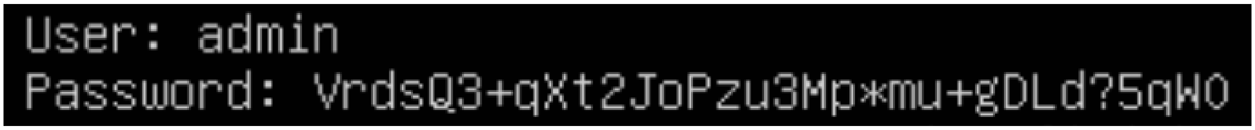
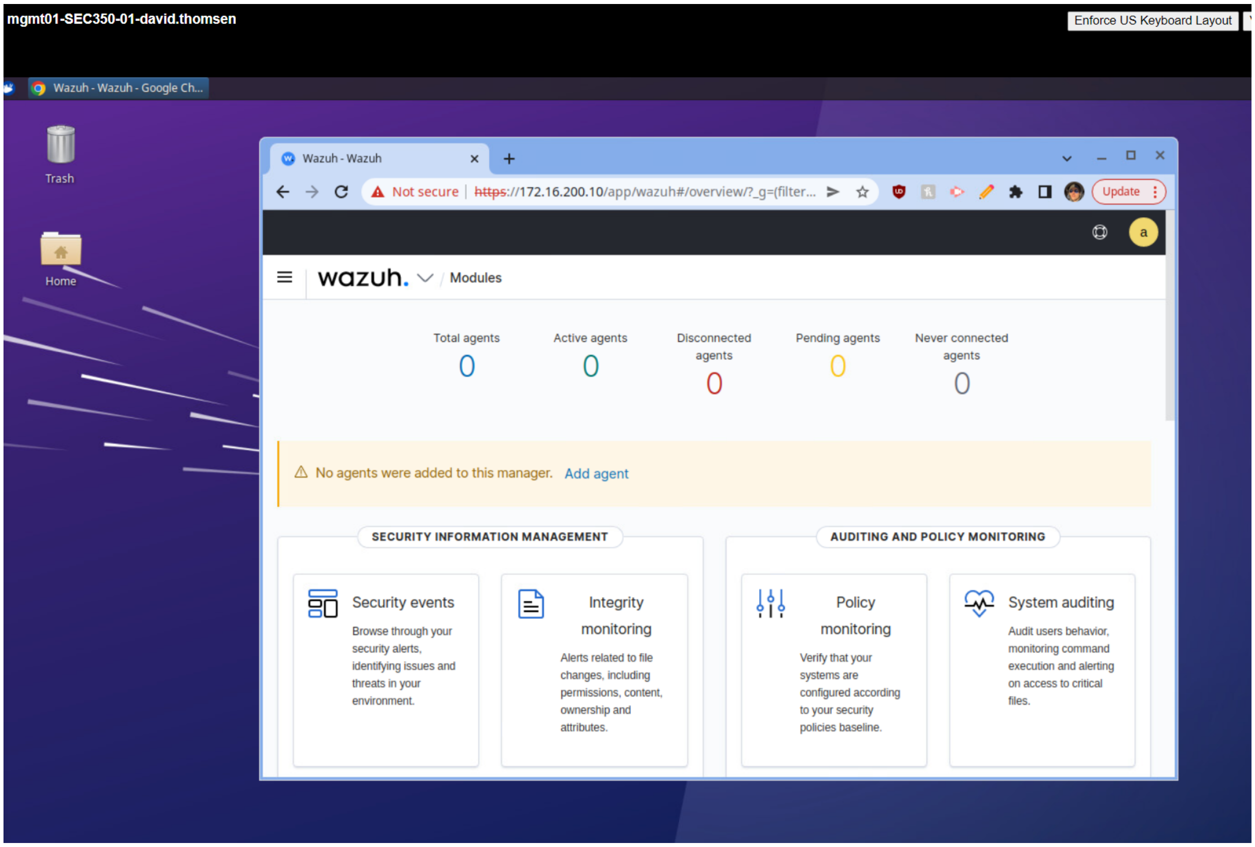


```
User: admin
Password: VrdsQ3+qXt2JoPzu3Mp*mu+gDLd?5qW0
```

