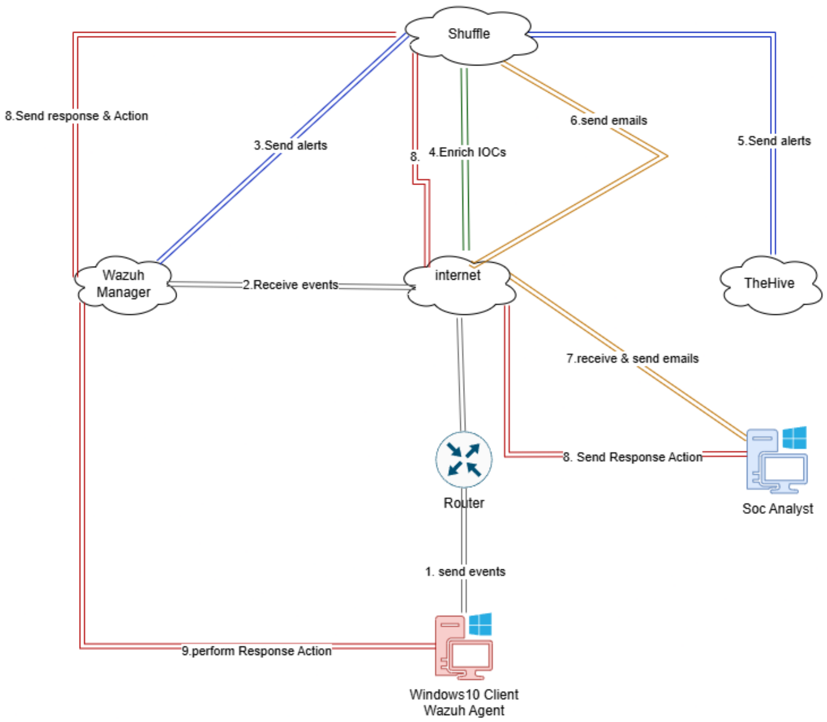
SOC Automation Project –1

Homelab project to gain hands-on experience working with SOC automation procedures and protocols. This project explores:

- Setting up a SOC automation Lab,
- Explore how automation enhances incident response,
- Accelerate threat detection and threat intelligence
- Streamline SOC workflows

LAB DIAGRAM



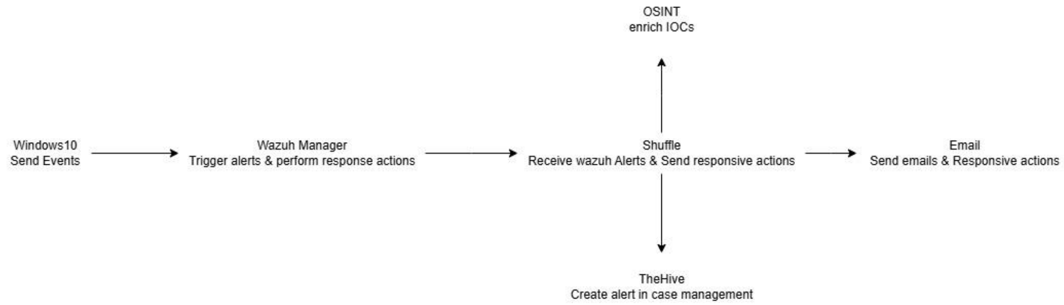

OSINT
enrich IOCs
Windows10
Send Events
Wazuh Manager
Trigger alerts & perform response actions
Shuffle
Receive wazuh Alerts & Send responsive actions
Email
Send emails & Responsive actions
TheHive
Create alert in case management

Diagram details.

- Grey link lines indicate sending events to wazuh manager, Blue link lines sends alerts to shuffle, Green link lines indicates enriching IOCs,
- Blue link lines indicates sending alerts from shufle to TheHive, Orange link lines indicates sending emails to Soc analyst. Red link lines indicates sending response action from SOC analyst to shuffle, then from shuffle to wazuh manager, Wazuh manager then instructs agent to perform response action.

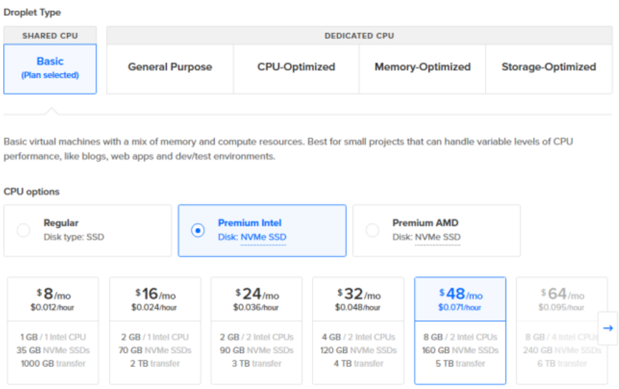
This Lab was set up using Digital Ocean cloud platform. Wazuh manager and TheHive hosted on the Cloud.

WAZUH INSTALLATION

Wazuh is an open-source cybersecurity platform that integrates SIEM and XDR capabilities in a unique solution, it has multiple capabilities such as; Security analytics, Intrusion detection, Log data analysis, File integrity monitoring, Vulnerability Detection, Configuration Assessment, Incident Response, Regulatory Compliance etc.

SETTING UP WAZUH ON DIGITAL OCEAN.

- Click on droplets on the top-right corner (droplets are like the virtual machines)
- Select Ubuntu 22.04, select premium intel, 8gb ram,
- Change hostname and create a password, create Wazuh manager.



Droplet Type

SHARED CPU	DEDICATED CPU			
Basic (Plan selected)	General Purpose	CPU-Optimized	Memory-Optimized	Storage-Optimized

Basic virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.

CPU options

○ Regular
Disk type: SSD

● Premium Intel
Disk: NVMe SSD

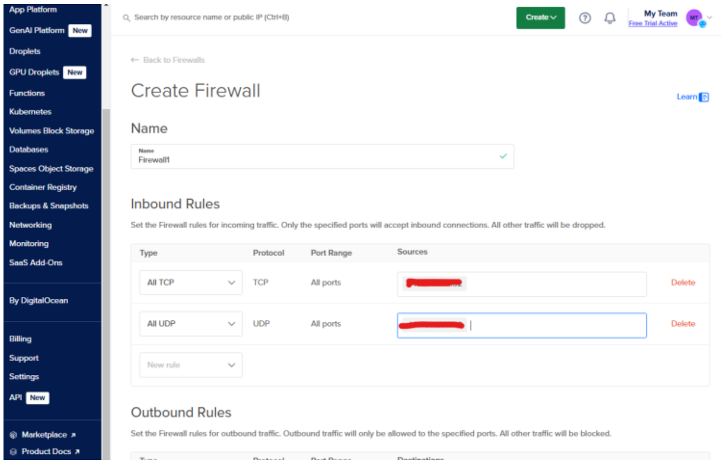
○ Premium AMD
Disk: NVMe SSD

$8/mo $0.012/hour	$16/mo $0.024/hour	$24/mo $0.036/hour	$32/mo $0.048/hour	$48/mo $0.071/hour	$64/mo $0.095/hour
1 GB / 1 Intel CPU 35 GB NVMe SSDs 1000 GB transfer	2 GB / 1 Intel CPU 70 GB NVMe SSDs 2 TB transfer	2 GB / 2 Intel CPUs 90 GB NVMe SSDs 3 TB transfer	4 GB / 2 Intel CPUs 120 GB NVMe SSDs 4 TB transfer	8 GB / 2 Intel CPUs 160 GB NVMe SSDs 5 TB transfer	8 GB / 4 Intel CPUs 240 GB NVMe SSDs 6 TB transfer

-

CREATE FIREWALL

- Go to Networking tab on the left-hand side
- Go to firewalls tab, create firewall, name firewall
- Change type to ‘all TCP’, Remove all IPs
- Only add public IP. Find this by simply browsing ‘what is my public IP’

- 

Create Firewall

Name

Name: Firewall1

Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be dropped.

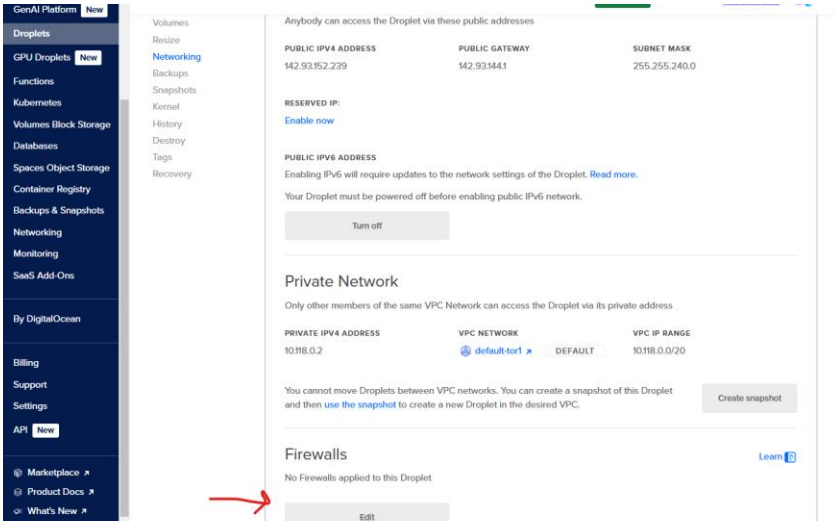
Type	Protocol	Port Range	Sources	
All TCP	TCP	All ports	[redacted]	Delete
All UDP	UDP	All ports	[redacted]	Delete
New rule				

Outbound Rules

Set the Firewall rules for outbound traffic. Outbound traffic will only be allowed to the specified ports. All other traffic will be blocked.

- Do the same for UDP
- Scroll down and create firewall
- Now add VM(Wazuh to firewall)
- The reason for doing this is to prevent access or scanning from just anybody and to make the VM accessible only through me.

ADD VM TO FIREWALL

- Select droplets on the left-hand side, copy the public IP
- Click on Wazuh, go to networking tab, scroll down to firewalls and click on edit
- Select the firewall just created, click on droplets and select ‘add droplets’
- Select wazuh and add droplet
- 

Anybody can access the Droplet via these public addresses

PUBLIC IPV4 ADDRESS	PUBLIC GATEWAY	SUBNET MASK
142.93.152.239	142.93.144.1	255.255.240.0

RESERVED IP:
Enable now

PUBLIC IPV6 ADDRESS
Enabling IPv6 will require updates to the network settings of the Droplet. Read more.

Your Droplet must be powered off before enabling public IPv6 network.

Private Network

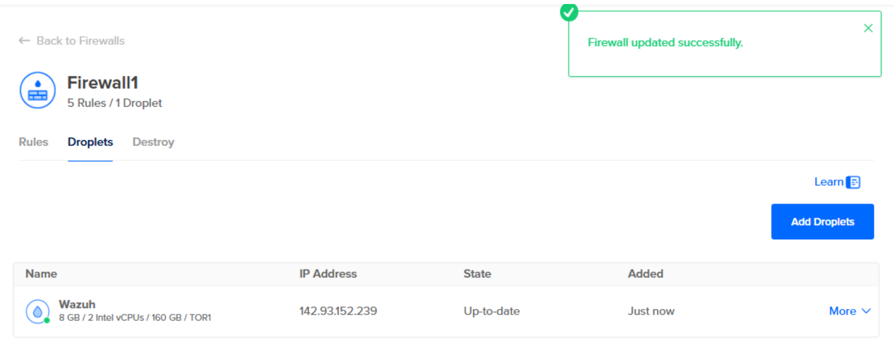
Only other members of the same VPC Network can access the Droplet via its private address

PRIVATE IPV4 ADDRESS	VPC NETWORK	VPC IP RANGE
10.118.0.2	default-tor1 DEFAULT	10.118.0.0/20

You cannot move Droplets between VPC networks. You can create a snapshot of this Droplet and then use the snapshot to create a new Droplet in the desired VPC.

