

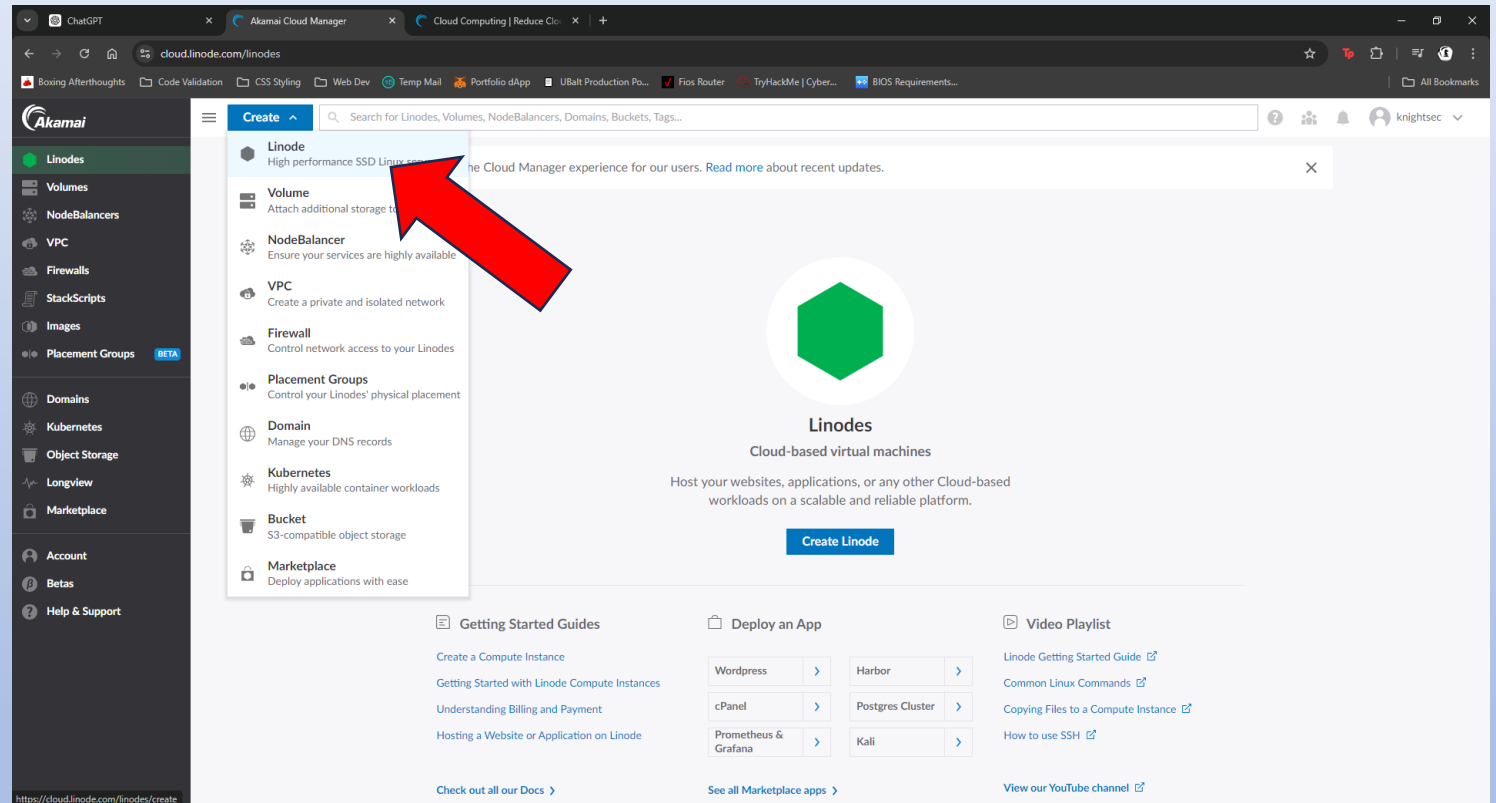


SIEM Home Lab

By: Miguel Denis

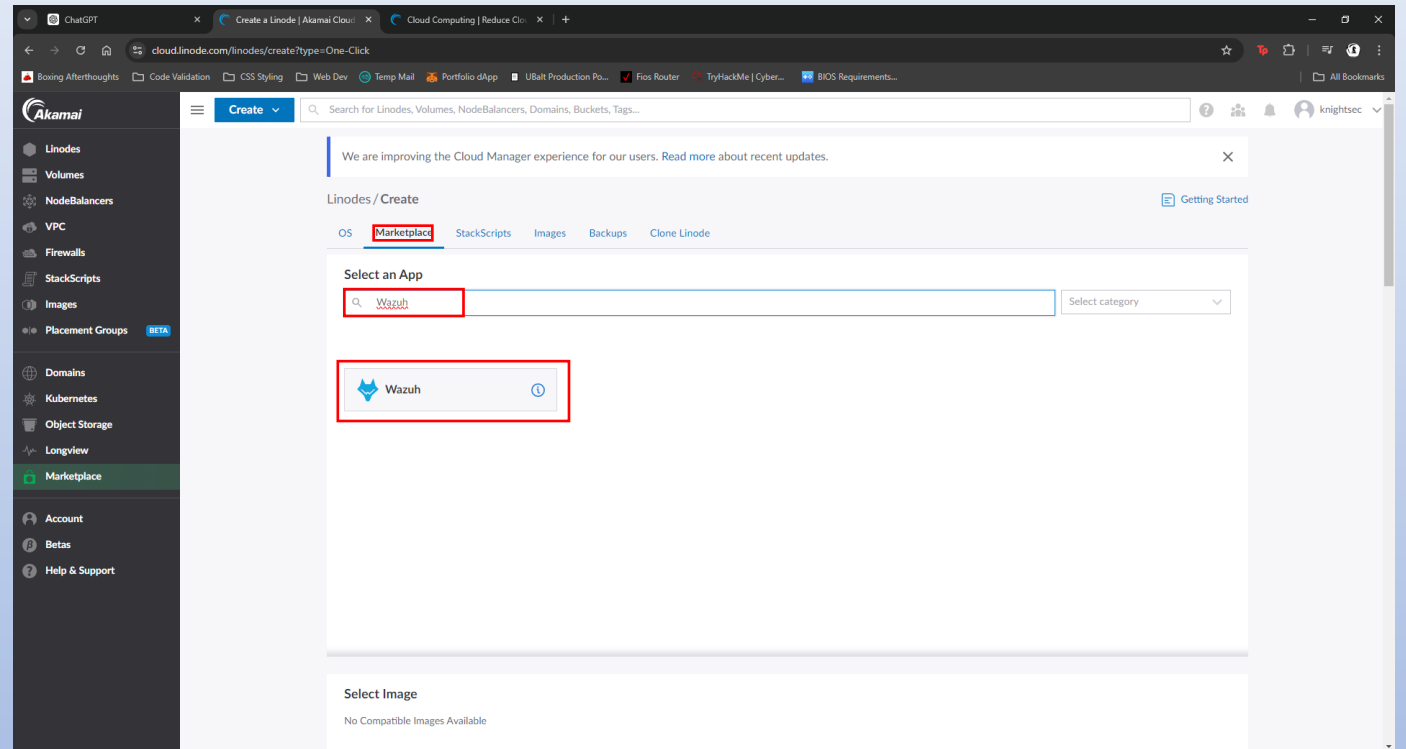
Create Linode Cloud Server

- 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

The screenshot shows the 'Wazuh Setup' page on the Linode cloud platform. The left sidebar contains navigation links for various services like Linodes, Volumes, NodeBalancers, VPC, Firewalls, StackScripts, Images, Placement Groups, Domains, Kubernetes, Object Storage, Longview, Marketplace, Account, Betas, and Help & Support. The main content area is titled 'Wazuh Setup' and includes several configuration sections:

- Email address (for the Let's Encrypt SSL certificate) (required):** A text input field containing 'mjdenis84@gmail.com'.
- The limited sudo user to be created for the Linode:** A text input field containing 'knightsec'.
- Select an Image:** A dropdown menu showing 'Ubuntu 22.04 LTS'.
- Region:** A dropdown menu with the text 'Select a Region'.
- Linode Plan:** A section with tabs for 'Dedicated CPU', 'Shared CPU' (which is selected), 'High Memory', 'GPU', and 'Premium CPU'.

