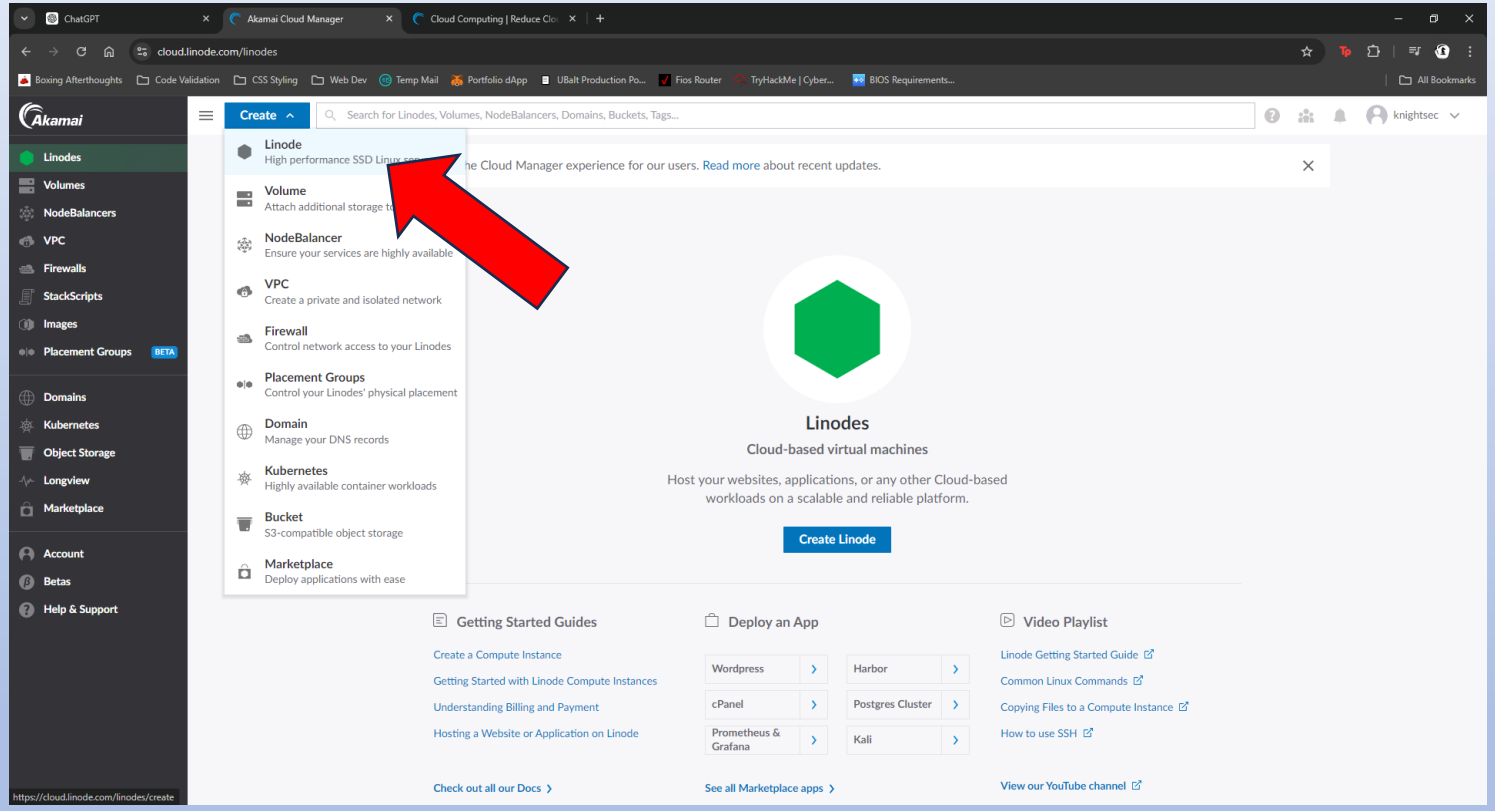
SIEM Home Lab

By: Miguel Denis

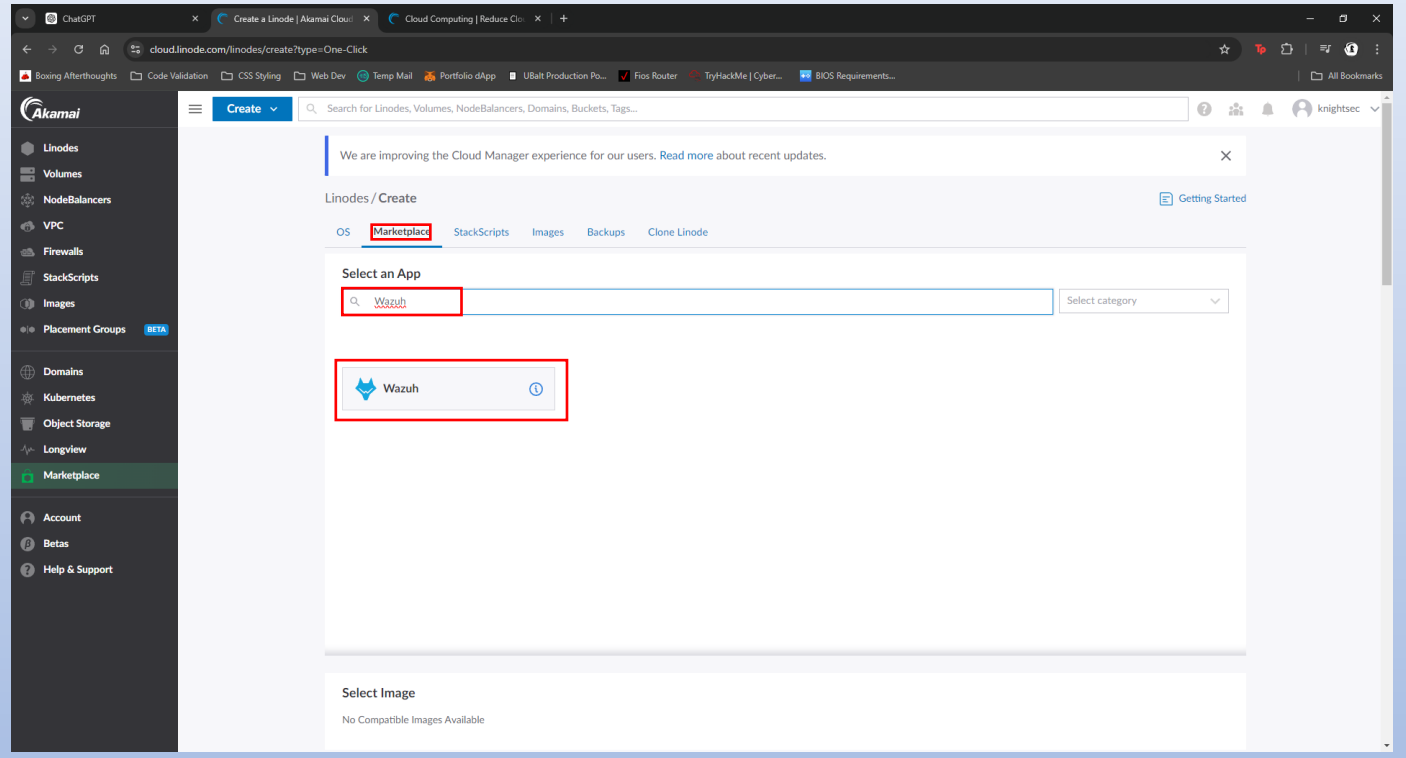
Create Linode Cloud Server

- Sign up for Linode
- At the home screen click Create
- In the drop down menu click Linode



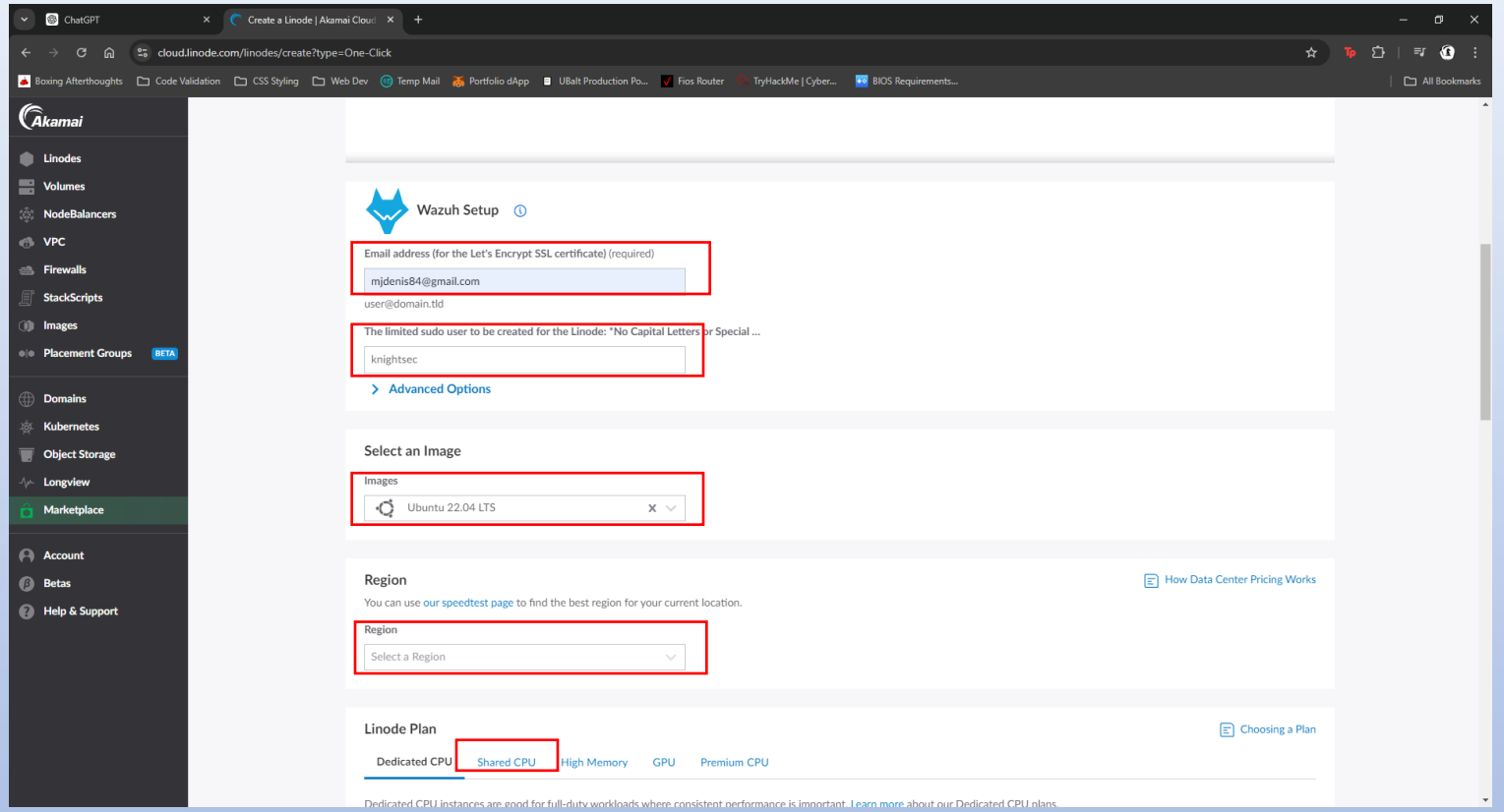
Add Wazuh

- Click On Marketplace
- Click in the search bar
- Type Wazuh
- Click on the Wazuh Icon



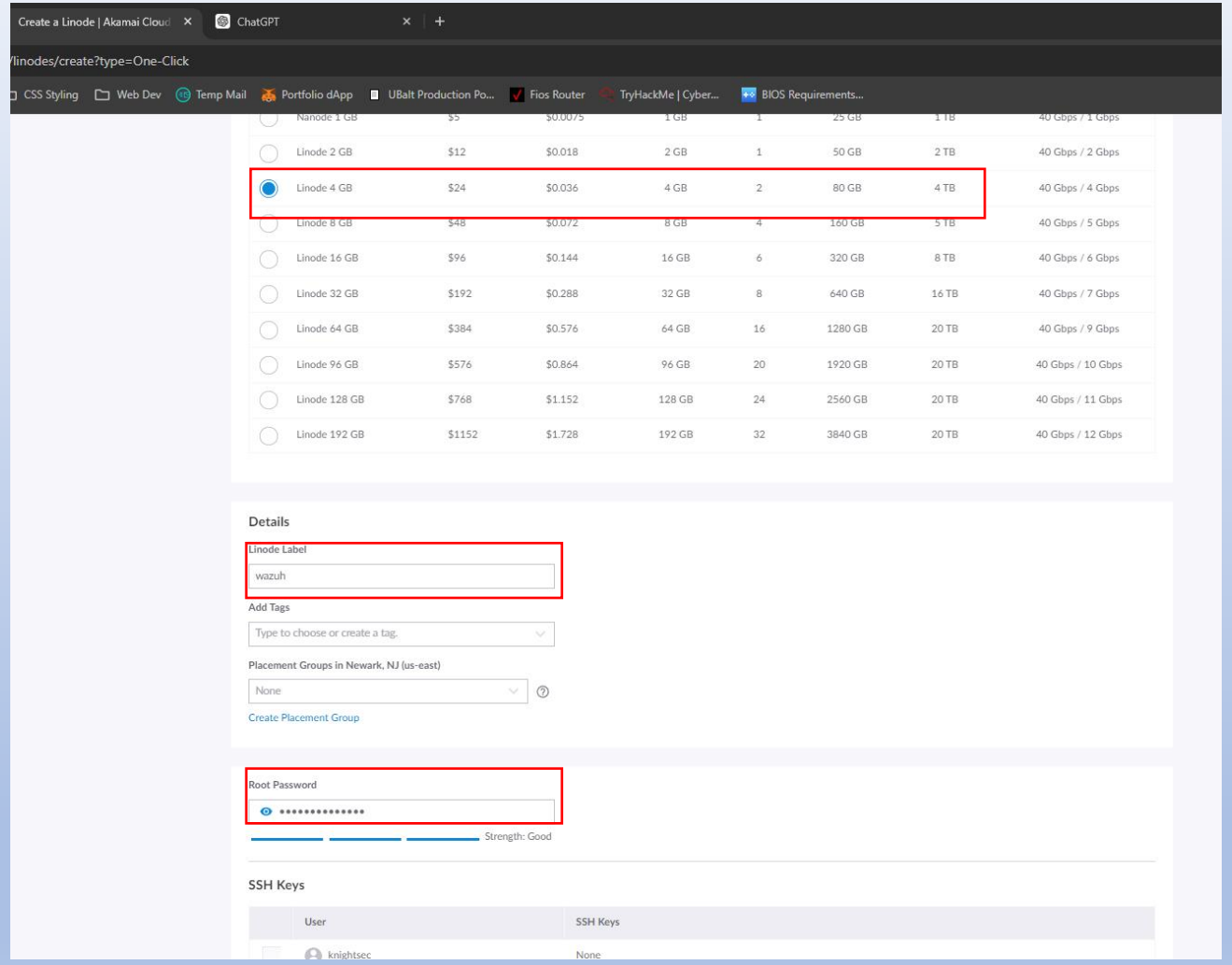
Setup cont.

- Enter your email for your SSL Cert
- Enter your sudo user name
- Select your image type. Here we will use Ubuntu
- Select a region near your location
- Click on Shared CPU under Linode Plan



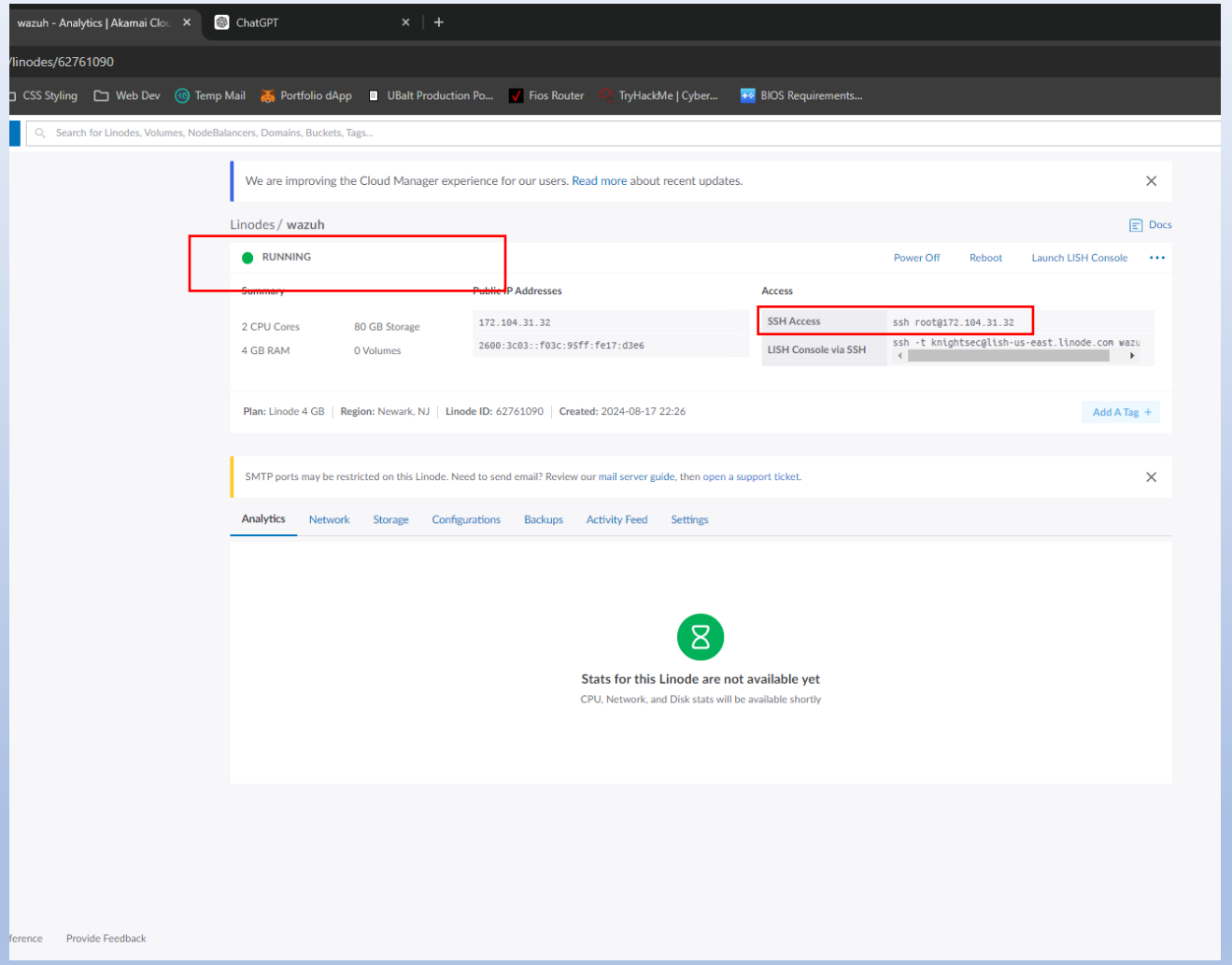
Setup cont.

- Choose your plan, for this lab I chose the 8 GB plan because Wazuh needs these as a minimum system requirement
- Choose a Linode Lable and enter it in the box
- Set a root password
- Click Create Linode at the bottom right of the page



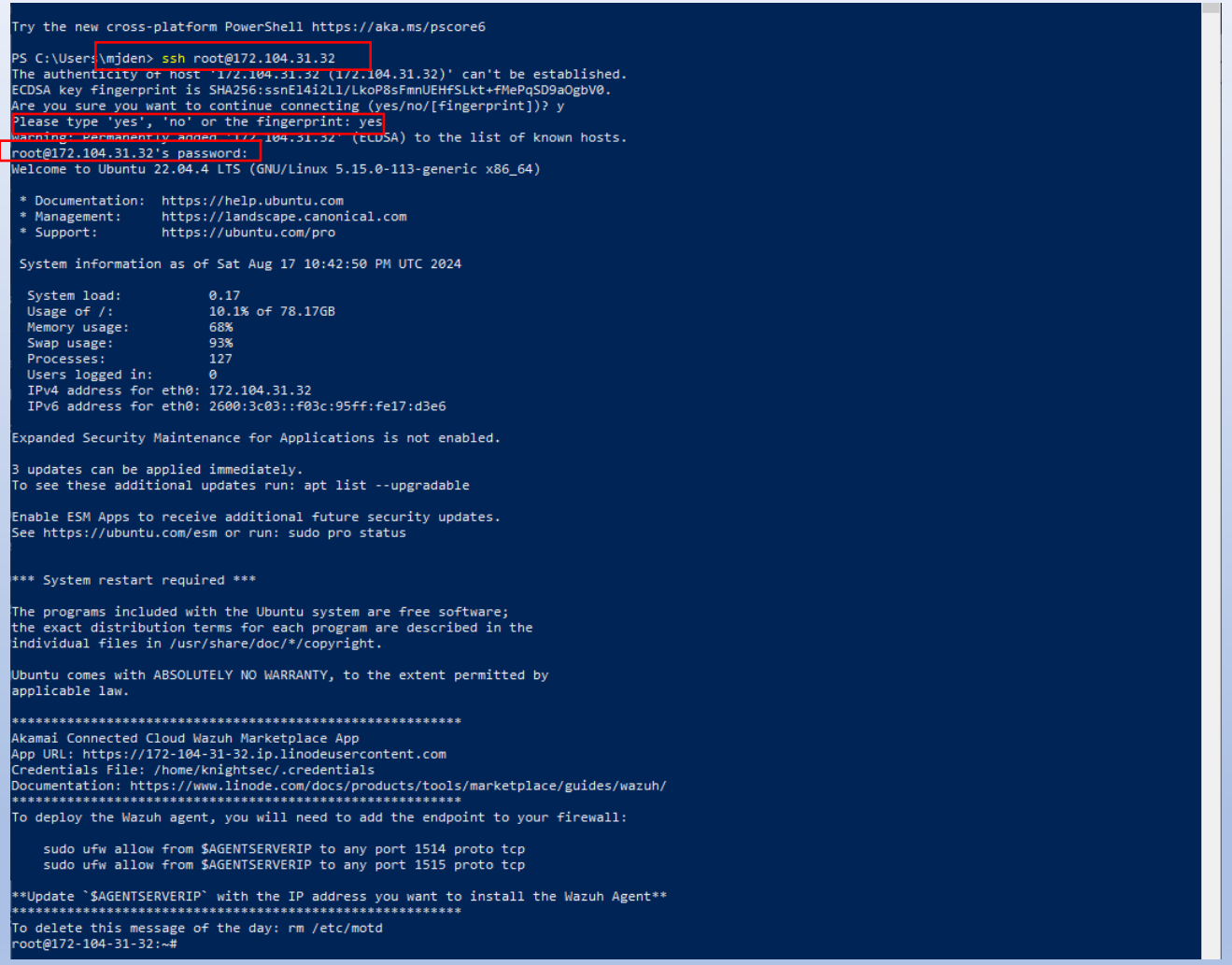
Wazuh Install

- Wazuh will automatically install itself. You will know it is finished when you see the circle turn green and say, “Running”
- Copy your SSH access command so you can connect using your terminal



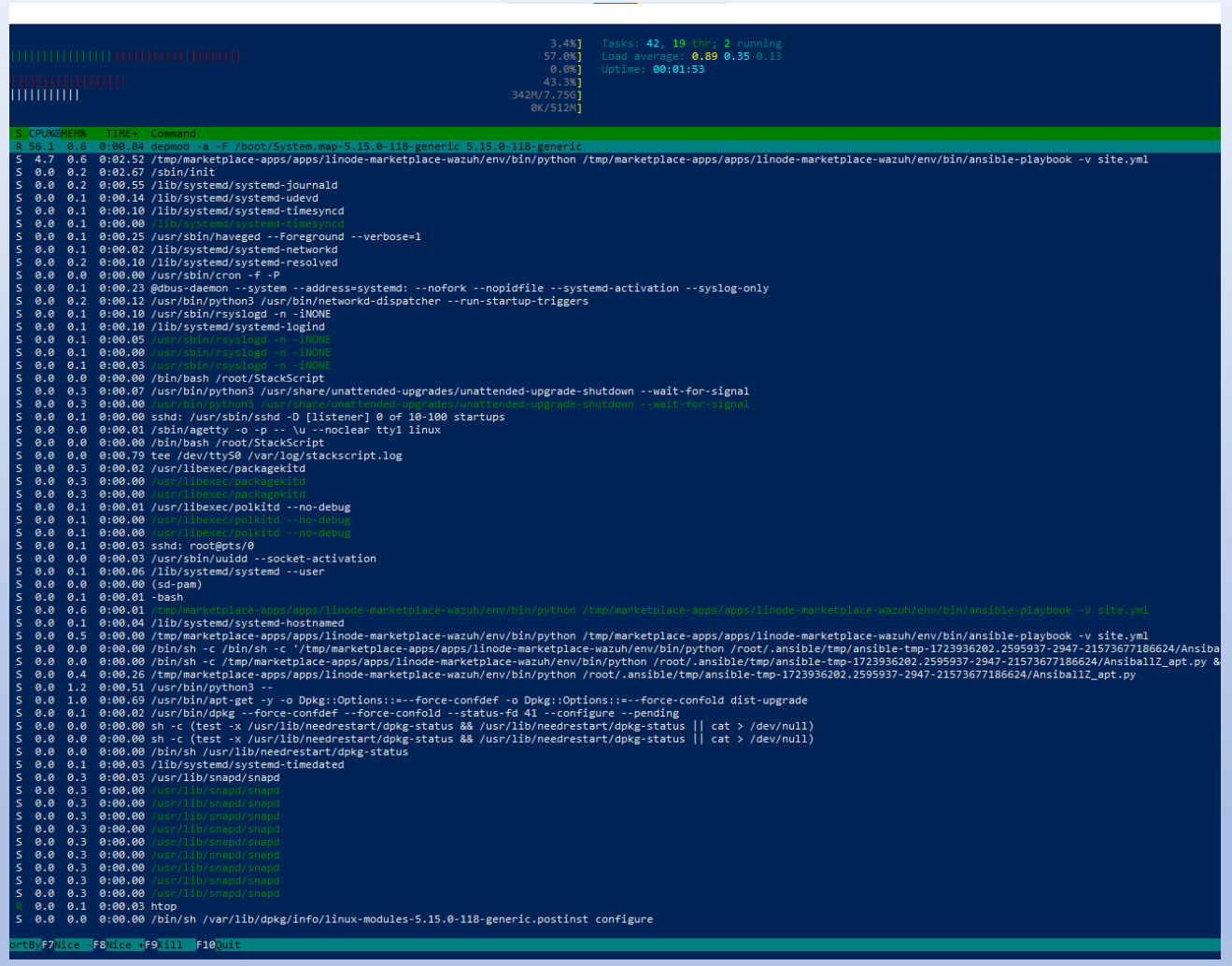
SSH

- SSH into your Wazuh Server using the SSH command you just copied
- Enter yes to connect
- Enter your root password you just set



