

## Практика №3 по предмету СДССил - Wazuh

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

Развертывание ВМ:

Серверная ВМ:

```
* Support:      https://ubuntu.com/pro

System information as of Вт 10 дек 2024 17:41:53 UTC

System load:  0.5          Processes:           247
Usage of /:   27.8% of 23.45GB Users logged in:     0
Memory usage: 8%          IPv4 address for ens33: 192.168.106.131
Swap usage:   0%

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

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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

nik@wazuh:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e4:14:1f brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.106.131/24 metric 100 brd 192.168.106.255 scope global dynamic ens33
        valid_lft 1716sec preferred_lft 1716sec
    inet6 fe80::20c:29ff:ee4:141f/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
nik@wazuh:~$ ping 192.168.106.129
PING 192.168.106.129 (192.168.106.129) 56(84) bytes of data.
64 bytes from 192.168.106.129: icmp_seq=1 ttl=64 time=4.70 ms
64 bytes from 192.168.106.129: icmp_seq=2 ttl=64 time=1.55 ms
64 bytes from 192.168.106.129: icmp_seq=3 ttl=64 time=1.07 ms
64 bytes from 192.168.106.129: icmp_seq=4 ttl=64 time=1.35 ms
64 bytes from 192.168.106.129: icmp_seq=5 ttl=64 time=1.57 ms
^C
--- 192.168.106.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.068/2.049/4.701/1.338 ms
nik@wazuh:~$ _
```

Клиентская ВМ:

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    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 noprefixroute ens33
        valid_lft 1341sec preferred_lft 1341sec
    inet6 fe80::20c:29ff:fe49:f99e/64 scope link
        valid_lft forever preferred_lft forever
```

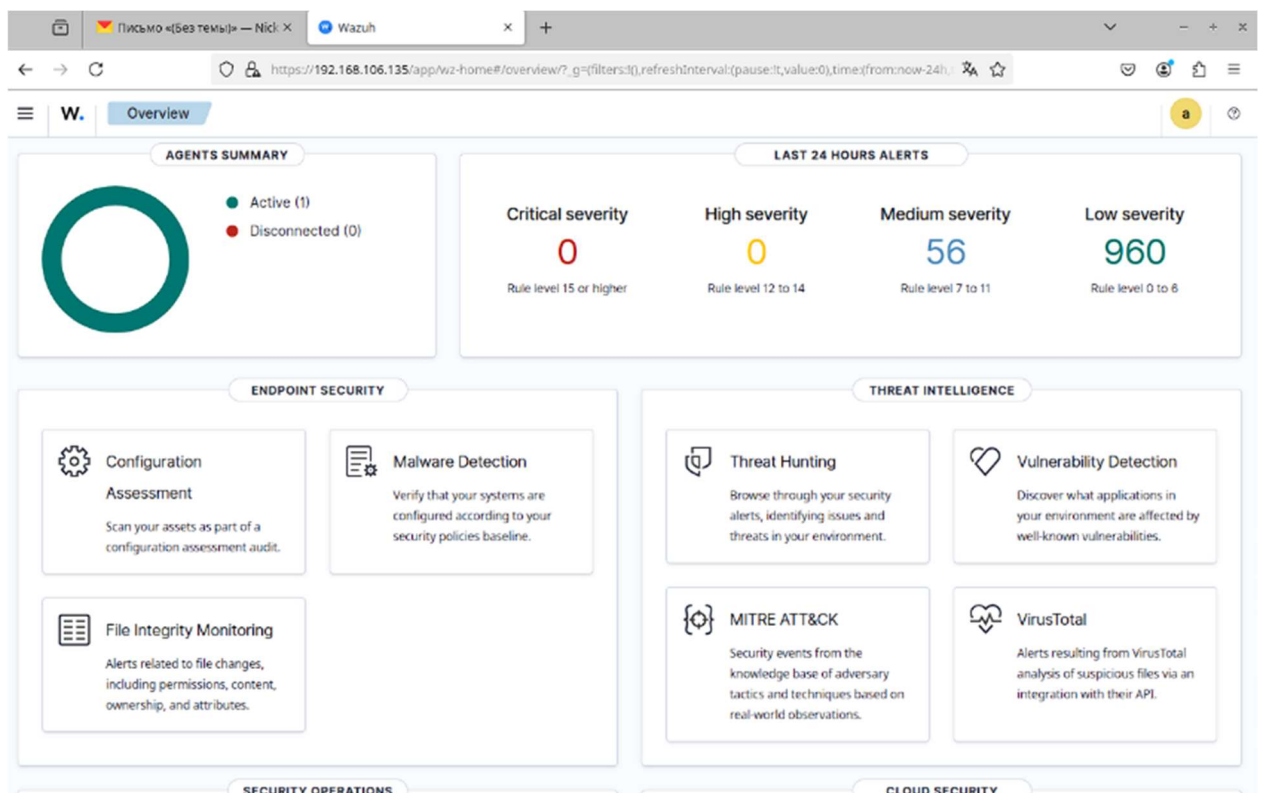
## Обеспечение сетевого обмена между 2 VM:

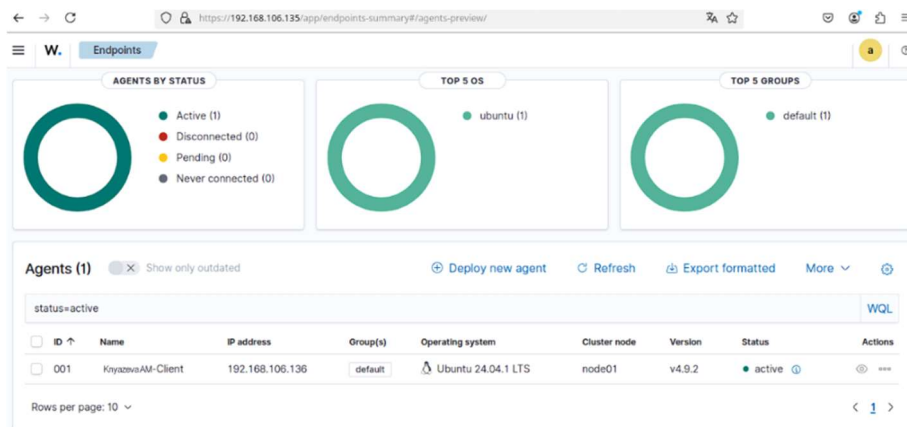
```
link/ether 00:0c:29:49:f9:9e brd ff:ff:ff:ff:ff:ff
aliasname enp2s1
inet 192.168.106.129/24 brd 192.168.106.255 scope global dynamic noprefixrou
te ens33
    valid_lft 1341sec preferred_lft 1341sec
inet6 fe80::20c:29ff:fe49:f99e/64 scope link
    valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$ 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 VM Wazuh-сервера:

