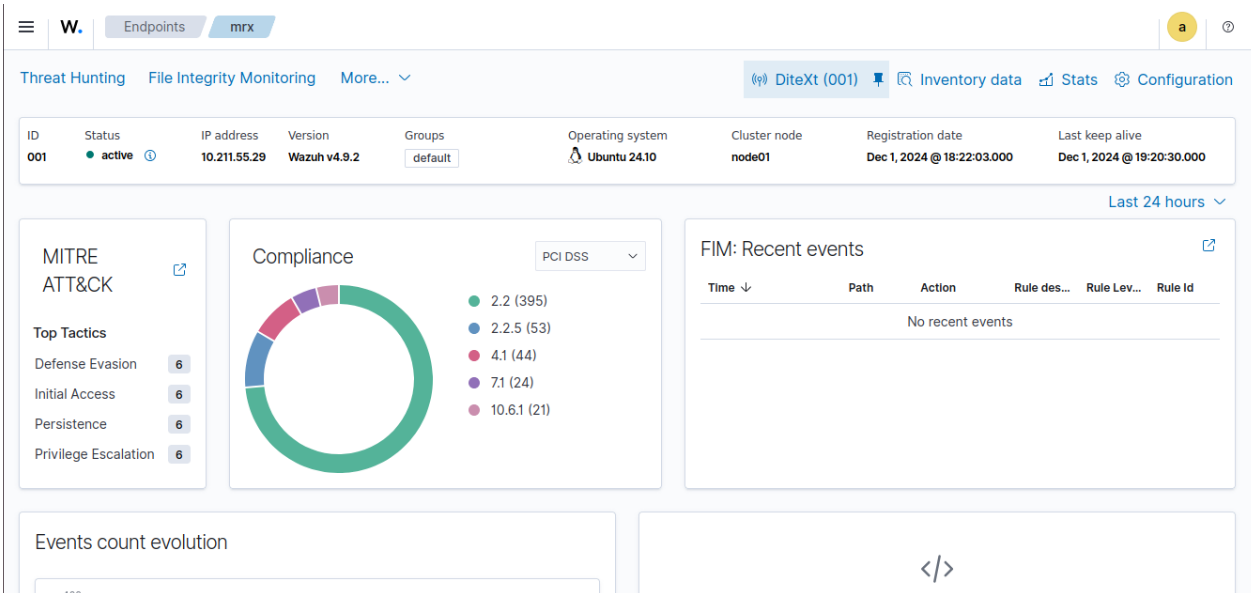
Практическая работа №5

Выполнил студент группы ББМО-02-23 Ионов Максим Сергеевич

Ход работы

1) Используя навыки полученные на предыдущем практическом занятии, устанавливаем Wazuh и подключаем агента



ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	● active	10.211.55.29	Wazuh v4.9.2	default	Ubuntu 24.10	node01	Dec 1, 2024 @ 18:22:03.000	Dec 1, 2024 @ 19:20:30.000

MITRE ATT&CK

Top Tactics

Defense Evasion	6
Initial Access	6
Persistence	6
Privilege Escalation	6

Compliance

PCI DSS

- ● 2.2 (395)
- ● 2.2.5 (53)
- ● 4.1 (44)
- ● 7.1 (24)
- ● 10.6.1 (21)

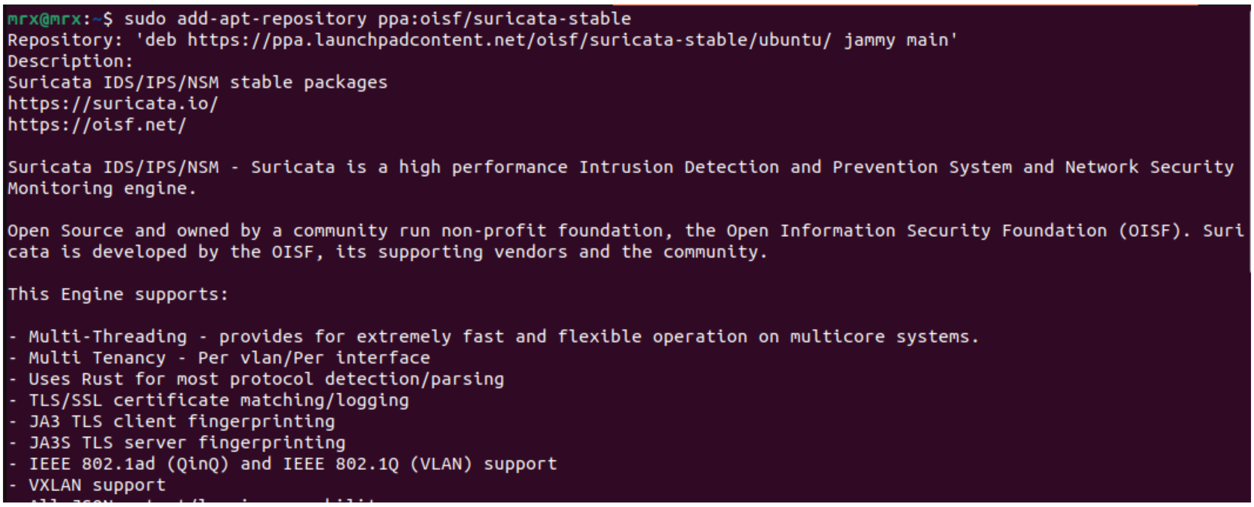
FIM: Recent events

Time	Path	Action	Rule des...	Rule Lev...	Rule Id

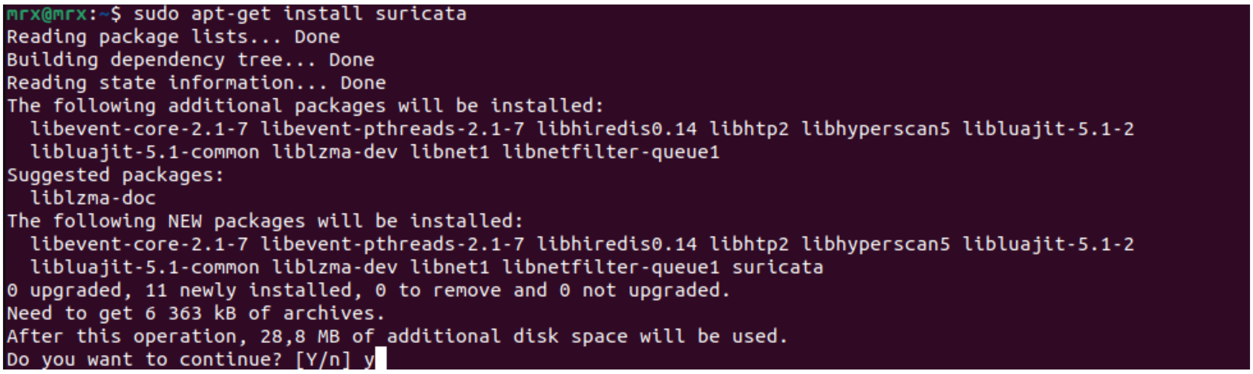
No recent events

Events count evolution

2) Устанавливаем и запускам Suricata

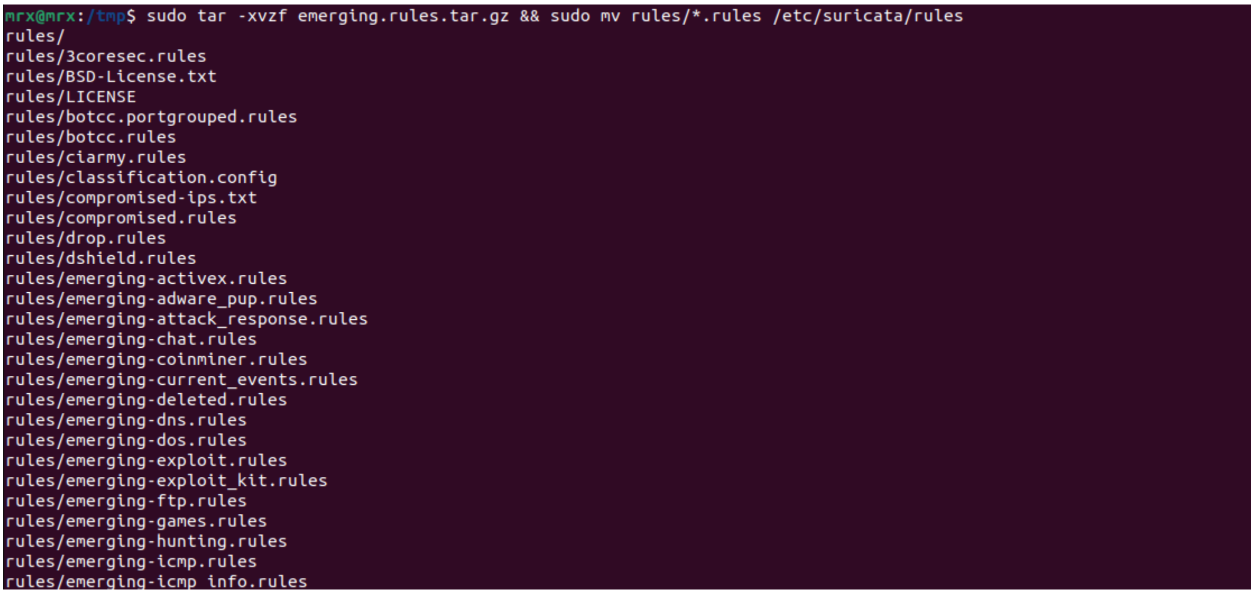


```
mrx@mrx:~$ sudo add-apt-repository ppa:oisf/suricata-stable
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy main'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security
Monitoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suri
cata is developed by the OISF, its supporting vendors and the community.

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
```