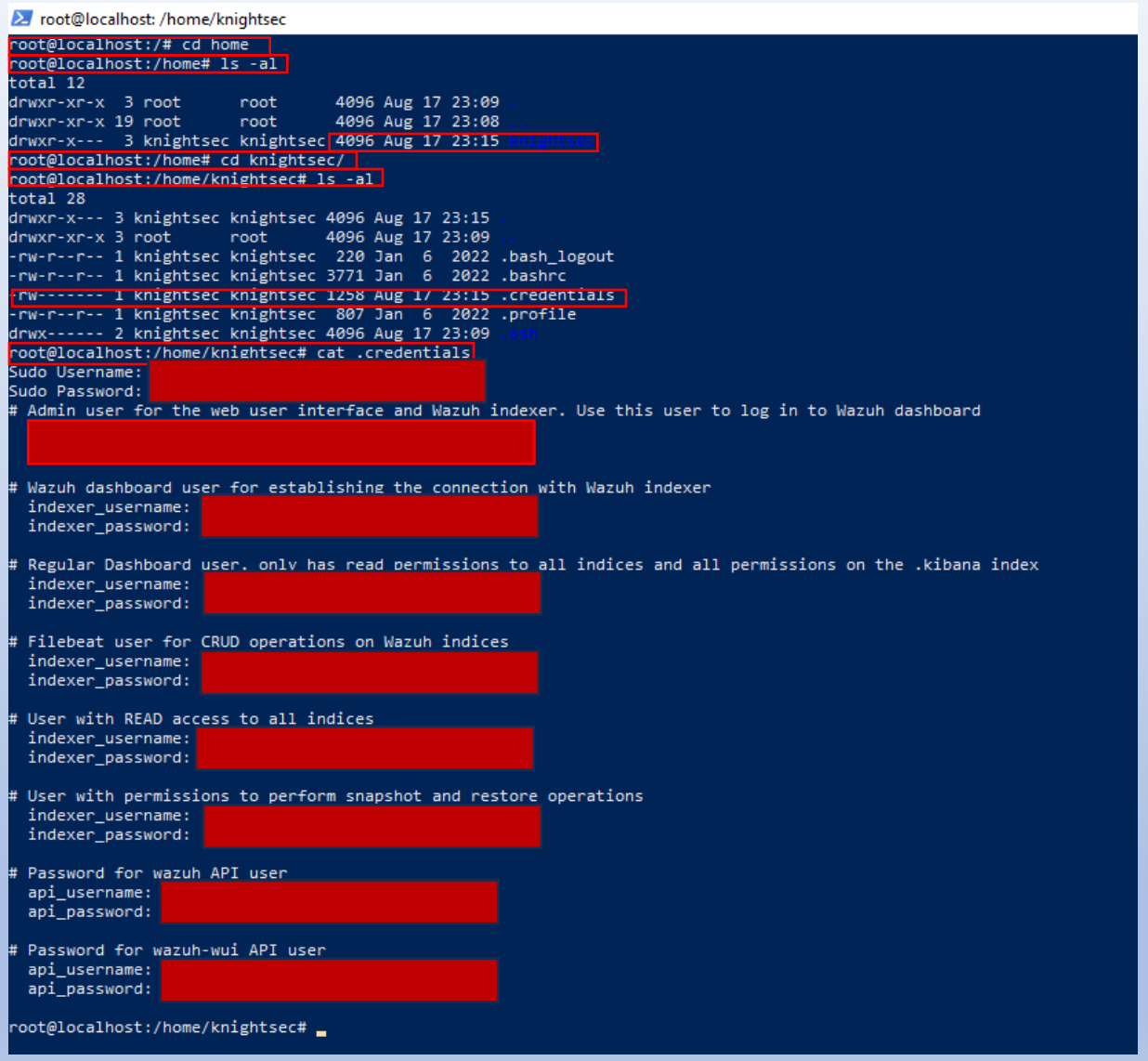
Install Wazuh

- It takes Wazuh a little while to install
- Using the command, htop, you can monitor the install



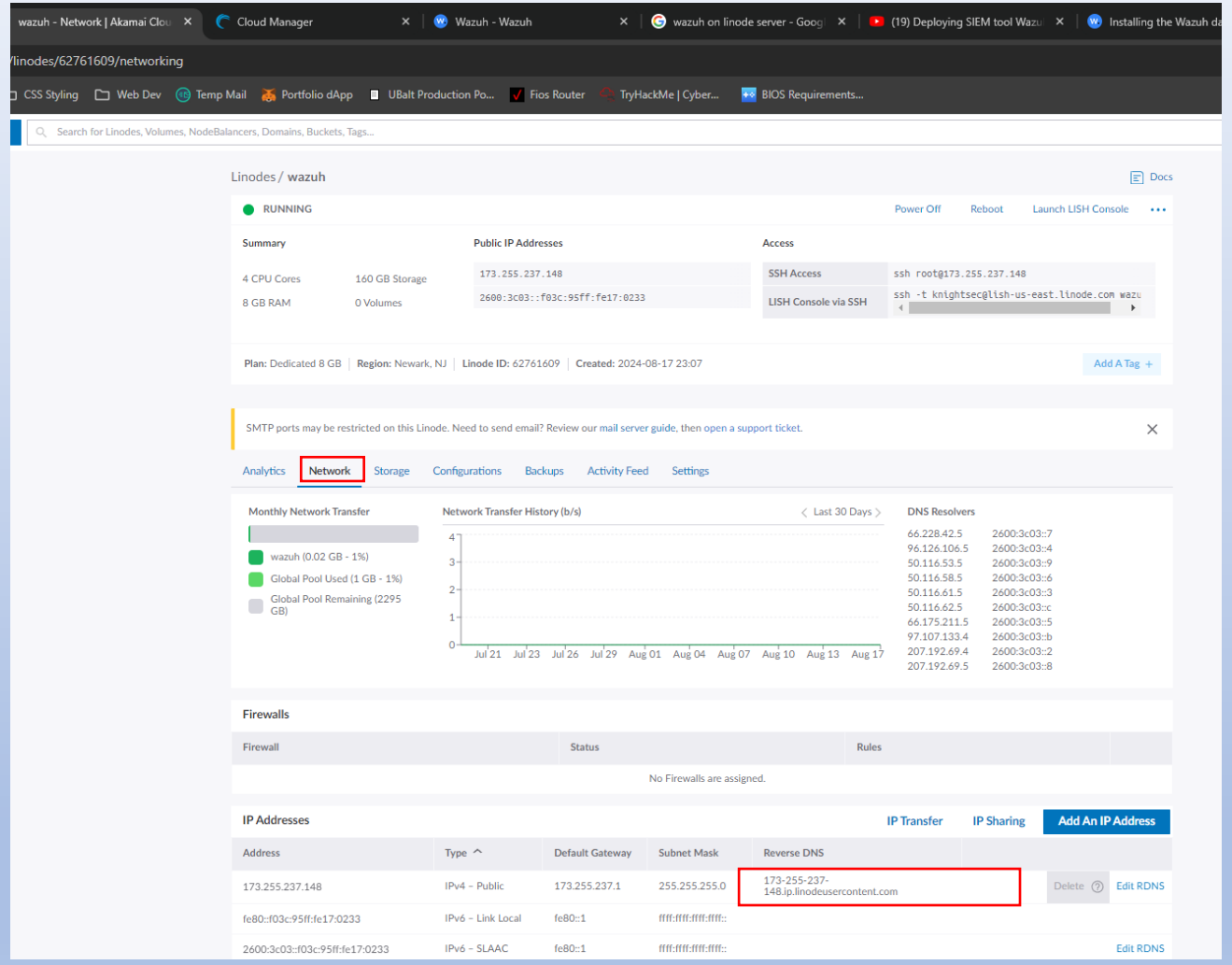
Admin password for Wazuh

- Your credentials are not at your root directory, so we have to locate them
- Change your directory one step back by using the command, cd ..
- Then change your directory to home by using, cd home
- List the files in that directory with, ls –al
- Take note of your user name folder and change your directory into that by typing, cd knightsec (or whatever your user name is)
- List the files in your directory with, ls –al
- Print the .credentials file with the following command, cat .credentials
- Copy your admin password to your clipboard



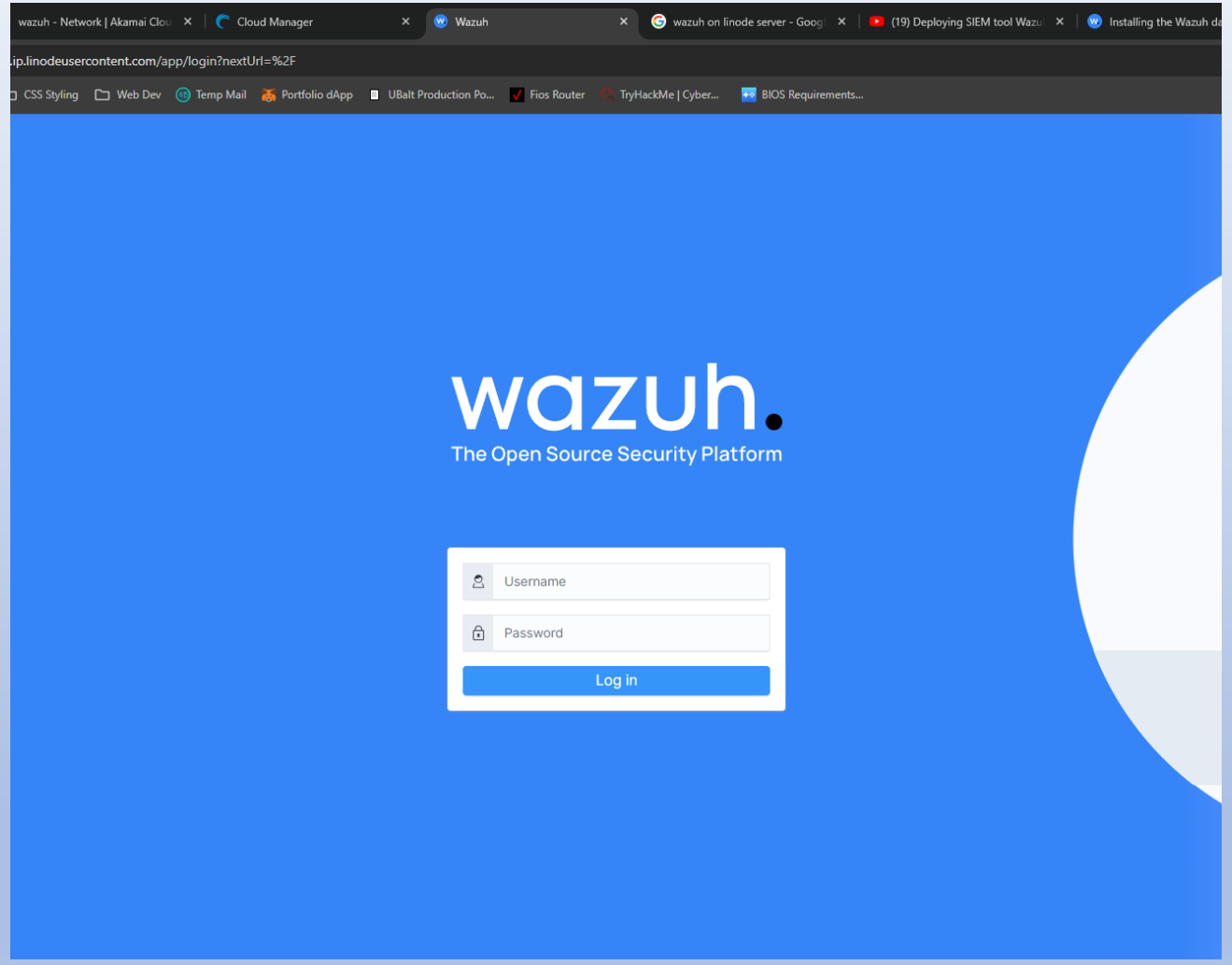
Obtaining Dashboard URL

- On your Linode page click on your Network tab
- At the bottom of that page copy your Reverse DNS