Firewalls

No Firewalls applied to this Droplet



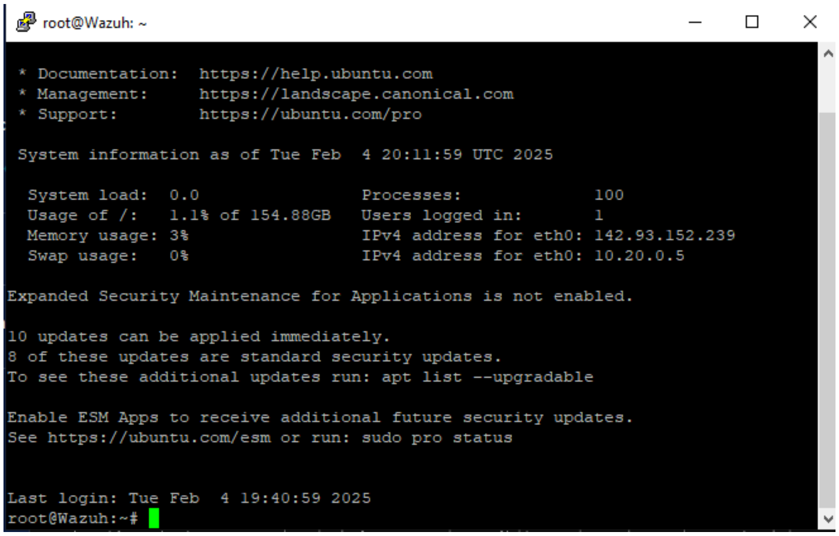
Firewall updated successfully.

Firewall1
5 Rules / 1 Droplet

Name	IP Address	State	Added
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / TOR1	142.93.152.239	Up-to-date	Just now

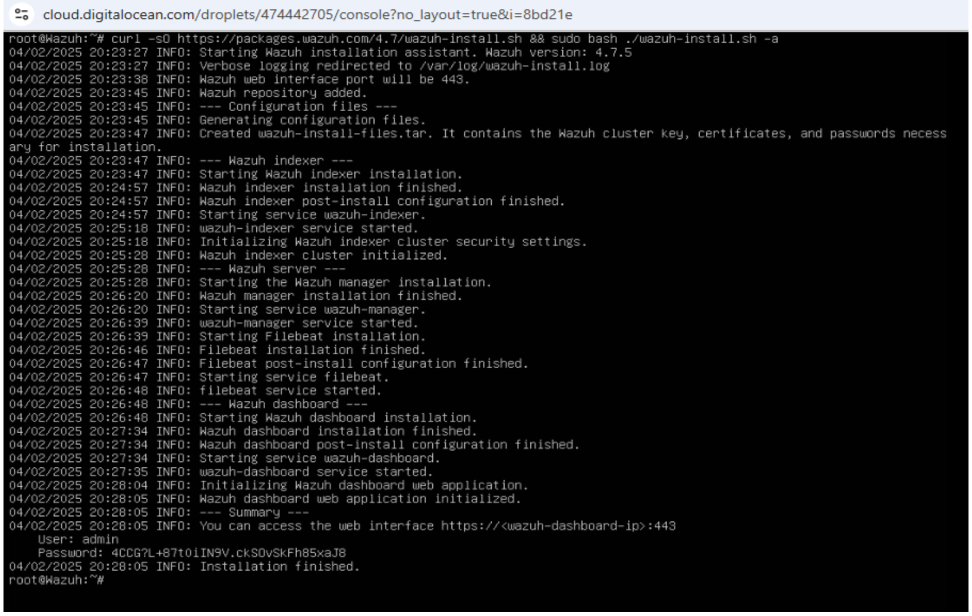
-
- Now firewall will be protecting the Wazuh

VM can now be accessed through SSH with putty or directly from the digital ocean platform by going to the Access Tab on the dashboard .



```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Feb  4 20:11:59 UTC 2025

  System load:  0.0               Processes:             100
  Usage of /:   1.1% of 154.88GB  Users logged in:       1
  Memory usage: 3%                IPv4 address for eth0: 142.93.152.239
  Swap usage:   0%                IPv4 address for eth0: 10.20.0.5

Expanded Security Maintenance for Applications is not enabled.

10 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Tue Feb  4 19:40:59 2025
root@Wazuh:~#
```

- After launching console , perform update and upgrade on the console
- To install Wazuh on the console, run the curl command which can be found on the wazuh website



cloud.digitalocean.com/droplets/474442705/console?no_layout=true&i=8bd21e

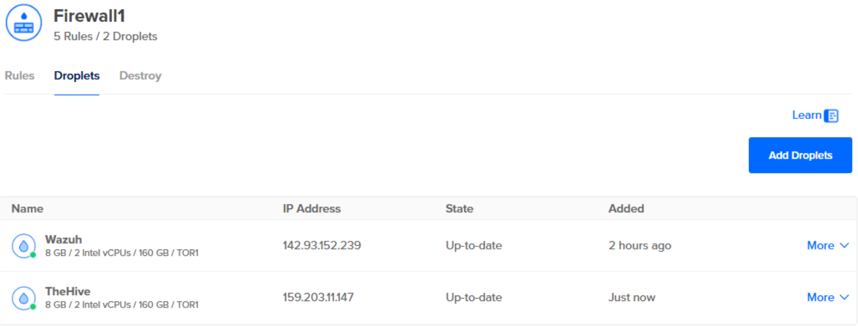
```
root@Wazuh:~# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
04/02/2025 20:23:27 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
04/02/2025 20:23:27 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/02/2025 20:23:38 INFO: Wazuh web interface port will be 443.
04/02/2025 20:23:45 INFO: Wazuh repository added.
04/02/2025 20:23:45 INFO: --- Configuration files ---
04/02/2025 20:23:45 INFO: Generating configuration files.
04/02/2025 20:23:47 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necess
ary for installation.
04/02/2025 20:23:47 INFO: --- Wazuh indexer ---
04/02/2025 20:23:47 INFO: Starting Wazuh indexer installation.
04/02/2025 20:24:57 INFO: Wazuh indexer installation finished.
04/02/2025 20:24:57 INFO: Wazuh indexer post-install configuration finished.
04/02/2025 20:24:57 INFO: Starting service wazuh-indexer.
04/02/2025 20:25:18 INFO: wazuh-indexer service started.
04/02/2025 20:25:18 INFO: Initializing Wazuh indexer cluster security settings.
04/02/2025 20:25:28 INFO: Wazuh indexer cluster initialized.
04/02/2025 20:25:28 INFO: --- Wazuh server ---
04/02/2025 20:25:28 INFO: Starting the Wazuh manager installation.
04/02/2025 20:26:20 INFO: Wazuh manager installation finished.
04/02/2025 20:26:20 INFO: Starting service wazuh-manager.
04/02/2025 20:26:39 INFO: wazuh-manager service started.
04/02/2025 20:26:39 INFO: Starting Filebeat installation.
04/02/2025 20:26:46 INFO: Filebeat installation finished.
04/02/2025 20:26:47 INFO: Filebeat post-install configuration finished.
04/02/2025 20:26:47 INFO: Starting service filebeat.
04/02/2025 20:26:48 INFO: filebeat service started.
04/02/2025 20:26:48 INFO: --- Wazuh dashboard ---
04/02/2025 20:26:48 INFO: Starting Wazuh dashboard installation.
04/02/2025 20:27:34 INFO: Wazuh dashboard installation finished.
04/02/2025 20:27:34 INFO: Wazuh dashboard post-install configuration finished.
04/02/2025 20:27:34 INFO: Starting service wazuh-dashboard.
04/02/2025 20:27:35 INFO: wazuh-dashboard service started.
04/02/2025 20:28:04 INFO: Initializing Wazuh dashboard web application.
04/02/2025 20:28:05 INFO: Wazuh dashboard web application initialized.
04/02/2025 20:28:05 INFO: --- Summary ---
04/02/2025 20:28:05 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: 4CCG?L+87t0iIN9V.ckSOvSkFh85xaJ8
04/02/2025 20:28:05 INFO: Installation finished.
root@Wazuh:~#
```

- Take note of login details to login to wazuh dashboard
- Go to ‘https://publicIP’
- Login with the details provided

INSTALLING THEHIVE

TheHive is a 4-in-1 open-source security incident response platform, it is a scalable incident response platform tightly integrated with MISP(Malware Information Sharing Platform).

- Similar to Wazuh, add ubuntu 22.04 droplet on digital ocean platform using the same steps
- Ensure TheHive is protected by the same firewall, so add the droplet to the firewall created using the same steps as wazuh



Firewall1

5 Rules / 2 Droplets

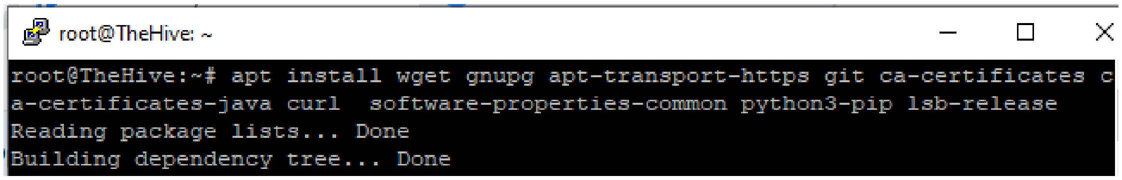
Name	IP Address	State	Added	
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / TOR1	142.93.152.239	Up-to-date	2 hours ago	More
TheHive 8 GB / 2 Intel vCPUs / 160 GB / TOR1	159.203.11.147	Up-to-date	Just now	More

- SSH into to thehive console

-

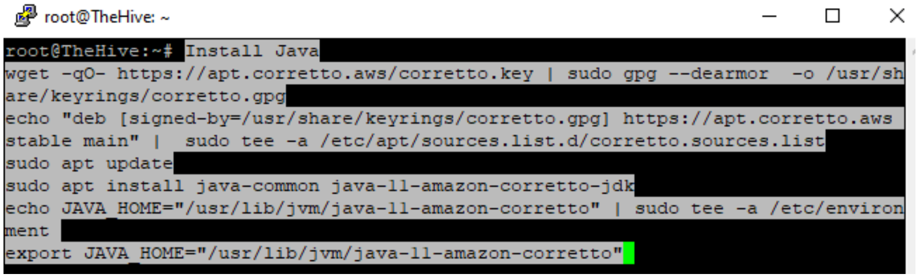
```
root@TheHive:~#
```

- Now to install Dependencies, using the commands provided in the Instructions file

