

## Extra S9L3

### Traccia:

Installare Wazuh (SIEM/XDR) in versione OVA nella rete laboratorio e il suo agent su Kali.

Collegare l'agent a Wazuh e interpretare le informazioni raccolte (appena avviato le informazioni saranno poche e Wazuh necessita di ulteriori configurazioni di cui non ci occuperemo).

Wazuh OVA (impostare correttamente la rete in modo che Wazuh e Kali siano nella stessa rete):

<https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html>

Wazuh agent (seguire APT e Systemd):

<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html>

Enrollment dell'agent suggerito:

<https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/enrollment-methods/via-agent-configuration/linux-endpoint.html>

La traccia chiedeva di installare, creare un agente e analizzare i risultati di Wazuh.

Wazuh è una piattaforma gratuita e open-source che aiuta a proteggere i sistemi informatici. La sua funzione principale è il **monitoraggio della sicurezza** e la **rilevazione delle minacce**.

Possiamo considerare Wazuh come un sistema di allarme intelligente per la rete e i computer. Questo tool è composto da tre elementi principali:

- **Agente:** un piccolo programma che installi su ogni computer o server che vuoi proteggere (Windows, Linux, macOS). L'agente raccoglie dati e informazioni sulla sicurezza del sistema.
- **Server:** l'unità centrale che riceve le informazioni dagli agenti. Analizza i dati per identificare eventuali minacce o attività sospette.
- **Interfaccia web:** una dashboard facile da usare che ti permette di visualizzare tutti gli allarmi, gestire le configurazioni e consultare i report.

Wazuh offre diverse funzionalità: **Rilevamento delle intrusioni (HIDS/NIDS), monitoraggio dell'integrità dei file, analisi dei log, valutazione delle vulnerabilità e risposta agli incidenti**

In sintesi, Wazuh è uno strumento potente che fornisce una visibilità completa sulla sicurezza dell'infrastruttura IT, aiutando a proteggere i dati e a rispondere in modo efficace alle minacce informatiche.

## Installazione dell'agente Wazuh

Il primo **Comando** utilizzato serve per scaricare e installare il pacchetto dell'agente Wazuh

```
curl -so | sudo WAZUH_MANAGER='10.0.2.4' dpkg -i ./wazuh-agent.deb
```

### Significato:

`curl -so https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb`: Questo segmento del comando **scarica** il pacchetto dell'agente Wazuh (.deb) dal repository ufficiale.

**WAZUH\_MANAGER='10.0.2.4'**: Questa parte è cruciale, imposta la variabile d'ambiente che specifica l'indirizzo IP del server Wazuh Manager a cui l'agente dovrà connettersi. Nel nostro caso, l'indirizzo IP è **10.0.2.4**.

**dpkg -i ./wazuh-agent.deb**: Questo comando **installa** il pacchetto scaricato.

## Risultato:

L'output del terminale mostra che il pacchetto è stato scaricato correttamente e l'installazione è andata a buon fine

Dopo aver installato il servizio, è necessario informare il sistema operativo delle nuove configurazioni.

## Comando: `sudo systemctl daemon-reload`

**Significato:** Questo comando **ricarica** il gestore di sistema **systemd**. In questo modo, il sistema riconosce immediatamente il nuovo servizio wazuh-agent e il suo file di configurazione.

