

---

## Mayukh Borana

1007395

# SOC : Security Ops Centre

4<sup>th</sup> May 2023

## OVERVIEW

SIEM SOC detect attacks //multiple monitoring and analysis components meant to help organizations detect threats and mitigate them

This project involves the creation of an internal network with some benign clients and servers with an external malicious attacker(s) launching different types of attack. The network can either be done through either connected VMs or Mininet or some other network virtualization tool. The goal is to use an open-source SIEM in the internal network to detect the attacks.

These are some of the open-source SIEM available :

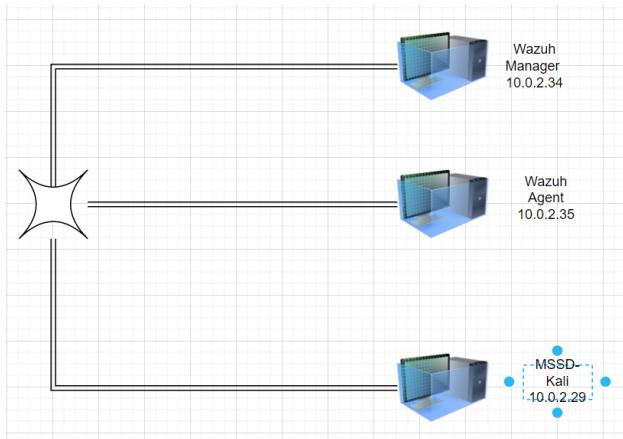
- Security Onion
- OSSIM
- Wazuh
- IBM QRadar CE
- Splunk Demo version

You can choose one of them to build a proof-of-concept (POC). Simple attacks (at least 5) should be detected from the default configuration. At least 2 complex attacks which are not detected by the SIEM should be crafted. SIEM rules should then be updated to ultimately detect these complex attacks. On top of the report, you'll have to produce a recorded video demo to show the functioning of the SIEM, detection of simple attacks, non-detection of complex attacks and their eventual detection after rule creation.

- Implementation – 14
- Attack Variety & Network Size – 8
- Complexity of Work – 8
- Report - 8
- Demo – 6

## Requirement:

## Network Topology



## IP of my Virtual Network

Hostname	IP Adress	Role
Wazuh.OVA	10.0.2.34	Wazuh Manager
Server	10.0.2.35	Wazuh Agent
MSSD-Kali	10.0.2.29	Kali Attacker

Wazuh v4.4.1 OVA [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to

```
WAZUH Open Source Security Platform
https://wazuh.com

[waZuH-user@waZuH-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:00:27:84:03:24 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.34/24 brd 10.0.2.255 scope global dynamic eth0
        valid_lft 375sec preferred_lft 375sec
    inet6 fe80::a00:27ff:fe84:d324/64 scope link
        valid_lft forever preferred_lft forever
[waZuH-user@waZuH-server ~]$
```

Right Ctrl

https://10.0.2.34/app/wazuh

File Edit View Terminal Tabs Help

May 02 08:09:35 osboxes systemd[1]: Starting The Apache HTTP Server...
May 02 08:09:39 osboxes apachectl[1863]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.0.2.34.
May 02 08:09:39 osboxes systemd[1]: Started The Apache HTTP Server.

```
root@osboxes:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.34 brd 10.0.2.255 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe84:d324/64 brd fe80::ff:fe84:d324/128 scopeid 0x20<link>
    ether 00:00:27:84:03:24 txqueuelen 1000 (Ethernet)
    RX packets 5692 bytes 7448839 (7.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1945 bytes 250545 (250.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1/128 brd 00:00:00:00:00:00 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 426 bytes 44707 (44.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 426 bytes 44707 (44.7 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

MSSD Kali 2022 [Running] - Oracle VM VirtualBox

File Actions Edit View Help

(root@kali)-[~]

```
# ping 10.0.2.35
PING 10.0.2.35 (10.0.2.35) 56(84) bytes of data.
64 bytes from 10.0.2.35: icmp_seq=1 ttl=64 time=0.888 ms
64 bytes from 10.0.2.35: icmp_seq=2 ttl=64 time=0.704 ms
^C
--- 10.0.2.35 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.704/0.796/0.888/0.092 ms

(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.29 brd 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe65:b9de/64 brd fe80::ff:fe65:b9de/128 scopeid 0x20<link>
        ether 00:00:27:65:b9:de txqueuelen 1000 (Ethernet)
        RX packets 13 bytes 3222 (3.1 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 32 bytes 4320 (4.2 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1/128 brd 00:00:00:00:00:00 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```

└─(root㉿kali)-[~]
└─# nmap 10.0.2.35
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 08:39 EDT
Nmap scan report for 10.0.2.35
Host is up (0.00028s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:CA:53:81 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

└─# ┌─

```

## Attack Variety

SrNo.	Name of attack which has been detected By Open Source Wazuh
1	Detection of BruteForce on FTP server Login credentials
2	Detecting SQLi in Apache Web Server
3	Detecting Ransomware with Wazuh
4	File Integrity Monitoring Attack Detection
5	Detecting MetaSploit attack
5	
7	Detecting ShellShock attack(Using Nikto)

## Lab Setup:

Configuring Wazuh Manager and agent

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh x Apache2 Ubuntu Default x +

Help Manual Support Forums Google Search

wazuh Modules

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

**THREAT DETECTION AND RESPONSE**

- Vulnerabilities**  
Discover what applications in your environment are affected by well-known vulnerabilities.
- MITRE ATT&CK**  
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

**REGULATORY COMPLIANCE**

- PCI DSS**  
Global security standard for entities that process, store or transmit payment cardholder data.
- NIST 800-53**  
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

Menu Wazuh - Wazuh - Mozilla Firefox [Linux Lite Terminal - ] 8:13 25.8

The screenshot shows the Wazuh web interface running in Mozilla Firefox. At the top, it displays basic navigation like File, Machine, View, Input, Devices, Help, and tabs for Wazuh - Wazuh and Apache2 Ubuntu Default. Below the tabs is a search bar with the URL https://10.0.2.34/app/wazuh#/overview/?\_g=(filters:(),refreshInterval:(pause:0,value:0),time,(from:now-24h,to:now))&\_a=(color:). The main content area has a header "wazuh" with a dropdown arrow and a yellow badge with the letter 'a'. It features five main sections: 1. **SECURITY INFORMATION MANAGEMENT** with cards for Security events and Integrity monitoring. 2. **AUDITING AND POLICY MONITORING** with cards for Policy monitoring and System auditing. 3. **THREAT DETECTION AND RESPONSE** with cards for Vulnerabilities and MITRE ATT&CK. 4. **REGULATORY COMPLIANCE** with cards for PCI DSS and NIST 800-53. At the bottom, there's a Linux Lite Terminal window and a system tray with icons for battery, signal, and time (8:13 25.8).

# Detecting a brute-force attack

```
[root@kali:~/Desktop]# hydra -L username.txt -P password.txt 192.0.2.35 ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-02 09:21:48
[DATA] max 10 tasks per server, overall 16 tasks, 153 login tries (l:17/p:9), -10 tries per task
[DATA] host: 192.0.2.35, service: ftp, user: ftpuser, password: password
[+] [ftp] host: 192.0.2.35, service: ftp, user: ftpuser, password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-02 09:22:25
```

Brute-forcing is a common attack vector that threat actors use to gain unauthorized access to endpoints and services. Services like ftp on Linux endpoints and RDP on Windows endpoints are usually prone to brute-force attacks. Wazuh identifies brute-force attacks by correlating multiple authentication failure events.

## Configuration

Perform the following steps to configure the Ubuntu endpoint. This allows performing authentication failure attempts on the monitored RHEL and Windows endpoints.

1. On the attacker endpoint, install Hydra and use it to execute the brute-force attack:

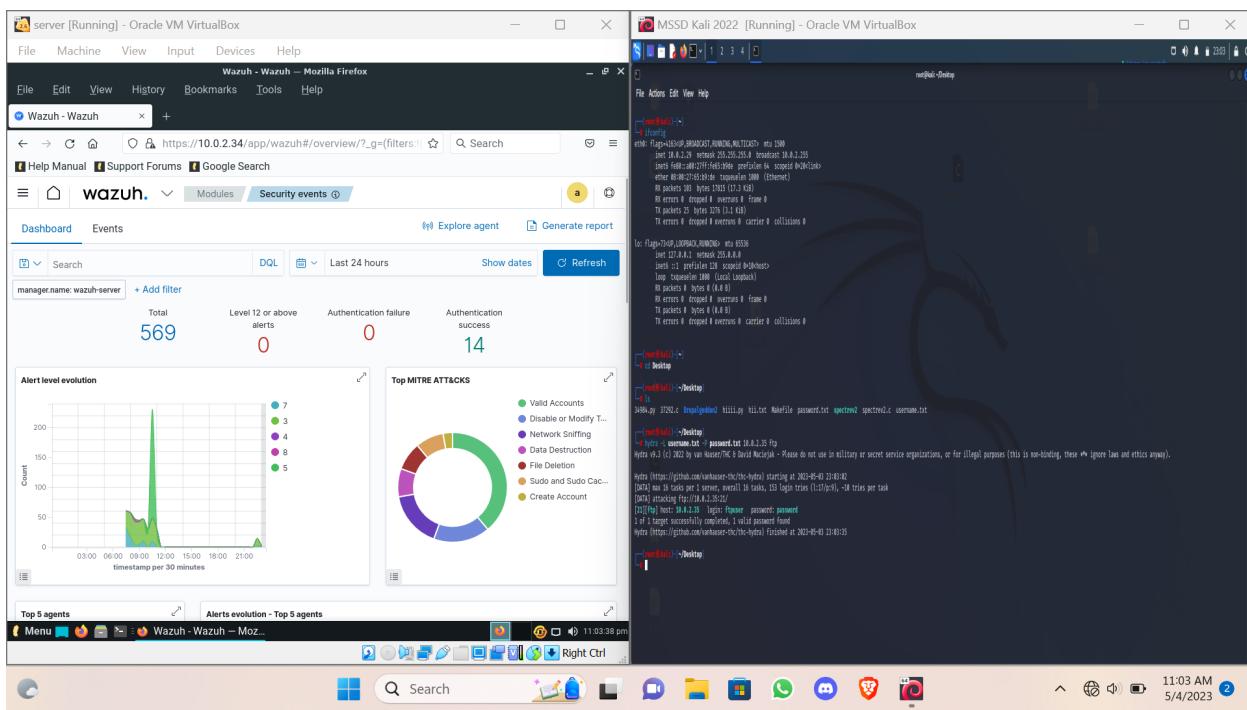
```
sudo apt update
```

