🛠️ Cybersecurity Lab: Day 2 — Setting Up Wazuh Agent on Red Hat Server

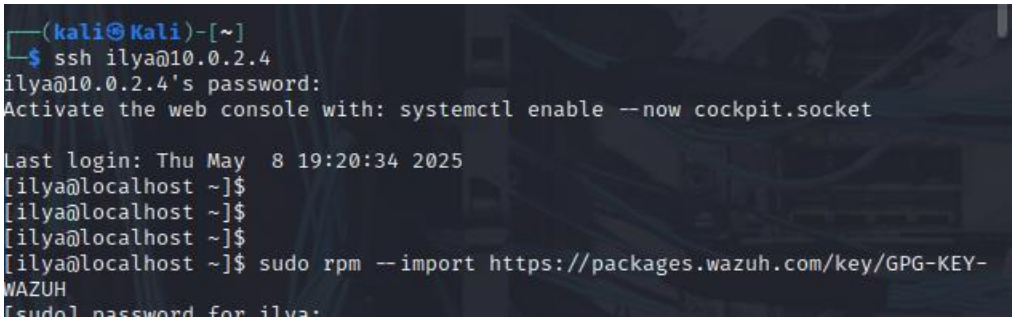
✅ Objectives Completed:

1. **Prepared Red Hat Server for Wazuh Agent**
    - Verified internet connection.
    - Confirmed basic server readiness (Apache and SSH running).

    Chose to install wazuh agent on redhat remotely using ssh

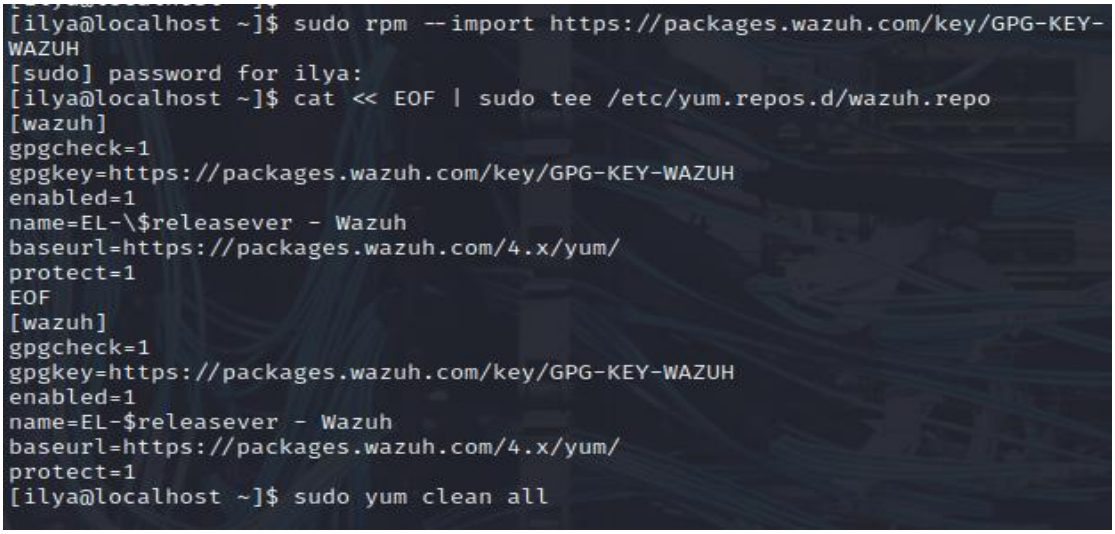
2. **Added Wazuh Repository on Red Hat Server**
    - Logged into the Red Hat server via SSH from the Kali machine.

      Ssh username@<ip>



    - **Added the Wazuh repository to the Red Hat server:**

      sudo rpm --import https://packages.wazuh.com/key/GPG-KEY-



3. **Installed Wazuh Agent on Red Hat Server Remotely via SSH**

sudo yum install wazuh-agent -y

```
Metadata cache created.
[ilya@localhost ~]$ sudo yum install wazuh-agent -y
Updating Subscription Management repositories.
Last metadata expiration check: 0:01:25 ago on Thu 08 May 2025 08:00:59 PM EDT.
Dependencies resolved.
================================================================================
 Package             Architecture    Version          Repository      Size
================================================================================
Installing:
 wazuh-agent         x86_64          4.12.0-1         wazuh          9.6 M

Transaction Summary
================================================================================
Install  1 Package
```

4. **Configured Agent to Connect to Wazuh Server**

- Edited the ossec.conf file on the Red Hat server:

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

- Set the Wazuh manager IP (10.0.2.6): edit this part only

  <server>

  <address>10.0.2.6</address>

  <protocol>tcp</protocol>

  </server>

5. **Started Wazuh Agent and Verified Status**

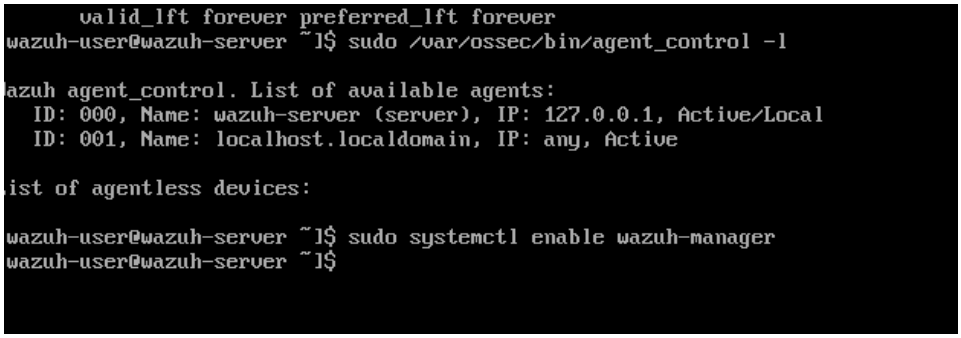
- Started and enabled the agent service on the Red Hat server:

```
[ilya@localhost ~]$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; disabled; >
     Active: active (running) since Thu 2025-05-08 20:10:52 EDT; 13s ago
    Process: 10418 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start>
      Tasks: 28 (limit: 23006)
     Memory: 49.2M
        CPU: 8.123s
     CGroup: /system.slice/wazuh-agent.service
             ├─10446 /var/ossec/bin/wazuh-execd
             ├─10458 /var/ossec/bin/wazuh-agentd
             ├─10472 /var/ossec/bin/wazuh-syscheckd
             ├─10486 /var/ossec/bin/wazuh-logcollector
             └─10504 /var/ossec/bin/wazuh-modulesd

May 08 20:10:43 localhost.localdomain systemd[1]: Starting Wazuh agent ...
May 08 20:10:43 localhost.localdomain env[10418]: Starting Wazuh v4.12.0 ...
May 08 20:10:45 localhost.localdomain env[10418]: Started wazuh-execd ...
May 08 20:10:46 localhost.localdomain env[10418]: Started wazuh-agentd ...
```

6. **Verified Agent Connection from Wazuh Manager**

- From the Wazuh server, confirmed the agent connection:



Troubleshooting steps done: The Wazuh agent on the RedHat server was not connecting to the Wazuh Manager, and the following steps were done

1. Allow connection through the ports choosen

Outcome: Did not solve the problem but useful.

2. **Check the config files for correct ip address to server**
    - *sudo nano /var/ossec/etc/ossec.conf*

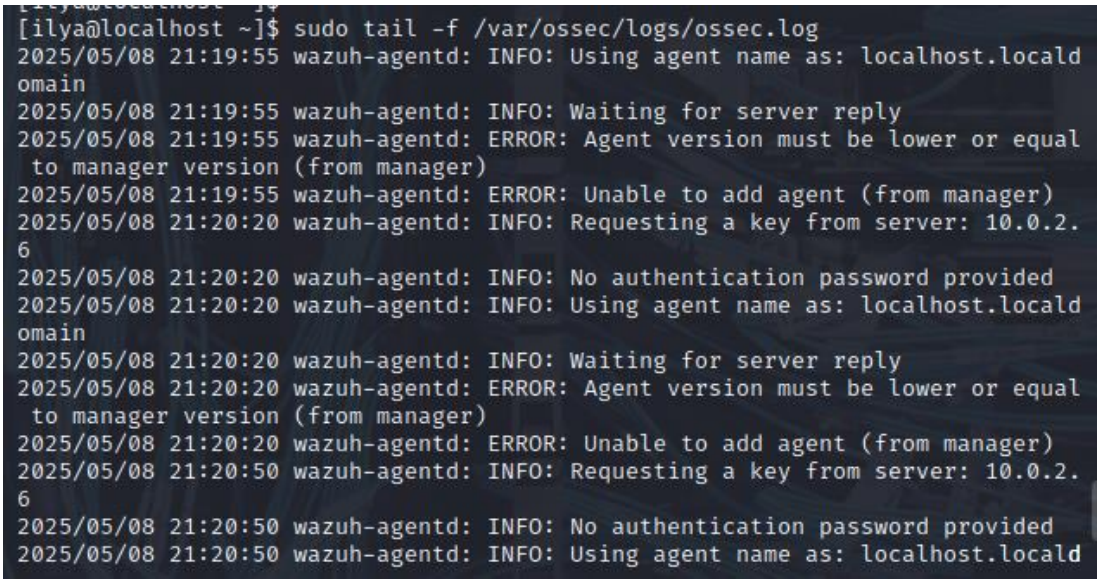
    finding :the ip address was correctly set

3. **checked the log files**

sudo tail -f /var.....

finding: an error the agent and server were of different verision

correction: re installed the current version of wazuh server



⚠️ Troubleshooting Summary Issue Fix Agent service failed to start Version mismatch error – upgraded Wazuh Manager Yum could not find package Used RPM manual installation Agent not listed in manager Use correct restarted services, and verified port connectivity

📝 Notes Ensure both agent and manager are running compatible Wazuh versions.

After configuration changes, always restart the services.

Use journalctl, ossec.log, and telnet for debugging.