Mayukh Borana
1007395

SOC : Security Ops Centre

4th 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 :

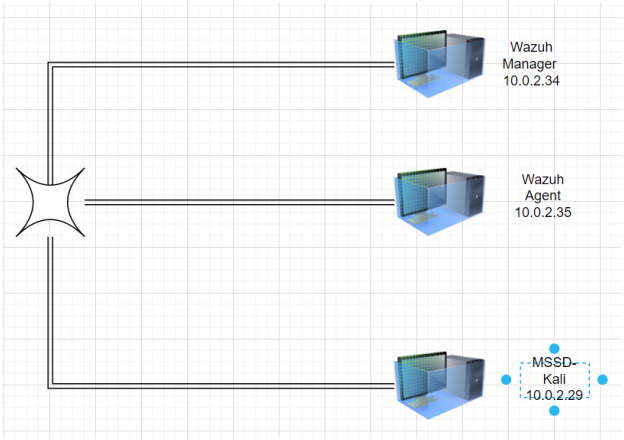
- Security Onion
- OSSIM
- Wazuh
- IBM QRadar CE
- Splunk Demo version

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

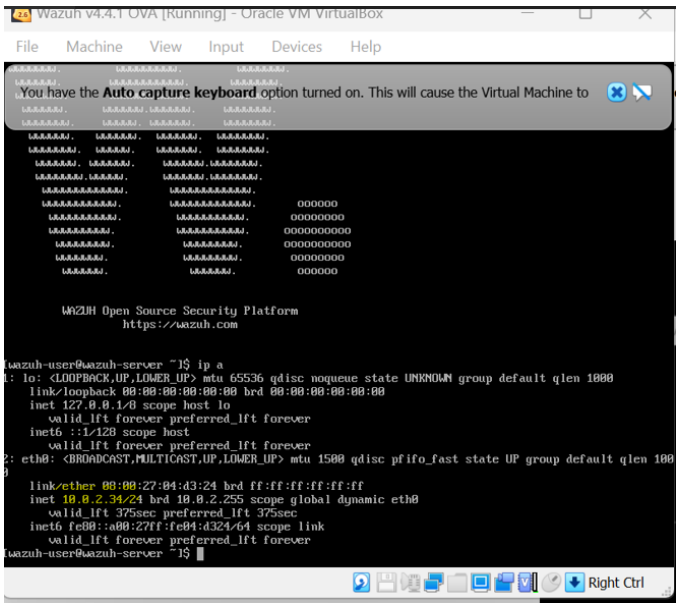
Requirement:

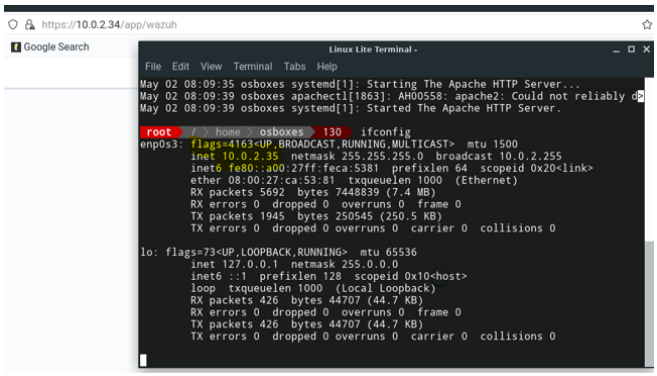
Network Topology

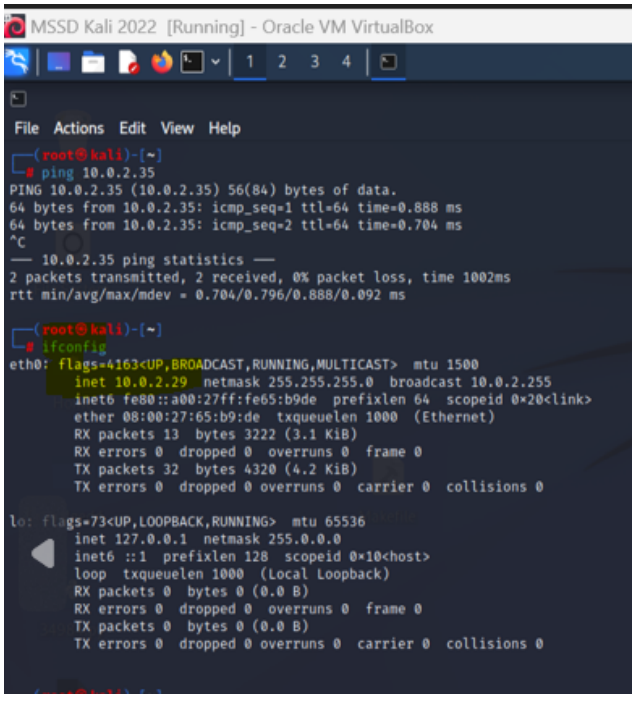


IP of my Virtual Network

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 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 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 100
0
link/ether 08:00:27:04:d3:24 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:fe04:d324/64 scope link
valid_lft forever preferred_lft forever
wazuh-user@wazuh-server ~]$
Right Ctrl


https://10.0.2.34/app/wazuh
Google Search
Linux Lite Terminal -
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 d
May 02 08:09:39 osboxes systemd[1]: Started The Apache HTTP Server.
root / home osboxes 130 ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.35 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:feca:5381 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:ca:53:81 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 prefixlen 128 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

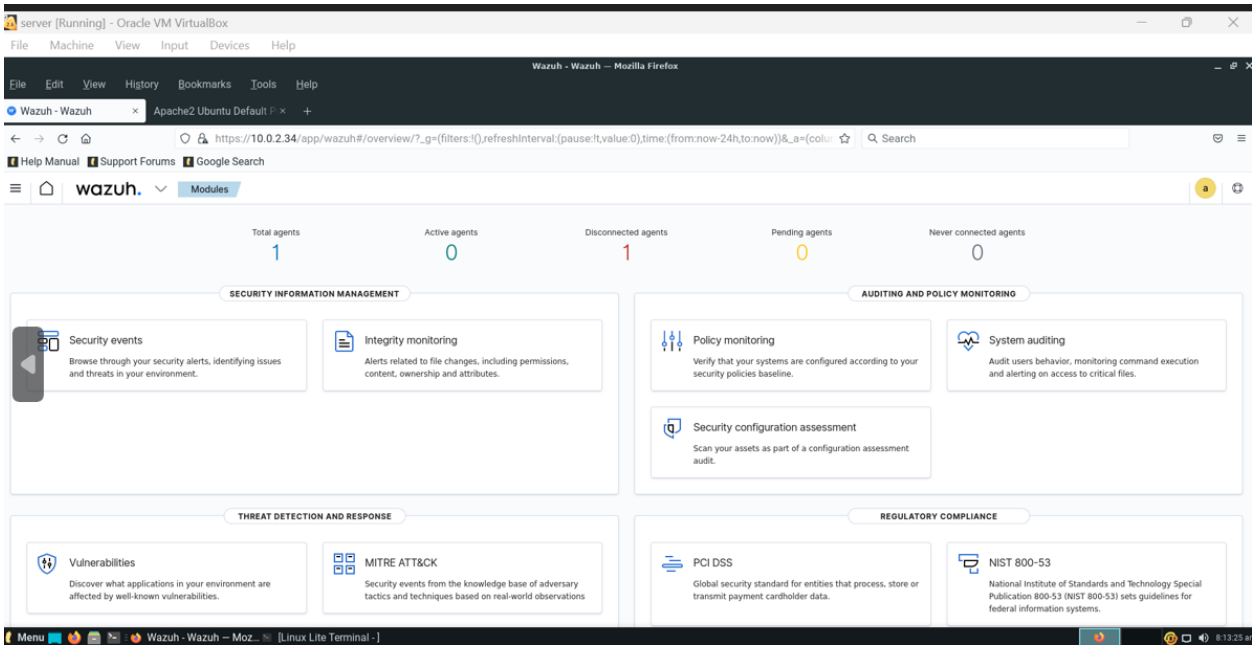

MSSD Kali 2022 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
(root㉿kali)-[~]
ping 10.0.2.35
PING 10.0.2.35 (10.0.2.35) 56(84) bytes of data.
64 bytes from 10.0.2.35: icmp_seq=1 ttl=64 time=0.888 ms
64 bytes from 10.0.2.35: icmp_seq=2 ttl=64 time=0.704 ms
^C
— 10.0.2.35 ping statistics —
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 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe65:b9de prefixlen 64 scopeid 0x20<link>
ether 08:00:27:65: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 prefixlen 128 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

Attack Variety

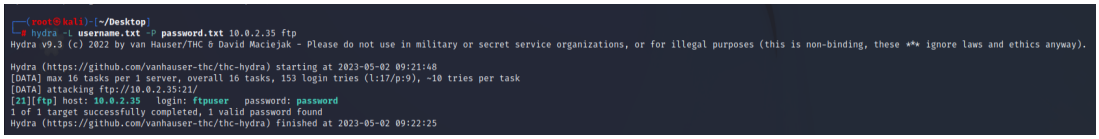
SrNo.	Name of attack which has been detected By Open Source Wazuh
1	Detection of BruteForce on FTP server Login credentials
2	Detecting SQLi in Apache Web Server
3	Detecting Ransomware with Wazuh
4	File Integrity Monitoring Attack Detection
5	Detecting MetaSploit attack
5	
7	Detecting ShellShock attack(Using 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
Apache2 Ubuntu Default P
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
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.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.
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 — Moz...
[Linux Lite Terminal -]