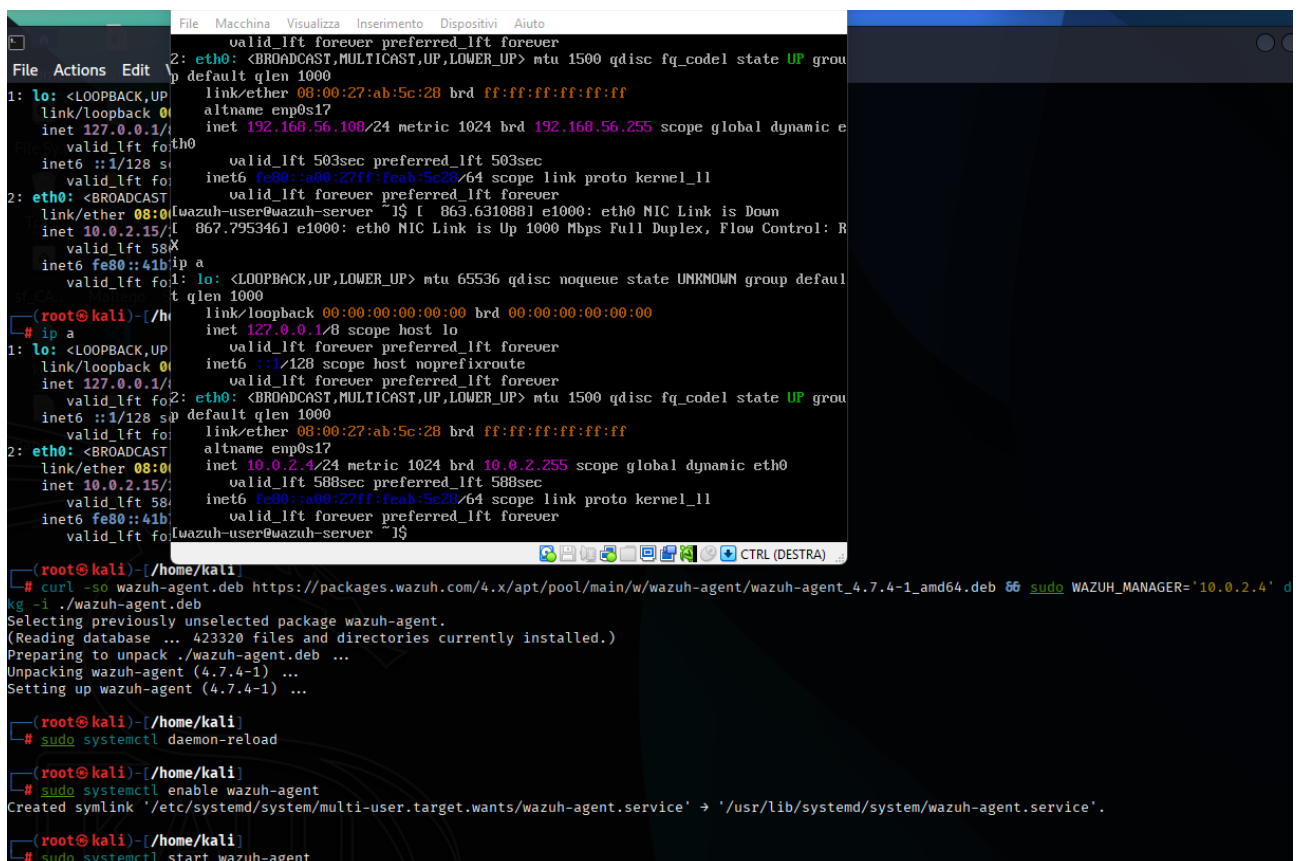
**Risultato:** Il sistema crea un link simbolico (symlink) per il servizio Wazuh, rendendolo disponibile per la gestione da parte di systemd.

Infine, hai avviato il servizio dell'agente Wazuh per farlo entrare in funzione.

## Comando: `sudo systemctl start wazuh-agent` (*per sicurezza fare anche un restart*)

**Significato:** Questo comando **avvia** il servizio dell'agente Wazuh. Da questo momento, l'agente inizia a comunicare con il server Wazuh Manager (con indirizzo **10.0.2.4**) per inviare dati di sicurezza e ricevere istruzioni.

