



## Security Operations Center

Cybersecurity & Security Operations Center

**Nagels Viktor**  
**R0840938**  
**3ITF – CCS01**

Academiejaar 2021-2022  
Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

## Table of Contents

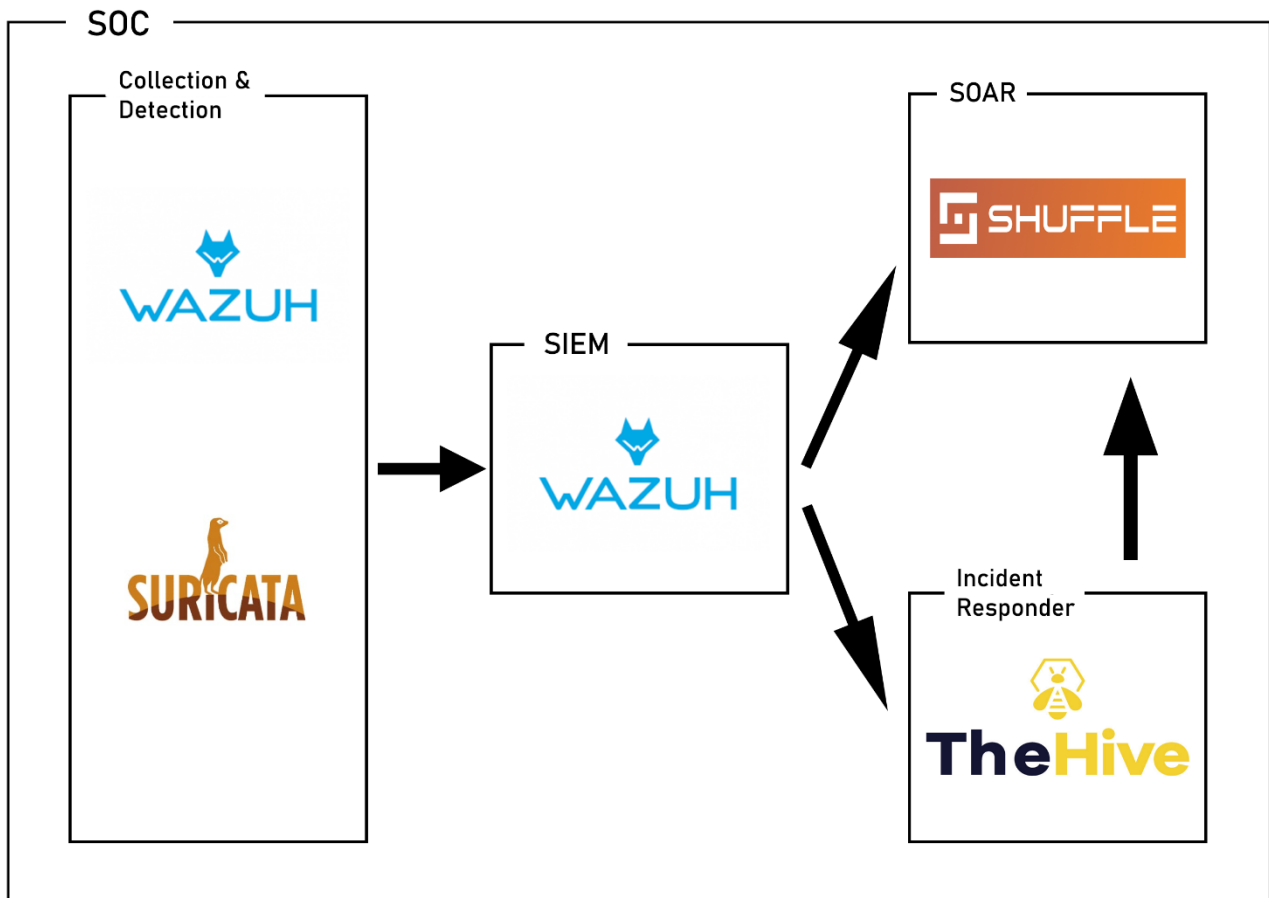
<b>1</b>	<b>OVERVIEW .....</b>	<b>2</b>
<b>1.1</b>	<b>Network .....</b>	<b>2</b>
<b>1.2</b>	<b>Technology's .....</b>	<b>2</b>
<b>1.3</b>	<b>Shuffle workflow .....</b>	<b>3</b>
<b>2</b>	<b>INSTALLATION .....</b>	<b>4</b>
<b>2.1</b>	<b>Wazuh server .....</b>	<b>4</b>
<b>2.2</b>	<b>Shuffle .....</b>	<b>5</b>
<b>2.3</b>	<b>TheHive.....</b>	<b>5</b>
<b>2.4</b>	<b>Suricata .....</b>	<b>7</b>
<b>3</b>	<b>CONFIGURATION .....</b>	<b>8</b>
<b>3.1</b>	<b>connect client to wazuh .....</b>	<b>8</b>
<b>3.2</b>	<b>connect wazuh with suricata.....</b>	<b>8</b>
<b>3.3</b>	<b>shuffle workflow .....</b>	<b>9</b>
<b>4</b>	<b>DEMO .....</b>	<b>10</b>
<b>4.1</b>	<b>Screenshots .....</b>	<b>10</b>
<b>4.2</b>	<b>Video.....</b>	<b>12</b>
<b>5</b>	<b>REFERENCES .....</b>	<b>13</b>