Detecting a brute-force attack



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:**

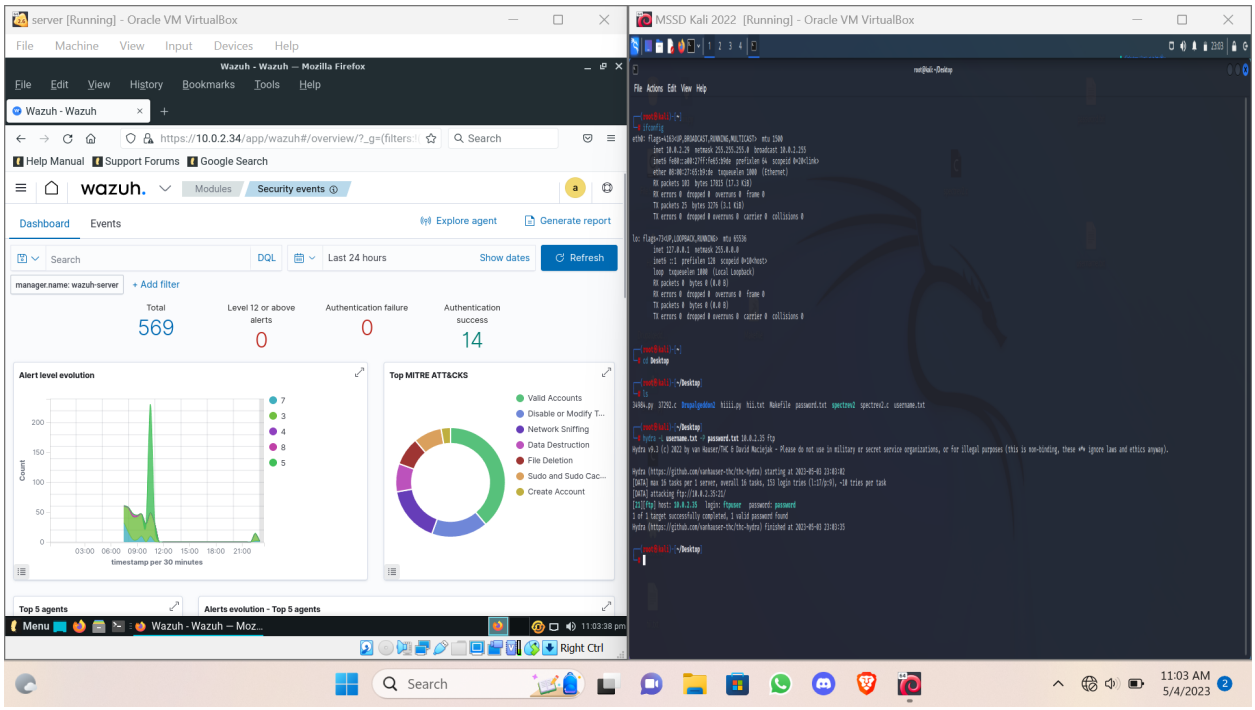
sudo apt update

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:**

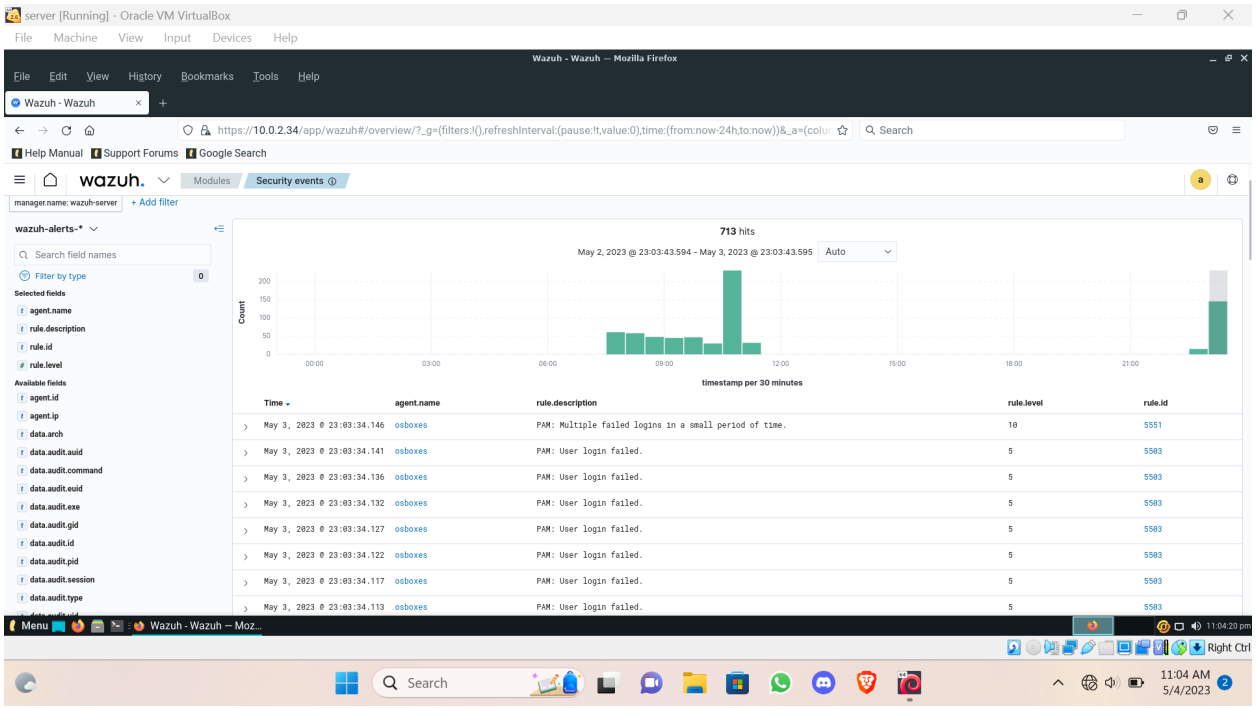
   sudo hydra -L <username.txt>-P <PASSWD_LIST.txt> <server_IP> ftp

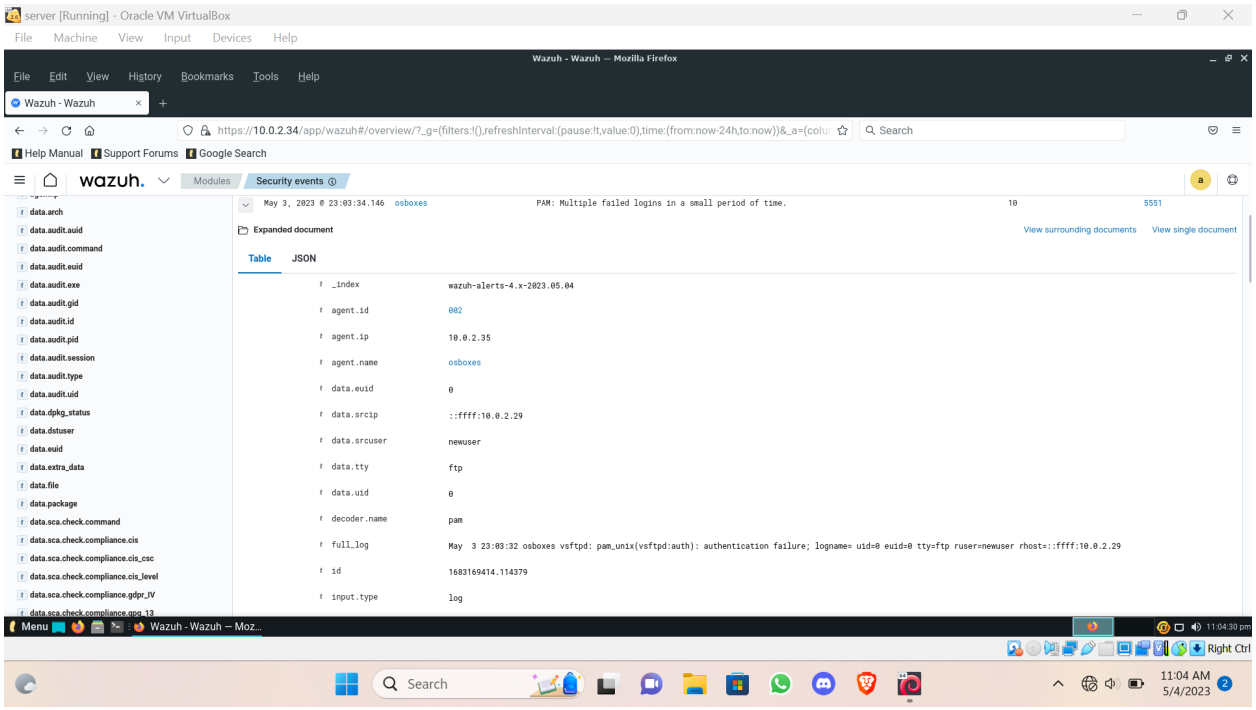


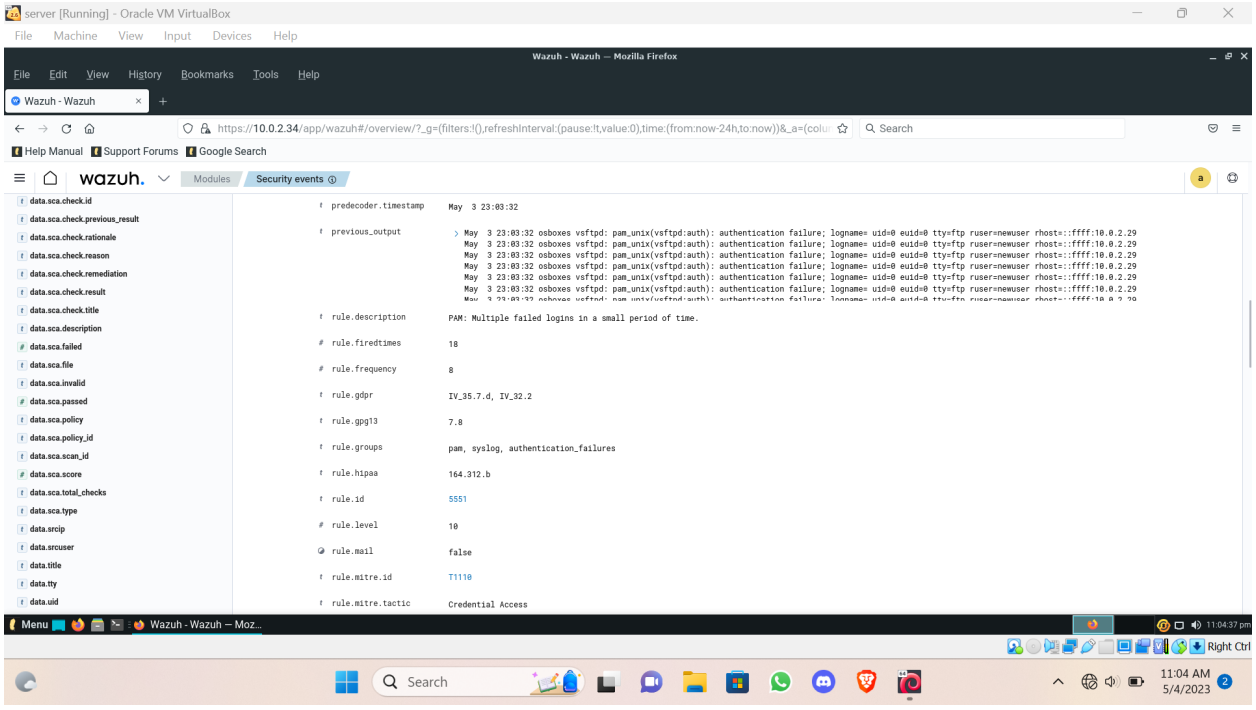
Visualize the alerts

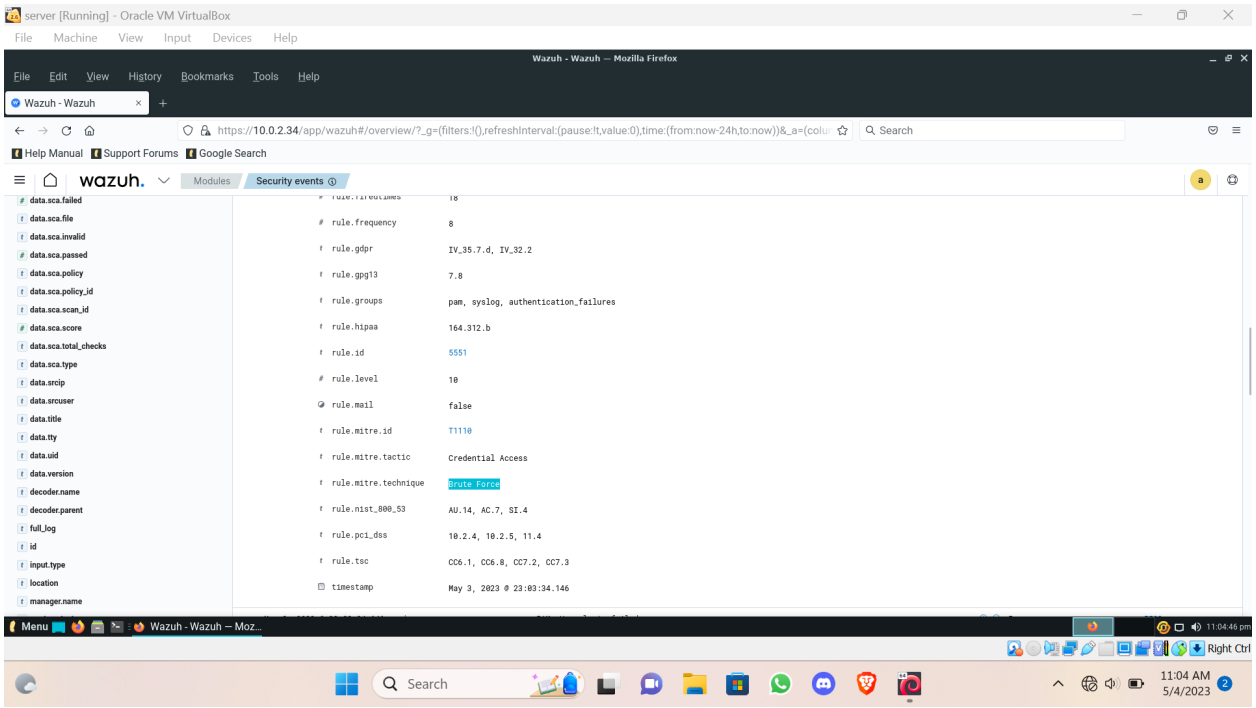
You can visualize the alert data in the Wazuh dashboard. To do this, go to the Security events module and add the filters in the search bar to query the alerts.

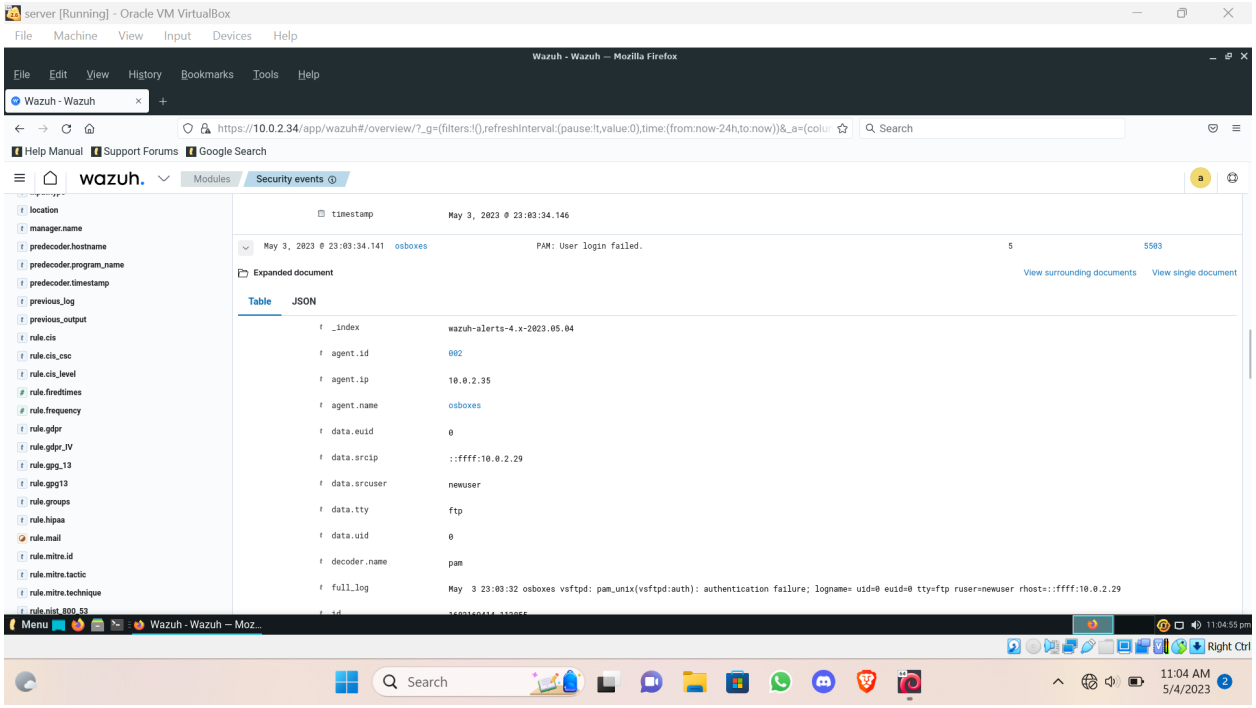
Linux - `rule.id:(5551 OR 5712)`. Other related rules are `5710`, `5711`, `5716`, `5720`, `5503`, `5504`.