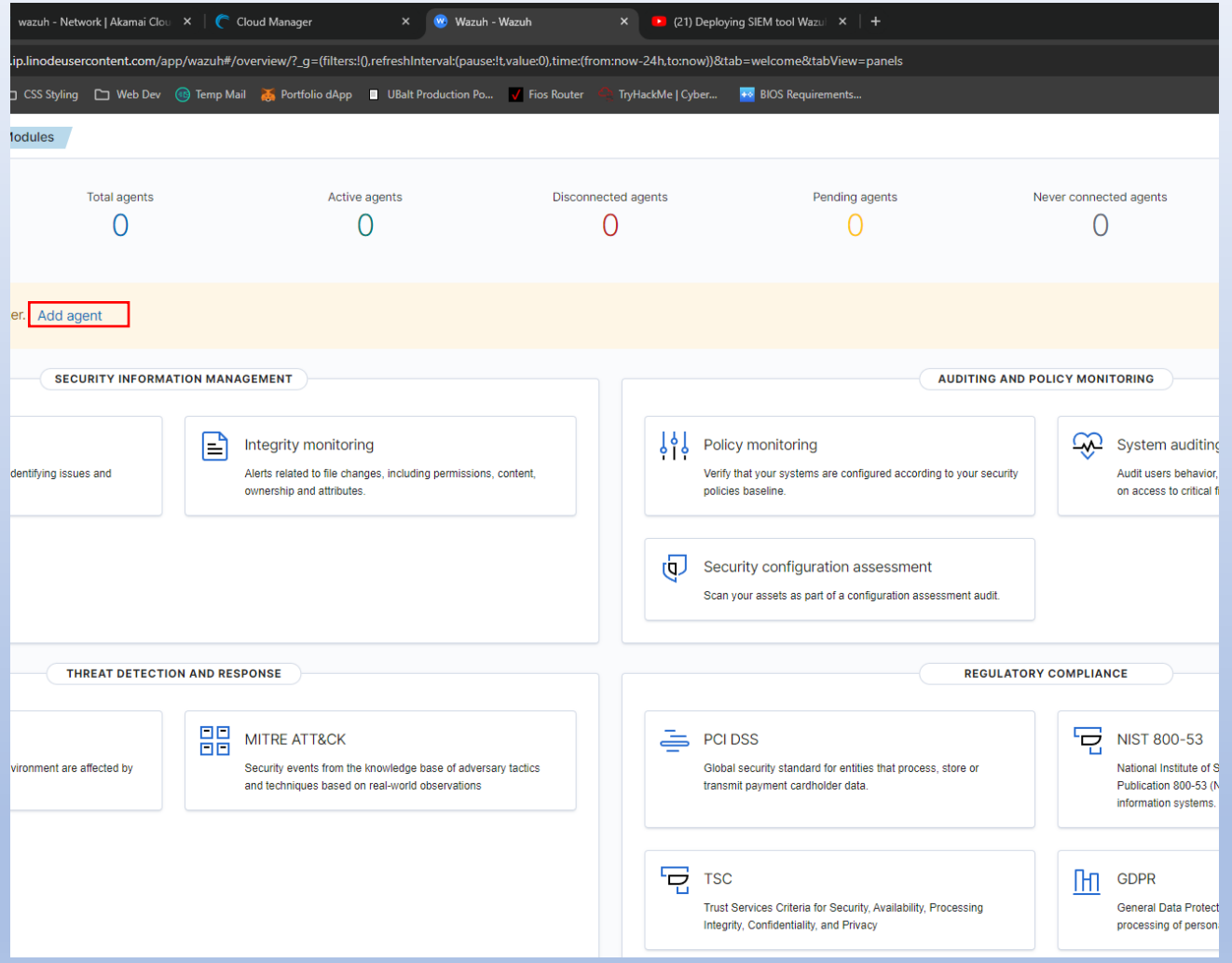
Log into Wazuh

- Paste the reverse DNS you just copied into your browser and it should direct you to a page like the one in the photo
- Enter the credentials you copied from your Powershell
- The user name is admin and the password you should have in your PowerShell SSH log



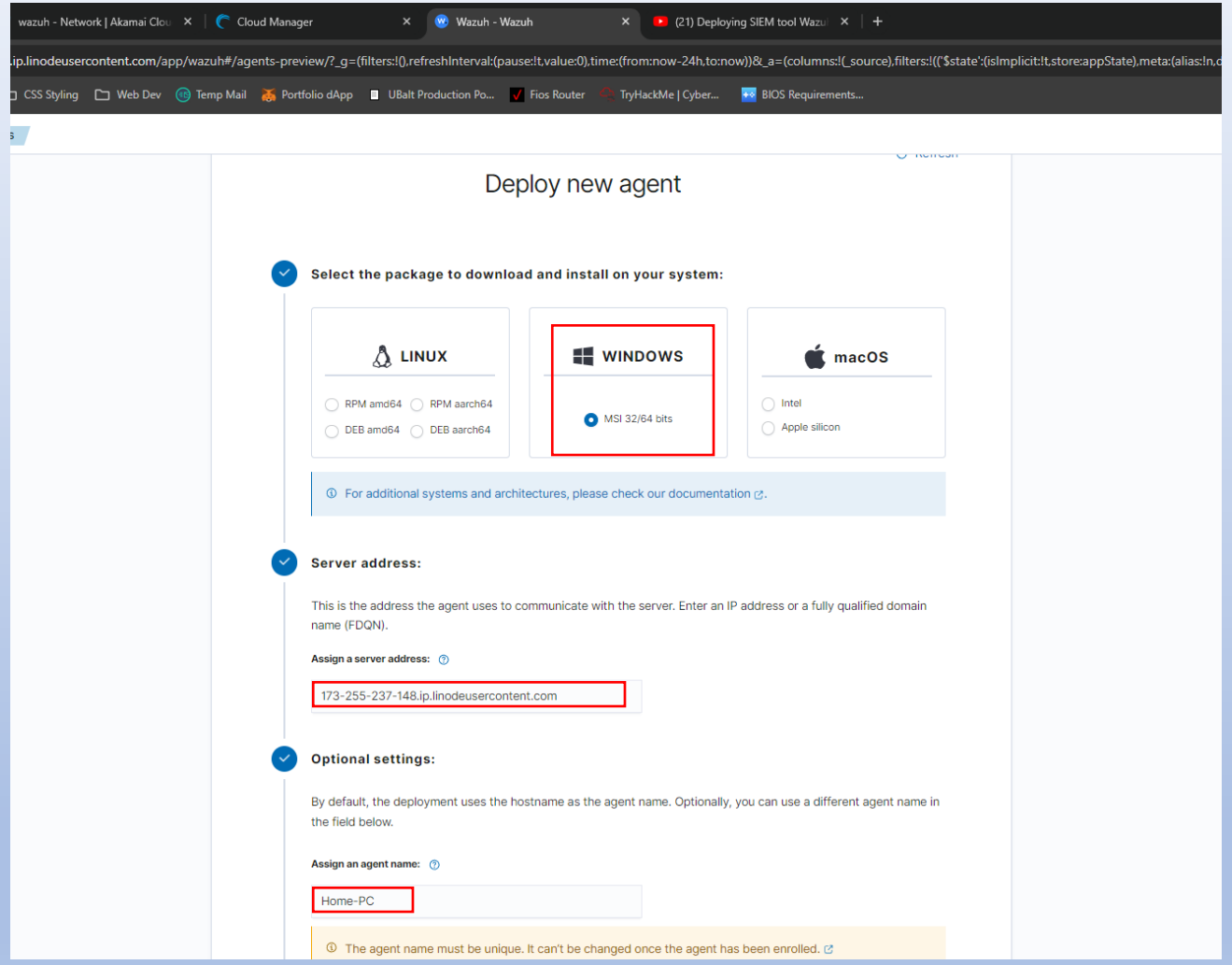
Wazuh Home Page

- Click on Add agent



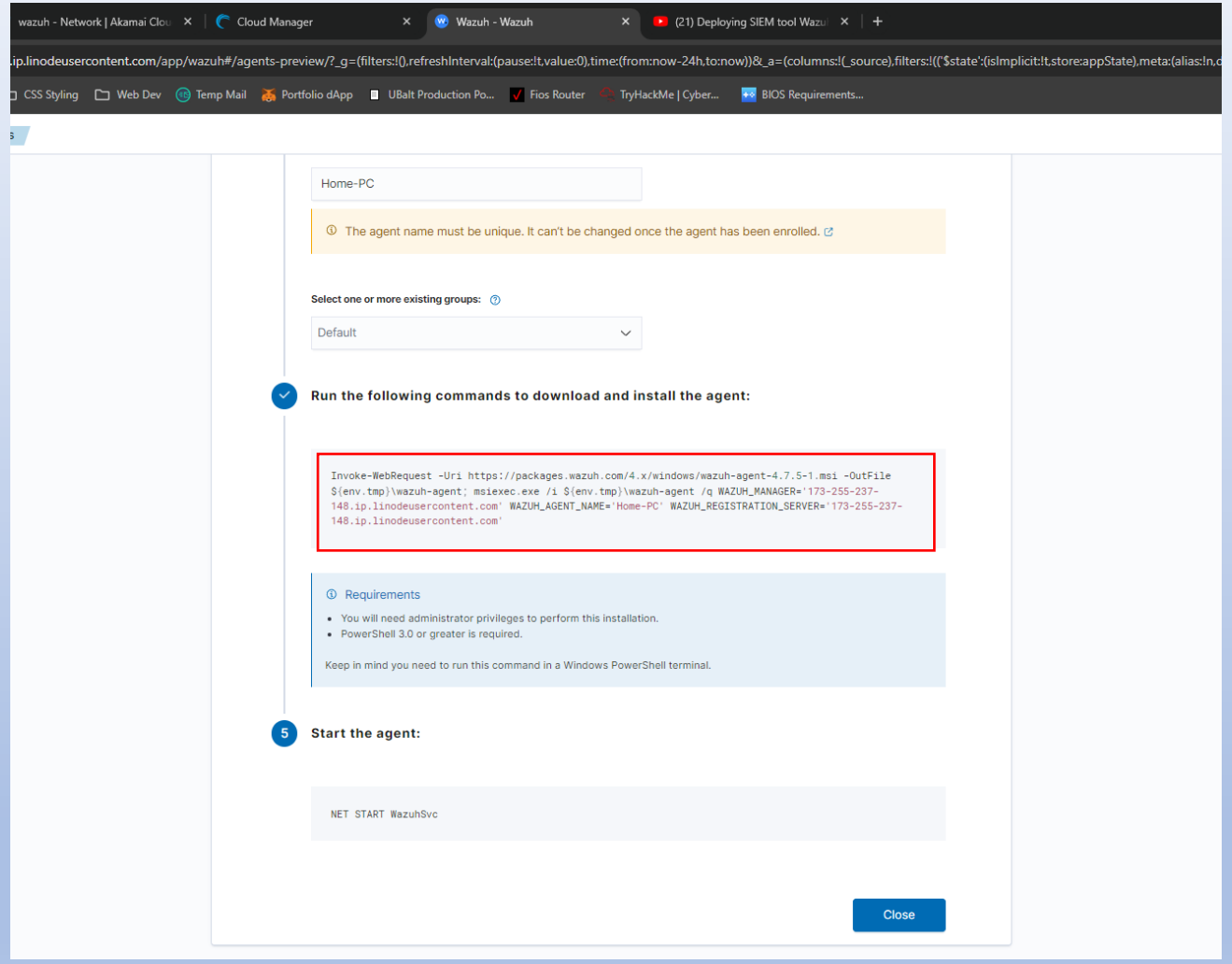
Adding a Windows agent

- Click the Windows button to deploy your new agent
- Your server address will be your Wazuh Reverse DNS server address you copied earlier
- Name your Agent



