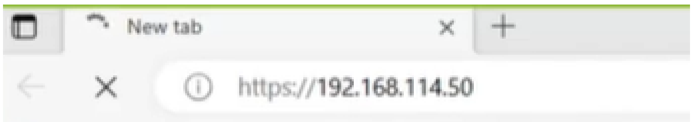
Allow and update Security Onion

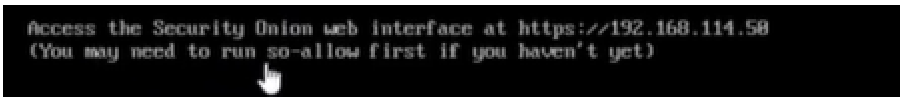
We install security onion but it will create some problems so we fixed it now.

If search the ip address of securityonion in web for web interface that we make, I cannot able ot search it



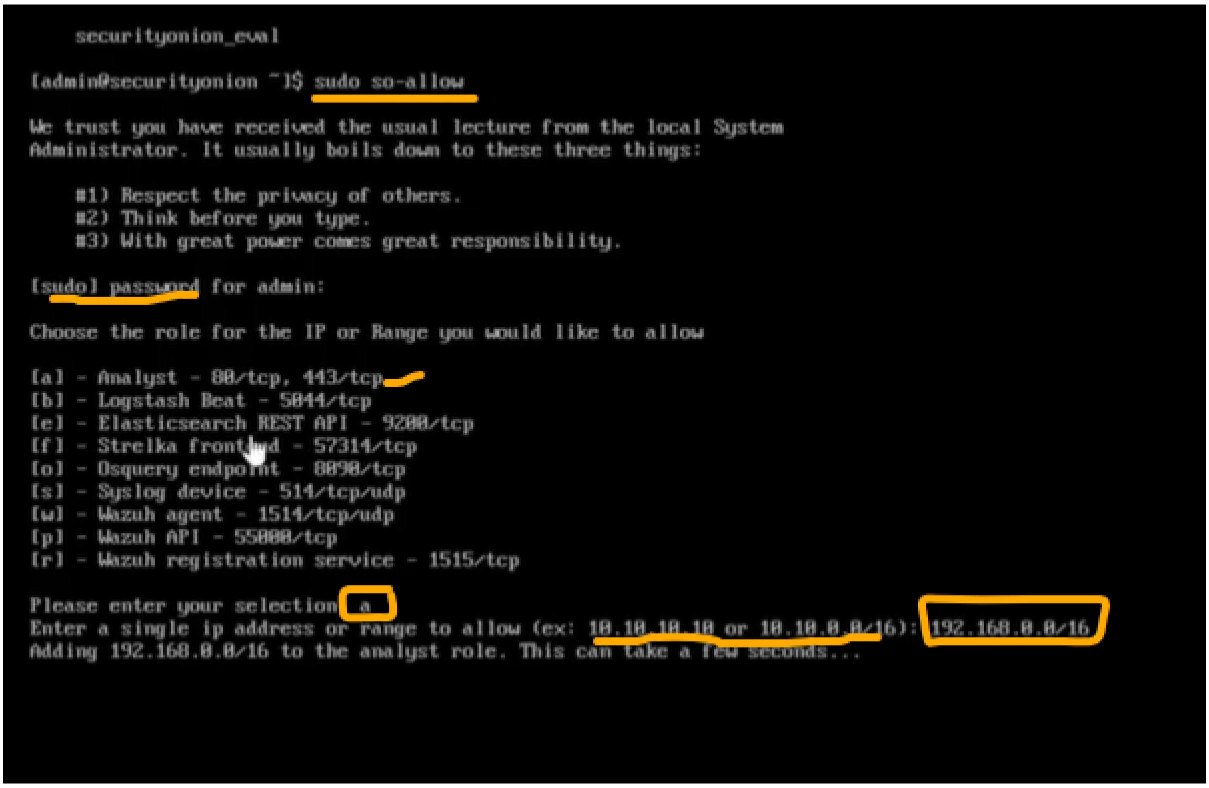
https://192.168.114.50

- It my have 2 reasons, one of them is written also on security onion cli that I get afater login



