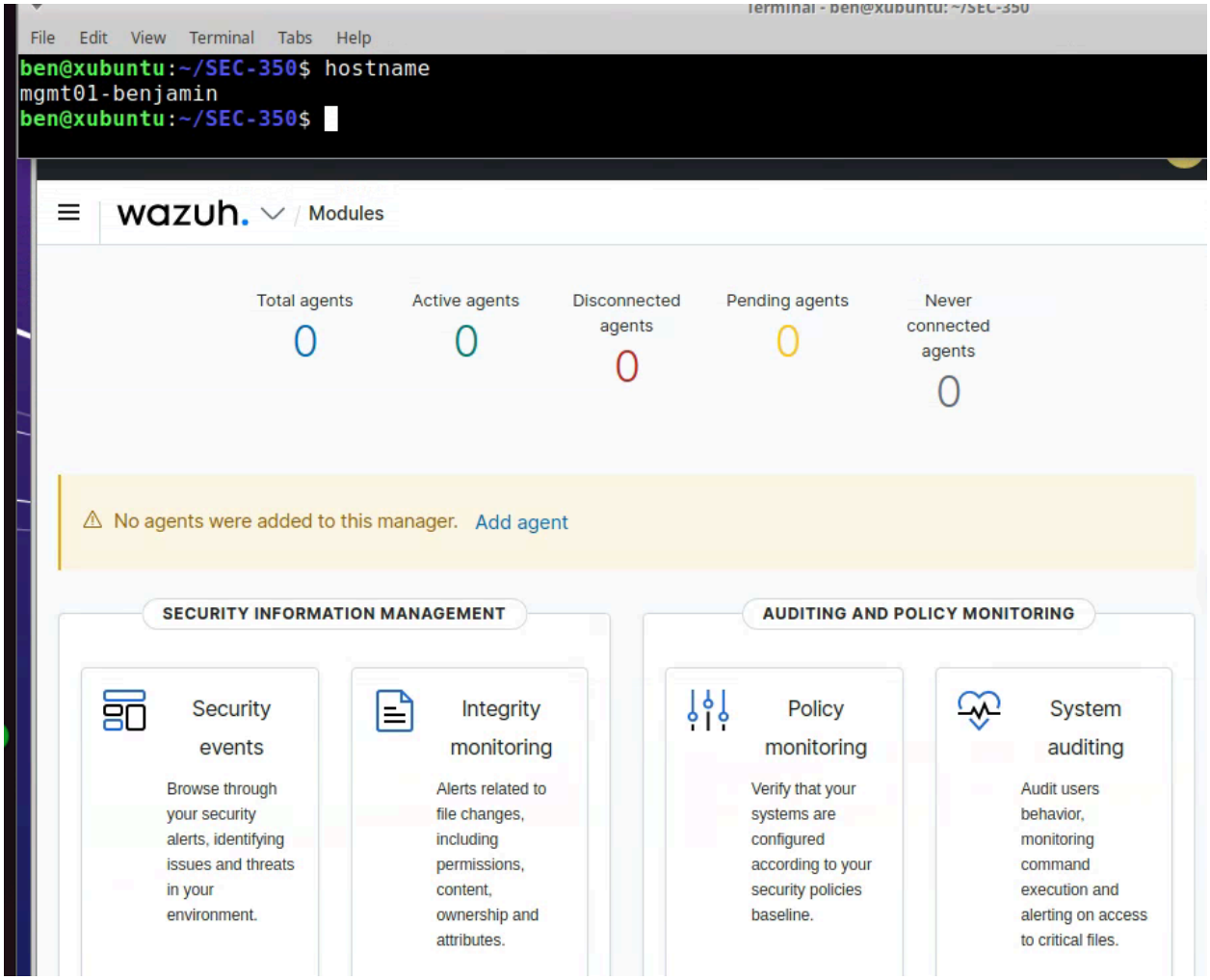
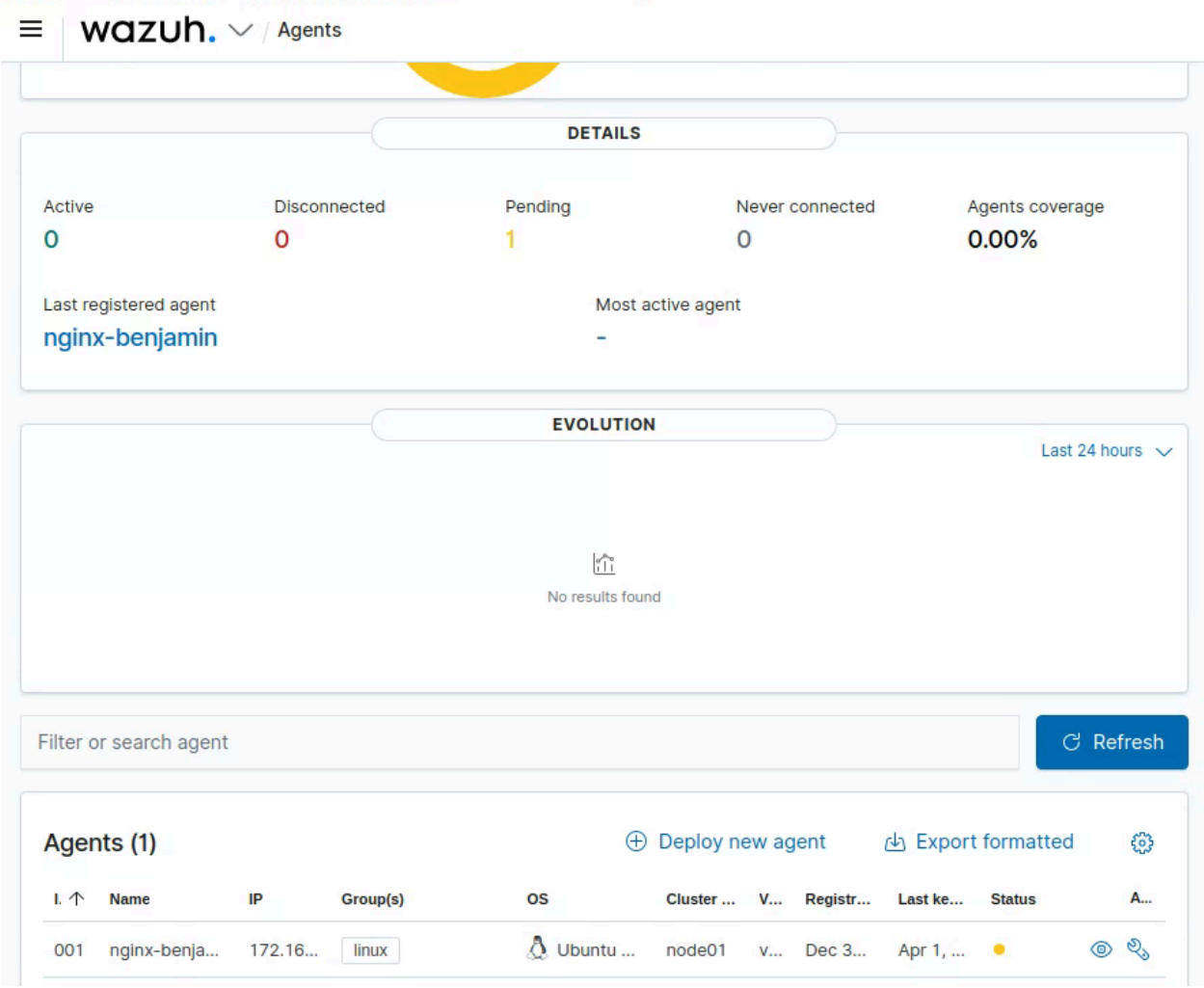
Lab3-2_Wazuh
SEC-350
Ben W
SP24

Deliverables:

1. Wazuh accessed on mgmto1



2. Agent in wazuh (nginx because web01 is gone)



3. Non-existent user login attempt

timestamp per 30 minutes

Time	rule.description	rule.level	rule.id
Apr 21, 2024 @ 13:48:56.110	syslog: User missed the password more than one time	10	2502
Apr 21, 2024 @ 13:48:56.105	sshd: Attempt to login using a non-existent user	5	5710
Apr 21, 2024 @ 13:48:52.099	sshd: Attempt to login using a non-existent user	5	5710
Apr 21, 2024 @ 13:48:48.095	sshd: Attempt to login using a non-existent user	5	5710
Apr 21, 2024 @ 13:48:46.100	PAM: User login failed.	5	5503
Apr 21, 2024 @ 13:48:44.091	sshd: Attempt to login using a non-existent user	5	5710

4. https://github.com/benjamin-weatherill/SEC-350/wiki/Wazuh-Installation-and-Implementation