Wazuh Server Installation

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Wazuh is an open-source security monitoring platform used for threat detection, integrity monitoring, and compliance. Installing Wazuh as an OVA (Open Virtual Appliance) provides a convenient way to set up the Wazuh environment within a virtualized environment. Here's a brief guide on how to install Wazuh as an OVA:

1. Download the OVA file: Begin by downloading the Wazuh OVA file from the official Wazuh website or repository. Ensure that you select the appropriate version of the OVA file compatible with your virtualization platform.

2. Import the OVA file: Open your virtualization platform (such as VMware, VirtualBox, or others) and import the downloaded OVA file. This process typically involves selecting "Import Appliance" or a similar option and choosing the OVA file from your local storage.

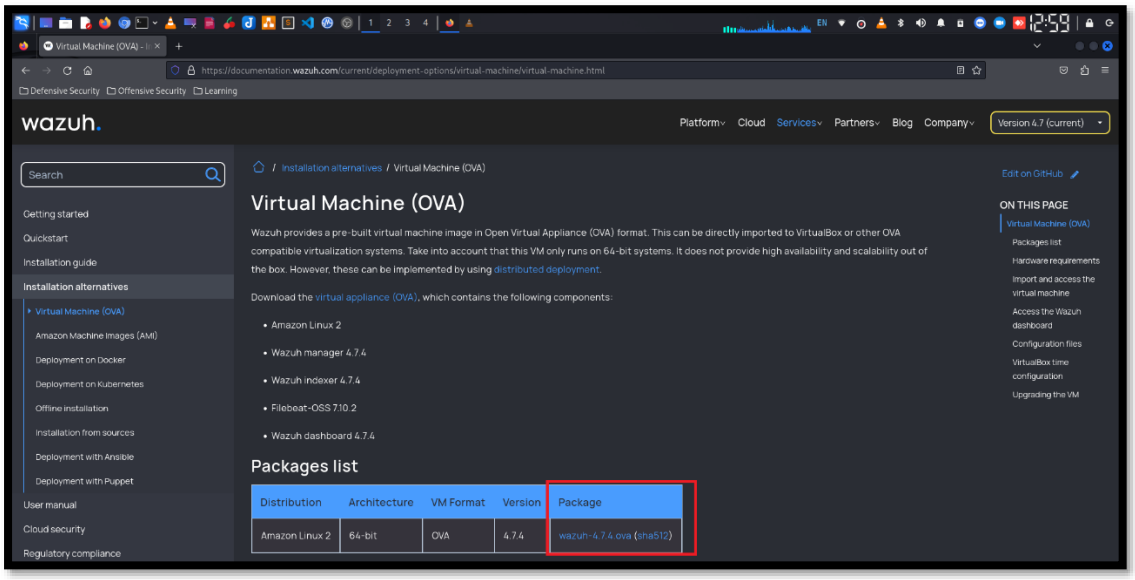
3. Configure virtual machine settings: After importing the OVA file, you may need to configure settings such as CPU, memory, network adapter, and disk size for the Wazuh virtual machine. Ensure that the settings meet the requirements specified by Wazuh for optimal performance.

4. Start the virtual machine: Once the settings are configured, start the virtual machine. The Wazuh virtual appliance will boot up, and you will be prompted to log in.

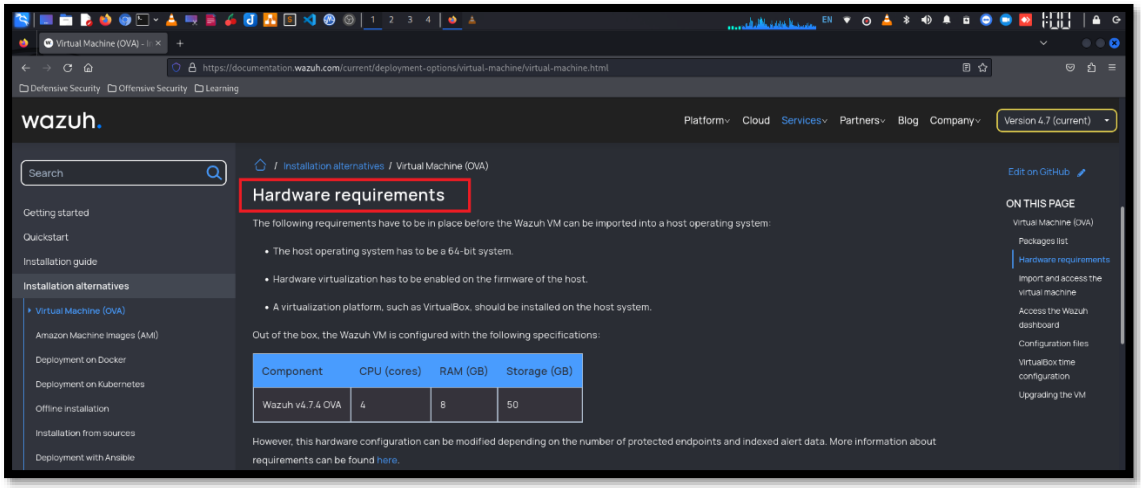
5. Access the Wazuh web interface: Once the setup is complete, you can access the Wazuh web interface using a web browser. Enter the IP address or hostname of the Wazuh virtual machine in the browser address bar to access the interface. From here, you can manage security alerts, view dashboards, and configure monitoring policies.

Step 01: Downloading Wazuh (OVA) file

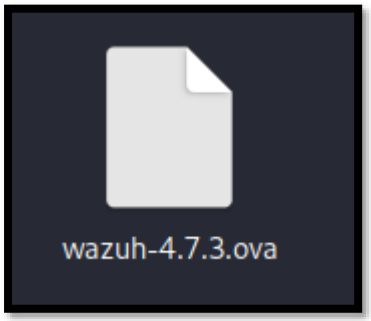
Link: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html



Read the hardware requirements for wazuh installation.

