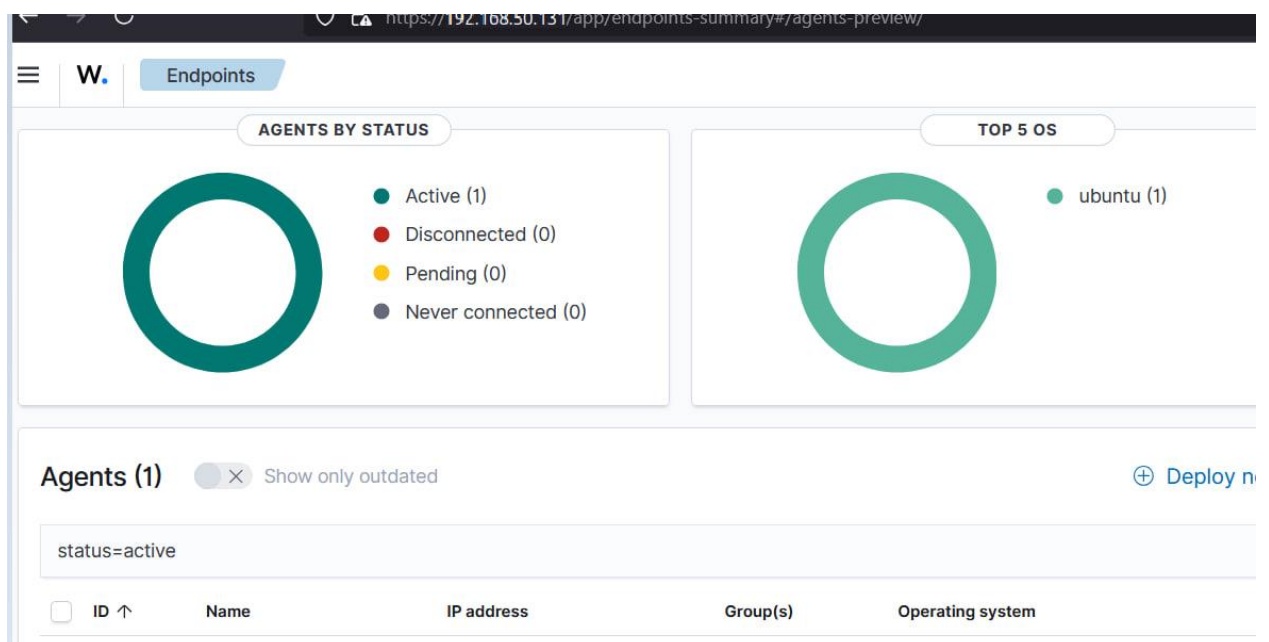


Для данной работы были использованы ВМ с **wazuh**, которые были созданы ранее в процессе 3 Практики

```
blagorazumov1@ubuntu: ~  
blagorazumov1@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  
        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:29:45:89:88 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.50.131/24 brd 192.168.50.255 scope global dynamic noprefixroute ens33  
        valid_lft 1133sec preferred_lft 1133sec  
    inet6 fe80::d0d9:fa41:4020:8ebd/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
blagorazumov1@ubuntu:~$
```



```
blagorazumov1@ubuntu: ~  
blagorazumov1@ubuntu:~$ sudo add-apt-repository ppa:oisf/suricata-stable  
[sudo] password for blagorazumov1:  
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  
em and Network Security Monitoring engine.  
  
Open Source and owned by a community run non-profit foundation, the Open Information Secu  
Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the com  
ty.  
  
This Engine supports:  
  
- Multi-Threading - provides for extremely fast and flexible operation on multicore syste  
- 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  
- IDS runmode  
- IPS runmode  
- IDPS runmode  
- NSM runmode  
- eBPF/XDP  
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH  
P, SMB, DNS, NFS, TFTP, KRBS, DHCP, IKEv2, SNMP, SIP, RDP  
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS  
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted f
```

Установка Suricata: добавление в пакетный менеджер

```
blagorazumov1@ubuntu:~$ sudo apt install suricata  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  dctrl-tools dmraid dmraid dpkg-repack gir1.2-timzone 1.0 gir1.2-xkl-1.0 kpartx  
  kpartx-boot libaio1 libdebian-installer4 libdevmapper-event1.02.1 libdmraid1.0.0.rc16  
  libflashrom1 libftdi1-2 liblvm13 liblvm2cmd2.03 libqt5designer5 libqt5help5  
  libqt5positioning5 libqt5sensors5 libqt5test5 libqt5webchannel5 libqt5webkit5  
  libtimezonemap-data libtimezonemap1 linux-headers-5.15.0-27  
  linux-headers-5.15.0-27-generic linux-image-5.15.0-27-generic  
  linux-modules-5.15.0-27-generic linux-modules-extra-5.15.0-27-generic lvm2  
  python3-dbus.mainloop.pyqt5 python3-icu python3-pam python3-pyqt5 python3-pyqt5.qtsvg  
  python3-pyqt5.qtwebkit python3-pyqt5.sip rdate thin-provisioning-tools  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5  
  liblua5.1-2 liblua5.1-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 libhttp2 libhyperscan5  
  liblua5.1-2 liblua5.1-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  
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libhyperscan5 amd64 5.4.0-2 [2  
485 kB]
```

