

# S9 – L3 EXTRA

## Installazione e primo utilizzo di Wazuh (SIEM/XDR) in ambiente di laboratorio

---

### Introduzione

In questo esercizio ho configurato un sistema SIEM/XDR basato su **Wazuh** all'interno di un ambiente di laboratorio controllato.

**L'obiettivo è stato installare la Wazuh Virtual Machine (OVA), collegarla alla rete del laboratorio, installare e configurare il Wazuh Agent su una macchina Kali Linux e verificare la corretta raccolta delle prime informazioni di sicurezza, in linea con i concetti di monitoraggio, logging centralizzato e incident response.**

---

### Prerequisiti e sicurezza

Prima di iniziare:

- Avvio esclusivamente macchine virtuali di laboratorio
  - Utilizzo una rete isolata (Host-Only)
  - Evito qualunque attività su sistemi reali
- 

### 1) Configurazione di rete VM Kali e Wazuh

1. Imposto la scheda di rete della VM **Wazuh** utilizzando lo stesso tipo di rete della VM **Kali Linux** (Host-Only).
2. Avvio entrambe le macchine virtuali.
3. Su **Kali Linux** verifico l'indirizzo IP con:

**ip a**

4. Sulla **Wazuh VM** individuo l'indirizzo IP mostrato a console dopo il login effettuato.
5. Da Kali verifico la raggiungibilità della Wazuh VM:

**ping 192.168.56.106 (IP\_WAZUH)**

```
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
            inetc6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b7:d3:1c brd ff:ff:ff:ff:ff:ff
    altname eno0s12
        inet 192.168.56.106/24 metric 1024 brd 192.168.56.255 scope global dynamic eth0
            valid_lft 368sec preferred_lft 368sec
            inetc6 fe80::a00:27ff:feb7:d31c/64 scope link proto kernel_11
                valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

- Output IP Wazuh: **192.168.56.106** dopo il comando **ip a**
  - Accesso con user **wazuh-user** e password **wazuh**

```
(kali㉿kali)-[~]
$ 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 noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
            valid_lft 379sec preferred_lft 379sec
        inet6 fe80::863d:5aa:c049:f864/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=127 time=1.61 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=127 time=5.04 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=127 time=0.703 ms
^C
--- 192.168.56.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.703/2.450/5.039/1.867 ms
```

La comunicazione tra le due macchine risulta corretta.

## 2) Accesso alla dashboard Wazuh

1. Apro il browser su **Kali Linux**.
2. Accedo alla dashboard Wazuh tramite browser utilizzando l'indirizzo:  
**https://192.168.56.106 (IP WAZUH)**



3. Effettuo il login utilizzando le **credenziali fornite dalla documentazione ufficiale della Wazuh OVA**.
4. Verifico il corretto accesso alla dashboard principale di Wazuh
5. Username: **admin** e Password: **admin**

The screenshot shows the Wazuh dashboard with the URL `192.168.56.106/app/wz-home#/overview/?_g=(filters:!)()` in the browser bar. The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. On the left, there's a sidebar with a 'W.' icon and an 'Overview' tab. The main content area has two sections: 'AGENTS SUMMARY' and 'LAST 24 HOURS A...'. The 'AGENTS SUMMARY' section states 'This instance has no agents registered. Please deploy agents to begin monitoring your endpoints.' It features a blue button labeled '+ Deploy new agent'. The 'LAST 24 HOURS A...' section shows statistics for 'Critical severity' (0), 'High severity' (0), and 'Medium severity' (0). Each severity level is accompanied by a large red number and a descriptive rule level range.

Output dopo il login effettuato con user e password admin

---

### 3) Installazione del Wazuh Agent su Kali Linux

1. Seguo la guida ufficiale per l'installazione dell'agent Wazuh su sistemi Linux tramite **APT e systemd**.
2. Aggiorno i repository e installo l'agent:

```
sudo apt update
sudo apt install wazuh-agent
```

```
(kali㉿kali)-[~]
$ sudo apt update

Get:1 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:2 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [50.0 kB]
Get:3 https://packages.wazuh.com/4.x/apt stable/main amd64 Contents (deb) [2,029 kB]
Hit:4 http://http.kali.org/kali kali-rolling InRelease
Fetched 2,096 kB in 24s (86.1 kB/s)
1564 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
(kali㉿kali)-[~]
$ sudo apt install wazuh-agent

Installing:
  wazuh-agent

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1564
  Download size: 13.1 MB
  Space needed: 48.5 MB / 62.9 GB available

Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.14.2-1 [13.1 MB]
Fetched 13.1 MB in 2s (6,896 kB/s)
Preconfiguring packages ...
Selecting previously unselected package wazuh-agent.
(Reading database ... 422160 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.14.2-1_amd64.deb ...
Unpacking wazuh-agent (4.14.2-1) ...
Setting up wazuh-agent (4.14.2-1) ...

