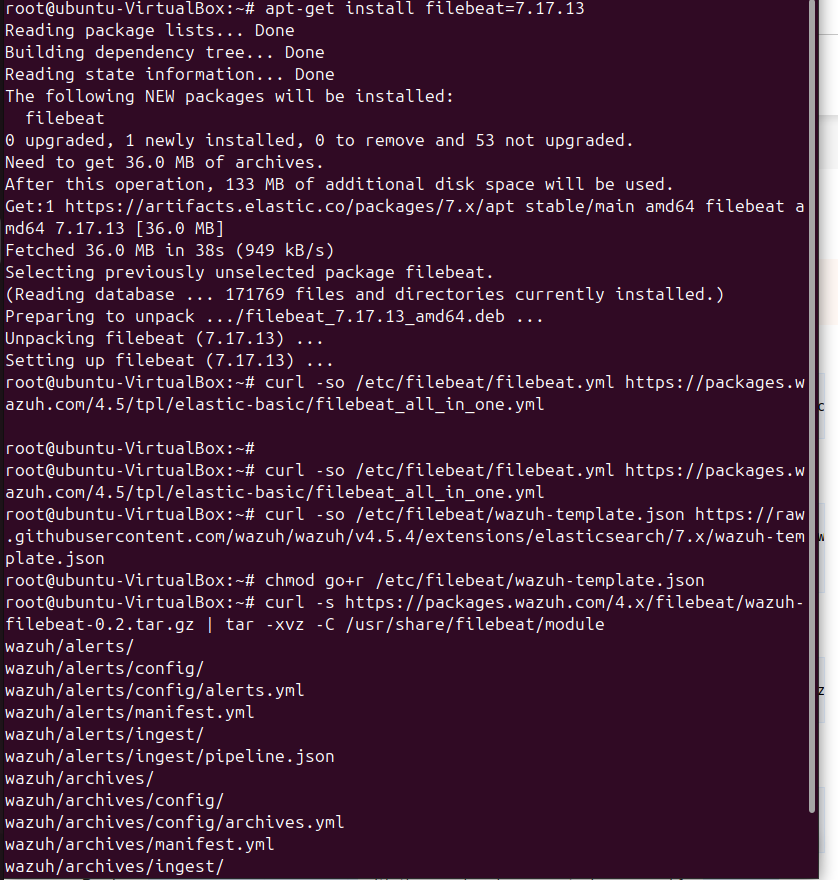
**Download the alerts template for Elasticsearch:**

**>** curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.5.4/extensions/elasticsearch/7.x/wazuh-template.json

> chmod go+r /etc/filebeat/wazuh-template.json

**Download the Wazuh module for Filebeat:**

> curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.2.tar.gz | tar -xvz -C /usr/share/filebeat/module



**Edit the file /etc/filebeat/filebeat.yml and add the following line:**

output.elasticsearch.password: <elasticsearch\_password>

Replace elasticsearch\_password with the previously generated password for elastic user.

**Copy the certificates into /etc/filebeat/certs/**

> cp -r /etc/elasticsearch/certs/ca/ /etc/filebeat/certs/

> cp /etc/elasticsearch/certs/elasticsearch.crt /etc/filebeat/certs/filebeat.crt

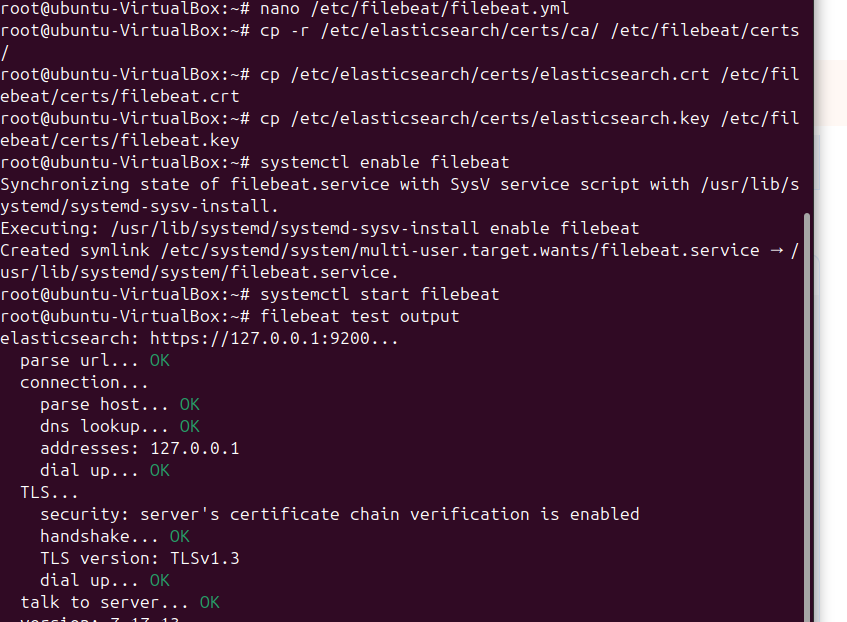
> cp /etc/elasticsearch/certs/elasticsearch.key /etc/filebeat/certs/filebeat.key