# 1 OVERVIEW

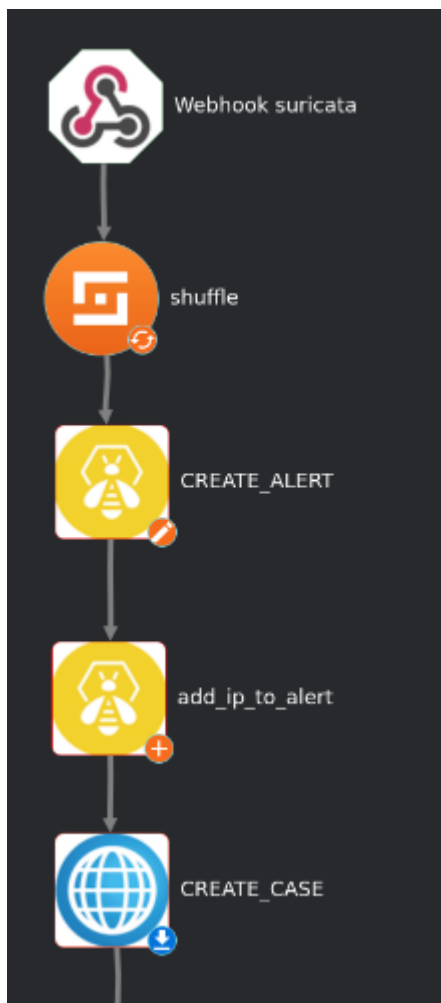
## 1.1 Network

Device	Ip address	Subnet	Default-gateway
Wazuh Server	10.0.2.2	255.255.255.0	10.0.2.1
Shuffle Server	10.0.2.3	255.255.255.0	10.0.2.1
TheHive server	10.0.2.4	255.255.255.0	10.0.2.1
Client	10.0.2.20 (DHCP)	255.255.255.0	10.0.2.1