(kali㉿kali)-[~]
$ systemctl status wazuh-agent

● wazuh-agent.service - Wazuh agent
    Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; disabled; preset: disabled)
      Active: inactive (dead)
```

3. Verifico la presenza del servizio:

```
systemctl status wazuh-agent
```

Il Wazuh Agent è stato installato correttamente sulla macchina Kali Linux. Subito dopo l'installazione, **il servizio risulta inattivo, come previsto, in attesa della configurazione del collegamento al manager e della registrazione dell'agent.**

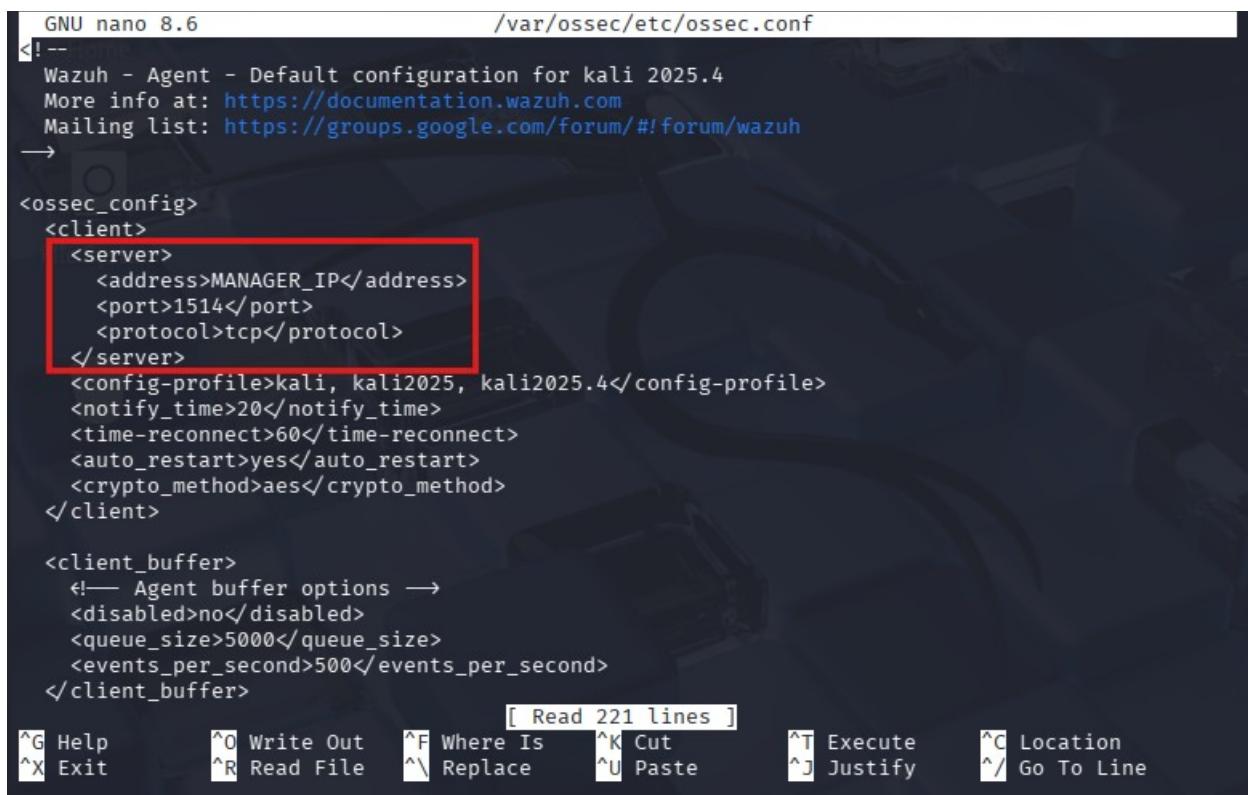
---

## 4) Configurazione dell'agent (collegamento al manager)

1. Modifico il file di configurazione dell'agent:

```
sudo nano /var/ossec/etc/ossec.conf
```

2. Inserisco l'indirizzo IP della **Wazuh VM** come manager.