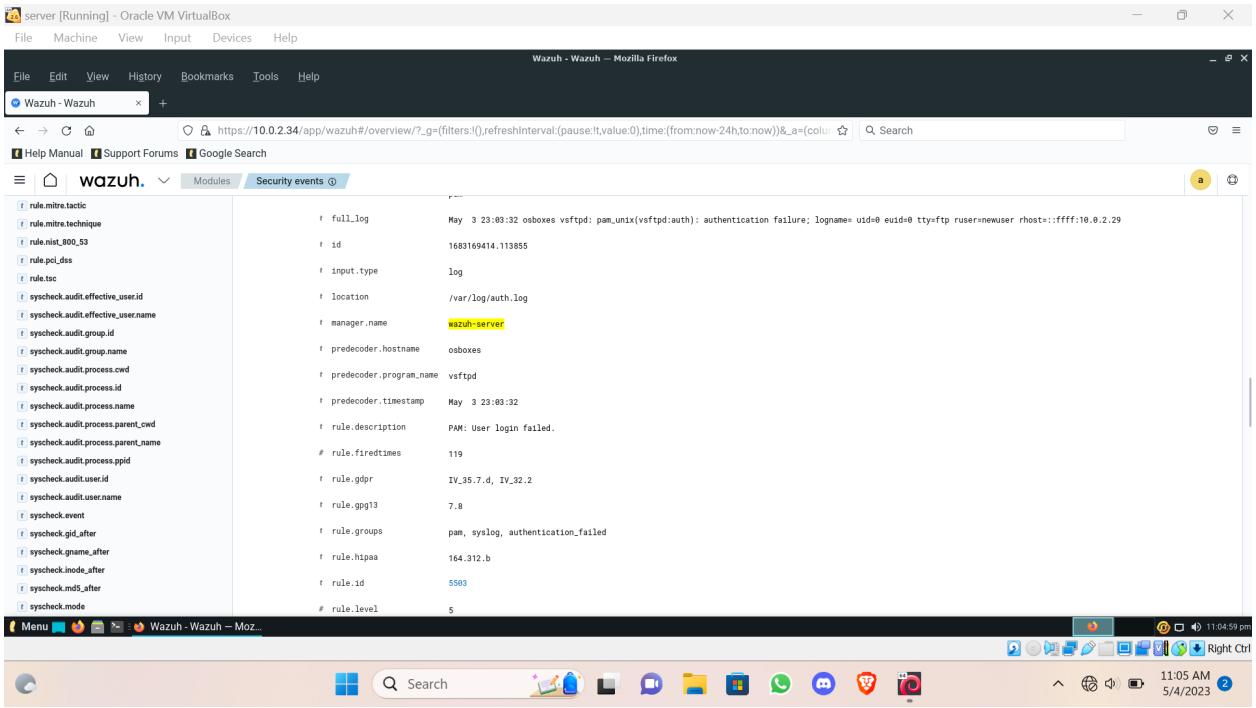

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
manager.name: wazuh-server
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
agent.name
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
data.arch
data.audit.auid
data.audit.command
data.audit.euid
data.audit.exe
data.audit.gid
data.audit.id
data.audit.pid
data.audit.session
data.audit.type
713 hits
May 2, 2023 @ 23:03:43.594 - May 3, 2023 @ 23:03:43.595
Auto
Count
200
150
100
50
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
timestamp per 30 minutes
Time
agent.name
rule.description
rule.level
rule.id
May 3, 2023 @ 23:03:34.146 osboxes PAM: Multiple failed logins in a small period of time. 10 5551
May 3, 2023 @ 23:03:34.141 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.136 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.132 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.127 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.122 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.117 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.113 osboxes PAM: User login failed. 5 5503
Menu
Wazuh - Wazuh — Moz...
11:04:20 pm
Right Ctrl
Search
11:04 AM
5/4/2023

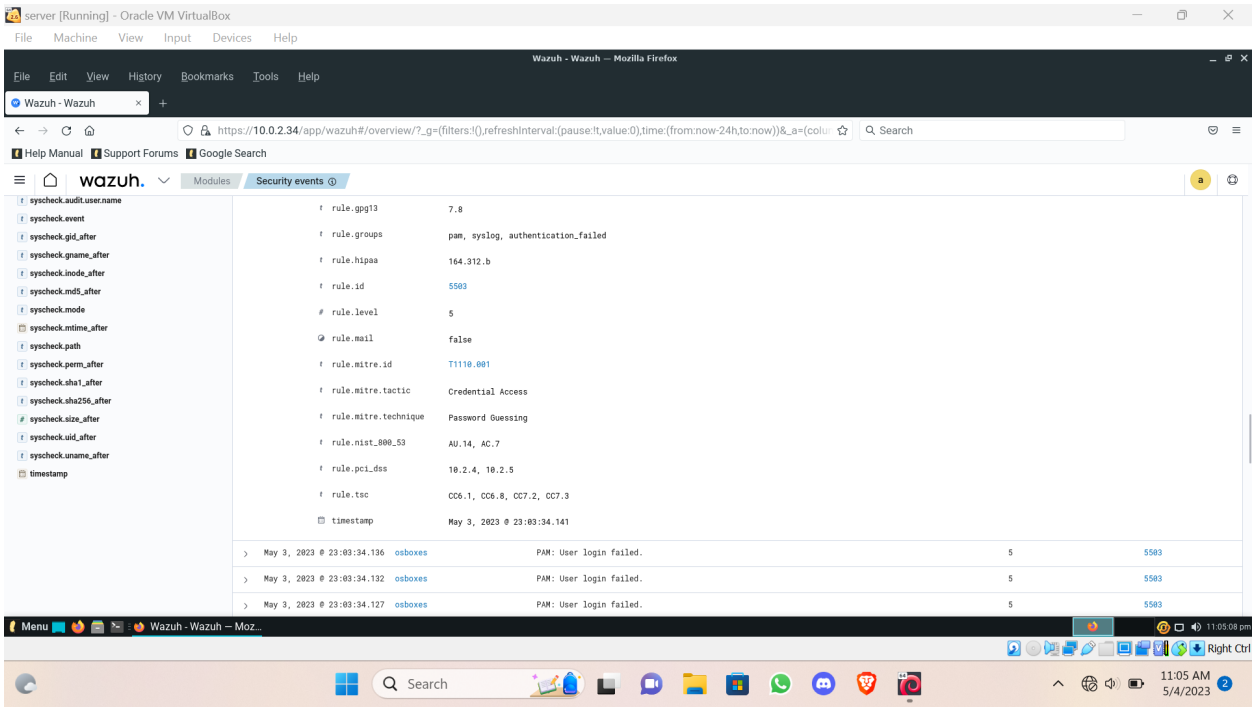

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
May 3, 2023 @ 23:03:34.146 osboxes PAM: Multiple failed logins in a small period of time. 10 5551
Expanded document
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.srcip ::ffff:10.0.2.29
data.srcuser 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
Menu
Wazuh - Wazuh — Moz...
11:04:30 pm
Right Ctrl
Search
11:04 AM
5/4/2023

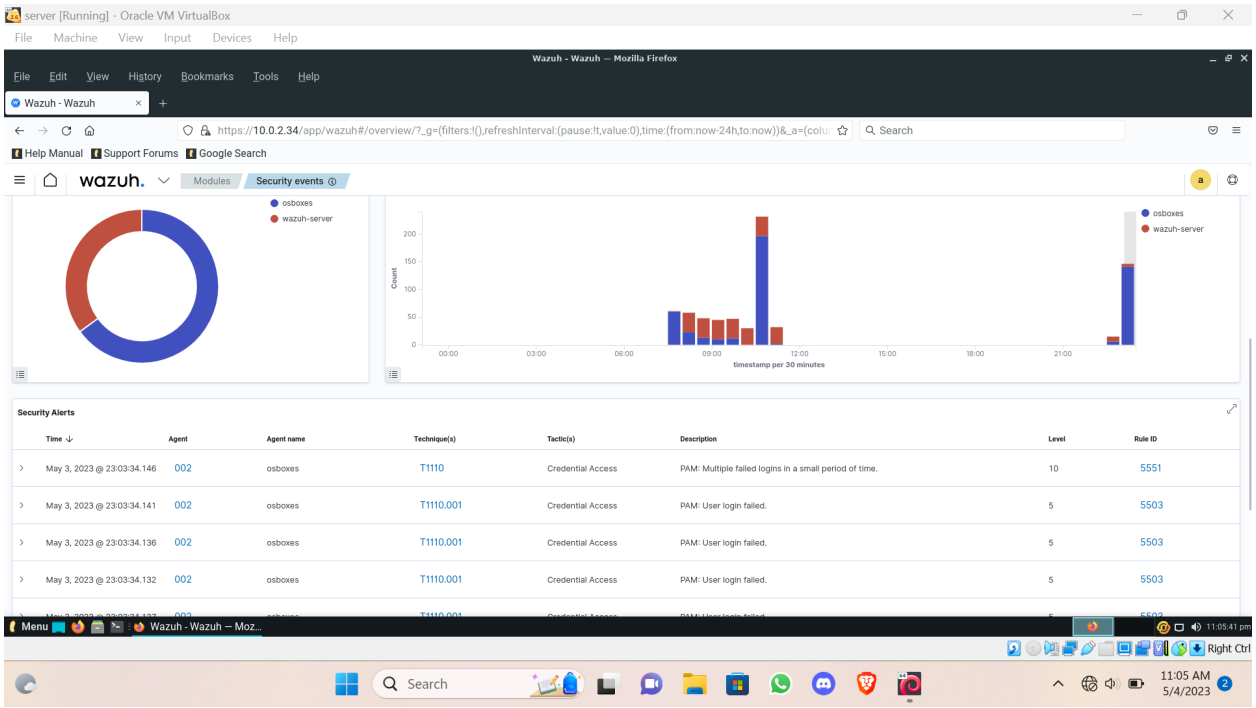

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
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
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 T1110
rule.mitre.tactic Credential Access
Menu
Wazuh - Wazuh — Moz...
11:04:37 pm
Right Ctrl
Search
11:04 AM
5/4/2023

