



wazuh.

Wazuh Server Installation

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: [linkedin.com/in/moizuddinrafay](https://www.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>

The screenshot shows the Wazuh documentation page for Virtual Machine (OVA) installation. The page is titled "Virtual Machine (OVA)" and provides information about the pre-built virtual machine image in Open Virtual Appliance (OVA) format. It lists the components included in the OVA: Amazon Linux 2, Wazuh manager 4.7.4, Wazuh indexer 4.7.4, Filebeat-OSS 7.10.2, and Wazuh dashboard 4.7.4. A "Packages list" table is also shown, with the "wazuh-4.7.4.ova (sha512)" package highlighted in a red box.

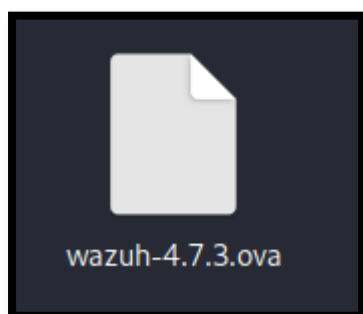
Distribution	Architecture	VM Format	Version	Package
Amazon Linux 2	64-bit	OVA	4.7.4	wazuh-4.7.4.ova (sha512)

Read the hardware requirements for wazuh installation.

The screenshot shows the Wazuh documentation page for Hardware requirements. The page is titled "Hardware requirements" and lists the requirements for the Wazuh VM. The requirements are: The host operating system has to be a 64-bit system, Hardware virtualization has to be enabled on the firmware of the host, and A virtualization platform, such as VirtualBox, should be installed on the host system. A table shows the out-of-the-box configuration for the Wazuh VM: CPU (cores) is 4, RAM (GB) is 8, and Storage (GB) is 50.

Component	CPU (cores)	RAM (GB)	Storage (GB)
Wazuh v4.7.4 OVA	4	8	50

Here is downloaded Wazuh-4.7.3.ova file

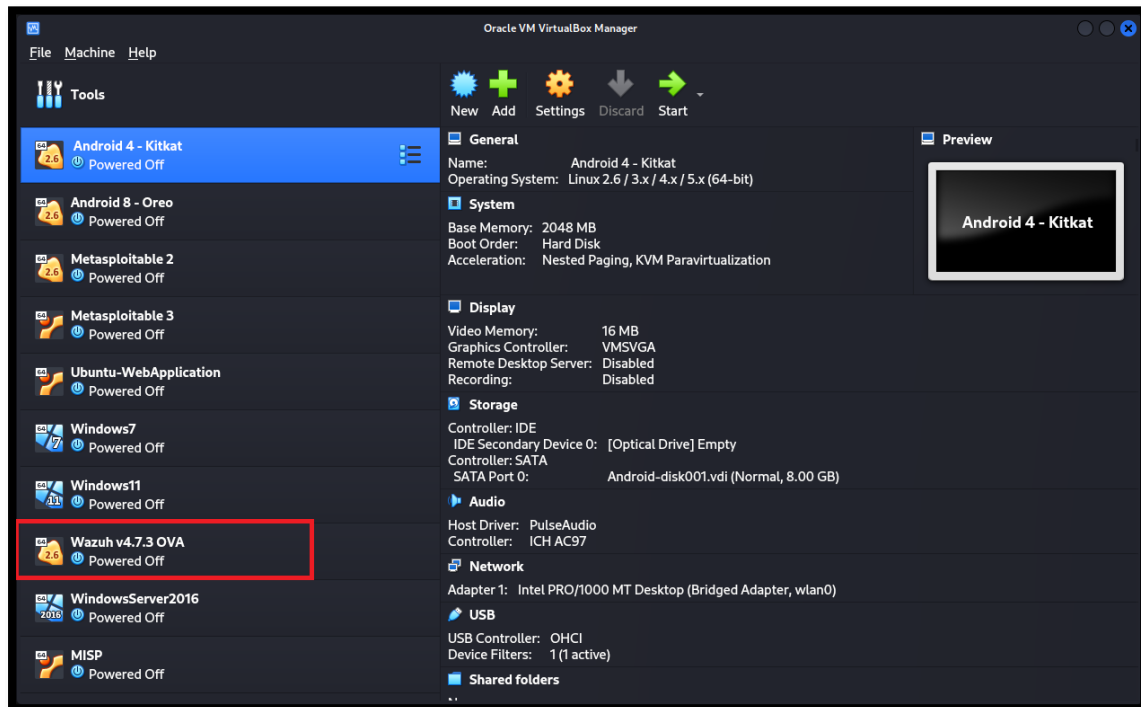


Wazuh Installation & Configuration Lab: 01

Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

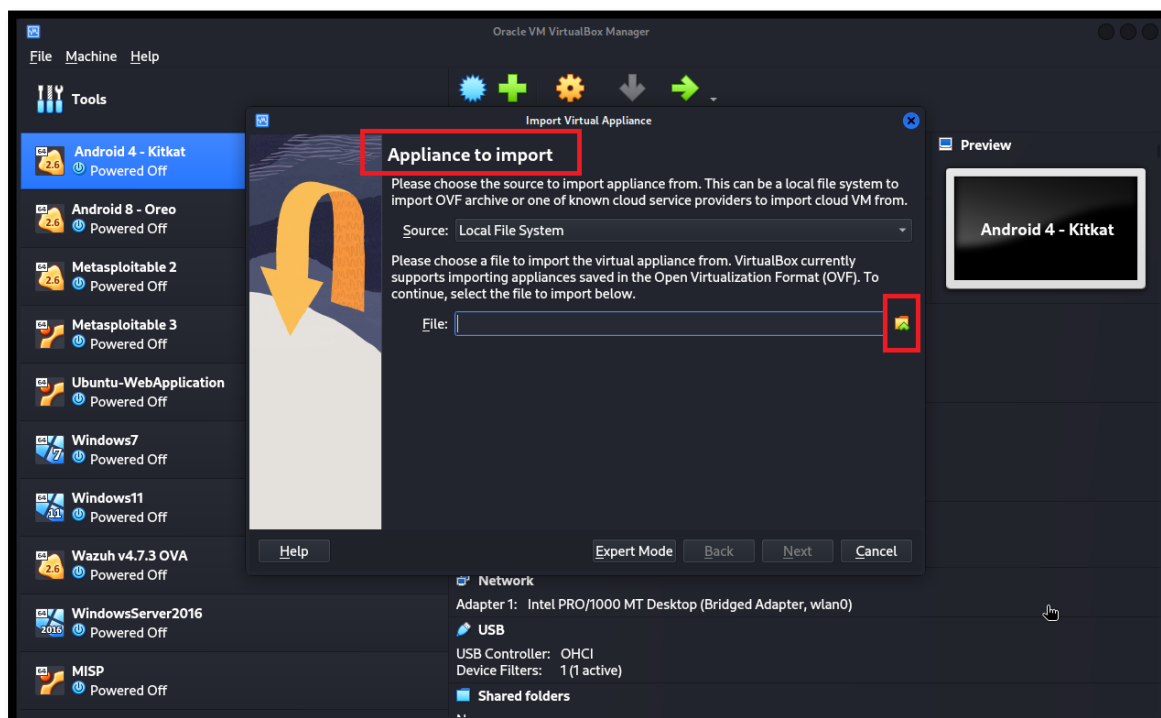
Step 02: Wazuh Installation on VirtualBox.

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...”.

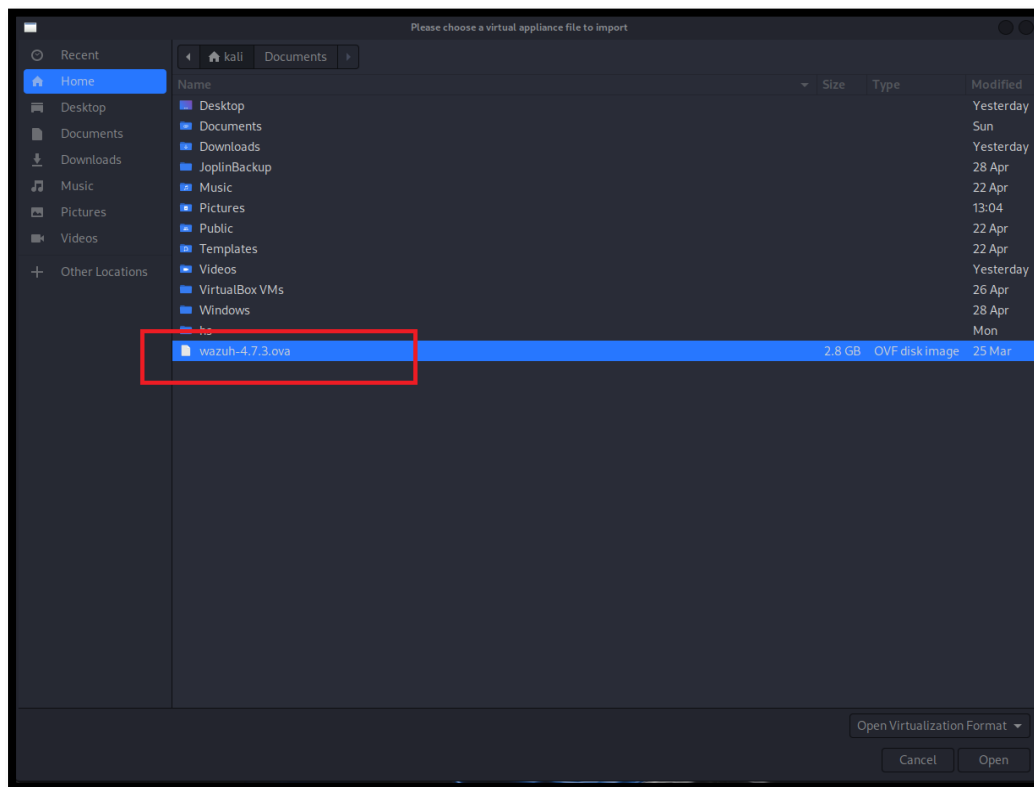
Import Appliance Wizard is open now select the location where Wazuh-4.7.3.ova file is downloaded.