**Enable and start the Filebeat service:**

> systemctl daemon-reload

> systemctl enable filebeat

> systemctl start filebeat



**Kibana installation and configuration**

Kibana is a flexible and intuitive web interface for mining and visualizing the events and archives stored in Elasticsearch.

**Install the Kibana package:**

> apt-get install kibana=7.17.13

**Copy the Elasticsearch certificates into the Kibana configuration folder:**

> mkdir /etc/kibana/certs/ca -p

> cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/

> cp /etc/elasticsearch/certs/elasticsearch.key /etc/kibana/certs/kibana.key

> cp /etc/elasticsearch/certs/elasticsearch.crt /etc/kibana/certs/kibana.crt

> chown -R kibana:kibana /etc/kibana/

> chmod -R 500 /etc/kibana/certs

> chmod 440 /etc/kibana/certs/ca/ca.\* /etc/kibana/certs/kibana.\*

**Download the Kibana configuration file**:

> curl -so /etc/kibana/kibana.yml <https://packages.wazuh.com/4.5/tpl/elastic-basic/kibana_all_in_one.yml>

**Edit the /etc/kibana/kibana.yml file:**

elasticsearch.password: <elasticsearch\_password>

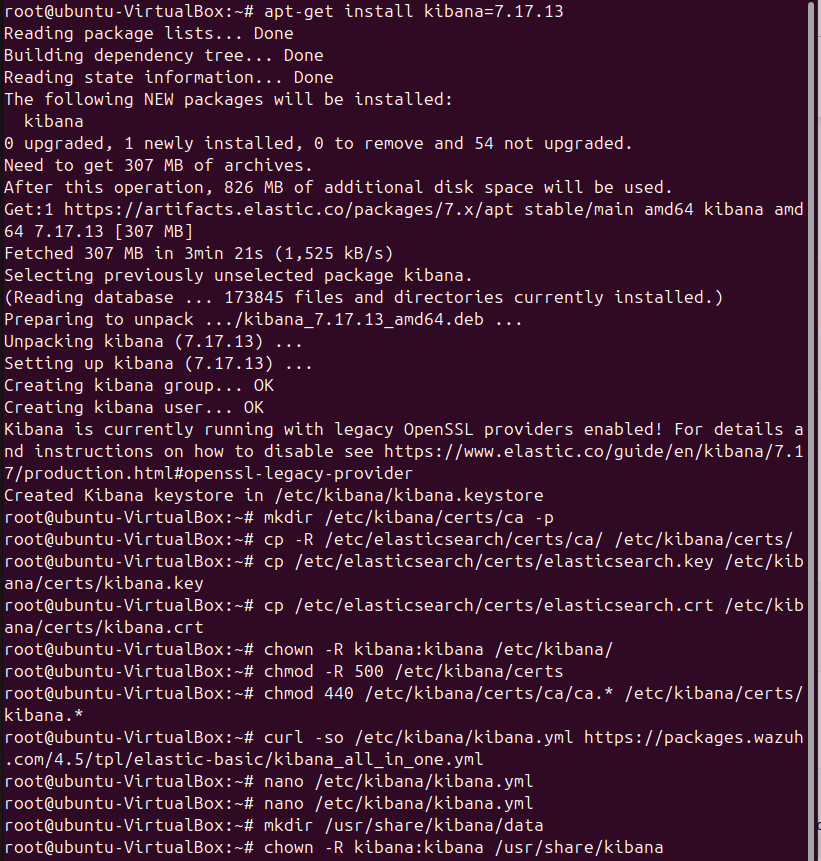
**Values to be replaced:**

<elasticsearch\_password>: the password generated during the Elasticsearch installation and configuration for the elastic user.

**Create the /usr/share/kibana/data directory:**

> mkdir /usr/share/kibana/data

> chown -R kibana:kibana /usr/share/kibana



**Install the Wazuh Kibana plugin. The installation of the plugin must be done from the Kibana home directory as follows:**

> cd /usr/share/kibana

> sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh\_kibana-4.5.4\_7.17.13-1.zip

**Link Kibana's socket to privileged port 443:**

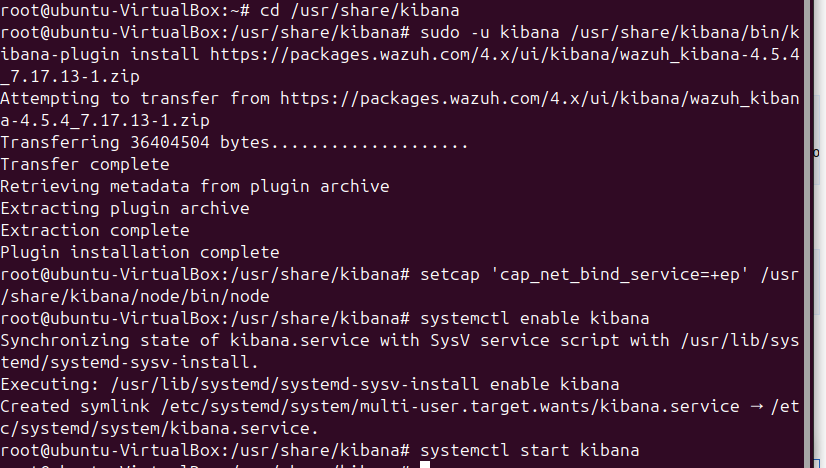
> setcap 'cap\_net\_bind\_service=+ep' /usr/share/kibana/node/bin/node

**Enable and start the Kibana service:**

> systemctl daemon-reload

> systemctl enable kibana

> systemctl start kibana



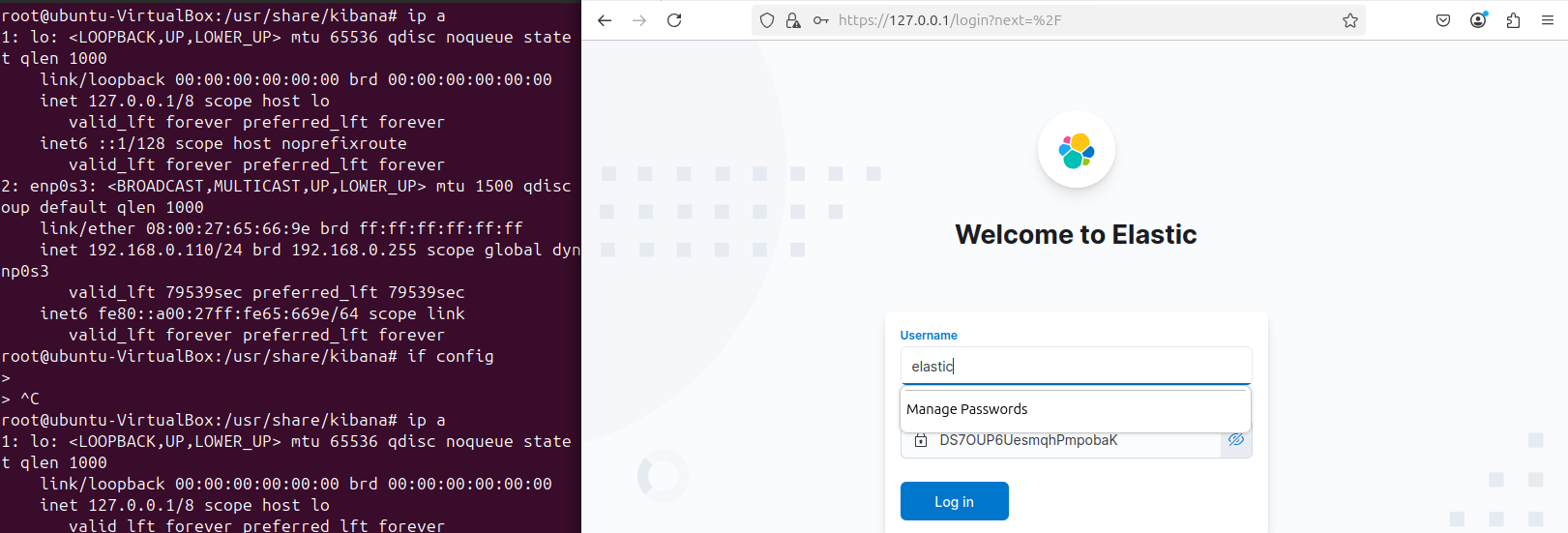
**Access the web interface using the password generated during the Elasticsearch installation process:**