Red rectangular boxes are drawn around the email field, the sudo user field, the image selection dropdown, the region dropdown, and the 'Shared CPU' tab to highlight these specific configuration steps.

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 Label and enter it in the box
- Set a root password
- Click Create Linode at the bottom right of the page

Create a Linode | Akamai Cloud | ChatGPT

/linodes/create?type=One-Click

CSS Styling Web Dev Temp Mail Portfolio dApp UBalt Production Po... Fios Router TryHackMe | Cyber... BIOS Requirements...

<input type="radio"/>	Nanode 1 GB	\$5	\$0.0075	1 GB	1	25 GB	1 TB	40 Gbps / 1 Gbps
<input type="radio"/>	Linode 2 GB	\$12	\$0.018	2 GB	1	50 GB	2 TB	40 Gbps / 2 Gbps
<input checked="" type="radio"/>	Linode 4 GB	\$24	\$0.036	4 GB	2	80 GB	4 TB	40 Gbps / 4 Gbps
<input type="radio"/>	Linode 8 GB	\$48	\$0.072	8 GB	4	160 GB	5 TB	40 Gbps / 5 Gbps
<input type="radio"/>	Linode 16 GB	\$96	\$0.144	16 GB	6	320 GB	8 TB	40 Gbps / 6 Gbps
<input type="radio"/>	Linode 32 GB	\$192	\$0.288	32 GB	8	640 GB	16 TB	40 Gbps / 7 Gbps
<input type="radio"/>	Linode 64 GB	\$384	\$0.576	64 GB	16	1280 GB	20 TB	40 Gbps / 9 Gbps
<input type="radio"/>	Linode 96 GB	\$576	\$0.864	96 GB	20	1920 GB	20 TB	40 Gbps / 10 Gbps
<input type="radio"/>	Linode 128 GB	\$768	\$1.152	128 GB	24	2560 GB	20 TB	40 Gbps / 11 Gbps
<input type="radio"/>	Linode 192 GB	\$1152	\$1.728	192 GB	32	3840 GB	20 TB	40 Gbps / 12 Gbps

Details

Linode Label

wazuh

Add Tags

Type to choose or create a tag.

Placement Groups in Newark, NJ (us-east)

None

Create Placement Group

Root Password

Strength: Good

SSH Keys

User	SSH Keys
knightsec	None

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

The screenshot displays the Linode Cloud Manager interface for a Linode instance named 'wazuh'. The instance is in a 'RUNNING' state, indicated by a green circle and the word 'RUNNING'. A red box highlights this status. Below the status, the 'Summary' tab shows the instance's specifications: 2 CPU Cores, 80 GB Storage, and 4 GB RAM. The 'Public IP Addresses' section lists the IP address 172.104.31.32. The 'Access' section provides the SSH command: `ssh root@172.104.31.32`. A red box highlights this command. The interface also includes a 'Launch LISH Console' button and a 'Stats for this Linode are not available yet' message.

SSH

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

```
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\mjden> ssh root@172.104.31.32
The authenticity of host '172.104.31.32 (172.104.31.32)' can't be established.
ECDSA key fingerprint is SHA256:ssnE14i2L1/LkoP8sFmnUEHfSLkt+fMePqSD9aOgbV0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.104.31.32' (ECDSA) to the list of known hosts.
root@172.104.31.32's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-113-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sat Aug 17 10:42:50 PM UTC 2024

System load:          0.17
Usage of /:            10.1% of 78.17GB
Memory usage:         68%
Swap usage:           93%
Processes:            127
Users logged in:      0
IPv4 address for eth0: 172.104.31.32
IPv6 address for eth0: 2600:3c03::f03c:95ff:fe17:d3e6

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

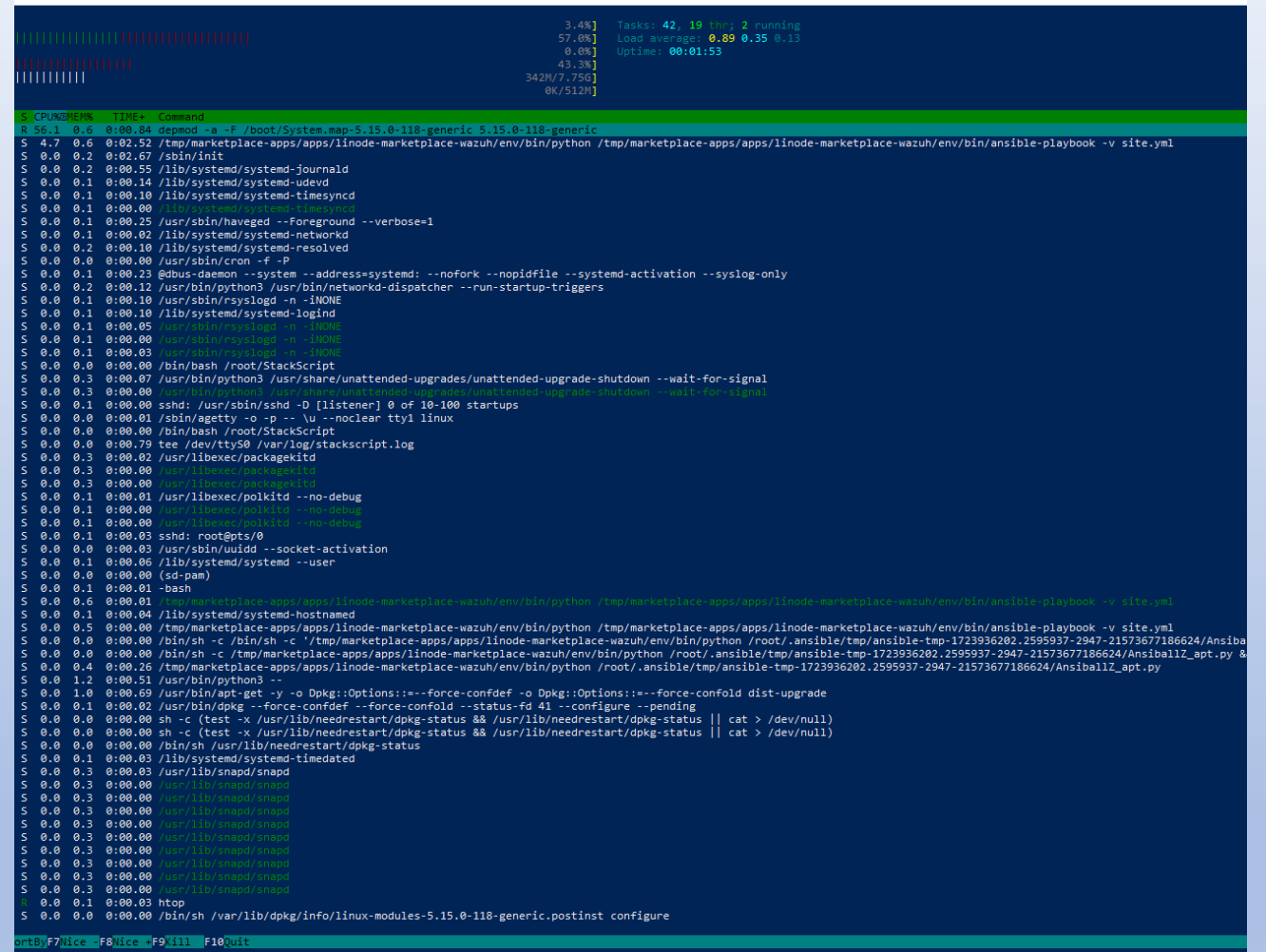
*****
Akamai Connected Cloud Wazuh Marketplace App
App URL: https://172-104-31-32.ip.linodeusercontent.com
Credentials File: /home/knightsec/.credentials
Documentation: https://www.linode.com/docs/products/tools/marketplace/guides/wazuh/
*****
To deploy the Wazuh agent, you will need to add the endpoint to your firewall:

    sudo ufw allow from $AGENTSERVERIP to any port 1514 proto tcp
    sudo ufw allow from $AGENTSERVERIP to any port 1515 proto tcp

**Update `AGENTSERVERIP` with the IP address you want to install the Wazuh Agent**
*****
To delete this message of the day: rm /etc/motd
root@172-104-31-32:~#
```