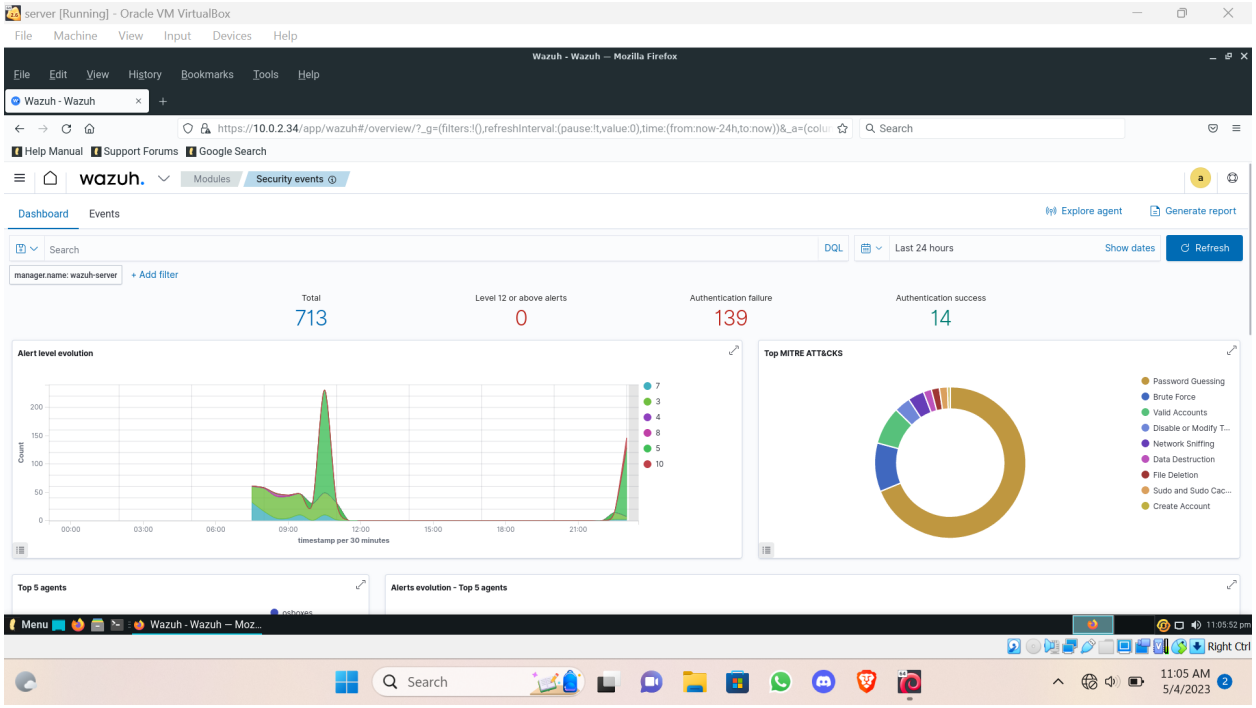

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
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.srcip
data.srcuser
data.title
data.tty
data.uid
data.version
decoder.name
decoder.parent
full_log
id
input.type
location
manager.name
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 T1110
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
Wazuh - Wazuh — Moz...
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 History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
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.cis
rule.cis_csc
rule.cis_level
rule.firedtimes
rule.frequency
rule.gdpr
rule.gdpr_IV
rule.gpg_13
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. 5 5503
Expanded document
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.srcip ::ffff:10.0.2.29
data.srcuser 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
Menu
Wazuh - Wazuh — Moz...
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 History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
rule.mitre.tactic
rule.mitre.technique
rule.nist_800_53
rule.pci_dss
rule.tsc
syscheck.audit.effective_user.id
syscheck.audit.effective_user.name
syscheck.audit.group.id
syscheck.audit.group.name
syscheck.audit.process.cwd
syscheck.audit.process.id
syscheck.audit.process.name
syscheck.audit.process.parent_cwd
syscheck.audit.process.parent_name
syscheck.audit.process.ppid
syscheck.audit.user.id
syscheck.audit.user.name
syscheck.event
syscheck.gid_after
syscheck.gname_after
syscheck.inode_after
syscheck.md5_after
syscheck.mode
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 1683169414.113855
input.type log
location /var/log/auth.log
manager.name wazuh-server
predecoder.hostname osboxes
predecoder.program_name vsftpd
predecoder.timestamp May 3 23:03:32
rule.description PAM: User login failed.
rule.firedtimes 119
rule.gdpr IV_35.7.d, IV_32.2
rule.gpg13 7.8
rule.groups pam, syslog, authentication_failed
rule.hipaa 164.312.b
rule.id 5503
rule.level 5
Menu
Wazuh - Wazuh — Moz...
Right Ctrl
Search
11:05 AM
5/4/2023


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/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
syscheck.audit.user.name
syscheck.event
syscheck.gid_after
syscheck.gname_after
syscheck.inode_after
syscheck.md5_after
syscheck.mode
syscheck.mtime_after
syscheck.path
syscheck.perm_after
syscheck.sha1_after
syscheck.sha256_after
syscheck.size_after
syscheck.uid_after
syscheck.uname_after
timestamp
rule.gpg13 7.8
rule.groups pam, syslog, authentication_failed
rule.hipaa 164.312.b
rule.id 5503
rule.level 5
rule.mail false
rule.mitre.id T1110.001
rule.mitre.tactic Credential Access
rule.mitre.technique Password Guessing
rule.nist_800_53 AU.14, AC.7
rule.pci_dss 10.2.4, 10.2.5
rule.tsc CC6.1, CC6.8, CC7.2, CC7.3
timestamp May 3, 2023 @ 23:03:34.141
May 3, 2023 @ 23:03:34.136 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.132 osboxes PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.127 osboxes PAM: User login failed. 5 5503
Menu
Wazuh - Wazuh — Moz...
Right Ctrl
Search
11:05 AM
5/4/2023


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/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
osboxes
wazuh-server
Count
timestamp per 30 minutes
Security Alerts
Time
Agent
Agent name
Technique(s)
Tactic(s)
Description
Level
Rule ID
May 3, 2023 @ 23:03:34.146 002 osboxes T1110 Credential Access PAM: Multiple failed logins in a small period of time. 10 5551
May 3, 2023 @ 23:03:34.141 002 osboxes T1110.001 Credential Access PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.136 002 osboxes T1110.001 Credential Access PAM: User login failed. 5 5503
May 3, 2023 @ 23:03:34.132 002 osboxes T1110.001 Credential Access PAM: User login failed. 5 5503
Menu
Wazuh - Wazuh — Moz...
Right Ctrl
Search
11:05 AM
5/4/2023


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/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu
Search
Help Manual Support Forums Google Search
wazuh.
Modules
Security events
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
+ Add filter
Total
713
Level 12 or above alerts
0
Authentication failure
139
Authentication success
14
Alert level evolution
Count
timestamp per 30 minutes
Top MITRE ATT&CKS
Password Guessing
Brute Force
Valid Accounts
Disable or Modify T...
Network Sniffing
Data Destruction
File Deletion
Sudo and Sudo Cac...
Create Account
Top 5 agents
Alerts evolution - Top 5 agents
Menu
Wazuh - Wazuh — Moz...
Right Ctrl
Search
11:05 AM
5/4/2023

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

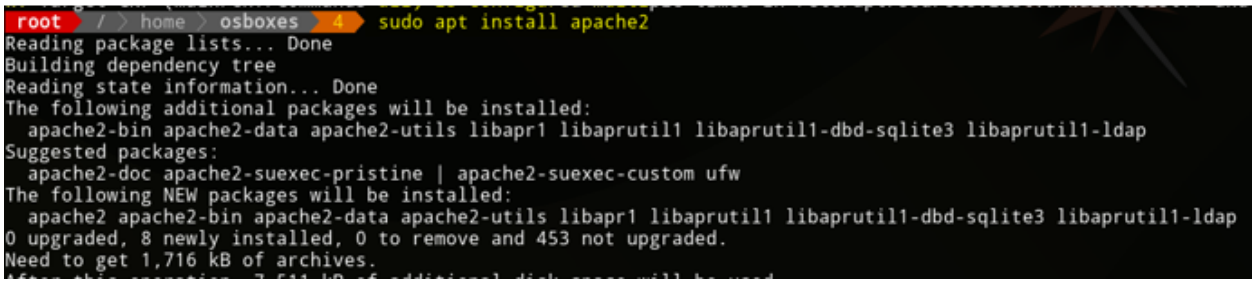
Perform the following steps to install Apache and configure the Wazuh agent to monitor the

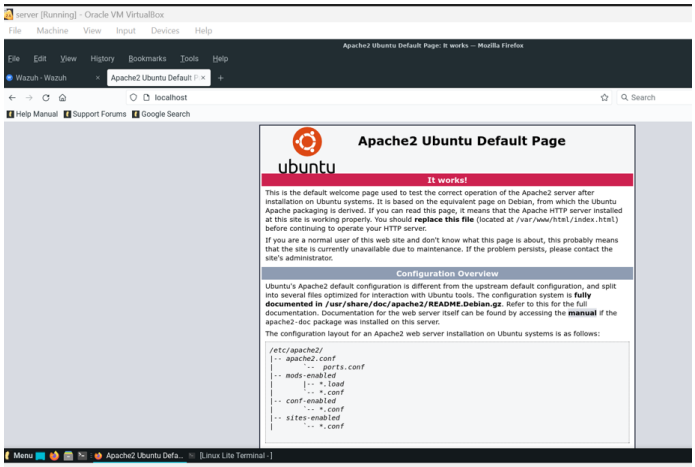
Apache logs.

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

sudo apt update

sudo apt install apache2





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:

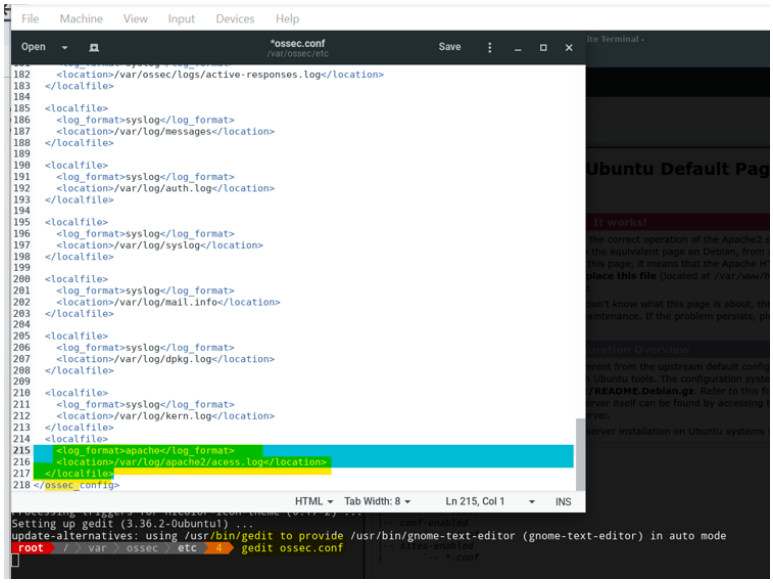
sudo systemctl status apache2

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>
```



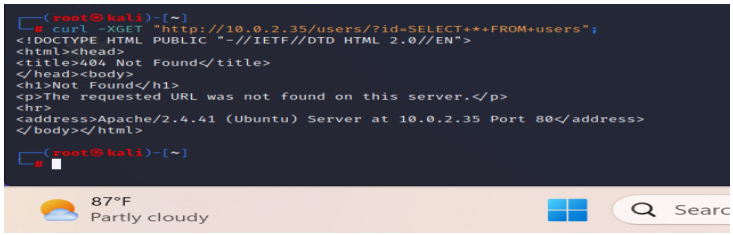
6. Restart the Wazuh agent to apply the configuration changes

sudo systemctl restart wazuh-agent

Attack emulation

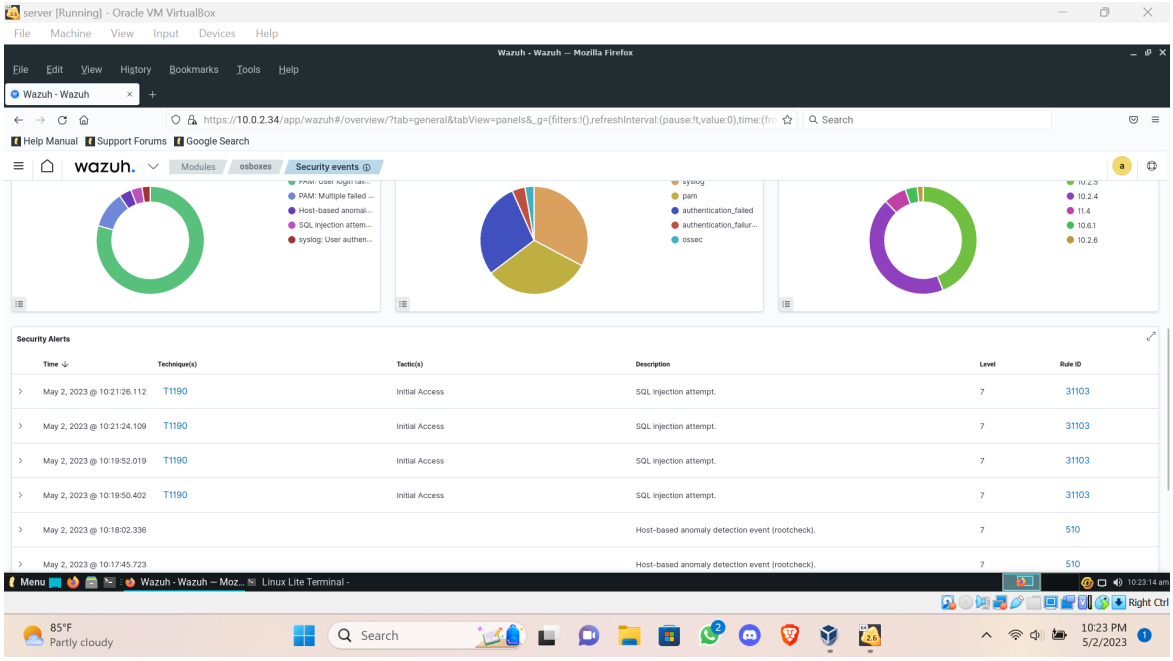
Replace `<UBUNTU_IP>` with the appropriate IP address and execute the following command from the attacker endpoint:

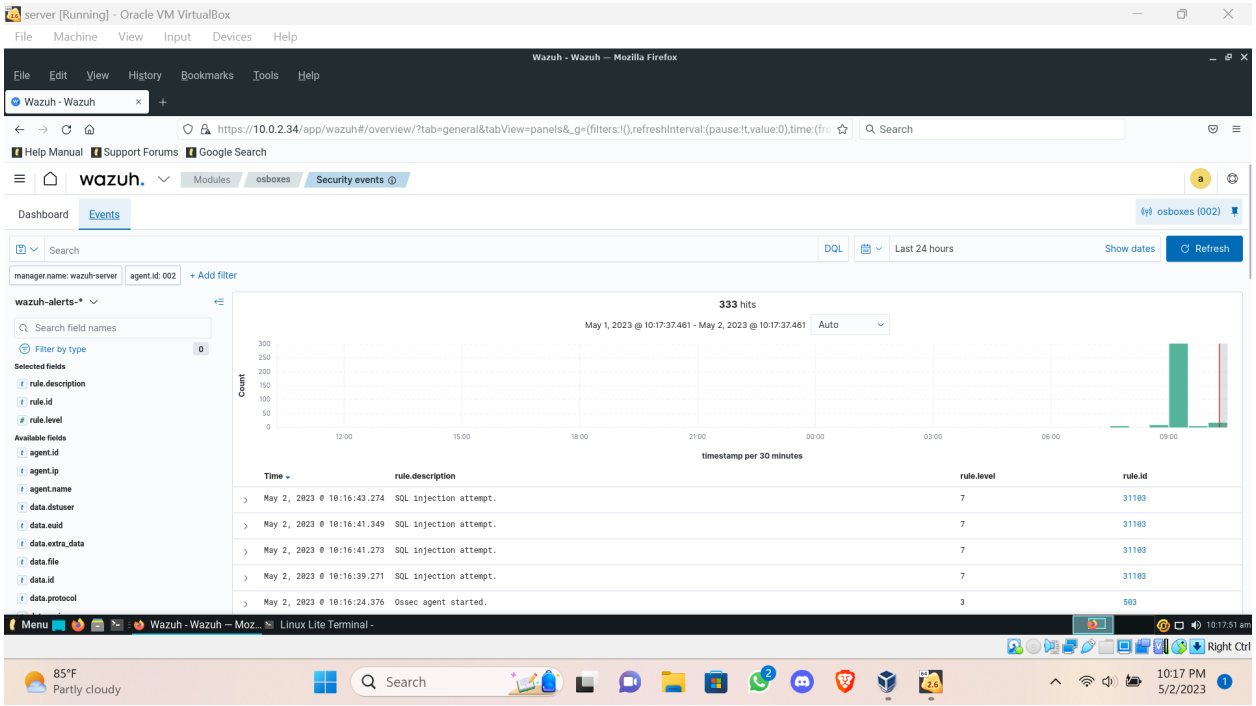
curl -XGET "http://<UBUNTU_IP>/users/?id=SELECT+*+FROM+users";

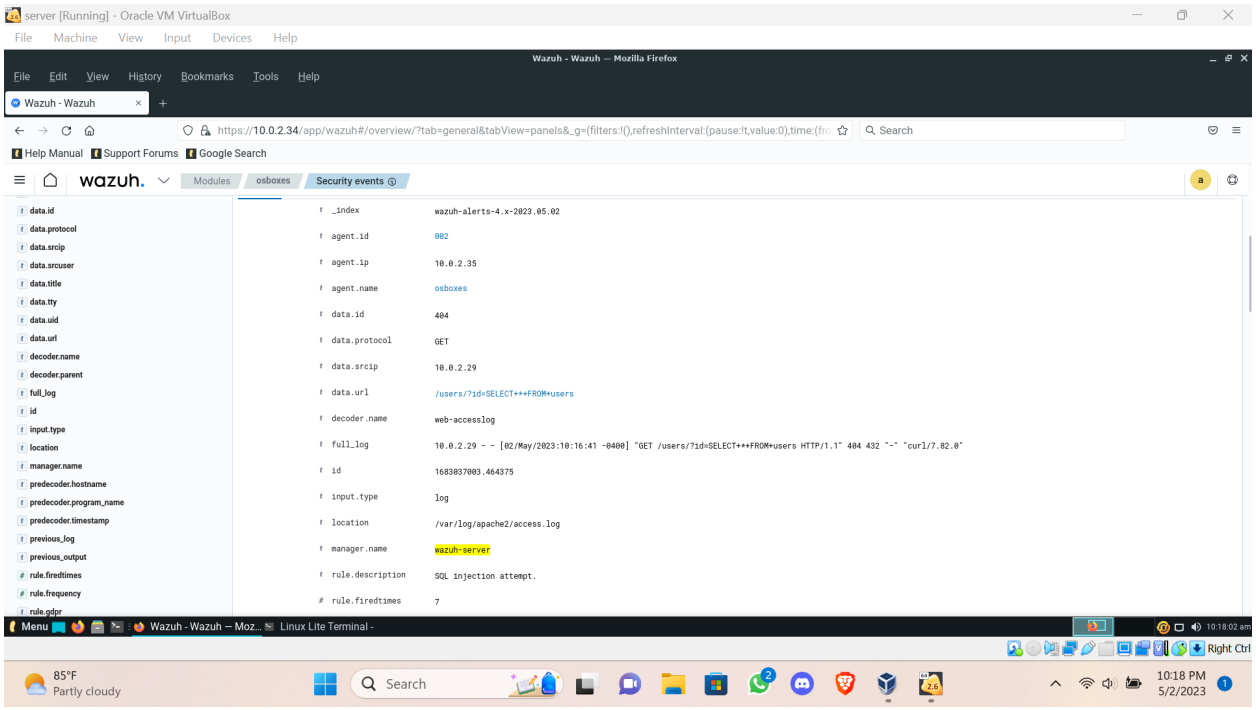


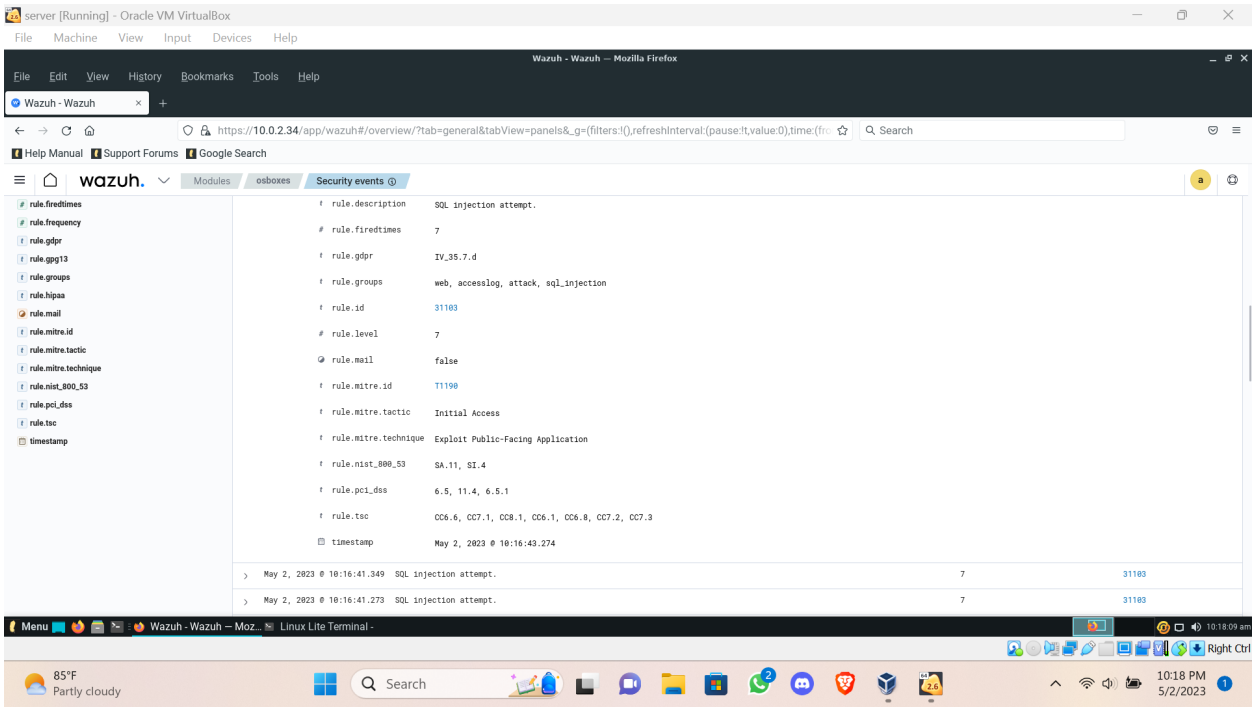
The expected result here is an alert with rule ID 31103 but a successful SQL injection attempt generates an alert with rule ID 31106.

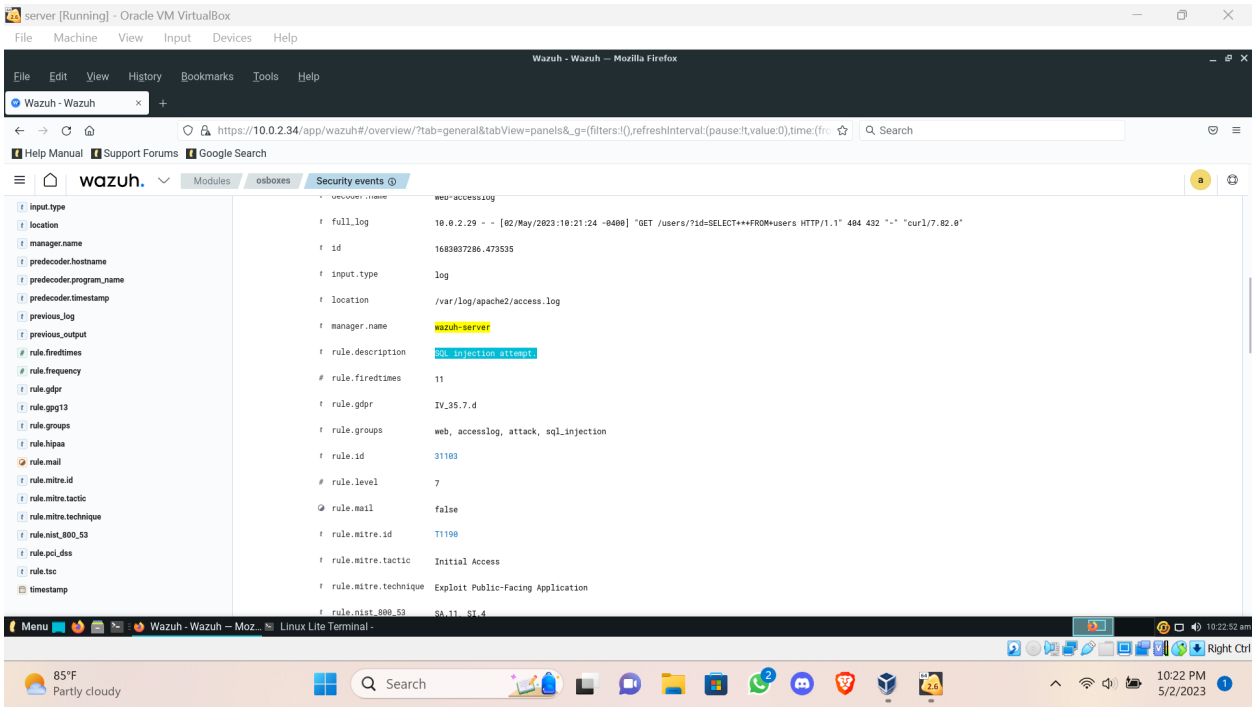
Visualize the alerts

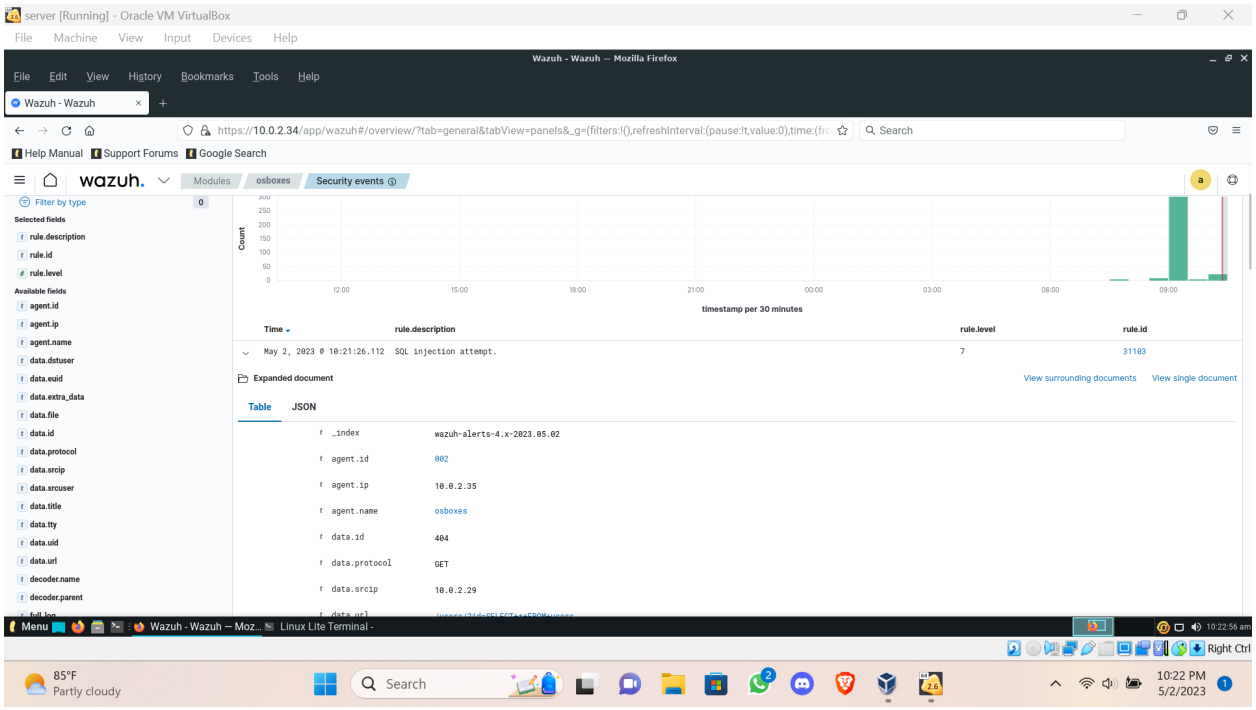

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
https://10.0.2.34/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fr
Search
Help Manual Support Forums Google Search
wazuh.
Modules osboxes Security events
PAM: Multiple failed ...
Host-based anomal...
SQL injection attem...
syslog: User authen...
pam
authentication_failed
authentication_failur...
ossec
10.2.4
11.4
10.6.1
10.2.6
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). 7 510
May 2, 2023 @ 10:17:45.723 Host-based anomaly detection event (rootcheck). 7 510
Menu Wazuh - Wazuh — Moz... Linux Lite Terminal -
Right Ctrl
85°F Partly cloudy
Search
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:!t,value:0),time:(fr
Search
Help Manual Support Forums Google Search
wazuh.
Modules osboxes Security events
Dashboard Events
osboxes (002)
Search
DQL
Last 24 hours
Show dates
Refresh
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.dstuser
data.euid
data.extra_data
data.file
data.id
data.protocol
333 hits
May 1, 2023 @ 10:17:37.461 - May 2, 2023 @ 10:17:37.461
Auto
Count
timestamp per 30 minutes
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
Menu Wazuh - Wazuh — Moz... Linux Lite Terminal -
Right Ctrl
85°F Partly cloudy
Search
10:17 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:!t,value:0),time:(fr
Search
Help Manual Support Forums Google Search
wazuh.
Modules osboxes Security events
data.id
data.protocol
data.srcip
data.srcuser
data.title
data.tty
data.uid
data.url
decoder.name
decoder.parent
full_log
id
input.type
location
manager.name
predecoder.hostname
predecoder.program_name
predecoder.timestamp
previous_log
previous_output
rule.firedtimes
rule.frequency
rule.gdpr
_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
data.url /users/?id=SELECT+++FROM+users
decoder.name web-accesslog
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 1683037003.464375
input.type log
location /var/log/apache2/access.log
manager.name wazuh-server
rule.description SQL injection attempt.
rule.firedtimes 7
Menu Wazuh - Wazuh — Moz... Linux Lite Terminal -
Right Ctrl
85°F Partly cloudy
Search
10:18 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:!t,value:0),time:(fr
Search
Help Manual Support Forums Google Search
wazuh.
Modules osboxes Security events
rule.firedtimes
rule.frequency
rule.gdpr
rule.gpg13
rule.groups
rule.hipaa
rule.mail
rule.mitre.id
rule.mitre.tactic
rule.mitre.technique
rule.nist_800_53
rule.pci_dss
rule.tsc
timestamp
rule.description SQL injection attempt.
rule.firedtimes 7
rule.gdpr IV_35.7.d
rule.groups web, accesslog, attack, sql_injection
rule.id 31103
rule.level 7
rule.mail false
rule.mitre.id T1190
rule.mitre.tactic Initial Access
rule.mitre.technique Exploit Public-Facing Application
rule.nist_800_53 SA.11, SI.4
rule.pci_dss 6.5, 11.4, 6.5.1
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
Menu Wazuh - Wazuh — Moz... Linux Lite Terminal -
Right Ctrl
85°F Partly cloudy
Search
10:18 PM 5/2/2023





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:

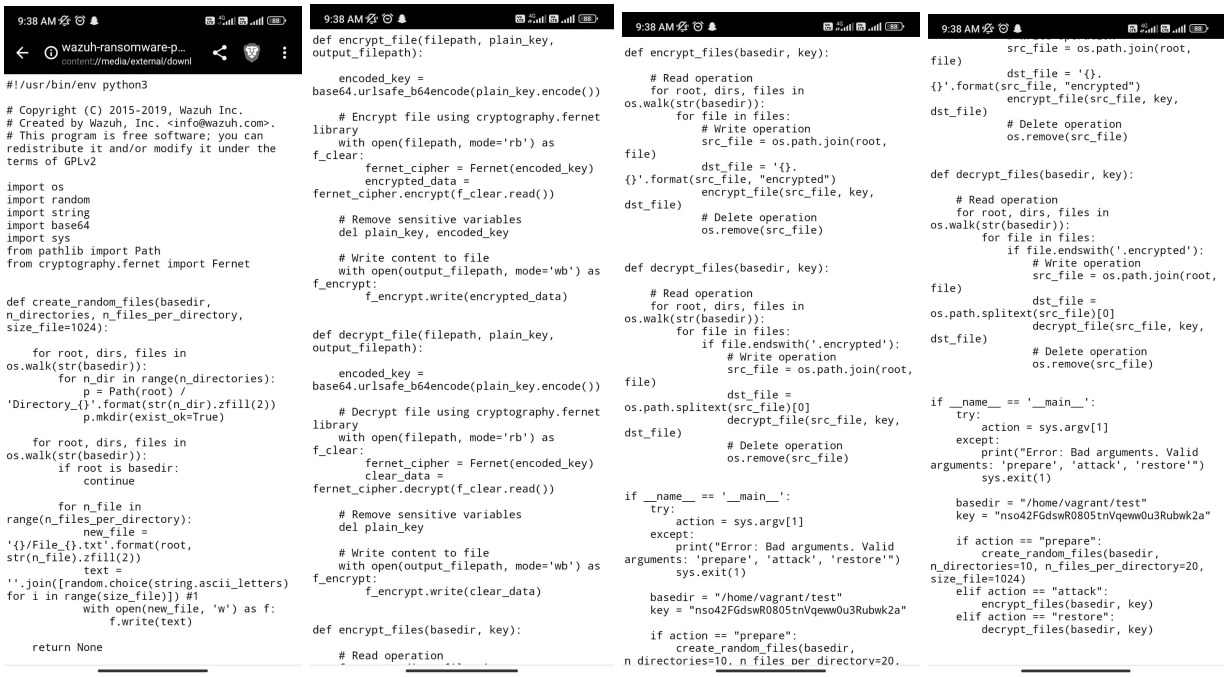
The following actions are performed by the ransomware during an attack:

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.