- 

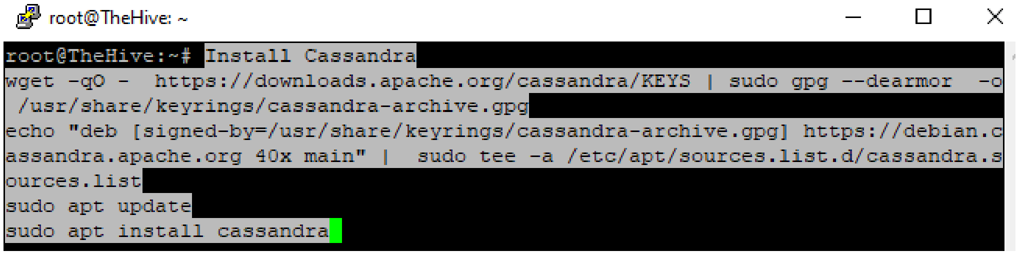
```
root@TheHive:~# apt install wget gnupg apt-transport-https git ca-certificates c
a-certificates-java curl  software-properties-common python3-pip lsb-release
Reading package lists... Done
Building dependency tree... Done
```

- Install Java

- 

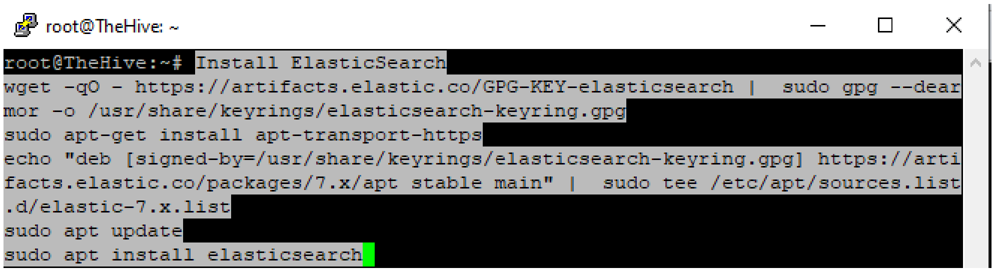
```
root@TheHive:~# Install Java
wget -qO- https://apt.corretto.aws/corretto.key | sudo gpg --dearmor  -o /usr/sh
are/keyrings/corretto.gpg
echo "deb [signed-by=/usr/share/keyrings/corretto.gpg] https://apt.corretto.aws
stable main" |  sudo tee -a /etc/apt/sources.list.d/corretto.sources.list
sudo apt update
sudo apt install java-common java-11-amazon-corretto-jdk
echo JAVA_HOME="/usr/lib/jvm/java-11-amazon-corretto" | sudo tee -a /etc/environ
ment
export JAVA_HOME="/usr/lib/jvm/java-11-amazon-corretto"
```

- Install Cassandra

- 

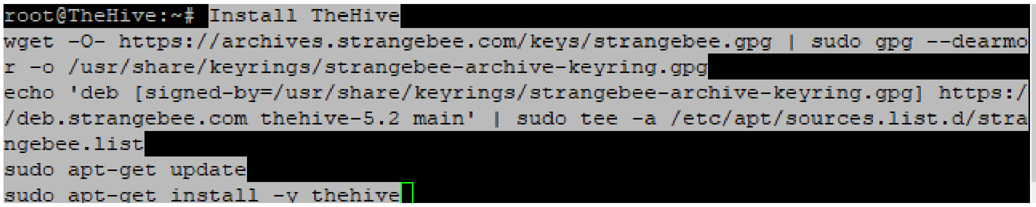
```
root@TheHive:~# Install Cassandra
wget -qO -  https://downloads.apache.org/cassandra/KEYS | sudo gpg --dearmor  -o
 /usr/share/keyrings/cassandra-archive.gpg
echo "deb [signed-by=/usr/share/keyrings/cassandra-archive.gpg] https://debian.c
assandra.apache.org 40x main" |  sudo tee -a /etc/apt/sources.list.d/cassandra.s
ources.list
sudo apt update
sudo apt install cassandra
```

- Install Elasticsearch

- 

```
root@TheHive:~# Install ElasticSearch
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch |  sudo gpg --dear
mor -o /usr/share/keyrings/elasticsearch-keyring.gpg
sudo apt-get install apt-transport-https
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://arti
facts.elastic.co/packages/7.x/apt stable main" |  sudo tee /etc/apt/sources.list
.d/elastic-7.x.list
sudo apt update
sudo apt install elasticsearch
```

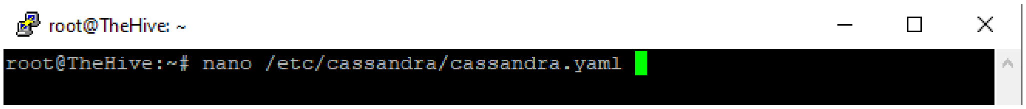
- Finally, Install TheHive

- 

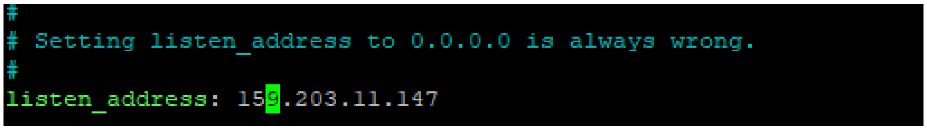
```
root@TheHive:~# Install TheHive
wget -O- https://archives.strangebee.com/keys/strangebee.gpg | sudo gpg --dearmo
r -o /usr/share/keyrings/strangebee-archive-keyring.gpg
echo 'deb [signed-by=/usr/share/keyrings/strangebee-archive-keyring.gpg] https:/
/deb.strangebee.com thehive-5.2 main' | sudo tee -a /etc/apt/sources.list.d/stra
ngebee.list
sudo apt-get update
sudo apt-get install -y thehive
```

CONFIGURING THEHIVE & WAZUH SERVERS

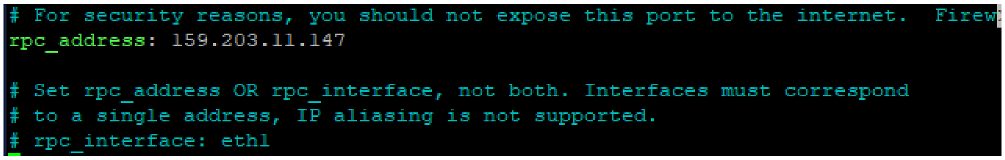
EDIT CASSANDRA’S CONFIGURATION FILE

- Nano /etc/cassandra/
- 

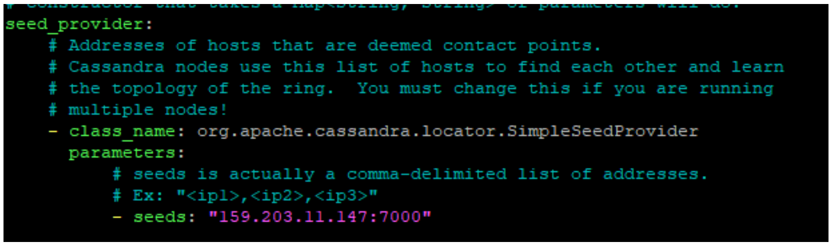
```
root@TheHive:~# nano /etc/cassandra/cassandra.yaml
```

- Customize listen address to publicIP or ports along with clustername in this file
- 

```
#
# Setting listen_address to 0.0.0.0 is always wrong.
#
listen_address: 159.203.11.147
```

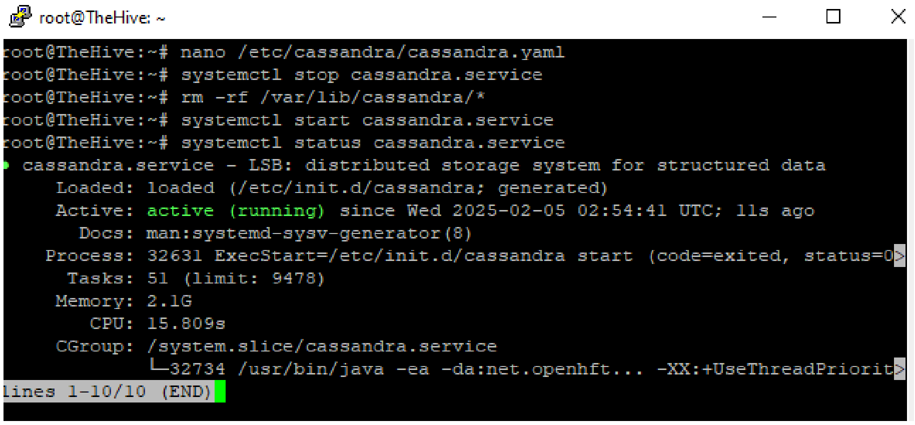
- To change RPC address , ‘CTRL +W’ to search, then search for rpc_address, change from localhost to publicIP of theHive
- 

```
# For security reasons, you should not expose this port to the internet.  Firew
rpc_address: 159.203.11.147

# Set rpc_address OR rpc_interface, not both. Interfaces must correspond
# to a single address, IP aliasing is not supported.
# rpc_interface: eth1
```

- Next change seed addresses. ‘CTRL +w’ search for seed_provider, change to publicIp of TheHive
- 

```
# constructor that takes a Map<String, String> of parameters will do.
seed_provider:
    # Addresses of hosts that are deemed contact points.
    # Cassandra nodes use this list of hosts to find each other and learn
    # the topology of the ring.  You must change this if you are running
    # multiple nodes!
    - class_name: org.apache.cassandra.locator.SimpleSeedProvider
      parameters:
          # seeds is actually a comma-delimited list of addresses.
          # Ex: "<ip1>,<ip2>,<ip3>"
          - seeds: "159.203.11.147:7000"
```

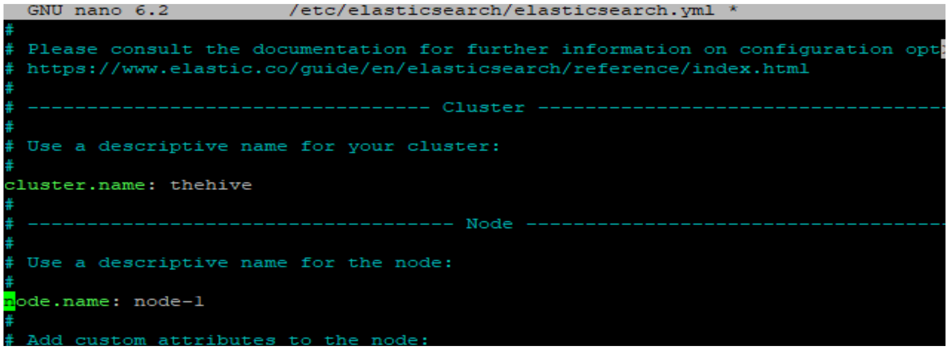
- Because TheHive is installed using their package, must remove old files. ‘rm -rf /var/lib/cassandra/*
- Restart Cassandra service by running ‘systemctl restart cassamdra.service’
- Enable the service and verify that it is running

- 

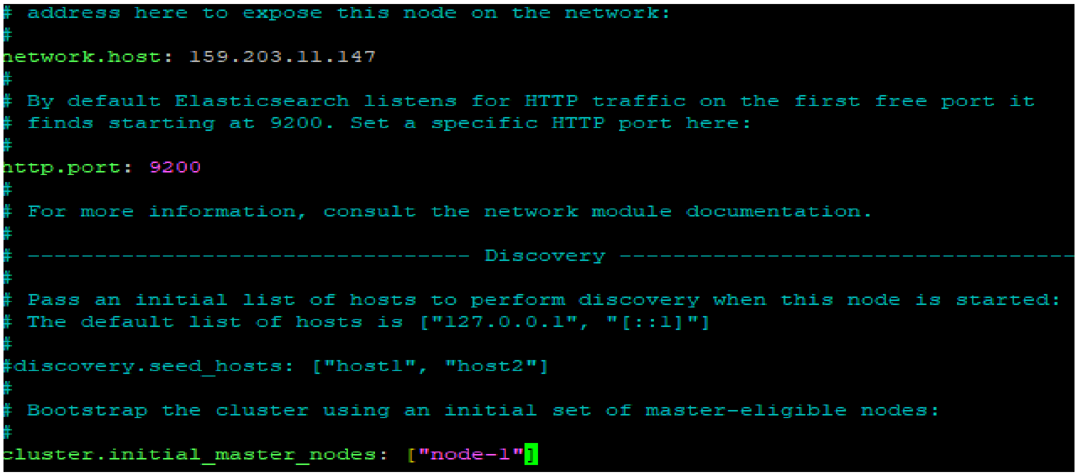
```
root@TheHive:~# nano /etc/cassandra/cassandra.yaml
root@TheHive:~# systemctl stop cassandra.service
root@TheHive:~# rm -rf /var/lib/cassandra/*
root@TheHive:~# systemctl start cassandra.service
root@TheHive:~# systemctl status cassandra.service
● cassandra.service - LSB: distributed storage system for structured data
     Loaded: loaded (/etc/init.d/cassandra; generated)
     Active: active (running) since Wed 2025-02-05 02:54:41 UTC; 11s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 32631 ExecStart=/etc/init.d/cassandra start (code=exited, status=0>
      Tasks: 51 (limit: 9478)
     Memory: 2.1G
        CPU: 15.809s
     CGroup: /system.slice/cassandra.service
             └─32734 /usr/bin/java -ea -da:net.openhft... -XX:+UseThreadPriorit>
lines 1-10/10 (END)
```

NOW SETUP ELASTIC SEARCH

Elasticsearch is used to manage data indices AKA querying data

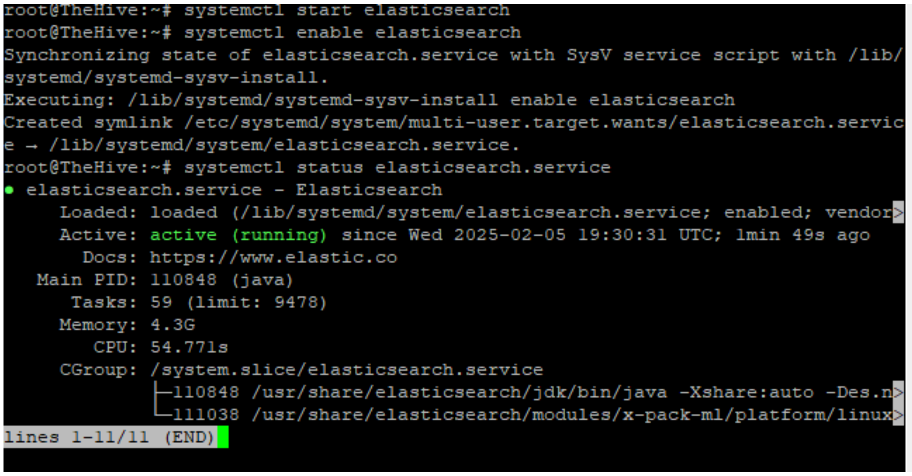
- ‘nano /etc/elasticsearch/elasticsearch.yml’
- Change clustername to ‘Thehive’
- Remove comment from node.name, leave as node-1
- 

```
  GNU nano 6.2              /etc/elasticsearch/elasticsearch.yml *
#
# Please consult the documentation for further information on configuration opt
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: thehive
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node-1
#
# Add custom attributes to the node:
```

- Scroll down to find network.host, remove comment then put in publicIP of TheHive
- Scroll down to find cluster.initial_master_nodes, remove comment and remove node-2
- 

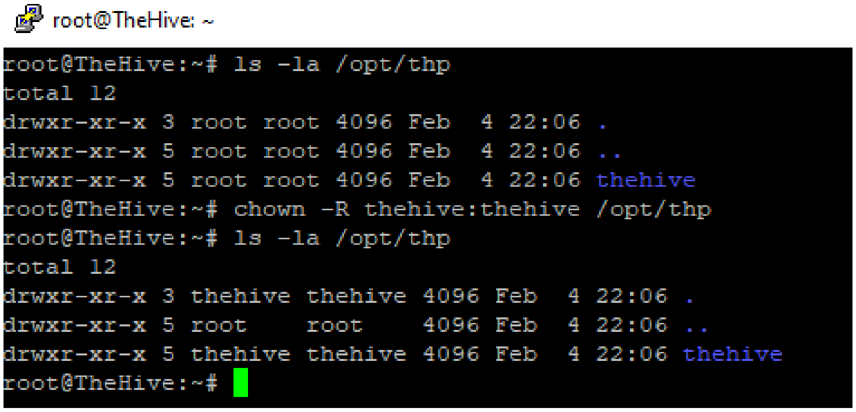
```
# address here to expose this node on the network:
#
network.host: 159.203.11.147
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
cluster.initial_master_nodes: ["node-1"]
```

- Start the service for elasticsearch ‘systemctl start elasticsearch’

- Enable the service ‘systemctl enable elasticsearch’
- Check status ‘systemctl status elasticsearch’
- 

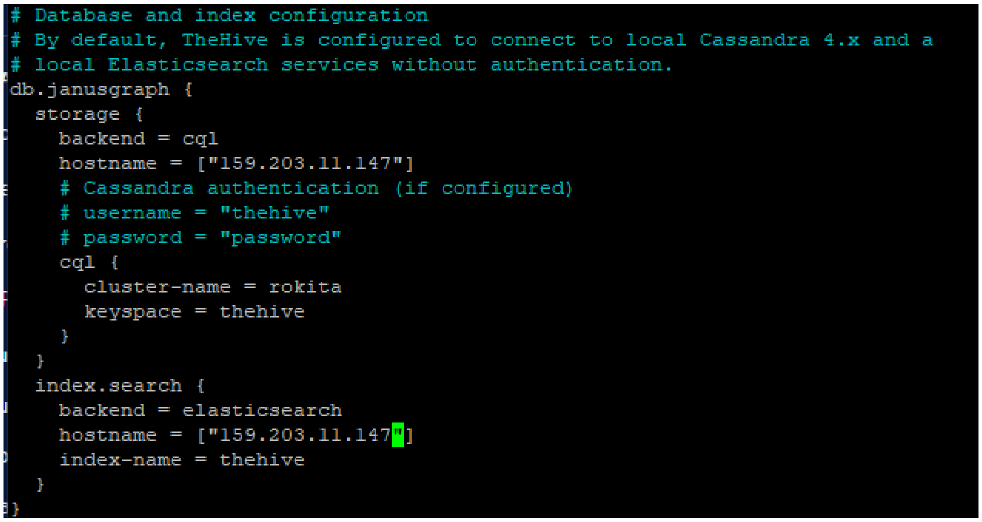
```
root@TheHive:~# systemctl start elasticsearch
root@TheHive:~# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.servic
e → /lib/systemd/system/elasticsearch.service.
root@TheHive:~# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Wed 2025-02-05 19:30:31 UTC; 1min 49s ago
       Docs: https://www.elastic.co
   Main PID: 110848 (java)
      Tasks: 59 (limit: 9478)
     Memory: 4.3G
        CPU: 54.771s
     CGroup: /system.slice/elasticsearch.service
             ├─110848 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.n>
             └─111038 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux>
lines 1-11/11 (END)
```

CONFIGURING THEHIVE

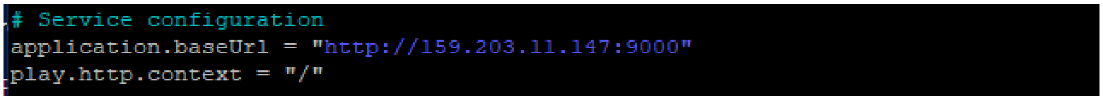
- Before configuring thehive, ensure user and group has access to a certain file path. Run ‘ls -la /opt/thp’ This is the file path TheHive requires access to
- Run ‘chown -R thehive:thehive /opt/thp’ to change owner to thehive user and thehive group over the destination group.
- 

```
root@TheHive:~# ls -la /opt/thp
total 12
drwxr-xr-x 3 root root 4096 Feb  4 22:06 .
drwxr-xr-x 5 root root 4096 Feb  4 22:06 ..
drwxr-xr-x 5 root root 4096 Feb  4 22:06 thehive
root@TheHive:~# chown -R thehive:thehive /opt/thp
root@TheHive:~# ls -la /opt/thp
total 12
drwxr-xr-x 3 thehive thehive 4096 Feb  4 22:06 .
drwxr-xr-x 5 root    root    4096 Feb  4 22:06 ..
drwxr-xr-x 5 thehive thehive 4096 Feb  4 22:06 thehive
root@TheHive:~#
```

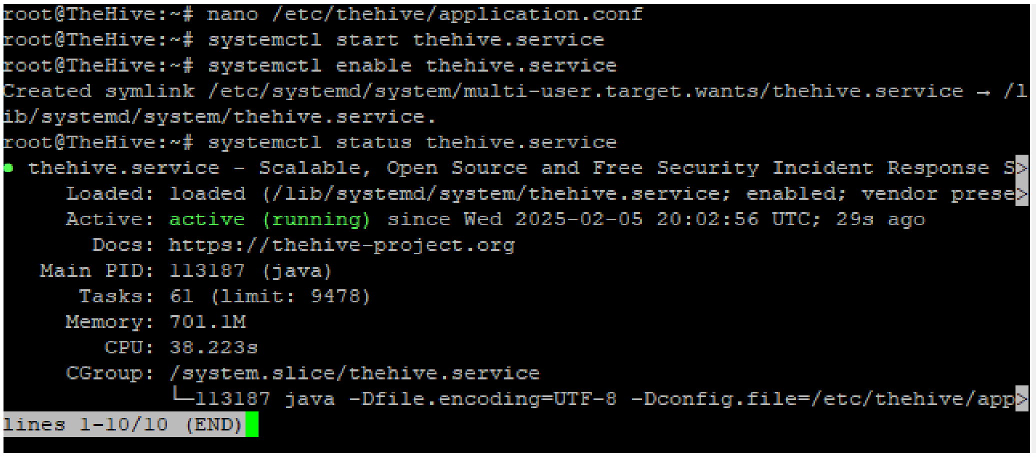
- Now I can configure thehive’s configuration file
- ‘nano /etc/thehive/application.conf’
- Scroll down to Database and index configuration, change hostname to the publicIP of TheHive
- Change cluster-name to the same name configured in Cassandra
- Scroll down to index.search, change hostname to thehive publicIP
- Scroll down to application.buseurl, remove localhost and change to thehive localIP

- 

```
# Database and index configuration
# By default, TheHive is configured to connect to local Cassandra 4.x and a
# local Elasticsearch services without authentication.
db.janusgraph {
  storage {
    backend = cql
    hostname = ["159.203.11.147"]
    # Cassandra authentication (if configured)
    # username = "thehive"
    # password = "password"
    cql {
      cluster-name = rokita
      keyspace = thehive
    }
  }
  index.search {
    backend = elasticsearch
    hostname = ["159.203.11.147"]
    index-name = thehive
  }
}
```