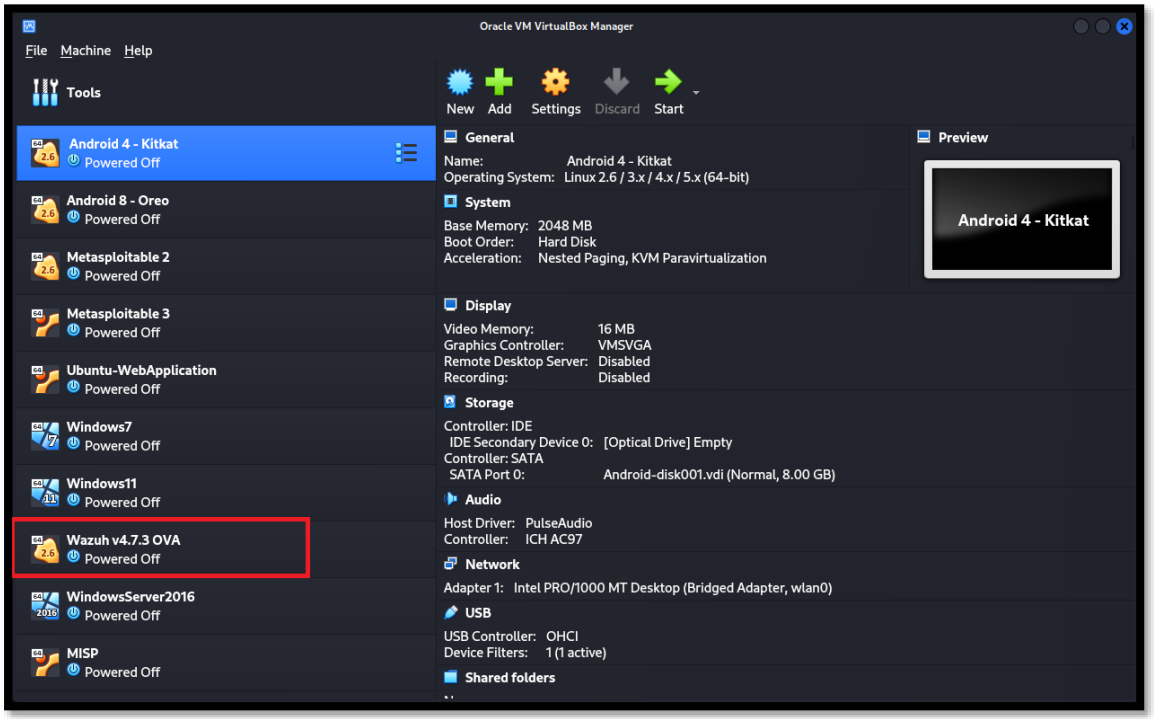


Here is downloaded Wazuh-4.7.3.ova file

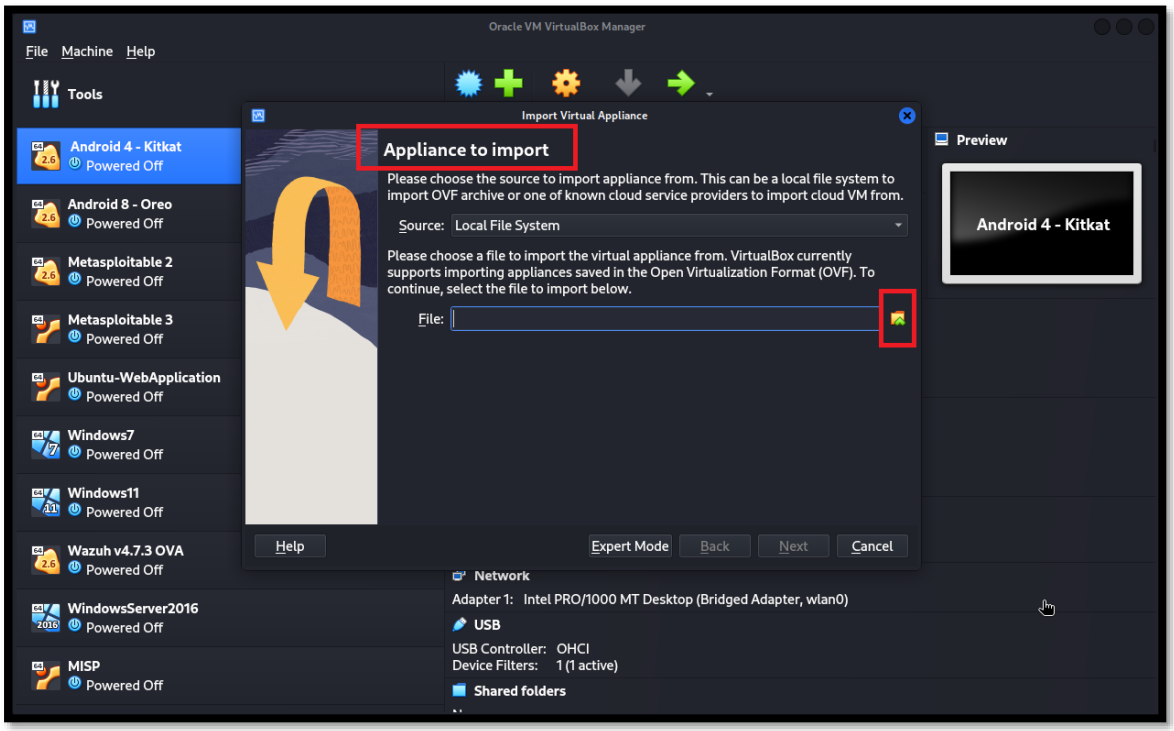


Step 02: Wazuh Installation on VirtualBox.

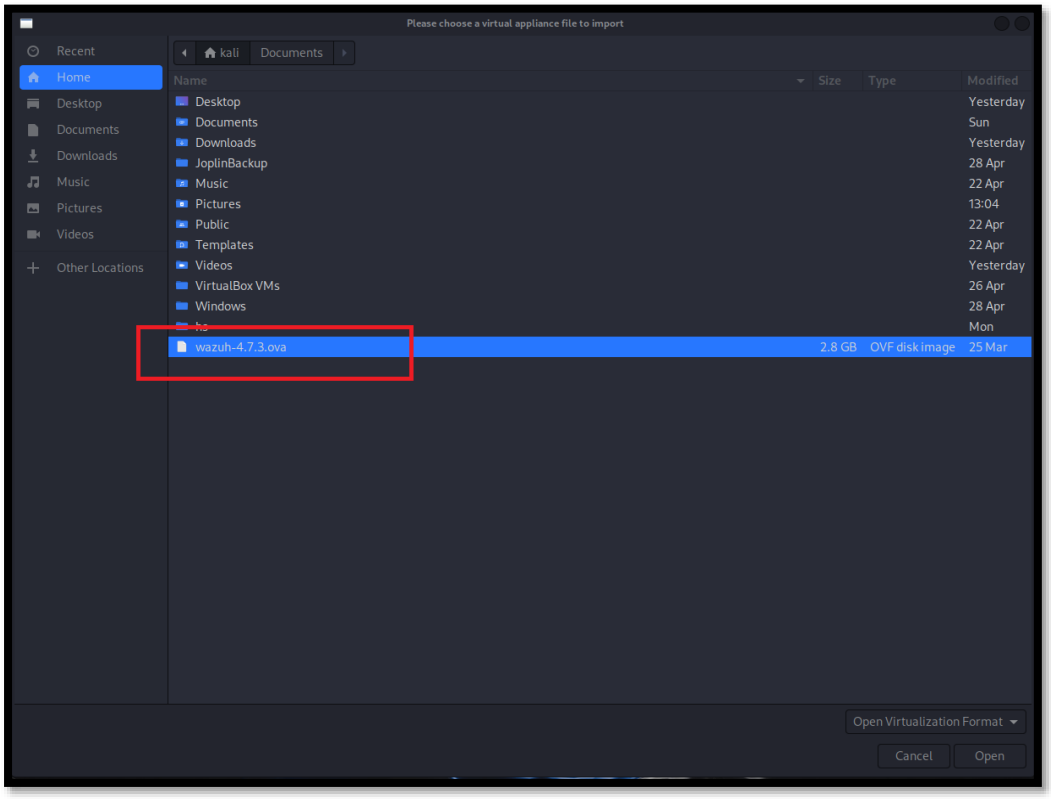
I already added Wazuh for my home lab but now again importing Wazuh.ova virtual machine in my VirtualBox as the name of Wazuh Server.



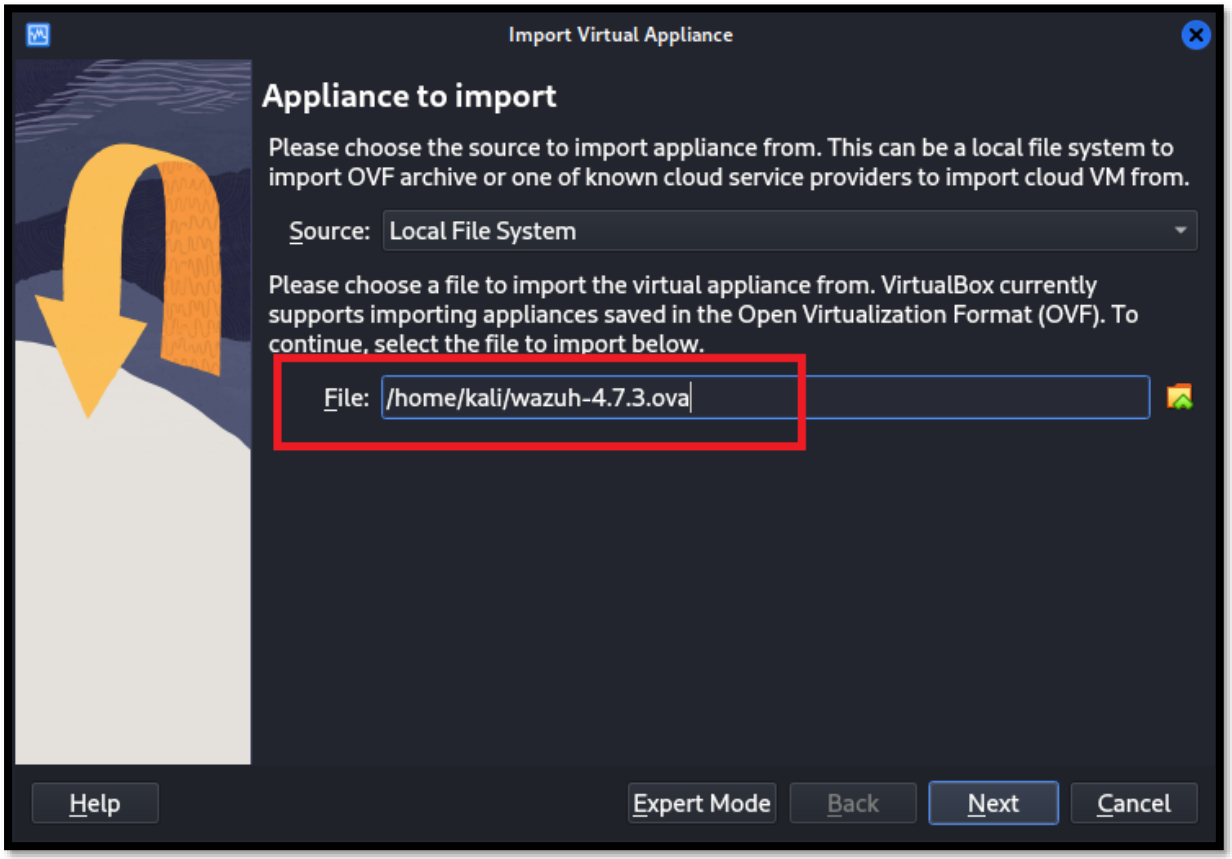
Go to File and select “Import Appliance...”.
Import Appliance Wizard is open now select the location where Wazuh-4.7.3.ova file is downloaded.