## 1.2 Technology's



### 1.3 Shuffle workflow

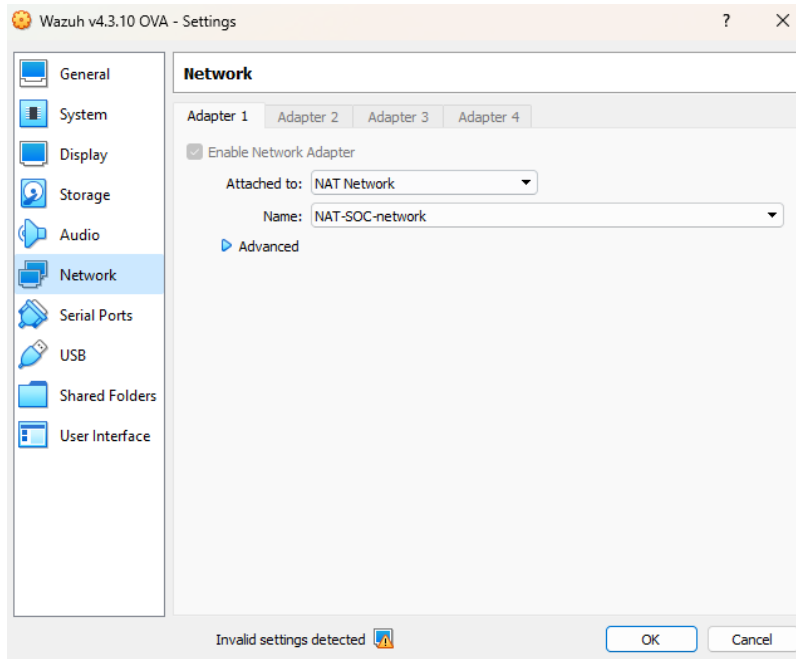


## 2 INSTALLATION

### 2.1 Wazuh server

Installed the Wazuh Virtual Machine.

Then change the network interface to NAT Network – Nat-SOC-network:



Set Static ip in `/etc/sysconfig/network-scripts/ifcfg-eth0`:

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=10.0.2.2
PREFIX=24

GATEWAY=10.0.2.1

DNS1=8.8.8.8
DNS2=8.8.4.4
DEFROUTE=yes
IPV4_FAILURE_FATAL=no

# disable ipv6 #
IPV6INIT=no
NAME=eth0

UUID=339f8584-c888-48aa-b33a-84b8d144a4d3
DEVICE=eth0
ONBOOT=yes
```

## 2.2 Shuffle

Setup ubuntu server.

Give network interface: NAT network – NAT-SOC-network

Set static ip in: /etc/netplan/00...

Execute following commands

```
##install docker-compose
sudo apt-get install docker-compose -y

##clone github repo
git clone https://github.com/Shuffle/Shuffle
cd Shuffle

##make shuffle-database directory & give rights
mkdir shuffle-database
sudo chown -R 1000:1000 shuffle-database

#Start shuffle
docker-compose up -d
```

## 2.3 TheHive

Setup ubuntu server.

Give network interface: NAT network – NAT-SOC-network

Set static ip in: /etc/netplan/00...

Execute following commands

```
##install java vm
apt-get install -y openjdk-8-jre-headless
echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" >> /etc/environment
export JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64"

##install cassandra
curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt-key
add -
echo "deb http://www.apache.org/dist/cassandra/debian 311x main" |
sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list
```

```
sudo apt update
sudo apt install cassandra

##change sql database
cqlsh localhost 9042
UPDATE system.local SET cluster_name = 'soc' where key='local';

##run
nodetool flush

## content from /etc/cassandra/cassandra.yaml
cluster_name: 'soc'
listen_address: '10.0.2.4' # address for nodes
rpc_address: '10.0.2.4' # address for clients
seed_provider:
  - class_name: org.apache.cassandra.locator.SimpleSeedProvider
    parameters:
      # Ex: "<ip1>,<ip2>,<ip3>"
      - seeds: '10.0.2.4' # self for the first node
data_file_directories:
  - '/var/lib/cassandra/data'
commitlog_directory: '/var/lib/cassandra/commitlog'
saved_caches_directory: '/var/lib/cassandra/saved_caches'
hints_directory:
  - '/var/lib/cassandra/hints'

##Restart cassandra
service cassandra restart

##get thehive packages
curl https://raw.githubusercontent.com/TheHive-Project/TheHive/master/PGP-PUBLIC-KEY | sudo apt-key add -