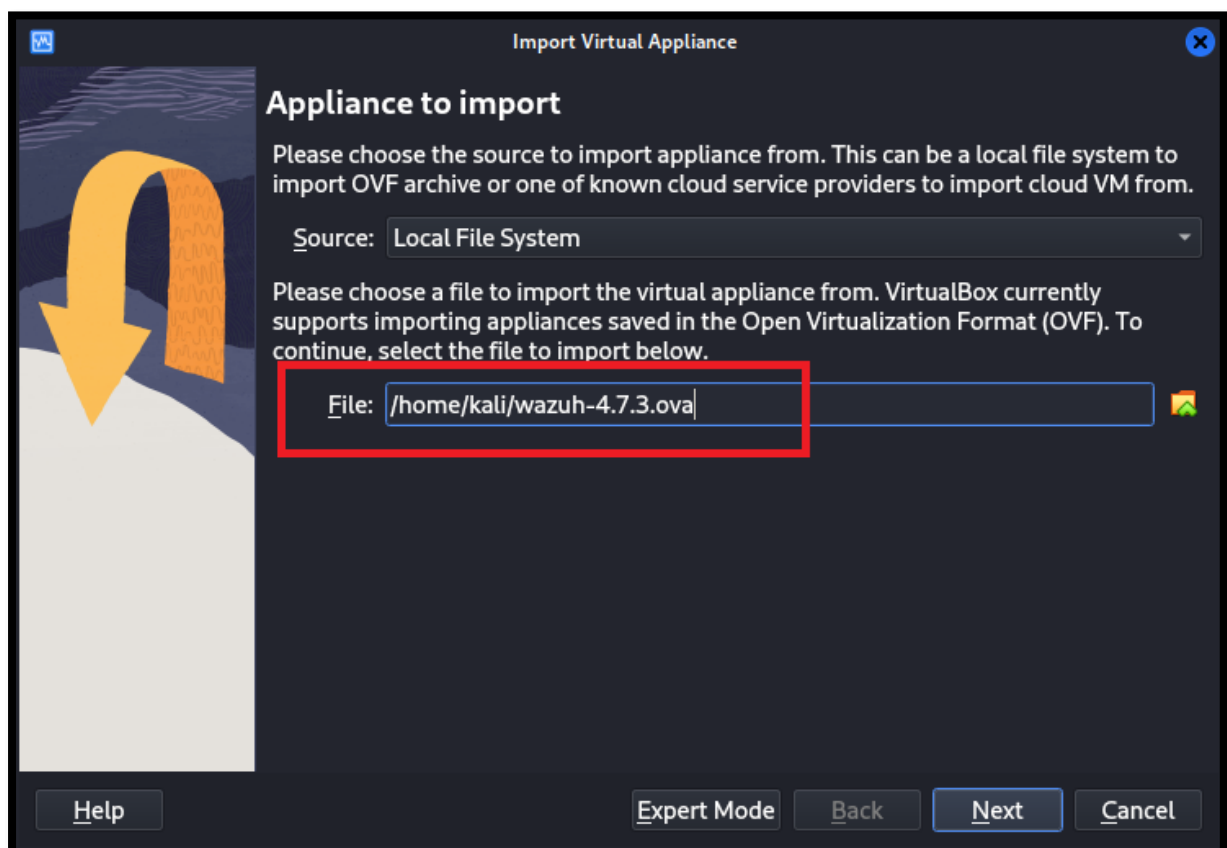
Wazuh Installation & Configuration Lab: 01

Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

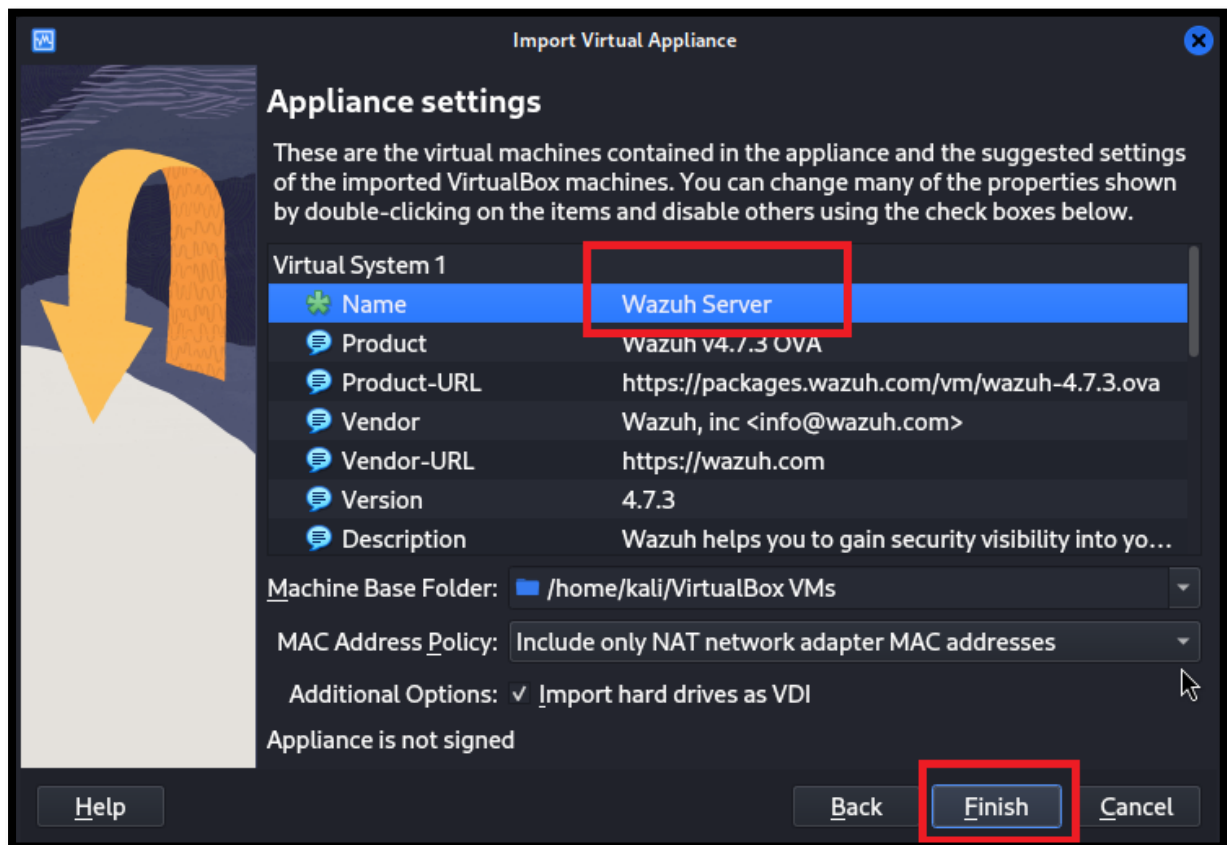
Select the Wazuh-4.7.3.ova file.



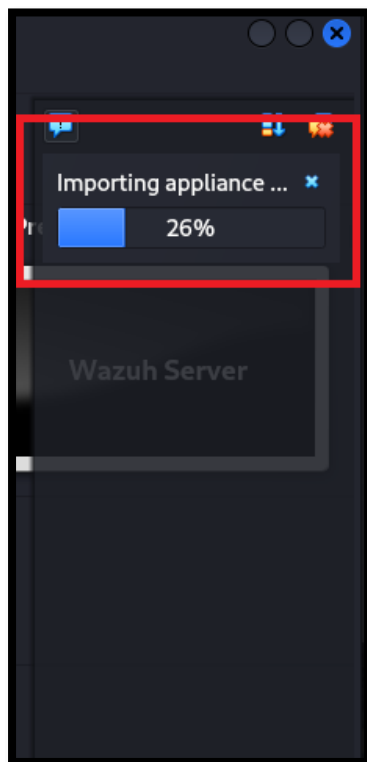
After selection click on next.