**Risultato:** Il servizio viene avviato senza messaggi di errore, indicando che l'agente è ora attivo e funzionante.



```
(root@kali)~# ip a
1: lo: <LOOPBACK,UP> state UNKNOWN mtu 65536 qdisc noqueue 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> state UP mtu 1500 qdisc fq_codel group default qlen 1000
    link/ether 08:00:27:ab:5c:28 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 1024 brd 10.0.2.255 scope global dynamic eth0
        valid_lft 588sec preferred_lft 588sec
    inet6 fe80::a00:27ff:feab:5c28/64 scope link proto kernel lladdr fe80::a00:27ff:feab:5c28
    wazuh-agent@wazuh-server ~$

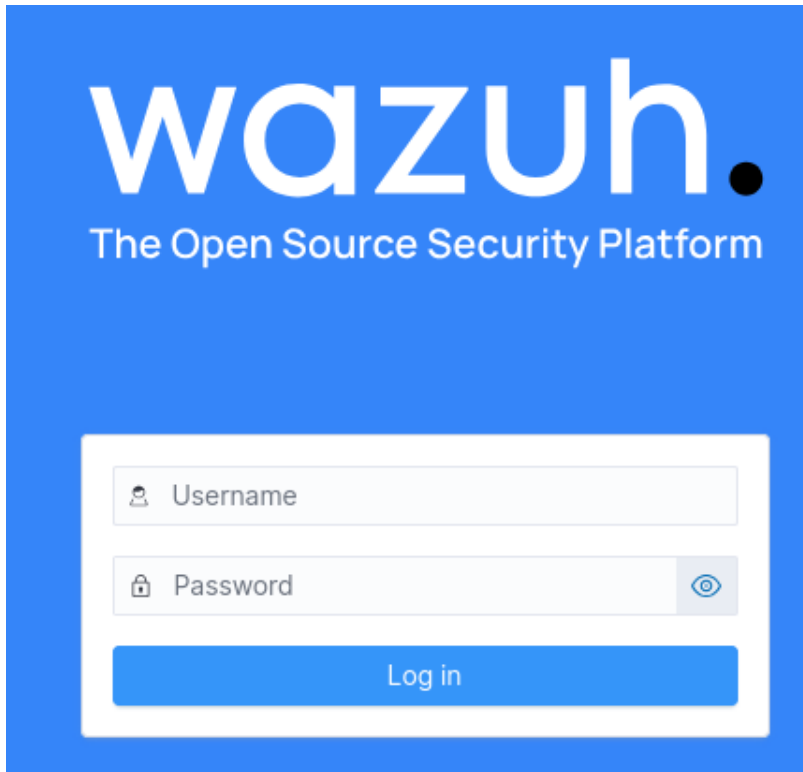
(root@kali)~# curl -sO wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb
Selecting previously unselected package wazuh-agent.
(Reading database ... 423320 files and directories currently installed.)
Preparing to unpack ./wazuh-agent.deb ...
Unpacking wazuh-agent (4.7.4-1) ...
Setting up wazuh-agent (4.7.4-1) ...

(root@kali)~# sudo systemctl daemon-reload
(root@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'.

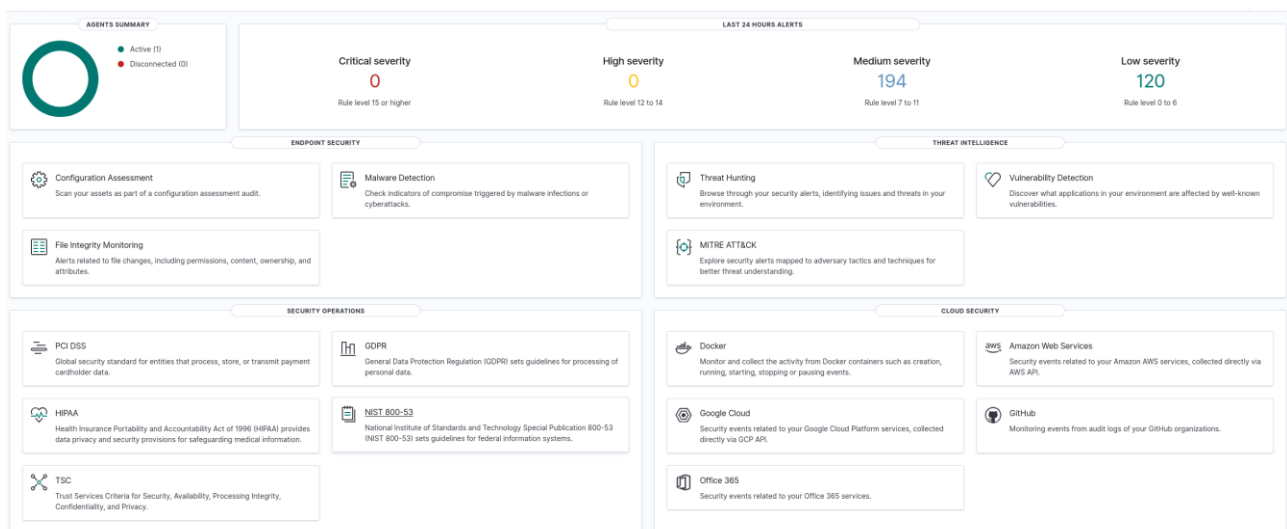
(root@kali)~# sudo systemctl start wazuh-agent
```