```
sudo apt install -y hydra
```

## Attack emulation

1. Create a text file with 10 random passwords.
2. Run Hydra from the attacker endpoint to execute brute-force attacks against the RHEL endpoint. To do this, replace `<RHEL_IP>` with the IP address of the RHEL endpoint and run the command below:

```
sudo hydra -L <username.txt>-P <PASSWORD_LIST.txt> <server_IP> ftp
```

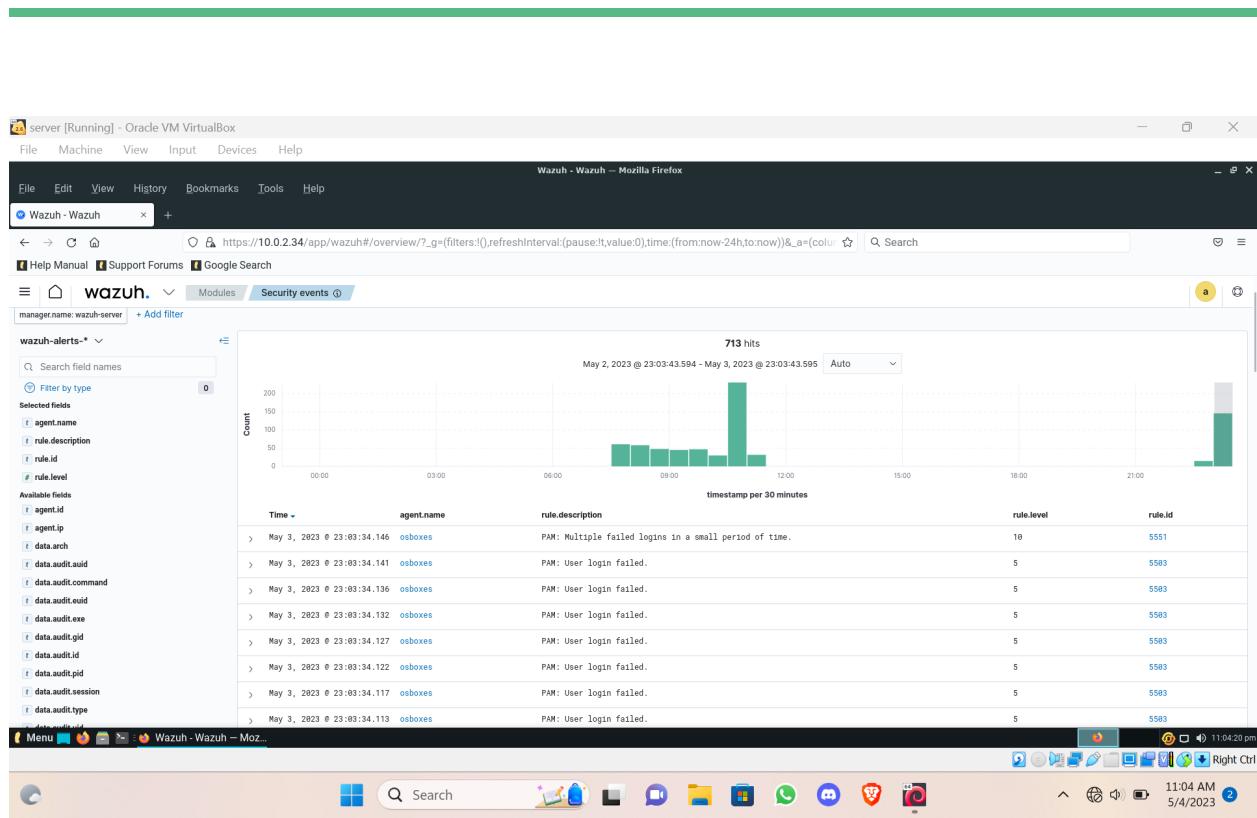


## Visualize the alerts

You can visualize the alert data in the Wazuh dashboard. To do this, go to the Security events module and add the filters in the search bar to query the alerts.

Linux - `rule.id: (5551 OR 5712)`. Other related rules are [5710](#), [5711](#), [5716](#), [5720](#), [5503](#), [5504](#).





server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules Security events

May 3, 2023 0 23:03:34.146 osboxes PAM: Multiple failed logins in a small period of time.

Expanded document

Table JSON

\_index: wazuh-alerts-4.x-2023.05.04  
agent\_id: 002  
agent\_ip: 10.0.2.35  
agent\_name: osboxes  
data.euid: 0  
data.scpip: ::ffff:10.0.2.29  
data.scruser: newuser  
data.tty: ftp  
data.uid: 0  
decoder.name: pam  
full\_log: May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
id: 1683169414.114379  
input.type: log

View surrounding documents View single document

10 5551

Menu Mozilla Firefox 11:04:30 pm Right Ctrl

Search

11:04 AM 5/4/2023 2

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules Security events

data.sca.check.id  
data.sca.check.previous\_result  
data.sca.check.rationale  
data.sca.check.reason  
data.sca.check.remediation  
data.sca.check.result  
data.sca.check.title  
data.sca.description  
data.sca.failed  
data.sca.file  
data.sca.invalid  
data.sca.passed  
data.sca.policy  
data.sca.policy\_id  
data.sca.scan\_id  
data.sca.score  
data.sca.total\_checks  
data.sca.type  
data.scpip  
data.scruser  
data.title  
data.tty  
data.uid

predecoder.timestamp: May 3 23:03:32  
previous\_output: May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29  
rule.description: PAM: Multiple failed logins in a small period of time.  
rule.firedtimes: 18  
rule.frequency: 8  
rule.gdpr: IV\_35\_7.d, IV\_32.2  
rule.gpg13: 7.8  
rule.groups: pam, syslog, authentication\_failures  
rule.hipaa: 164.312.b  
rule.id: 5551  
rule.level: 10  
rule.mail: false  
rule.mitre.id: T1118  
rule.mitre.tactic: Credential Access

View surrounding documents View single document

10 5551

Menu Mozilla Firefox 11:04:37 pm Right Ctrl

Search

11:04 AM 5/4/2023 2

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules Security events

data.sca.failed

# rule.frequency 8

# rule.gdpr IV.35.7.d, IV.32.2

# rule.gpg13 7.8

# rule.groups pam, syslog, authentication\_failures

# rule.hipaa 164.312.b

# rule.id 5551

# rule.level 10

# rule.mail false

# rule.mitre.id T1118

# rule.mitre.tactic Credential Access

# rule.mitre.technique Brute Force

# rule.nist\_800\_53 AU.14, AC.7, SI.4

# rule.pci\_dss 10.2.4, 10.2.5, 11.4

# rule.tsc CC6.1, CC6.8, CC7.2, CC7.3

timestamp May 3, 2023 @ 23:03:34.146

Menu Mozilla Firefox 11:04:46 pm Right Ctrl

Search

11:04 AM 5/4/2023

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules Security events

location

manager.name

predecoder.hostname

predecoder.program.name

predecoder.timestamp

previous\_log

previous\_output

rule.cls

rule.cis

rule.cis\_csc

rule.cis\_level

rule.firetimes

rule.frequency

rule.gdpr

rule.gdp\_IV

rule.gpg13

rule.gpg13

rule.groups

rule.hipaa

rule.mail

rule.mitre.id

rule.mitre.tactic

rule.mitre.technique

rule.nist\_800\_53

timestamp May 3, 2023 @ 23:03:34.146

May 3, 2023 @ 23:03:34.141 osboxes PAM: User login failed.

View surrounding documents View single document

Table JSON

\_index wazuh-alerts-4.x-2023.05.04

agent.id 002

agent.ip 10.0.2.35

agent.name osboxes

data.euid 0

data.srccip ::ffff:10.0.2.29

data.srouser newuser

data.tty ftp

data.uid 0

decoder.name pam

full.log May 3 23:03:32 osboxes vsftpd: pam\_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29