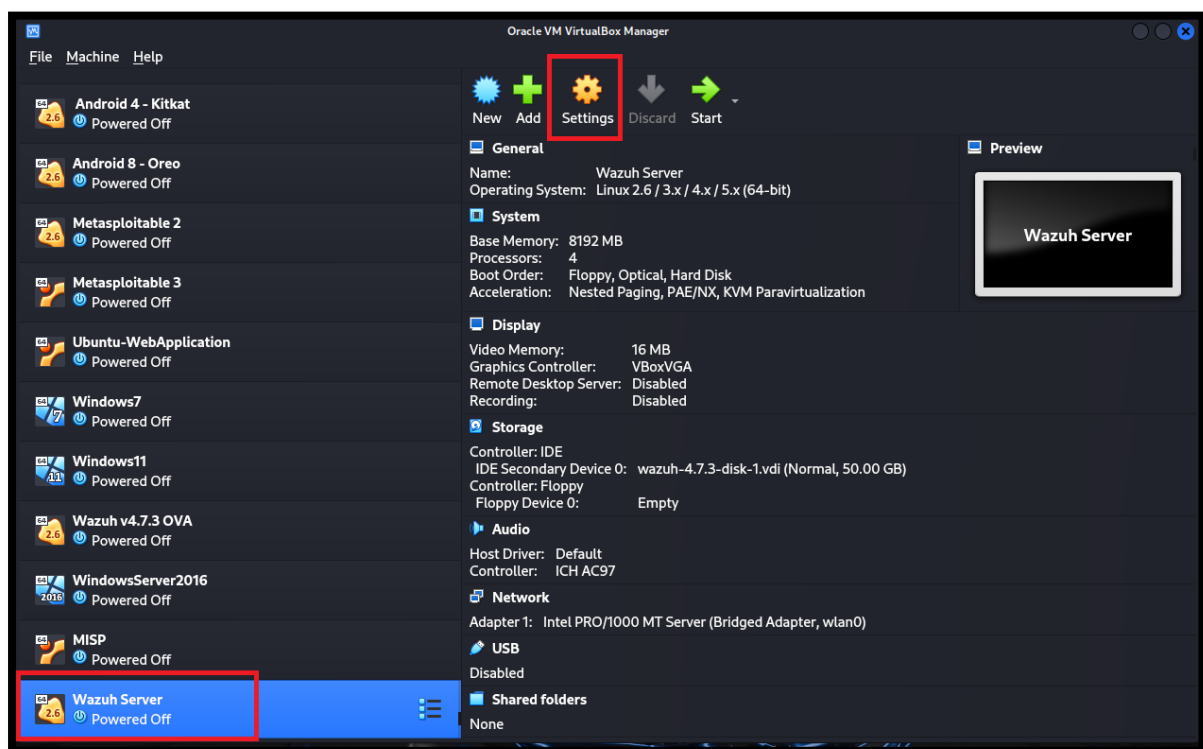
Change the Name what you want in my case I am using “Wazuh Server”



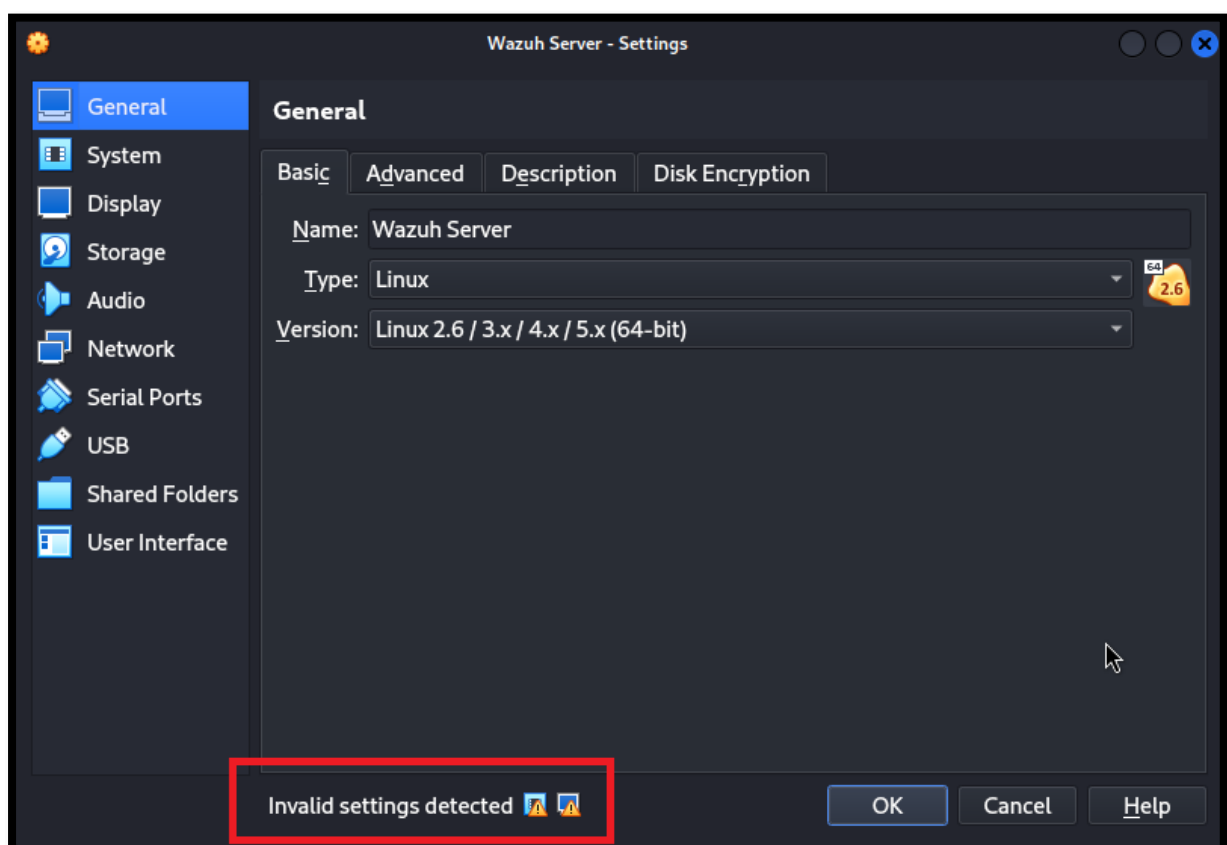
After click on Finish button Wazuh OVA will starting import.



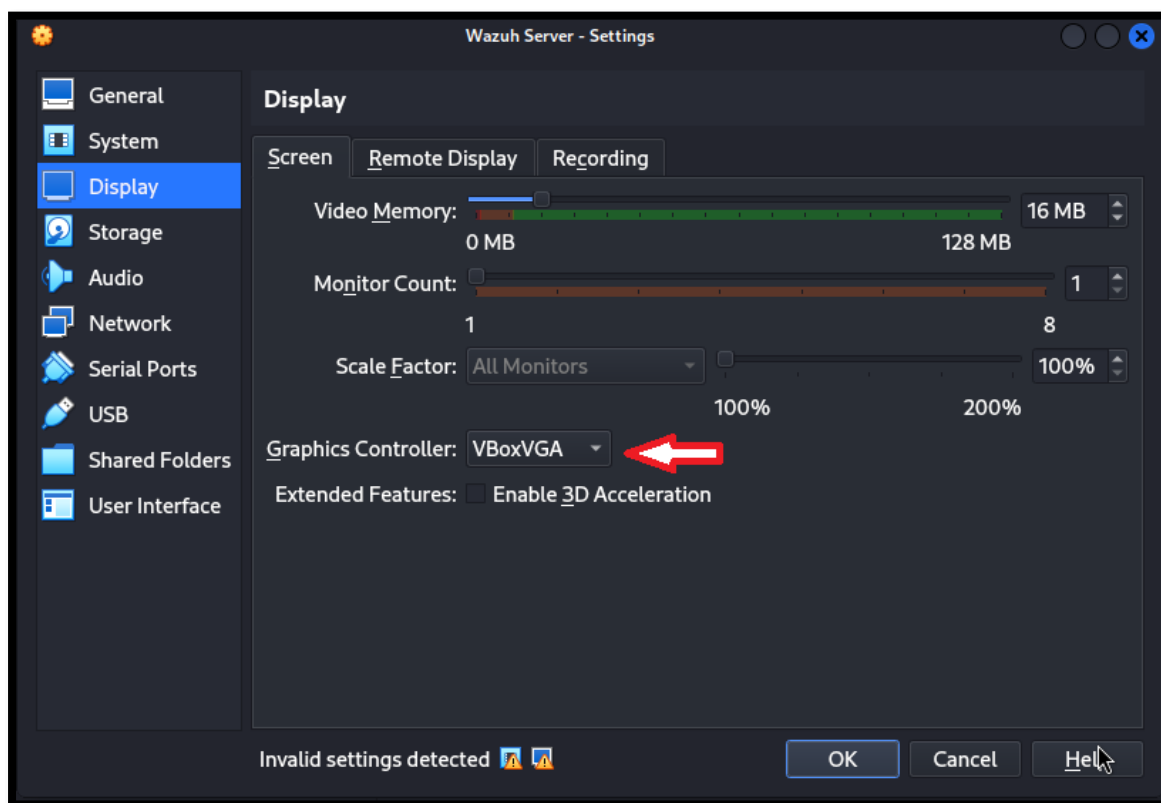
After few minutes Wazuh is imported in VirtualBox.