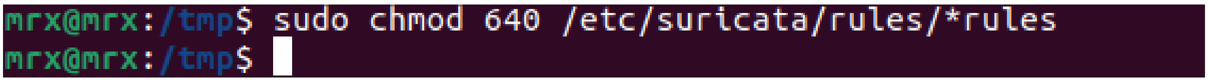


```
mrx@mrx:~$ sudo apt-get install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2
  libluajit-5.1-common liblzma-dev libnet1 libnetfilter-queue1
Suggested packages:
  liblzma-doc
The following NEW packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2
  libluajit-5.1-common liblzma-dev libnet1 libnetfilter-queue1 suricata
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 6 363 kB of archives.
After this operation, 28,8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

3) Скачиваем набор правил

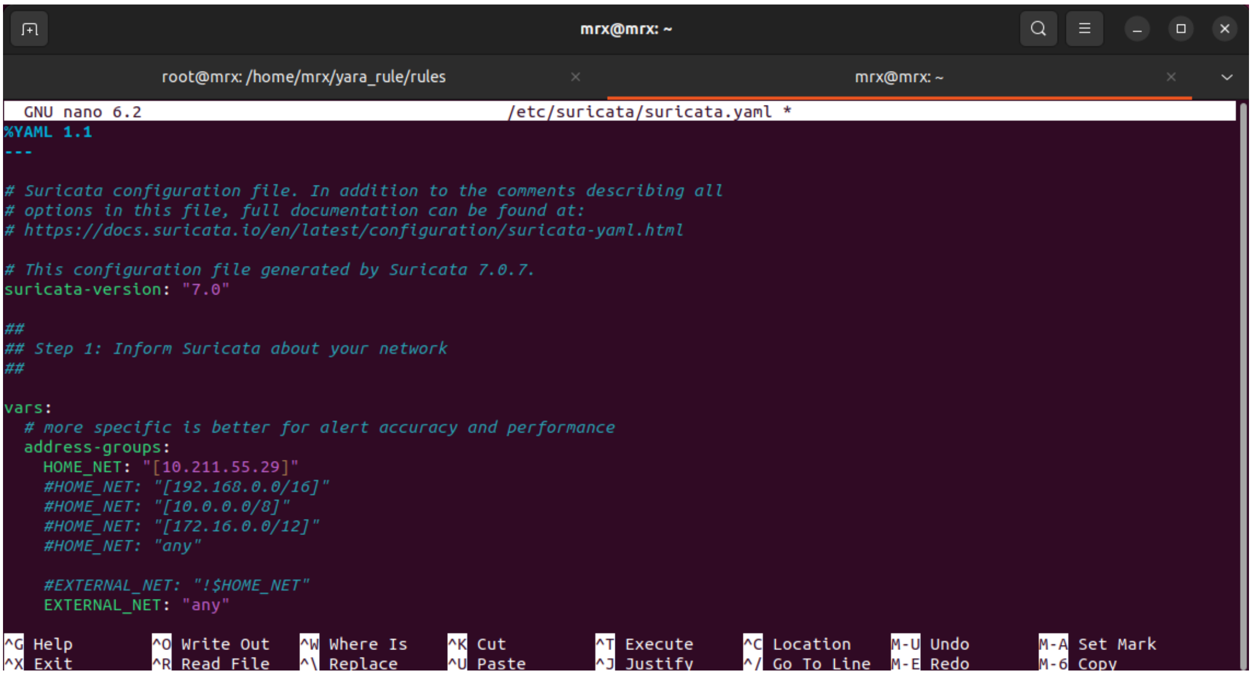