id 10000000000000000000000000000000

Menu Mozilla Firefox 11:04:55 pm Right Ctrl

Search

11:04 AM 5/4/2023

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

t rule.mitre.tactic	t full_log	May 3 23:03:32 osboxes vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=newuser rhost=:ffff:10.0.2.29
t rule.mitre.technique	t id	1683169414..113855
t rule.nist_800_53	t input.type	log
t rule.pci_dss	t location	/var/log/auth.log
t rule.tsc	t manager.name	wazuh-server
t syscheck.audit.effective_user_id	t predecoder.hostname	osboxes
t syscheck.audit.effective_user_name	t predecoder.program_name	vsftpd
t syscheck.audit.group_id	t predecoder.timestamp	May 3 23:03:32
t syscheck.audit.group.name	t rule.description	PAM: User login failed.
t syscheck.audit.process.cwd	# rule.firetimes	119
t syscheck.audit.process.id	t rule.gidr	IV_35..7..d, IV_32..2
t syscheck.audit.process.name	t rule.gpg13	7..8
t syscheck.audit.process.parent_cwd	t rule.groups	pam, syslog, authentication_failed
t syscheck.audit.process.parent_name	t rule.hipaa	164..312..b
t syscheck.audit.process.pid	t rule.id	5583
t syscheck.audit.user_id	# rule.level	5
t syscheck.audit.user.name		
t syscheck.event		
t syscheck.gid_after		
t syscheck.gname_after		
t syscheck.inode_after		
t syscheck.mds_after		
t syscheck.mds_before		
t syscheck.mode		
t syscheck.mtime_after		
t syscheck.path		
t syscheck.perm_after		
t syscheck.sh1_after		
t syscheck.sh256_after		
t syscheck.size_after		
t syscheck.uid_after		
t syscheck.uname_after		
timestamp	timestamp	May 3, 2023 @ 23:03:34.141

Wazuh - Wazuh - Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

t syscheck.audit.user.name	t rule.gpg13	7..8
t syscheck.event	t rule.groups	pam, syslog, authentication_failed
t syscheck.gid_after	t rule.hipaa	164..312..b
t syscheck.gname_after	t rule.id	5583
t syscheck.inode_after	# rule.level	5
t syscheck.mds_after	@ rule.mail	false
t syscheck.mode	t rule.mitre.id	T1110..001
t syscheck.mtime_after	t rule.mitre.tactic	Credential Access
t syscheck.path	t rule.mitre.technique	Password Guessing
t syscheck.perm_after	t rule.nist_800_53	AU..14, AC..7
t syscheck.sh1_after	t rule.pci.dss	10..2..4, 10..2..5
t syscheck.sh256_after	t rule.tsc	CC6..1, CC6..8, CC7..2, CC7..3
t syscheck.size_after	timestamp	May 3, 2023 @ 23:03:34.141
t syscheck.uid_after		
t syscheck.uname_after		
timestamp		

Wazuh - Wazuh - Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

> May 3, 2023 @ 23:03:34.136 osboxes	PAM: User login failed.	5 5583
> May 3, 2023 @ 23:03:34.132 osboxes	PAM: User login failed.	5 5583
> May 3, 2023 @ 23:03:34.127 osboxes	PAM: User login failed.	5 5583

Wazuh - Wazuh - Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

Wazuh - Wazuh — Mozilla Firefox

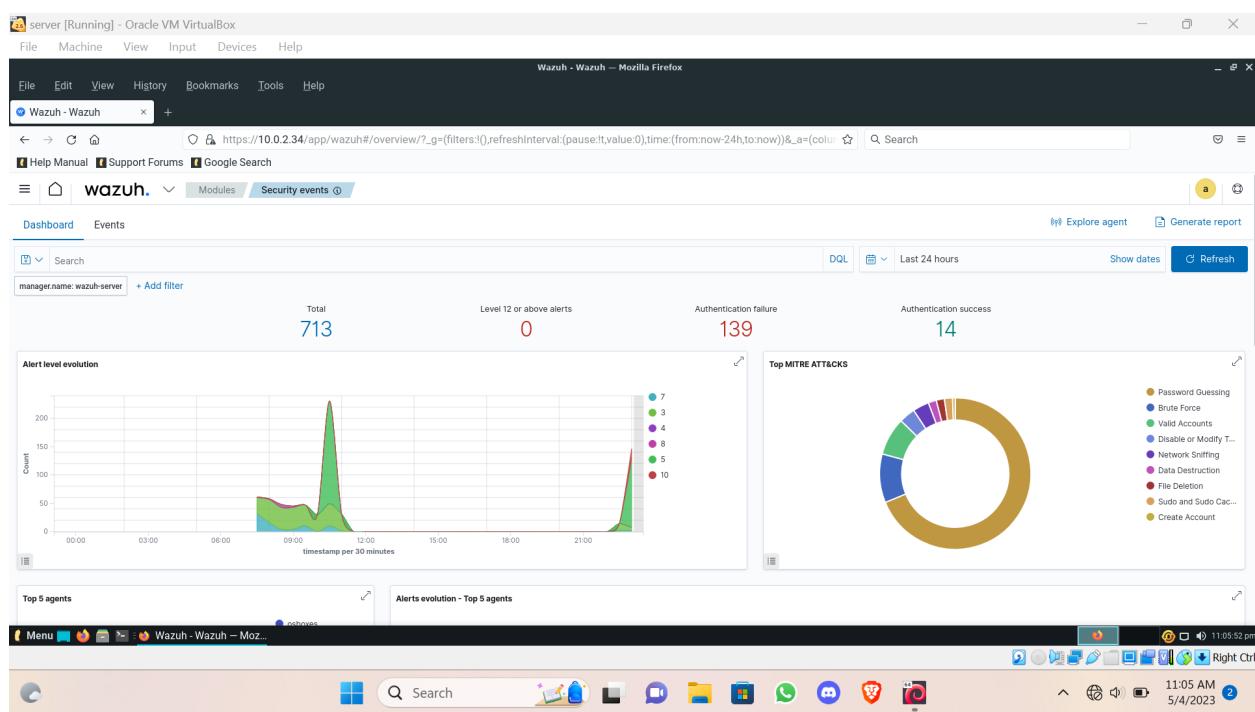
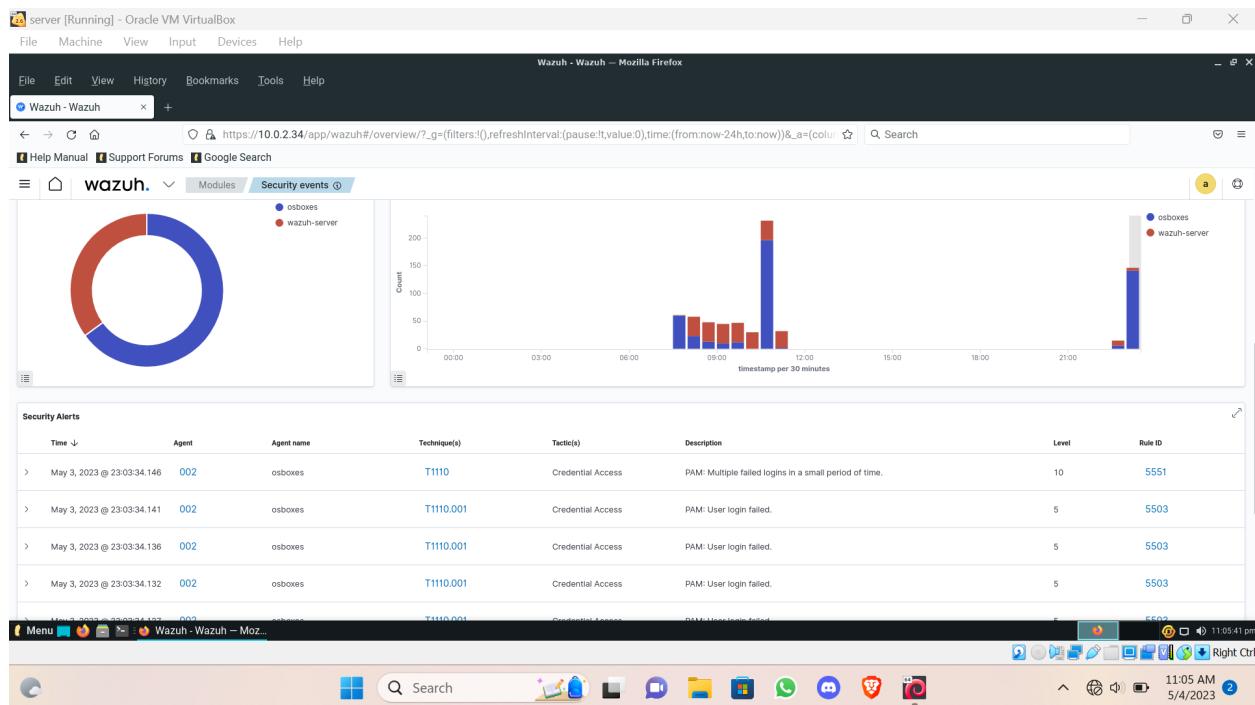
File Edit View Bookmarks Tools Help

Wazuh - Wazuh | +

Help Manual Support Forums Google Search

wazuh. Modules Security events

> May 3, 2023 @ 23:03:34.136 osboxes	PAM: User login failed.	5 5583
> May 3, 2023 @ 23:03:34.132 osboxes	PAM: User login failed.	5 5583
> May 3, 2023 @ 23:03:34.127 osboxes	PAM: User login failed.	5 5583



# Detecting an SQL injection attack

You can use Wazuh to detect SQL injection attacks from web server logs that contain patterns like `select`, `union`, and other common SQL injection patterns.

SQL injection is an attack in which a threat actor inserts malicious code into strings transmitted to a database server for parsing and execution. A successful SQL injection attack gives unauthorized access to confidential information contained in the database.

In this use case, you simulate an SQL injection attack against an Ubuntu endpoint and detect it with Wazuh

## Configuration

Perform the following steps to install Apache and configure the Wazuh agent to monitor the Apache logs.

1. Update the local packages and install the Apache web server:

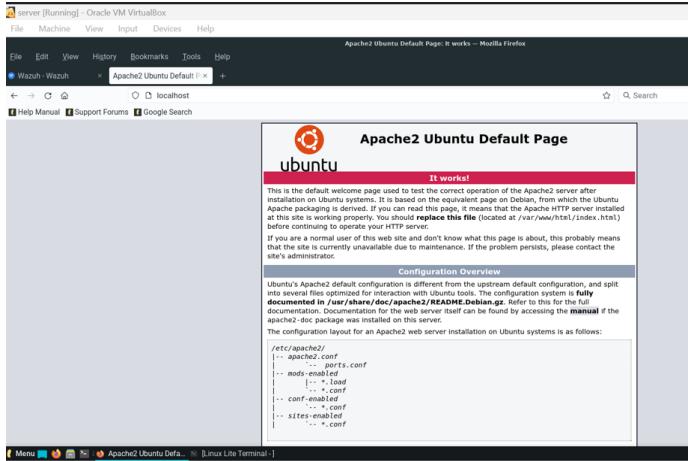
```
sudo apt update
```

