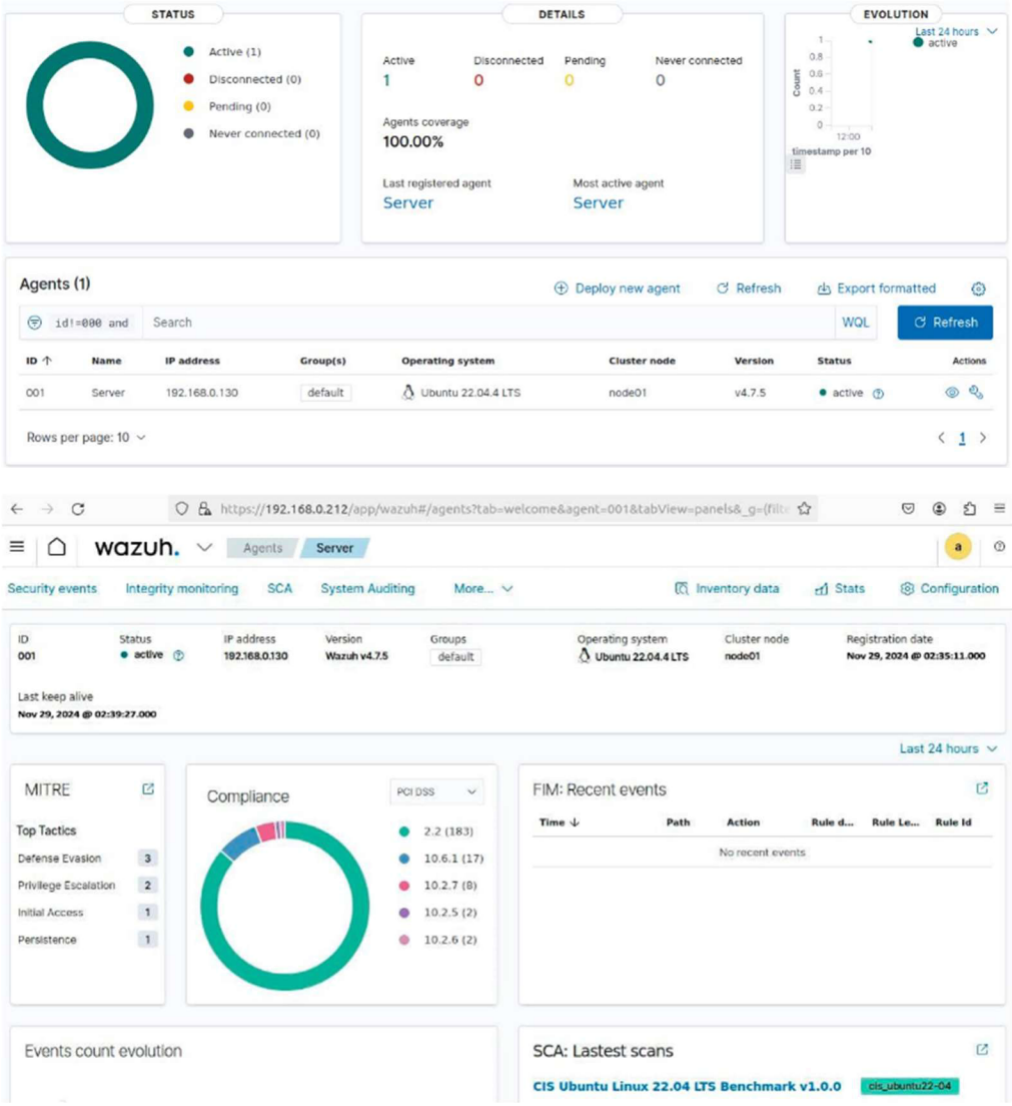
Практическая работа №5

Выполнил студент – Сапов Александр Дмитриевич группа: ББМО-02-23

Демонстрация подключения агента к серверу:



Разворачиваем IDS Суриката:

```
sssl@sssl-VirtualBox:~$ sudo docker pull quay.io/jasonish/suricata:latest
latest: Pulling from jasonish/suricata
9215f449d8af: Pull complete
f28531a8beee: Pull complete
e10638bcf333: Pull complete
ab5113f8cd48: Pull complete
26f0f0d9a56c: Pull complete
0f151f5dd0b5: Pull complete
bd30f7bbb2b5: Pull complete
cd39f002aba7: Pull complete
4f2a19df112d: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:89b300fb5d00f182359a1305543e828a804ede7f1685e75b05f607f7372428c6
Status: Downloaded newer image for quay.io/jasonish/suricata:latest
quay.io/jasonish/suricata:latest
sssl@sssl-VirtualBox:~$
```

Внесение изменений для дальнейшего сбора логов suricata в конфиг xdr wazuh

```
 GNU nano 6.2                  /var/ossec/etc/ossec.conf *
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>

  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>
```

Сканер уязвимостей NIKTO

Установка сканер уязвимостей Nikto:

```
root@Ubuntu:/home/knyaz# sudo apt install nikto -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libsigsegv2
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libwhisker2-perl
```