https://github.com/dthomsen116/SEC-350/wiki/Lab-3.1---Segmentation-1

https://github.com/dthomsen116/SEC-350/wiki/Lab-3.2---Wazuh

Deliverable 1. A screenshot that clearly shows your wazuh server as accessed via mgmt01 similar to the one below



⚠ No agents were added to this manager.

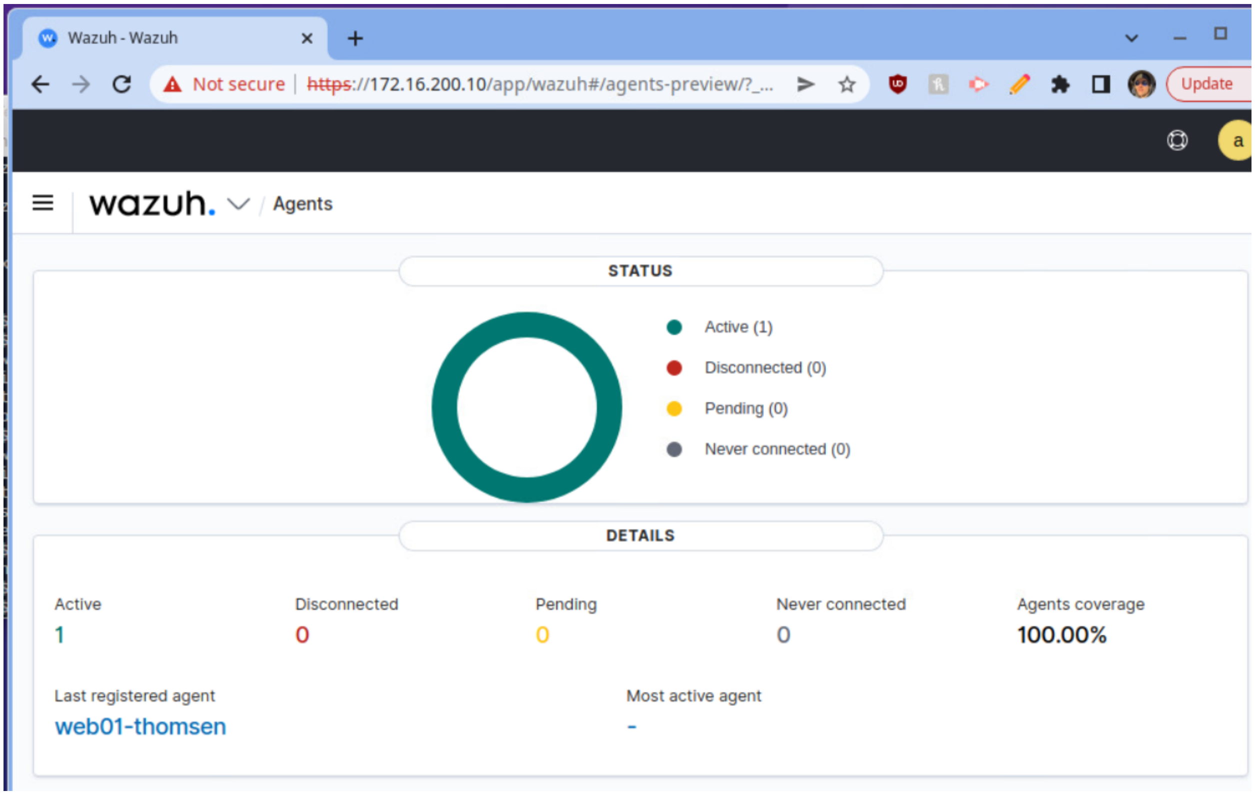
Browse through your security alerts, identifying issues and threats in your environment.