```
sudo apt install apache2
```

```
root@osboxes:~# sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom ufw
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 453 not upgraded.
Need to get 1,716 kB of archives.
All selected components are already the newest version.
```

```
root@osboxes:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-05-02 07:41:48 EDT; 1min 6s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 9478 (apache2)
      Tasks: 55 (limit: 1360)
        Memory: 5.5M
       CGroup: /system.slice/apache2.service
               ├─9478 /usr/sbin/apache2 -k start
               ├─9480 /usr/sbin/apache2 -k start
               └─9481 /usr/sbin/apache2 -k start

May 02 07:41:47 osboxes systemd[1]: Starting The Apache HTTP Server...
May 02 07:41:48 osboxes apache2[9477]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive
May 02 07:41:48 osboxes systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```



2. If the firewall is enabled, modify it to allow external access to web ports. Skip this step if the firewall is disabled.

`sudo ufw app list`

`sudo ufw allow 'Apache'`

`sudo ufw status`

3. Check the status of the Apache service to verify that the web server is running:

`sudo systemctl status apache2`

**4. Use the `curl` command or open <http://10.0.2.35> in a browser to view the Apache landing page and verify the installation:**

`curl http://<UBUNTU_IP>`

**5. Add the following lines to the Wazuh agent `/var/ossec/etc/ossec.conf` file. This allows the Wazuh agent to monitor the access logs of your Apache server:**

`<ossec_config>`

`<localfile>`

`<log_format>apache</log_format>`

`<location>/var/log/apache2/access.log</location>`

`</localfile>`

`</ossec_config>`

```

File Machine View Input Devices Help
Open *ossec.conf /var/ossec/etc Save ... x it's Terminal ...
182 <location>/var/ossec/logs/active-responses.log</location>
183 </localfile>
184 <localfile>
185 <log_format>syslog</log_format>
186 <location>/var/log/messages</location>
187 </localfile>
188 <localfile>
189 <log_format>syslog</log_format>
190 <location>/var/log/auth.log</location>
191 </localfile>
192 <localfile>
193 <log_format>syslog</log_format>
194 <location>/var/log/syslog</location>
195 </localfile>
196 <localfile>
197 <log_format>syslog</log_format>
198 <location>/var/log/mail.info</location>
199 </localfile>
200 <localfile>
201 <log_format>syslog</log_format>
202 <location>/var/log/kern.log</location>
203 </localfile>
204 <localfile>
205 <log_format>syslog</log_format>
206 <location>/var/log/dpkg.log</location>
207 </localfile>
208 <localfile>
209 <log_format>syslog</log_format>
210 <location>/var/log/kern.log</location>
211 </localfile>
212 <localfile>
213 <log_format>apache</log_format>
214 <location>/var/log/apache2/access.log</location>
215 </localfile>
216 <localfile>
217 </localfile>
218 </ossec>.conf

```

HTML Tab Width: 8 Ln 215, Col 1 INS

```

Setting up gedit (3.36.2-Ubuntu) ... config-enabled
update-alternatives: using /usr/bin/gedit to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
root@ / var > ossec > etc > | gedit ossec.conf | xterm-enabled | .conf

```

## 6. Restart the Wazuh agent to apply the configuration changes

**sudo systemctl restart wazuh-agent**

## Attack emulation

Replace **<UBUNTU\_IP>** with the appropriate IP address and execute the following command from the attacker endpoint:

**curl -XGET "http://<UBUNTU\_IP>/users/?id=SELECT+\*+FROM+users";**

```

root@kali: [~] curl -XGET "http://10.0.2.35/users/?id=SELECT+*+FROM+users"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 10.0.2.35 Port 80</address>
</body></html>

```

The expected result here is an alert with rule ID 31103 but a successful SQL injection attempt generates an alert with rule ID 31106.

## Visualize the alerts

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh

https://10.0.2.34/app/wazuh#/overview/?tab=general&tabView=panels&\_g=(filters:(),refreshInterval(pause:0,value:0),time:(from:now-1h,to:now))&\_t=

Help Manual Support Forums Google Search

wazuh. Modules osboxes Security events

Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 2, 2023 @ 10:21:26.112	T1190	Initial Access	SQL injection attempt.	7	31103
May 2, 2023 @ 10:21:24.109	T1190	Initial Access	SQL injection attempt.	7	31103
May 2, 2023 @ 10:19:52.019	T1190	Initial Access	SQL injection attempt.	7	31103
May 2, 2023 @ 10:19:50.402	T1190	Initial Access	SQL injection attempt.	7	31103
May 2, 2023 @ 10:18:02.336		Host-based anomaly detection event (rootcheck).	Host-based anomaly detection event (rootcheck).	7	510
May 2, 2023 @ 10:17:45.723		Host-based anomaly detection event (rootcheck).	Host-based anomaly detection event (rootcheck).	7	510

Linux Lite Terminal - 10:23:14 am

85°F Partly cloudy

Search

Right Ctrl

10:23 PM 5/2/2023

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh

https://10.0.2.34/app/wazuh#/overview/?tab=general&tabView=panels&\_g=(filters:(),refreshInterval(pause:0,value:0),time:(from:now-1h,to:now))&\_t=

Help Manual Support Forums Google Search

wazuh. Modules osboxes Security events

Dashboard Events

manager.name:wazuh-server agent.id:002 + Add filter

wazuh-alerts\* ▾

Search field names

Filter by type

Selected fields

rule.description rule.id rule.level

Available fields

agent.id agent.ip agent.name data.dsuser data.euid data.extra\_data data.file data.id data.protocol

Count

333 hits

May 1, 2023 @ 10:17:37.461 - May 2, 2023 @ 10:17:37.461 Auto

timestamp per 30 minutes

DQL Last 24 hours Show dates Refresh

Time	rule.description	rule.level	rule.id
May 2, 2023 @ 10:16:43.274	SQL injection attempt.	7	31103
May 2, 2023 @ 10:16:41.349	SQL injection attempt.	7	31103
May 2, 2023 @ 10:16:41.273	SQL injection attempt.	7	31103
May 2, 2023 @ 10:16:39.271	SQL injection attempt.	7	31103
May 2, 2023 @ 10:16:24.376	Ossec agent started.	3	503