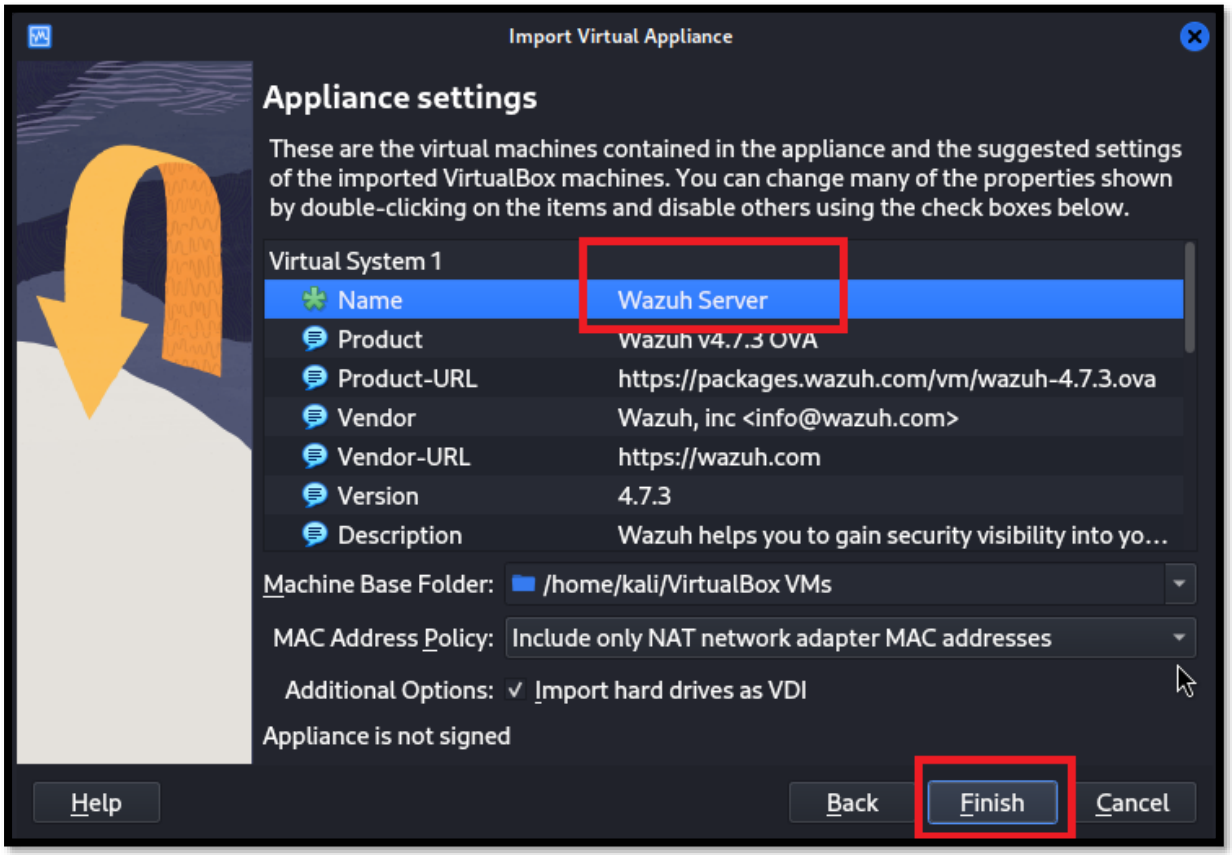
Select the Wazuh-4.7.3.ova file.



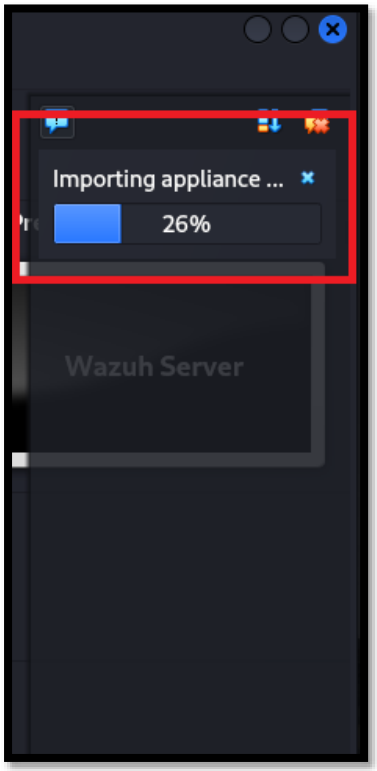
After selection click on next.



Change the Name what you want in my case I am using “Wazuh Server”

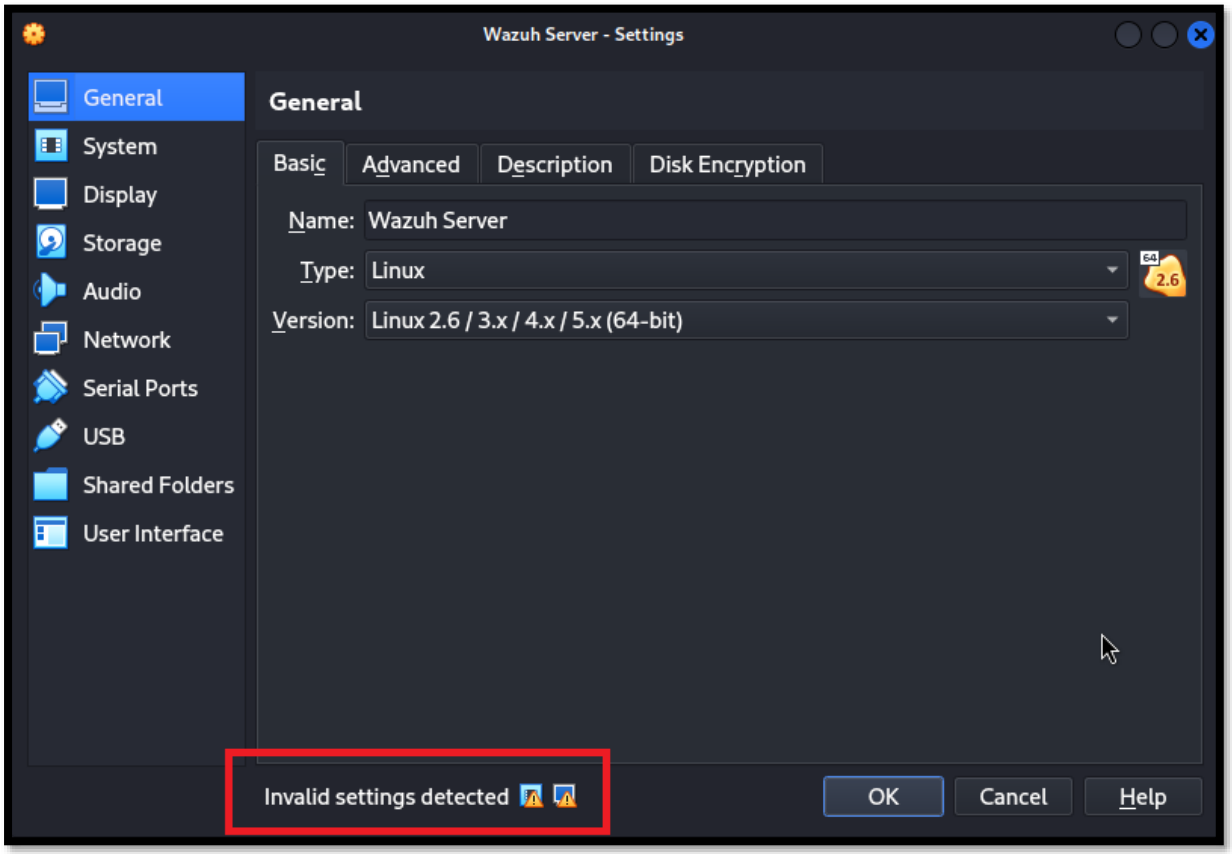


After click on Finish button Wazuh OVA will starting import.

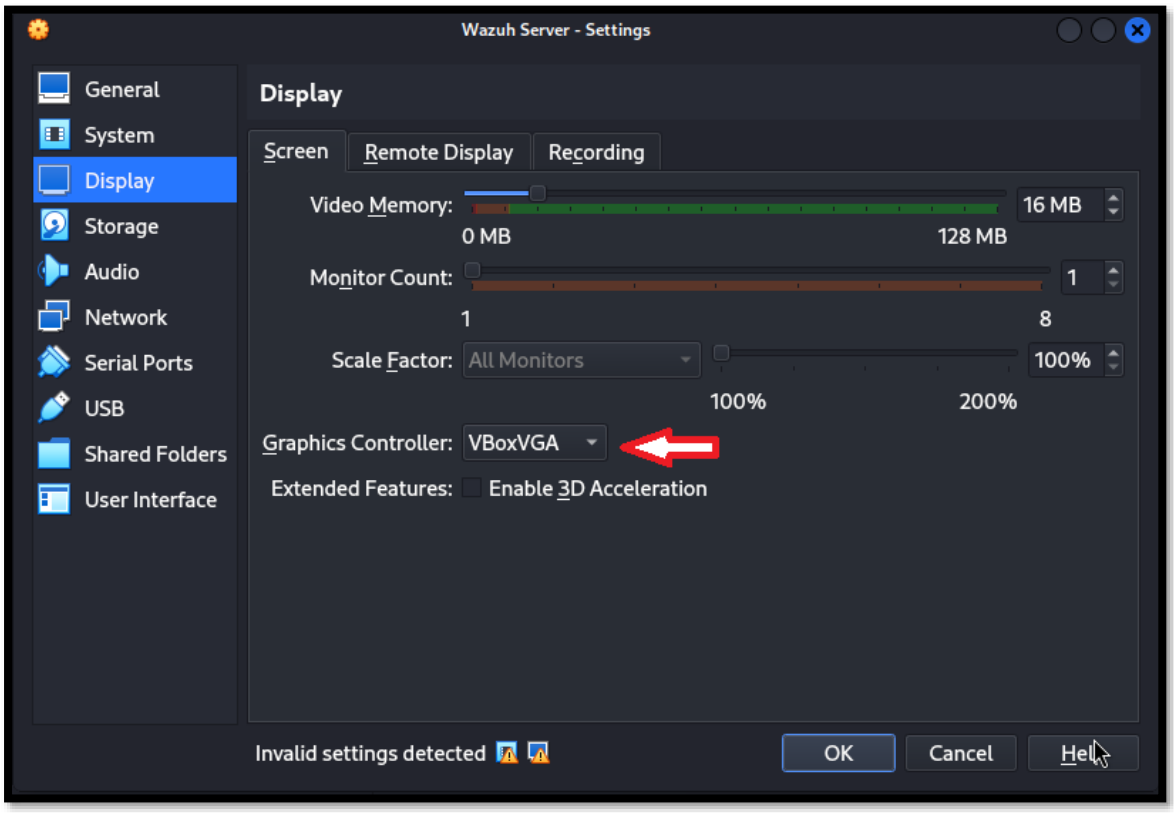


After few minutes Wazuh is imported in VirtualBox.