```
GNU nano 8.6                               /var/ossec/etc/ossec.conf
<!--
Wazuh - Agent - Default configuration for kali 2025.4
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>MANAGER_IP</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>kali, kali2025, kali2025.4</config-profile>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>
[ Read 221 lines ]
^G Help          ^O Write Out    ^F Where Is    ^K Cut          ^T Execute      ^C Location
^X Exit          ^R Read File    ^\ Replace     ^U Paste        ^J Justify      ^/ Go To Line
```

```
GNU nano 8.6                               /var/ossec/etc/ossec.conf *
←→
Wazuh - Agent - Default configuration for kali 2025.4
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#forum/wazuh
→

<ossec_config>
  <client>
    <server>
      <address>192.168.56.106</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>kali, kali2025, kali2025.4</config-profile>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    ←→ Agent buffer options →
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

^G Help          ^O Write Out   ^F Where Is     ^K Cut          ^T Execute      ^C Location
^X Exit          ^R Read File   ^\ Replace      ^U Paste         ^J Justify      ^/ Go To Line
```

3. Salvo la configurazione ed esco (**Ctrl + O** poi **Invio** poi **Ctrl + X**)

## 5) Enrollment e avvio del Wazuh Agent

1. Procedo con la registrazione (enrollment) dell'agent seguendo la procedura prevista per endpoint Linux.
2. Avvio e abilito il servizio:

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

```
(kali㉿kali)-[~]
$ sudo systemctl enable wazuh-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-agent.service' → '/usr/lib/systemd/system/wazuh-agent.service'.

(kali㉿kali)-[~]
$ sudo systemctl restart wazuh-agent

(kali㉿kali)-[~]
$
```

3. Verifico che l'agent sia correttamente in esecuzione:

```
systemctl status wazuh-agent
```

```
(kali㉿kali)-[~]
$ systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: disabled)
   Active: active (running) since Wed 2026-02-04 16:19:22 EST; 1min 47s ago
     Invocation: 42a76be58aa84121a44068dea06498ed
      Process: 16859 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, sta>
     Process: 18872 ExecReload=/usr/bin/env /var/ossec/bin/wazuh-control reload (code=exited, s>
     Tasks: 34 (limit: 2115)
    Memory: 442.9M (peak: 519.1M)
      CPU: 52.800s
     CGroup: /system.slice/wazuh-agent.service
             ├─16889 /var/ossec/bin/wazuh-agentd
             ├─18951 /var/ossec/bin/wazuh-execd
             ├─18972 /var/ossec/bin/wazuh-syscheckd
             ├─18990 /var/ossec/bin/wazuh-logcollector
             └─18997 /var/ossec/bin/wazuh-modulesd