Linux Lite Terminal - 10:17:51 am

85°F Partly cloudy

Search

Right Ctrl

10:17 PM 5/2/2023

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules osboxes Security events

data\_id \_index wazuh-alerts-4.x-2023.05.02

data\_protocol agent\_id 002

data.scrip agent.ip 10.0.2.35

data.scp agent.name osboxes

data.title data.id 404

data.ty data.protocol GET

data.uid data.scrip 10.0.2.29

data.url /users/?id=SELECT\*\*\*FROM+users

decoder.name decoder.name web-accesslog

full\_log full\_log 10.0.2.29 - - [02/May/2023:10:16:41 -0400] "GET /users/?id=SELECT\*\*\*FROM+users HTTP/1.1" 404 432 "-" "curl/7.82.0"

id id 1683837083\_464375

input.type input.type log

location location /var/log/apache2/access.log

manager.name manager.name wazuh-server

predecoder.hostname rule.description SQL injection attempt.

predecoder.program\_name rule.firetimes 7

predecoder.timestamp rule.frequency

rule.gdr rule.gdr IV\_35.7.d

rule.groups rule.groups web, accesslog, attack, sql\_injection

rule.hipa rule.id 31103

rule.mail rule.level 7

rule.mitre.id rule.mail false

rule.mitre.tactic rule.mitre.id T1198

rule.mitre.technique rule.mitre.tactic Initial Access

rule.nist\_800\_53 rule.nist\_800\_53 SA.11, SI.4

rule.pc1\_dss rule.pc1\_dss 6.5, 11.4, 6.5.1

rule.tsc rule.tsc CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3

timestamp May 2, 2023 @ 10:16:43.274

May 2, 2023 @ 10:16:41.349 SQL injection attempt. 7 31103

May 2, 2023 @ 10:16:41.273 SQL injection attempt. 7 31103

Linux Lite Terminal

85°F Partly cloudy

Search

10:18 PM 5/2/2023 Right Ctrl

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules osboxes Security events

rule.firetimes rule.description SQL injection attempt.

rule.frequency # rule.firetimes 7

rule.gdr rule.gdr IV\_35.7.d

rule.gpg13 rule.groups web, accesslog, attack, sql\_injection

rule.groups rule.id 31103

rule.hipa rule.level 7

rule.mail rule.mail false

rule.mitre.id rule.mitre.technique Initial Access

rule.mitre.tactic rule.nist\_800\_53 rule.nist\_800\_53 SA.11, SI.4

rule.pc1\_dss rule.pc1\_dss 6.5, 11.4, 6.5.1

rule.tsc rule.tsc CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3

timestamp May 2, 2023 @ 10:16:43.274

> May 2, 2023 @ 10:16:41.349 SQL injection attempt. 7 31103

> May 2, 2023 @ 10:16:41.273 SQL injection attempt. 7 31103

Linux Lite Terminal

85°F Partly cloudy

Search

10:18 PM 5/2/2023 Right Ctrl

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules osboxes Security events

File description rule.id rule.level

Selected fields

Available fields

Count

Time rule.description rule.level rule.id

May 2, 2023 10:21:26.112 SQL injection attempt.

View surrounding documents View single document

Table JSON

\_index wazuh-alerts-4.x-2023.05.02

agent\_id 002

agent\_ip 10.0.2.35

agent\_name osboxes

data\_id 404

data.protocol GET

data.srcip 10.0.2.29

decoder.name decoder.parent

data.url /index.html

File Menu Mozilla Firefox 10:22:52 am 5/2/2023 Right Ctrl

85°F Partly cloudy

Search

Linux Lite Terminal

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh — Mozilla Firefox

File Edit View Bookmarks Tools Help

Wazuh - Wazuh

Help Manual Support Forums Google Search

wazuh. Modules osboxes Security events

Filter by type

Selected fields

Available fields

Count

Time rule.description rule.level rule.id

May 2, 2023 10:21:26.112 SQL injection attempt.

View surrounding documents View single document

Table JSON

\_index wazuh-alerts-4.x-2023.05.02

agent\_id 002

agent\_ip 10.0.2.35

agent\_name osboxes

data\_id 404

data.protocol GET

data.srcip 10.0.2.29

decoder.name decoder.parent

data.url /index.html

File Menu Mozilla Firefox 10:22:56 pm 5/2/2023 Right Ctrl

85°F Partly cloudy

Search

Linux Lite Terminal

You can visualize the alert data in the Wazuh dashboard. To do this, go to the Security events module and add the filters in the search bar to query the alerts.

Rule.id:31103 rule.id:31106

---

# Detecting ransomware with Wazuh

Actions to prevent and detect ransomware attacks are mandatory to keep your system safe. In this article you will learn how Wazuh can help detect ransomware attacks in progress using the file integrity monitoring module.

In recent years increasing waves of attacks with ransomware have been reported targeting different business sectors. This particular type of malware is designed to deny access to a computer system or data, via encryption, until a ransom is paid.

Ransomware spreads typically through email phishing and spam (messages with links to compromised websites or malicious attachments). Besides, some ransomware families, like *WannaCry*, do take advantage of exploits to infect other systems in the network, meaning that they do not require human help to propagate. In order to avoid ransomware, it is recommended to keep your systems updated and properly secured, backup your data on a regular basis and educate your end-users in security. The modules that help prevent and detect ransomware are:

- Scanless vulnerability detection: Identifies vulnerable systems and applications correlating inventory data with well known CVEs.
- Security Configuration Assessment: Used to expose poorly configured systems. It runs configuration checks periodically, enforcing good practices by following standards such as CIS (Center of Internet Security).
- File integrity monitoring: Monitors changes to the file system, and can be used to detect the presence of malicious files (see, for example, our integration with VirusTotal).

File system events during a ransomware attack:

The following actions are performed by the ransomware during an attack:

- Read the file content.
- Encrypt the content and write it into a new file.
- Remove the original file.

Since Wazuh file integrity monitoring is able to monitor addition, changes, and deletion of files in directories, we can easily detect that new files are being created when encrypted and the original ones are removed. If an unlikely high number of file creation and deletion alerts are reported, we could be facing a ransomware attack.

[Detecting ransomware with Wazuh by monitoring the file system](#)