- 

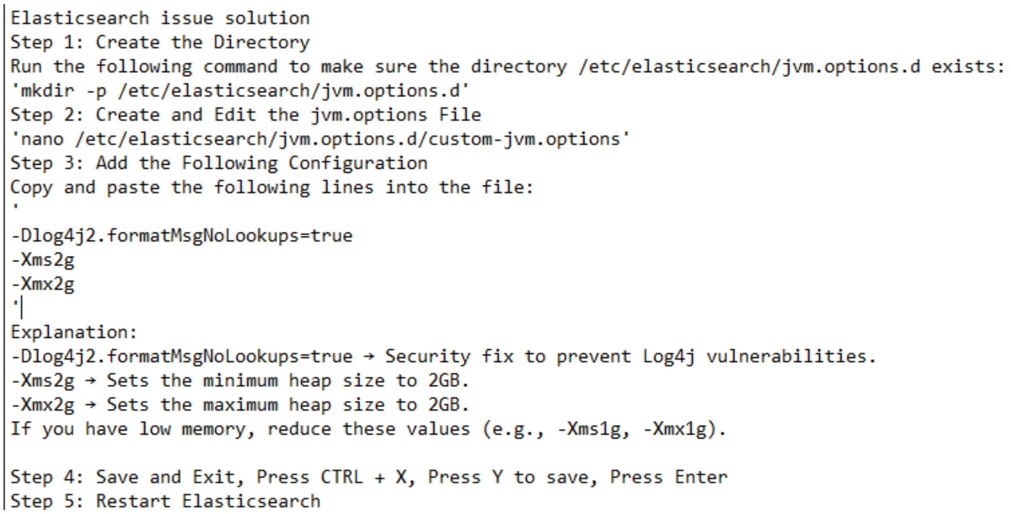
```
# Service configuration
application.baseUrl = "http://159.203.11.147:9000"
play.http.context = "/"
```

- By default, thehive has both cortex and MISP enabled. Cortex is their data enrichment and response capability whereas MISP is used as their cyber threat intelligence platform
- Start and enable the service
- 

```
root@TheHive:~# nano /etc/thehive/application.conf
root@TheHive:~# systemctl start thehive.service
root@TheHive:~# systemctl enable thehive.service
Created symlink /etc/systemd/system/multi-user.target.wants/thehive.service → /l
ib/systemd/system/thehive.service.
root@TheHive:~# systemctl status thehive.service
● thehive.service - Scalable, Open Source and Free Security Incident Response S>
     Loaded: loaded (/lib/systemd/system/thehive.service; enabled; vendor prese>
     Active: active (running) since Wed 2025-02-05 20:02:56 UTC; 29s ago
       Docs: https://thehive-project.org
   Main PID: 113187 (java)
      Tasks: 61 (limit: 9478)
     Memory: 701.1M
        CPU: 38.223s
     CGroup: /system.slice/thehive.service
             └─113187 java -Dfile.encoding=UTF-8 -Dconfig.file=/etc/thehive/app>
lines 1-10/10 (END)
```

- Double check amd ensure cassandra, elasticsearch and thehive are all running to ensure proper functionality.

NB: Error encountered while doublechecking, elasticsearch was not running and failed to restart. Turns out it was a memory issue and required configuring the memory usage for elastic search. Follow steps below.

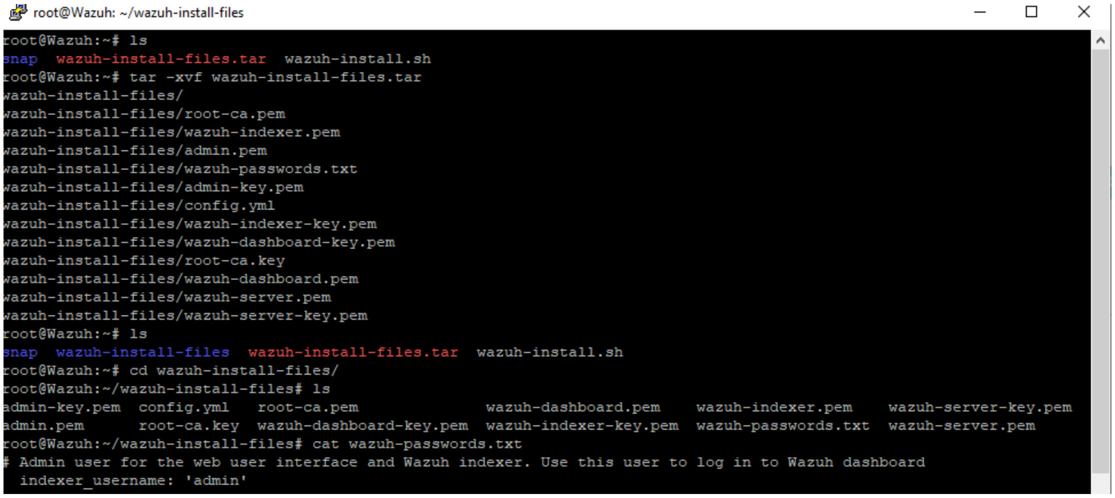


```
Elasticsearch issue solution
Step 1: Create the Directory
Run the following command to make sure the directory /etc/elasticsearch/jvm.options.d exists:
'mkdir -p /etc/elasticsearch/jvm.options.d'
Step 2: Create and Edit the jvm.options File
'nano /etc/elasticsearch/jvm.options.d/custom-jvm.options'
Step 3: Add the Following Configuration
Copy and paste the following lines into the file:
'
-Dlog4j2.formatMsgNoLookups=true
-Xms2g
-Xmx2g
'
Explanation:
-Dlog4j2.formatMsgNoLookups=true → Security fix to prevent Log4j vulnerabilities.
-Xms2g → Sets the minimum heap size to 2GB.
-Xmx2g → Sets the maximum heap size to 2GB.
If you have low memory, reduce these values (e.g., -Xms1g, -Xmx1g).

Step 4: Save and Exit, Press CTRL + X, Press Y to save, Press Enter
Step 5: Restart Elasticsearch
```

- Now able to access thehive dashboard by browsing 'TheHiveIP:9000'
- Login with 'admin@thehive.local ' , 'password: secret'

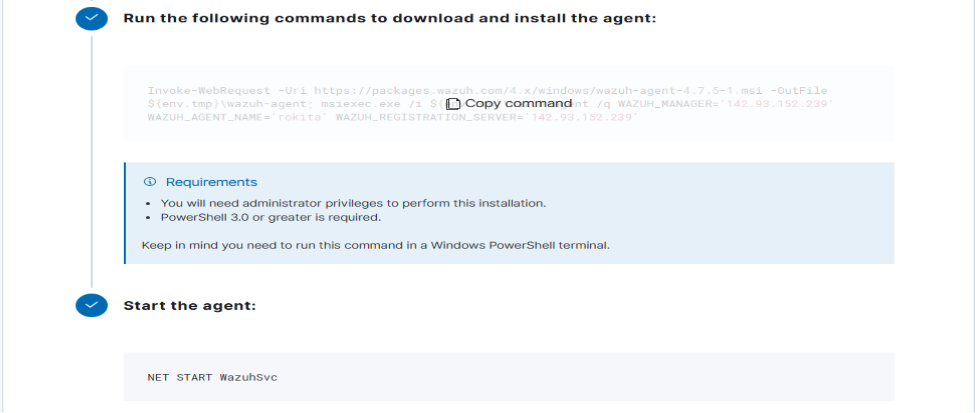
OVER TO WAZUH TO ADD AGENT TO WAZUH MANAGER

Incase the wazuh password was missed, it can be achieved on the console by navigating to the passwords file as seen below. Take note of admin details and API user details.



```
root@Wazuh:~# ls
snap  wazuh-install-files.tar  wazuh-install.sh
root@Wazuh:~# tar -xvf wazuh-install-files.tar
wazuh-install-files/
wazuh-install-files/root-ca.pem
wazuh-install-files/wazuh-indexer.pem
wazuh-install-files/admin.pem
wazuh-install-files/wazuh-passwords.txt
wazuh-install-files/admin-key.pem
wazuh-install-files/config.yml
wazuh-install-files/wazuh-indexer-key.pem
wazuh-install-files/wazuh-dashboard-key.pem
wazuh-install-files/root-ca.key
wazuh-install-files/wazuh-dashboard.pem
wazuh-install-files/wazuh-server.pem
wazuh-install-files/wazuh-server-key.pem
root@Wazuh:~# ls
snap  wazuh-install-files  wazuh-install-files.tar  wazuh-install.sh
root@Wazuh:~# cd wazuh-install-files/
root@Wazuh:~/wazuh-install-files# ls
admin-key.pem  config.yml   root-ca.pem              wazuh-dashboard.pem    wazuh-indexer.pem    wazuh-server-key.pem
admin.pem      root-ca.key  wazuh-dashboard-key.pem  wazuh-indexer-key.pem  wazuh-passwords.txt  wazuh-server.pem
root@Wazuh:~/wazuh-install-files# cat wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
```

- To add agent to wazuh manager
- On the wazuh dashboard, click on 'add agent', select windows (as is the case for my lab)
- Put in wazuh publicIP for server address, Assign the agent name
- Copy the command in step4 to download and install agent on windows client

- 

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile
${env.tmp}\wazuh-agent; msiexec.exe /i ${ Copy command nt /q WAZUH_MANAGER='142.93.152.239'
WAZUH_AGENT_NAME='rokita' WAZUH_REGISTRATION_SERVER='142.93.152.239'
```

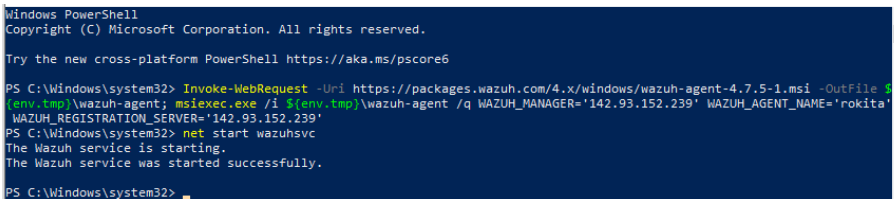
Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

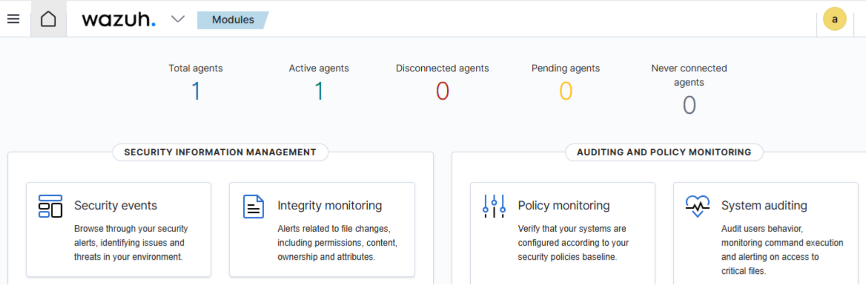
Keep in mind you need to run this command in a Windows PowerShell terminal.

Start the agent:

```
NET START WazuhSvc
```

- Run the command on Powershell as Administrator on the windows machine
- 

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $
{env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='142.93.152.239' WAZUH_AGENT_NAME='rokita'
 WAZUH_REGISTRATION_SERVER='142.93.152.239'
PS C:\Windows\system32> net start wazuhsvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32> _
```

- The agent is now added, that means the windows machine is now checking into wazuh successfully
- 

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
1	1	0	0	0

SECURITY INFORMATION MANAGEMENT

Security events — Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring — Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

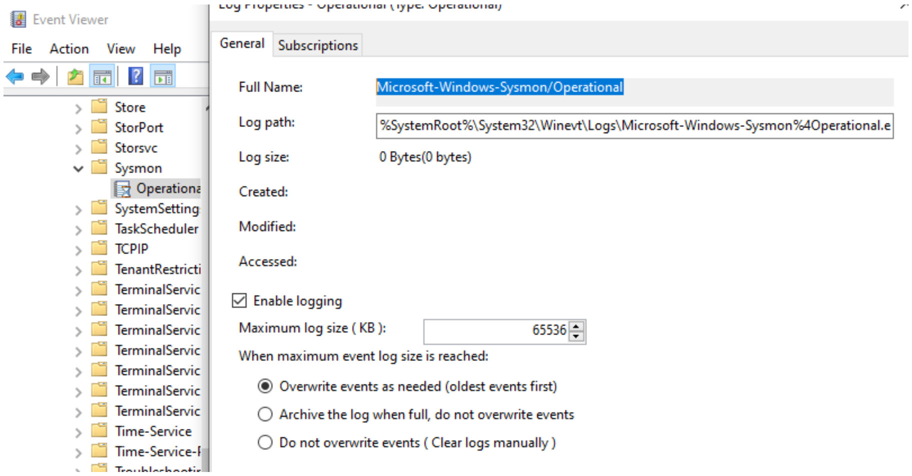
Policy monitoring — Verify that your systems are configured according to your security policies baseline.

System auditing — Audit users behavior, monitoring command execution and alerting on access to critical files.

Generate Telemetry from Windows & Ingest into Wazuh

ON WINDOWS MACHINE

- Modify wazuh configuration file; ‘ossec.conf’. This file is located in ‘ossec-agent’ under ‘program files x86’ under ‘This PC’
- Right click and open with notepad. This conf file contains everything related to wazuh.
- First make a backup copy of ossec.conf file, now configure.
- Scroll down to log analysis, copy the local file data for application and paste right below.

- Change from application to sysmon channel name.
- To get sysmon channel name, go to event viewer,expand application and services, expand microsoft, expand windows, locate sysmon, right click on operational, go to properties, copy channal name 'full name'.
- 

  Full Name: Microsoft-Windows-Sysmon/Operational

  Log path: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Sysmon%4Operational.e

  Log size: 0 Bytes(0 bytes)

  Created:

  Modified:

  Accessed:

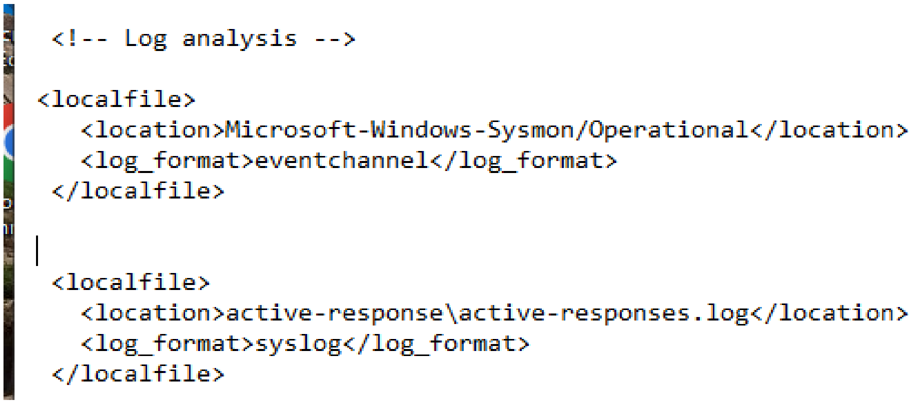
  ☑ Enable logging

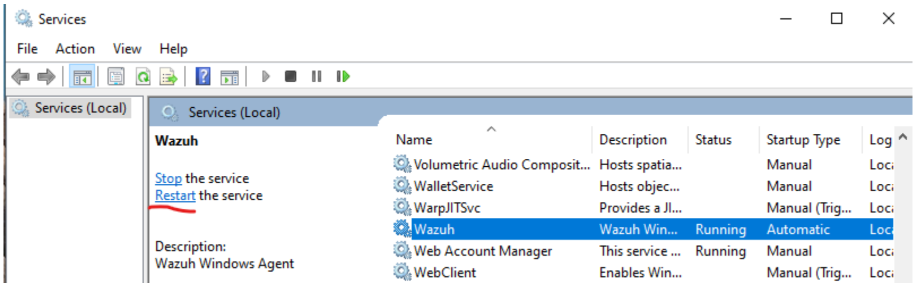
  Maximum log size (KB): 65536

  When maximum event log size is reached:

  ● Overwrite events as needed (oldest events first)

  ○ Archive the log when full, do not overwrite events

  ○ Do not overwrite events (Clear logs manually)
- Next, on the ossec.conf file, clear out system, application and security configuration data. For the sake of this task, only sysmon telemetry required.
- 

```
 <!-- Log analysis -->

<localfile>
   <location>Microsoft-Windows-Sysmon/Operational</location>
   <log_format>eventchannel</log_format>
 </localfile>


 <localfile>
   <location>active-response\active-responses.log</location>
   <log_format>syslog</log_format>
 </localfile>
```
- Open up services, locate wazuh and restart the service (this is always required after modifying configuration files).
- 

  Wazuh

  Stop the service
  Restart the service

  Description:
  Wazuh Windows Agent

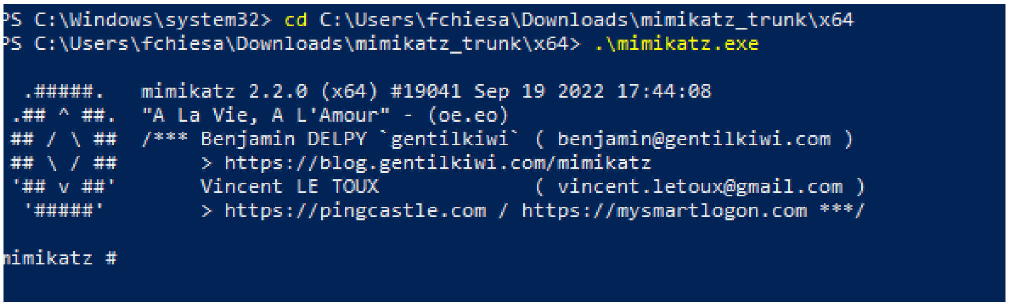
Name	Description	Status	Startup Type	Log
Volumetric Audio Composit...	Hosts spatia...		Manual	Loc
WalletService	Hosts objec...		Manual	Loc
WarpJITSvc	Provides a JI...		Manual (Trig...	Loc
Wazuh	Wazuh Win...	Running	Automatic	Loc
Web Account Manager	This service ...	Running	Manual	Loc
WebClient	Enables Win...		Manual (Trig...	Loc
- Head over to the wazuh dashboard, under security events, search for sysmon to check for successful configuration.

DOWNLOAD & RUN MIMIKATZ

Mimikatz is an application attackers and red-teamers use to extract credentials from a machine.

Before downloading mimikats, need to exclude Downloads

- Go to windows security,
- Under virus & threat protection, manage settings,
- Under Exclusion, click on 'add or remove' exclusion , add as folder, select downloads folder where mimikatz will be downloaded.
- Download mimikatz and save in the folder, then extract all.
- Head back over to powershell, change into mimikatz directory
- Run mimikatz.

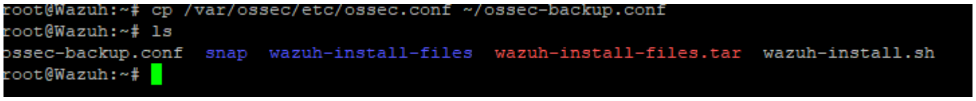


```
PS C:\Windows\system32> cd C:\Users\fchiesa\Downloads\mimikatz_trunk\x64
PS C:\Users\fchiesa\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
```

-
- Head over to wazuh dashboard to check if there are any mimikatz logs
- No results, because wazuh is not confiured to trigger the alerts.
- I need to change this by configuring the ossec.conf file on the wazuh manager to make it log everything or create rules that look at specific events so when a particular event does exist, it will trigger an alert inside wazuh.

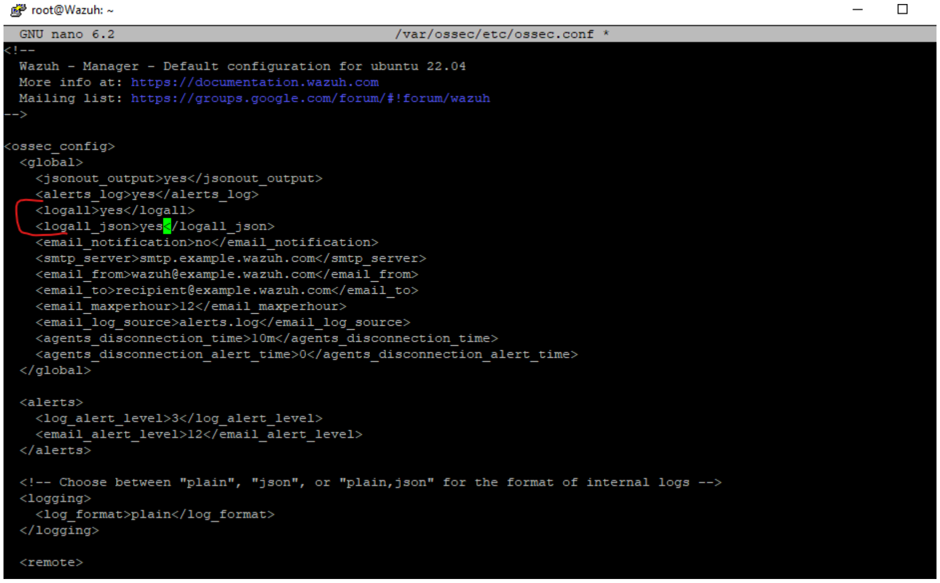
HEAD OVER TO WAZUH MANAGER CONSOLE TO CONFIGURE OSSEC.CONF

- Firstly, create a backup of the file



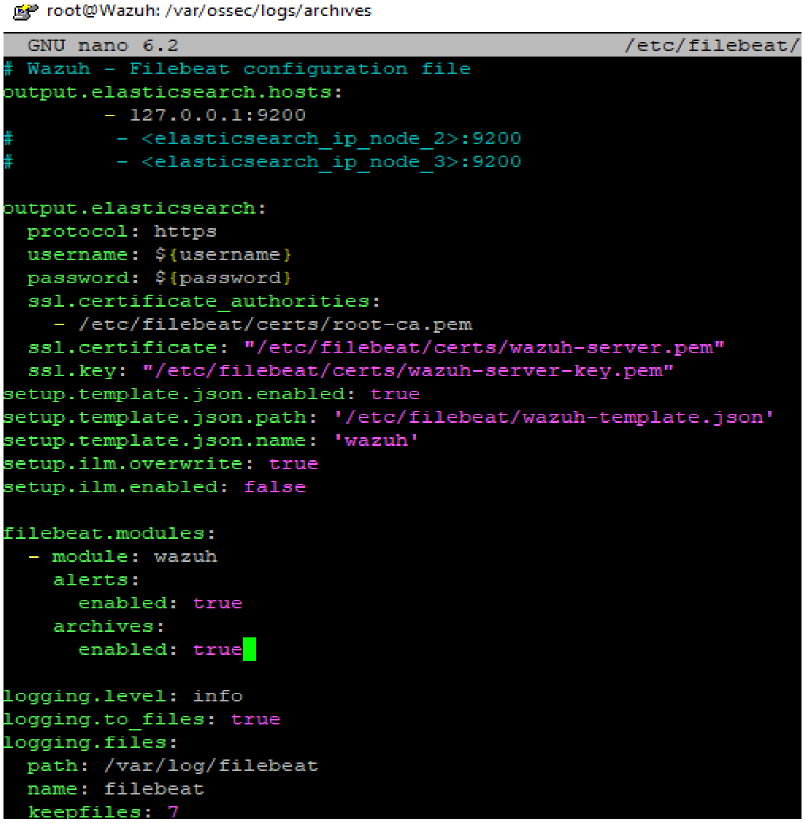
```
root@Wazuh:~# cp /var/ossec/etc/ossec.conf ~/ossec-backup.conf
root@Wazuh:~# ls
ossec-backup.conf  snap  wazuh-install-files  wazuh-install-files.tar  wazuh-install.sh
root@Wazuh:~#
```