```
#!/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)]) #1
            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
```

```
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")
            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]
                decrypt_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 = "nso42FGdswR0805tnVqeww0u3Rubwk2a"

    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)
```

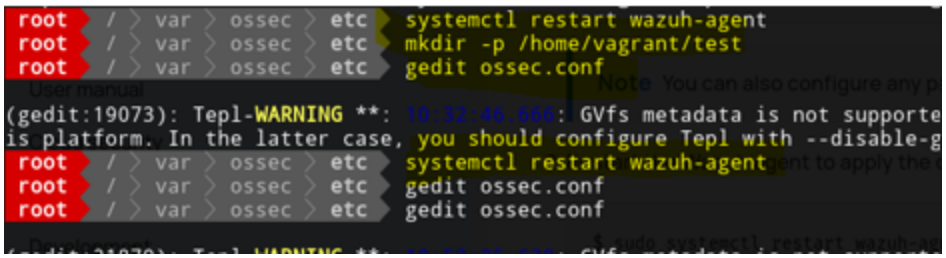
```
            src_file = os.path.join(root,
file)
            dst_file = '{}.
{}'.format(src_file, "encrypted")
            encrypt_file(src_file, key,
dst_file)
            # Delete operation
            os.remove(src_file)


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]
                decrypt_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 = "nso42FGdswR0805tnVqeww0u3Rubwk2a"

    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

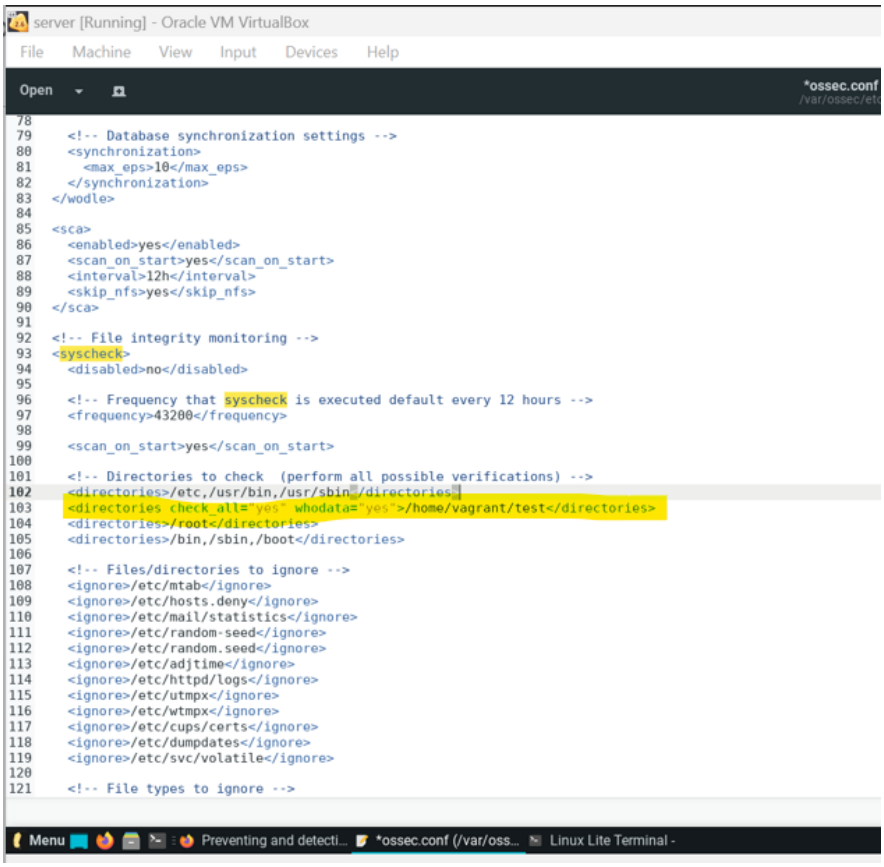
First, we create the `/home/vagrant/test` directory:

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



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

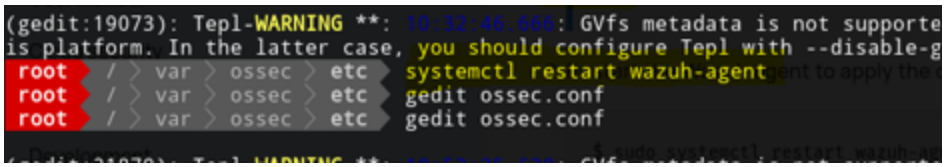
```
<syscheck>

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

</syscheck>
```



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.