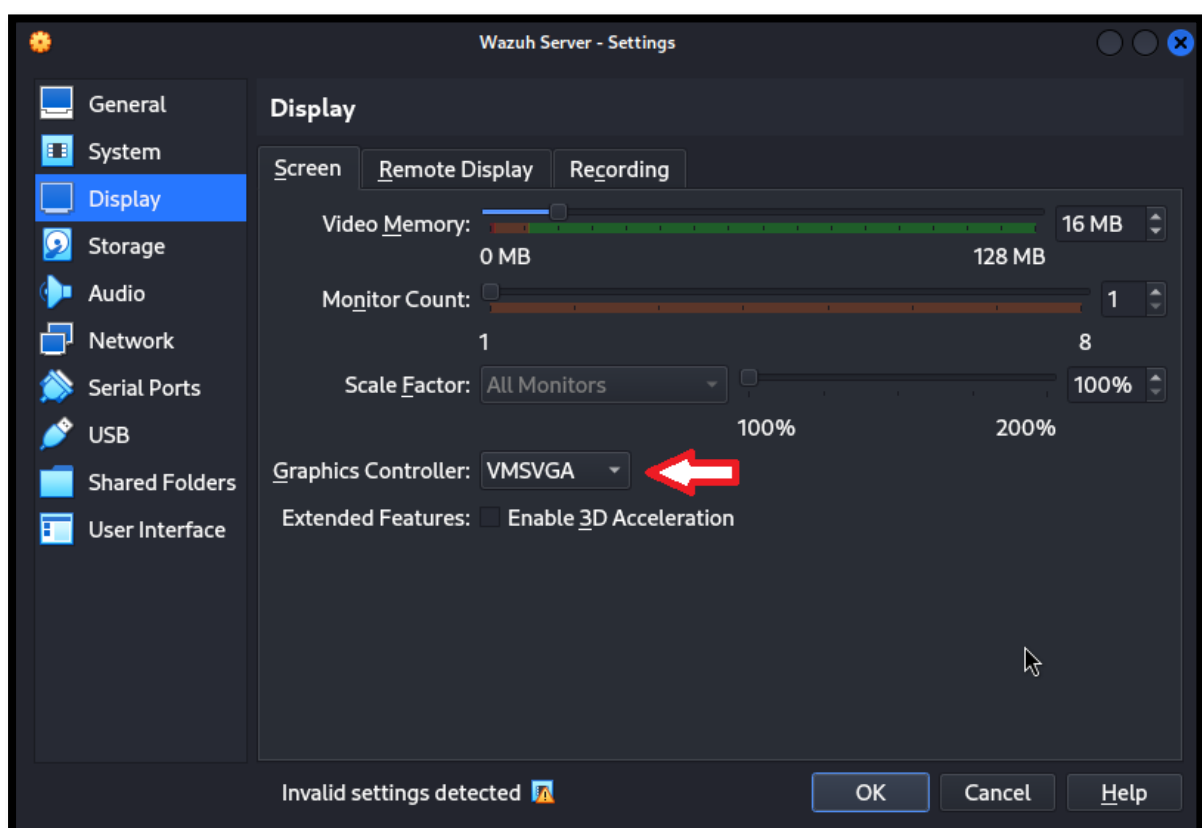
Now select “Wazuh Server” and click on Setting button. Here you can see “Invalid setting detected”



The invalid setting in Graphics Controller section.

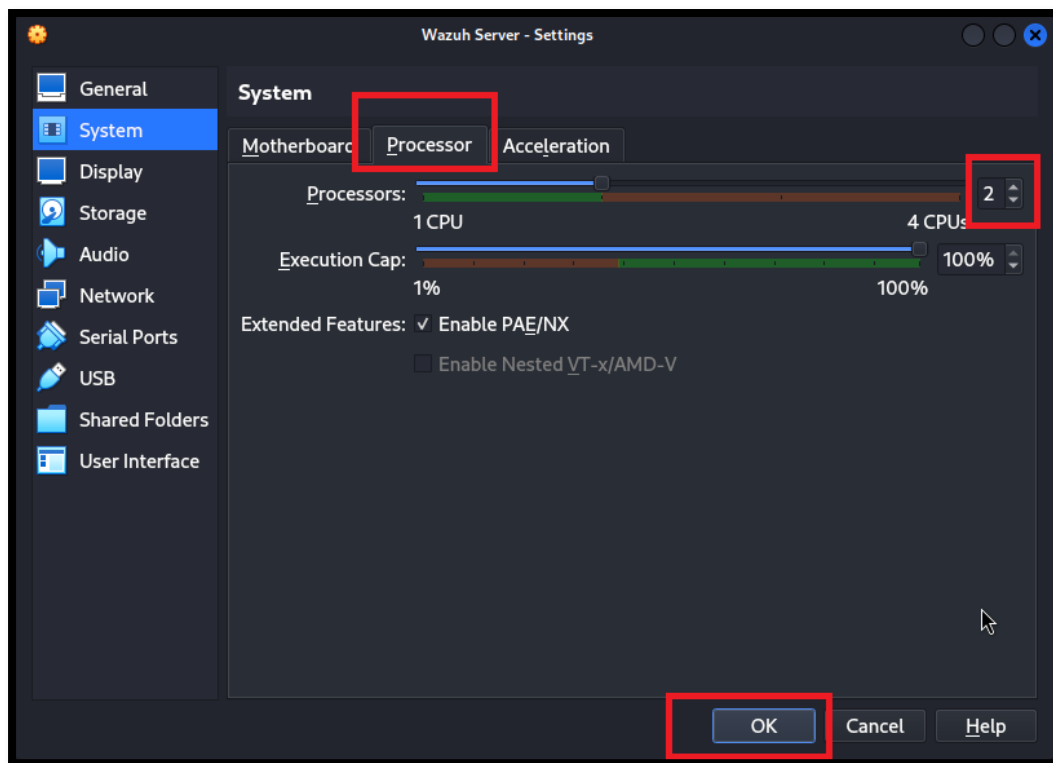


Now change "VBoxVGA" to "VMSVGA"

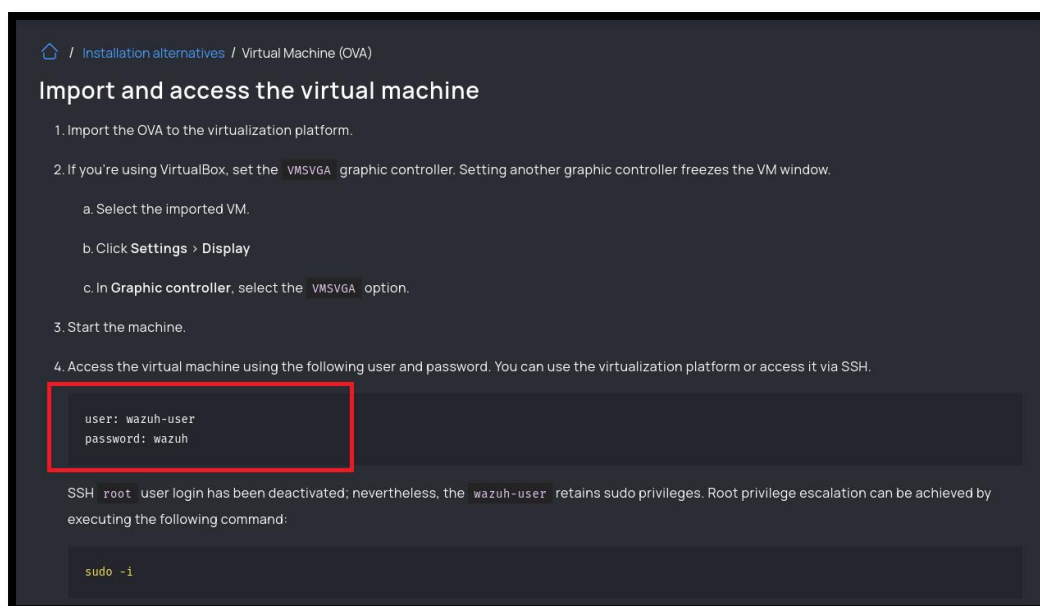


Now fixing other invalid setting by selecting Processors: In my case I have only 4 CPUs so I am selecting 2 CPUs for Wazuh Server.

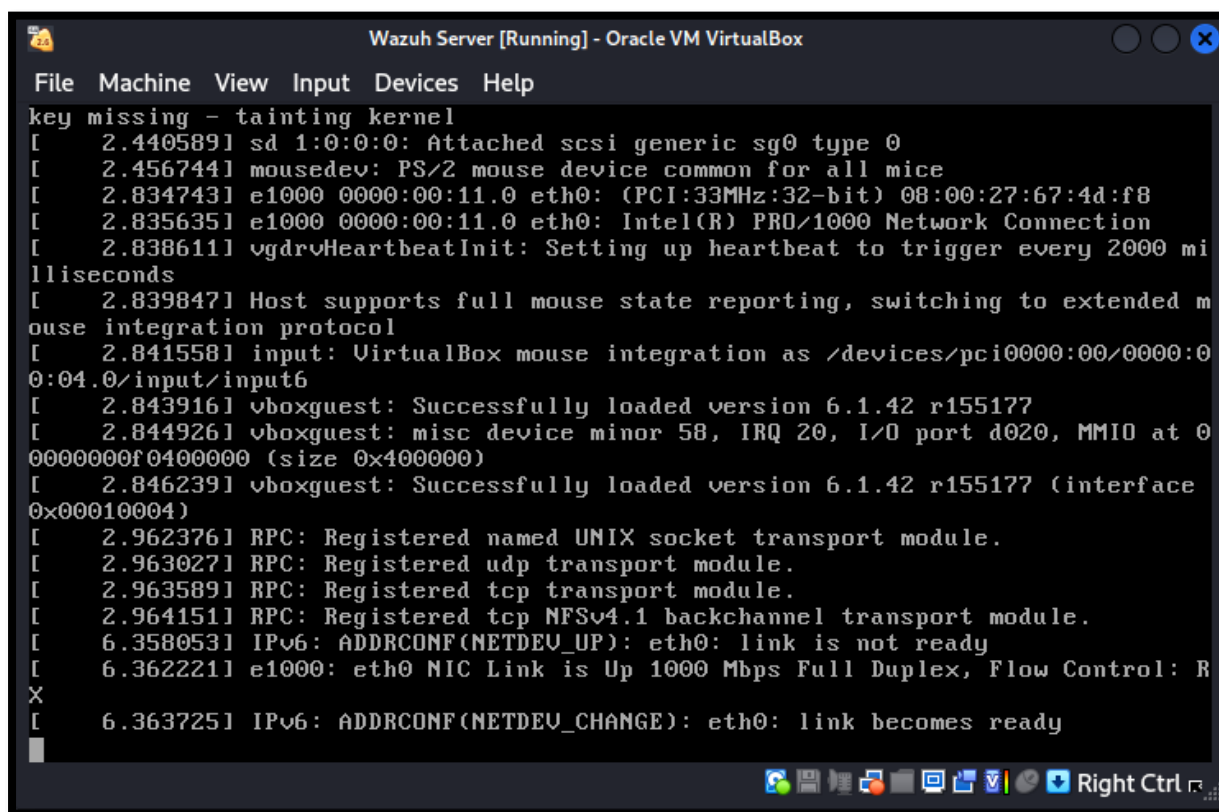
After selecting click on OK button and Start the machine.