##install thehive4
echo 'deb https://deb.thehive-project.org release main' | sudo tee -a
/etc/apt/sources.list.d/thehive-project.list
sudo apt-get update
sudo apt-get install thehive4

## Create dedicated folders
mkdir /opt/thp/thehive/index
chown thehive:thehive -R /opt/soc/thehive/index
mkdir /opt/thp/thehive/files
chown thehive:thehive -R /opt/soc/thehive/files
mkdir /opt/thp/thehive/database
chown thehive:thehive -R /opt/soc/thehive/database
```

```
## Storage configuration
storage {
  provider = localfs
  localfs.location = /opt/thp/thehive/files
}

##start the hive
service thehive start
```

## 2.4 Suricata

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y

##download rulesets
cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-
6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules
/etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
```



## 3 CONFIGURATION

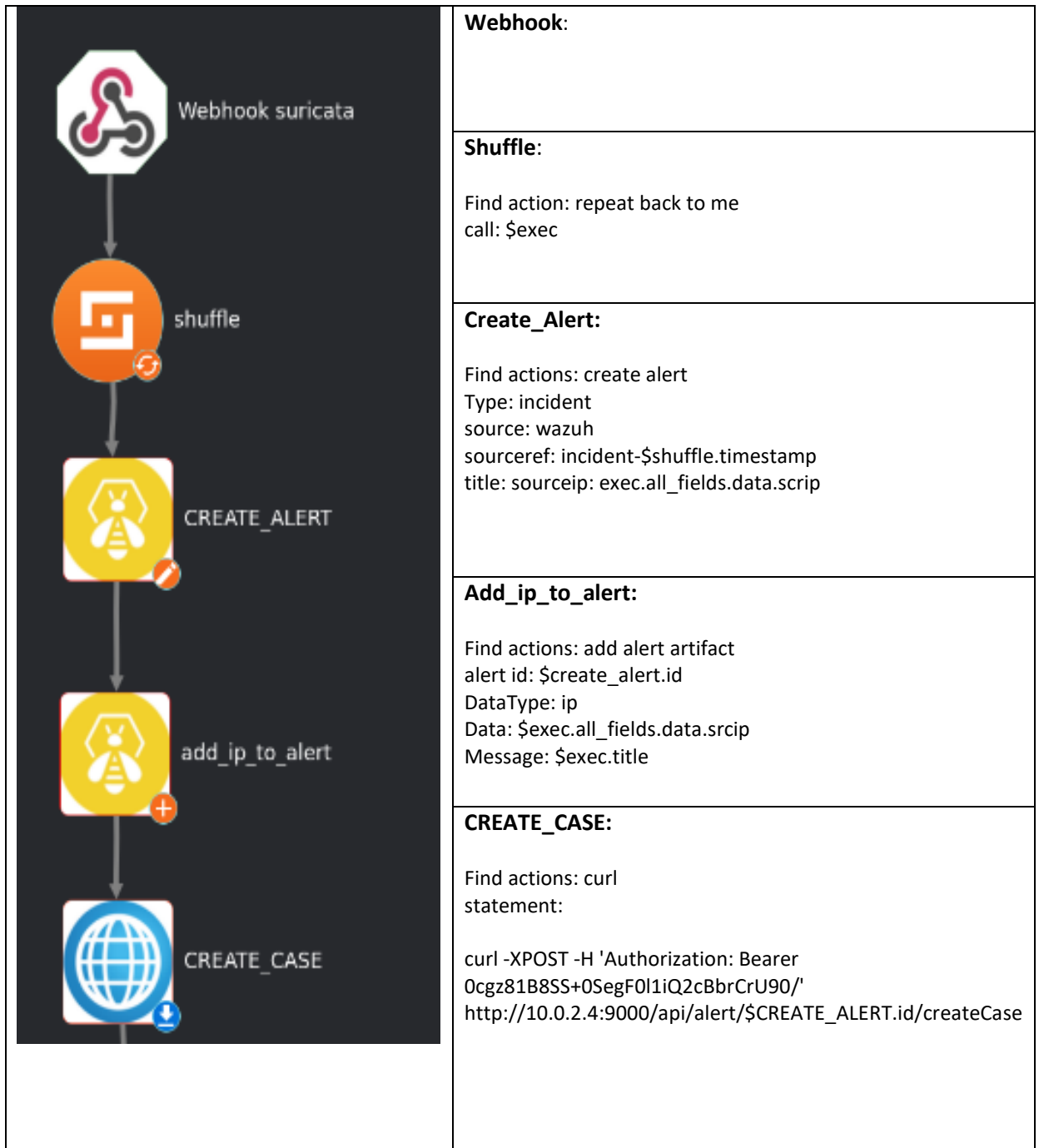
### 3.1 connect client to wazuh

```
curl -so wazuh-agent-4.3.10.deb  
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-  
agent_4.3.10-1_amd64.deb && sudo WAZUH_MANAGER='10.0.2.2'  
WAZUH_AGENT_GROUP='default' dpkg -i ./wazuh-agent-4.3.10.deb
```