```
mrx@mrx:/tmp$ sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules
rules/
rules/3coresec.rules
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/drop.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-adware_pup.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coinminer.rules
rules/emerging-current_events.rules
rules/emerging-deleted.rules
rules/emerging-dns.rules
rules/emerging-dos.rules
rules/emerging-exploit.rules
rules/emerging-exploit_kit.rules
rules/emerging-ftp.rules
rules/emerging-games.rules
rules/emerging-hunting.rules
rules/emerging-icmp.rules
rules/emerging-icmp_info.rules
```



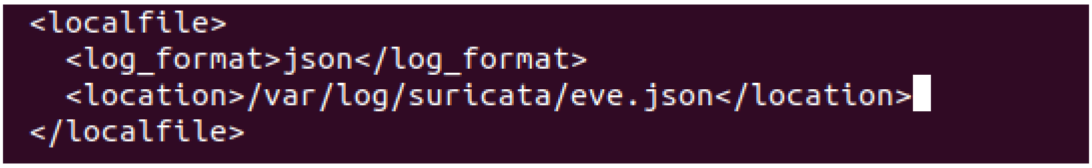
```
mrx@mrx:/tmp$ sudo chmod 640 /etc/suricata/rules/*rules
mrx@mrx:/tmp$ 
```

4) Настраиваем Suricata



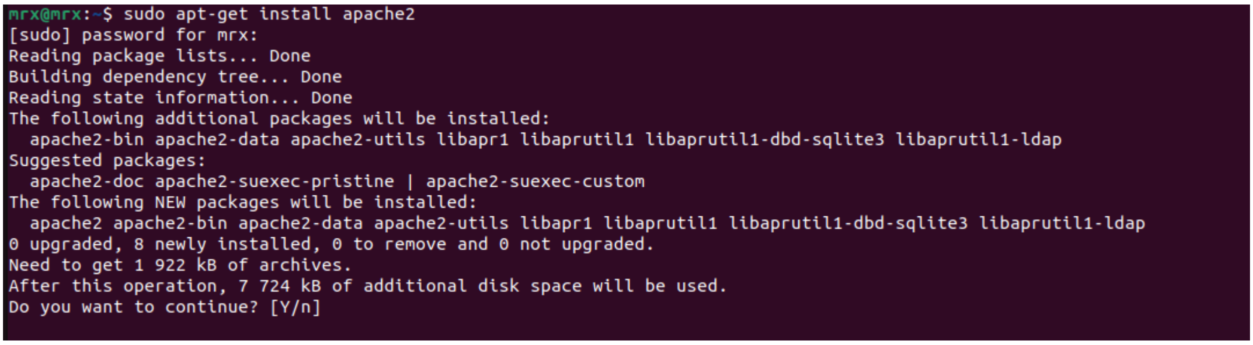
```
  GNU nano 6.2                         /etc/suricata/suricata.yaml *
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.7.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[10.211.55.29]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    #EXTERNAL_NET: "!$HOME_NET"
    EXTERNAL_NET: "any"

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location   M-U Undo    M-A Set Mark
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line M-E Redo    M-6 Copy
```

5) Подключаем логи Suricata в Wazuh

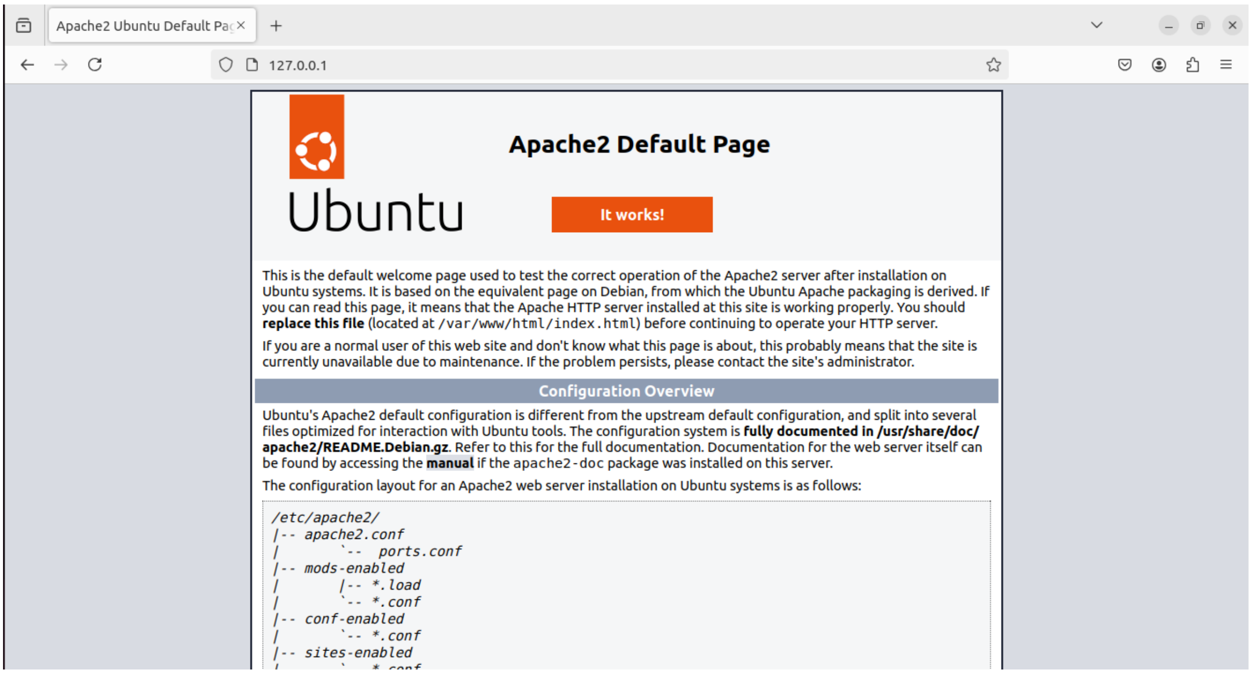


```
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
```

6) Устанавливаем и запускаем Apache



```
mrx@mrx:~$ sudo apt-get install apache2
[sudo] password for mrx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 1 922 kB of archives.
After this operation, 7 724 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

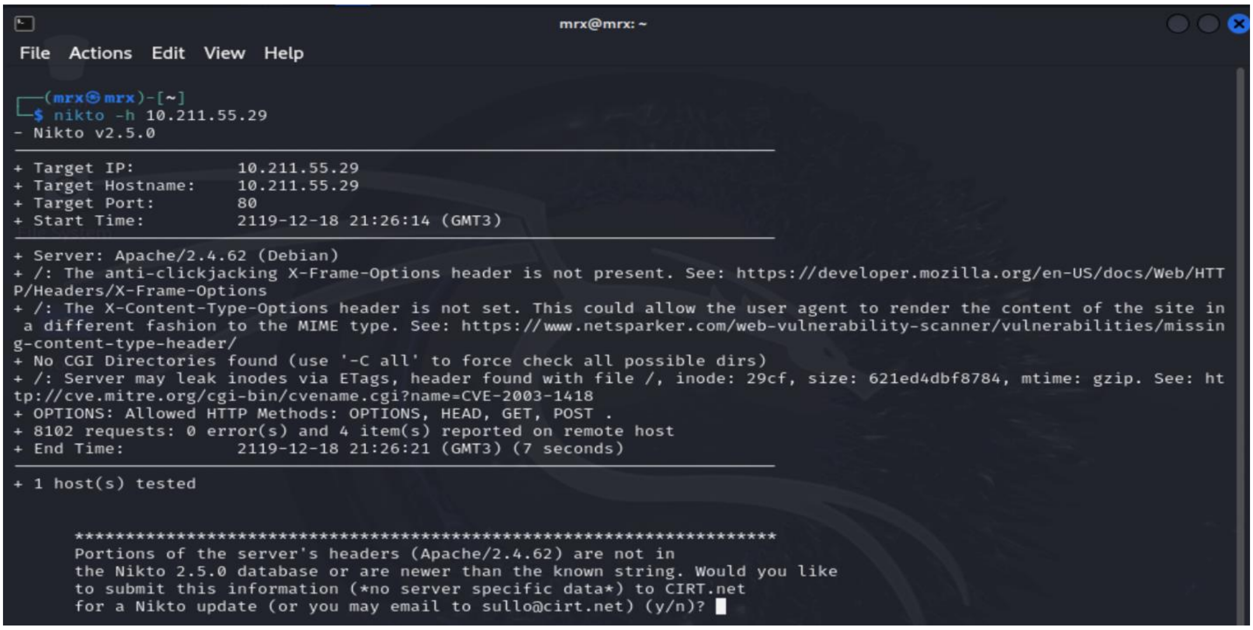
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

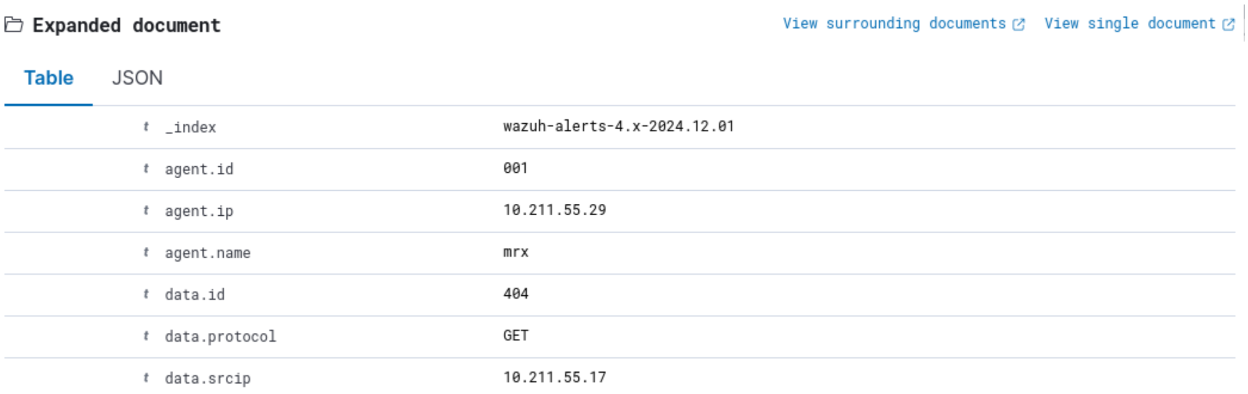
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
```

7) Запустим сканирование с помощью Nikto



```
┌──(mrx㉿mrx)-[~]
└─$ nikto -h 10.211.55.29
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.211.55.29
+ Target Hostname:    10.211.55.29
+ Target Port:        80
+ Start Time:         2119-12-18 21:26:14 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTT
P/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
 a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missin
g-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 621ed4dbf8784, mtime: gzip. See: ht
tp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ 8102 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2119-12-18 21:26:21 (GMT3) (7 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (Apache/2.4.62) are not in
      the Nikto 2.5.0 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)?
```

8) Смотрим вывод полученный от Suricata



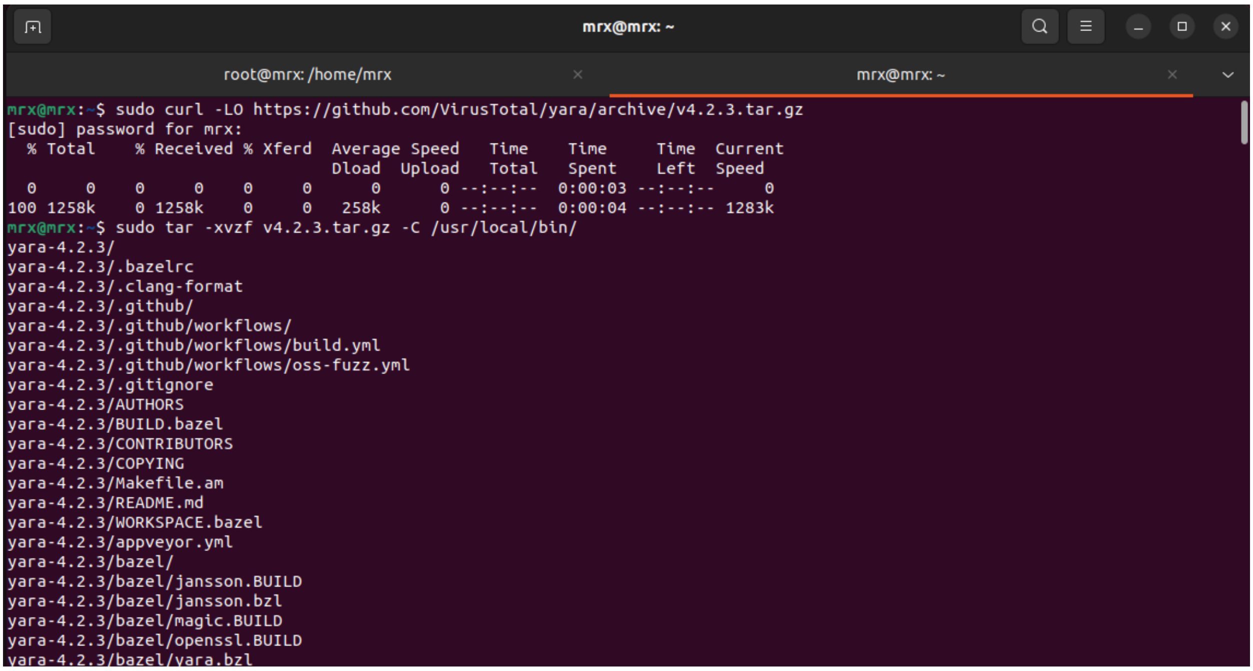
Expanded document

View surrounding documents View single document

Table JSON

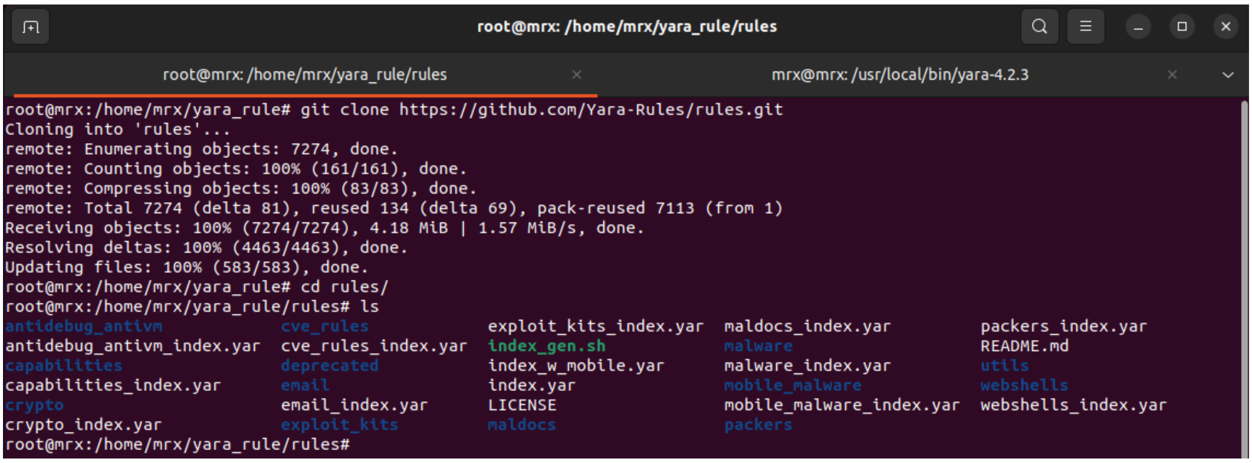
_index	wazuh-alerts-4.x-2024.12.01
agent.id	001
agent.ip	10.211.55.29
agent.name	mrx
data.id	404
data.protocol	GET
data.srcip	10.211.55.17

9) Устанавливаем и запускаем YARA