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

```
root@localhost: /home/knightsec
root@localhost: /# cd home
root@localhost: /home# ls -al
total 12
drwxr-xr-x  3 root    root      4096 Aug 17 23:09 .
drwxr-xr-x 19 root    root      4096 Aug 17 23:08 ..
drwxr-x---  3 knightsec knightsec 4096 Aug 17 23:15 knightsec
root@localhost: /home# cd knightsec/
root@localhost: /home/knightsec# ls -al
total 28
drwxr-x---  3 knightsec knightsec 4096 Aug 17 23:15 .
drwxr-xr-x  3 root      root      4096 Aug 17 23:09 ..
-rw-r--r--  1 knightsec knightsec 220 Jan  6 2022 .bash_logout
-rw-r--r--  1 knightsec knightsec 3771 Jan  6 2022 .bashrc
-rw-r--r--  1 knightsec knightsec 1258 Aug 17 23:15 .credentials
-rw-r--r--  1 knightsec knightsec 807 Jan  6 2022 .profile
drwx----- 2 knightsec knightsec 4096 Aug 17 23:09 .ssh
root@localhost: /home/knightsec# cat .credentials
Sudo Username:
Sudo Password:
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
indexer_username:
indexer_password:
# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username:
indexer_password:
# Regular Dashboard user. only has read permissions to all indices and all permissions on the .kibana index
indexer_username:
indexer_password:
# Filebeat user for CRUD operations on Wazuh indices
indexer_username:
indexer_password:
# User with READ access to all indices
indexer_username:
indexer_password:
# User with permissions to perform snapshot and restore operations
indexer_username:
indexer_password:
# Password for wazuh API user
api_username:
api_password:
# Password for wazuh-wui API user
api_username:
api_password:
root@localhost: /home/knightsec#
```

Obtaining Dashboard URL

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

The screenshot shows the Linode Cloud Manager interface for a Linode instance named 'wazuh'. The 'Network' tab is selected and highlighted with a red box. The interface displays various network-related metrics and settings.

Linodes / wazuh

Summary: 4 CPU Cores, 160 GB Storage, 8 GB RAM, 0 Volumes. Public IP Addresses: 173.255.237.148, 2600:3c03::f03c:95ff:fe17:0233. Access: SSH Access (ssh root@173.255.237.148), LISH Console via SSH (ssh -t knightsec@linus-east.linode.com wazu).

Plan: Dedicated 8 GB | Region: Newark, NJ | Linode ID: 62761609 | Created: 2024-08-17 23:07

SMTP ports may be restricted on this Linode. Need to send email? Review our [mail server guide](#), then open a support ticket.

Network | Analytics | Storage | Configurations | Backups | Activity Feed | Settings

Monthly Network Transfer

- wazuh (0.02 GB - 1%)
- Global Pool Used (1 GB - 1%)
- Global Pool Remaining (2295 GB)

Network Transfer History (b/s)

DNS Resolvers

66.228.42.5	2600:3c03::7
96.126.106.5	2600:3c03::4
50.116.53.5	2600:3c03::9
50.116.58.5	2600:3c03::6
50.116.61.5	2600:3c03::3
50.116.62.5	2600:3c03::c
66.175.211.5	2600:3c03::5
97.107.133.4	2600:3c03::b
207.192.69.4	2600:3c03::2
207.192.69.5	2600:3c03::8

Firewalls

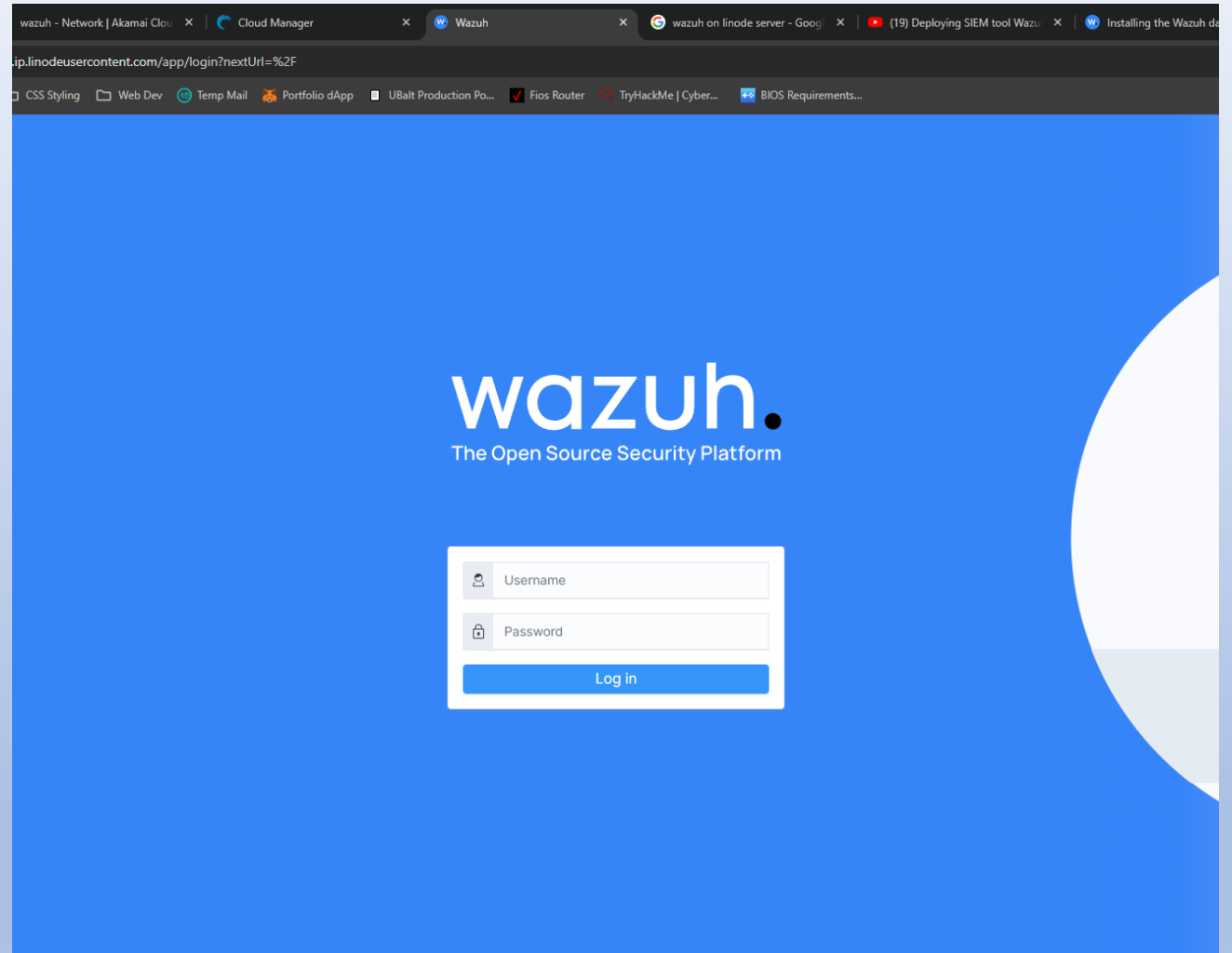
Firewall	Status	Rules
No Firewalls are assigned.		