### 3.2 connect wazuh with suricata

```
## modify suricata settings to /etc/suricata/suricata.yaml  
HOME_NET: "10.0.2.20"  
EXTERNAL_NET: "any"  
  
default-rule-path: /etc/suricata/rules  
rule-files:  
- "*.rules"  
  
# Global stats configuration  
stats:  
enabled: no  
  
# Linux high speed capture support  
af-packet:  
- interface: enp0s3  
  
##resetart suricata  
sudo systemctl restart suricata  
  
##add following configuration to /var/ossec/etc/ossec.conf  
<ossec_config>  
  <localfile>  
    <log_format>json</log_format>  
    <location>/var/log/suricata/eve.json</location>  
  </localfile>  
</ossec_config>  
  
##restart wazuh-agent
```

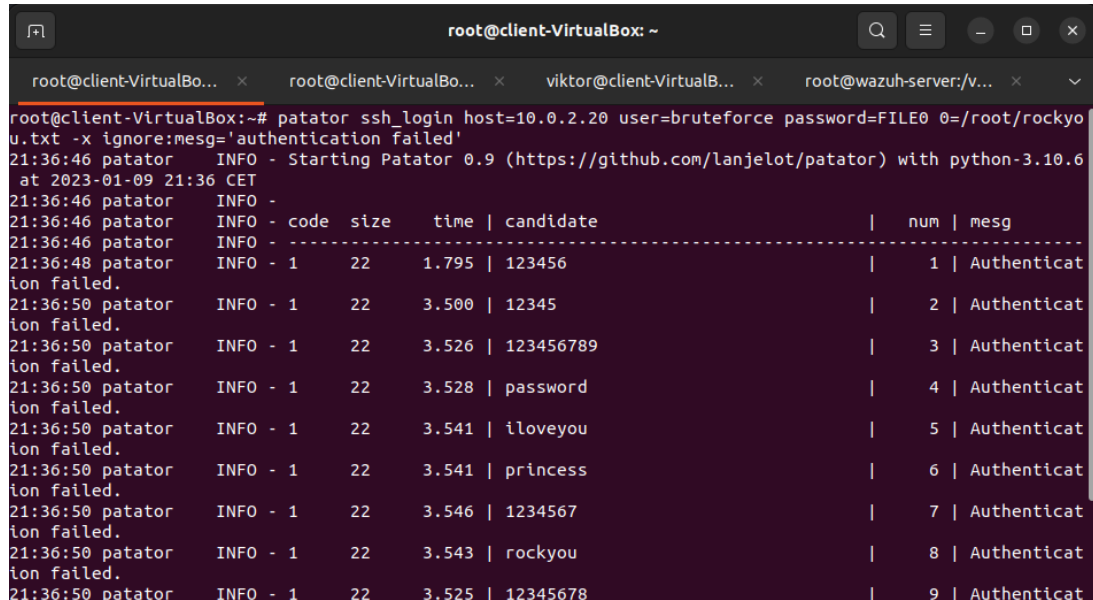
### 3.3 shuffle workflow



## 4 DEMO

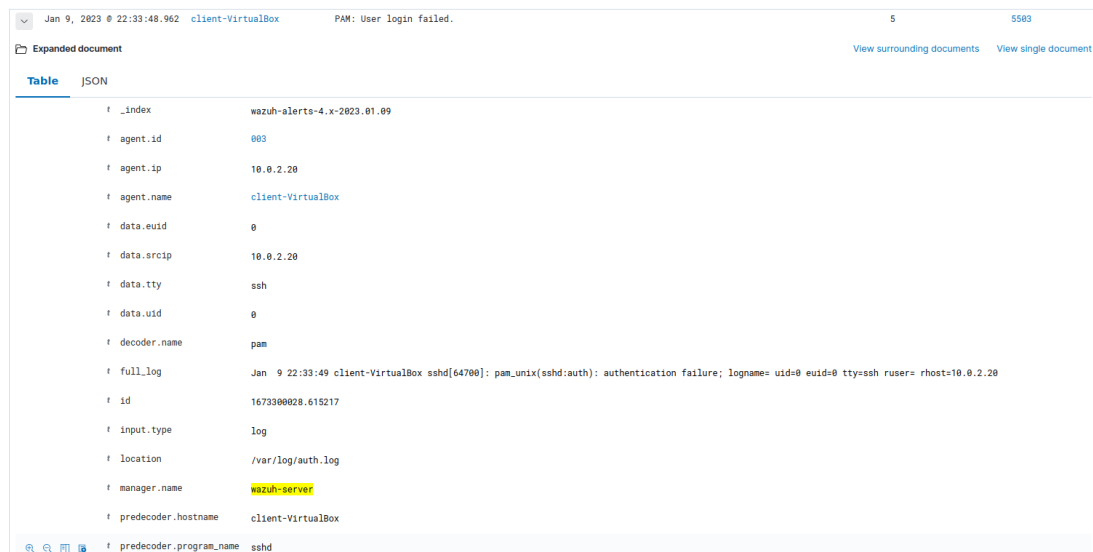
### 4.1 Screenshots

Bruteforce attack ssh:



```
root@client-VirtualBox: ~
root@client-VirtualBo... x root@client-VirtualBo... x viktor@client-VirtualB... x root@wazuh-server:/v... x
root@client-VirtualBox:~# patator ssh_login host=10.0.2.20 user=bruteforce password=FILE0 0=/root/rockyou.txt -x ignore:mesg='authentication failed'
21:36:46 patator INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.10.6 at 2023-01-09 21:36 CET
21:36:46 patator INFO -
21:36:46 patator INFO - code size time | candidate | num | mesg
21:36:48 patator INFO - 1 22 1.795 | 123456 | 1 | Authentication failed.
21:36:50 patator INFO - 1 22 3.500 | 12345 | 2 | Authentication failed.
21:36:50 patator INFO - 1 22 3.526 | 123456789 | 3 | Authentication failed.
21:36:50 patator INFO - 1 22 3.528 | password | 4 | Authentication failed.
21:36:50 patator INFO - 1 22 3.541 | iloveyou | 5 | Authentication failed.
21:36:50 patator INFO - 1 22 3.541 | princess | 6 | Authentication failed.
21:36:50 patator INFO - 1 22 3.546 | 1234567 | 7 | Authentication failed.
21:36:50 patator INFO - 1 22 3.543 | rockyou | 8 | Authentication failed.
21:36:50 patator INFO - 1 22 3.525 | 12345678 | 9 | Authentication failed.
```

Wazuh dashboard alert:



Field	Value
_index	wazuh-alerts-4.x-2023.01.09
agent.id	003
agent.ip	10.0.2.20
agent.name	client-VirtualBox
data.euid	0
data.srcip	10.0.2.20
data.tty	ssh
data.uid	0
decoder.name	pam
full_log	Jan 9 22:33:49 client-VirtualBox sshd[64700]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.20
id	1673300028.615217
input.type	log
location	/var/log/auth.log
manager.name	wazuh-server
predecoder.hostname	client-VirtualBox
predecoder.program_name	sshd

Thehive cases:

TheHive - Cases Workflow - Brute force S: X Wazuh - Wazuh

10.0.2.4:9000/index.html#/cases

TheHive + New Case My tasks 1 Waiting tasks 0 Alerts 0 Dashboards Search

List of cases (9 of 9)

No case selected Quick Filters Sort by Custom Fields Stats Filters 15 per page

Filters

status Any Of Open Enter a status

+ Add a filter Clear Search

1 filter(s) applied: status: Open Clear filters

Status	Number	Title	Severity	Details	Assignee	Dates
Open	#28	source ip: 10.0.2.20 DESC: PAM: User login failed.	Low	Tasks: 0 Observables: 1 TTPs: 0	V	S: 01/09/23 22:34 C: 01/09/23 22:34
Open	#27	source ip: 10.0.2.20 DESC: PAM: User login failed.	Low	Tasks: 0 Observables: 1 TTPs: 0	V	S: 01/09/23 22:34 C: 01/09/23 22:34
Open	#26	source ip: 10.0.2.20 DESC: PAM: User login failed.	Low	Tasks: 0 Observables: 1	V	S: 01/09/23 22:34 C: 01/09/23 22:34

## Thehive alerts:

Severity	Read	Title	# Case	Type	Source	Reference	Observables	Dates
Low	Read	source ip: 10.0.2.20 DESC: PAM: User login failed.	#28	incident	WAZUH	incident:Hello world ["severity":2,"pretext":"WAZUH Alert","title":"PAM: User login failed","text":"Jan 9 22:33:49 client-VirtualBox sshd(64700): pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser=rhost=10.0.2.20","rule_id":"5503","timestamp":"2023-01-09T21:33:48.962+0000","id":"1673300028.615217","all_fields":{"timestamp":"2023-01-09T21:33:48.962+0000","id":"1673300028.615217","all_fields":{"timestamp":"2023-01-09T21:33:48.962+0000","rule":{"level":5,"description":"PAM: User login failed","id":"5503","mitre":{"id":"T1110.001","tactic":["Credential Access"],"technique":["Password Guessing"],"firedtimes":27,"mail":false,"groups":["pam"],"syslog":{"authentication_failed"},"pci_dss":["10.2.4","10.2.5"],"gpg13":["7.8"],"gdpr":["IV_35.7.d","IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.3.4","AC.7"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"],"agent":{"id":"003","name":"client-VirtualBox","ip":"10.0.2.20"},"manager":{"name":"wazuh-server"},"id":"1673300028.615217"},"full_log":{"full_log":{"authentication_failure":{"logname":"uid=0 euid=0 tty=ssh ruser=rhost=10.0.2.20"},"predecoder":{"program_name":"sshd","timestamp":"Jan 9 22:33:49","hostname":"client-VirtualBox"},"decoder":{"name":"pam"},"data":{"script":"10.0.2.20","uid":"0","euid":"0","tty":"ssh"},"location":{"varlog/auth.log}}}} Source: WAZUH	1	O: 01/09/23 22:34 C: 01/09/23 22:34 U: 01/09/23 22:34 a few seconds

Alert Preview Imported

source ip: 10.0.2.20 DESC: PAM: User login failed.