Let's now run a simple proof of concept using Wazuh file integrity monitoring module. For it, we created a Python script (wazuh-ransomware-poc.py) to simulate a ransomware attack. The script requires [Python 3](#) and the [cryptography](#) package.

```

9:38 AM ✨ 9:38 AM ✨ 9:38 AM ✨ 9:38 AM ✨
wazuh-ransomware-p... content://media/external/download
content://media/external/download

#!/usr/bin/env python3

# Copyright (C) 2015-2019, Wazuh Inc.
# Created by Wazuh, Inc. <info@wazuh.com>.
# This program is free software; you can
# redistribute it and/or modify it under the
# terms of GPLv2

import os
import random
import string
import base64
import sys
from pathlib import Path
from cryptography.fernet import Fernet

def create_random_files(basedir,
n_directories, n_files_per_directory,
size_file=1024):
    for root, dirs, files in
os.walk(str(basedir)):
        for n_dir in range(n_directories):
            p = Path(root) /
'Directory_{:}'.format(str(n_dir).zfill(2))
            p.mkdir(exist_ok=True)

        for root, dirs, files in
os.walk(str(basedir)):
            if root is basedir:
                continue

            for n_file in
range(n_files_per_directory):
                new_file =
'{}/File_{}.txt'.format(root,
str(n_file).zfill(2))
                text =
''.join([random.choice(string.ascii_letters)
for i in range(size_file)]) #!
                with open(new_file, 'w') as f:
                    f.write(text)

    return None

def encrypt_file(filepath, plain_key,
output_filepath):
    encoded_key =
base64.urlsafe_b64encode(plain_key.encode())
    # Encrypt file using cryptography.fernet
library
    with open(filepath, mode='rb') as
f_clear:
        fernet_cipher = Fernet(encoded_key)
        encrypted_data =
fernet_cipher.encrypt(f_clear.read())
        # Remove sensitive variables
        del plain_key, encoded_key
        # Write content to file
        with open(output_filepath, mode='wb') as
f_encrypt:
            f_encrypt.write(encrypted_data)

def decrypt_file(filepath, plain_key,
output_filepath):
    encoded_key =
base64.urlsafe_b64encode(plain_key.encode())
    # Decrypt file using cryptography.fernet
library
    with open(filepath, mode='rb') as
f_clear:
        fernet_cipher = Fernet(encoded_key)
        clear_data =
fernet_cipher.decrypt(f_clear.read())
        # Remove sensitive variables
        del plain_key
        # Write content to file
        with open(output_filepath, mode='wb') as
f_encrypt:
            f_encrypt.write(clear_data)

def encrypt_files(basedir, key):
    # Read operation
    for root, dirs, files in
os.walk(str(basedir)):
        for file in files:
            # Write operation
            src_file = os.path.join(root,
file)
            dst_file = '{}.format(src_file, encrypted")'
            dst_file = os.path.join(root,
dst_file)
            # Delete operation
            os.remove(src_file)

def decrypt_files(basedir, key):
    # Read operation
    for root, dirs, files in
os.walk(str(basedir)):
        for file in files:
            if file.endswith('.encrypted'):
                # Write operation
                src_file = os.path.join(root,
file)
                dst_file =
os.path.splitext(src_file)[0]
                dst_file = os.path.join(root,
dst_file)
                # Delete operation
                os.remove(src_file)
                if __name__ == '__main__':
                    try:
                        action = sys.argv[1]
                    except:
                        print("Error: Bad arguments. Valid
arguments: 'prepare', 'attack', 'restore'")
                        sys.exit(1)
                    basedir = "/home/vagrant/test"
                    key = "nsa42FgdsR0805nVqeww0u3Rubwk2a"
                    if action == "prepare":
                        create_random_files(basedir,
n_directories=10, n_files_per_directory=20,
size_file=1024)
                    elif action == "attack":
                        encrypt_files(basedir, key)
                    elif action == "restore":
                        decrypt_files(basedir, key)
src_file = os.path.join(root,
file)
dst_file = '{}.format(src_file, encrypted")'
dst_file = os.path.join(root,
dst_file)
encrypt_file(src_file, key,
dst_file)
# Delete operation
os.remove(src_file)

def decrypt_files(basedir, key):
    # Read operation
    for root, dirs, files in
os.walk(str(basedir)):
        for file in files:
            if file.endswith('.encrypted'):
                # Write operation
                src_file = os.path.join(root,
file)
                dst_file =
os.path.splitext(src_file)[0]
                dst_file = os.path.join(root,
dst_file)
                # Delete operation
                os.remove(src_file)
                if __name__ == '__main__':
                    try:
                        action = sys.argv[1]
                    except:
                        print("Error: Bad arguments. Valid
arguments: 'prepare', 'attack', 'restore'")
                        sys.exit(1)
                    basedir = "/home/vagrant/test"
                    key = "nsa42FgdsR0805nVqeww0u3Rubwk2a"
                    if action == "prepare":
                        create_random_files(basedir,
n_directories=10, n_files_per_directory=20,
size_file=1024)
                    elif action == "attack":
                        encrypt_files(basedir, key)
                    elif action == "restore":
                        decrypt_files(basedir, key)
src_file = os.path.join(root,
file)
dst_file = '{}.format(src_file, encrypted")'
dst_file = os.path.join(root,
dst_file)
encrypt_file(src_file, key,
dst_file)
# Delete operation
os.remove(src_file)

if __name__ == '__main__':
    try:
        action = sys.argv[1]
    except:
        print("Error: Bad arguments. Valid
arguments: 'prepare', 'attack', 'restore'")
        sys.exit(1)
    basedir = "/home/vagrant/test"
    key = "nsa42FgdsR0805nVqeww0u3Rubwk2a"
    if action == "prepare":
        create_random_files(basedir,
n_directories=10, n_files_per_directory=20,
size_file=1024)
    elif action == "attack":
        encrypt_files(basedir, key)
    elif action == "restore":
        decrypt_files(basedir, key)

```

## <Python File>

### Step 1: Prepare the test environment

First, we create the [/home/vagrant/test](#) directory:

```
[root@agent01 vagrant]# mkdir -p /home/vagrant/test
```

```

root /> var > ossec > etc > systemctl restart wazuh-agent
root /> var > ossec > etc > mkdir -p /home/vagrant/test
root /> var > ossec > etc > gedit ossec.conf
Note You can also configure any p
(gedit:19073): Tepl-WARNING **: 10:32:46.666: GVfs metadata is not supporte
is platform. In the latter case, you should configure Tepl with --disable-g
root /> var > ossec > etc > systemctl restart wazuh-agent
root /> var > ossec > etc > gedit ossec.conf
root /> var > ossec > etc > gedit ossec.conf

```

We need to configure the Wazuh agent to monitor the previous directory:

```
<syscheck>
```

```

<directories check_all="yes"
whodata="yes">/home/vagrant/test</directories>

</syscheck>
```

```

78      <!-- Database synchronization settings -->
79      <synchronization>
80          <max_eps>10</max_eps>
81      </synchronization>
82      </wodle>
83
84
85      <sca>
86          <enabled>yes</enabled>
87          <scan_on_start>yes</scan_on_start>
88          <interval>12h</interval>
89          <skip_nfs>yes</skip_nfs>
90      </sca>
91
92      <!-- File integrity monitoring -->
93      <syscheck>
94          <disabled>no</disabled>
95
96          <!-- Frequency that syscheck is executed default every 12 hours -->
97          <frequency>43200</frequency>
98
99          <scan_on_start>yes</scan_on_start>
100
101         <!-- Directories to check (perform all possible verifications) -->
102         <directories>/etc,/usr/bin,/usr/sbin</directories>
103         <directories check_all="yes" whodata="yes"/>/home/vagrant/test</directories>
104         <directories>/root</directories>
105         <directories>/bin,/sbin,/boot</directories>
106
107         <!-- Files/directories to ignore -->
108         <ignore>/etc/mtab</ignore>
109         <ignore>/etc/hosts.deny</ignore>
110         <ignore>/etc/mail/statistics</ignore>
111         <ignore>/etc/random.seed</ignore>
112         <ignore>/etc/random.seed</ignore>
113         <ignore>/etc/adjtime</ignore>
114         <ignore>/etc/httpd/logs</ignore>
115         <ignore>/etc/utmpx</ignore>
116         <ignore>/etc/wtmpx</ignore>
117         <ignore>/etc/cups/certs</ignore>
118         <ignore>/etc/dumpdates</ignore>
119         <ignore>/etc/svc/volatile</ignore>
120
121         <!-- File types to ignore -->

```

Note that we enabled whodata. This will make the Wazuh agent use an integration with the operating system kernel in order to report file changes in real-time and include details on who and how those changes were made.

Restart the agent to apply changes:

```

[root@agent01 vagrant]# systemctl restart wazuh-agent

(gedit:19073): Tepl-WARNING **: 10:32:46.666: GVfs metadata is not supported by this platform. In the latter case, you should configure Tepl with --disable-gvfs
root /var/ ossec/etc systemctl restart wazuh-agent
root /var/ ossec/etc gedit ossec.conf
root /var/ ossec/etc gedit ossec.conf
$ sudo systemctl restart wazuh-agent

```

We create several files and subdirectories in our agent. By default, the script will add 10 directories with 20 files each of 1KB in `/home/vagrant/test`:

```

[root@agent01 vagrant]# python3 wazuh-ransomware-poc.py prepare

Error: Bad arguments. Valid arguments: prepare, attack, restore
root /home/ osboxes/Downloads/1 python3 wazuh-ransomware-poc.py prepare
root /home/ osboxes/Downloads/

```

Now the directories and files created can be listed:

```

root / > home > osboxes > Downloads ls
wazuh-ransomware-poc.py
root / > home > osboxes > Downloads python wazuh-ransomware-poc.py
Error: Bad arguments. Valid arguments: 'prepare', 'attack', 'restore'
root / > home > osboxes > Downloads 1 python3 wazuh-ransomware-poc.py prepare
root / > home > osboxes > Downloads ls -lRh /home/vagrant/test/
/home/vagrant/test/:
total 40K
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_00
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_01
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_02
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_03
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_04
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_05
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_06
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_07
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_08
drwxr-xr-x 2 root root 4.0K May  3 10:37 Directory_09
agent.name
/home/vagrant/test/Directory_00:
total 80K
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_00.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_01.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_02.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_03.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_04.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_05.txt
agent.name
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_06.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_07.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_08.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_09.txt
osboxes
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_10.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_11.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_12.txt
osboxes
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_13.txt
osboxes
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_14.txt
osboxes
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_15.txt
osboxes

```

Count

agent.name

osboxes

File Manager

Linux Lite Terminal

From the Wazuh UI, we can see the new files:

The screenshot shows the Wazuh UI interface. At the top, there's a navigation bar with links for 'File', 'Machine', 'View', 'Input', 'Devices', 'Help', and a search bar. Below that is a sub-navigation bar with 'Wazuh - Wazuh' selected, along with other tabs like 'Preventing and detecting', 'wazuh.com/resources/blocks...', and 'Help Manual'. The main area has a title 'Dashboard' and a sub-section 'Events'. On the left, there's a sidebar with a search field and a list of available fields including 'agent.id', 'agent.ip', 'data.arch', etc. The main content area features a histogram titled '659 hits' showing file creation counts over time (May 2, 2023 @ 10:37:43.094 - May 3, 2023 @ 10:37:43.095). Below the histogram is a table with columns: 'Time', 'agent.name', 'rule.description', 'rule.level', and 'rule.id'. The table contains several rows, each with a timestamp, the agent name 'osboxes', and the rule description 'file added to the system'. The rule level is consistently '5' and the rule ID is '554'. The table is sorted by 'Time'.