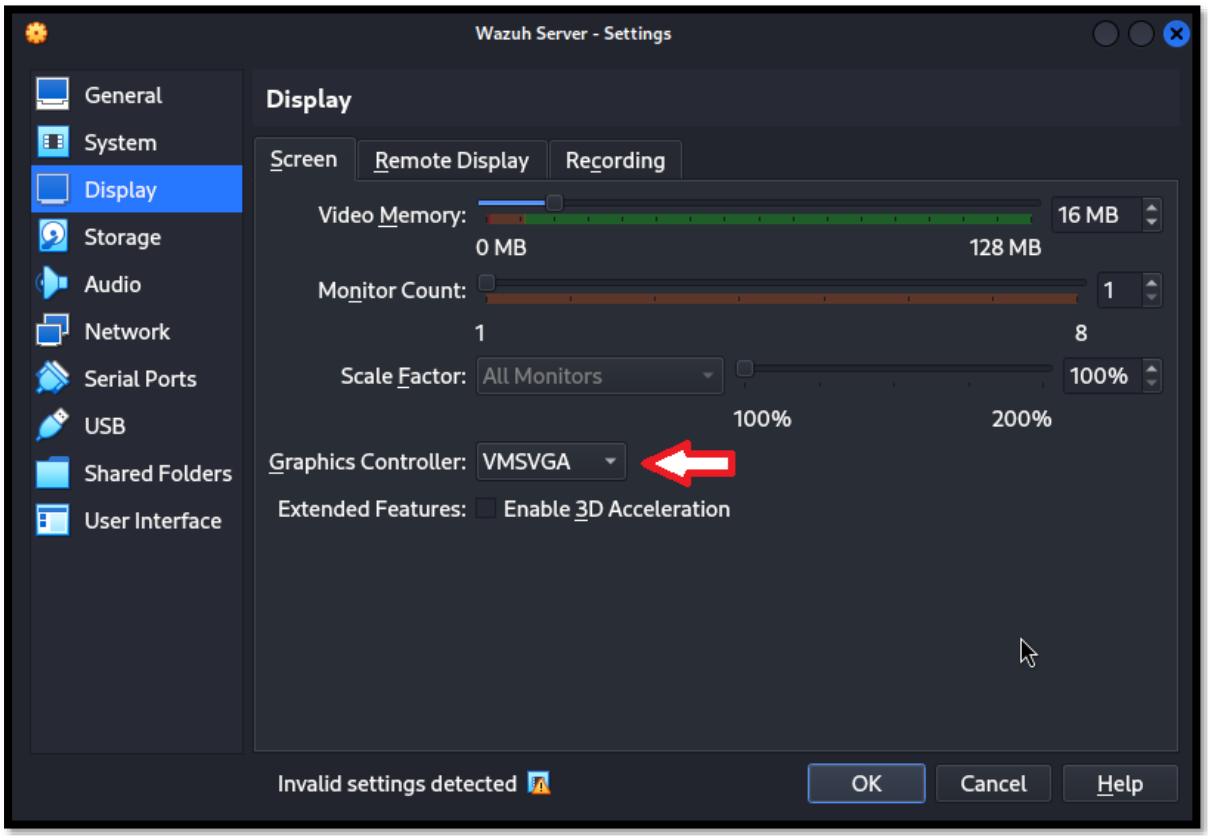
Now select “Wazuh Server” and click on Setting button. Here you can se “Invalid setting detected”



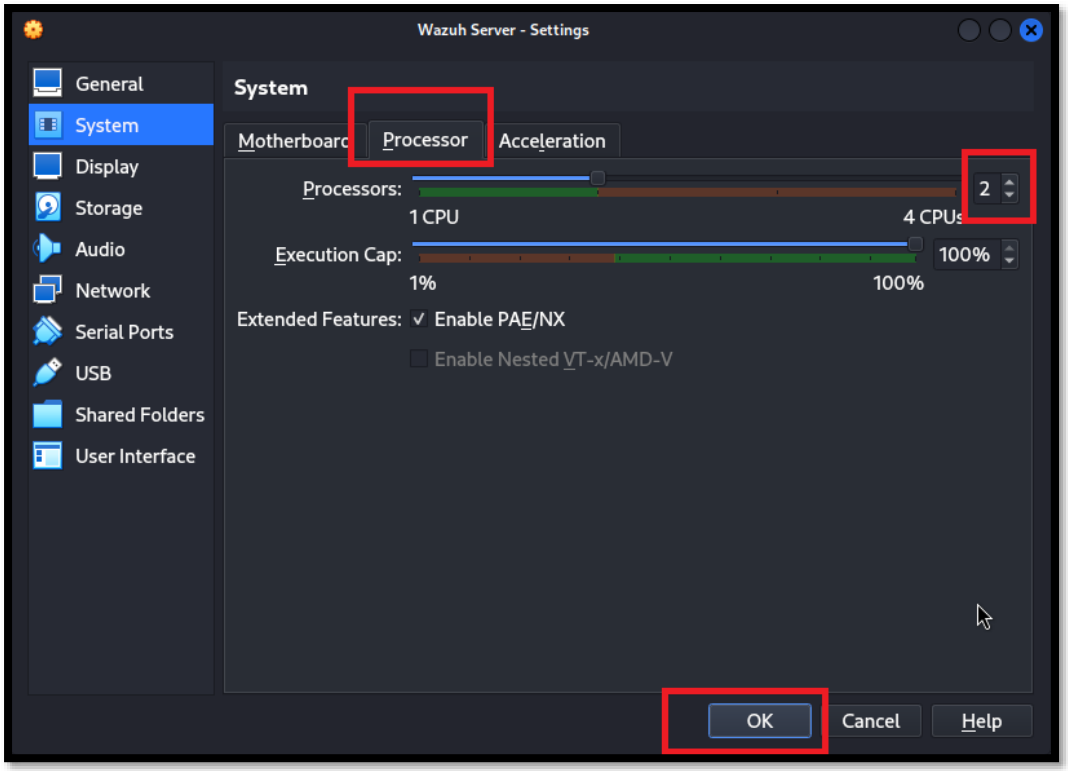
The invalid setting in Graphics Controller section.



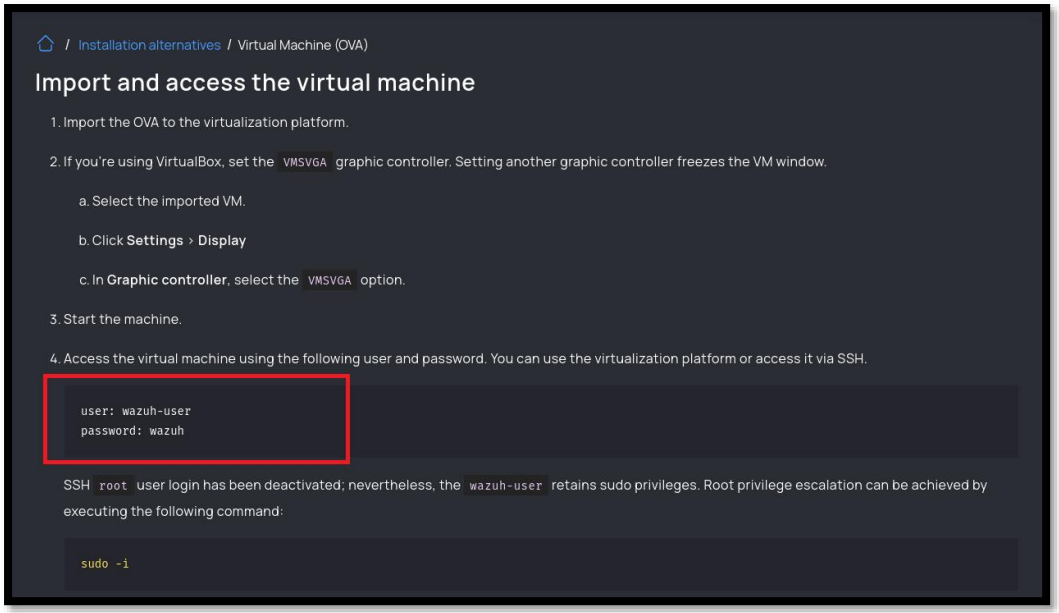
Now change “VBoxVGA” to “VMSVGA”