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



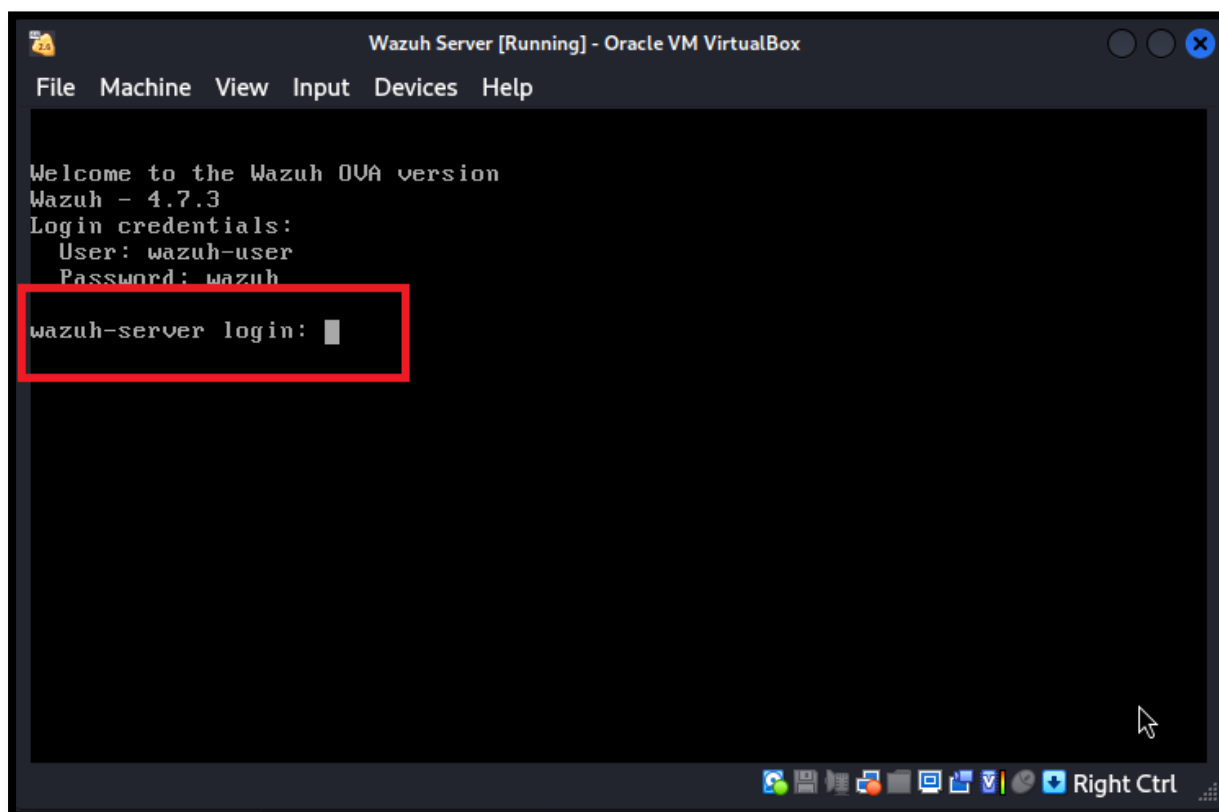
Wazuh virtual machine is booting.



The screenshot shows a terminal window titled "Wazuh Server [Running] - Oracle VM VirtualBox". The terminal displays various boot logs, including kernel messages and hardware initialization. The logs show the system is booting, with messages like "key missing - tainting kernel", "sd 1:0:0:0: Attached scsi generic sg0 type 0", "mousedev: PS/2 mouse device common for all mice", and "eth0: Intel(R) PRO/1000 Network Connection". The terminal also shows the successful loading of the vboxguest module and the registration of various transport modules like RPC, udp, tcp, and NFSv4.1. The network interface eth0 is shown as being up and ready.

```
key missing - tainting kernel
[ 2.440589] sd 1:0:0:0: Attached scsi generic sg0 type 0
[ 2.456744] mousedev: PS/2 mouse device common for all mice
[ 2.834743] e1000 0000:00:11:0 eth0: (PCI:33MHz:32-bit) 08:00:27:67:4d:f8
[ 2.835635] e1000 0000:00:11:0 eth0: Intel(R) PRO/1000 Network Connection
[ 2.838611] vgdvHeartbeatInit: Setting up heartbeat to trigger every 2000 milliseconds
[ 2.839847] Host supports full mouse state reporting, switching to extended mouse integration protocol
[ 2.841558] input: VirtualBox mouse integration as /devices/pci0000:00/0000:00:04.0/input/input6
[ 2.843916] vboxguest: Successfully loaded version 6.1.42 r155177
[ 2.844926] vboxguest: misc device minor 58, IRQ 20, I/O port d020, MMIO at 00000000f0400000 (size 0x400000)
[ 2.846239] vboxguest: Successfully loaded version 6.1.42 r155177 (interface 0x00010004)
[ 2.962376] RPC: Registered named UNIX socket transport module.
[ 2.963027] RPC: Registered udp transport module.
[ 2.963589] RPC: Registered tcp transport module.
[ 2.964151] RPC: Registered tcp NFSv4.1 backchannel transport module.
[ 6.358053] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 6.362221] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[ 6.363725] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
```

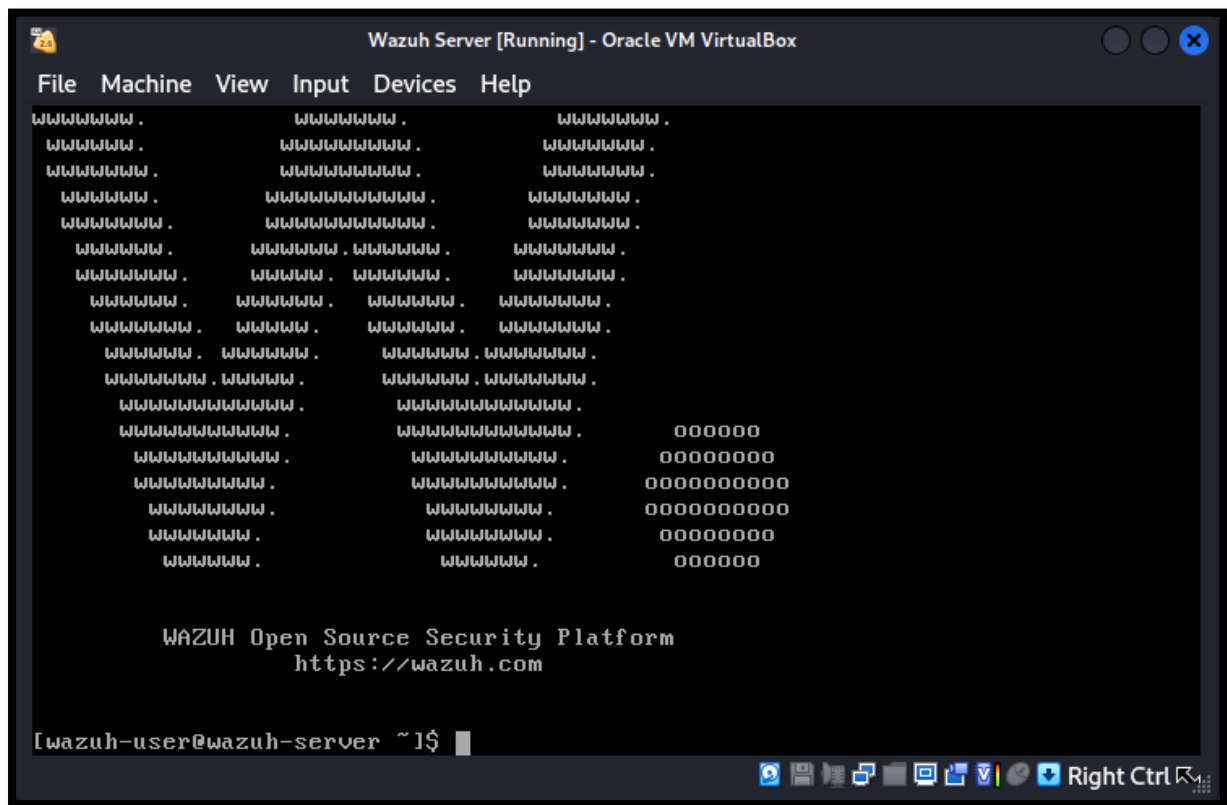
Now enter the login: Wazuh-user



The screenshot shows the same terminal window as before, but now it displays a login prompt. The text "Welcome to the Wazuh OVA version Wazuh - 4.7.3" is shown, followed by "Login credentials:". The user is prompted to enter their username and password. The user has entered "wazuh-user" for the username and "wazuh" for the password. The terminal then shows "wazuh-server login:" followed by a cursor, indicating that the user is now logged in.