-
- 'nano /var/ossec/etc/ossec.conf'
- Change logall and logall.json from no to yes
- Restart wazuh service.
- Wazuh will begin to archive all the logs and put them into a file called Archives located in /var/ossec/logs/archives/

- 

```
  GNU nano 6.2                                       /var/ossec/etc/ossec.conf *
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

  <remote>
```

In order for wazuh to start ingesting all these logs, I need to change the configuration in filebeat.

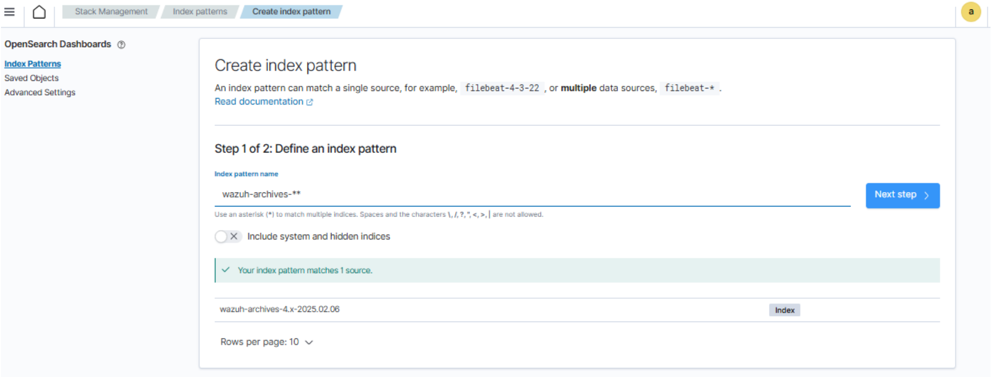
- ‘nano /etc/filebeat/filebeat.yml’
- Change ‘archives_enabled’ settings from false to true


```
  GNU nano 6.2                                /etc/filebeat/
# Wazuh - Filebeat configuration file
output.elasticsearch.hosts:
        - 127.0.0.1:9200
#         - <elasticsearch_ip_node_2>:9200
#         - <elasticsearch_ip_node_3>:9200

output.elasticsearch:
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/wazuh-server.pem"
  ssl.key: "/etc/filebeat/certs/wazuh-server-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: true

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
```

- Restart the filebeat service

CREATE NEW INDEX ON WAZUH DASHBOARD

- Head over to wazuh dashboard to create new index, click on hamburger icon at top-left corner and scroll down to stack management.
- Click on index patterns then create index pattern, input name 'wazuh-archives*'



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
Read documentation

Step 1 of 2: Define an index pattern

Index pattern name: wazuh-archives-**

Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.

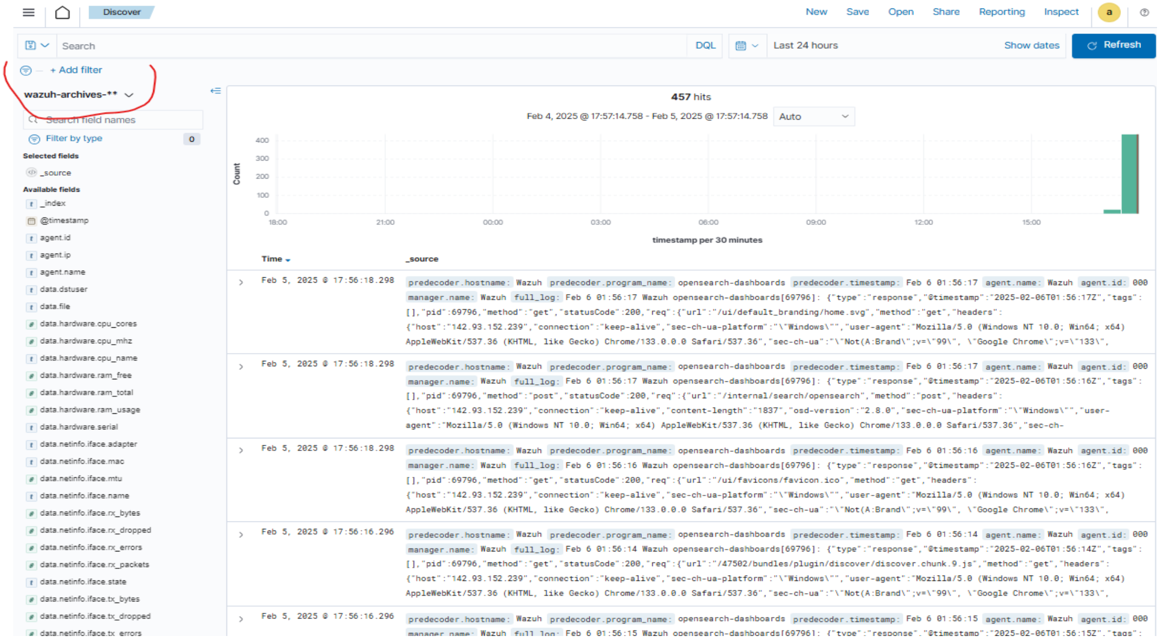
○ ✕ Include system and hidden indices

✓ Your index pattern matches 1 source.

wazuh-archives-4.x-2025.02.06 — Index

Rows per page: 10

-
- For time field, select timestamp at the bottom
- Now click on the hamburger icon and head over to discover, change to archives index

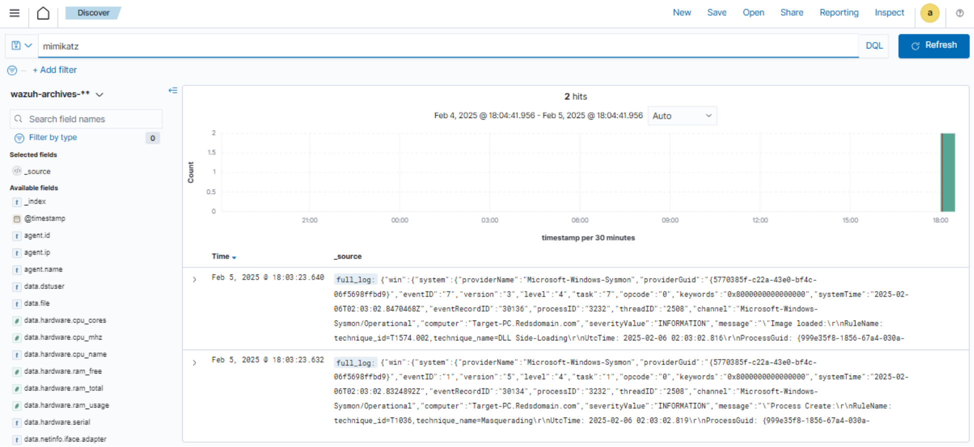


Selected fields: _source

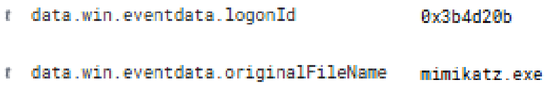
Available fields: _index, @timestamp, agent.id, agent.ip, agent.name, data.dstuser, data.file, data.hardware.cpu_cores, data.hardware.cpu_mhz, data.hardware.cpu_name, data.hardware.ram_free, data.hardware.ram_total, data.hardware.ram_usage, data.hardware.serial, data.netinfo.iface.adapter, data.netinfo.iface.mac, data.netinfo.iface.mtu, data.netinfo.iface.name, data.netinfo.iface.rx_bytes, data.netinfo.iface.rx_dropped, data.netinfo.iface.rx_errors, data.netinfo.iface.rx_packets, data.netinfo.iface.state, data.netinfo.iface.tx_bytes, data.netinfo.iface.tx_dropped, data.netinfo.iface.tx_errors

```
Time                         _source
Feb 5, 2025 @ 17:56:18.298   predecoder.hostname: Wazuh predecoder.program_name: opensearch-dashboards predecoder.timestamp: Feb 6 01:56:17 agent.name: Wazuh agent.id: 000
                             manager.name: Wazuh full_log: Feb 6 01:56:17 Wazuh opensearch-dashboards[69796]: {"type":"response","@timestamp":"2025-02-06T01:56:17Z","tags":
                             [],"pid":69796,"method":"get","statusCode":200,"req":{"url":"/ui/default_branding/home.svg","method":"get","headers":
                             {"host":"142.93.152.239","connection":"keep-alive","sec-ch-ua-platform":"\"Windows\"","user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                             AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36","sec-ch-ua":"\"Not(A:Brand\";v=\"99\", \"Google Chrome\";v=\"133\",
Feb 5, 2025 @ 17:56:18.298   predecoder.hostname: Wazuh predecoder.program_name: opensearch-dashboards predecoder.timestamp: Feb 6 01:56:17 agent.name: Wazuh agent.id: 000
                             manager.name: Wazuh full_log: Feb 6 01:56:17 Wazuh opensearch-dashboards[69796]: {"type":"response","@timestamp":"2025-02-06T01:56:16Z","tags":
                             [],"pid":69796,"method":"post","statusCode":200,"req":{"url":"/internal/search/opensearch","method":"post","headers":
                             {"host":"142.93.152.239","connection":"keep-alive","content-length":"1837","osd-version":"2.8.0","sec-ch-ua-platform":"\"Windows\"","user-
                             agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36","sec-ch-
Feb 5, 2025 @ 17:56:18.298   predecoder.hostname: Wazuh predecoder.program_name: opensearch-dashboards predecoder.timestamp: Feb 6 01:56:16 agent.name: Wazuh agent.id: 000
                             manager.name: Wazuh full_log: Feb 6 01:56:16 Wazuh opensearch-dashboards[69796]: {"type":"response","@timestamp":"2025-02-06T01:56:16Z","tags":
                             [],"pid":69796,"method":"get","statusCode":200,"req":{"url":"/ui/favicons/favicon.ico","method":"get","headers":
                             {"host":"142.93.152.239","connection":"keep-alive","sec-ch-ua-platform":"\"Windows\"","user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                             AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36","sec-ch-ua":"\"Not(A:Brand\";v=\"99\", \"Google Chrome\";v=\"133\",
Feb 5, 2025 @ 17:56:16.296   predecoder.hostname: Wazuh predecoder.program_name: opensearch-dashboards predecoder.timestamp: Feb 6 01:56:14 agent.name: Wazuh agent.id: 000
                             manager.name: Wazuh full_log: Feb 6 01:56:14 Wazuh opensearch-dashboards[69796]: {"type":"response","@timestamp":"2025-02-06T01:56:14Z","tags":
                             [],"pid":69796,"method":"get","statusCode":200,"req":{"url":"/47502/bundles/plugin/discover/discover.chunk.9.js","method":"get","headers":
                             {"host":"142.93.152.239","connection":"keep-alive","sec-ch-ua-platform":"\"Windows\"","user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                             AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36","sec-ch-ua":"\"Not(A:Brand\";v=\"99\", \"Google Chrome\";v=\"133\",
Feb 5, 2025 @ 17:56:16.296   predecoder.hostname: Wazuh predecoder.program_name: opensearch-dashboards predecoder.timestamp: Feb 6 01:56:15 agent.name: Wazuh agent.id: 000
                             manager.name: Wazuh full_log: Feb 6 01:56:15 Wazuh opensearch-dashboards[69796]: {"type":"response","@timestamp":"2025-02-06T01:56:15Z","tags":
```