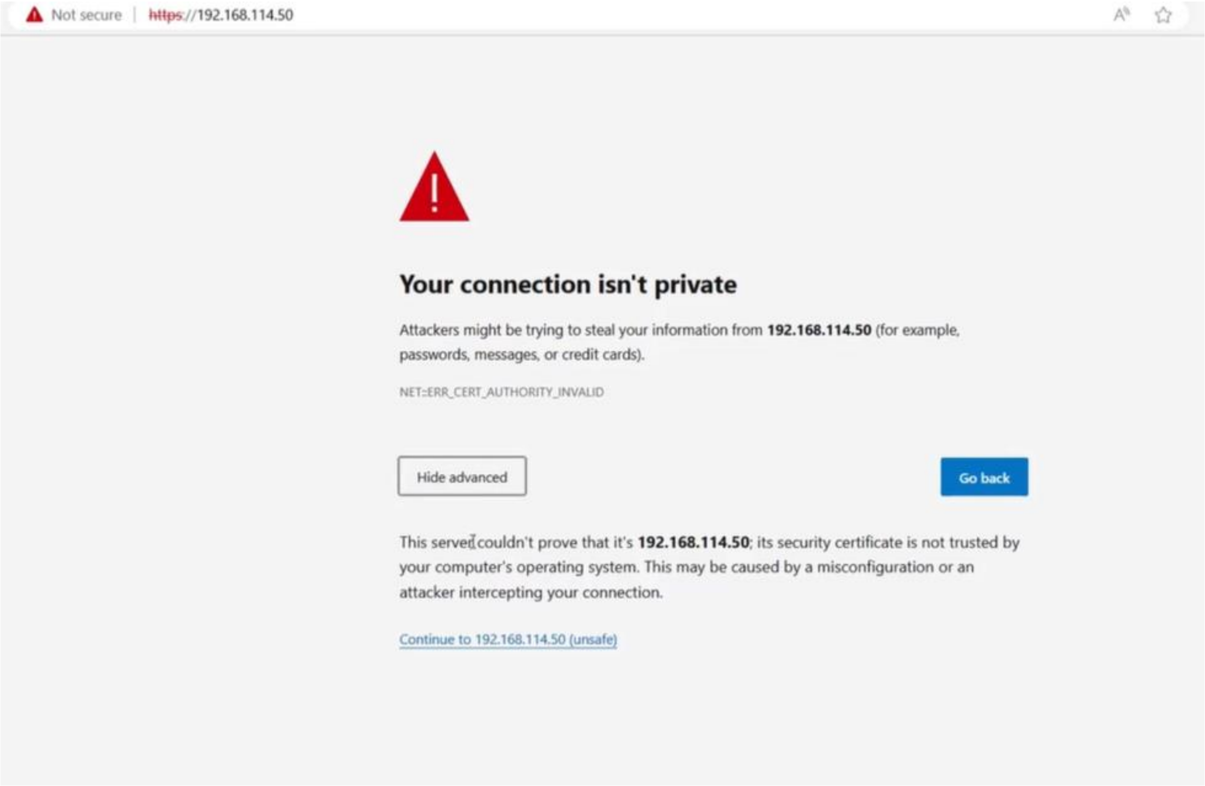
```
Access the Security Onion web interface at https://192.168.114.50
(You may need to run so-allow first if you haven't yet)
```

- We run command **sudo so-allow**
- Enter password
- Select option **a** for http services enable
- Allowed ip subnet 192.168.0.0/16
- And press enter



```
    securityonion_eval

[admin@securityonion ~]$ sudo so-allow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for admin:

Choose the role for the IP or Range you would like to allow

[a] - Analyst - 80/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[e] - Elasticsearch REST API - 9200/tcp
[f] - Strelka frontend - 57314/tcp
[o] - Osquery endpoint - 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: a
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 192.168.0.0/16
Adding 192.168.0.0/16 to the analyst role. This can take a few seconds...
```