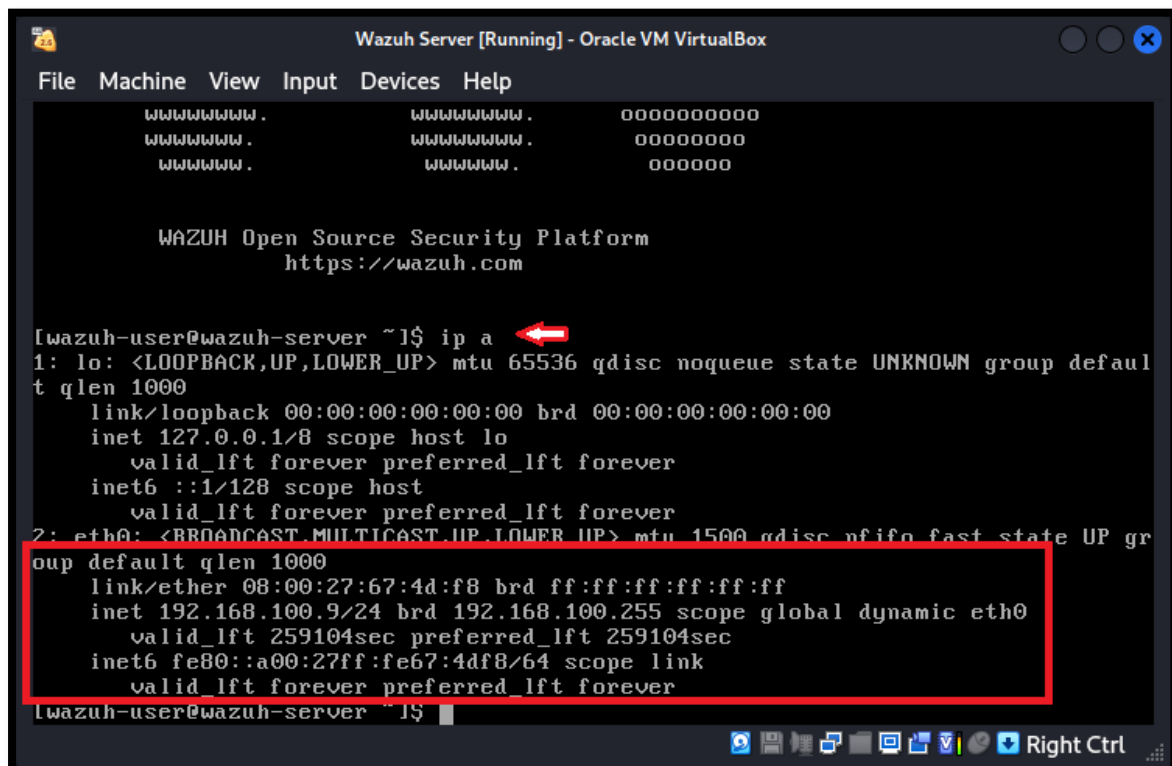
```
Welcome to the Wazuh OVA version
Wazuh - 4.7.3
Login credentials:
User: wazuh-user
Password: wazuh
wazuh-server login: █
```

Wazuh is now running



Check the IP Address of Wazuh with "ip a" command.

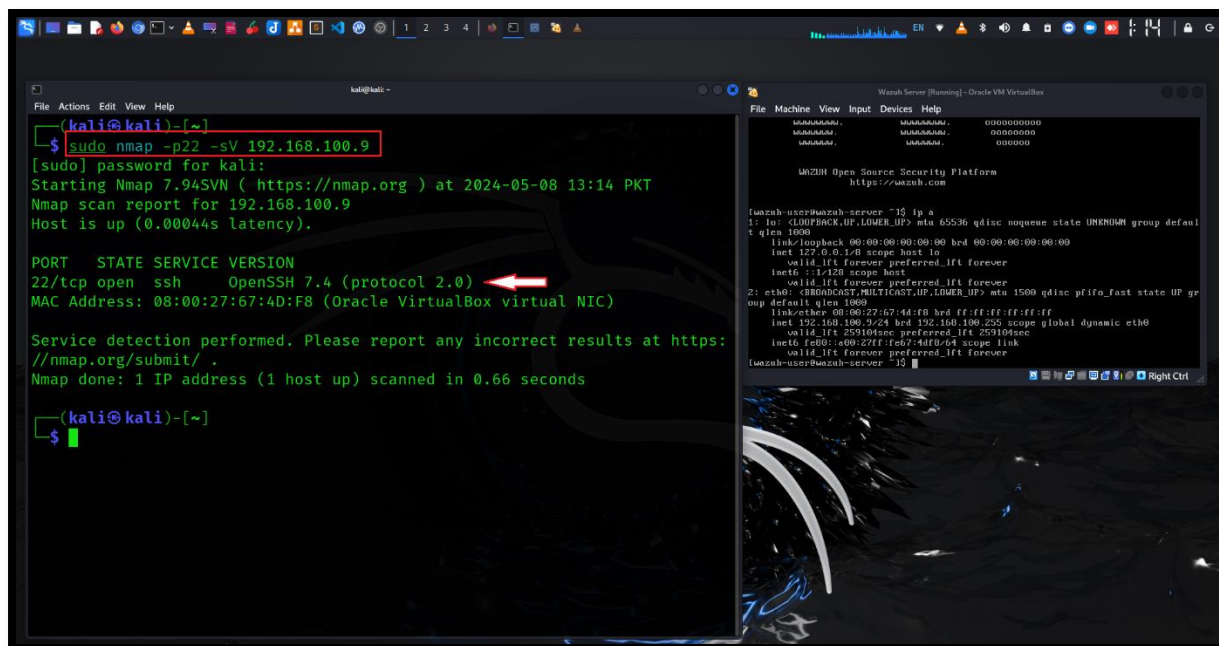
In my case it's "192.168.100.9" We will change the IP Address in next Lab.



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.

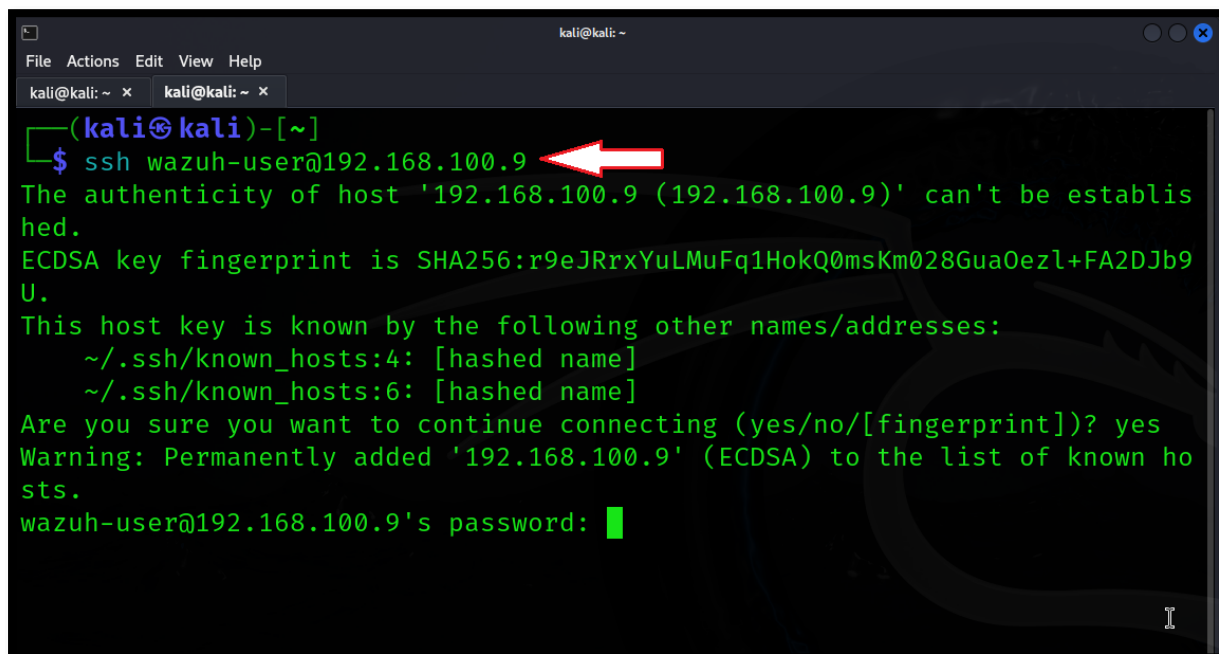


```
kali@kali: ~  
$ sudo nmap -p22 -sV 192.168.100.9  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 13:14 PKT  
Nmap scan report for 192.168.100.9  
Host is up (0.00044s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0) ←  
MAC Address: 08:00:27:67:4D:F8 (Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds  
  
kali@kali: ~  
$
```

Now we have to access the Wazuh machine via SSH.