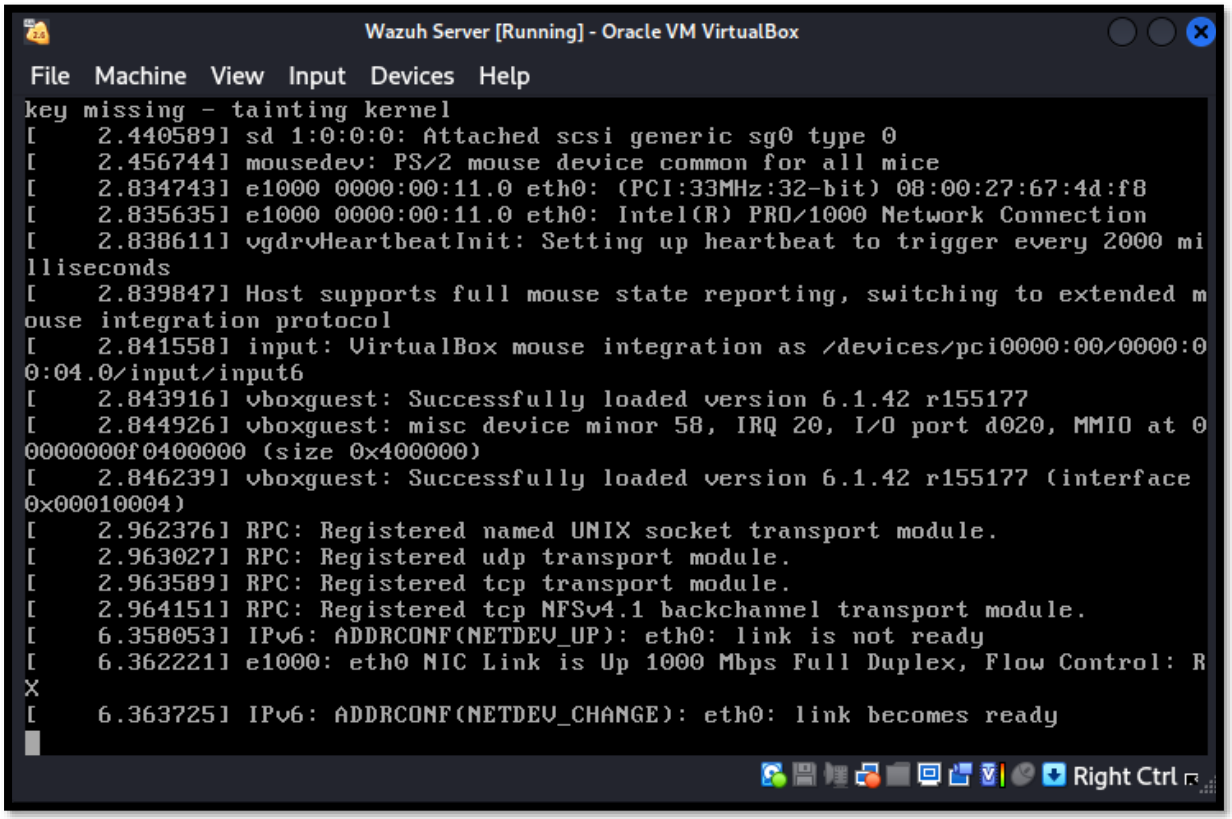
Now fixing other invalid setting by selecting Processors: In my case I have only 4 CPUs so I am selecting 2 CPUs for Wazuh Server.
After selecting click on OK button and Start the machine.



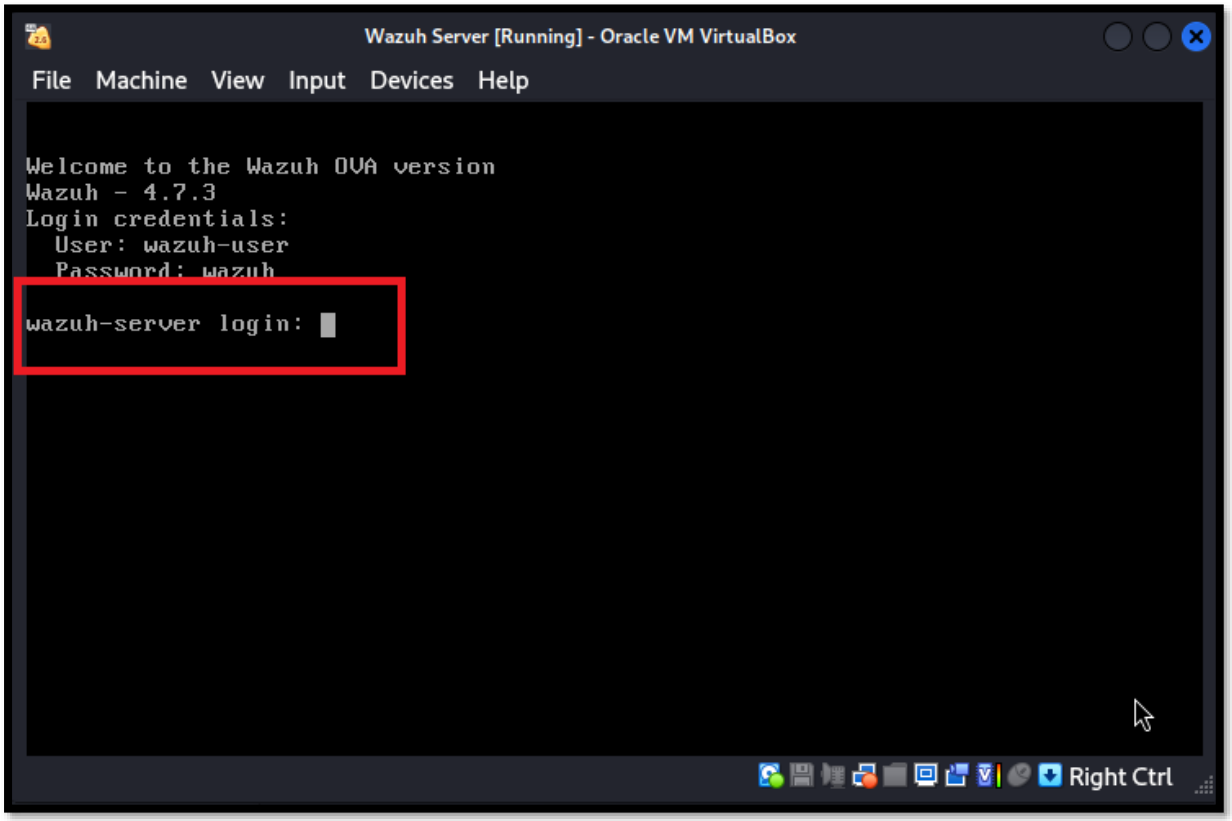
Credentials require for accessing Wazuh virtual machine is available of Wazuh official website. Also available on Wazuh virtual machine screen.



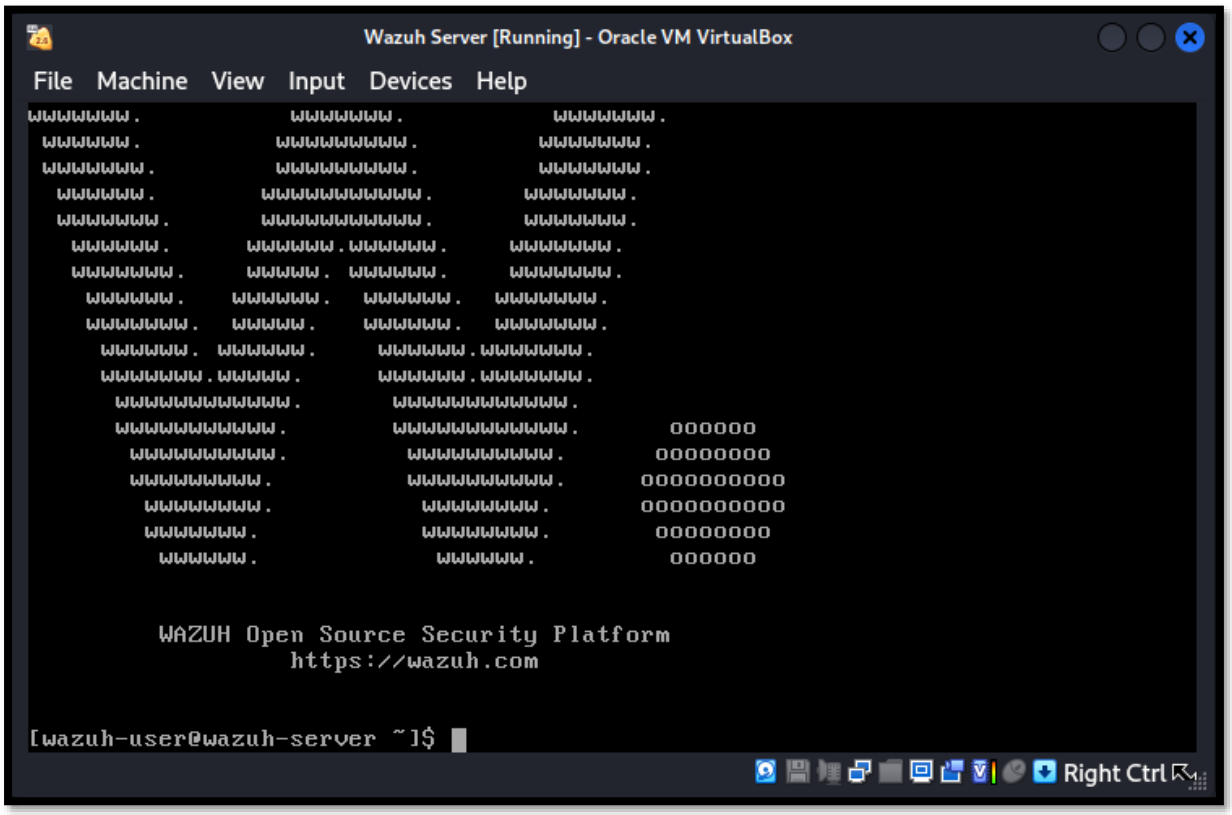
Wazuh virtual machine is booting.



