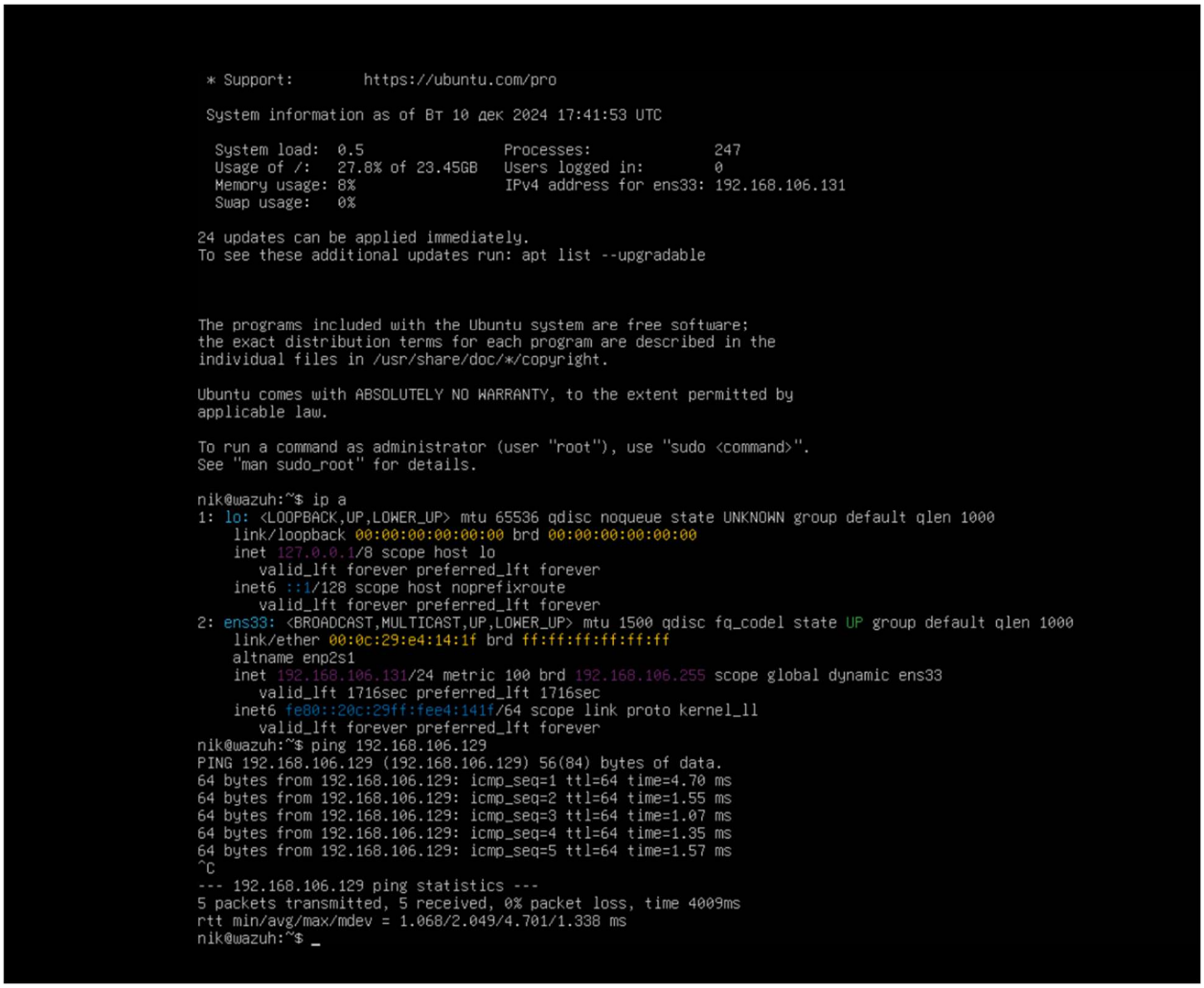
Практика №3 по предмету СДССиЛ - Wazuh

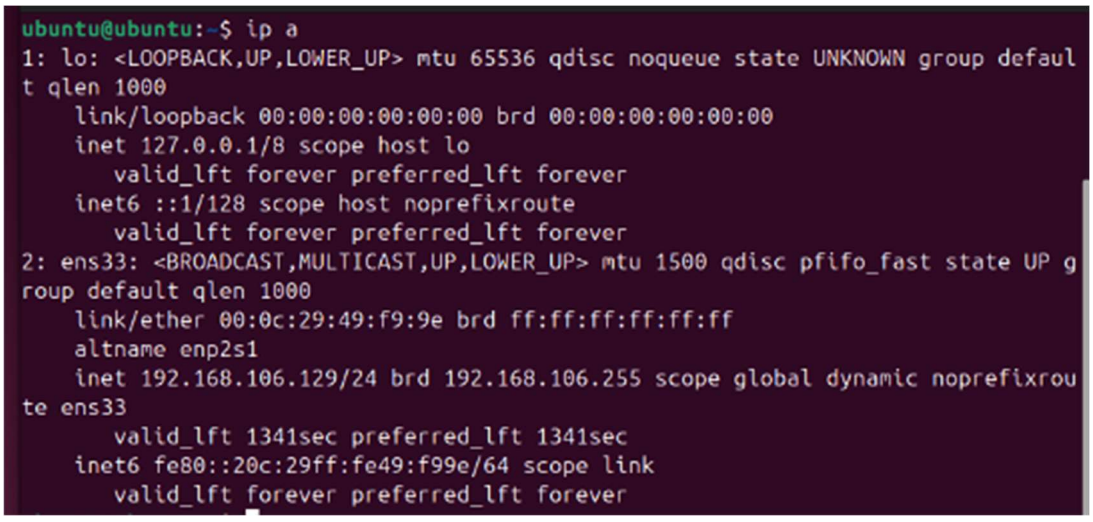
Выполнил студент - Князева Анастасия