IP Addresses

Address	Type	Default Gateway	Subnet Mask	Reverse DNS	IP Transfer	IP Sharing	Add An IP Address
173.255.237.148	IPv4 - Public	173.255.237.1	255.255.255.0	173-255-237-148.ip.linodeusercontent.com			Delete Edit RDNS
fe80::f03c:95ff:fe17:0233	IPv6 - Link Local	fe80::1	ffff:ffff:ffff::				
2600:3c03::f03c:95ff:fe17:0233	IPv6 - SLAAC	fe80::1	ffff:ffff:ffff::				Edit RDNS

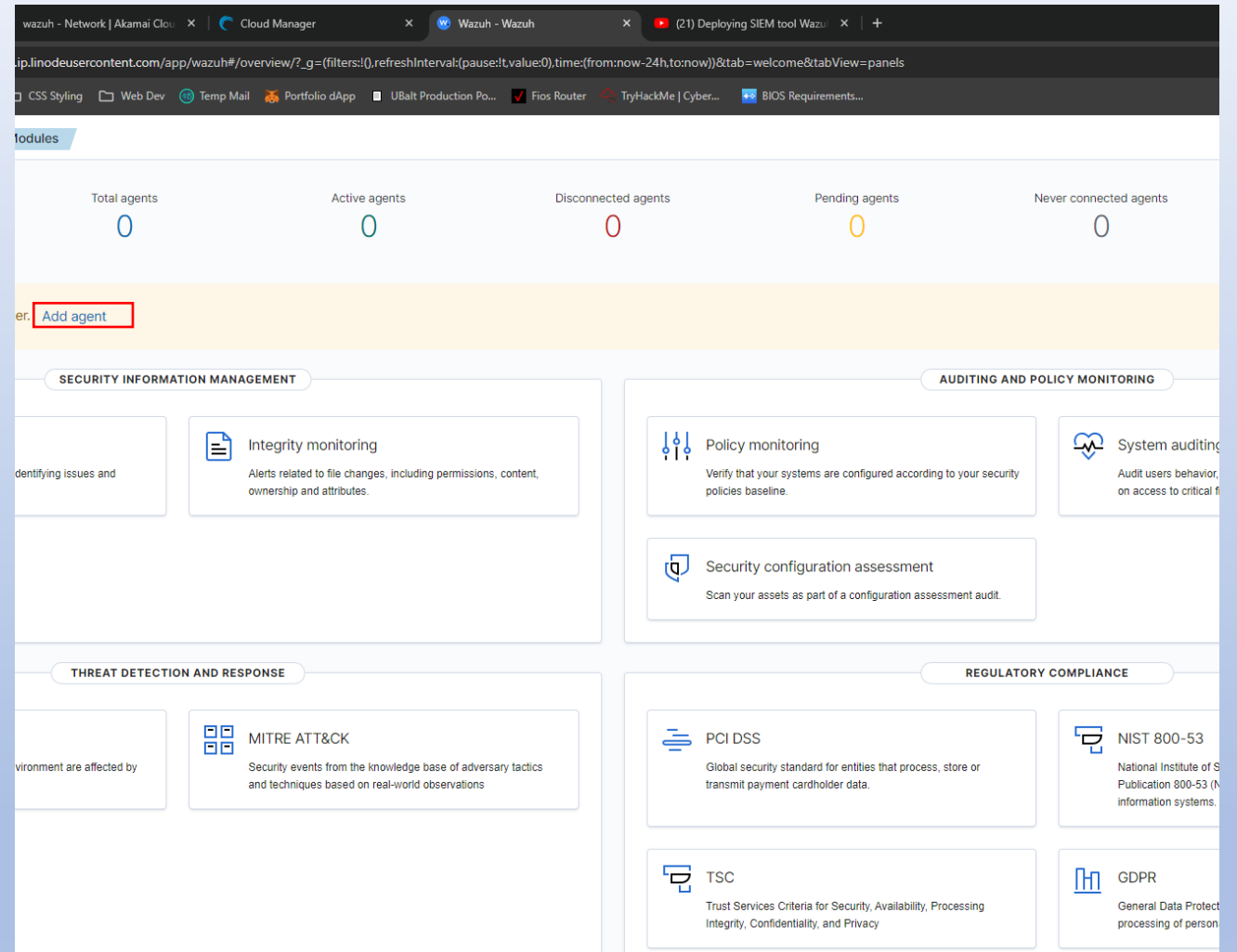
Log into Wazuh

- 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

The screenshot shows the 'Deploy new agent' page in the Wazuh web interface. The browser tabs at the top include 'wazuh - Network | Akamai Cloud', 'Cloud Manager', 'Wazuh - Wazuh', and '(2/1) Deploying SIEM tool Wazuh'. The URL bar shows a path to the Wazuh agents page. The main content area is titled 'Deploy new agent' and contains three sections:

- Select the package to download and install on your system:** This section has three columns: 'LINUX' (with options for RPM amd64, RPM aarch64, DEB amd64, and DEB aarch64), 'WINDOWS' (with the 'MSI 32/64 bits' option selected and highlighted by a red box), and 'macOS' (with options for Intel and Apple silicon). A link to documentation is provided below these options.
- Server address:** This section explains that the address is used for communication with the server. It includes a field to 'Assign a server address' which contains the value '173-255-237-148.ip.linodeusercontent.com' and is highlighted by a red box.
- Optional settings:** This section explains that the deployment uses the hostname as the agent name by default. It includes a field to 'Assign an agent name' which contains the value 'Home-PC' and is highlighted by a red box. A yellow warning message at the bottom states: 'The agent name must be unique. It can't be changed once the agent has been enrolled.'

Adding a Windows agent cont.

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

Home-PC

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $(env.tmp)\wazuh-agent; msixec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='173-255-237-148.ip.linodeusercontent.com' WAZUH_AGENT_NAME='Home-PC' WAZUH_REGISTRATION_SERVER='173-255-237-148.ip.linodeusercontent.com'
```

Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

5 Start the agent:

```
NET START WazuhSvc
```

Close

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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $(env.tmp)\wazuh-agent; msixec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='173-255-237-148.ip.linodeusercontent.com' WAZUH_AGENT_NAME='Home-PC' WAZUH_REGISTRATION_SERVER='173-255-237-148.ip.linodeusercontent.com'
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

Adding a Windows agent cont.

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

The screenshot shows the Wazuh web interface for adding a Windows agent. The browser tabs at the top include 'wazuh - Network | Akamai Cloud', 'Cloud Manager', 'Wazuh - Wazuh', and '(2/1) Deploying SIEM tool Wazuh'. The URL bar shows a path to the Wazuh agents-preview page.

The main content area is a form for configuring the agent. At the top, there is a text input field for the agent name, currently containing 'Home-PC'. Below this is a yellow warning box with the message: 'The agent name must be unique. It can't be changed once the agent has been enrolled.' Below the warning is a dropdown menu for selecting an existing group, currently set to 'Default'.

Below the group selection is a blue checkmark icon followed by the text: 'Run the following commands to download and install the agent:'. This is followed by a code block containing the following command:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $(env:tmp)\wazuh-agent; msexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='173-255-237-148.ip.linodeusercontent.com' WAZUH_AGENT_NAME='Home-PC' WAZUH_REGISTRATION_SERVER='173-255-237-148.ip.linodeusercontent.com'
```

Below the code block is a blue box with the heading 'Requirements' and two bullet points:

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

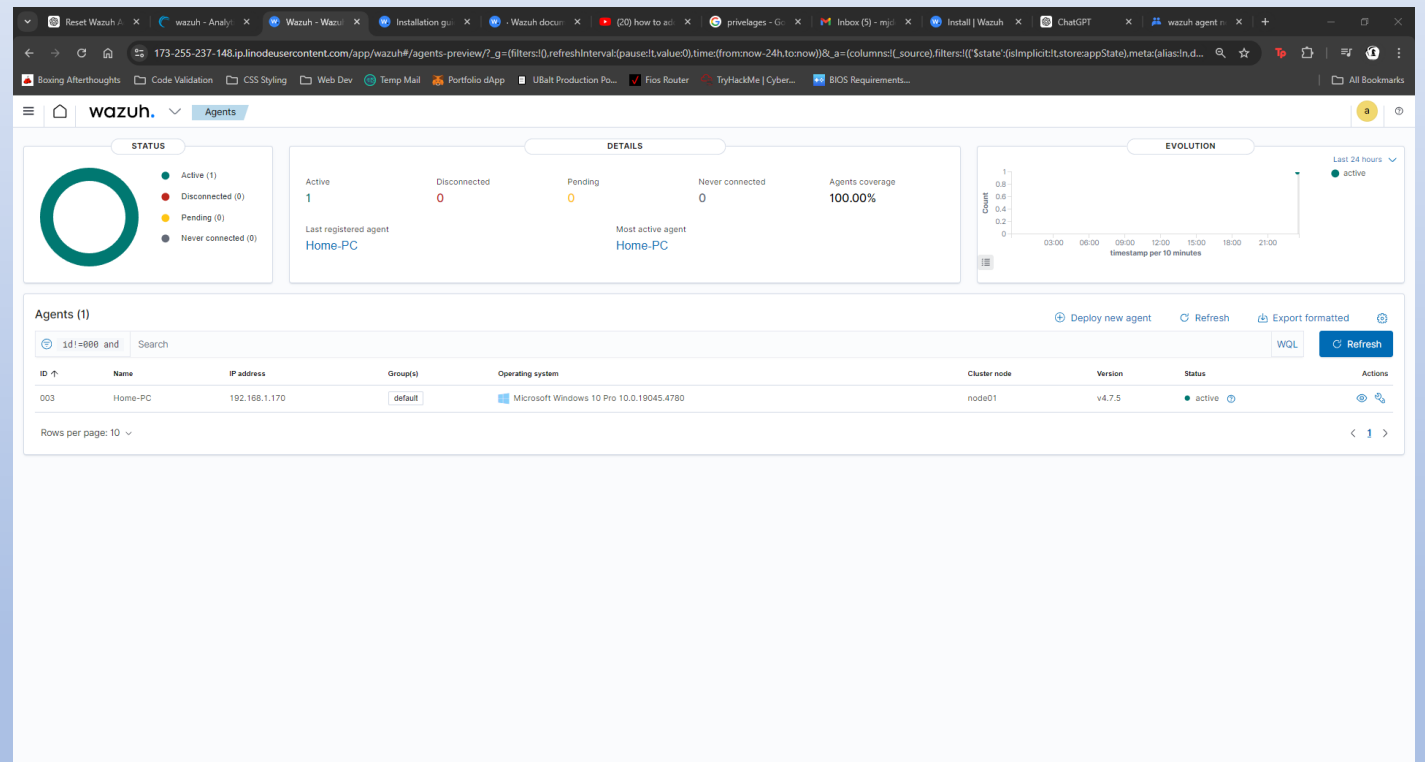
Below the requirements is a note: 'Keep in mind you need to run this command in a Windows PowerShell terminal.'

Below this is a blue circle with the number '5' followed by the text: 'Start the agent:'. This is followed by a text input field containing the command: 'NET START WazuhSvc'.

At the bottom right of the form is a blue button labeled 'Close', which is highlighted with a red rectangle.

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

```
root@173-255-237-148:~# sudo /var/ossec/bin/manage_agents

*****
* Wazuh v4.7.5 Agent manager.                *
* The following options are available:        *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E
```