```
mrx@mrx:~$ sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
[sudo] password for mrx:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:03 --:--:--     0
100 1258k    0 1258k    0     0   258k      0 --:--:--  0:00:04 --:--:-- 1283k
mrx@mrx:~$ sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/
yara-4.2.3/
yara-4.2.3/.bazelrc
yara-4.2.3/.clang-format
yara-4.2.3/.github/
yara-4.2.3/.github/workflows/
yara-4.2.3/.github/workflows/build.yml
yara-4.2.3/.github/workflows/oss-fuzz.yml
yara-4.2.3/.gitignore
yara-4.2.3/AUTHORS
yara-4.2.3/BUILD.bazel
yara-4.2.3/CONTRIBUTORS
yara-4.2.3/COPYING
yara-4.2.3/Makefile.am
yara-4.2.3/README.md
yara-4.2.3/WORKSPACE.bazel
yara-4.2.3/appveyor.yml
yara-4.2.3/bazel/
yara-4.2.3/bazel/jansson.BUILD
yara-4.2.3/bazel/jansson.bzl
yara-4.2.3/bazel/magic.BUILD
yara-4.2.3/bazel/openssl.BUILD
yara-4.2.3/bazel/yara.bzl
```

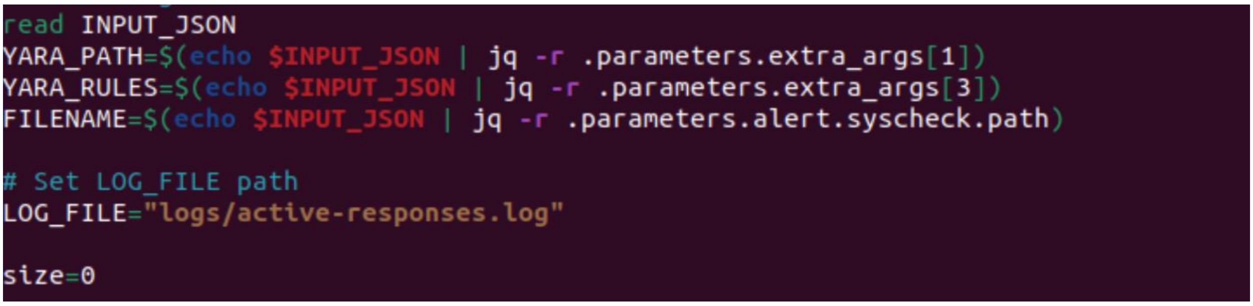
10) Скачиваем набор правил



root@mrx: /home/mrx/yara_rule/rules
root@mrx: /home/mrx/yara_rule/rules
mrx@mrx: /usr/local/bin/yara-4.2.3

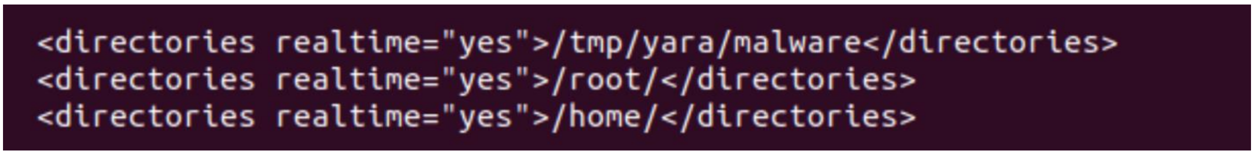
```
root@mrx:/home/mrx/yara_rule# git clone https://github.com/Yara-Rules/rules.git
Cloning into 'rules'...
remote: Enumerating objects: 7274, done.
remote: Counting objects: 100% (161/161), done.
remote: Compressing objects: 100% (83/83), done.
remote: Total 7274 (delta 81), reused 134 (delta 69), pack-reused 7113 (from 1)
Receiving objects: 100% (7274/7274), 4.18 MiB | 1.57 MiB/s, done.
Resolving deltas: 100% (4463/4463), done.
Updating files: 100% (583/583), done.
root@mrx:/home/mrx/yara_rule# cd rules/
root@mrx:/home/mrx/yara_rule/rules# ls
antidebug_antivm            cve_rules            exploit_kits_index.yar  maldocs_index.yar          packers_index.yar
antidebug_antivm_index.yar  cve_rules_index.yar  index_gen.sh            malware                    README.md
capabilities                deprecated           index_w_mobile.yar      malware_index.yar          utils
capabilities_index.yar      email                index.yar               mobile_malware             webshells
crypto                      email_index.yar      LICENSE                 mobile_malware_index.yar   webshells_index.yar
crypto_index.yar            exploit_kits         maldocs                 packers
root@mrx:/home/mrx/yara_rule/rules#
```

11) Создаем конфигурацию для YARA



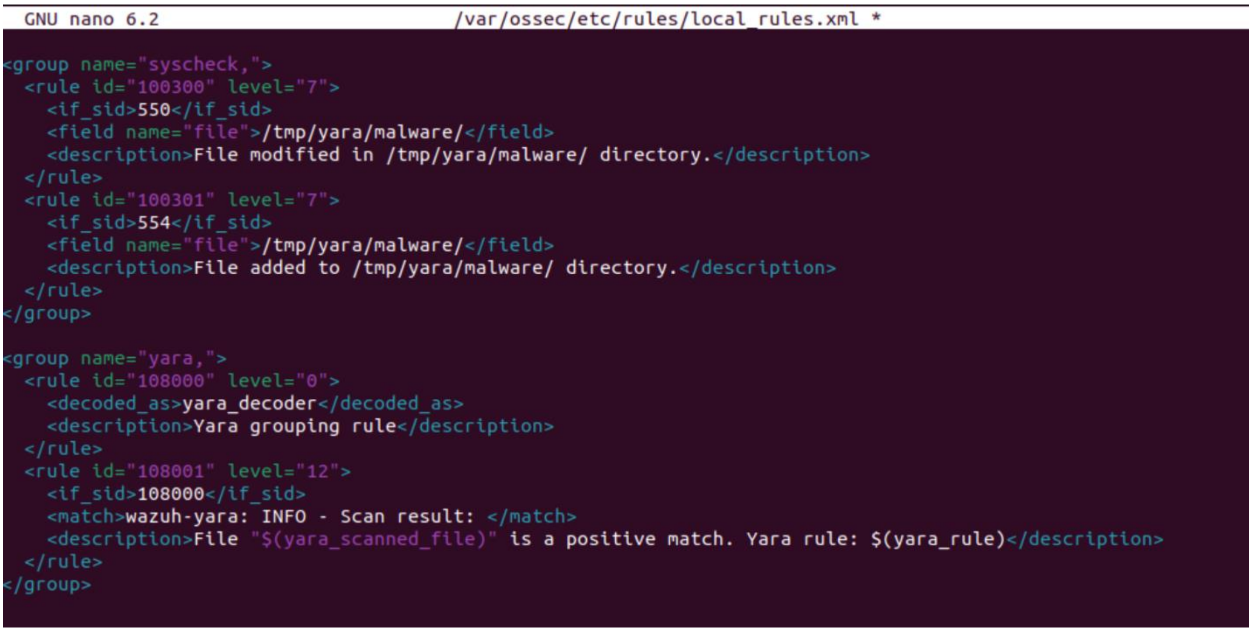
```
read INPUT_JSON
YARA_PATH=$(echo $INPUT_JSON | jq -r .parameters.extra_args[1])
YARA_RULES=$(echo $INPUT_JSON | jq -r .parameters.extra_args[3])
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.syscheck.path)