URL: https://<wazuh\_server\_ip>

user: elastic

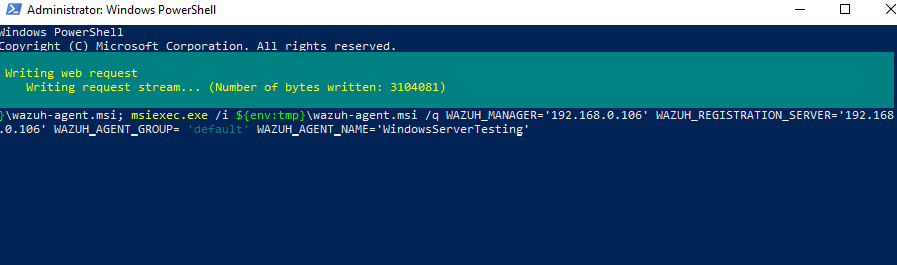
password: <PASSWORD\_elastic>

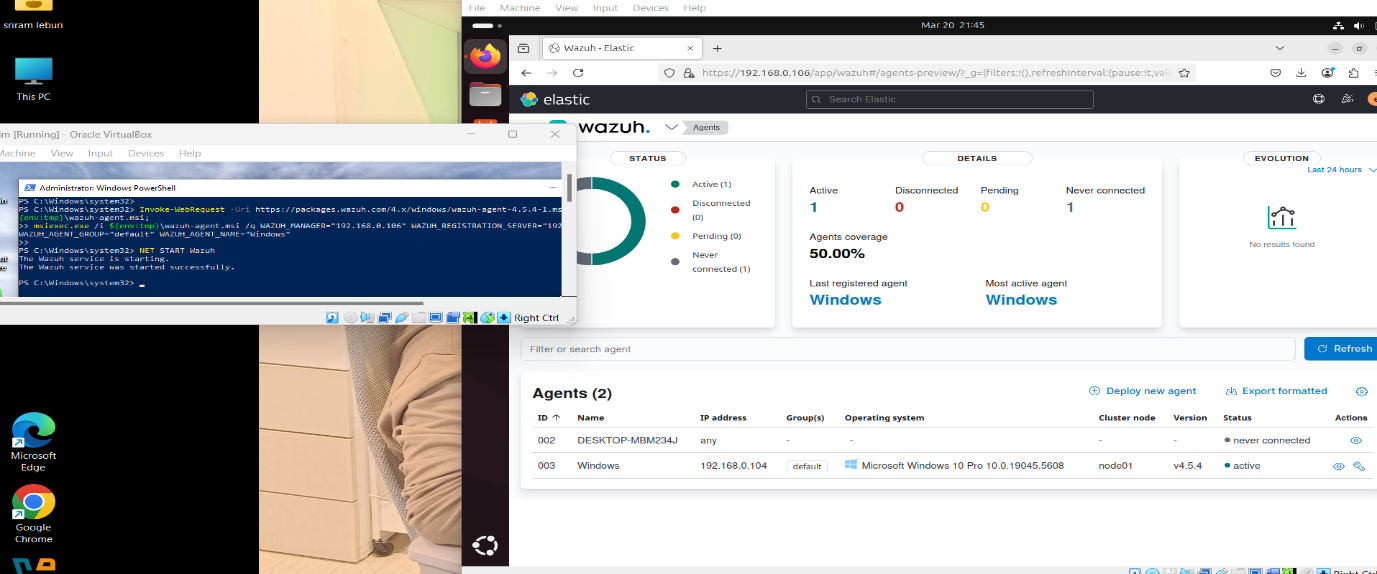
Upon the first access to Kibana, the browser shows a warning message stating that the certificate was not issued by a trusted authority. An exception can be added in the advanced options of the web browser or, for increased security, the ca.crt file previously generated can be imported to the certificate manager of the browser. Alternatively, a certificate from a trusted authority can be configured.



