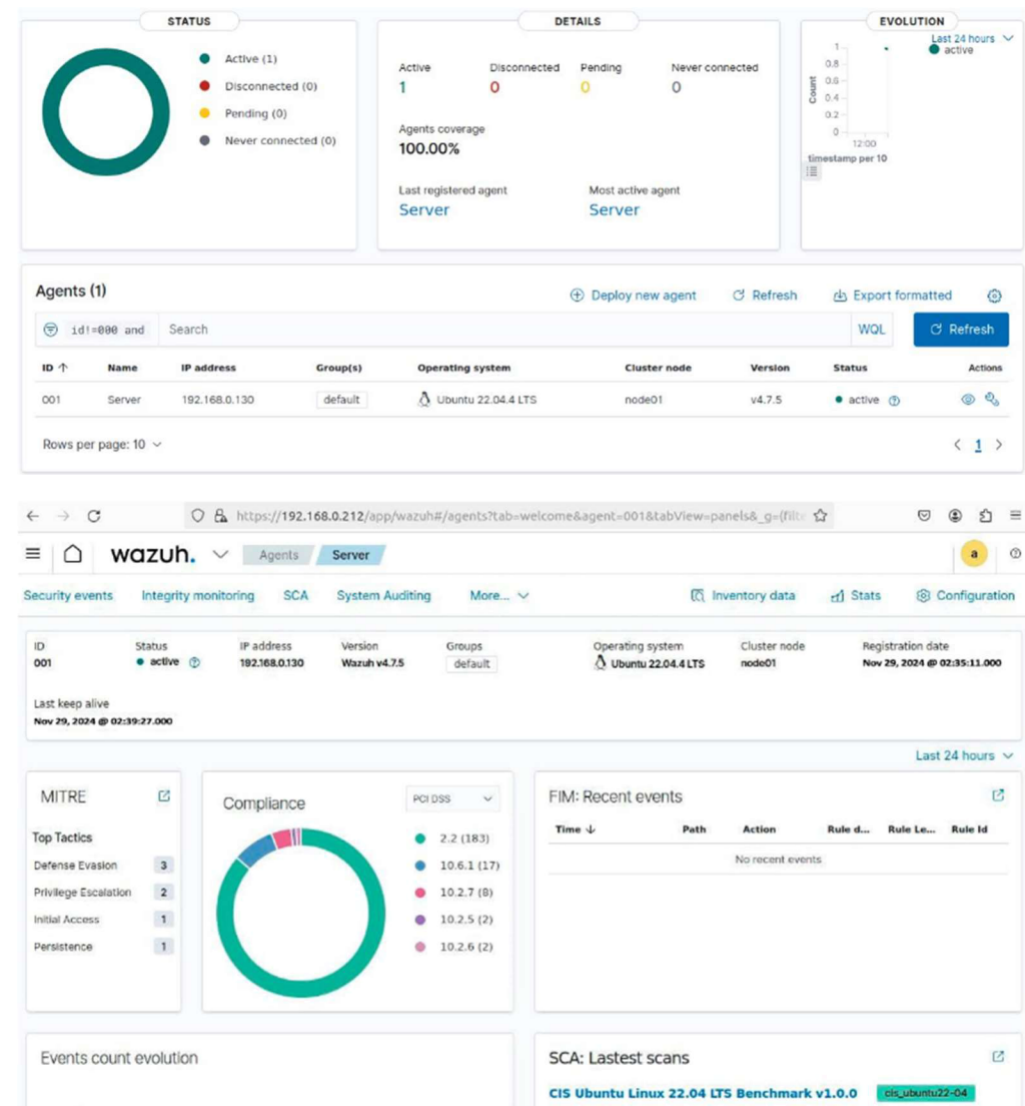


Практическая работа №5

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:

← → ↺

https://192.168.0.212/app/wazuh#overview/tab-general&\_g=(filters:(),refreshinterval(pause:0,va

🔍 👤 🏠 ≡

☰ 🏠 wazuh. ▾

Modules Security events

🔔 ⚙

data.http.length276

data.http.protocolHTTP/1.1

data.http.status404

data.http.url/+CISCO+/config-table?type=abc&devIdonah+%2DCISCOE%2b/setting.htmldefault-langauge&lang=.

data.in\_ifaceenp0s3

data.pkt\_sr/wire/pkcap

data.protoTCP

data.src\_ip192.168.0.130

data.src\_port47380

data.timestamp2024-11-28T13:12:01.804Z

data.tx\_id4

decoder.namejson

id1732799521.666807

input.typelog

location/var/log/suricata/eve.json

manager.nameUbuntu

rule.descriptionSuricata: Alert - ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read CVE-2020-34525 M3

## 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/local/lib'
libtool: install: /usr/bin/install -c .libs/libyara.so.9.0.1 /usr/local/lib/libyara.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.la
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" ldconfig -n /usr/local/lib
.....
```

## Конфигурационный файл активного реагирования под утилиту yara:

```
GNU nano 6.2 /var/ossec/active-response/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:**

← → ↺ [https://192.168.0.212/app/wazuh#/overview/?tab=general&\\_q={filters:{},refreshInterval:\(pause,{val...](https://192.168.0.212/app/wazuh#/overview/?tab=general&_q={filters:{},refreshInterval:(pause,{val...)

≡ 🏠 wazuh. ▾ Modules Security events ⓘ

@timestamp	2024-11-28T12:09:37.699Z
_id	9aatcpM87_1zE9dZTr58
agent.id	001
agent.ip	192.168.0.212
agent.name	server
decoder.name	ossec-syscheck-audit
full_log	File /home/impacket/test/doorpc/test_isad.py added Mode: realtime
id	1732795777.666016
input.type	log
location	syscheck
manager.name	Ubuntu
rule.description	File added to /home directory.
rule.firedtimes	342
rule.groups	syscheck
rule.id	100301
rule.level	7
rule.mali	false

[https://192.168.0.212/app/wazuh#/overview/?tab=general&\\_q={filters:{},refreshInterval\(pause:t,v\)}](https://192.168.0.212/app/wazuh#/overview/?tab=general&_q={filters:{},refreshInterval(pause:t,v)})

Modules Security events

@timestamp	2024-11-28T12:09:29.688Z
_id	9KatzpM87_1zE9cZNDSO
agent.id	001
agent.ip	192.168.0.212
agent.name	server
decoder.name	yara_decoder
full_log	wazuh-yara: INFO - Scan result: Impacket [{"id":"BsnkIOFsty6GEY3AcfpCd","fingerprint":"8f78bd35375bd6752d18464h4545676bvd56qwc382ngd957482tndc78545n32","version":"","creation_date":"2020-08-01","first_imported":"2021-12-30","last_modified":"2021-12-30","status":"RELEASED","sharing":"TLP:WHITE",so urce":"BARTBLAZE","author":"@bartblaze","description":"Identifies Impacket, a collection of Python classes for working with network protocols.",category:"TOOL",tool:"IMPACKET",mitre_att":"S0357","reference":"https://github.com/SecureAythCorp/impacket"/home/ impacket/impacket/csrc/v5/dnsuapi.py}
id	1732795769.665565
input.type	log
location	/var/ossec/logs/active-responses.log
manager.name	Ubuntu
rule.description	File "" is a positive match. Yara rule:
rule.firedtimes	30
rule.groups	yara
rule.id	106001