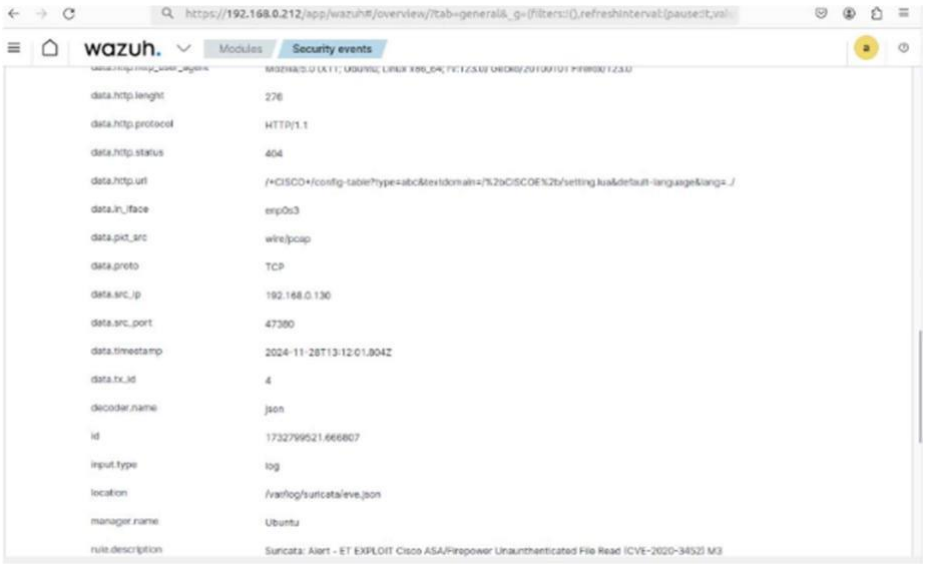
Устанавливает интерпретатор Perl:

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.34.1-1ubuntu1.11).
git set to manually installed.
perl is already the newest version (5.34.0-3ubuntu1.3).
perl set to manually installed.
The following package was automatically installed and is no longer required:
  libsigsegv2
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 271 not upgraded.
root@Ubuntu:/home/knyaz# git clone https://github.com/sullo/nikto.git
Cloning into 'nikto'...
remote: Enumerating objects: 7457, done.
remote: Counting objects: 100% (1477/1477), done.
remote: Compressing objects: 100% (513/513), done.
remote: Total 7457 (delta 1112), reused 1256 (delta 963), pack-reused 5980 (from
 1)
Receiving objects: 100% (7457/7457), 4.57 MiB | 3.68 MiB/s, done.
Resolving deltas: 100% (5422/5422), done.
```

Запуск Nikto:

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.0.212
+ Target Hostname:    192.168.0.212
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /C=US/L=California/O=Wazuh/OU=Wazuh/CN=wazuh-dashboa
rd
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer:  /OU=Wazuh/O=Wazuh/L=California
+ Start Time:         2024-11-28 02:20:17 (GMT3)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Uncommon header 'osd-name' found, with contents: Ubuntu
+ Uncommon header 'x-frame-options' found, with contents: sameorigin
+ Cookie security_authentication created without the secure flag
+ Cookie security_authentication created without the httponly flag
+ Root page / redirects to: /app/login?
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '192.168.0.212' does not match certificate's CN 'wazuh-dashboard'
```

События от сурикаты в SIEM:



Полная установка Yara:

```
root@Ubuntu:/home/knyaz/yara-4.2.1# sudo make install
Making install in libyara
make[1]: Entering directory '/home/knyaz/yara-4.2.1/libyara'
make  install-am
make[2]: Entering directory '/home/knyaz/yara-4.2.1/libyara'
make[3]: Entering directory '/home/knyaz/yara-4.2.1/libyara'
 /usr/bin/mkdir -p '/usr/local/lib'
 /bin/bash ../libtool   --mode=install /usr/bin/install -c   libyara.la '/usr/lo
cal/lib'
libtool: install: /usr/bin/install -c .libs/libyara.so.9.0.1 /usr/local/lib/liby
ara.so.9.0.1
libtool: install: (cd /usr/local/lib && { ln -s -f libyara.so.9.0.1 libyara.so.9
 || { rm -f libyara.so.9 && ln -s libyara.so.9.0.1 libyara.so.9; }; })
libtool: install: (cd /usr/local/lib && { ln -s -f libyara.so.9.0.1 libyara.so |
| { rm -f libyara.so && ln -s libyara.so.9.0.1 libyara.so; }; })
libtool: install: /usr/bin/install -c .libs/libyara.lai /usr/local/lib/libyara.l
a
libtool: install: /usr/bin/install -c .libs/libyara.a /usr/local/lib/libyara.a
libtool: install: chmod 644 /usr/local/lib/libyara.a
libtool: install: ranlib /usr/local/lib/libyara.a
libtool: finish: PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/
bin:/snap/bin:/sbin" ldconfig -n /usr/local/lib
----------------------------------------------------------------------
```

Конфигурационный файл активного реагирования под утилиту yara:

```
  GNU nano 6.2                  /var/ossec/active-responce/bin/yara.sh *
#!/bin/bash
# Wazuh - Yara active response
# Copyright (C) 2015-2022, Wazuh Inc.
#
# This program is free software; you can redistribute it
# and/or modify it under the terms of the GNU General Public
# License (version 2) as published by the FSF - Free Software
# Foundation.


#------------------------ Gather parameters ------------------------#

# Extra arguments
read INPUT_JSON
YARA_PATH=$(echo $INPUT_JSON | jq -r .parameters.extra_args[1])
YARA_RULES=$(echo $INPUT_JSON | jq -r .parameters.extra_args[3])
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.syscheck.path)

#Set LOG_FILE path
LOG_FILE="logs/active-response.log"

size=0
actual_size=$(stat -c %s ${FILENAME})
while [ ${size} -ne ${actual_size} ]; do
    sleep 1
    size=${actual_size}
    actual_size=$(stat -c %s ${FILENAME})
done

#------------------------ Analyze parameters ------------------------#

if [[ ! $YARA_PATH ]] || [[ ! $YARA_RULES ]]
then
```

Просмотр сработавших правил в истории логов: