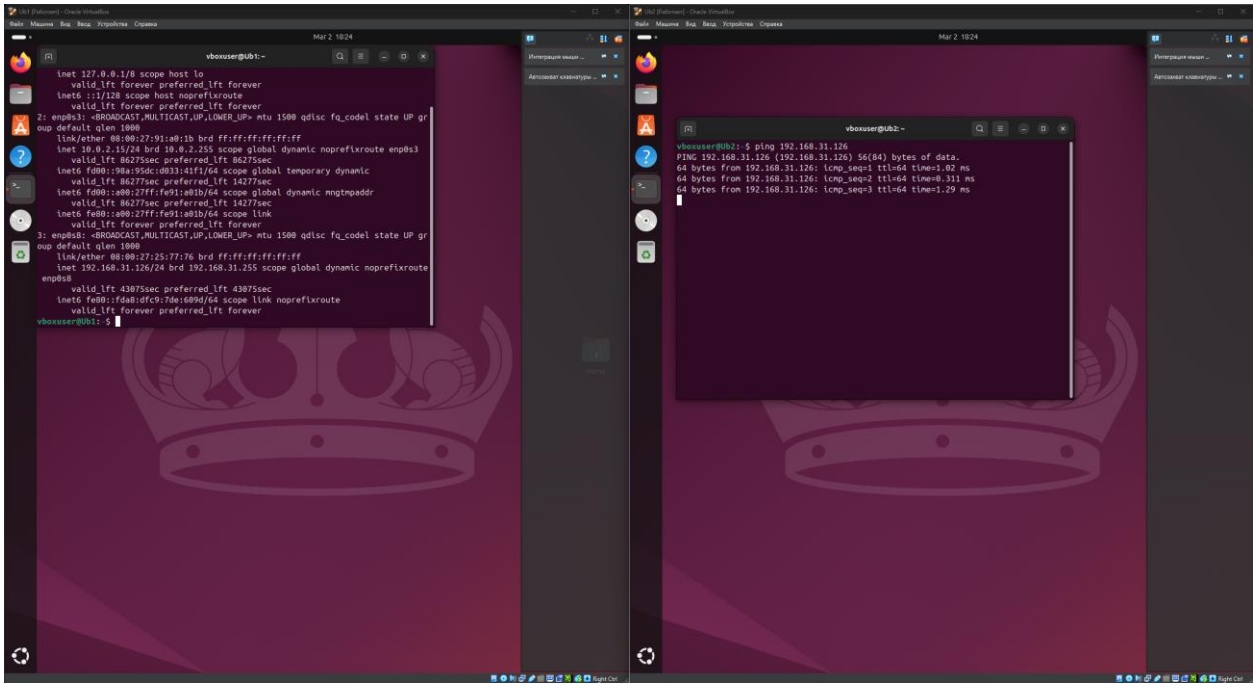
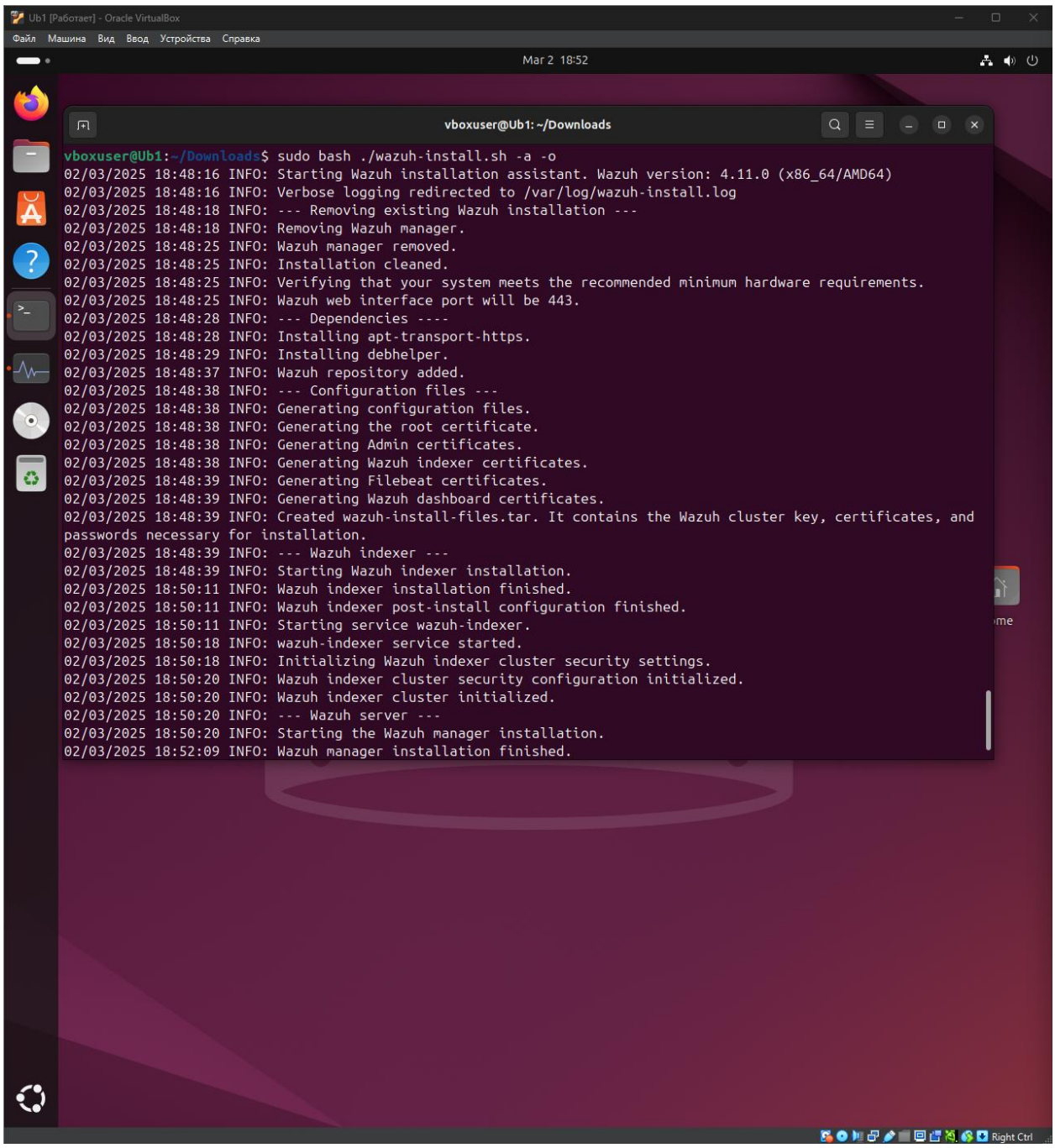
Разворачиваем 2 ВМ и пингуем на проверку связи



Инициализация wazuh на Ub1

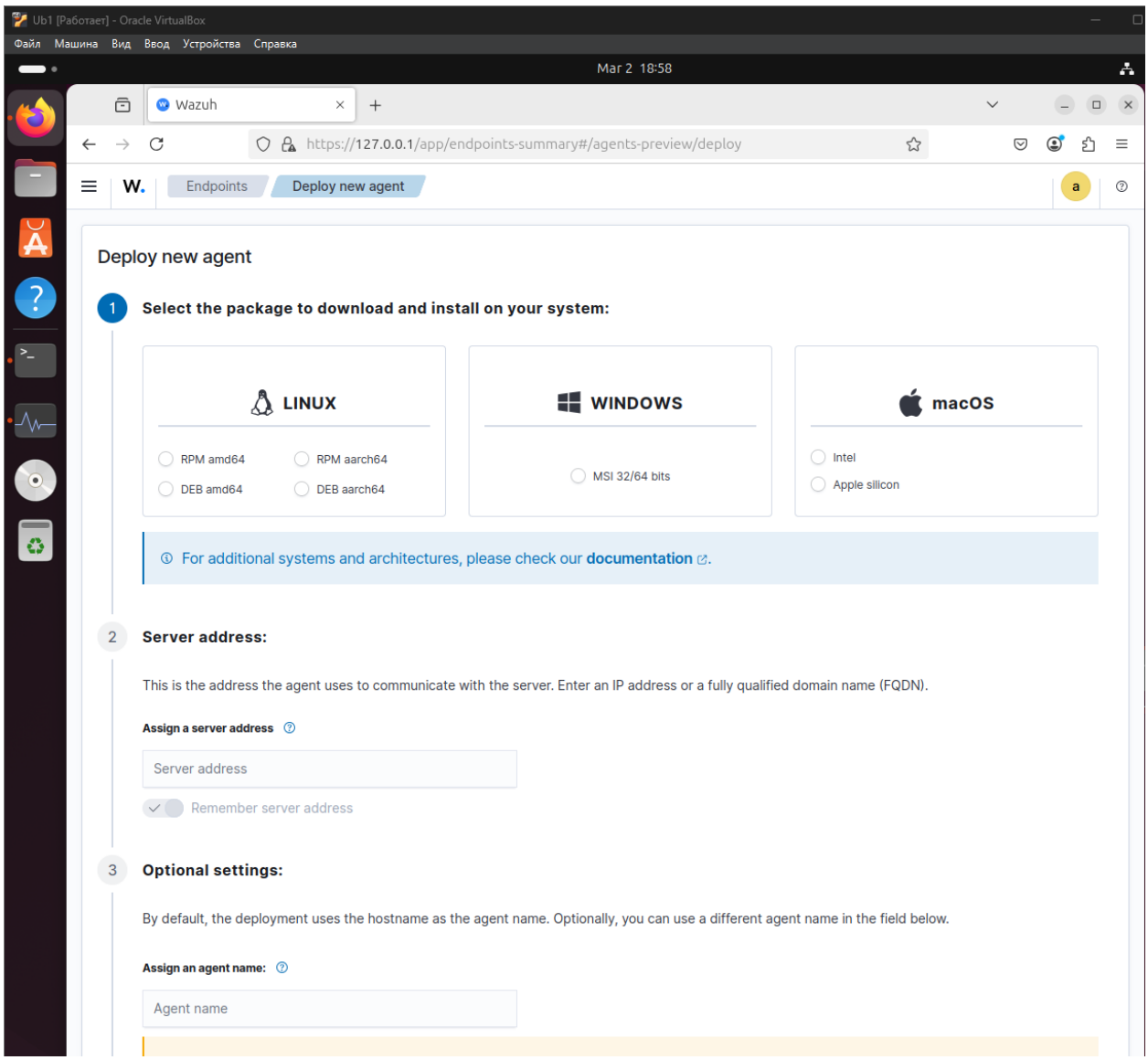
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh –a –o



Разворачиваем дашборд и получаем креды

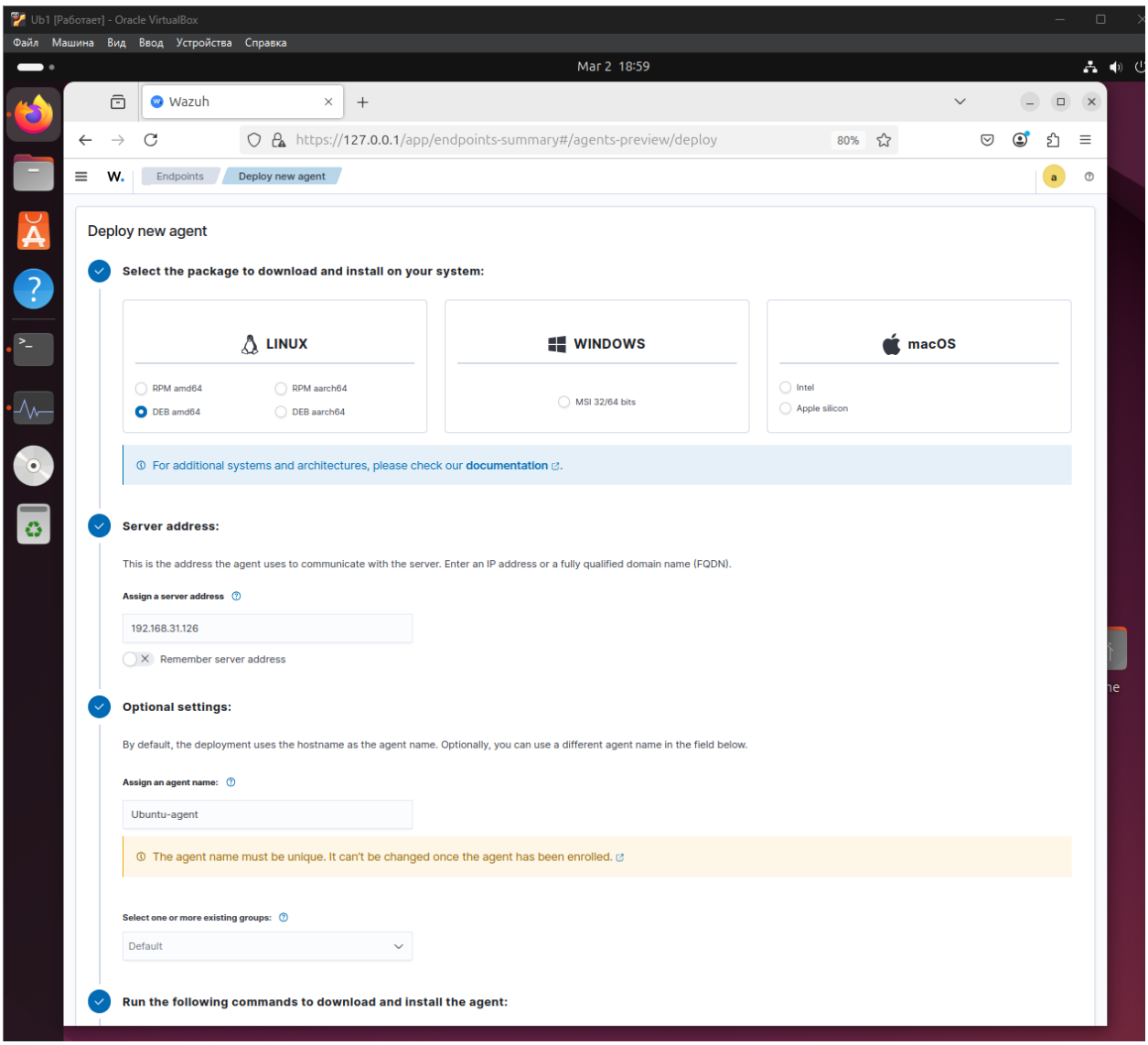
User: admin

Password: ?yjorfR4LTl7c5T8ZP4EokICuRAG?0EA



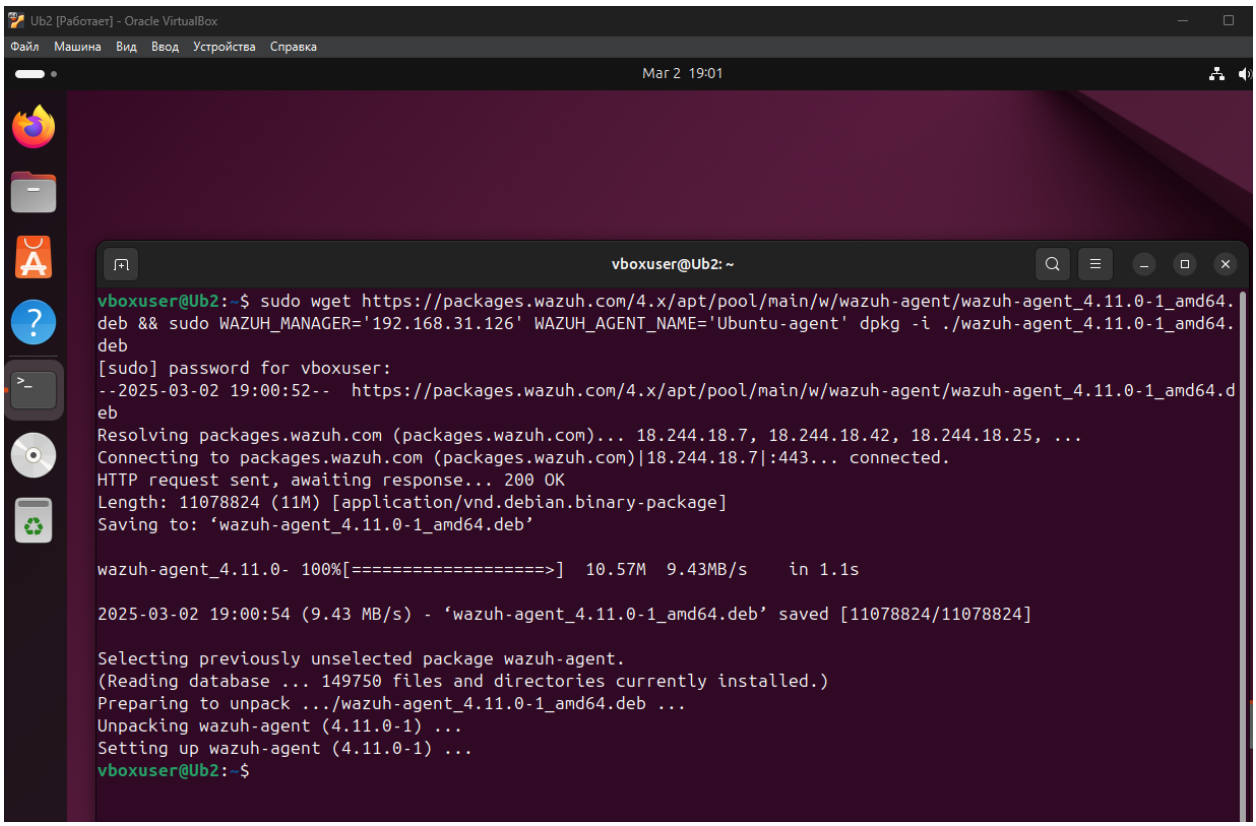
Получаем пресет для агента

wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.31.126' WAZUH_AGENT_NAME='Ubuntu-agent' dpkg -i ./wazuh-agent_4.11.0-1_amd64.deb



Устанавливаем агента по пресету

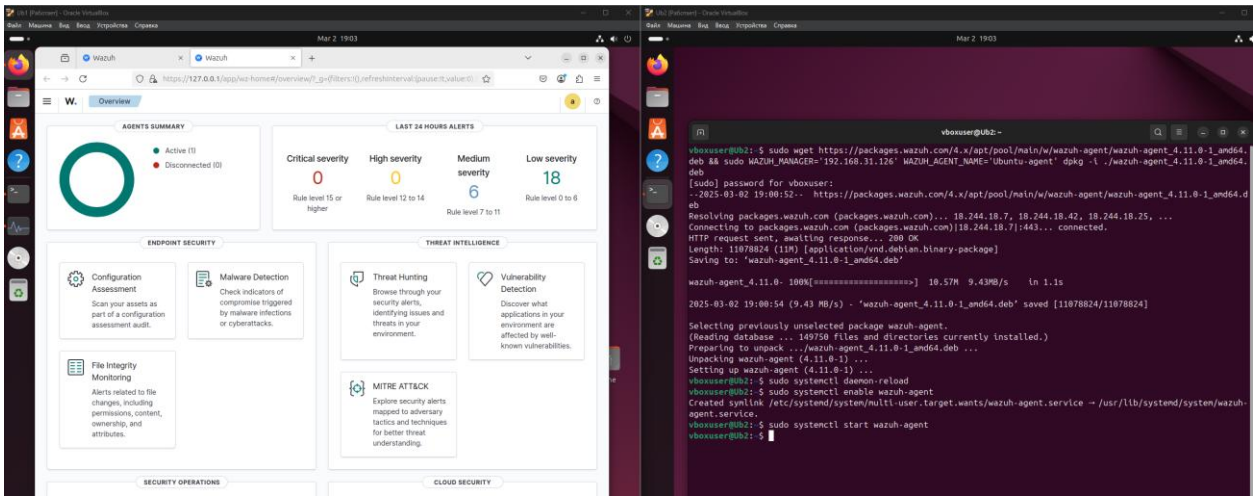
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.31.126' WAZUH_AGENT_NAME='Ubuntu-agent' dpkg -i ./wazuh-agent_4.11.0-1_amd64.deb



Запускаем демона на агенте

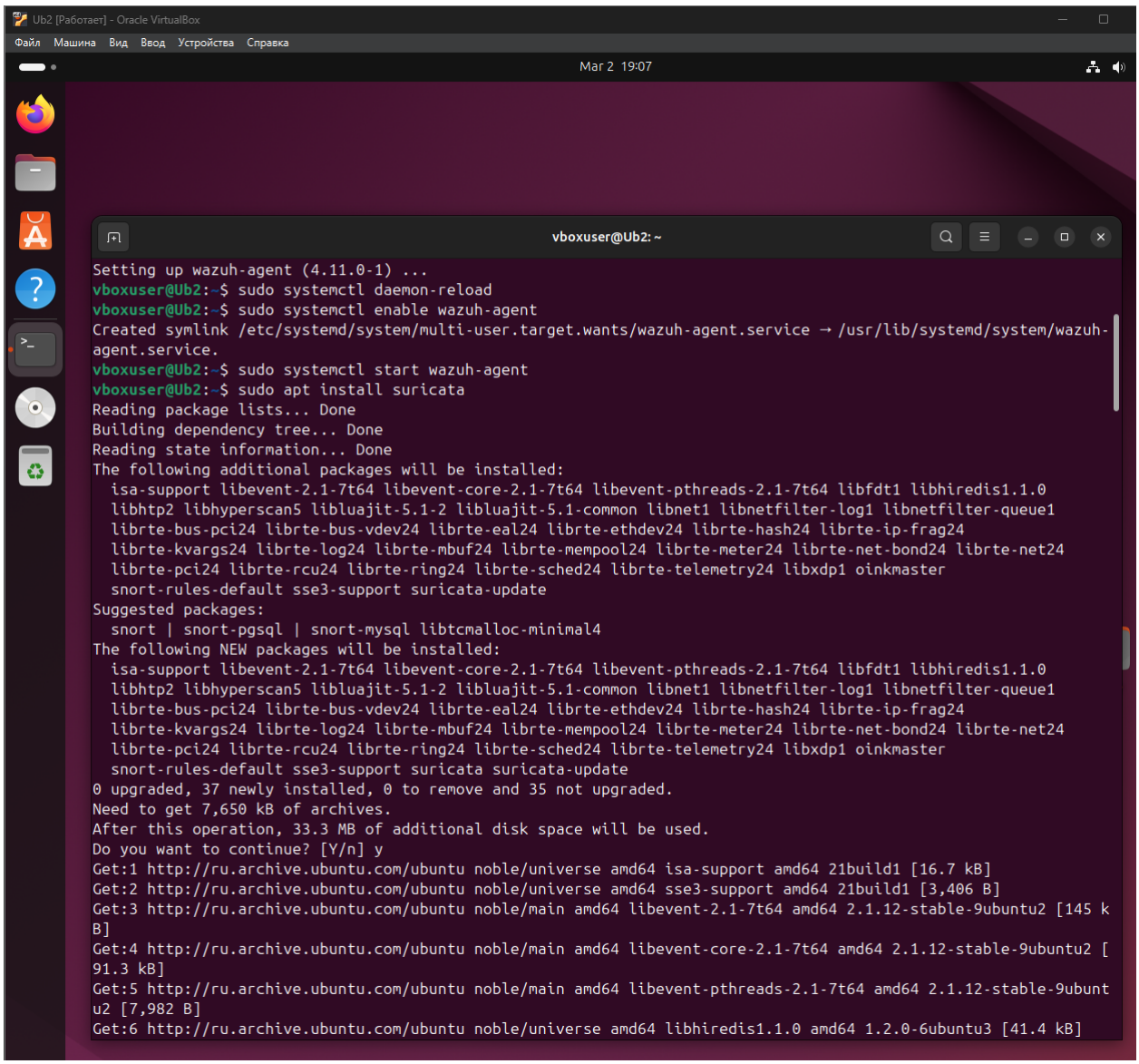
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent

И видим агента на сервере

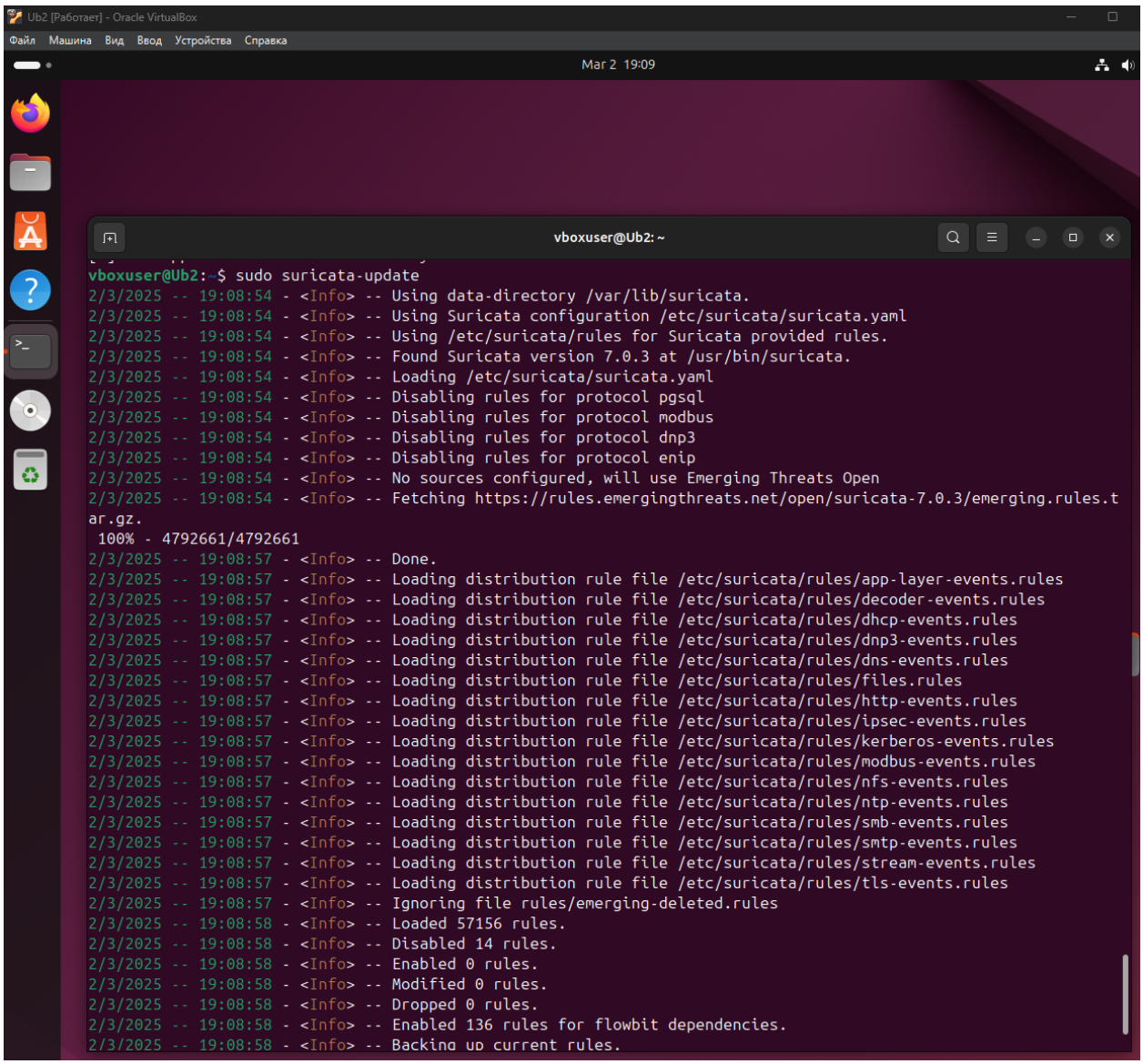


Устанавливаем suricata на агента

sudo apt install suricata



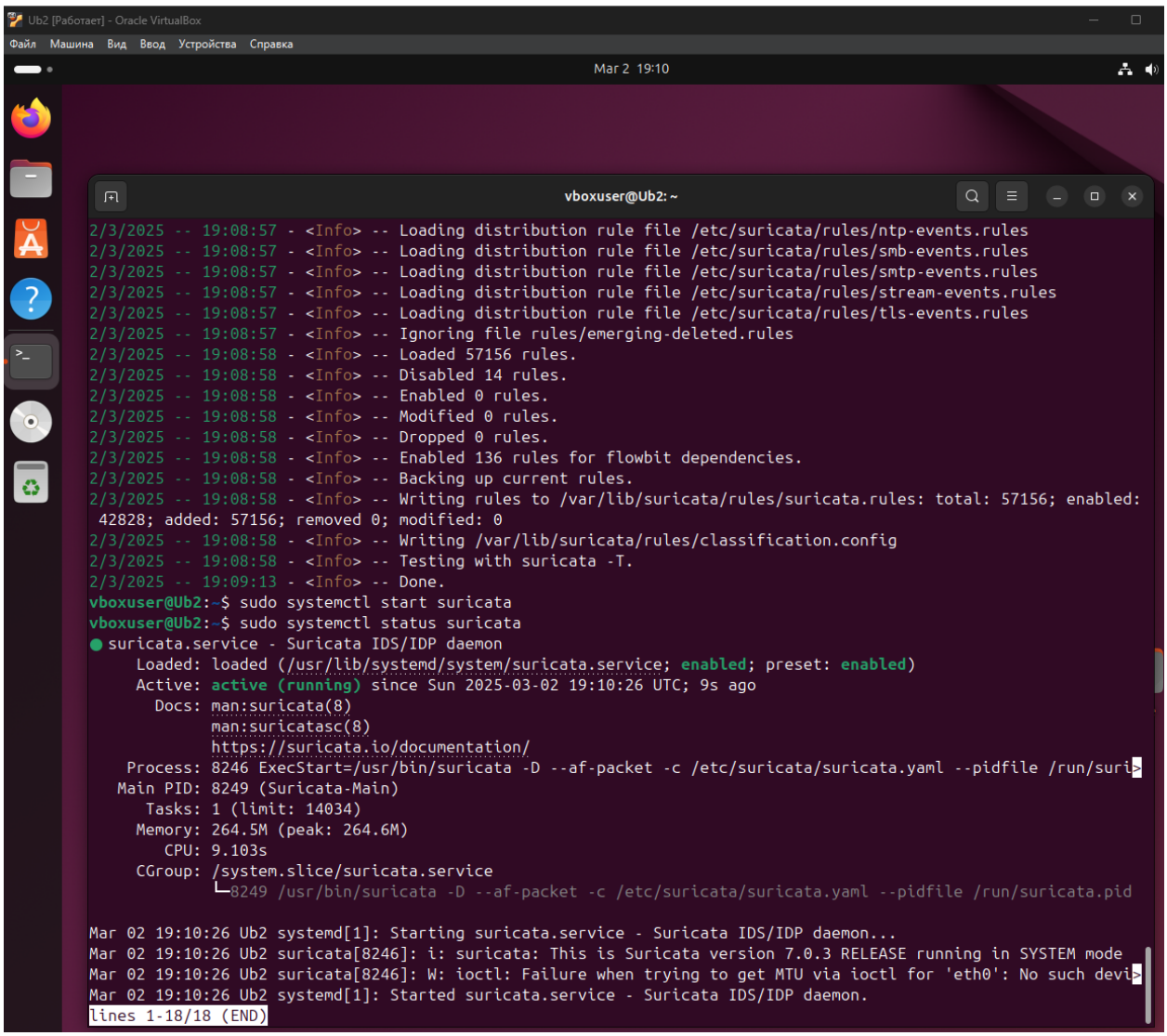
sudo suricata-update



Запускаем suricata и проверяем статус – всё ок

sudo systemctl start suricata

sudo systemctl status suricata

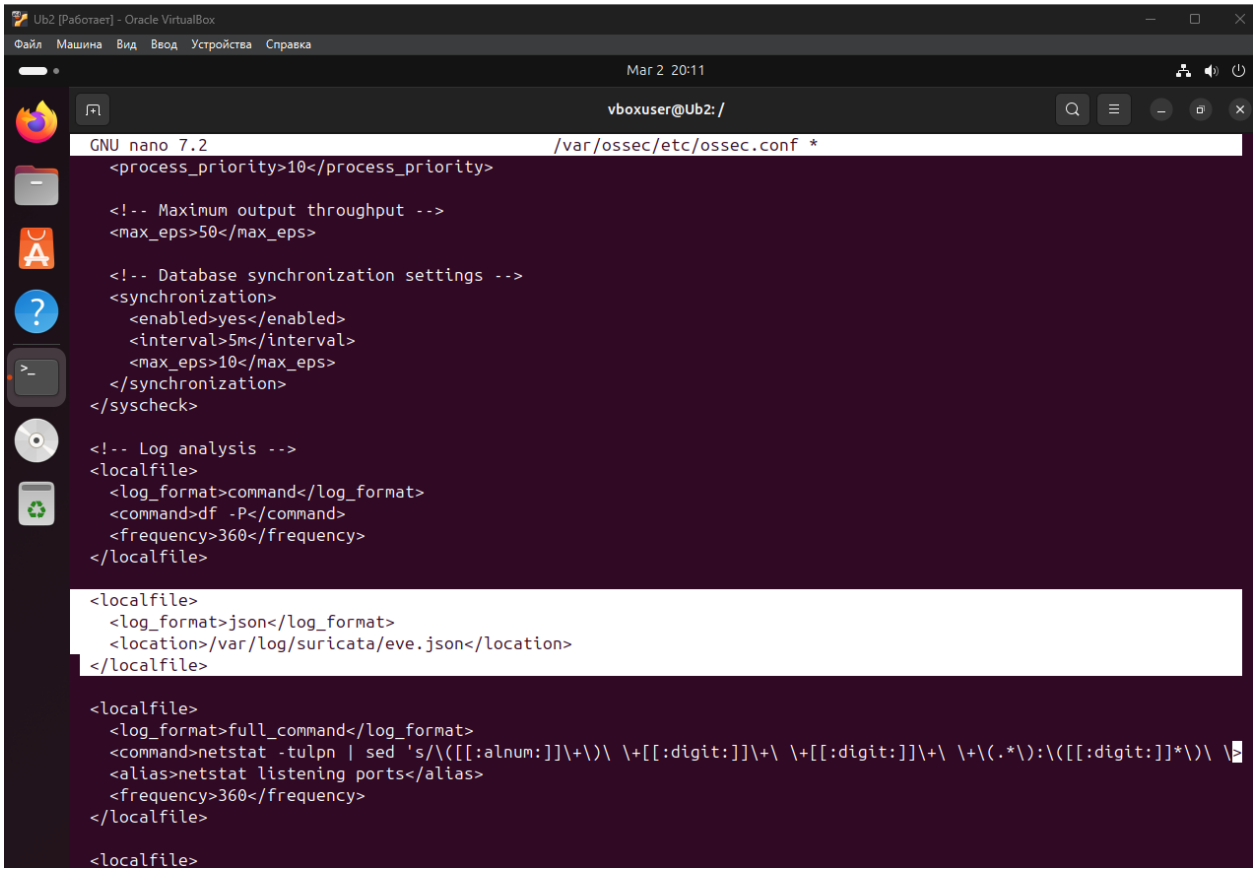


Добавляем логи к сурикате

sudo nano /var/ossec/etc/ossec.conf

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

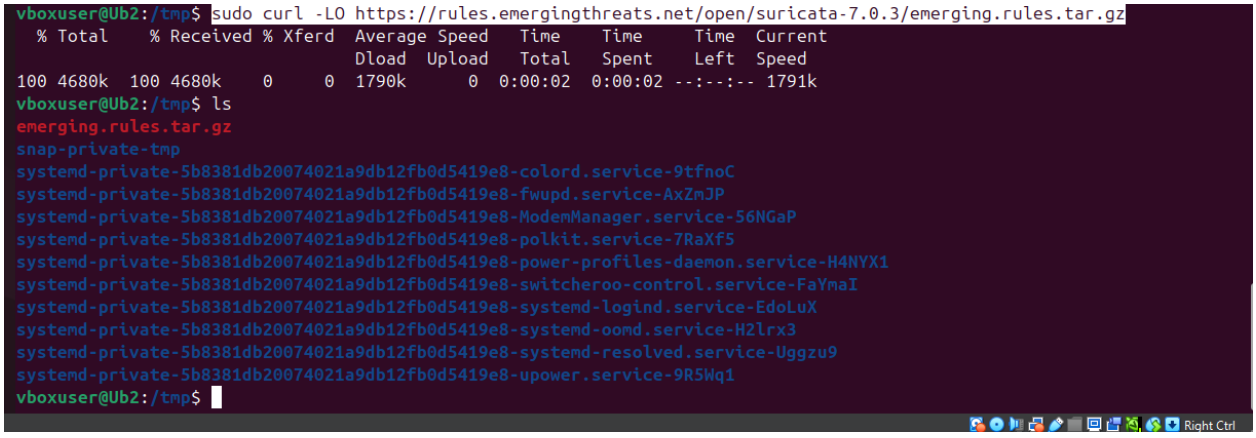
</localfile>



Скачиваем рулы для сурикаты

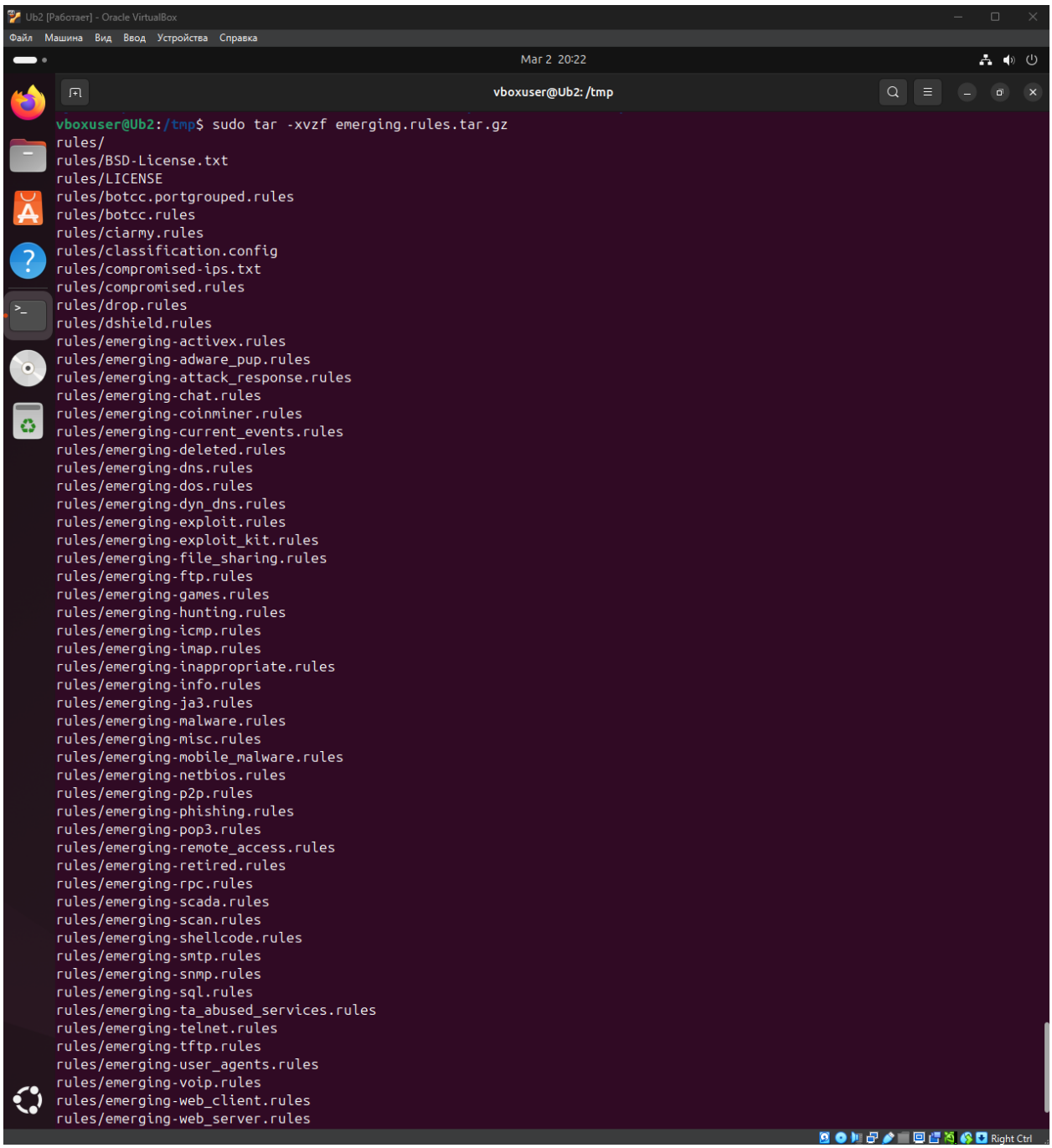
cd /tmp/

sudo curl -LO https://rules.emergingthreats.net/open/suricata-7.0.3/emerging.rules.tar.gz



Разорхивируем их

sudo tar -xvzf emerging.rules.tar.gz



Перемещение рулов в /etc/suricata/rules/

sudo mv rules/*.rules /etc/suricata/rules/

+ проверка

cd /etc/suricata/rules/

ls

```
vboxuser@Ub2:/tmp$ sudo mv rules/*.rules /etc/suricata/rules/
vboxuser@Ub2:/tmp$ cd /etc/suricata/rules/
vboxuser@Ub2:/etc/suricata/rules$ ls
app-layer-events.rules          emerging-hunting.rules            emerging-voip.rules
botcc.portgrouped.rules         emerging-icmp.rules               emerging-web_client.rules
botcc.rules                     emerging-imap.rules               emerging-web_server.rules
ciarmy.rules                    emerging-inappropriate.rules      emerging-web_specific_apps.rules
compromised.rules               emerging-info.rules               emerging-worm.rules
decoder-events.rules            emerging-ja3.rules                files.rules
dhcp-events.rules               emerging-malware.rules            ftp-events.rules
dnp3-events.rules               emerging-misc.rules               http2-events.rules
dns-events.rules                emerging-mobile_malware.rules     http-events.rules
drop.rules                      emerging-netbios.rules            ipsec-events.rules
dshield.rules                   emerging-p2p.rules                kerberos-events.rules
emerging-activex.rules          emerging-phishing.rules           modbus-events.rules
emerging-adware_pup.rules       emerging-pop3.rules               mqtt-events.rules
emerging-attack_response.rules  emerging-remote_access.rules      nfs-events.rules
emerging-chat.rules             emerging-retired.rules            ntp-events.rules
emerging-coinminer.rules        emerging-rpc.rules                quic-events.rules
emerging-current_events.rules   emerging-scada.rules              rfb-events.rules
emerging-deleted.rules          emerging-scan.rules               smb-events.rules
emerging-dns.rules              emerging-shellcode.rules          smtp-events.rules
emerging-dos.rules              emerging-smtp.rules               ssh-events.rules
emerging-dyn_dns.rules          emerging-snmp.rules               stream-events.rules
emerging-exploit_kit.rules      emerging-sql.rules                threatview_CS_c2.rules
emerging-exploit.rules          emerging-ta_abused_services.rules tls-events.rules
emerging-file_sharing.rules     emerging-telnet.rules             tor.rules
emerging-ftp.rules              emerging-tftp.rules
 Show Apps ames.rules           emerging-user_agents.rules
vboxuser@Ub2:/etc/suricata/rules$
```

Выдача прав рулам

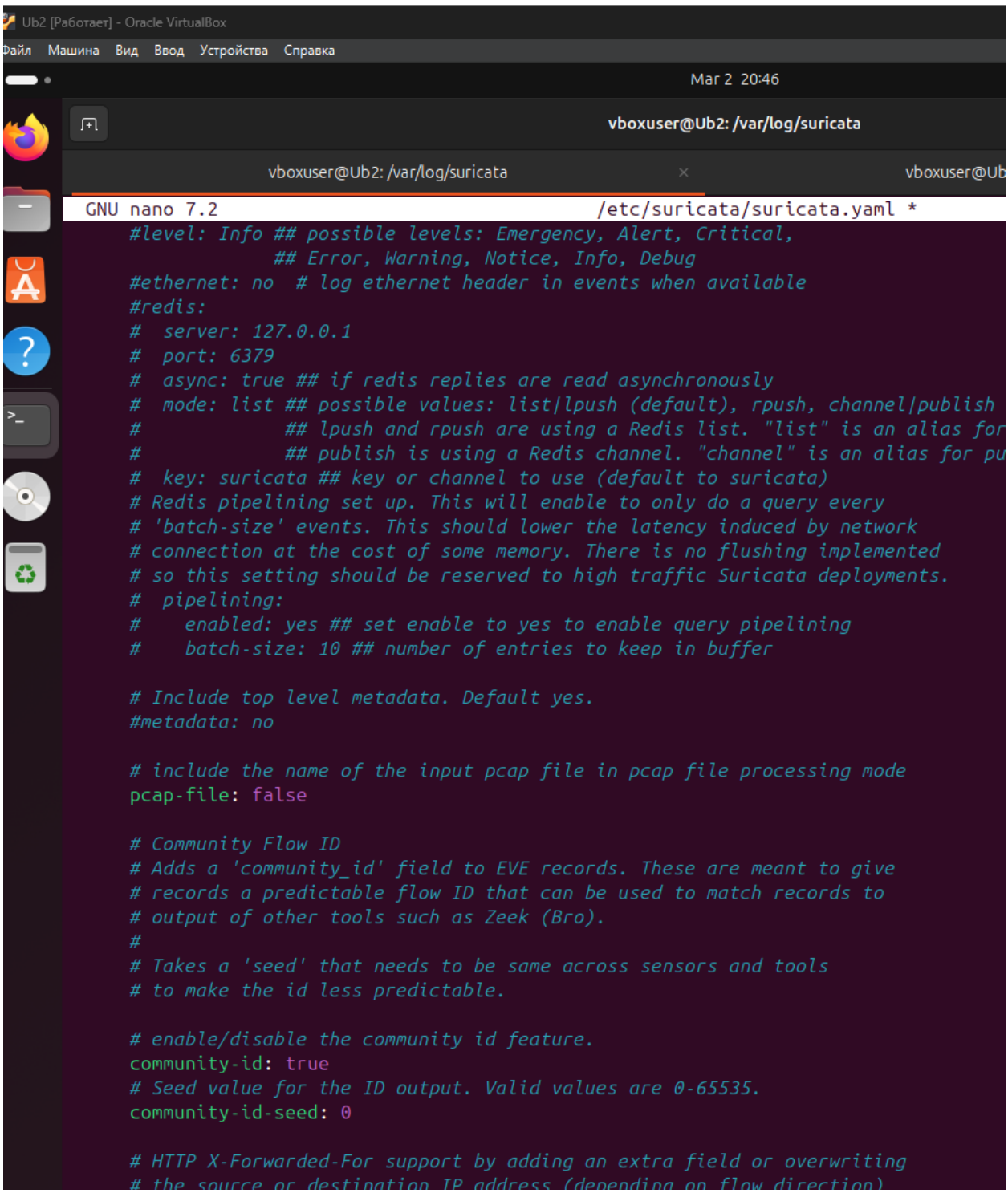
sudo chmod 640 /etc/suricata/rules/*.rules

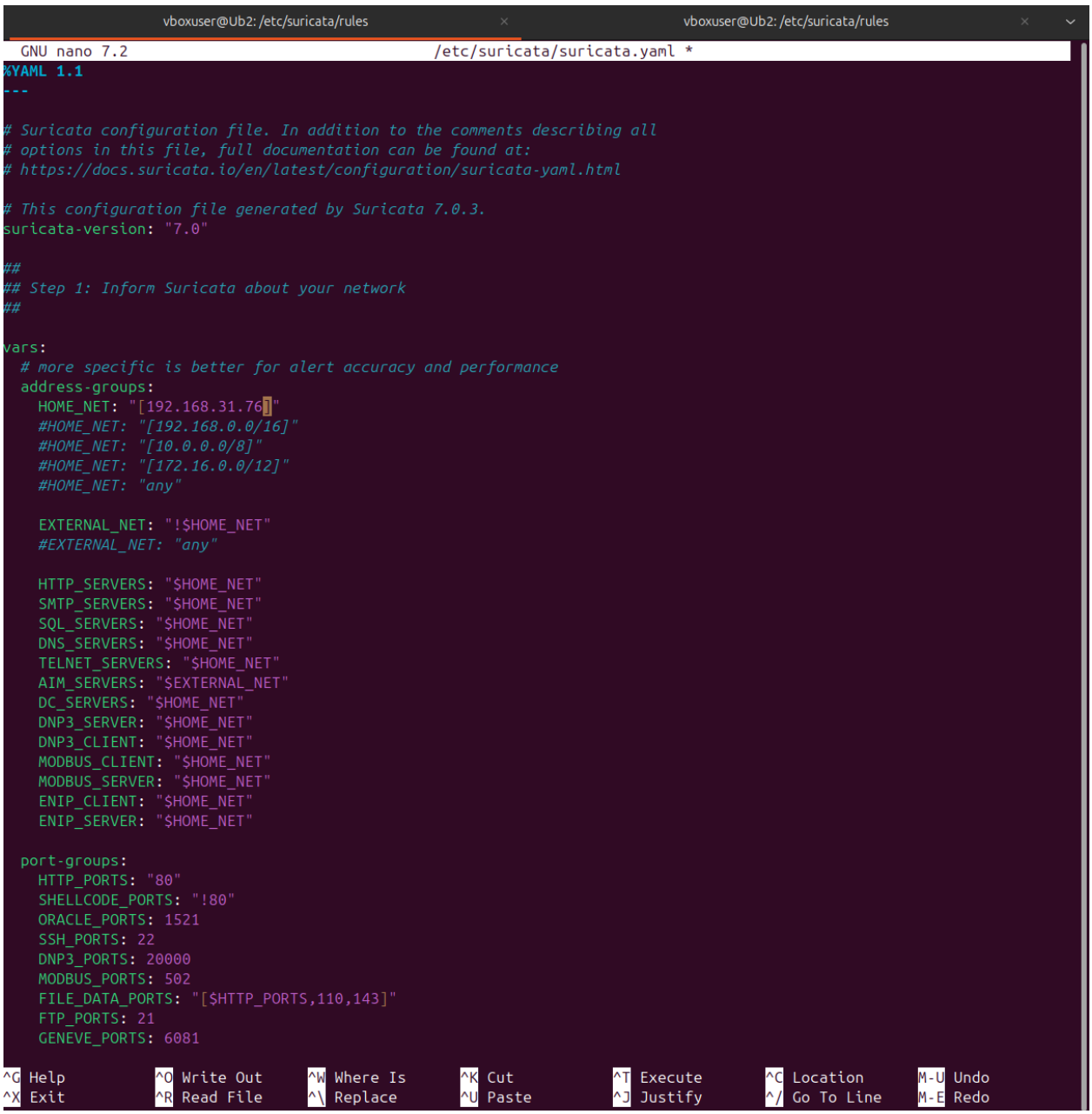
```
vboxuser@Ub2:/etc/suricata/rules$ sudo chmod 640 /etc/suricata/rules/*.rules
vboxuser@Ub2:/etc/suricata/rules$
```

Right Ctrl

Правим yaml сурикаты

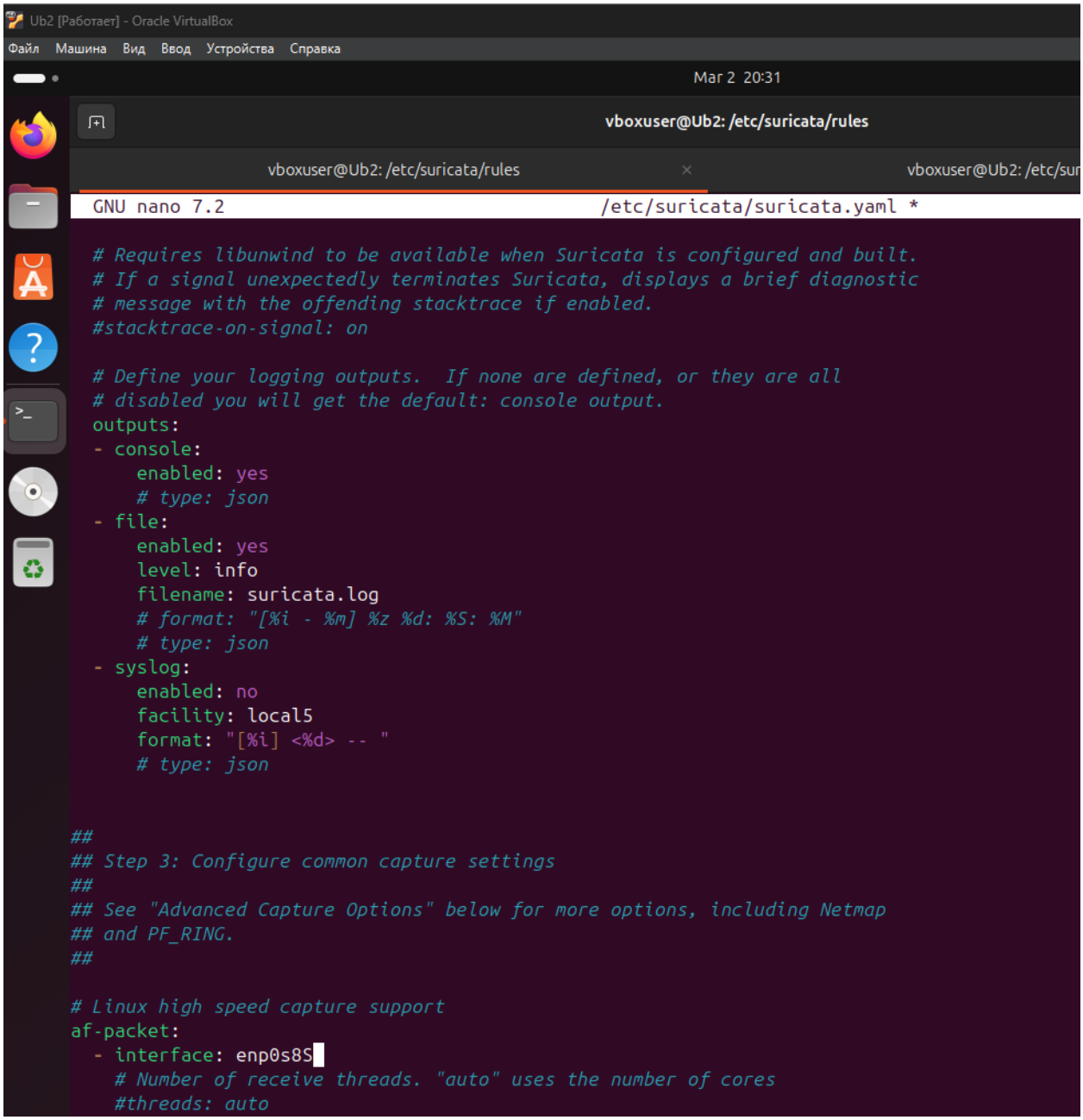
sudo nano /etc/suricata/suricata.yaml


Ub2 [Работает] - Oracle VirtualBox
Файл Машина Вид Ввод Устройства Справка
Mar 2 20:46
vboxuser@Ub2: /var/log/suricata
vboxuser@Ub2: /var/log/suricata
vboxuser@Ub
GNU nano 7.2 /etc/suricata/suricata.yaml *
#level: Info ## possible levels: Emergency, Alert, Critical,
Error, Warning, Notice, Info, Debug
#ethernet: no # log ethernet header in events when available
#redis:
server: 127.0.0.1
port: 6379
async: true ## if redis replies are read asynchronously
mode: list ## possible values: list|lpush (default), rpush, channel|publish
lpush and rpush are using a Redis list. "list" is an alias for
publish is using a Redis channel. "channel" is an alias for pu
key: suricata ## key or channel to use (default to suricata)
Redis pipelining set up. This will enable to only do a query every
'batch-size' events. This should lower the latency induced by network
connection at the cost of some memory. There is no flushing implemented
so this setting should be reserved to high traffic Suricata deployments.
pipelining:
enabled: yes ## set enable to yes to enable query pipelining
batch-size: 10 ## number of entries to keep in buffer
Include top level metadata. Default yes.
#metadata: no
include the name of the input pcap file in pcap file processing mode
pcap-file: false
Community Flow ID
Adds a 'community_id' field to EVE records. These are meant to give
records a predictable flow ID that can be used to match records to
output of other tools such as Zeek (Bro).
#
Takes a 'seed' that needs to be same across sensors and tools
to make the id less predictable.
enable/disable the community id feature.
community-id: true
Seed value for the ID output. Valid values are 0-65535.
community-id-seed: 0
HTTP X-Forwarded-For support by adding an extra field or overwriting


vboxuser@Ub2: /etc/suricata/rules
vboxuser@Ub2: /etc/suricata/rules
GNU nano 7.2 /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 7.0.3.
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: "[192.168.31.76]"
#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"
AIM_SERVERS: "$EXTERNAL_NET"
DC_SERVERS: "$HOME_NET"
DNP3_SERVER: "$HOME_NET"
DNP3_CLIENT: "$HOME_NET"
MODBUS_CLIENT: "$HOME_NET"
MODBUS_SERVER: "$HOME_NET"
ENIP_CLIENT: "$HOME_NET"
ENIP_SERVER: "$HOME_NET"
port-groups:
HTTP_PORTS: "80"
SHELLCODE_PORTS: "!80"
ORACLE_PORTS: 1521
SSH_PORTS: 22
DNP3_PORTS: 20000
MODBUS_PORTS: 502
FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
FTP_PORTS: 21
GENEVE_PORTS: 6081
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

как видно на этом скриншоте я неправильно указал интерфейс добавив в конце S делая скрин...(