Михайловна группы: ББМО-01-23

Развертывание ВМ:

Серверная ВМ:



Клиентская ВМ:



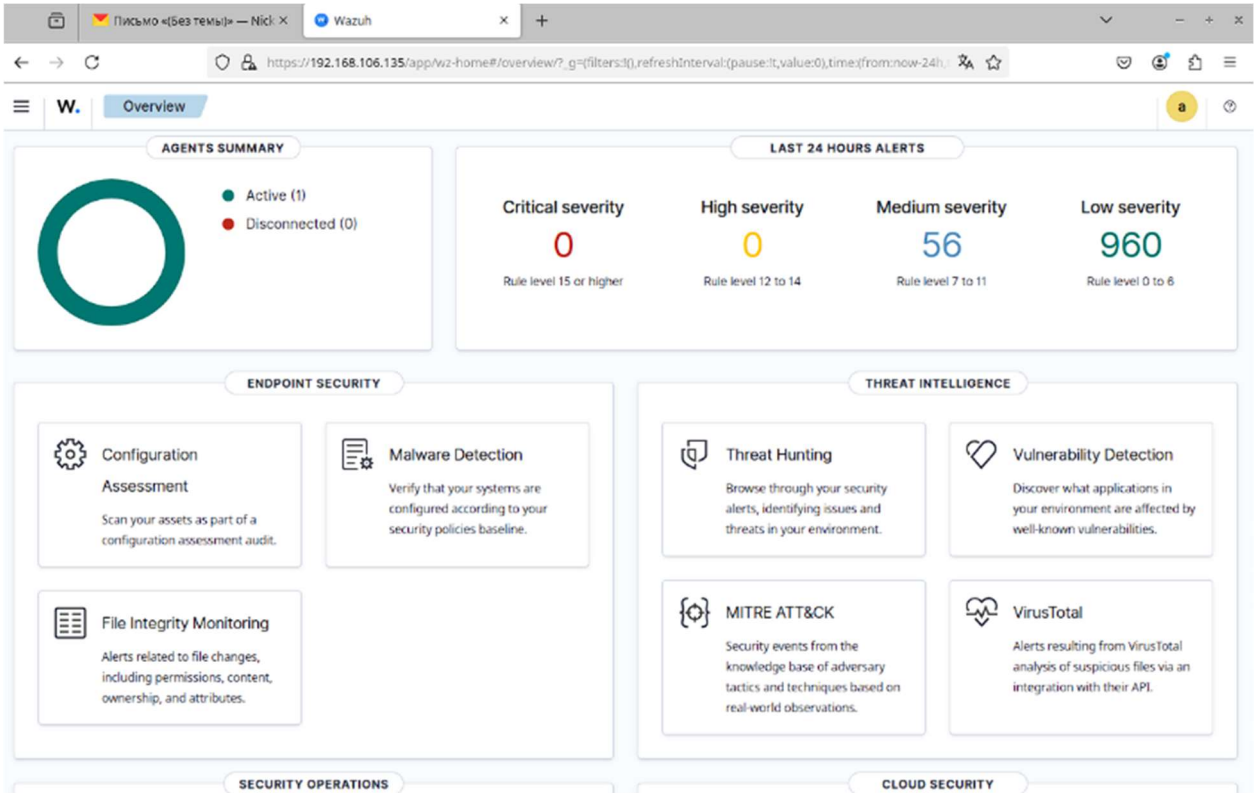
Обеспечение сетевого обмена между 2 ВМ:

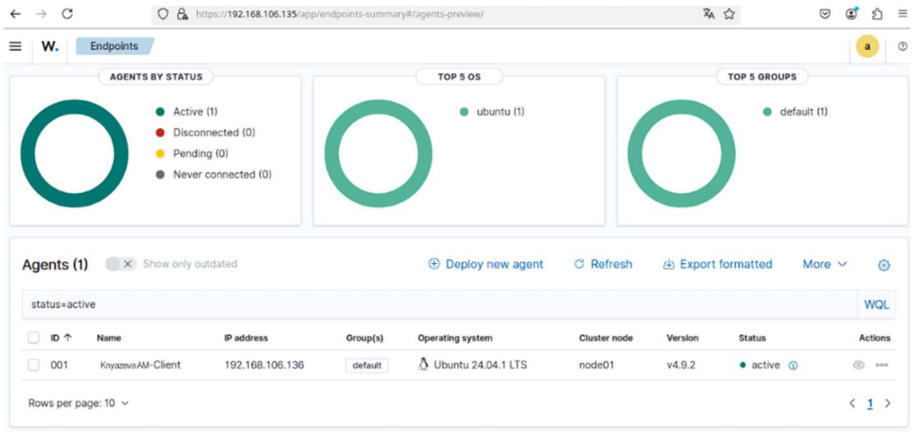
```
    link/ether 00:0c:29:49:f9:9e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.106.129/24 brd 192.168.106.255 scope global dynamic noprefixrou
te ens33
       valid_lft 1341sec preferred_lft 1341sec
    inet6 fe80::20c:29ff:fe49:f99e/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$ ping 192.168.106.131
PING 192.168.106.131 (192.168.106.131) 56(84) bytes of data.
64 bytes from 192.168.106.131: icmp_seq=1 ttl=64 time=62.7 ms
64 bytes from 192.168.106.131: icmp_seq=2 ttl=64 time=1.22 ms
64 bytes from 192.168.106.131: icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from 192.168.106.131: icmp_seq=4 ttl=64 time=1.28 ms
^C
--- 192.168.106.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.082/16.570/62.697/26.631 ms
ubuntu@ubuntu:~$
```

Развертывание на серверной ВМ Wazuh-сервера:

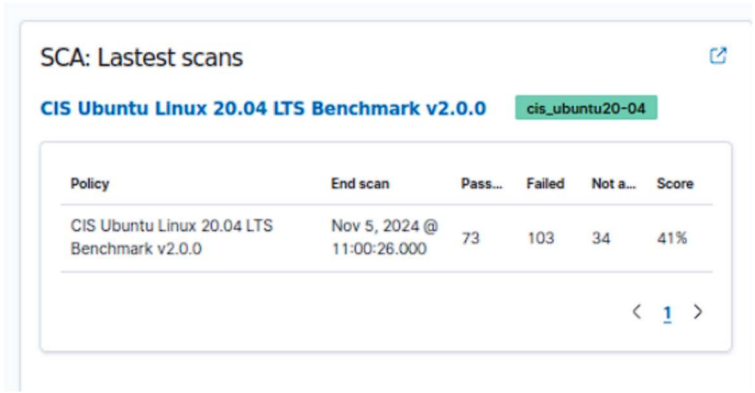
```
14/12/2024 09:17:58 INFO: Filebeat installation finished.
14/12/2024 09:17:59 INFO: Filebeat post-install configuration finished.
14/12/2024 09:18:00 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
14/12/2024 09:18:21 INFO: Starting service filebeat.
14/12/2024 09:18:23 INFO: filebeat service started.
14/12/2024 09:18:23 INFO: Installation finished.
root@nikitaserv:/home/nik# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
root@nikitaserv:/home/nik# bash wazuh-install.sh --wazuh-dashboard dashboard
14/12/2024 09:18:43 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
14/12/2024 09:18:43 INFO: Verbose logging redirected to /var/log/wazuh-install.log
14/12/2024 09:18:49 INFO: Verifying that your system meets the recommended minimum hardware requirements.
14/12/2024 09:18:49 INFO: Wazuh web interface port will be 443.
14/12/2024 09:18:54 INFO: --- Dependencies ----
14/12/2024 09:18:54 INFO: Installing debhelper.
14/12/2024 09:19:02 INFO: Wazuh repository added.
14/12/2024 09:19:02 INFO: --- Wazuh dashboard ----
14/12/2024 09:19:02 INFO: Starting Wazuh dashboard installation.
14/12/2024 09:19:29 INFO: Wazuh dashboard installation finished.
14/12/2024 09:19:29 INFO: Wazuh dashboard post-install configuration finished.
14/12/2024 09:19:29 INFO: Starting service wazuh-dashboard.
14/12/2024 09:19:30 INFO: wazuh-dashboard service started.
14/12/2024 09:19:44 INFO: Initializing Wazuh dashboard web application.
14/12/2024 09:19:44 INFO: Wazuh dashboard web application initialized.
14/12/2024 09:19:44 INFO: --- Summary ---
14/12/2024 09:19:44 INFO: You can access the web interface https://192.168.106.135:443
    User: admin
    Password: *AXKNpx713FhrfM1fITc5068hpb+n8Y*
14/12/2024 09:19:44 INFO: Installation finished.
root@nikitaserv:/home/nik#
```

Проверка правильности установки агента (отображение в Wazuh):