- Now we will gui to see and access http services of security onion
- Allowed advance and you will see the login page



Not secure | https://192.168.114.50

Your connection isn't private

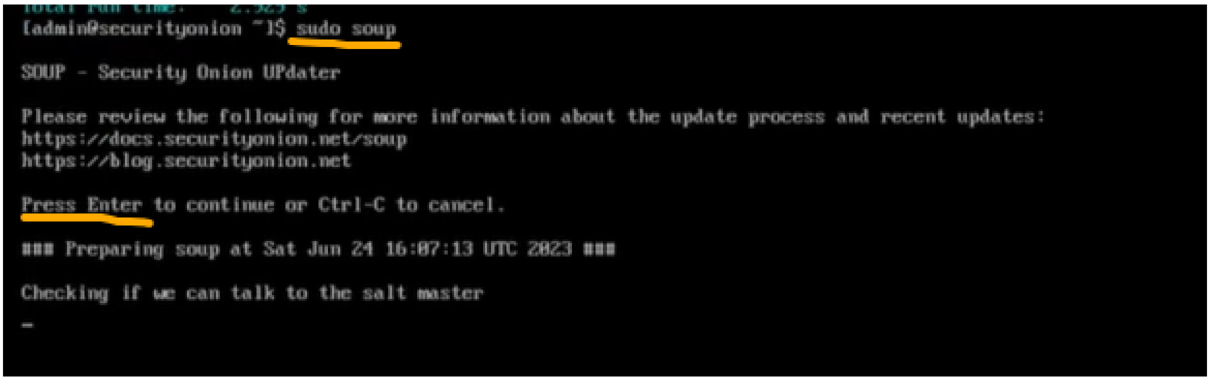
Attackers might be trying to steal your information from **192.168.114.50** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **192.168.114.50**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

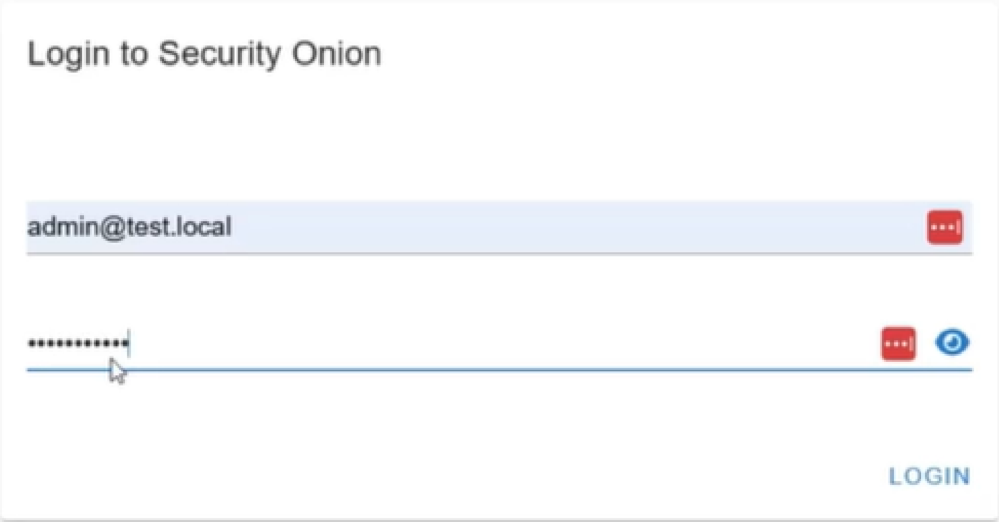
Continue to 192.168.114.50 (unsafe)