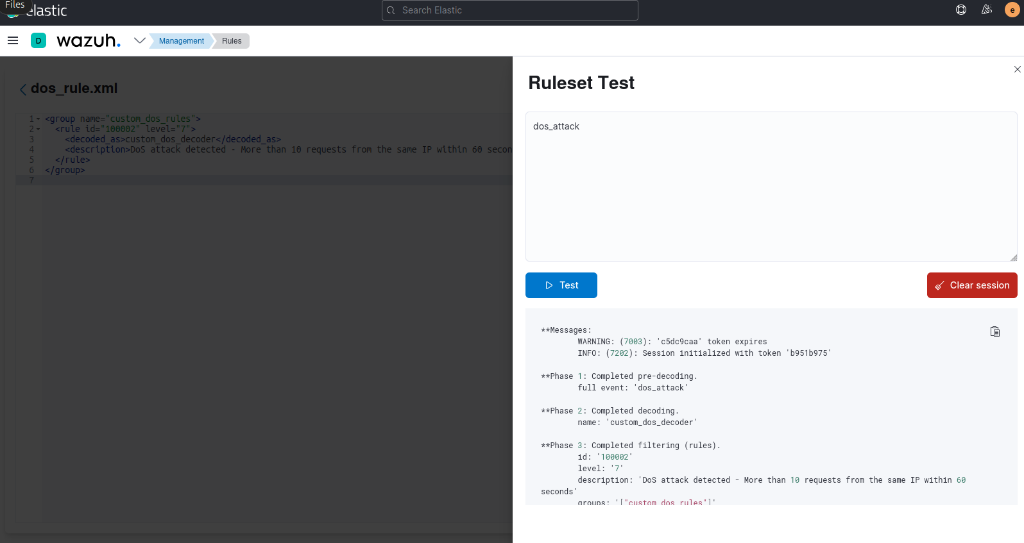
**Wazuh-Agent(Windows)**

Login>agent>add agent>windows>”wazuh server ip”>windows powershell>command>NET start Wazuh





**Custom Rule**



**Performing DoS Attack**

**Attack Execution**

To simulate a **Denial of Service (DoS) attack** on the Windows machine, various attack tools are used to generate excessive traffic and resource consumption.

**Using hping3 for SYN Flood Attack**

On the linux machine (attacker), run the following **hping3** command to send a **flood of SYN packets** to port **80** of the Windows machine:

> hping3 -S -p 80 --flood <Windows-IP>

* -S → Sends **SYN** packets
* -p 80 → Targets **port 80** (can be changed)
* --flood → Sends packets continuously at high speed

**Metasploit Auxiliary DoS Modules**

**Open Metasploit:**

> msfconsole

**Search for DoS modules:**

> search dos

**Use a specific DoS exploit:**

> use auxiliary/dos/tcp/synflood

> set RHOSTS <Windows-IP>

> run

**hping3**

hping3 -S --flood -p 80 192.168.0.102

**Conclusion**

* **SIEM is an important cybersecurity tool** that helps organizations find and respond to security threats in real time. It improves visibility, speeds up incident response, and helps meet security regulations.
* **SIEM has evolved** from basic log storage to advanced systems that use AI to detect threats automatically, reduce false alerts, and respond faster to cyberattacks.
* **Choosing the right SIEM** depends on the organization’s size, budget, and security needs—whether on-premises, cloud-based, or a mix of both.
* Integrating **Wazuh with ELK** transforms it into a **powerful open-source SIEM solution**, enabling organizations to **detect, analyze, and respond to security threats in real time**. This integration enhances **visibility**, accelerates **incident response**, and helps maintain **compliance** with security regulations.
* Over time, SIEM has evolved from **basic log management** to **intelligent threat detection** powered by **AI and machine learning**. The combination of **Wazuh’s security monitoring** and **ELK’s log analysis** provides an **efficient and cost-effective** alternative to commercial SIEM solutions like Splunk and QRadar.
* The future of **Wazuh + ELK** includes advancements in **automated threat intelligence, anomaly detection, and SOAR (Security Orchestration, Automation, and Response)** to further **strengthen cybersecurity defenses**. A well-implemented **Wazuh + ELK SIEM** ensures **proactive security monitoring**, reduces risks, and builds a **robust cybersecurity posture** for any organization.

**References**

* <https://en.wikipedia.org/wiki/Security_information_and_event_management?utm_source=chatgpt.com>
* <https://www.nhregister.com/opinion/article/ransomware-todays-business-arvin-chaudhary-20035891.php?utm_source=chatgpt.com>
* <https://www.ibm.com/think/topics/siem>
* <https://www.elastic.co/security/siem>
* <https://logz.io/blog/elk-siem/>
* <https://www.techtarget.com/searchsecurity/tip/The-history-evolution-and-current-state-of-SIEM>
* [https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/#:~:text=The%20SIEM%20architecture%20refers%20to,across%20an%20organization's%20IT%20infrastructure](https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/).
* <https://www.exabeam.com/explainers/siem/siem-architecture/>
* <https://www.fortinet.com/resources/cyberglossary/what-is-siem>