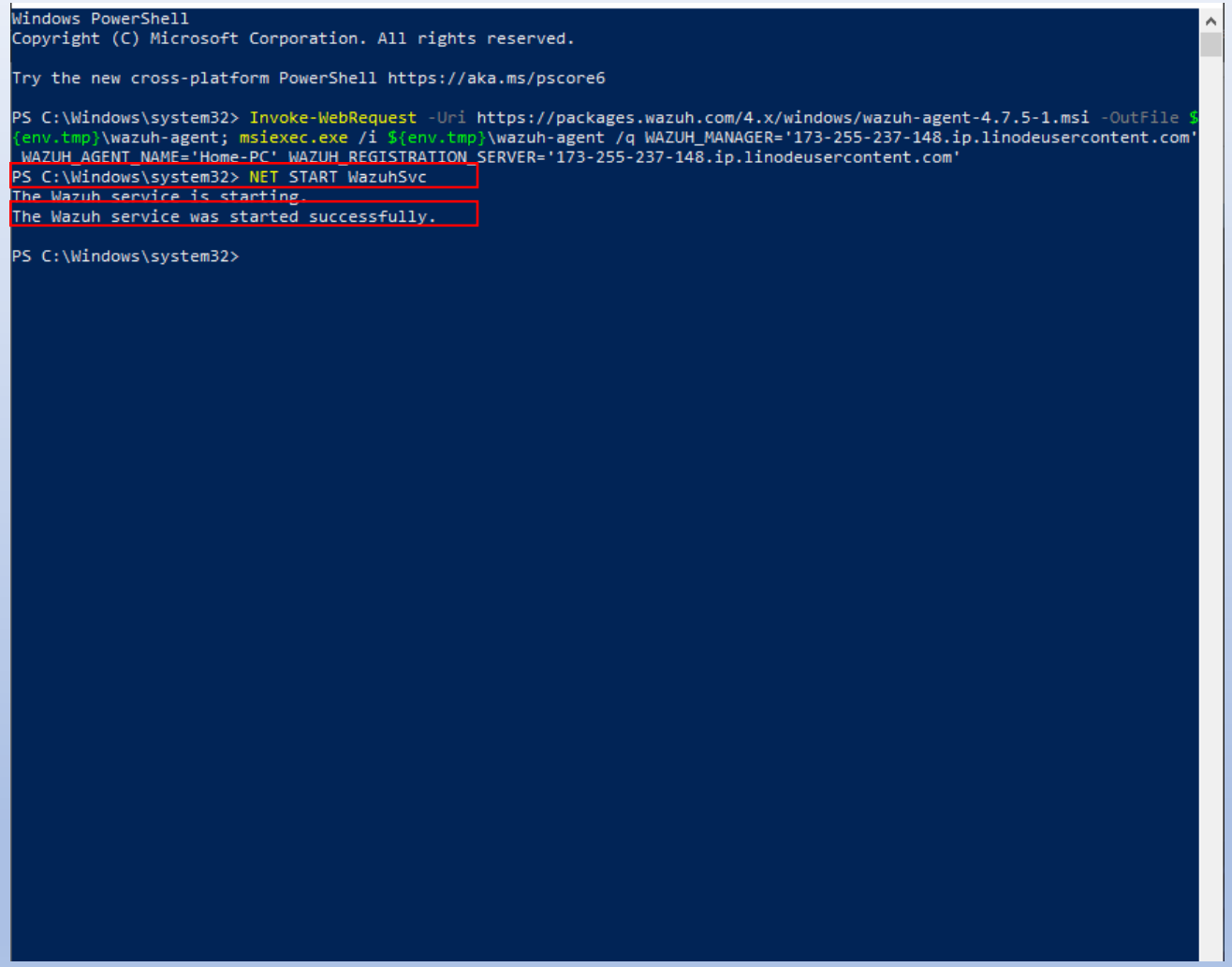
Adding a Windows agent cont.

- Under, “Run the following commands to download and install the agent” copy that code to your clipboard



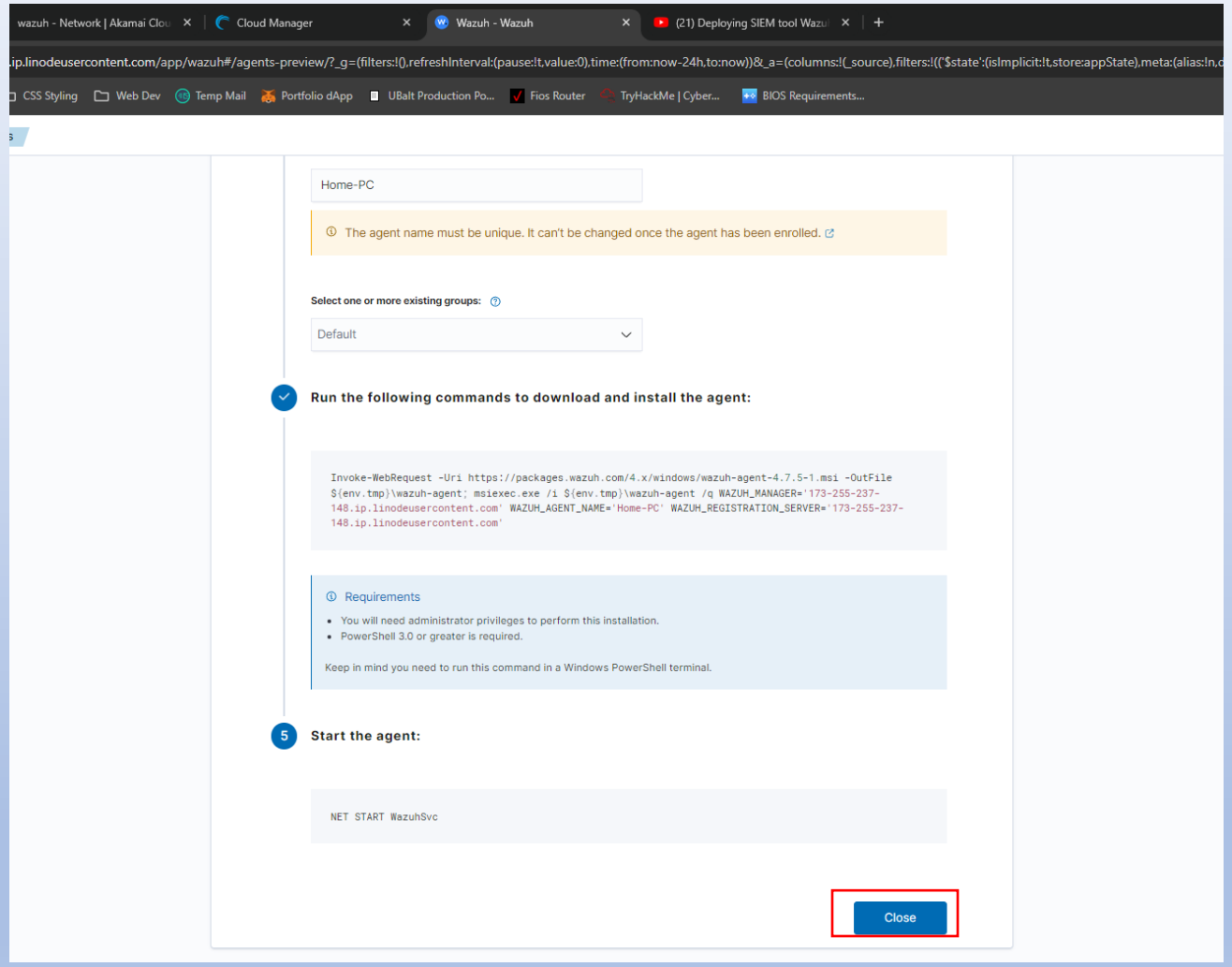
Adding a Windows agent cont.

- Open PowerShell on your Windows machine with administrator privileges
- Paste the code you just copied from the Wazuh agent deployment page and hit enter
- After that runs enter the following:
  - NET START WazuhSvc
- You should receive a successful startup notification



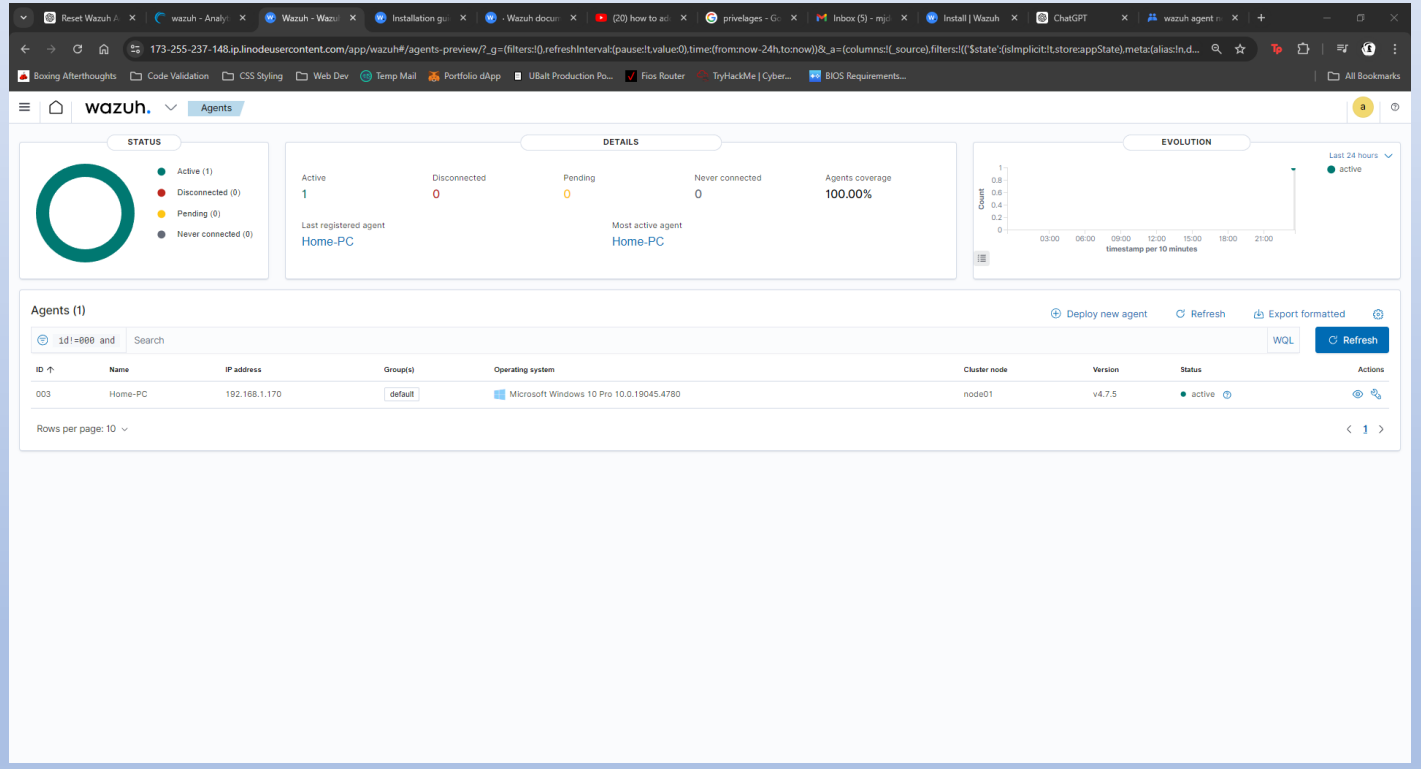
Adding a Windows agent cont.

- Close out the agent deployment by clicking the bottom close button



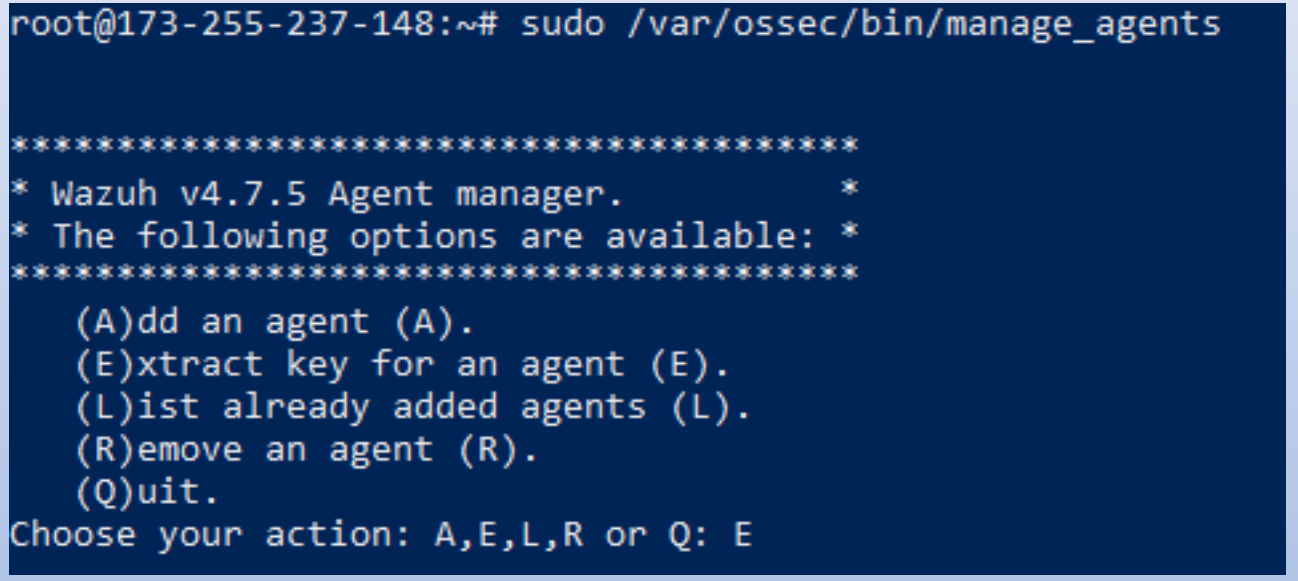
Agents

- This is how your agents should show up
- Troubleshooting tips for Windows machines:
  - You may need to manually add your agent through the Wazuh Ubuntu server



Troubleshooting Adding Agent

- If your agent does not show up on your dashboard you may have to manually add the agent using the following command:
  - sudo /var/ossec/bin/manage_agents
- You will do the following:
  - Add an agent
  - Put in the IP address of the agent you are adding