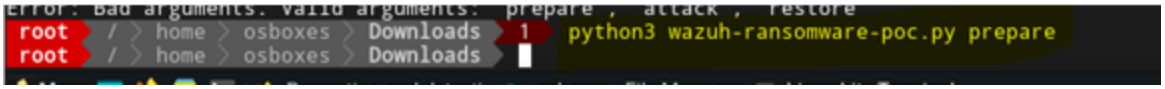
Restart the agent to apply changes:

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



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`:

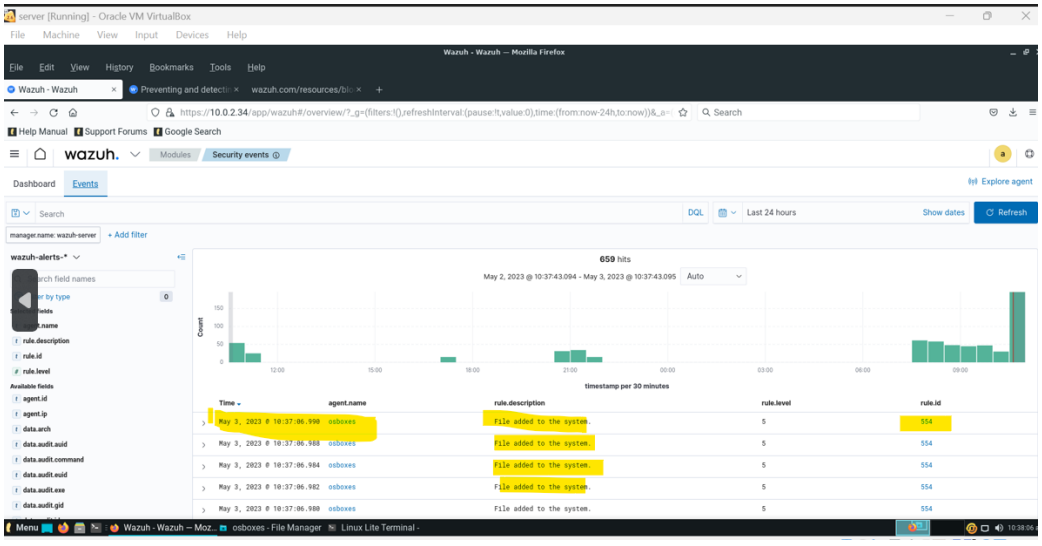
```
[root@agent01 vagrant]# python3 wazuh-ransomware-poc.py prepare
```

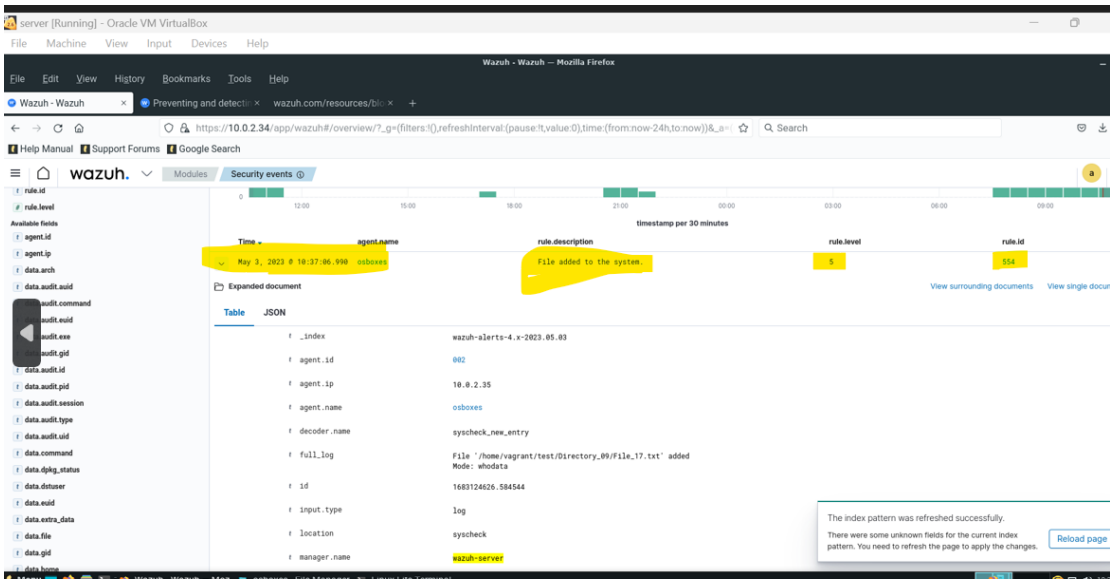


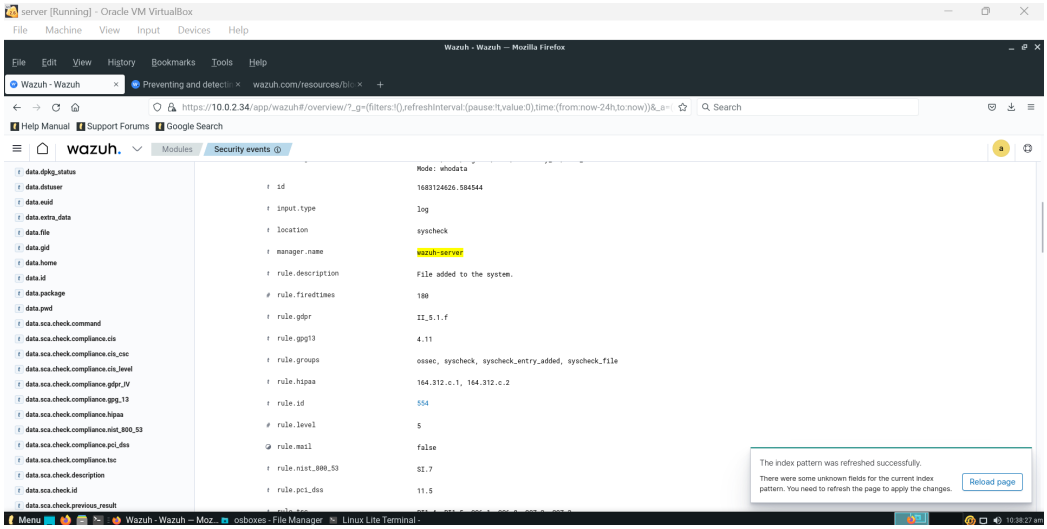
Now the directories and files created can be listed:

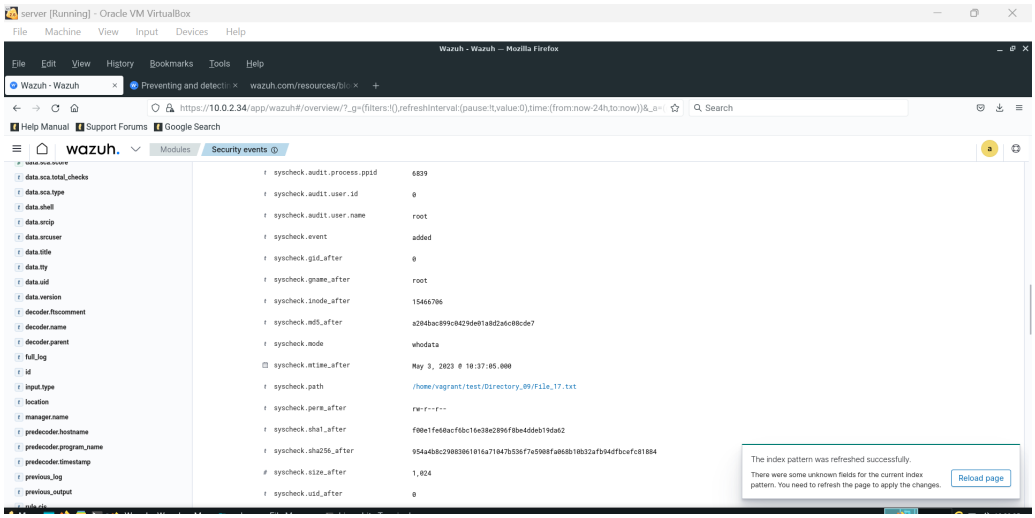
```
root / home osboxes Downloads ls
wazuh-ransomware-poc.py
root / home osboxes Downloads python wazuh-ransomware-poc.py
Error: Bad arguments. Valid arguments: 'prepare', 'attack', 'restore'
root / home osboxes Downloads 1 python3 wazuh-ransomware-poc.py prepare
root / home osboxes Downloads ls -lRh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

/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
-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
-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
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_13.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_14.txt
-rw-r--r-- 1 root root 1.0K May  3 10:37 File_15.txt
Menu  Wazuh - Wazuh — Moz...  osboxes - File Manager  Linux Lite Terminal -
```

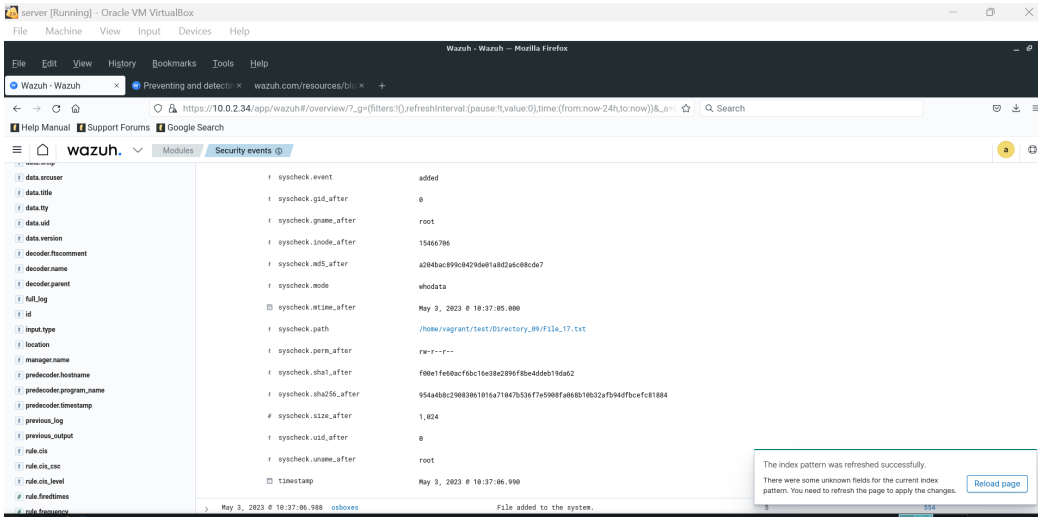
From the Wazuh UI, we can see the new files:

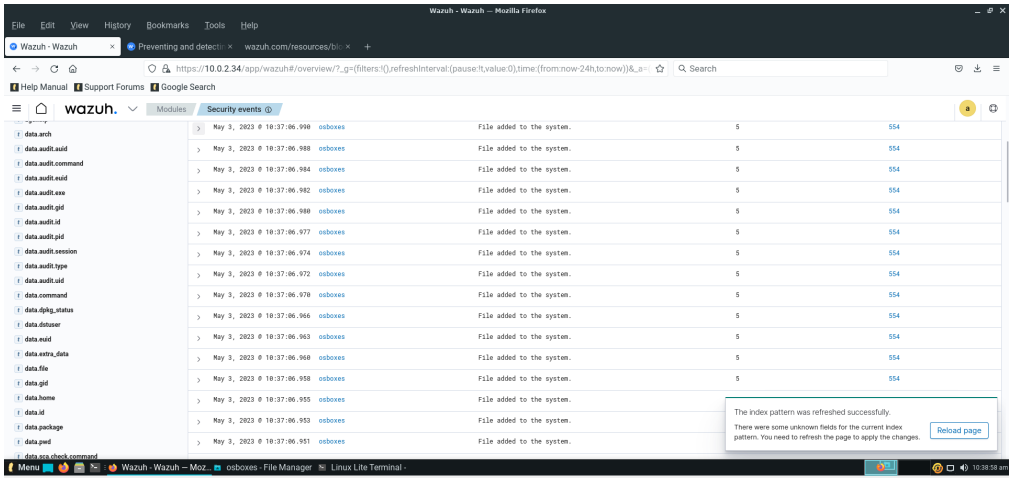



server [Running] - Oracle VM VirtualBox
Wazuh - Wazuh — Mozilla Firefox
wazuh.
Modules
Security events
timestamp per 30 minutes
Time
agent.name
rule.description
rule.level
rule.id
May 3, 2023 @ 10:37:06.990
osboxes
File added to the system.
5
554
Expanded document
Table
JSON
_index
wazuh-alerts-4.x-2023.05.03
agent.id
002
agent.ip
10.0.2.35
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.
Reload page


server [Running] - Oracle VM VirtualBox
Wazuh - Wazuh — Mozilla Firefox
wazuh.
Modules
Security events
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.mail
false
rule.nist_800_53
SI.7
rule.pci_dss
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.
Reload page


server [Running] - Oracle VM VirtualBox
Wazuh - Wazuh — Mozilla Firefox
wazuh.
Modules
Security events
syscheck.audit.process.ppid
6839
syscheck.audit.user.id
0
syscheck.audit.user.name
root
syscheck.event
added
syscheck.gid_after
0
syscheck.gname_after
root
syscheck.inode_after
15466706
syscheck.md5_after
a204bac899c0429de01a8d2a6c80cde7
syscheck.mode
whodata
syscheck.mtime_after
May 3, 2023 @ 10:37:05.000
syscheck.path
/home/vagrant/test/Directory_09/File_17.txt
syscheck.perm_after
rw-r--r--
syscheck.sha1_after
f00e1fe60acf6bc16e38e2896f8be4ddeb19da62
syscheck.sha256_after
954a4b8c29083061016a71047b536f7a5908fa068b10b32afb94dfbcefc81884
syscheck.size_after
1,024
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.
Reload page


server [Running] - Oracle VM VirtualBox
Wazuh - Wazuh — Mozilla Firefox
wazuh.
Modules
Security events
syscheck.event added
syscheck.gid_after 0
syscheck.gname_after root
syscheck.inode_after 15466706
syscheck.md5_after a204bac899c0429de01a8d2a6c08cde7
syscheck.mode whodata
syscheck.mtime_after May 3, 2023 @ 10:37:05.000
syscheck.path /home/vagrant/test/Directory_09/File_17.txt
syscheck.perm_after rw-r--r--
syscheck.sha1_after f00e1fe60acf6bc16e38e2896f8be4ddeb19da62
syscheck.sha256_after 954a4b8c290830610 16a71047b536f7e5908fa068b10b32afb94dfbcefc81884
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


Wazuh - Wazuh — Mozilla Firefox
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.
May 3, 2023 @ 10:37:06.953 osboxes File added to the system.
May 3, 2023 @ 10:37:06.951 osboxes File added to the system.
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