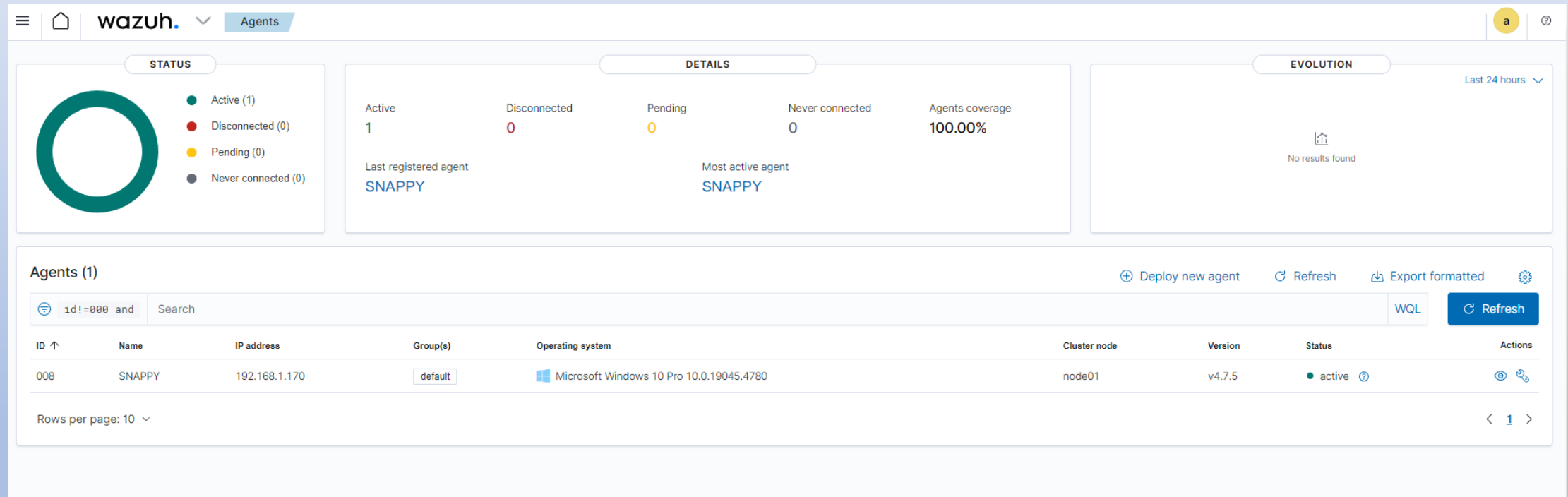
Firewall Issues

- 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
```

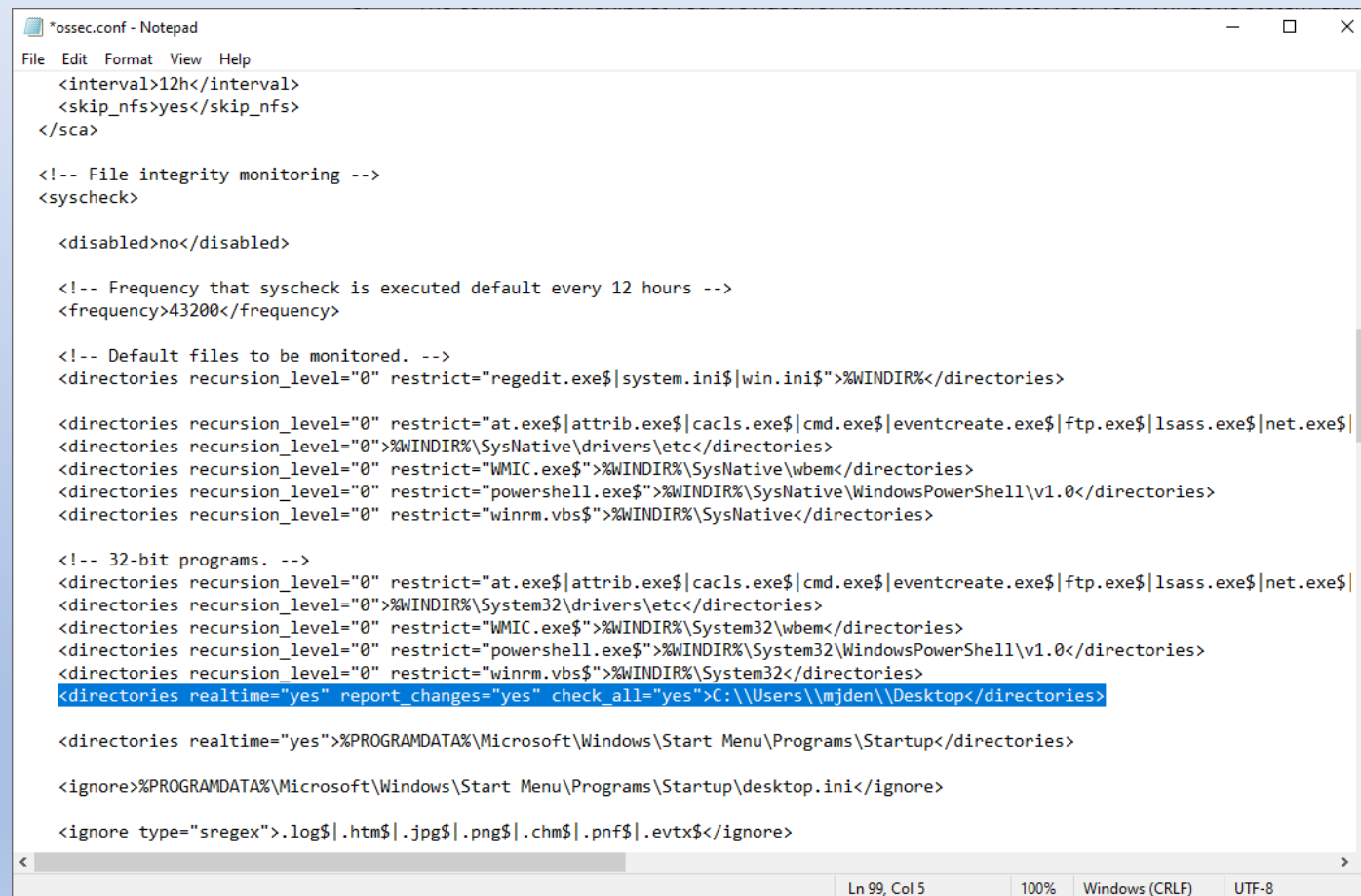
To	Action	From
--	-----	----
22/tcp	ALLOW	Anywhere
80/tcp	ALLOW	Anywhere
443/tcp	ALLOW	Anywhere
1514/udp	ALLOW	Anywhere
1515/tcp	ALLOW	Anywhere
1515/udp	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
80/tcp (v6)	ALLOW	Anywhere (v6)
443/tcp (v6)	ALLOW	Anywhere (v6)
1514/udp (v6)	ALLOW	Anywhere (v6)
1515/tcp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



```
*ossec.conf - Notepad
File Edit Format View Help
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$" %WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|
  <directories recursion_level="0" %WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\SysNative</directories>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|
  <directories recursion_level="0" %WINDIR%\System32\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\System32\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\System32\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\System32</directories>
  <directories realtime="yes" report_changes="yes" check_all="yes">C:\\Users\\mjden\\Desktop</directories>

  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

  <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

  <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

Ln 99, Col 5 100% Windows (CRLF) UTF-8
```

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	5583
> 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	5583
> 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		
> Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:31.097	PAM: User login failed.		
> Aug 18, 2024 @ 21:33:31.097	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:29.095	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:29.095	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:29.095	PAM: User login failed.		
> Aug 18, 2024 @ 21:33:27.093	PAM: User login failed.		
> Aug 18, 2024 @ 21:33:27.093	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:19.084	sshd: authentication failed.		
> Aug 18, 2024 @ 21:33:15.082	PAM: User login failed.		
> Aug 18, 2024 @ 21:33:07.074	sshd: Attempt to login using a non-existent user		
> Aug 18, 2024 @ 21:33:07.074	sshd: Attempt to login using a non-existent user		

Browser tabs: ChatGPT, wazuh - Network, Wazuh - Wazuh, Wazuh - Wazuh, Inbox (5) - mjd..., (23) The Wazuh..., What Is My IP Ad..., IP Address Looku..., ChatGPT, IP Address Looku...

Address bar: 173-255-237-148.ip.linodeusercontent.com/app/wazuh#/overview?tab=general&tabView=panels&_g=(filters:[]&refreshInterval:(pause:it.value:0),time:(from:now-24h,to:now))&_a=(columns:[]&rule.description,rule.level,rule.id),filters:[]&state...

Navigation: wazuh. Modules Home-PC Security events 0

> Aug 18, 2024 @ 21:36:33.283	sshd: Attempt to login using a non-existent user	5	5710
> Aug 18, 2024 @ 21:36:29.279	sshd: authentication failed.	5	5760
> Aug 18, 2024 @ 21:36:27.277	PAM: User login failed.	5	5583

Expanded document View surrounding documents View single document

Table JSON

r	GeoLocation.country_name	Russia
@	GeoLocation.location	{ "lon": 37.6068, "lat": 55.7386 }
r	_index	wazuh-alerts-4.x-2024.08.19
r	agent.id	000
r	agent.name	173-255-237-148.ip.linodeusercontent.com
r	data.dstuser	root
r	data.euid	0
r	data.scrip	83.217.17.37
r	data.tty	ssh
r	data.uid	0
r	decoder.name	pam
r	full_log	Aug 19 01:36:26 173-255-237-148 sshd[25810]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=83.217.17.37 user=root
r	id	1724031387.1033348
r	input.type	log
r	location	/var/log/auth.log
r	manager.name	173-255-237-148.ip.linodeusercontent.com
r	predecoder.hostname	173-255-237-148
r	predecoder.program_name	sshd

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`