- Other **issue** that we will face is update
- Without this we cannot see logs here.
- So first update it by command **sudo soup**
- Soup stand for security onion updater



```
Total run time:    2.325 s
[admin@securityonion ~]$ sudo soup

SOUP - Security Onion UPdater

Please review the following for more information about the update process and recent updates:
https://docs.securityonion.net/soup
https://blog.securityonion.net

Press Enter to continue or Ctrl-C to cancel.

### Preparing soup at Sat Jun 24 16:07:13 UTC 2023 ###

Checking if we can talk to the salt master
_
```

- Login with administrator email and password that we set
- In my case it is admin@test.local and password is Admin@12345

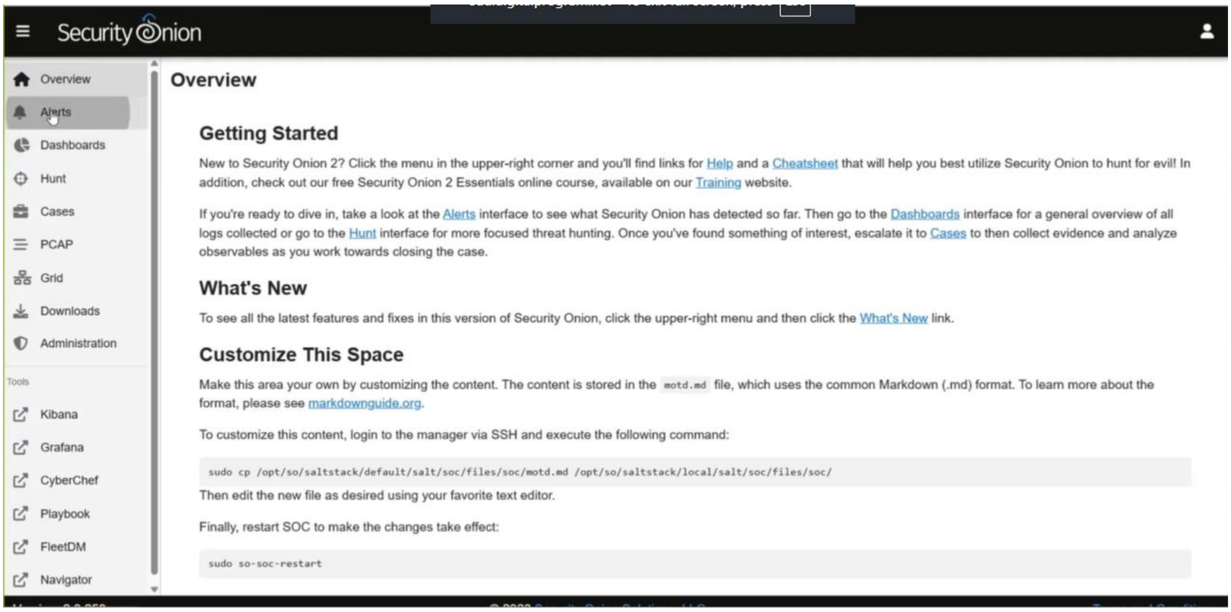


Login to Security Onion

admin@test.local

••••••••••••

- Then you see the securityonion interface



Overview

Getting Started

New to Security Onion 2? Click the menu in the upper-right corner and you'll find links for Help and a Cheatsheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion 2 Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. Then go to the Dashboards interface for a general overview of all logs collected or go to the Hunt interface for more focused threat hunting. Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Customize This Space

Make this area your own by customizing the content. The content is stored in the `motd.md` file, which uses the common Markdown (.md) format. To learn more about the format, please see markdownguide.org.

To customize this content, login to the manager via SSH and execute the following command:

```
sudo cp /opt/so/saltstack/default/salt/soc/files/soc/motd.md /opt/so/saltstack/local/salt/soc/files/soc/
```

Then edit the new file as desired using your favorite text editor.

Finally, restart SOC to make the changes take effect:

```
sudo so-soc-restart
```

Here we see different options like

- Dashboard
- Hunt
- Cases
- PCAP and etc.

Here you will see the log, these logs are of security onion .

---complete---