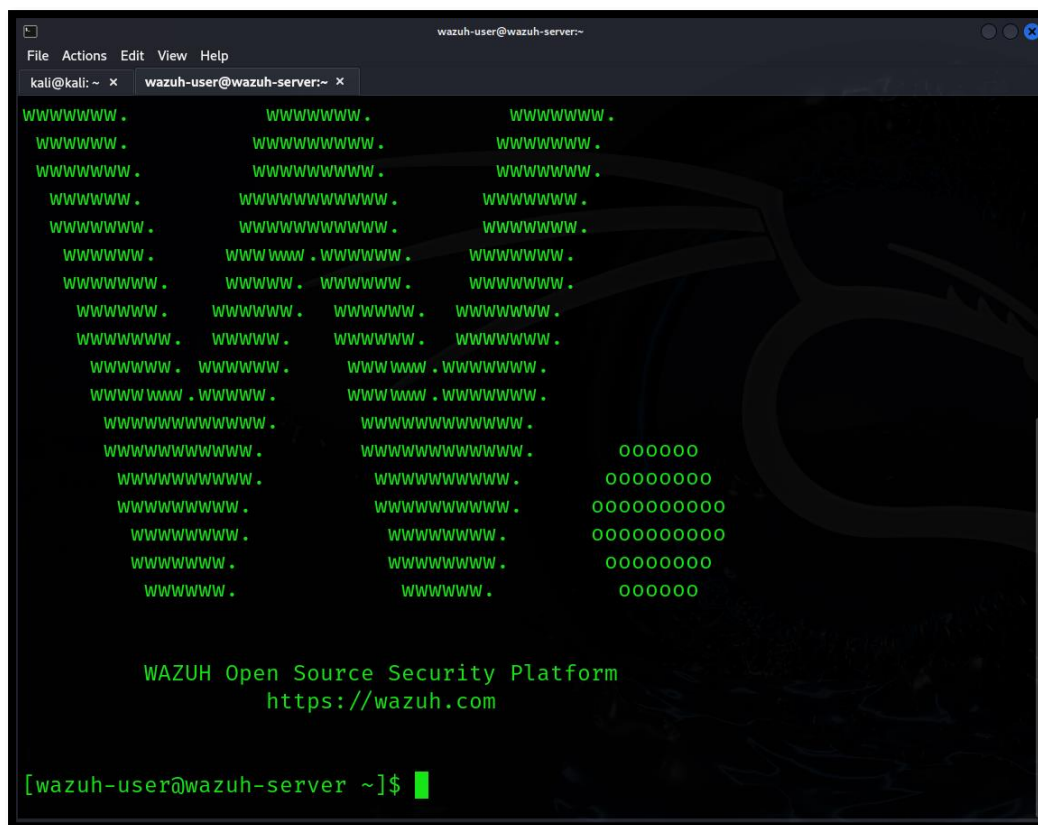
Command: `ssh wazuh-user@192.168.100.9`

Accept the connection with “Yes” and enter the Wazuh password.

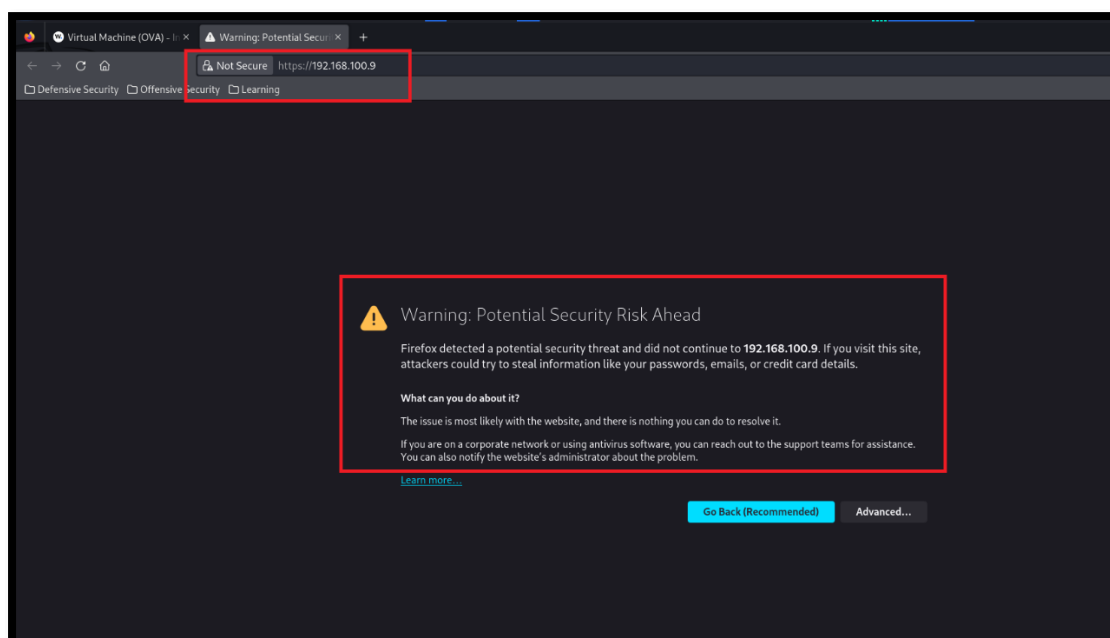


```
kali@kali: ~  
$ ssh wazuh-user@192.168.100.9 ←  
The authenticity of host '192.168.100.9 (192.168.100.9)' can't be established.  
ECDSA key fingerprint is SHA256:r9eJRrxYuLMuFq1HokQ0msKm028Gua0ezl+FA2DJB9U.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:4: [hashed name]  
  ~/.ssh/known_hosts:6: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.100.9' (ECDSA) to the list of known hosts.  
wazuh-user@192.168.100.9's password: █
```

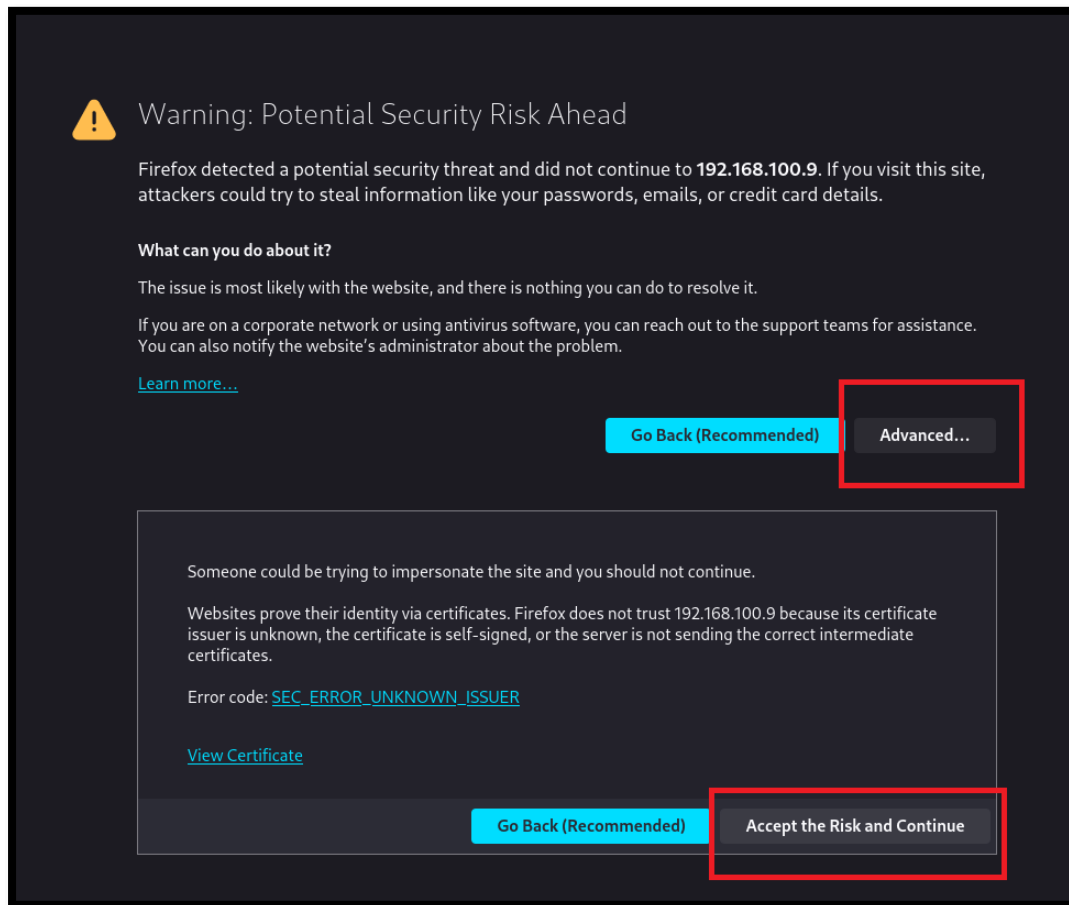
Now we successfully login via SSH, we can edit or modify configuration via SSH Connection (Recommended)



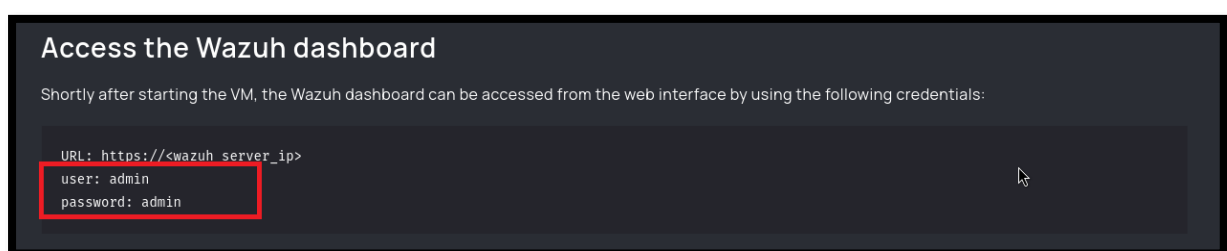
Now it's time to access Wazuh Dashboard form any browser. Type the IP Address of Wazuh in URL bar.