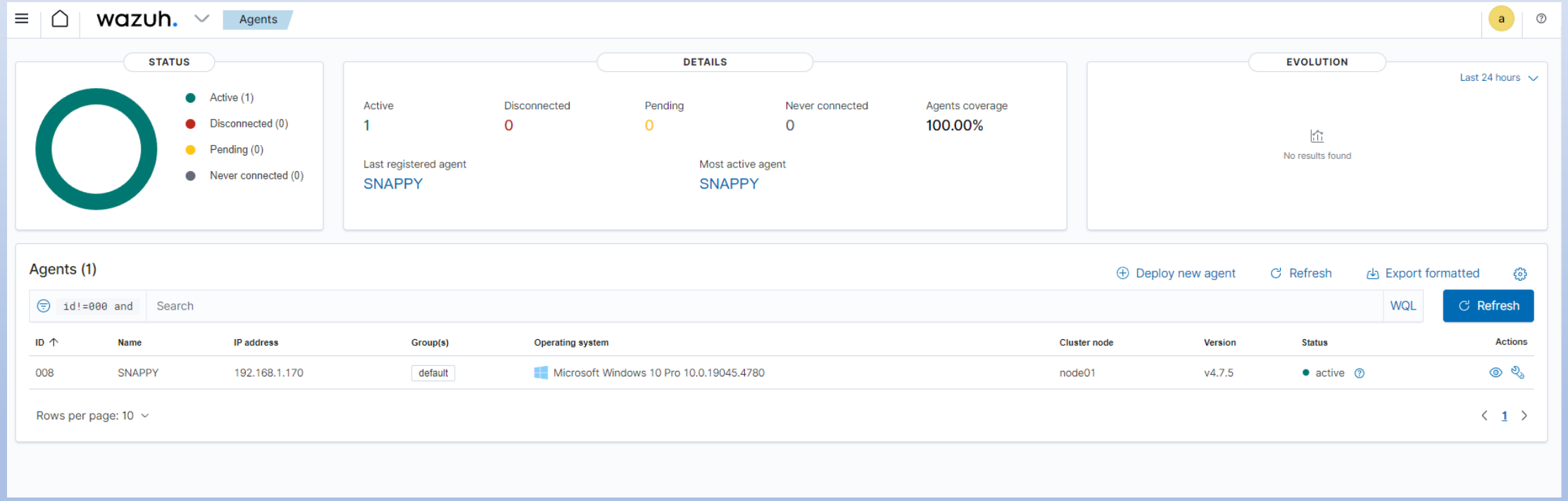


Firewall Issues

- Sometimes your firewall may not be allowing traffic for port 1514/tcp. You must enable this for your agent to connect. First, check your firewall settings on your Wazuh Manager using the following command:
  - sudo ufw status
- You will see something like the photo on the right
- If you do not see 1514/tcp enter the following command to open that port:
  - Sudo ufw allow 1514/tcp

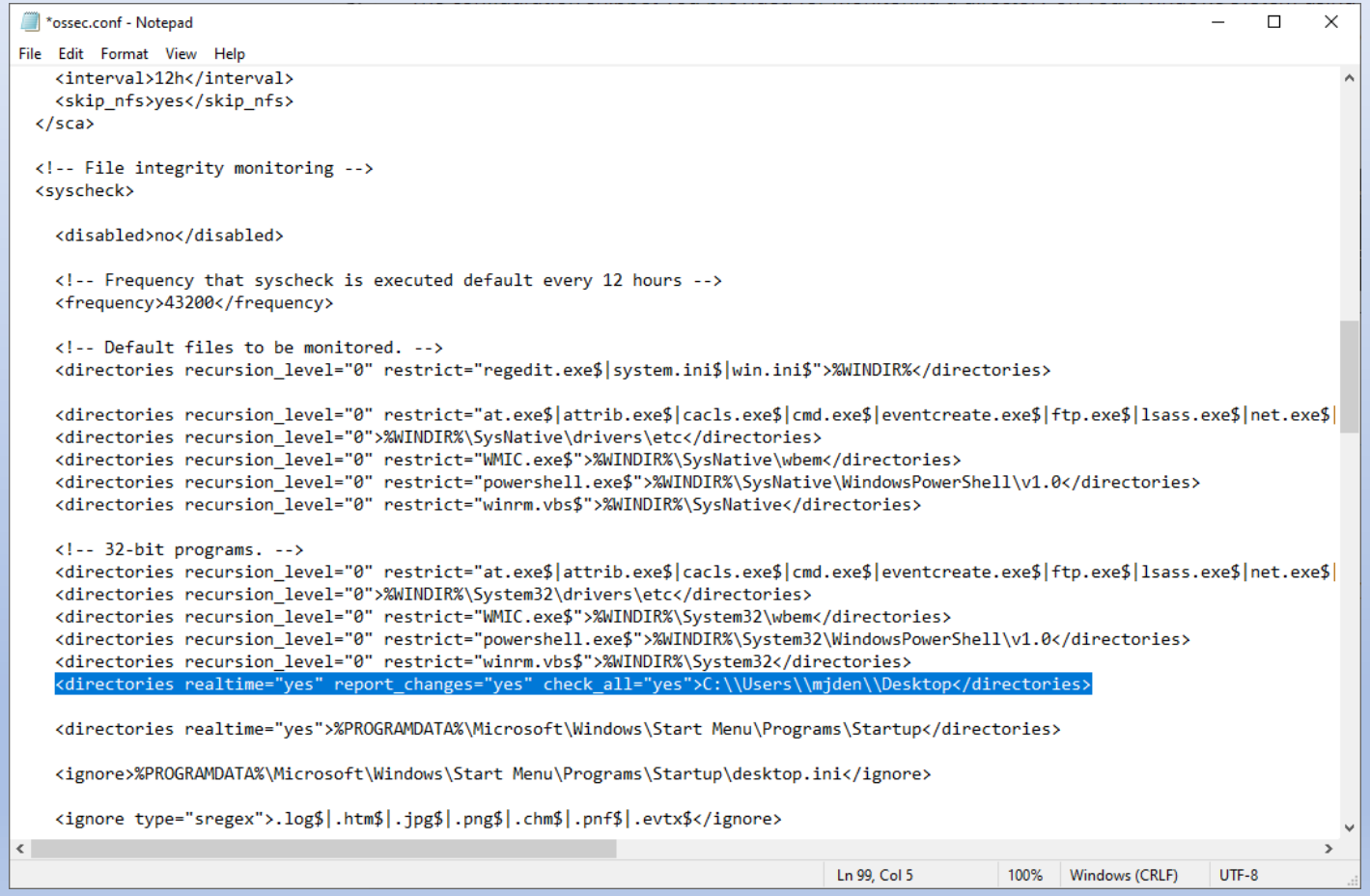
```
sudo ufw allow 1514/tcp
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
1514/udp                   ALLOW       Anywhere
1515/tcp                   ALLOW       Anywhere
1515/udp                   ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
1514/udp (v6)              ALLOW       Anywhere (v6)
1515/tcp (v6)              ALLOW       Anywhere (v6)
1515/udp (v6)              ALLOW       Anywhere (v6)
```

Agent Dashboard



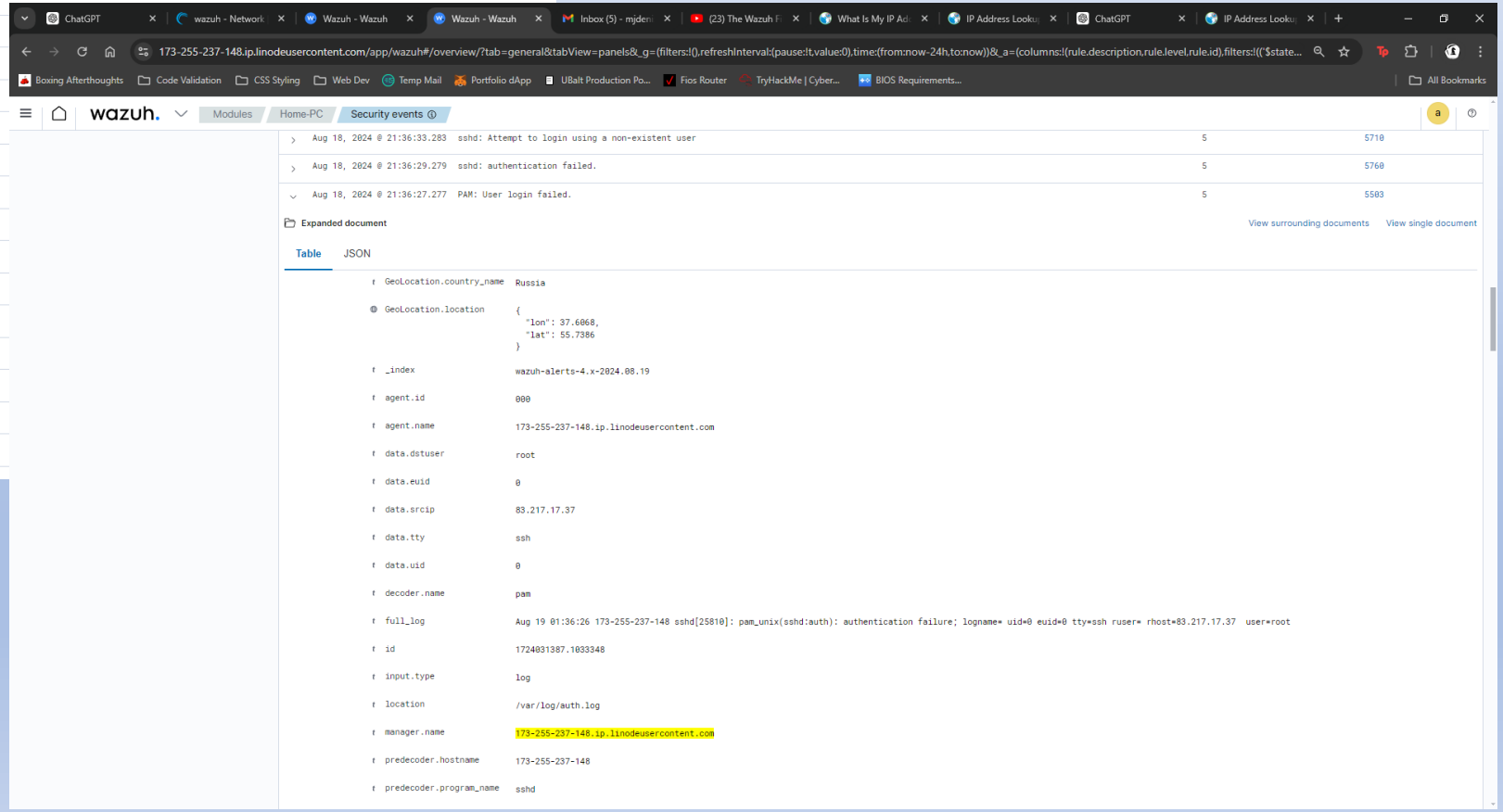
Setting up Alerts

- Navigate to your ossec.conf file and open it with notepad
- Add the following text in the directories section (Windows systems need double back slashes on their file paths):
  - <directories realtime="yes" report_changes="yes" check_all="yes">C:\\Users\\mjden\\Desktop</directories>
- Save the file.
- Note: you need admin privileges to do this
- Restart your Wazuh Service



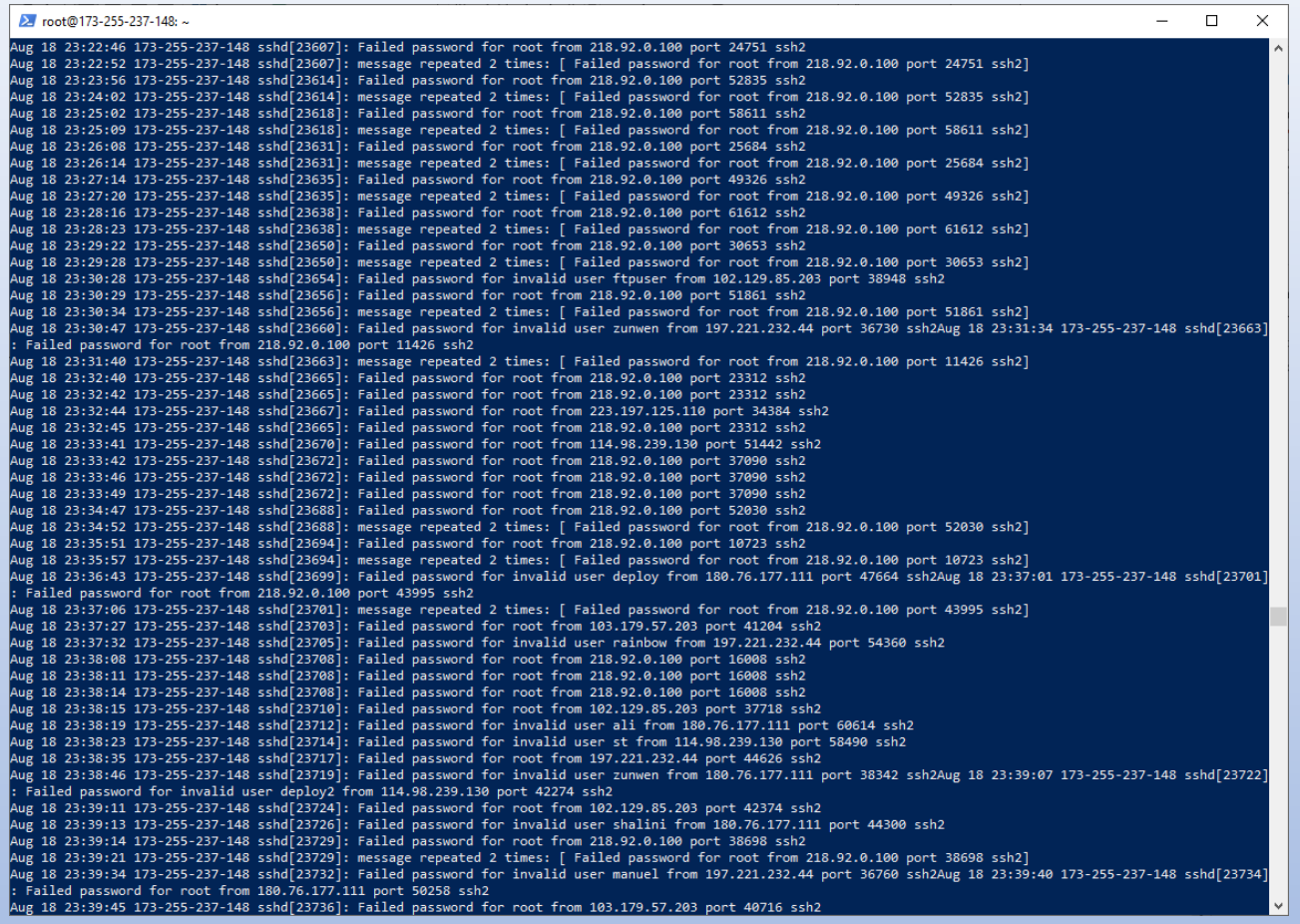
I was brute forced attacked!