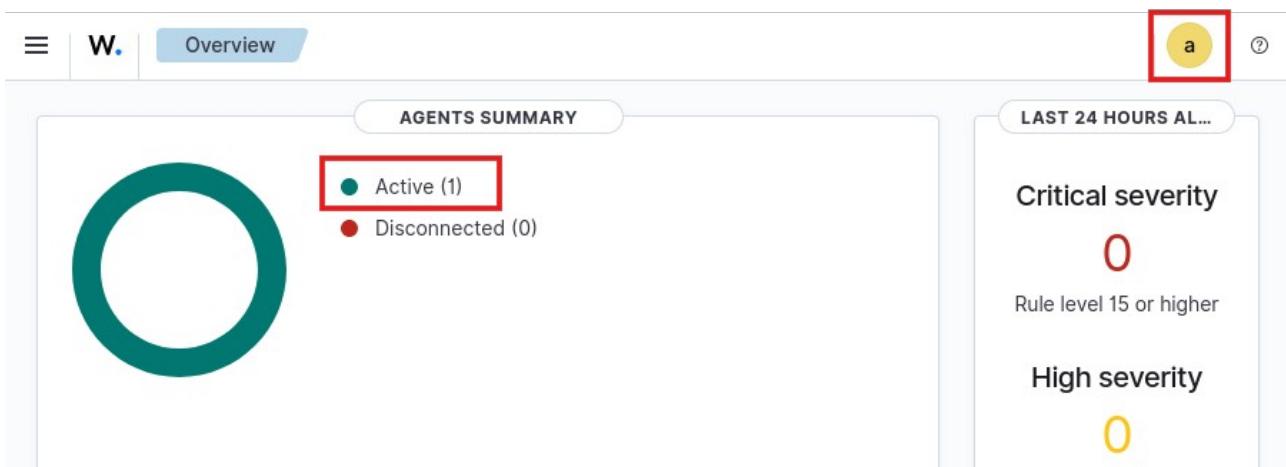
Feb 04 16:19:38 kali env[18872]: Killing wazuh-execd ...
Feb 04 16:19:39 kali env[18872]: Wazuh v4.14.2 Stopped
Feb 04 16:19:40 kali env[18872]: Starting Wazuh v4.14.2 ...
Feb 04 16:19:41 kali env[18872]: Started wazuh-execd ...
Feb 04 16:19:41 kali env[18872]: wazuh-agentd already running ...
Feb 04 16:19:41 kali env[18872]: Started wazuh-syscheckd ...
Feb 04 16:19:41 kali env[18872]: Started wazuh-logcollector ...
Feb 04 16:19:42 kali env[18872]: Started wazuh-modulesd ...
Feb 04 16:19:44 kali env[18872]: Completed.
Feb 04 16:19:44 kali systemd[1]: Reloaded wazuh-agent.service - Wazuh agent.
lines 1-26/26 (END)
```

**Output dell'agent correttamente in esecuzione**

---

## 6) Verifica dell'agent nella dashboard Wazuh

1. Accedo nuovamente alla dashboard Wazuh (User e Password admin)
2. Apro la sezione **Agents**.
3. Verifico che l'agent installato su Kali Linux risulti:
  - Presente
  - Attivo (status *Active*)
  - Con informazioni coerenti su sistema operativo e indirizzo IP



The screenshot shows the Wazuh Endpoints page. At the top, it says 'Agents (1)'. Below is a table with the following data:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kali	192.168.56.107	default	Kali GNU/Linux 2025.4	node01	v4.14.2	<span style="color: green;">●</span>	<span style="color: blue;"> ⓘ</span> <span style="color: grey;">⟳</span> <span style="color: orange;">...</span>

Below the table, it says 'Rows per page: 10' and has navigation arrows. The 'IP address' and 'Operating system' columns are highlighted with red boxes.

## 7) Analisi delle prime informazioni raccolte

1. Osservo le informazioni iniziali fornite da Wazuh:

- Stato dell'agent
- Dati di inventario del sistema
- Eventi di base e log di sistema

2. Genero attività lecite su Kali Linux (aggiornamento pacchetti, creazione di file) per stimolare la raccolta di eventi:

```
sudo apt update
echo "test wazuh" | sudo tee /tmp/wazuh_test.txt
```

```
(kali㉿kali)-[~]
$ sudo apt update
Hit:1 https://packages.wazuh.com/4.x/apt stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
1564 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ echo "test wazuh" | sudo tee /tmp/wazuh_test.txt
test wazuh

(kali㉿kali)-[~]
$
```

3. Verifico nella dashboard Wazuh la comparsa dei primi eventi associati all'agent Kali.

Come previsto, la quantità di informazioni iniziali è limitata e richiederebbe configurazioni avanzate aggiuntive non richieste dall'esercizio.

---

## Conclusioni

In questo esercizio ho installato e configurato correttamente un sistema **Wazuh SIEM/XDR** in ambiente di laboratorio.

Ho collegato una macchina **Kali Linux** come endpoint monitorato tramite Wazuh Agent, verificandone lo stato attivo e la corretta comunicazione con il manager.

L'attività ha permesso di comprendere il funzionamento di base di una soluzione SIEM/XDR, il ruolo degli agent e l'importanza della raccolta centralizzata dei log e degli eventi di sicurezza, in linea con i concetti di monitoraggio e incident response affrontati.