-

- 

```
Feb 5, 2025 @ 18:03:23.640  full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-
06f5698ffbd9}","eventID":"7","version":"3","level":"4","task":"7","opcode":"0","keywords":"0x8000000000000000","systemTime":"2025-02-
06T02:03:02.8470468Z","eventRecordID":"30136","processID":"3232","threadID":"2508","channel":"Microsoft-Windows-
Sysmon/Operational","computer":"Target-PC.Redsdomain.com","severityValue":"INFORMATION","message":"\"Image loaded:\r\nRuleName:
technique_id=T1574.002,technique_name=DLL Side-Loading\r\nUtcTime: 2025-02-06 02:03:02.816\r\nProcessGuid: {999e35f8-1856-67a4-030a-

Feb 5, 2025 @ 18:03:23.632  full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-
06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2025-02-
06T02:03:02.8324892Z","eventRecordID":"30134","processID":"3232","threadID":"2508","channel":"Microsoft-Windows-
Sysmon/Operational","computer":"Target-PC.Redsdomain.com","severityValue":"INFORMATION","message":"\"Process Create:\r\nRuleName:
technique_id=T1036,technique_name=Masquerading\r\nUtcTime: 2025-02-06 02:03:02.819\r\nProcessGuid: {999e35f8-1856-67a4-030a-
```

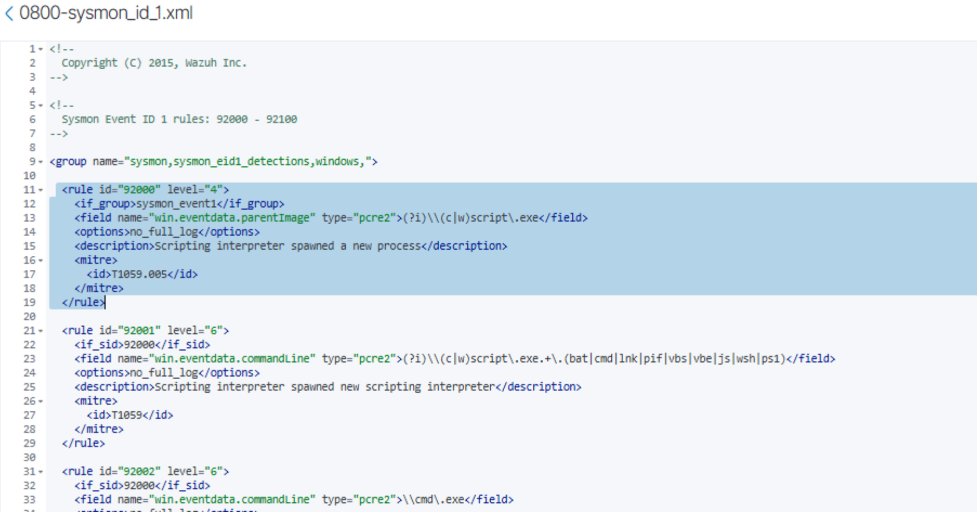


```
t  data.win.eventdata.logonId             0x3b4d20b

t  data.win.eventdata.originalFileName    mimikatz.exe
```

-
- The ‘originalfilename’ field is what in extended event data is what I use to create a trigger.

TO CREATE TRIGGER ALERT

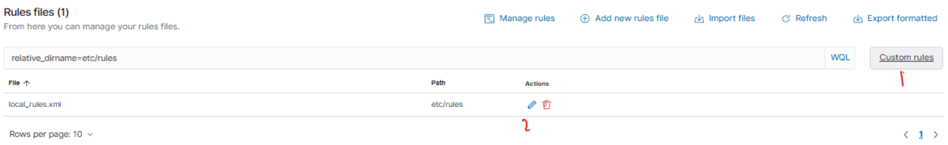
- Wazuh manager has some built-in rules that can be used
- Go to homepage, click on dropdown next to it
- Go to management, then rules, click on ‘manage rules files’.
- Search for sysmon; these are sysmon rules built into wazuh.
- View the Id-1 rule, copy one of the rulesets in the rule



< 0800-sysmon_id_1.xml

```
<!--
  Copyright (C) 2015, Wazuh Inc.
-->

<!--
  Sysmon Event ID 1 rules: 92000 - 92100
-->

<group name="sysmon,sysmon_eid1_detections,windows,">

  <rule id="92000" level="4">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.parentImage" type="pcre2">(?i)\\(c|w)script\.exe</field>
    <options>no_full_log</options>
    <description>Scripting interpreter spawned a new process</description>
    <mitre>
      <id>T1059.005</id>
    </mitre>
  </rule>

  <rule id="92001" level="6">
    <if_sid>92000</if_sid>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)\\(c|w)script\.exe.+\.(bat|cmd|lnk|pif|vbs|vbe|js|wsh|ps1)</field>
    <options>no_full_log</options>
    <description>Scripting interpreter spawned new scripting interpreter</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="92002" level="6">
    <if_sid>92000</if_sid>
    <field name="win.eventdata.commandLine" type="pcre2">\\cmd\.exe</field>
```

-
- Head back to the rules files, click on custom rules, click on the edit icon.

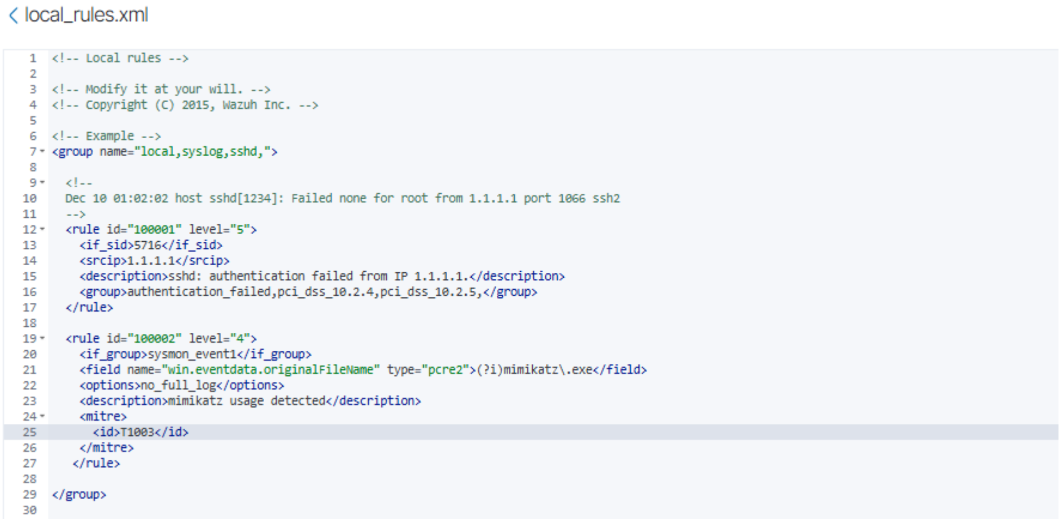
-

Rules files (1)

From here you can manage your rules files.

relative_dirname=etc/rules

File	Path	Actions
local_rules.xml	etc/rules	

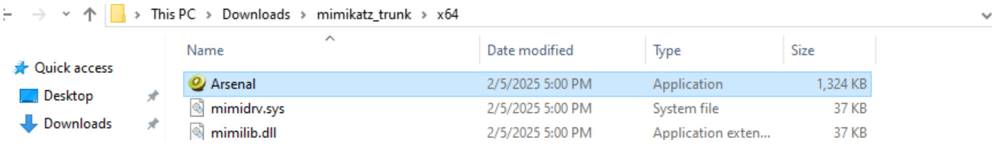
- Paste the copied rule into this file and modify.
  - ❖ Custom ruleIDs always start from 100000. Change to 100002
  - ❖ Change level to 15 (highest)
  - ❖ Fieldname = originalFileName (case sensitivity is important)
  - ❖ Change mitre Id to T1003 (credential dumping)
  - ❖ Restart manager


< local_rules.xml

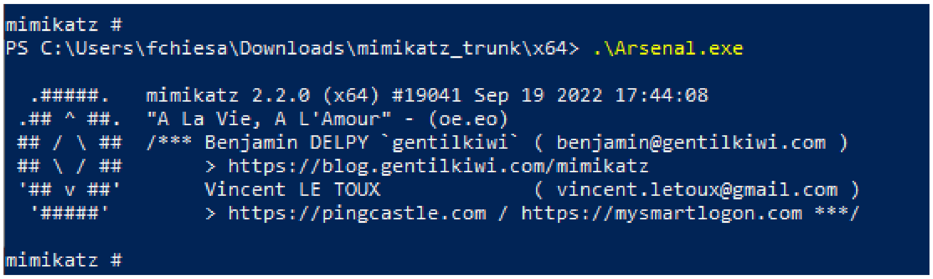
```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100002" level="4">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.originalFileName" type="pcre2">(?i)mimikatz\.exe</field>
    <options>no_full_log</options>
    <description>mimikatz usage detected</description>
    <mitre>
      <id>T1003</id>
    </mitre>
   </rule>

</group>

```

- Ruleset configured.

- Change mimikatz filename just to test the rule
- Mimikatz renamed to ‘Arsenal’
- Head over to powershell and run Arsenal



Name	Date modified	Type	Size
Arsenal	2/5/2025 5:00 PM	Application	1,324 KB
mimidrv.sys	2/5/2025 5:00 PM	System file	37 KB
mimilib.dll	2/5/2025 5:00 PM	Application exten...	37 KB



```
mimikatz #
PS C:\Users\fchiesa\Downloads\mimikatz_trunk\x64> .\Arsenal.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
```

- Back to wazuh dashboard, refresh security events

- Mimikatz still detected because we configured the alerts to be triggered by originalFileName

In the next part of this SOC-Automation Project, I will be configuring and setting up my workflow with shuffle and other resources.