```
root@173-255-237-148: ~  
Aug 18 23:22:46 173-255-237-148 sshd[23607]: Failed password for root from 218.92.0.100 port 24751 ssh2  
Aug 18 23:22:52 173-255-237-148 sshd[23607]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 24751 ssh2]  
Aug 18 23:23:56 173-255-237-148 sshd[23614]: Failed password for root from 218.92.0.100 port 52835 ssh2  
Aug 18 23:24:02 173-255-237-148 sshd[23614]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 52835 ssh2]  
Aug 18 23:25:02 173-255-237-148 sshd[23618]: Failed password for root from 218.92.0.100 port 58611 ssh2  
Aug 18 23:25:09 173-255-237-148 sshd[23618]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 58611 ssh2]  
Aug 18 23:26:08 173-255-237-148 sshd[23631]: Failed password for root from 218.92.0.100 port 25684 ssh2  
Aug 18 23:26:14 173-255-237-148 sshd[23631]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 25684 ssh2]  
Aug 18 23:27:14 173-255-237-148 sshd[23635]: Failed password for root from 218.92.0.100 port 49326 ssh2  
Aug 18 23:27:20 173-255-237-148 sshd[23635]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 49326 ssh2]  
Aug 18 23:28:16 173-255-237-148 sshd[23638]: Failed password for root from 218.92.0.100 port 61612 ssh2  
Aug 18 23:28:23 173-255-237-148 sshd[23638]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 61612 ssh2]  
Aug 18 23:29:22 173-255-237-148 sshd[23650]: Failed password for root from 218.92.0.100 port 30653 ssh2  
Aug 18 23:29:28 173-255-237-148 sshd[23650]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 30653 ssh2]  
Aug 18 23:30:28 173-255-237-148 sshd[23654]: Failed password for invalid user ftpuser from 102.129.85.203 port 38948 ssh2  
Aug 18 23:30:29 173-255-237-148 sshd[23656]: Failed password for root from 218.92.0.100 port 51861 ssh2  
Aug 18 23:30:34 173-255-237-148 sshd[23656]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 51861 ssh2]  
Aug 18 23:30:47 173-255-237-148 sshd[23660]: Failed password for invalid user zunwen from 197.221.232.44 port 36730 ssh2Aug 18 23:31:34 173-255-237-148 sshd[23663]: Failed password for root from 218.92.0.100 port 11426 ssh2  
Aug 18 23:31:40 173-255-237-148 sshd[23663]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 11426 ssh2]  
Aug 18 23:32:40 173-255-237-148 sshd[23665]: Failed password for root from 218.92.0.100 port 23312 ssh2  
Aug 18 23:32:42 173-255-237-148 sshd[23665]: Failed password for root from 218.92.0.100 port 23312 ssh2  
Aug 18 23:32:44 173-255-237-148 sshd[23667]: Failed password for root from 223.197.125.110 port 34384 ssh2  
Aug 18 23:32:45 173-255-237-148 sshd[23665]: Failed password for root from 218.92.0.100 port 23312 ssh2  
Aug 18 23:33:41 173-255-237-148 sshd[23670]: Failed password for root from 114.98.239.130 port 51442 ssh2  
Aug 18 23:33:42 173-255-237-148 sshd[23672]: Failed password for root from 218.92.0.100 port 37090 ssh2  
Aug 18 23:33:46 173-255-237-148 sshd[23672]: Failed password for root from 218.92.0.100 port 37090 ssh2  
Aug 18 23:33:49 173-255-237-148 sshd[23672]: Failed password for root from 218.92.0.100 port 37090 ssh2  
Aug 18 23:34:47 173-255-237-148 sshd[23688]: Failed password for root from 218.92.0.100 port 52030 ssh2  
Aug 18 23:34:52 173-255-237-148 sshd[23688]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 52030 ssh2]  
Aug 18 23:35:51 173-255-237-148 sshd[23694]: Failed password for root from 218.92.0.100 port 10723 ssh2  
Aug 18 23:35:57 173-255-237-148 sshd[23694]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 10723 ssh2]  
Aug 18 23:36:43 173-255-237-148 sshd[23699]: Failed password for invalid user deploy from 180.76.177.111 port 47664 ssh2Aug 18 23:37:01 173-255-237-148 sshd[23701]: Failed password for root from 218.92.0.100 port 43995 ssh2  
Aug 18 23:37:06 173-255-237-148 sshd[23701]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 43995 ssh2]  
Aug 18 23:37:27 173-255-237-148 sshd[23703]: Failed password for root from 103.179.57.203 port 41204 ssh2  
Aug 18 23:37:32 173-255-237-148 sshd[23705]: Failed password for invalid user rainbow from 197.221.232.44 port 54360 ssh2  
Aug 18 23:38:08 173-255-237-148 sshd[23708]: Failed password for root from 218.92.0.100 port 16008 ssh2  
Aug 18 23:38:11 173-255-237-148 sshd[23708]: Failed password for root from 218.92.0.100 port 16008 ssh2  
Aug 18 23:38:14 173-255-237-148 sshd[23708]: Failed password for root from 218.92.0.100 port 16008 ssh2  
Aug 18 23:38:15 173-255-237-148 sshd[23710]: Failed password for root from 102.129.85.203 port 37718 ssh2  
Aug 18 23:38:19 173-255-237-148 sshd[23712]: Failed password for invalid user ali from 180.76.177.111 port 60614 ssh2  
Aug 18 23:38:23 173-255-237-148 sshd[23714]: Failed password for invalid user st from 114.98.239.130 port 58490 ssh2  
Aug 18 23:38:35 173-255-237-148 sshd[23717]: Failed password for root from 197.221.232.44 port 44626 ssh2  
Aug 18 23:38:46 173-255-237-148 sshd[23719]: Failed password for invalid user zunwen from 180.76.177.111 port 38342 ssh2Aug 18 23:39:07 173-255-237-148 sshd[23722]: Failed password for invalid user deploy2 from 114.98.239.130 port 42274 ssh2  
Aug 18 23:39:11 173-255-237-148 sshd[23724]: Failed password for root from 102.129.85.203 port 42374 ssh2  
Aug 18 23:39:13 173-255-237-148 sshd[23726]: Failed password for invalid user shalini from 180.76.177.111 port 44300 ssh2  
Aug 18 23:39:14 173-255-237-148 sshd[23729]: Failed password for root from 218.92.0.100 port 38698 ssh2  
Aug 18 23:39:21 173-255-237-148 sshd[23729]: message repeated 2 times: [ Failed password for root from 218.92.0.100 port 38698 ssh2]  
Aug 18 23:39:34 173-255-237-148 sshd[23732]: Failed password for invalid user manuel from 197.221.232.44 port 36760 ssh2Aug 18 23:39:40 173-255-237-148 sshd[23734]: Failed password for root from 180.76.177.111 port 50258 ssh2  
Aug 18 23:39:45 173-255-237-148 sshd[23736]: Failed password for root from 103.179.57.203 port 40716 ssh2
```