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

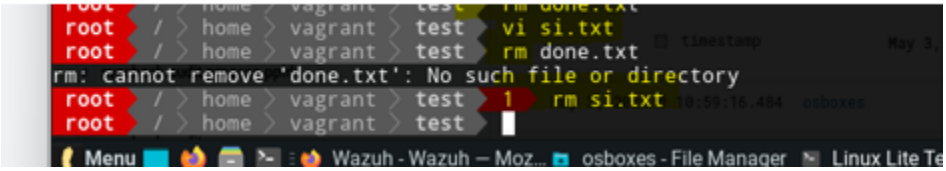
Attack Test the configuration

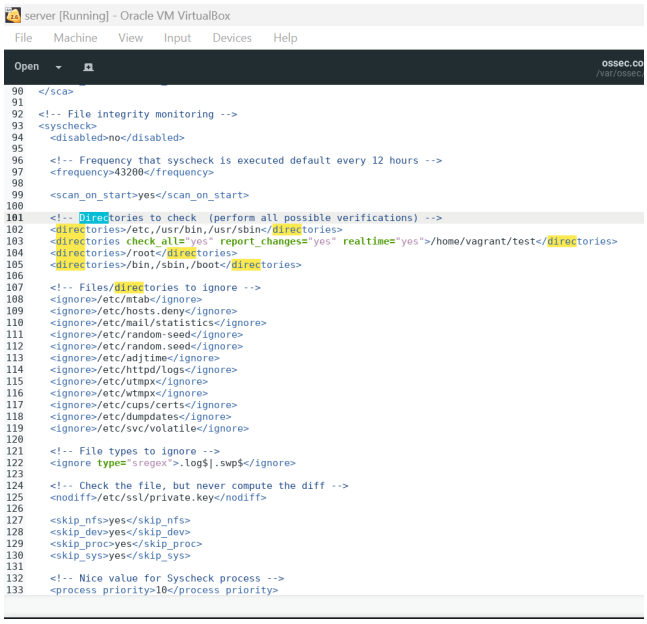
1. Create a text file in the monitored directory then wait for 5 seconds.
2. Add content to the text file and save it. Wait for 5 seconds.
3. Delete the text file from the monitored directory.

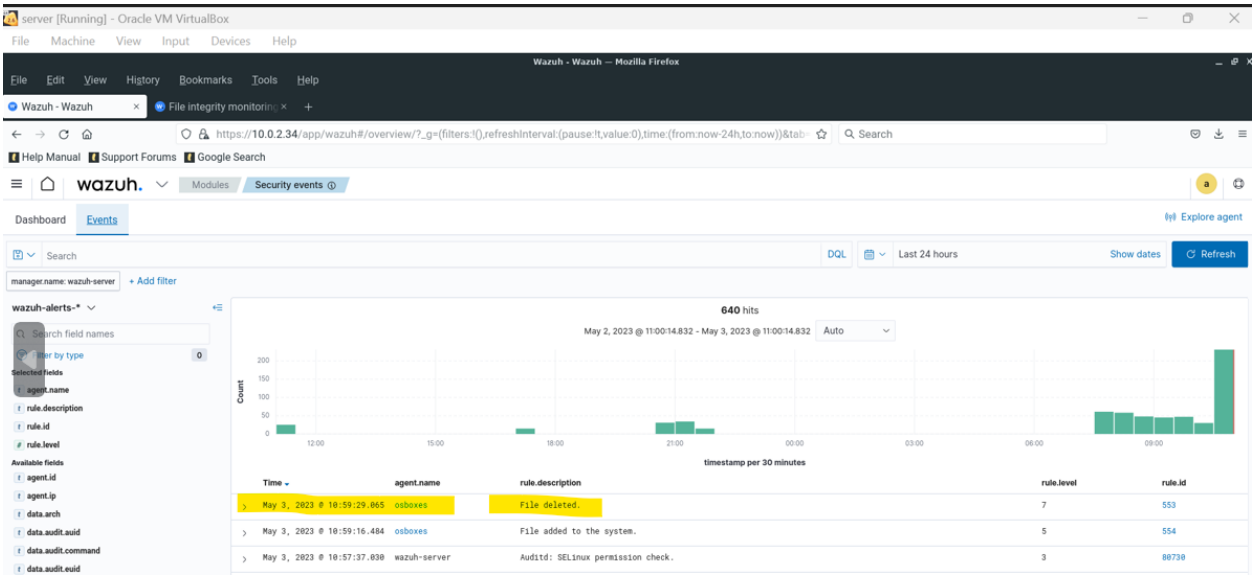
Visualize the alerts

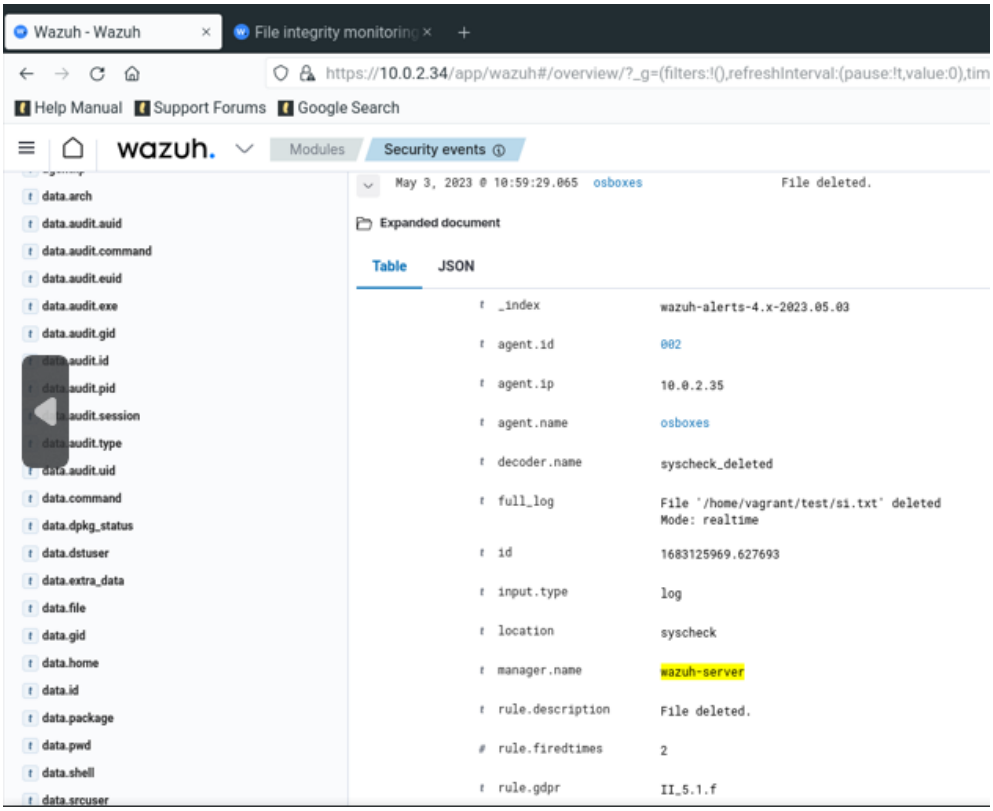
You can visualize the alert data in the Wazuh dashboard. To do this, go to the Security events module and add the filters in the search bar to query the alerts:

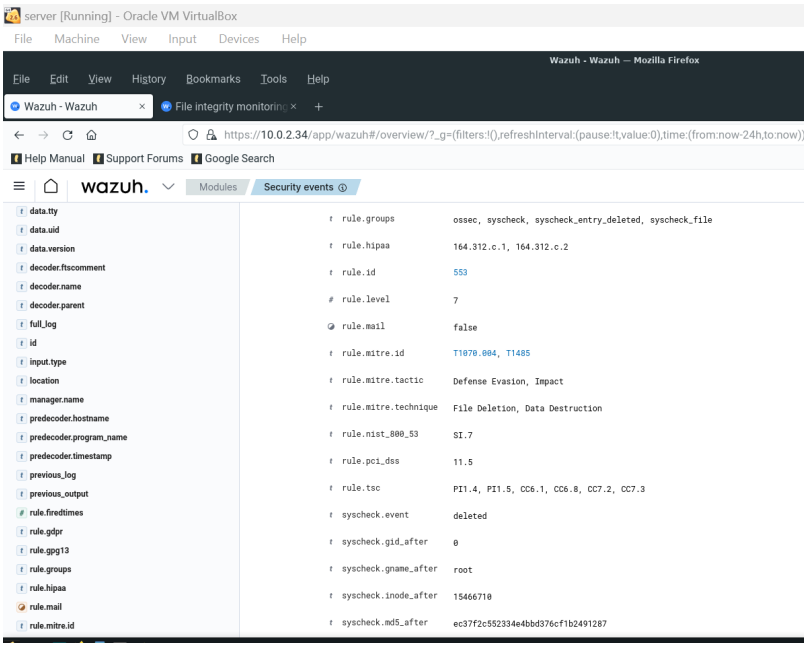
Ubuntu - `rule.id: is one of 550,553,554`

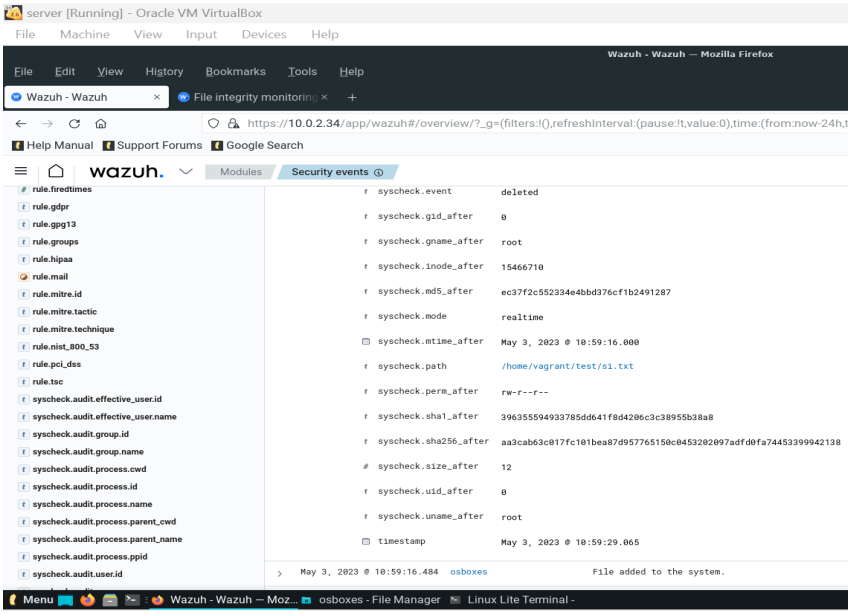



server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Open
ossec.co
/var/ossec/
</sca>
<!-- File integrity monitoring -->
<syscheck>
<disabled>no</disabled>
<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>
<scan_on_start>yes</scan_on_start>
<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/home/vagrant/test</directories>
<directories>/root</directories>
<directories>/bin,/sbin,/boot</directories>
<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random.seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/wtmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>
<!-- File types to ignore -->
<ignore type="sregex">.log$|.swp$</ignore>
<!-- Check the file, but never compute the diff -->
<nodiff>/etc/ssl/private.key</nodiff>
<skip_nfs>yes</skip_nfs>
<skip_dev>yes</skip_dev>
<skip_proc>yes</skip_proc>
<skip_sys>yes</skip_sys>
<!-- Nice value for Syscheck process -->
<process priority>10</process priority>


server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
File integrity monitoring
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&tab
Search
Help Manual
Support Forums
Google Search
wazuh.
Modules
Security events
Dashboard
Events
Explore agent
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
agent.name
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
data.arch
data.audit.auid
data.audit.command
data.audit.euid
640 hits
May 2, 2023 @ 11:00:14.832 - May 3, 2023 @ 11:00:14.832
Auto
Count
timestamp per 30 minutes
Time
agent.name
rule.description
rule.level
rule.id
May 3, 2023 @ 10:59:29.065
osboxes
File deleted.
7
553
May 3, 2023 @ 10:59:16.484
osboxes
File added to the system.
5
554
May 3, 2023 @ 10:57:37.030
wazuh-server
Auditd: SELinux permission check.
3
80730


Wazuh - Wazuh
File integrity monitoring
https://10.0.2.34/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),tim
Help Manual
Support Forums
Google Search
wazuh.
Modules
Security events
data.arch
data.audit.auid
data.audit.command
data.audit.euid
data.audit.exe
data.audit.gid
data.audit.id
data.audit.pid
data.audit.session
data.audit.type
data.audit.uid
data.command
data.dpkg_status
data.dstuser
data.extra_data
data.file
data.gid
data.home
data.id
data.package
data.pwd
data.shell
data.srcuser
May 3, 2023 @ 10:59:29.065
osboxes
File deleted.
Expanded document
Table
JSON
_index
wazuh-alerts-4.x-2023.05.03
agent.id
002
agent.ip
10.0.2.35
agent.name
osboxes
decoder.name
syscheck_deleted
full_log
File '/home/vagrant/test/si.txt' deleted
Mode: realtime
id
1683125969.627693
input.type
log
location
syscheck
manager.name
wazuh-server
rule.description
File deleted.
rule.firedtimes
2
rule.gdpr
II_5.1.f





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