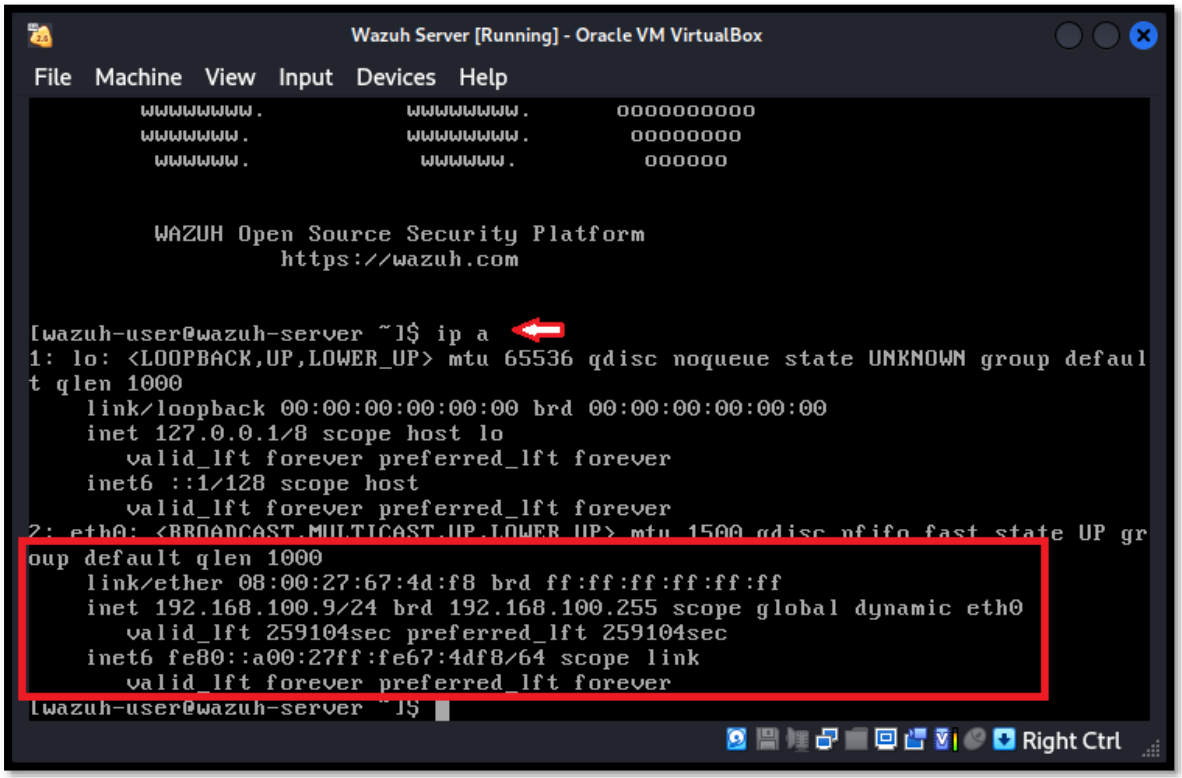
Now enter the login: Wazuh-user



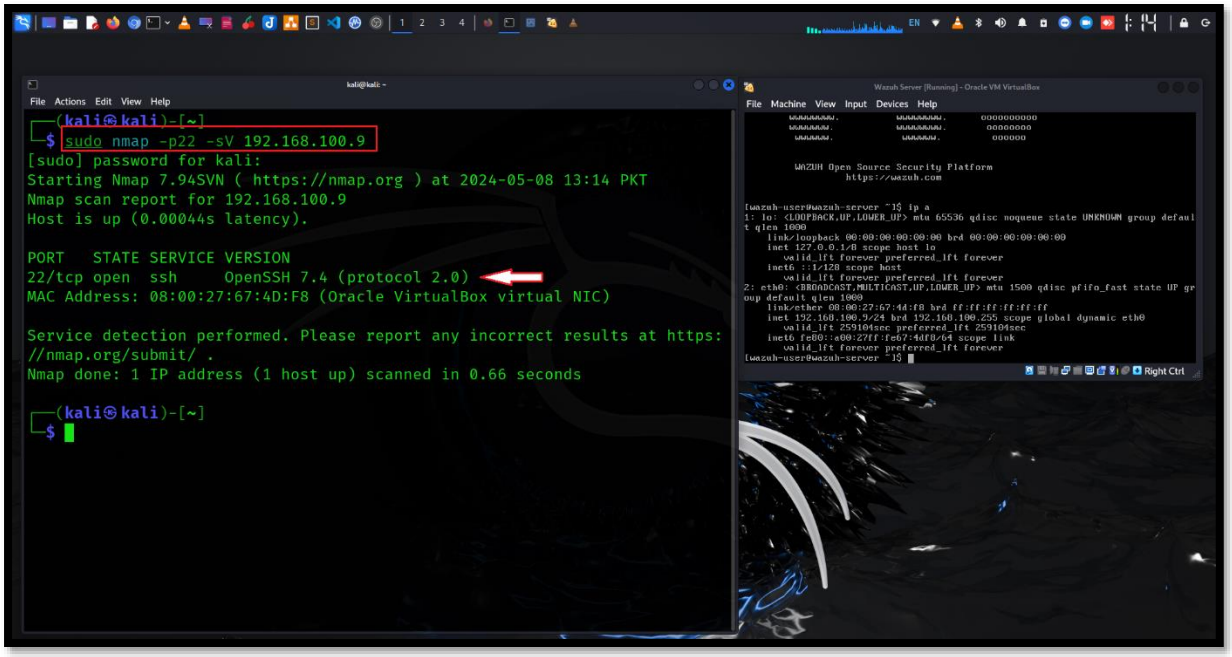
Wazuh is now running



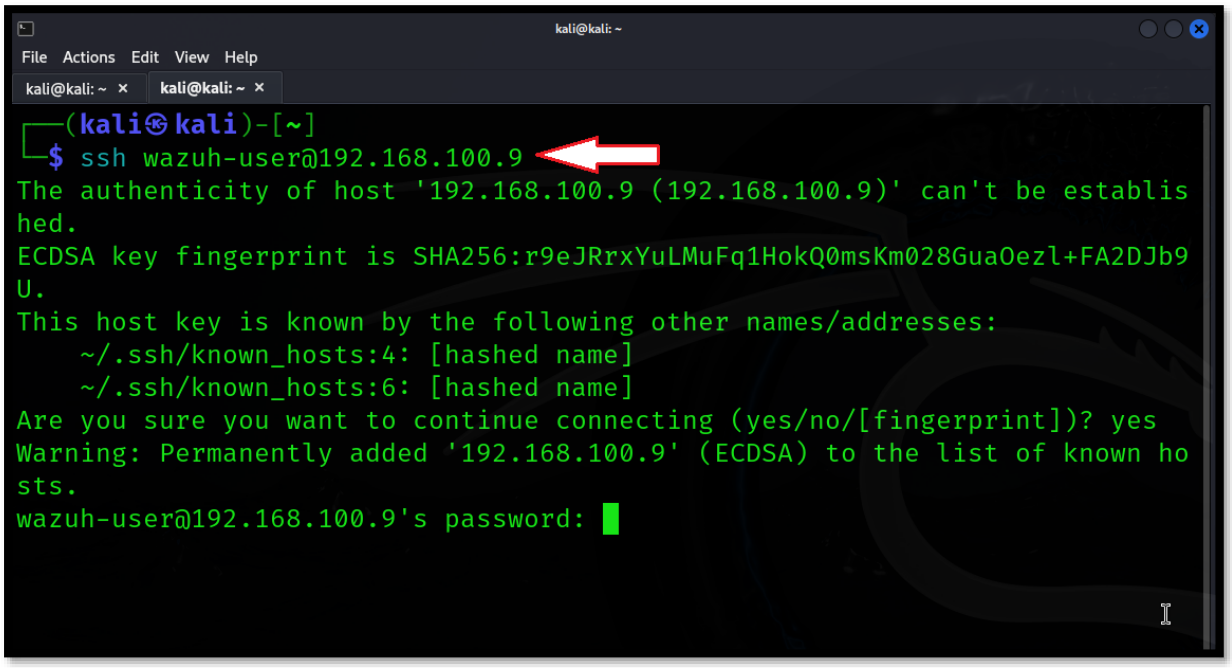
Check the IP Address of Wazuh with “ip a” command.
In my case it’s “192.168.100.9” We will change the IP Address in next Lab.