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

size=0
```

12) Добавляем в Wazuh

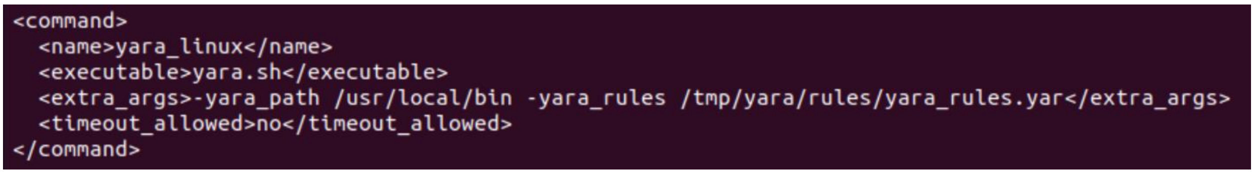


```
  <directories realtime="yes">/tmp/yara/malware</directories>
  <directories realtime="yes">/root/</directories>
  <directories realtime="yes">/home/</directories>
```

13) Проводим настройку на сервере



```
  GNU nano 6.2                          /var/ossec/etc/rules/local_rules.xml *

<group name="syscheck,">
  <rule id="100300" level="7">
    <if_sid>550</if_sid>
    <field name="file">/tmp/yara/malware/</field>
    <description>File modified in /tmp/yara/malware/ directory.</description>
  </rule>
  <rule id="100301" level="7">
    <if_sid>554</if_sid>
    <field name="file">/tmp/yara/malware/</field>
    <description>File added to /tmp/yara/malware/ directory.</description>
  </rule>
</group>

<group name="yara,">
  <rule id="108000" level="0">
    <decoded_as>yara_decoder</decoded_as>
    <description>Yara grouping rule</description>
  </rule>
  <rule id="108001" level="12">
    <if_sid>108000</if_sid>
    <match>wazuh-yara: INFO - Scan result: </match>
    <description>File "$(yara_scanned_file)" is a positive match. Yara rule: $(yara_rule)</description>
  </rule>
</group>
```



```
<command>
  <name>yara_linux</name>
  <executable>yara.sh</executable>
  <extra_args>-yara_path /usr/local/bin -yara_rules /tmp/yara/rules/yara_rules.yar</extra_args>
  <timeout_allowed>no</timeout_allowed>
</command>
```