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh x Preventing and detecting x wazuh.com/resources/blo... +

Help Manual Support Forums Google Search

wazuh. Modules Security events

rule.id rule.level

Available fields

- agent.id
- agent.ip
- data.arch
- data.audit.aud
- audit.command
- audit.euid
- audit.exe
- audit.gid
- data.audit.id
- data.audit.pid
- data.audit.session
- data.audit.type
- data.audit.uid
- data.command
- data.dpkg.status
- data.dbusser
- data.euid
- data.extra\_data
- data.file
- data.gid
- data.home
- data.id
- data.package
- data.ppid
- data.sca.check.command
- data.sca.check.compliance.cis
- data.sca.check.compliance.cis\_ec
- data.sca.check.compliance.cis\_level
- data.sca.check.compliance.gpg\_IV
- data.sca.check.compliance.gpg\_13
- data.sca.check.compliance.hipaa
- data.sca.check.compliance.nist\_800\_53
- data.sca.check.compliance.pc1\_des
- data.sca.check.compliance.tsc
- data.sca.check.description
- data.sca.check.id
- data.sca.check.previous\_result

Time agent.name rule.description rule.level rule.id

May 3, 2023 0 18:17:06.998 osboxes File added to the system. 5 264

Expanded document

Table JSON

# _index	wazuh-alerts-4.x-2023.05.03
# agent.id	002
# agent.ip	10.8.2.35
# agent.name	osboxes
# decoder.name	syscheck_new_entry
# full_log	File '/home/vagrant/test/Directory_09/File_17.txt' added Mode: whodata
# id	1683124626.584544
# input.type	log
# location	syscheck
# manager.name	wazuh-server

The index pattern was refreshed successfully.  
There were some unknown fields for the current index pattern. You need to refresh the page to apply the changes.

View surrounding documents View single document

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh x Preventing and detecting x wazuh.com/resources/blo... +

Help Manual Support Forums Google Search

wazuh. Modules Security events

data.dpkg.status data.euid

data.extra\_data data.gid

data.home data.id

data.package data.ppid

data.sca.check.command data.sca.check.compliance.cis

data.sca.check.compliance.cis\_ec data.sca.check.compliance.cis\_level

data.sca.check.compliance.gpg\_IV data.sca.check.compliance.gpg\_13

data.sca.check.compliance.hipaa data.sca.check.compliance.nist\_800\_53

data.sca.check.compliance.pc1\_des data.sca.check.compliance.tsc

data.sca.check.description data.sca.check.id

data.sca.check.previous\_result

Mode: whodata

# id 1683124626.584544  
# input.type log  
# location syscheck  
# manager.name wazuh-server  
# rule.description File added to the system.  
# rule.firedtimes 180  
# rule.gdpr II\_5.1.f  
# rule.gpg13 4.11  
# rule.groups ossec, syscheck, syscheck\_entry\_added, syscheck\_file  
# rule.hipaa 164.312.c.1, 164.312.c.2  
# rule.id 554  
# rule.level 5  
# rule.mal false  
# rule.mist\_800\_53 SI.7  
# rule.pc1\_des 11.5

The index pattern was refreshed successfully.  
There were some unknown fields for the current index pattern. You need to refresh the page to apply the changes.

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh x Preventing and detecting x wazuh.com/resources/blo... +

Help Manual Support Forums Google Search

wazuh. Modules Security events

data.sca.total\_checks data.sca.type

data.shell data.scp

data.scp data.ssh

data.ssh data.sudo

data.sudo data.syscheck

data.syscheck data.syscheck.event

data.syscheck data.syscheck.gid\_after

data.syscheck data.syscheck.gname\_after

data.syscheck data.syscheck.inode\_after

data.syscheck data.syscheck.mds\_after

data.syscheck data.syscheck.mode

data.syscheck data.syscheck.atime\_after

data.syscheck data.syscheck.path

data.syscheck data.syscheck.perm\_after

data.syscheck data.syscheck.sha1\_after

data.syscheck data.syscheck.size\_after

data.syscheck data.syscheck.uid\_after

syscheck.audit\_process\_ppid 689  
syscheck.audit\_user\_id 0  
syscheck.audit\_user\_name root  
syscheck.event added  
syscheck.gid\_after 0  
syscheck.gname\_after root  
syscheck.inode\_after 15466796  
syscheck.mds\_after a20bac999c0429de1a8d2adcc80cd7  
syscheck.mode whodata  
syscheck.atime\_after May 3, 2023 0 18:37:05.000  
syscheck.path /home/vagrant/test/Directory\_09/File\_17.txt  
syscheck.perm\_after r--r--r--  
syscheck.sha1\_after f0be1fed8eacf0bc1ed28e2896f0be4dd6b19d9f2  
syscheck.size\_after 1,924  
syscheck.uid\_after 0

The index pattern was refreshed successfully.  
There were some unknown fields for the current index pattern. You need to refresh the page to apply the changes.

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh | Preventing and detecting | wazuh.com/resources/blo... +

Help Manual Support Forums Google Search

wazuh. Modules Security events ⓘ

syscheck.event added

syscheck.gid\_after 0

syscheck.gname\_after root

syscheck.inode\_after 15466798

syscheck.md5\_after a294bac899c8429d6d1a8d2adcc8cd7

syscheck.mode whodata

syscheck.atime\_after May 3, 2023 10:37:05.000

syscheck.path /home/vagrant/text/Directory\_09/File\_17.txt

syscheck.perm\_after rw-r--r--

syscheck.shah\_after f90e1fed0acf1bc10e38e289f58e4dd0b79da2

syscheck.sha56\_after 954a4db29083061016a71847b536f7e5908fa68010032af994dfbcfc81884

syscheck.size\_after 1,024

syscheck.uid\_after 0

syscheck.uname\_after root

timestamp May 3, 2023 10:37:06.990

The index pattern was refreshed successfully.

There were some unknown fields for the current index pattern. You need to refresh the page to apply the changes.

Reload page

May 3, 2023 10:37:06.988 osboxes File added to the system.

5 554

Wazuh - Wazuh - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wazuh - Wazuh | Preventing and detecting | wazuh.com/resources/blo... +

Help Manual Support Forums Google Search

wazuh. Modules Security events ⓘ

May 3, 2023 10:37:06.990 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.988 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.984 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.982 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.980 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.977 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.974 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.972 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.970 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.966 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.963 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.960 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.958 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.955 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.953 osboxes File added to the system. 5 554

May 3, 2023 10:37:06.951 osboxes File added to the system. 5 554

The index pattern was refreshed successfully.

There were some unknown fields for the current index pattern. You need to refresh the page to apply the changes.

Reload page

May 3, 2023 10:37:06.970 osboxes File added to the system.

5 554

# File integrity monitoring attack detection

File Integrity Monitoring (FIM) helps in auditing sensitive files and meeting regulatory compliance requirements. Wazuh has an inbuilt FIM module that monitors file system changes to detect the creation, modification, and deletion of files.

This use case uses the Wazuh FIM module to detect changes in monitored directories on Ubuntu and Windows endpoints. The Wazuh FIM module enriches alert data by fetching information about the user and process that made the changes using who-data audit.

## Configuration

Perform the following steps to configure the Wazuh agent to monitor filesystem changes in the `/root` directory.

1. Edit the Wazuh agent `/var/ossec/etc/ossec.conf` configuration file. Add the directories for monitoring within the `<syscheck>` block. For this use case, you configure Wazuh to monitor the `/root` directory. To get additional information about the user and process that made the changes, enable `who-data audit`:

```
<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
```

**Note** You can also configure any path of your choice in the `<directories>` block.

2. Restart the Wazuh agent to apply the configuration changes:

```
sudo systemctl restart wazuh-agent
```

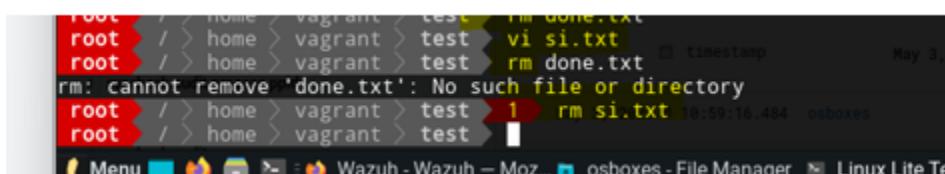
## Attack Test the configuration

1. Create a text file in the monitored directory then wait for 5 seconds.
2. Add content to the text file and save it. Wait for 5 seconds.
3. Delete the text file from the monitored directory.