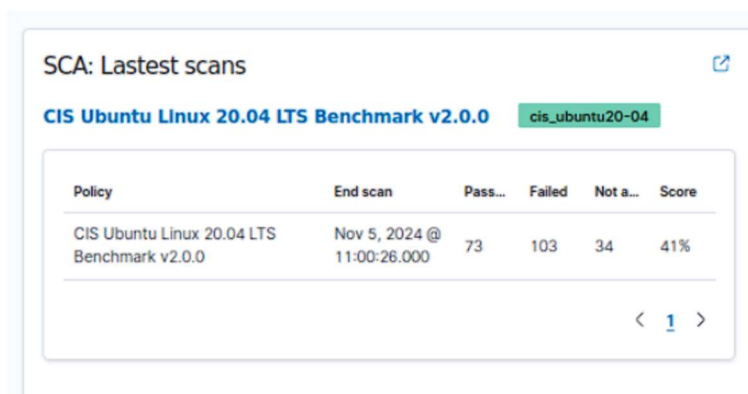
```
14/12/2024 09:17:58 INFO: Filebeat installation finished.
14/12/2024 09:17:59 INFO: Filebeat post-install configuration finished.
14/12/2024 09:18:00 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
14/12/2024 09:18:21 INFO: Starting service filebeat.
14/12/2024 09:18:23 INFO: filebeat service started.
14/12/2024 09:18:23 INFO: Installation finished.
root@nikitaser:~/home/nik# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
root@nikitaser:~/home/nik# bash wazuh-install.sh --wazuh-dashboard dashboard
14/12/2024 09:18:43 INFO: Starting Mazuh 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: Mazuh 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: Mazuh repository added.
14/12/2024 09:19:02 INFO: --- Mazuh dashboard ---
14/12/2024 09:19:02 INFO: Starting Mazuh dashboard installation.
14/12/2024 09:19:29 INFO: Mazuh dashboard installation finished.
14/12/2024 09:19:29 INFO: Mazuh 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 Mazuh dashboard web application.
14/12/2024 09:19:44 INFO: Mazuh 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: *AXXNpx713FhrfM1fITc5068hpbio8Y*
14/12/2024 09:19:44 INFO: Installation finished.
root@nikitaser:~/home/nik#
```

## Проверка правильности установки агента (отображение в Wazuh):





Детектор уязвимостей для установленного агента:



Создание проверки целостности файлов:

```
GNU nano 7.2 /var/ossec/etc/ossec.conf
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

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

  <scan_on_start>yes</scan_on_start>

  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>

  <!-- Don't ignore files that change more than 'frequency' times -->
  <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>

  <!-- File types to ignore -->
  <ignore type="sregex">.log$.sup$</ignore>

  <!-- Check the file, but never compute the diff -->
  <nodiff>/etc/ssl/private.key</nodiff>

  <skip_nfs>yes</skip_nfs>
  <skip_dev>yes</skip_dev>
  <skip_proc>yes</skip_proc>
  <skip_sys>yes</skip_sys>

  <!-- Nice value for Syscheck process -->
  <process_priority>10</process_priority>
```