Установка Suricata из репозитория


```

root@ubuntu:~# cd /etc/suricata/
root@ubuntu:/etc/suricata# suricata-update
14/12/2024 -- 10:45:39 - <Info> -- Using data-directory /var/lib/suricata.
14/12/2024 -- 10:45:39 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
14/12/2024 -- 10:45:39 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
14/12/2024 -- 10:45:39 - <Info> -- Found Suricata version 7.0.8 at /usr/bin/suricata.
14/12/2024 -- 10:45:39 - <Info> -- Loading /etc/suricata/suricata.yaml
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol pgsql
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol modbus
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol dnp3
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol enip
14/12/2024 -- 10:45:39 - <Info> -- No sources configured, will use Emerging Threats Open
14/12/2024 -- 10:45:39 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7
.0.8/emerging.rules.tar.gz.
100% - 4648678/4648678

```

Прогрузка всех правил для обнаружения

```

root@ubuntu:/etc/suricata
GNU nano 4.8 /etc/suricata/suricata.yaml Modified
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 7.0.8.
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: "192.168.50.131"
  #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"

  HTTP_SERVERS: "$HOME_NET"
  SMTP_SERVERS: "$HOME_NET"
  SQL_SERVERS: "$HOME_NET"
  DNS_SERVERS: "$HOME_NET"
  TELNET_SERVERS: "$HOME_NET"

```

Настройка соответствующих переменных конфигурации в текущем файле

```

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

<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
/ossec_config>
ossec.conf" 207L, 5817B written

```

Настройка импорта журнала Suricata в wazuh

```

root@ubuntu: /var/ossec/etc
root@ubuntu: /var/ossec/etc# nano ossec.conf
root@ubuntu: /var/ossec/etc# systemctl restart wazuh-agent
root@ubuntu: /var/ossec/etc#

```

перезапуск агента

```

blagorazumov1@ubuntu: ~
blagorazumov1@ubuntu:~$ sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
  0     0    0     0    0     0      0      0  --:--:-- --:--:-- --:--:--    0
100 1258k  0 1258k    0     0 1083k      0  --:--:--  0:00:01 --:--:-- 1083k
blagorazumov1@ubuntu:~$ sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f v4.2.3.tar.gz
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

```

Загрузка и распаковка дистрибутива yara


```

blagorazumov1@ubuntu:~$ cd /usr/local/bin/yara-4.2.3/
blagorazumov1@ubuntu:~/usr/local/bin/yara-4.2.3$ sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make
in stall && sudo sudo make check
libtoolize: putting auxiliary files in AC_CONFIG_AUX_DIR, 'build-aux'.
libtoolize: copying file 'build-aux/ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt-obsolete.m4'
configure.ac:23: warning: The macro `AC_PROG_CC_C99' is obsolete.
configure.ac:23: You should run autoupdate.
./lib/autoconf/c.m4:1659: AC_PROG_CC_C99 is expanded from...
configure.ac:23: the top level
configure.ac:25: warning: AC_PROG_LEX without either yywrap or noyywrap is obsolete
./lib/autoconf/programs.m4:716: _AC_PROG_LEX is expanded from...

```

установка yara

```

blagorazumov1@ubuntu:~$ yara -version
4.2.3
blagorazumov1@ubuntu:~$

```

проверка установленной версии yara

```

blagorazumov1@ubuntu:~/yara-rules$ git clone https://github.com/Yara-Rules/rules
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 | 5.82 MiB/s, done.
Resolving deltas: 100% (4463/4463), done.
blagorazumov1@ubuntu:~/yara-rules$ ls -l rules
total 187
drwxrwxr-x 2 blagorazumov1 blagorazumov1 4096 дек 14 21:49 antidebug_antivm
-rw-rw-r-- 1 blagorazumov1 blagorazumov1 94 дек 14 21:49 antidebug_antivm_index.yar
drwxrwxr-x 2 blagorazumov1 blagorazumov1 4096 дек 14 21:49 capabilities
-rw-rw-r-- 1 blagorazumov1 blagorazumov1 86 дек 14 21:49 capabilities_index.ya
drwxrwxr-x 2 blagorazumov1 blagorazumov1 4096 дек 14 21:49 scripts

```

загрузка yara-правил

```

root@ubuntu:/var/ossec/active-response/bin# nano yara.sh
root@ubuntu:/var/ossec/active-response/bin# chown root:wazuh /var/ossec/active-response/response/bin/yara.sh
root@ubuntu:/var/ossec/active-response/bin# chmod 750 /var/ossec/active-response/bin/yara.sh
root@ubuntu:/var/ossec/active-response/bin# ls -l yara.sh
-rwxr-x-- 1 root wazuh 1486 дек 14 21:55 yara.sh
root@ubuntu:/var/ossec/active-response/bin#

```

создание скрипта для wazuh по документации

```

!-- 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>

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

```

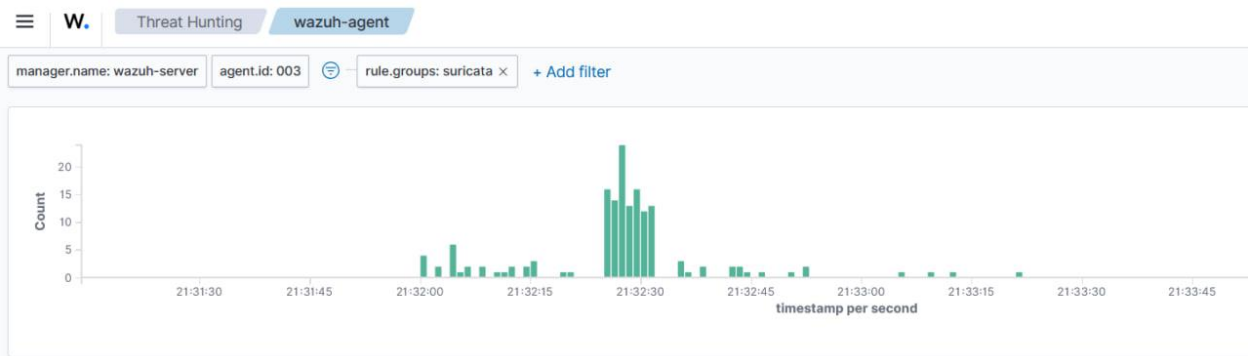
настраиваем правила мониторинга в ossec.conf

```

root@ubuntu:/var/ossec/etc# nano ossec.conf
root@ubuntu:/var/ossec/etc# systemctl restart wazuh-agent
root@ubuntu:/var/ossec/etc#

```

перезапуск агента wazuh



157 hits

Dec 14, 2024 @ 21:51:13.909 - Dec 14, 2024 @ 21:34:56.020

Export Formatted 495 columns hidden Density 1 fields sorted Full screen

timestamp	agent.name	rule.description	rule.level
Dec 14, 2024 @ 21:33:56.020	wazuh-agent	Suricata: Alert - SURICATA SSH invalid banner	3
Dec 14, 2024 @ 21:33:56.014	wazuh-agent	Suricata: Alert - SURICATA SSH invalid banner	3
Dec 14, 2024 @ 21:33:21.072	wazuh-agent	Suricata: Alert - SURICATA HTTP Request unrecognized authorization method	3
Dec 14, 2024 @ 21:33:12.261	wazuh-agent	Suricata: Alert - SURICATA Applayer Detect protocol only one direction	3
Dec 14, 2024 @ 21:33:09.877	wazuh-agent	Suricata: Alert - ET WEB_SPECIFIC_APPS Spring Framework FileSystemResource Path Trav...	3
Dec 14, 2024 @ 21:33:05.421	wazuh-agent	Suricata: Alert - SURICATA HTTP Request unrecognized authorization method	3
Dec 14, 2024 @ 21:32:52.495	wazuh-agent	Suricata: Alert - ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (SWNetPe...	3
Dec 14, 2024 @ 21:32:52.451	wazuh-agent	Suricata: Alert - ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (web.confli...	3
Dec 14, 2024 @ 21:32:50.498	wazuh-agent	Suricata: Alert - ET INFO WinHttp AutoProxy Request wpad.dat Possible BadTunnel	3
Dec 14, 2024 @ 21:32:46.333	wazuh-agent	Suricata: Alert - SURICATA Applayer Detect protocol only one direction	3
Dec 14, 2024 @ 21:32:44.436	wazuh-agent	Suricata: Alert - SURICATA HTTP multipart generic error	3
Dec 14, 2024 @ 21:32:43.878	wazuh-agent	Suricata: Alert - ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Inbo...	3

события сканирования защищаемого узла, запущенные для проверки работоспособности зафиксированы в IDS suricata



8 hits

Dec 14, 2024 @ 21:31:13.909 - Dec 14, 2024 @ 21:34:52.495

Export Formatted 495 columns hidden Density 1 fields sorted Full screen

timestamp	agent.name	rule.description	rule.level
Dec 14, 2024 @ 21:32:52.495	wazuh-agent	Suricata: Alert - ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (SWNetPerfMon.db) (CVE-2020-10148)	3
Dec 14, 2024 @ 21:32:52.451	wazuh-agent	Suricata: Alert - ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (web.config) (CVE-2020-10148)	3
Dec 14, 2024 @ 21:32:43.878	wazuh-agent	Suricata: Alert - ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Inbound)	3
Dec 14, 2024 @ 21:32:43.471	wazuh-agent	Suricata: Alert - ET EXPLOIT Netis E1+ 1.2.32533 - Unauthenticated WiFi Password Leak	3
Dec 14, 2024 @ 21:32:04.249	wazuh-agent	Suricata: Alert - ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1	3
Dec 14, 2024 @ 21:32:04.243	wazuh-agent	Suricata: Alert - ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-6515) M2	3
Dec 14, 2024 @ 21:32:04.186	wazuh-agent	Suricata: Alert - ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1	3
Dec 14, 2024 @ 21:32:04.123	wazuh-agent	Suricata: Alert - ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1	3

фильтруем и просматриваем события по тегу exploit