Adesso che l'agente è configurato e invia i dati, per visualizzare e gestire questi dati bisogna accedere alla Wazuh Dashboard tramite browser. **(Si può accedere da qualsiasi pc all'interno della sottorete)**

Per accedere basta inserire nell'URL l'indirizzo IP del server Wazuh Dashboard, nel nostro caso <https://10.0.2.4>. La schermata che troveremo sarà questa:



Una volta inseriti i dati per il login ci troveremo nella "home" di Wazuh. Ogni tab rappresenta una funzionalità o lo stato di sicurezza



## Sicurezza dell'Endpoint (ENDPOINT SECURITY)

Questa tab si concentra sulla protezione dei singoli sistemi (gli "endpoint") dov'è installato l'agente.

- **Configuration Assessment:** Questa funzionalità scansiona i sistemi per rilevare errori di configurazione, impostazioni deboli o vulnerabilità che potrebbero essere sfruttate. Aiuta a mantenere i sistemi conformi alle "best practice" di sicurezza.
- **Malware Detection:** Analizza i file e i processi in esecuzione sui sistemi per identificare la presenza di software dannosi (malware) o attività sospette.
- **File Integrity Monitoring:** Controlla e registra ogni modifica, cancellazione o creazione di file importanti sui sistemi. Se un file critico viene alterato (ad esempio, un file di sistema), Wazuh genera un allarme.

## Informazioni sulle Minacce (THREAT INTELLIGENCE)

Questa sezione aiuta a capire e a contrastare le minacce in modo più proattivo.

- **Threat Hunting:** Permette di cercare attivamente minacce nascoste o indicatori di compromissione che potrebbero non essere stati rilevati dai sistemi di sicurezza automatici.
- **MITRE ATT&CK:** Mette in relazione gli allarmi di sicurezza con la matrice MITRE ATT&CK, un framework che descrive le tattiche e le tecniche degli attaccanti. Questo aiuta a comprendere il "come" e il "perché" di un attacco.
- **Vulnerability Detection:** Scansiona tutti i software installati sui tuoi sistemi e li confronta con un database di vulnerabilità note (CVE). Questo aiuta a identificare quali applicazioni necessitano di aggiornamenti (patching) per non essere a rischio.

## Conformità e Operazioni di Sicurezza (SECURITY OPERATIONS)

Questa sezione è fondamentale per le aziende che devono rispettare standard di sicurezza specifici.

- **PCI DSS, GDPR, HIPAA, NIST 800-53, TSC:** Questi riquadri non sono funzionalità a sé stanti, ma rappresentano dashboard e report preconfigurati che aiutano a monitorare e dimostrare la conformità ai rispettivi standard di sicurezza. Ad esempio, il riquadro **GDPR** mostrerà eventi rilevanti per la protezione dei dati personali.

## Sicurezza Cloud (CLOUD SECURITY)

Mostra la capacità di Wazuh di estendere il monitoraggio a piattaforme e servizi cloud, integrandosi con le API di questi fornitori.

- **Docker:** Monitora le attività all'interno dei container Docker.
- **Amazon Web Services, Google Cloud, Office 365, GitHub:** Questi riquadri indicano che Wazuh può raccogliere e analizzare i log e gli eventi di sicurezza da questi servizi, fornendo visibilità sulla sicurezza della tua infrastruttura cloud.