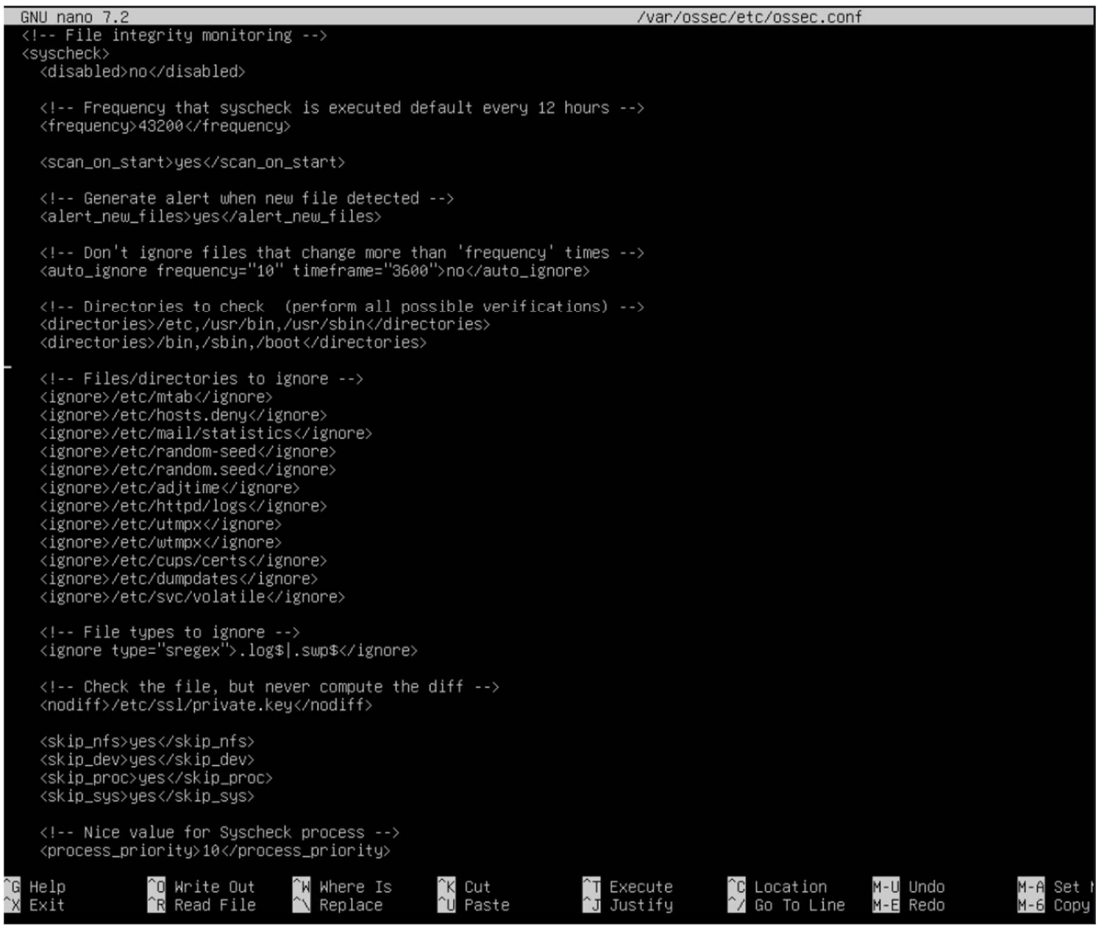




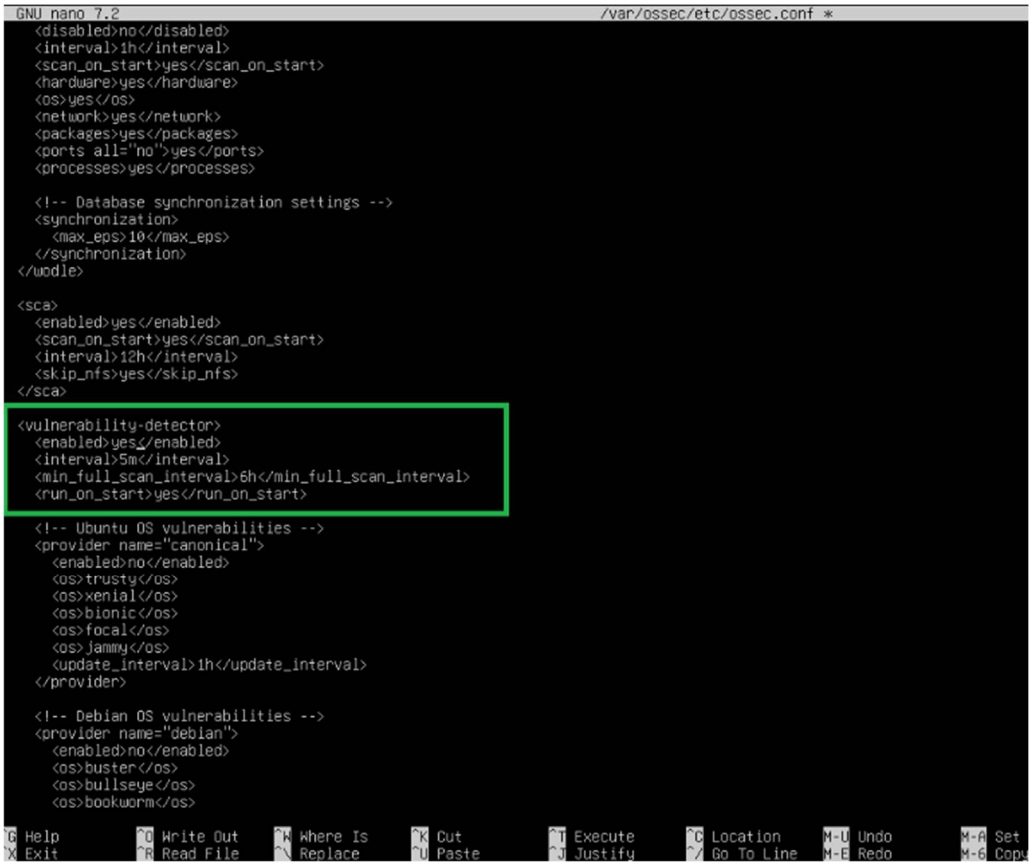
Детектор уязвимостей для установленного агента:



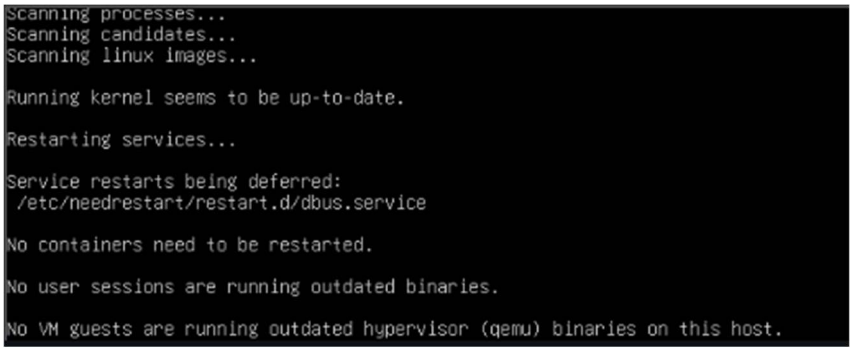
Создание проверки целостности файлов:



Настройка выявления уязвимостей:



Настройка выявления скрытых процессов:



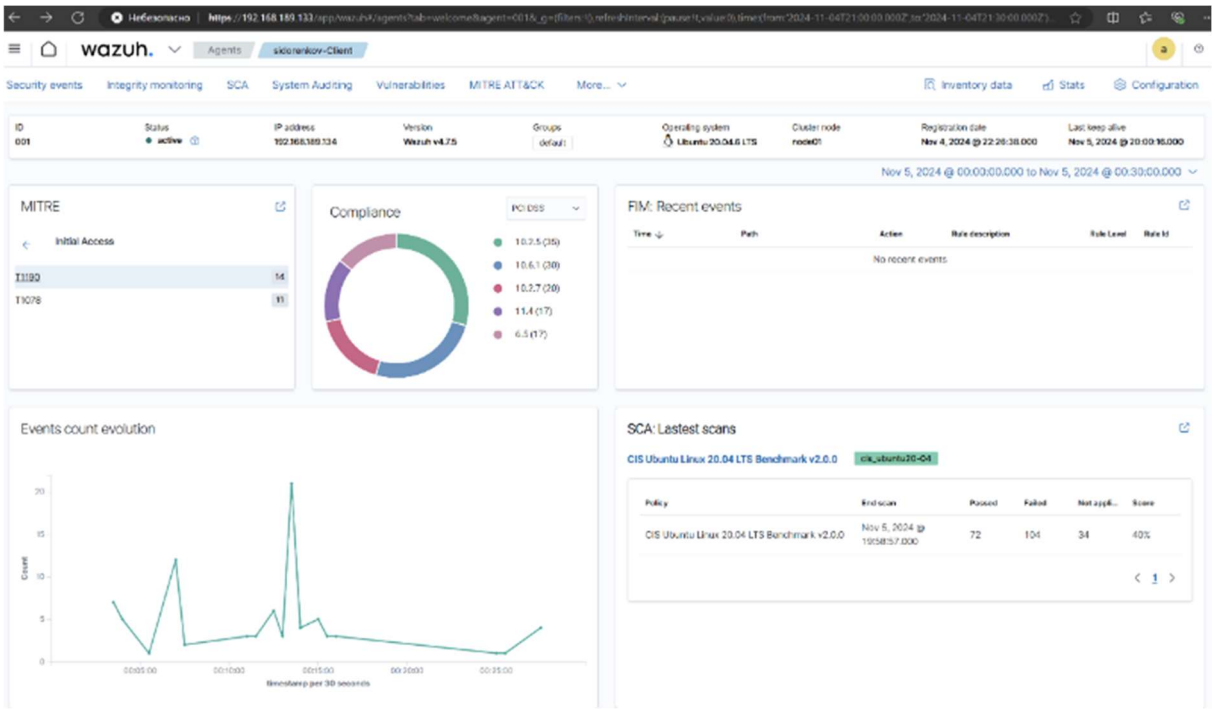
Настройка выявления SQL-инъекций:

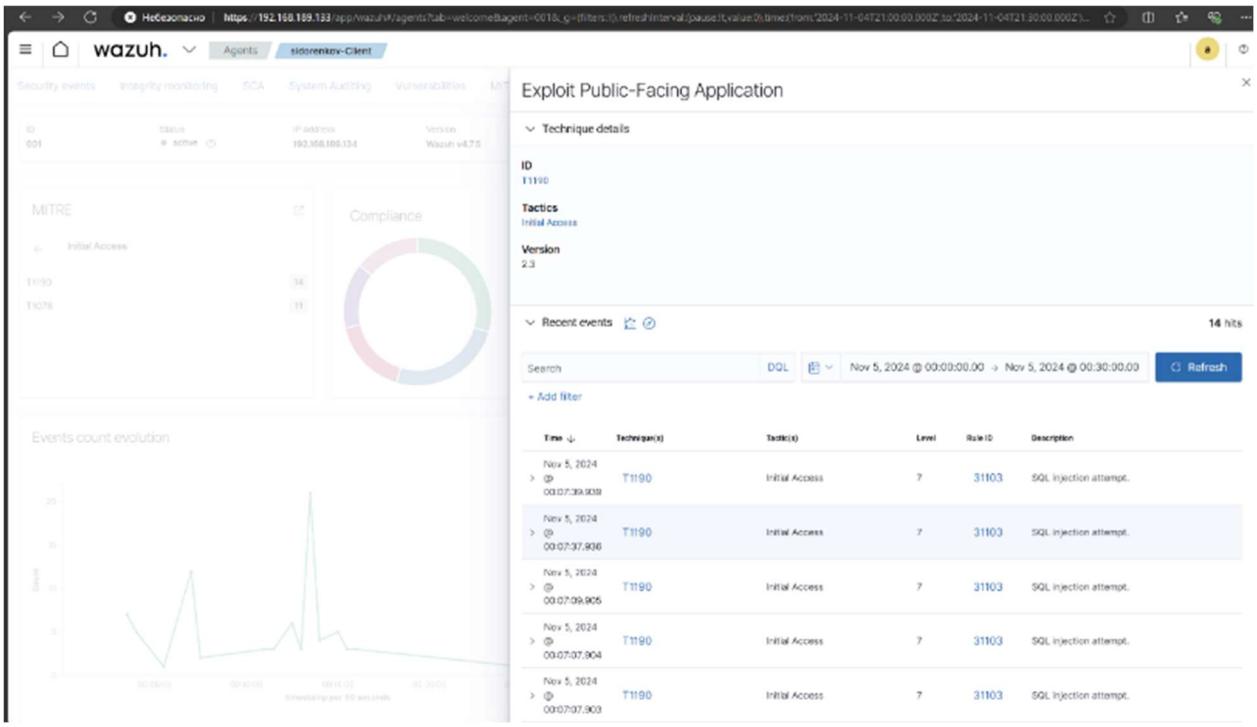
```
  GNU nano 7.2                                                    /var/ossec
<!--
  Wazuh - Manager - Default configuration for ubuntu 24.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <localfile>
    <lof_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>
```

Настройка выявления web shell attack:

```
  <!-- Log analysis -->
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
```

Проверка работы настроеннх ранее механизмов:




wazuh.
Agents
sidorenkov-Client
Exploit Public-Facing Application
Technique details
ID
T1190
Tactics
Initial Access
Version
2.3
Recent events
14 hits
Search
DQL
Nov 5, 2024 @ 00:00:00.00 → Nov 5, 2024 @ 00:30:00.00
Refresh
+ Add filter
Time
Technique(s)
Tactic(s)
Level
Rule ID
Description
Nov 5, 2024 @ 00:07:39.909
T1190
Initial Access
7
31103
SQL injection attempt.
Nov 5, 2024 @ 00:07:37.906
T1190
Initial Access
7
31103
SQL injection attempt.
Nov 5, 2024 @ 00:07:09.905
T1190
Initial Access
7
31103
SQL injection attempt.
Nov 5, 2024 @ 00:07:07.904
T1190
Initial Access
7
31103
SQL injection attempt.
Nov 5, 2024 @ 00:07:07.903
T1190
Initial Access
7
31103
SQL injection attempt.