```
root@173-255-237-148:~# 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:
 - `Whe`
- 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
```

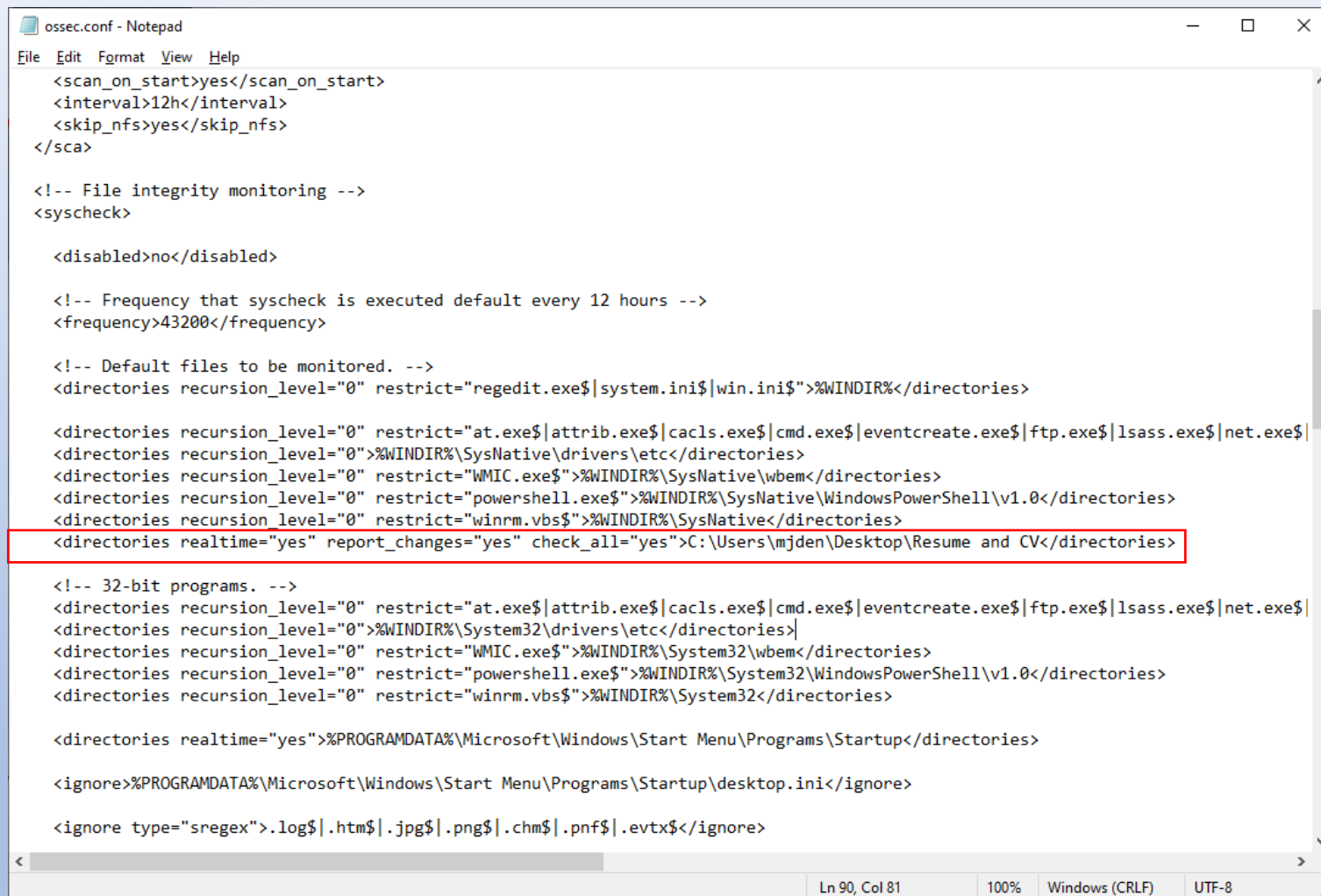
Verify no malicious packages were installed

- 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>`



```
ossec.conf - Notepad
File Edit Format View Help
<scan_on_start>yes</scan_on_start>
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$" %WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\SysNative</directories>
  <directories realtime="yes" report_changes="yes" check_all="yes">C:\Users\mjden\Desktop\Resume and CV</directories>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|
  <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\System32\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\System32\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\System32</directories>

  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

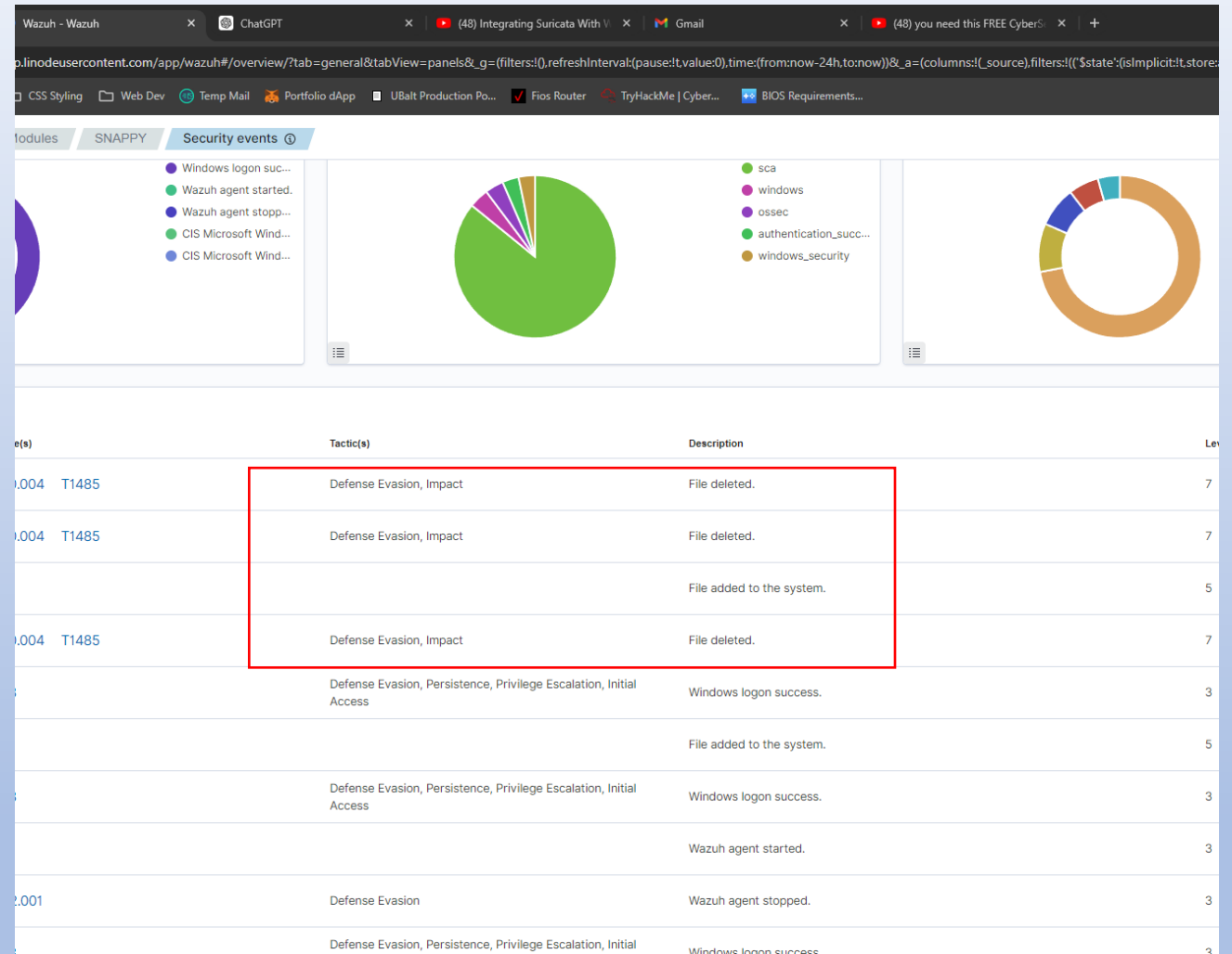
  <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

  <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

Ln 90, Col 81 100% Windows (CRLF) UTF-8
```

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.



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.