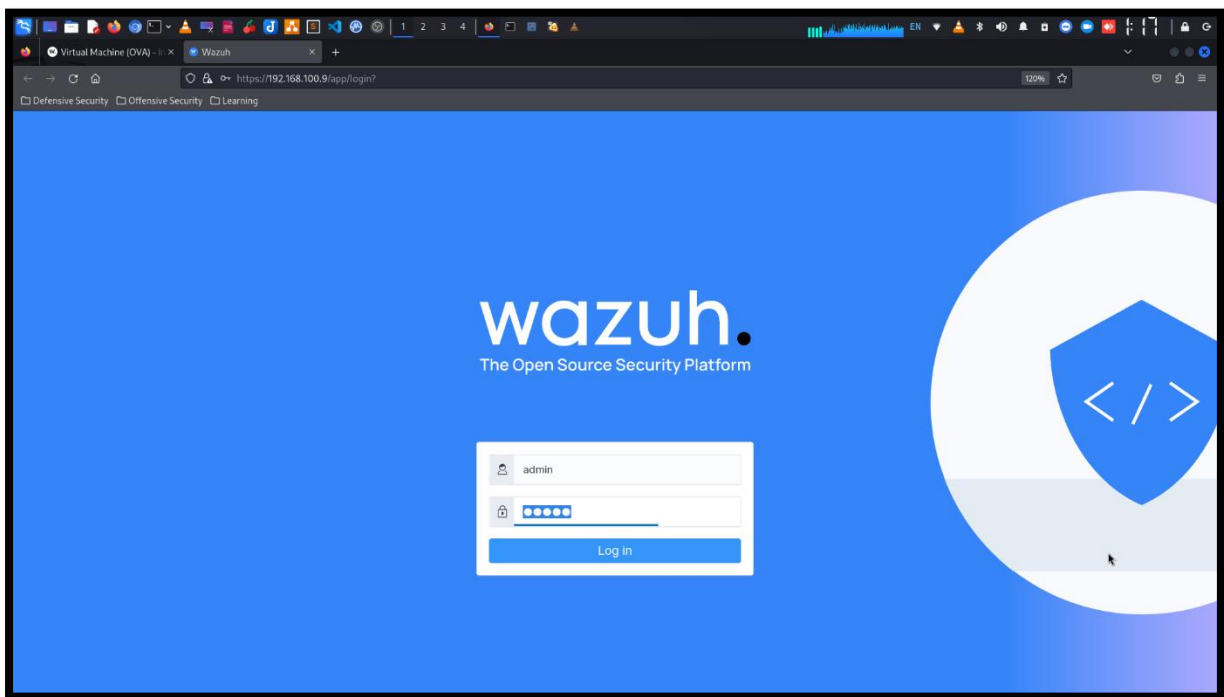
It's showed some security warning, click on Advanced and then click on "Accept the Risk and Continue"



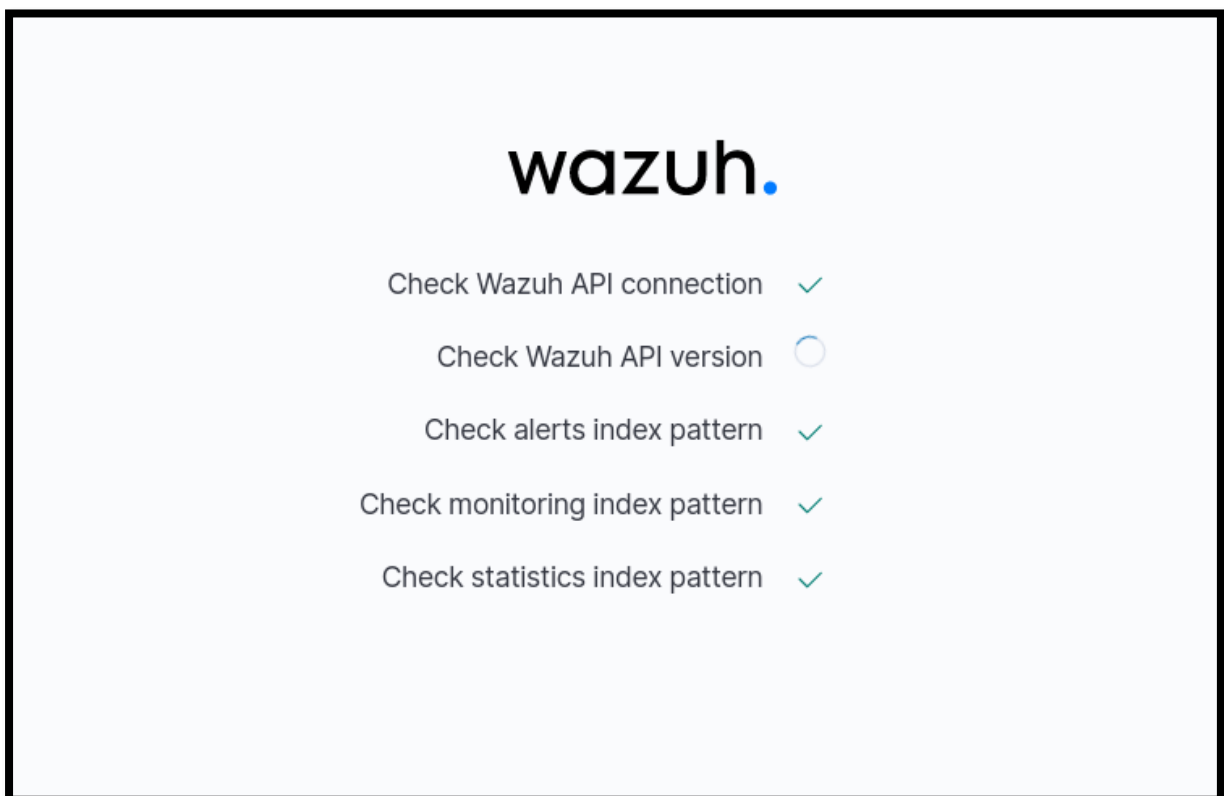
Here is we need credentials for accessing Wazuh Dashboard. It's available on Wazuh Official Website.



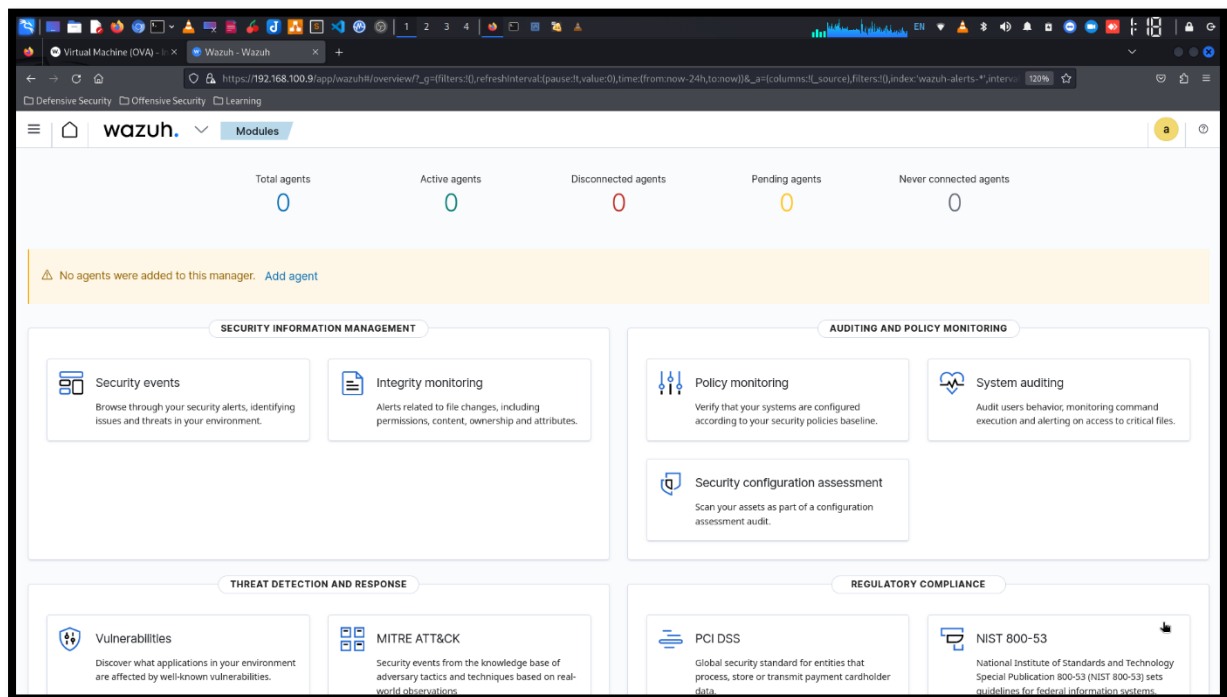
Entering the credentials and login.



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.