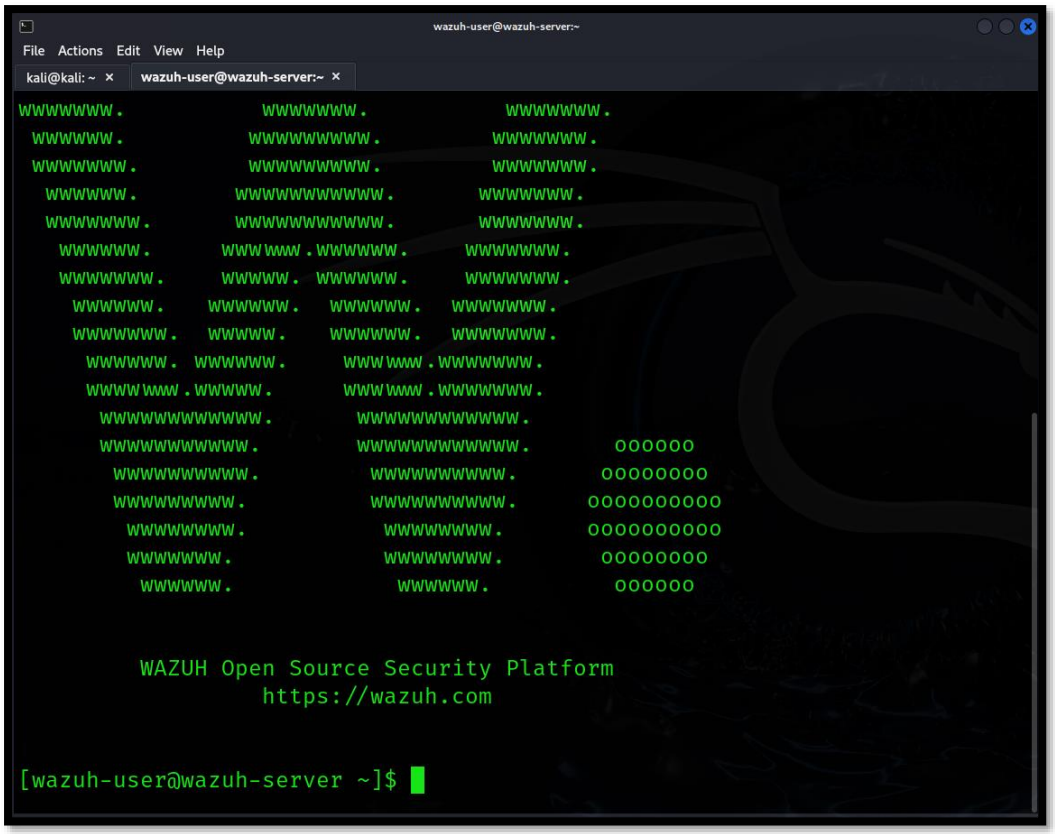
Now check if the SSH is running on Wazuh:
Type the command: sudo nmap -p22 -sV 192.168.100.9
SSH port is open and running.



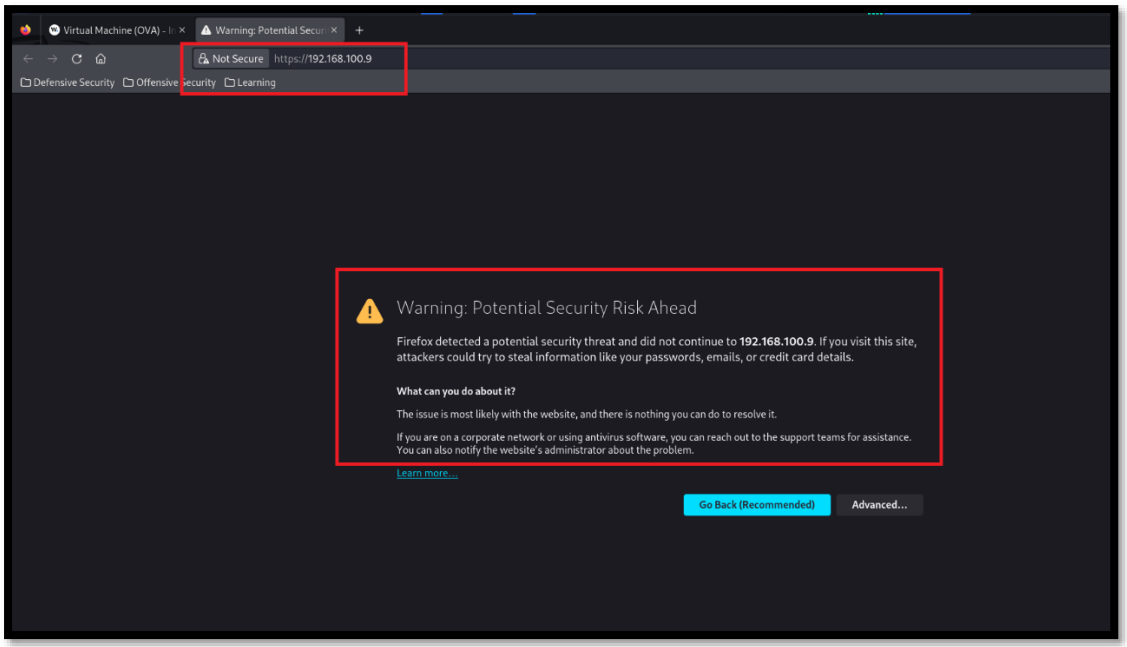
Now we have to access the Wazuh machine via SSH.
Command: ssh Wazuh-user@192.168.100.9
Accept the connection with “Yes” and enter the Wazuh password.



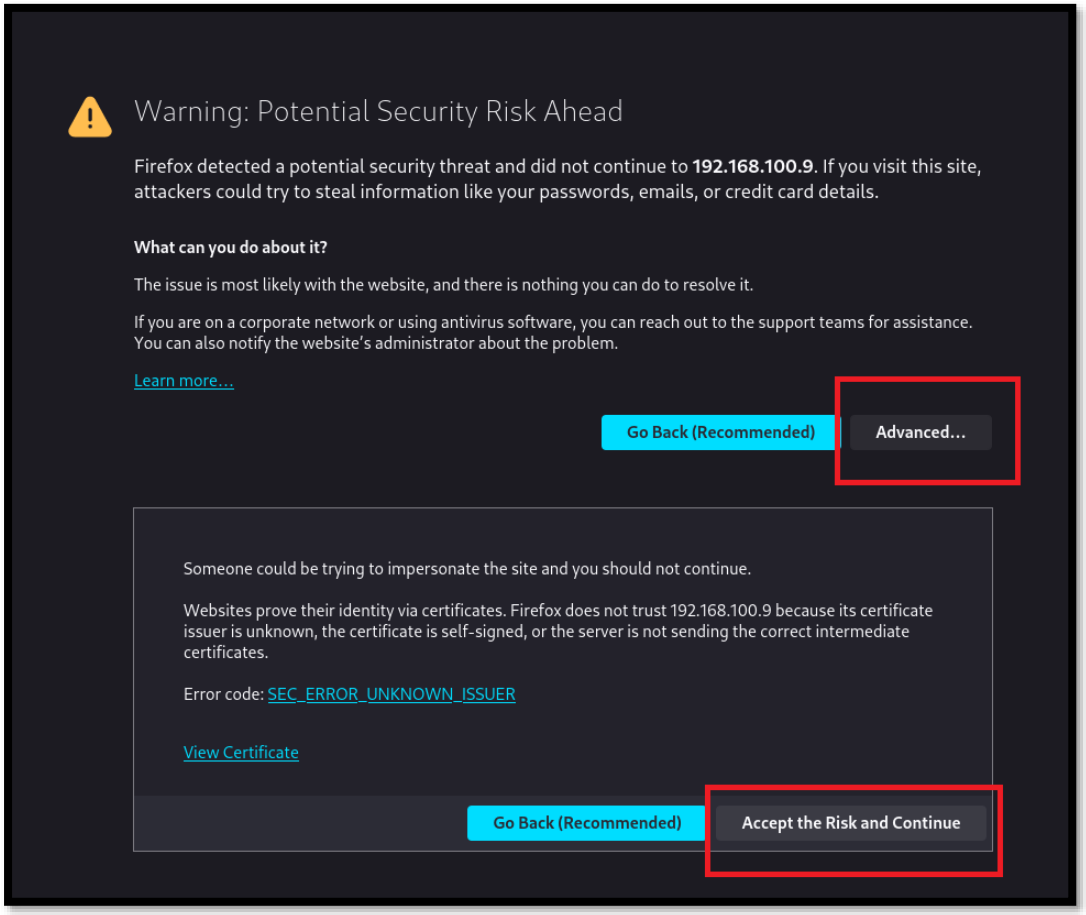
Now we successfully login via SSH, we can edit or modify configuration via SSH Connection (Recommended)



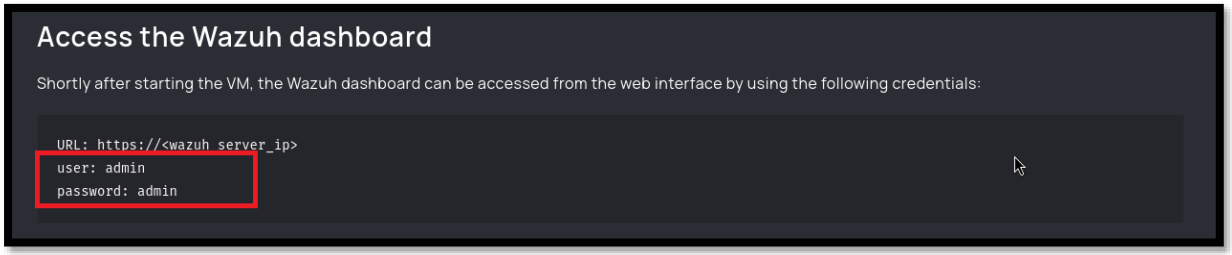
Now it’s time to access Wazuh Dashboard form any browser. Type the IP Address of Wazuh in URL bar.