## Настройка выявления уязвимостей:

```
GNU nano 7.2 /var/ossec/etc/ossec.conf *
<disabled>no</disabled>
<interval>1h</interval>
<scan_on_start>yes</scan_on_start>
<hardware>yes</hardware>
<os>yes</os>
<network>yes</network>
<packages>yes</packages>
<ports_all>'no'>yes</ports>
<processes>yes</processes>

<!-- Database synchronization settings -->
<synchronization>
  <max_eps>10</max_eps>
</synchronization>
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

<!-- Ubuntu OS vulnerabilities -->
<provider name="canonical">
  <enabled>no</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <os>jammy</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Debian OS vulnerabilities -->
<provider name="debian">
  <enabled>no</enabled>
  <os>buster</os>
  <os>bullseye</os>
  <os>bookworm</os>

G Help      W Write Out  R Where Is   K Cut        J Execute    C Location  M-U Undo    M-A Set
X Exit      R Read File  A Replace    U Paste      V Justify    G Go To Line M-E Redo    M-G Copy
```

## Настройка выявления скрытых процессов:

```
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...

Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service

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.
```

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
-->

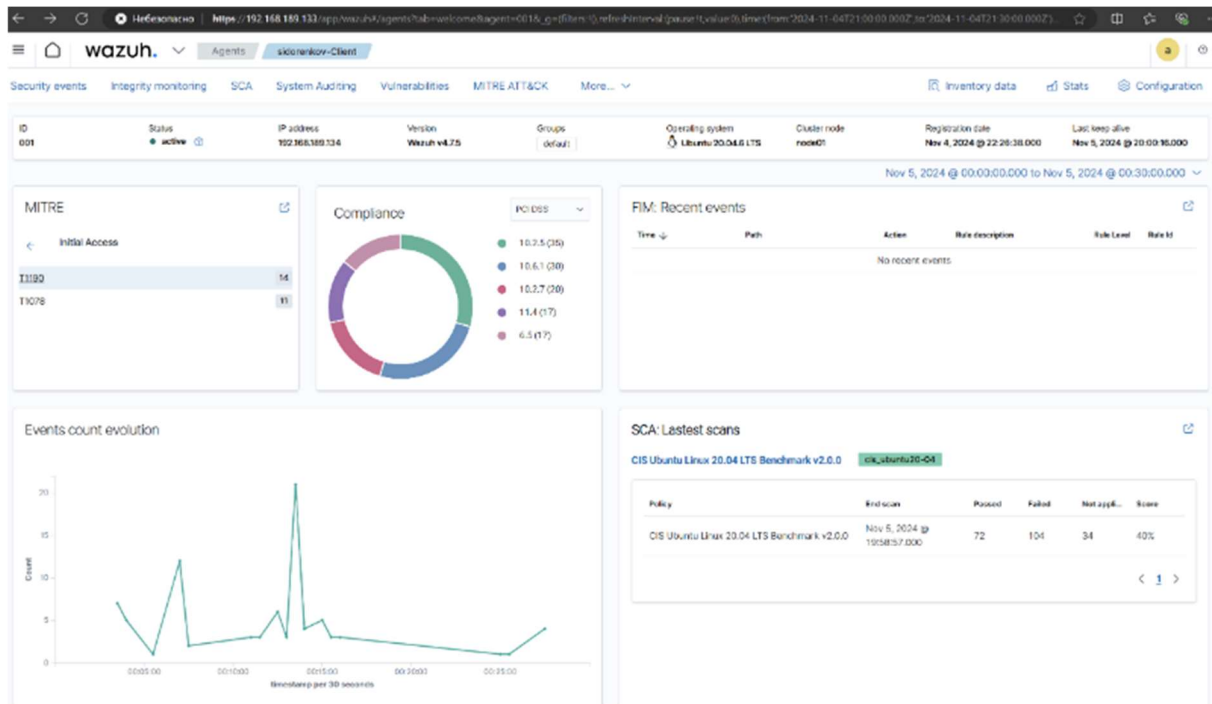
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  <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 настроенных ранее механизмов:



Wazuh

Agents

Windows-Client

Security events

Integrity monitoring

SCA

System Auditing

Vulnerability

MITRE

ID

001

Status

Active

IP address

192.168.100.134

Version

Wazuh v4.7.5

MITRE

Initial Access

T1190

T1078

Compliance

Events count evolution

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)	Tactics(s)	Level	Rule ID	Description
Nov 5, 2024 @ 00:07:39.939	T1190	Initial Access	7	31103	SQL injection attempt.
Nov 5, 2024 @ 00:07:37.936	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.