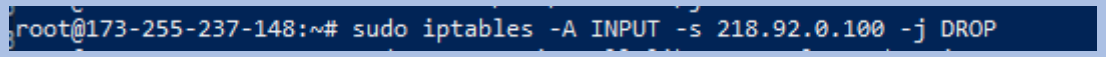
Aug 18, 2024 @ 21:34:05.132	sshd: authentication failed.	5	5760
Aug 18, 2024 @ 21:34:03.130	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:41.107	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:39.105	sshd: brute force trying to get access to the system. Non existent user.	10	5712
Aug 18, 2024 @ 21:33:37.103	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:37.103	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:33.099	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:33.099	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:29.095	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:29.095	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:29.095	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:27.093	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:27.093	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:19.084	sshd: authentication failed.	5	5760
Aug 18, 2024 @ 21:33:15.082	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:07.074	sshd: Attempt to login using a non-existent user	5	5710



Dropping the attacking IP address

- I noticed the dashboard telling me about the failed login attempts and SSH'd into my Wazuh Server. I then typed:
  - sudo grep "Failed password" /var/log/auth.log
- The logs showed hundreds of failed login attempts from IP address 218.92.0.100
- I blocked the IP address of the attacker using the following:
  - Sudo iptables –A INPUT –s 218.92.0.100 –j DROP





How I resolved the attack

- I had to act immediately and install google authenticator to enable 2 factor authentication using the following command:
  - sudo apt-get install libpam-google-authenticator

```
root@173-255-237-148:~# sudo apt-get install libpam-google-authenticator
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libqrencode4
The following NEW packages will be installed:
  libpam-google-authenticator libqrencode4
0 upgraded, 2 newly installed, 0 to remove and 3 not upgraded.
Need to get 69.7 kB of archives.
After this operation, 205 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrors.linode.com/ubuntu jammy/universe amd64 libqrencode4 amd64 4.1.1-1 [24.0 kB]
Get:2 http://mirrors.linode.com/ubuntu jammy/universe amd64 libpam-google-authenticator amd64 20191231-2 [45.7 kB]
Fetched 69.7 kB in 0s (318 kB/s)
Selecting previously unselected package libqrencode4:amd64.
(Reading database ... 239467 files and directories currently installed.)
Preparing to unpack .../libqrencode4_4.1.1-1_amd64.deb ...
Unpacking libqrencode4:amd64 (4.1.1-1) ...
Selecting previously unselected package libpam-google-authenticator.
Preparing to unpack .../libpam-google-authenticator_20191231-2_amd64.deb ...
Unpacking libpam-google-authenticator (20191231-2) ...
Setting up libqrencode4:amd64 (4.1.1-1) ...
Setting up libpam-google-authenticator (20191231-2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@173-255-237-148:~# google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
```

Check if anyone else is logged into my server

- See if there is anyone else logged into my server that I do not recognize by using the following command:
  - who
- I then checked who had established connections with the following command:
  - ss –tuna | grep ‘ESTAB’
- I noticed that I did not recognize IP address
- I had to remove the user I did not recognize using the following command:
  - sudo iptables –A INPUT –s 183.81.169.238 –j DROP

```
root@173-255-237-148:~# who
root     pts/0        2024-08-18 23:44 (71.179.53.234)
root@173-255-237-148:~# ss -tuna | grep 'ESTAB'
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62617
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62600
tcp   ESTAB     0      0         173.255.237.148:80       147.185.133.140:60206
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62590
tcp   ESTAB     0      0               127.0.0.1:52552          127.0.0.1:9200
tcp   ESTAB     0      0               127.0.0.1:56788          127.0.0.1:9200
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62620
tcp   ESTAB     0      0               127.0.0.1:46438          127.0.0.1:9200
tcp   ESTAB     0      184       173.255.237.148:22         71.179.53.234:62314
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62619
tcp   ESTAB     0      0         173.255.237.148:22       183.81.169.238:53138
tcp   ESTAB     0      0         173.255.237.148:1514       71.179.53.234:62181
tcp   ESTAB     0      0               127.0.0.1:48262          127.0.0.1:9200
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62618
tcp   ESTAB     0      0               127.0.0.1:52546          127.0.0.1:9200
tcp   ESTAB     0      0               127.0.0.1:52550          127.0.0.1:9200
tcp   ESTAB     0      0         173.255.237.148:443        71.179.53.234:62594
tcp   ESTAB     0      0               127.0.0.1:56790          127.0.0.1:9200
tcp   ESTAB     0      0               127.0.0.1:48258          127.0.0.1:9200
tcp   ESTAB     0      0               127.0.0.1:45756          127.0.0.1:9200
tcp   ESTAB     0      0               127.0.0.1:48266          127.0.0.1:9200
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:48266
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:46438
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:52552
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:48262
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:52550
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:48258
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:56788
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:52546
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:56790
tcp   ESTAB     0      0          [::ffff:127.0.0.1]:9200  [::ffff:127.0.0.1]:45756
root@173-255-237-148:~# sudo iptables -A INPUT -s 183.81.169.238 -j DROP
```

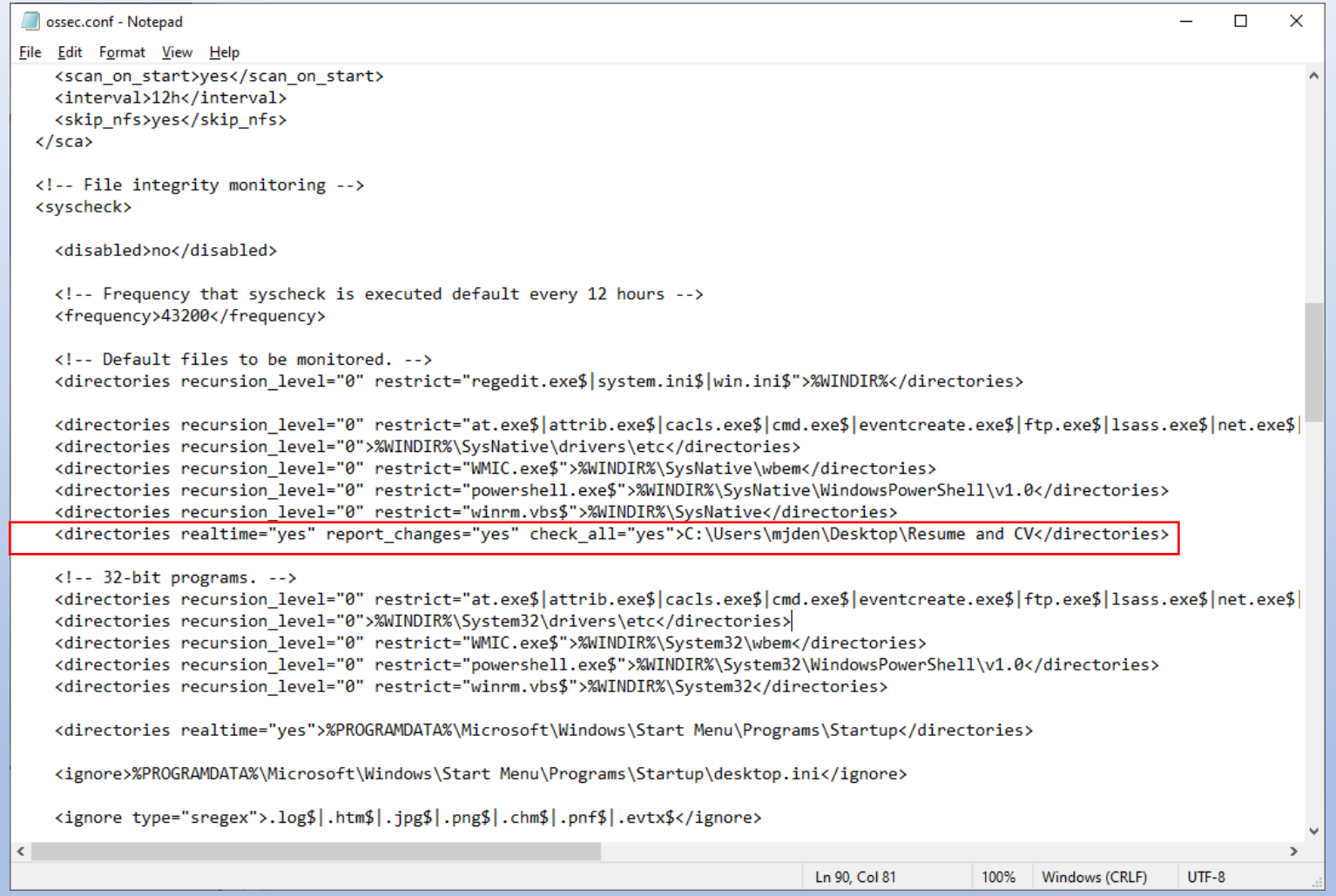
Verify no malicious packages were installed

- Check with the following command:
  - grep “install” /var/log/dpkg.log

```
root@173-255-237-148:~# grep "install " /var/log/dpkg.log
2024-08-17 23:09:06 install libc-dev-bin:amd64 <none> 2.35-0ubuntu3.8
2024-08-17 23:09:06 install linux-libc-dev:amd64 <none> 5.15.0-118.128
2024-08-17 23:09:07 install libcrypt-dev:amd64 <none> 1:4.4.27-1
2024-08-17 23:09:07 install rpcsvc-proto:amd64 <none> 1.4.2-0ubuntu6
2024-08-17 23:09:07 install libtirpc-dev:amd64 <none> 1.3.2-2ubuntu0.1
2024-08-17 23:09:07 install libnsl-dev:amd64 <none> 1.3.0-2build2
2024-08-17 23:09:07 install libc6-dev:amd64 <none> 2.35-0ubuntu3.8
2024-08-17 23:09:07 install gcc-11-base:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libisl23:amd64 <none> 0.24-2build1
2024-08-17 23:09:07 install libmpc3:amd64 <none> 1.2.1-2build1
2024-08-17 23:09:07 install cpp-11:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:07 install cpp:amd64 <none> 4:11.2.0-1ubuntu1
2024-08-17 23:09:07 install libcc1-0:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libgomp1:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libitm1:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libatomic1:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libasan6:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:07 install liblsan0:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libtsan0:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libubsan1:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libquadmath0:amd64 <none> 12.3.0-1ubuntu1~22.04
2024-08-17 23:09:07 install libgcc-11-dev:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:08 install gcc-11:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:08 install gcc:amd64 <none> 4:11.2.0-1ubuntu1
2024-08-17 23:09:08 install libstdc++-11-dev:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:08 install g++-11:amd64 <none> 11.4.0-1ubuntu1~22.04
2024-08-17 23:09:08 install g++:amd64 <none> 4:11.2.0-1ubuntu1
2024-08-17 23:09:08 install make:amd64 <none> 4.3-4.1build1
2024-08-17 23:09:08 install libdpkg-perl:all <none> 1.21.1ubuntu2.3
2024-08-17 23:09:08 install lto-disabled-list:all <none> 24
2024-08-17 23:09:08 install dpkg-dev:all <none> 1.21.1ubuntu2.3
2024-08-17 23:09:08 install build-essential:amd64 <none> 12.9ubuntu3
2024-08-17 23:09:08 install libfakeroot:amd64 <none> 1.28-1ubuntu1
2024-08-17 23:09:08 install fakeroot:amd64 <none> 1.28-1ubuntu1
2024-08-17 23:09:09 install fonts-dejavu-core:all <none> 2.37-2build1
2024-08-17 23:09:09 install fontconfig-config:all <none> 2.13.1-4.2ubuntu5
2024-08-17 23:09:09 install javascript-common:all <none> 11+nmu1
2024-08-17 23:09:09 install libalgorithm-diff-perl:all <none> 1.201-1
2024-08-17 23:09:09 install libalgorithm-diff-xs-perl:amd64 <none> 0.04-6build3
2024-08-17 23:09:09 install libalgorithm-merge-perl:all <none> 0.08-3
2024-08-17 23:09:09 install libfontconfig1:amd64 <none> 2.13.1-4.2ubuntu5
2024-08-17 23:09:09 install libjpeg-turbo8:amd64 <none> 2.1.2-0ubuntu1
2024-08-17 23:09:09 install libjpeg8:amd64 <none> 8c-2ubuntu10
2024-08-17 23:09:09 install libdeflate0:amd64 <none> 1.10-2
2024-08-17 23:09:09 install libjbig0:amd64 <none> 2.1-3.1ubuntu0.22.04.1
2024-08-17 23:09:09 install libwebp7:amd64 <none> 1.2.2-2ubuntu0.22.04.2
2024-08-17 23:09:09 install libtiff5:amd64 <none> 4.3.0-6ubuntu0.9
```