ID: -118832 Date: 01/09/23 22:34 Type: incident Reference: incident:Hello world ["severity":2,"pretext":"WAZUH Alert","title":"PAM: User login failed","text":"Jan 9 22:33:49 client-VirtualBox sshd(64700): pam\_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser=rhost=10.0.2.20","rule\_id":"5503","timestamp":"2023-01-09T21:33:48.962+0000","id":"1673300028.615217","all\_fields":{"timestamp":"2023-01-09T21:33:48.962+0000","rule":{"level":5,"description":"PAM: User login failed","id":"5503","mitre":{"id":"T1110.001","tactic":["Credential Access"],"technique":["Password Guessing"],"firedtimes":27,"mail":false,"groups":["pam"],"syslog":{"authentication\_failed"},"pci\_dss":["10.2.4","10.2.5"],"gpg13":["7.8"],"gdpr":["IV\_35.7.d","IV\_32.2"],"hipaa":["164.312.b"],"nist\_800\_53":["AU.3.4","AC.7"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"],"agent":{"id":"003","name":"client-VirtualBox","ip":"10.0.2.20"},"manager":{"name":"wazuh-server"},"id":"1673300028.615217"},"full\_log":{"full\_log":{"authentication\_failure":{"logname":"uid=0 euid=0 tty=ssh ruser=rhost=10.0.2.20"},"predecoder":{"program\_name":"sshd","timestamp":"Jan 9 22:33:49","hostname":"client-VirtualBox"},"decoder":{"name":"pam"},"data":{"script":"10.0.2.20","uid":"0","euid":"0","tty":"ssh"},"location":{"varlog/auth.log}}}} Source: WAZUH

Basic Information

Tags

Description

Additional fields Layout

No additional information has been specified

Observables 1 Similar cases 1



List of observables (1 of 1)

Flags	Type	Data	Date Added
🔍	ip	10.0.2.20	01/09/23 22:34

## Shuffle execution:

 **All Executions**

 **REFRESH EXECUTIONS**

	09/01/2023, 22:27:25	4/4	>
	09/01/2023, 22:27:25	4/4	>
	09/01/2023, 22:27:24	4/4	>
	09/01/2023, 22:27:24	4/4	>
	09/01/2023, 22:27:23	4/4	>
	09/01/2023, 22:27:23	4/4	>

## 4.2 Video

url: <https://youtu.be/R5WZ5Ux3VUE>

## 5 REFERENCES

- Choose Freedom. Choose Fedora.* (z.d.). <https://getfedora.org/en/server/configuration>
- Shuffle.* (z.d.). medium. <https://medium.com/shuffle-automation/indicators-and-webhooks-with-thehive-cortex-and-misp-open-source-soar-part-4-f70cde942e59>
- Docker.* (z.d.). <https://hub.docker.com/r/frikky/shuffle>
- Free and Open Search: The Creators of search, ELK & Kibana.* (z.d.). Elastic. <https://www.elastic.co/>
- Get Server | Download.* (z.d.). Ubuntu. <https://ubuntu.com/download/server>
- Habte, F. (2022, 11 mei). *What is SOC (Security Operation Center)?* Check Point Software. <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/>
- Overview (Java SE 11 & JDK 11 ).* (2022, 12 december). <https://docs.oracle.com/en/java/javase/11/docs/api/>
- Shuffle.* (z.d.). <https://github.com/Shuffle/Shuffle>.
- Step by step guide - TheHive Project Documentation.* (z.d.). <https://docs.thehive-project.org/thehive/installation-and-configuration/installation/step-by-step-guide/>
- Taylor Walton. (2021, 13 december). *Shuffle + Wazuh + TheHIVE + Cortex = Automation Bliss.* YouTube. <https://www.youtube.com/watch?v=FBISHA7V15c>
- Vim Cheat Sheet.* (z.d.). <https://vim.rtorr.com/>
- Wazuh installation.* (z.d.). [www.wazuh.com](http://www.wazuh.com). <https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html>
- Wazuh suricata configuration.* (z.d.). wazuh documentation. <https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html>