Alerts related to file changes, including permissions, content, ownership and attributes.

Verify that your systems are configured according to your security policies baseline.

Audit users behavior, monitoring command execution and alerting on access to critical files.

Deliverable 2. Provide a wazuh screenshot that shows the registered agent on web01



STATUS

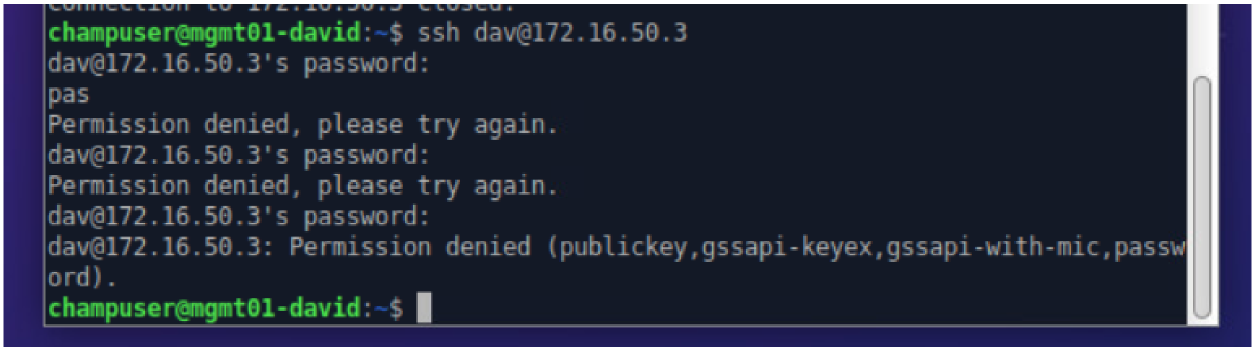
● Active (1)
● Disconnected (0)
● Pending (0)
● Never connected (0)

DETAILS

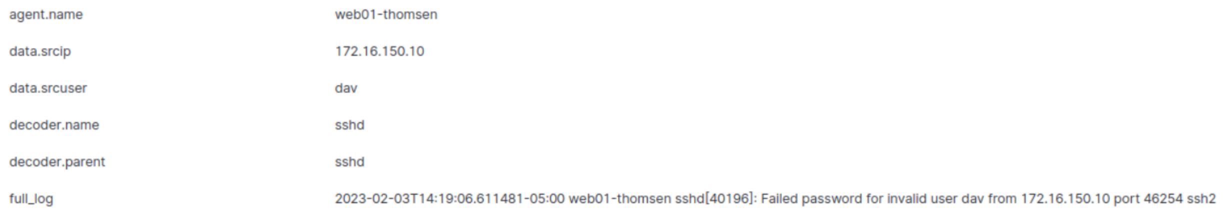
| Active | Disconnected | Pending | Never connected | Agents coverage |
|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 100.00% |

| Last registered agent | Most active agent |
|---|---|
| web01-thomsen | - |

Deliverable 3. Attempt an ssh login using an invalid user on web01 similar to the screenshot below. Search web01's wazuh security events until you find the associated event.



```
Connection to 172.16.50.3 closed.
champuser@mgmt01-david:~$ ssh dav@172.16.50.3
dav@172.16.50.3's password:
pas
Permission denied, please try again.
dav@172.16.50.3's password:
Permission denied, please try again.
dav@172.16.50.3's password:
dav@172.16.50.3: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,passw
ord).
champuser@mgmt01-david:~$ 
```



| | |
|---|---|
| agent.name | web01-thomsen |
| data.srcip | 172.16.150.10 |
| data.srcuser | dav |
| decoder.name | sshd |
| decoder.parent | sshd |
| full_log | 2023-02-03T14:19:06.611481-05:00 web01-thomsen sshd[40196]: Failed password for invalid user dav from 172.16.150.10 port 46254 ssh2 |