## Visualize the alerts

You can visualize the alert data in the Wazuh dashboard. To do this, go to the Security events module and add the filters in the search bar to query the alerts:

```
Ubuntu - rule.id: is one of 550,553,554
```



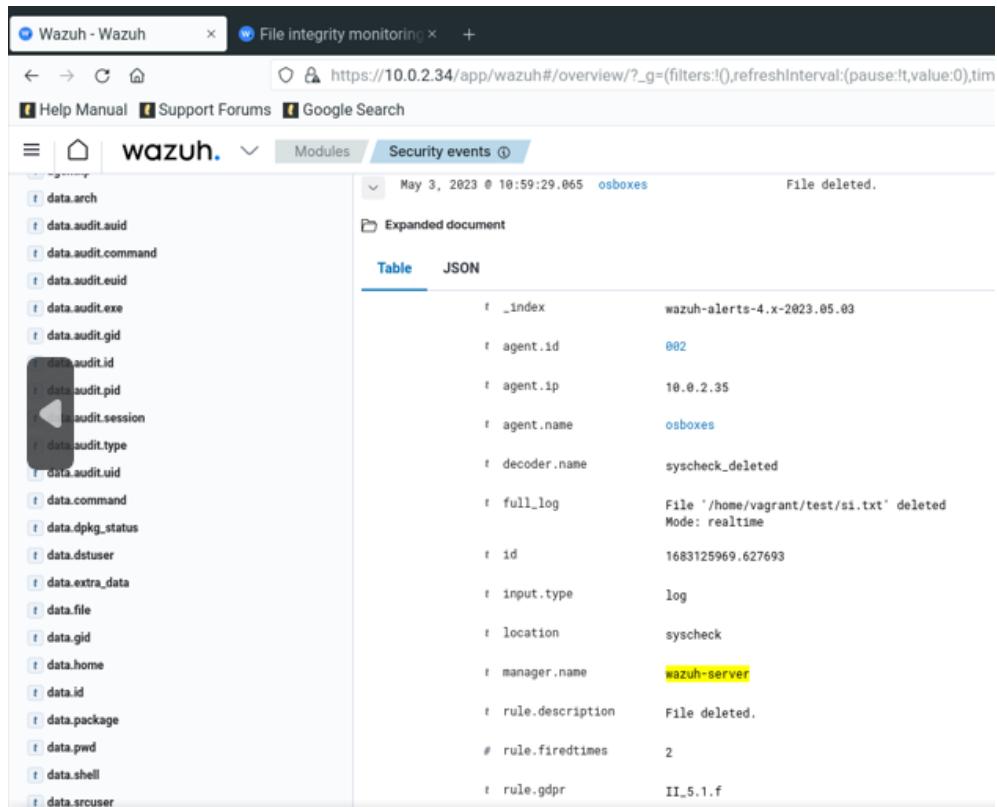
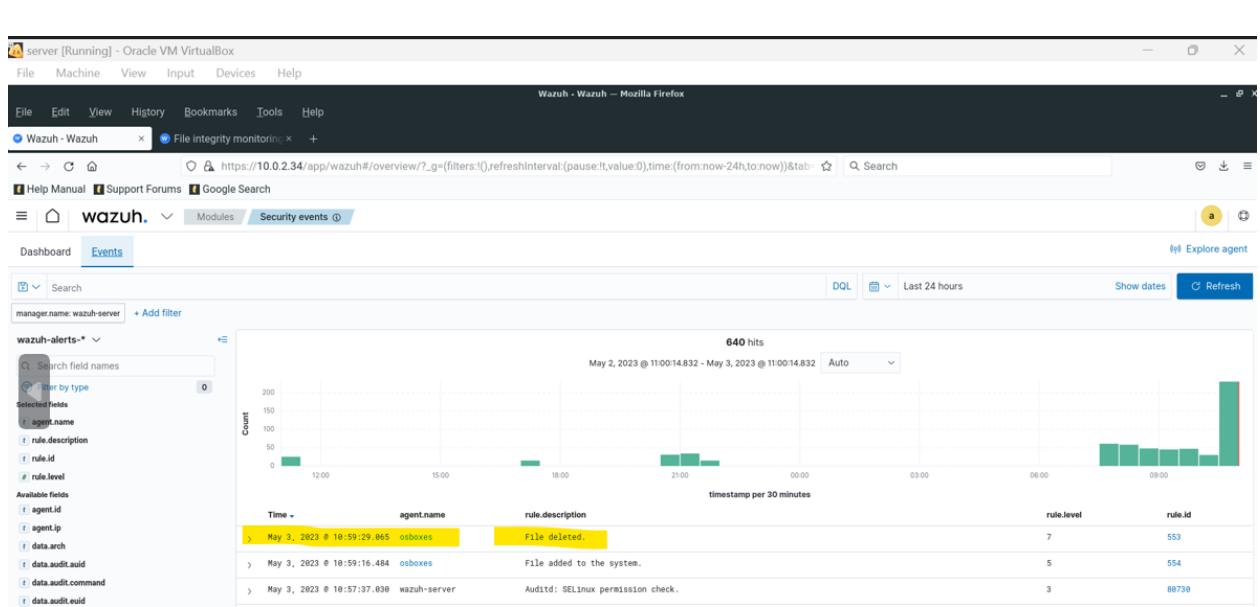
```
root@vagrant:~/test# rm done.txt
root@vagrant:~/test# vi si.txt
root@vagrant:~/test# rm done.txt
rm: cannot remove 'done.txt': No such file or directory
root@vagrant:~/test# rm si.txt
root@vagrant:~/test#
```

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Open ossec.conf

```
90  </sca>
91  <!-- File integrity monitoring -->
92  <syscheck>
93  <disabled=noc</disabled>
94
95  <!-- Frequency that syscheck is executed default every 12 hours -->
96  <frequency>43200</frequency>
97
98
99  <scan_on_start>yes</scan_on_start>
100
101 <!-- Directories to check (perform all possible verifications) -->
102 <directories>/etc,/usr/bin,/usr/sbin</directories>
103 <directories check_all="yes" report_changes="yes" realtime="yes">/home/vagrant/test</directories>
104 <directories>/root</directories>
105 <directories>/bin,/sbin,/boot</directories>
106
107 <!-- Files/directories to ignore -->
108 <ignore>/etc/mtab</ignore>
109 <ignore>/etc/mtab</ignore>
110 <ignore>/etc/mail/statistics</ignore>
111 <ignore>/etc/random.seed</ignore>
112 <ignore>/etc/random.seed</ignore>
113 <ignore>/etc/adjtime</ignore>
114 <ignore>/etc/httpd/logs</ignore>
115 <ignore>/etc/utmpx</ignore>
116 <ignore>/etc/utmp</ignore>
117 <ignore>/etc/cups/certs</ignore>
118 <ignore>/etc/dumpdates</ignore>
119 <ignore>/etc/svc/volatile</ignore>
120
121 <!-- File types to ignore -->
122 <ignore type="sregex">.log$|.swp$</ignore>
123
124 <!-- Check the file, but never compute the diff -->
125 <nodiff>/etc/sasl/private.key</nodiff>
126
127 <skip_nfs>yes</skip_nfs>
128 <skip_dev>yes</skip_dev>
129 <skip_proc>yes</skip_proc>
130 <skip_sys>yes</skip_sys>
131
132 <!-- Nice value for Syscheck process -->
133 <process priority>10</process priority>
```



The screenshots show the Wazuh web interface displaying security event logs. The top screenshot shows a detailed log entry for a file integrity monitoring rule, with fields like rule.id (553), rule.level (7), rule.mail (false), rule.mitre.id (T1870\_004, T1485), rule.mitre.tactic (Defense Evasion, Impact), rule.mitritechnique (File Deletion, Data Destruction), rule.nist\_800\_53 (SI.7), rule.pcidds (11.5), rule.tsc (PII.4, PII.5, CC6.1, CC6.8, CC7.2, CC7.3), rule.syscheck.event (deleted), rule.syscheck.gid\_after (0), rule.syscheck.gname\_after (root), rule.syscheck.inode\_after (15466710), and rule.syscheck.md5\_after (ec37f2c552334e4bbd376cf1b2491287). The bottom screenshot shows a summary log entry for a file added to the system, with fields like rule.firetimes (deleted), rule.gid (0), rule.gname (root), rule.inode (15466710), rule.mode (realtime), rule.mtime (May 3, 2023 @ 10:59:16.000), rule.path (/home/vagrant/test/s1.txt), rule.perm (rw-r--r--), rule.sha1 (396355594933785dd641f8d4206c3c38955b38a8), rule.sha256 (aa3cab63c017fc101bea87d957765150c0453202097adfd0fa74453399942198), rule.size (12), rule.uid (0), rule.uname (root), and rule.timestamp (May 3, 2023 @ 10:59:29.065). Both screenshots also show navigation links for Help Manual, Support Forums, and Google Search.

This attack will be done again in reverse shell Execution attack!