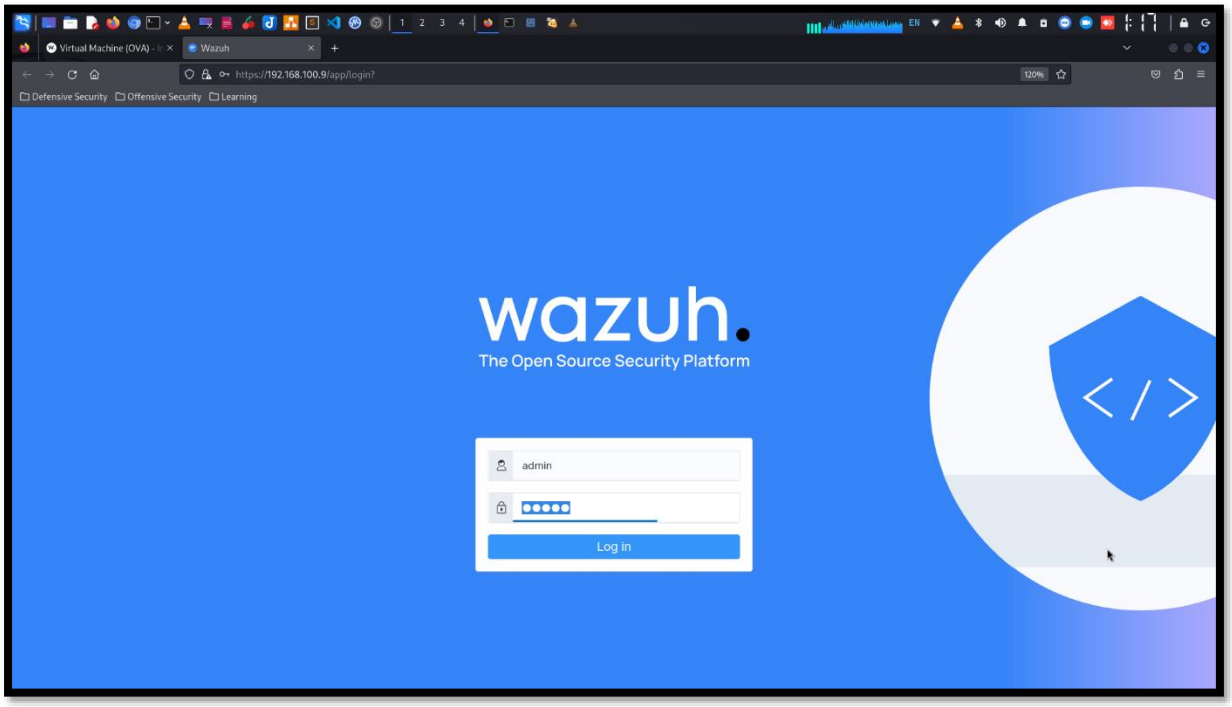
It’s showed some security warning, click on Advanced and then click on “Accept the Risk and Continue”



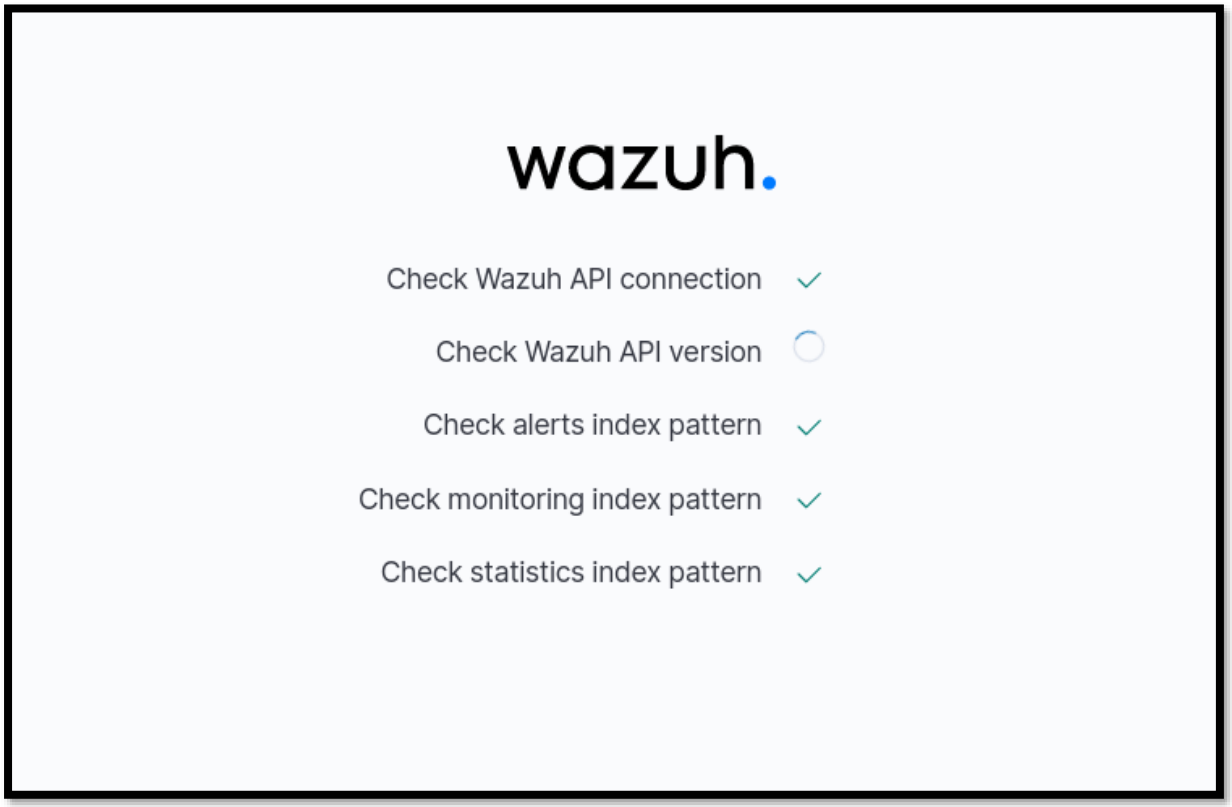
Here is we need credentials for accessing Wazuh Dashboard. It’s available on Wazuh Official Website.



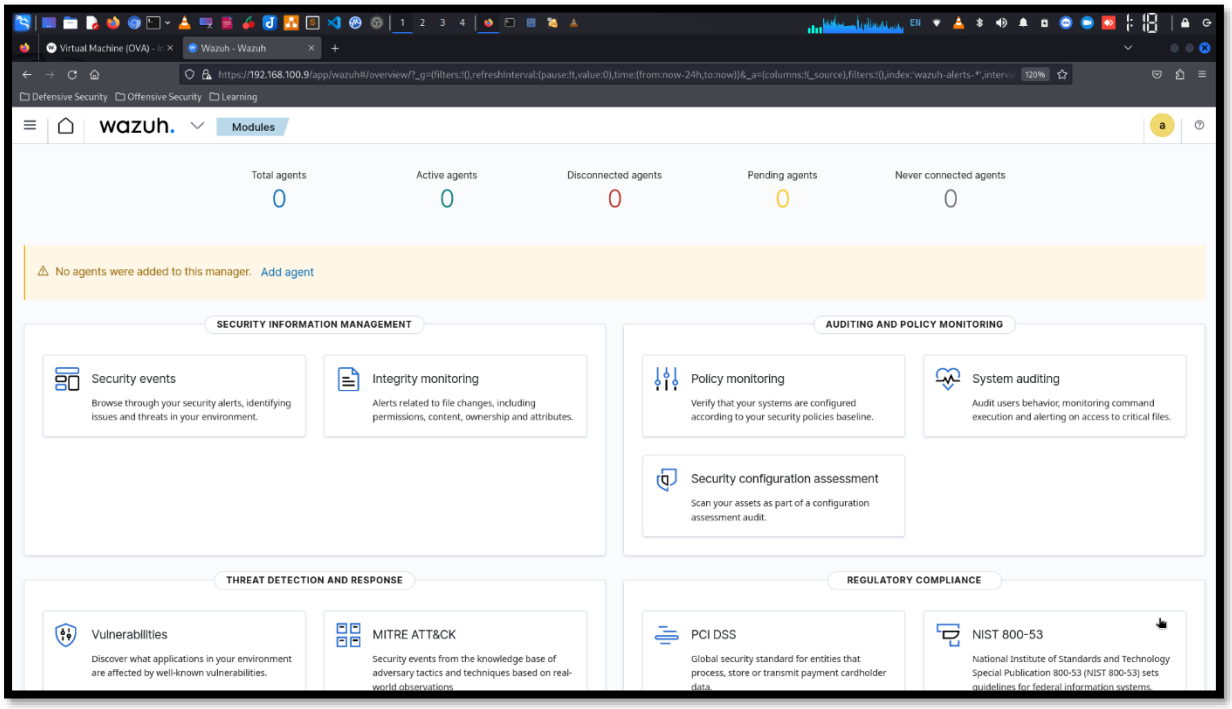
Entering the credentials and login.



Wazuh is checking some configuration related to API version.



Here is the awesome Dashboard of Wazuh.



SUMMARY

In summary, by following these steps, you can successfully install Wazuh as an OVA and leverage its capabilities for security monitoring and threat detection within your virtualized environment.