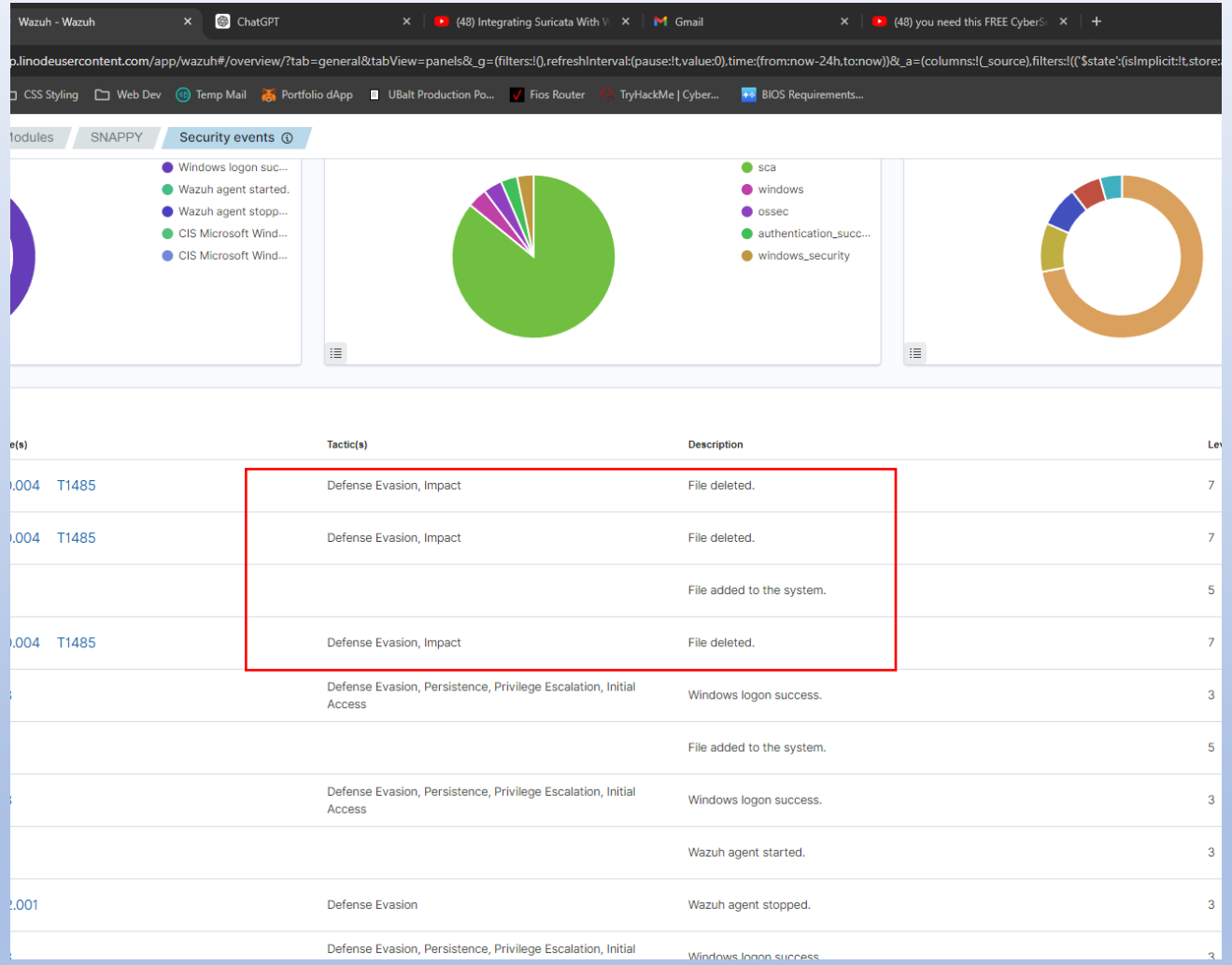
Adding rules to monitor files

- Open your ossec.conf file and add the following line to the default files to be monitored. This will monitor my Resume and CV folder on my Desktop.
  - <directories realtime="yes" report_changes="yes" check_all="yes">C:\Users\mjden\Desktop\Resume and CV</directories>



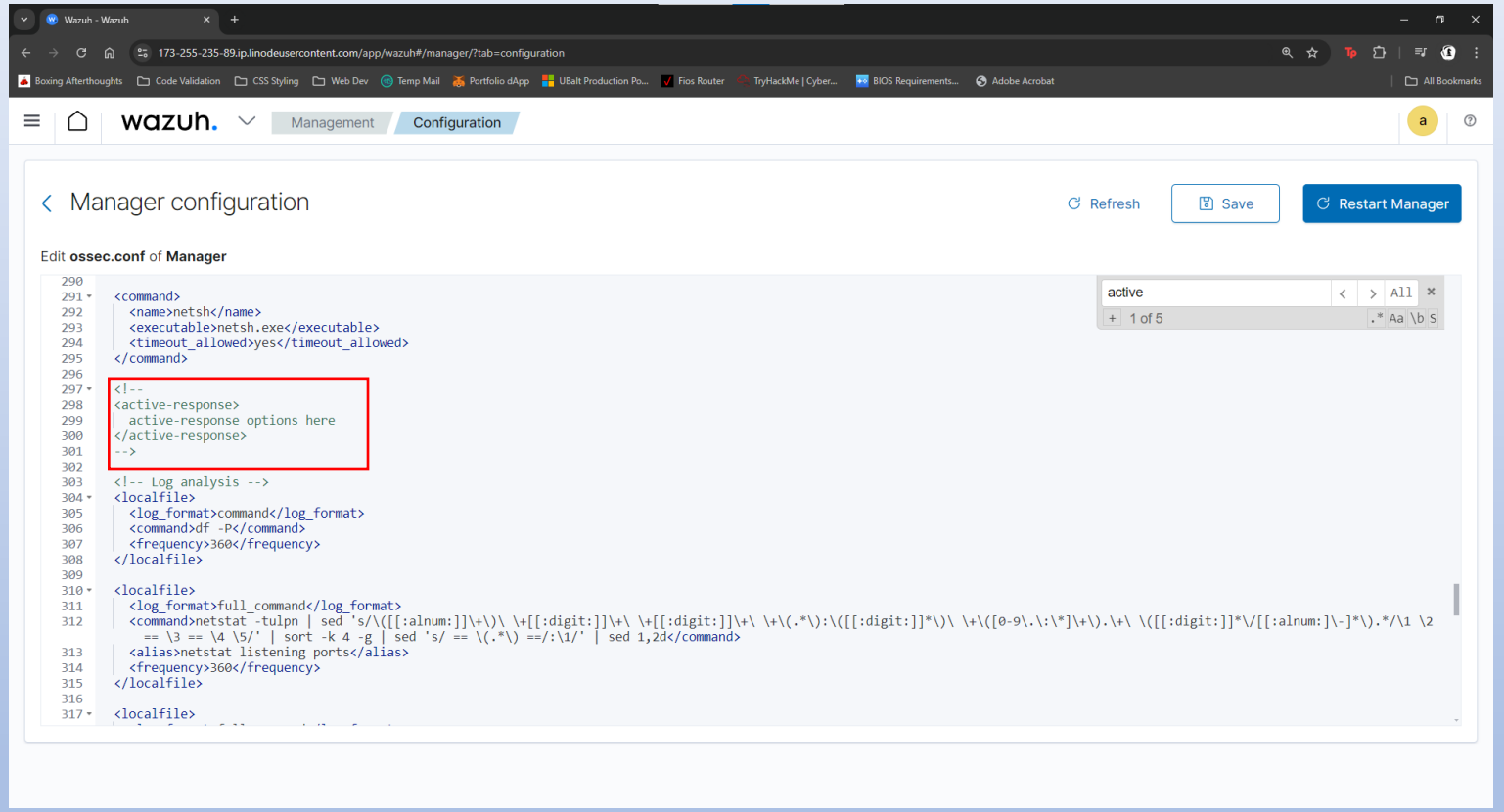
Verify rule works on dashboard

- Look at your dashboard and verify that our rule is working. I added and deleted a few files to give the folder some activity, which showed up on my dashboard.



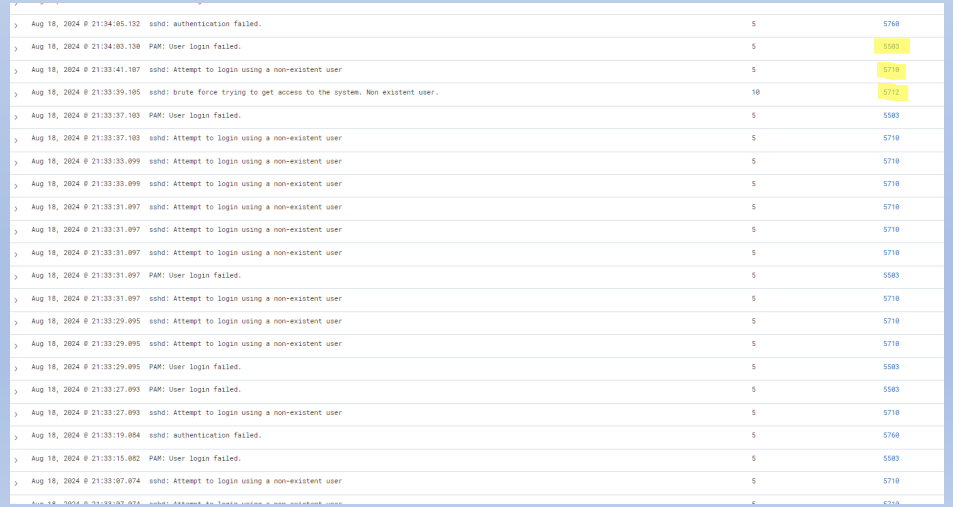
Active Response Option

- Go into Manager Configuration on your Wazuh Dashboard and scroll down to active response. You will see a section that is commented out. This is your template to insert your active response rules.



Set up Active Response

- You can use this template to block out the rules violated by your brute-force attack.
- In your security events log there will be a Rule ID that is tied to the authentication failures. You can set an automated response to ensure users cannot brute-force attack you with ease.



Aug 18, 2024 @ 21:34:05.132	sshd: authentication failed.	5	5760
Aug 18, 2024 @ 21:34:03.130	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:41.107	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:39.105	sshd: brute force trying to get access to the system. Non existent user.	10	5712
Aug 18, 2024 @ 21:33:37.103	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:37.103	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:33.099	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:33.099	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:31.097	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:29.095	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:29.095	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:29.095	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:27.093	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:27.093	sshd: Attempt to login using a non-existent user	5	5710
Aug 18, 2024 @ 21:33:19.084	sshd: authentication failed.	5	5760
Aug 18, 2024 @ 21:33:15.082	PAM: User login failed.	5	5503
Aug 18, 2024 @ 21:33:07.074	sshd: Attempt to login using a non-existent user	5	5710

```
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5710</rules_id>
  <timeout>300</timeout>
</active-response>

<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5712</rules_id>
  <timeout>300</timeout>
</active-response>

 <active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>60122</rules_id>
  <timeout>300</timeout>
</active-response>

  <active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5503</rules_id>
  <timeout>300</timeout>
</active-response>
```

Conclusion

- Through this lab, we successfully set up a Wazuh SIEM environment on a Linode cloud server and integrated it with a Windows agent. The process involved configuring real-time monitoring for critical directories, responding to a brute force attack, and implementing advanced security measures like two-factor authentication.
- By completing this lab, we demonstrated the ability to deploy and configure a comprehensive security monitoring solution that can be customized to meet specific needs. This foundational setup not only helps in detecting and mitigating threats but also provides a scalable framework for future enhancements. As we move forward, we can continue to refine our monitoring capabilities, adding more alerts, fine-tuning our configurations, and ensuring that our security posture evolves alongside emerging threats.
- This lab is a strong starting point for any organization looking to enhance its security monitoring and incident response capabilities.