Рестарт сурикаты

sudo systemctl restart suticata

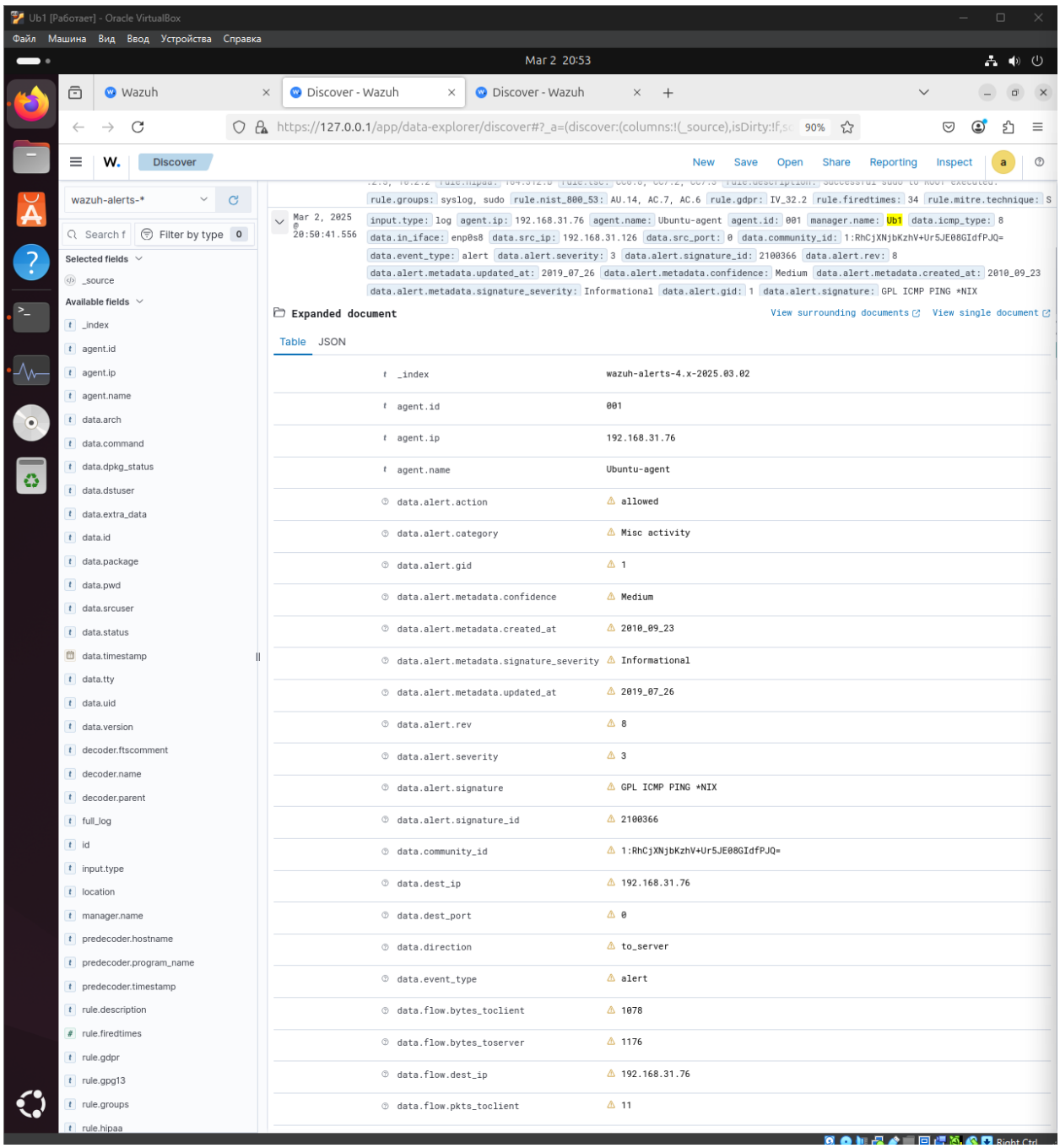
```
vboxuser@Ub2:/etc/suricata/rules$ sudo systemctl restart suricata
vboxuser@Ub2:/etc/suricata/rules$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-02 20:34:44 UTC; 4s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 12986 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.p>
   Main PID: 12989 (Suricata-Main)
      Tasks: 1 (limit: 14034)
     Memory: 173.7M (peak: 173.7M)
        CPU: 4.088s
     CGroup: /system.slice/suricata.service
             └─12989 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Mar 02 20:34:44 Ub2 systemd[1]: suricata.service: Failed with result 'exit-code'.
Mar 02 20:34:44 Ub2 systemd[1]: suricata.service: Consumed 17.155s CPU time.
Mar 02 20:34:44 Ub2 systemd[1]: suricata.service: Scheduled restart job, restart counter is at 1.
Mar 02 20:34:44 Ub2 systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Mar 02 20:34:44 Ub2 suricata[12986]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Mar 02 20:34:44 Ub2 suricata[12986]: W: ioctl: Failure when trying to get MTU via ioctl for 'enp0s8S': No such device >
Mar 02 20:34:44 Ub2 systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-21/21 (END)
```

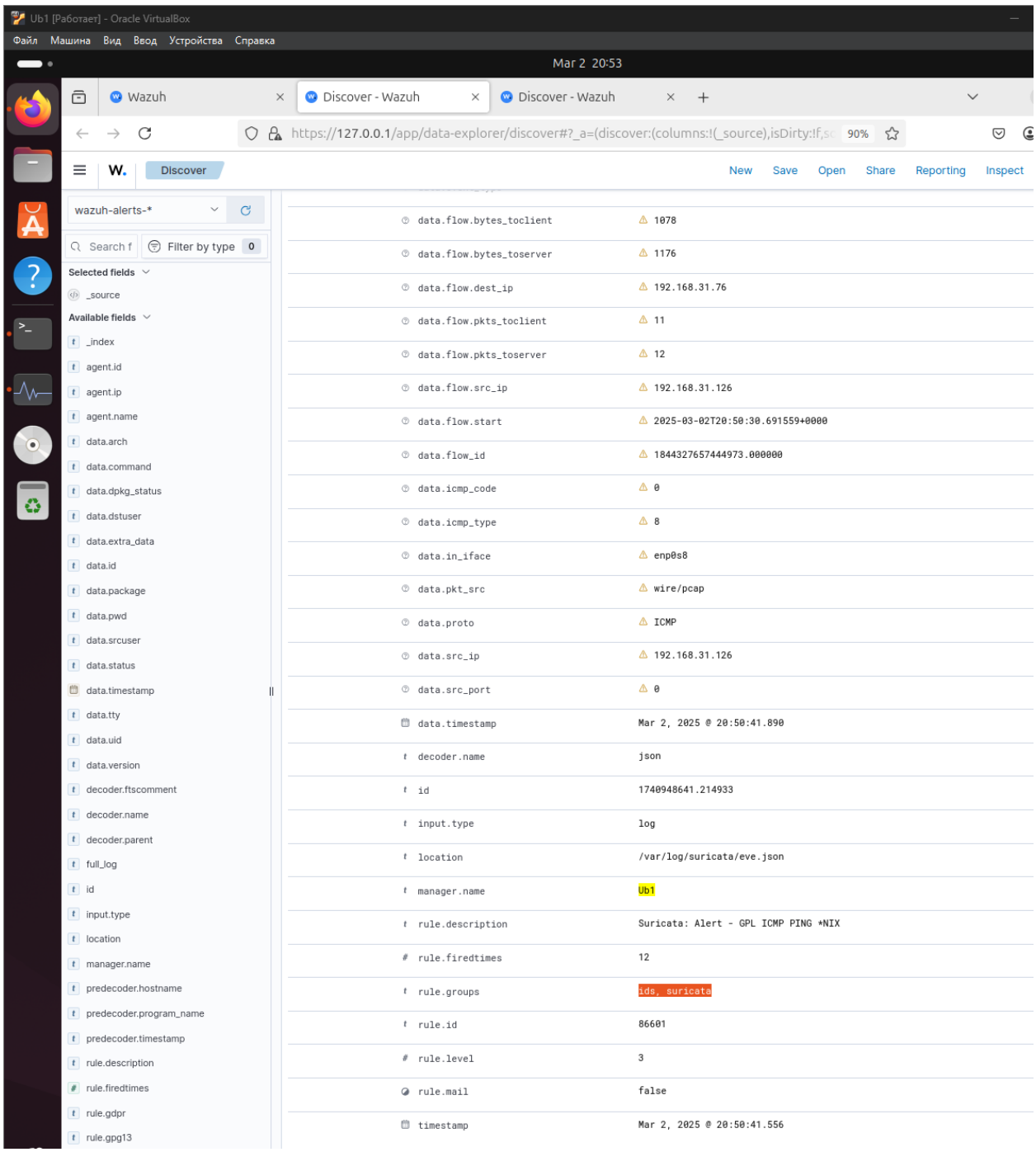
Перезапуск wazuh-agent

sudo systemctl restart wazuh-agent

```
vboxuser@Ub2:/etc/suricata/rules$ sudo systemctl restart wazuh-agent
vboxuser@Ub2:/etc/suricata/rules$
```

Пингуем агента и получаем события от сурикаты

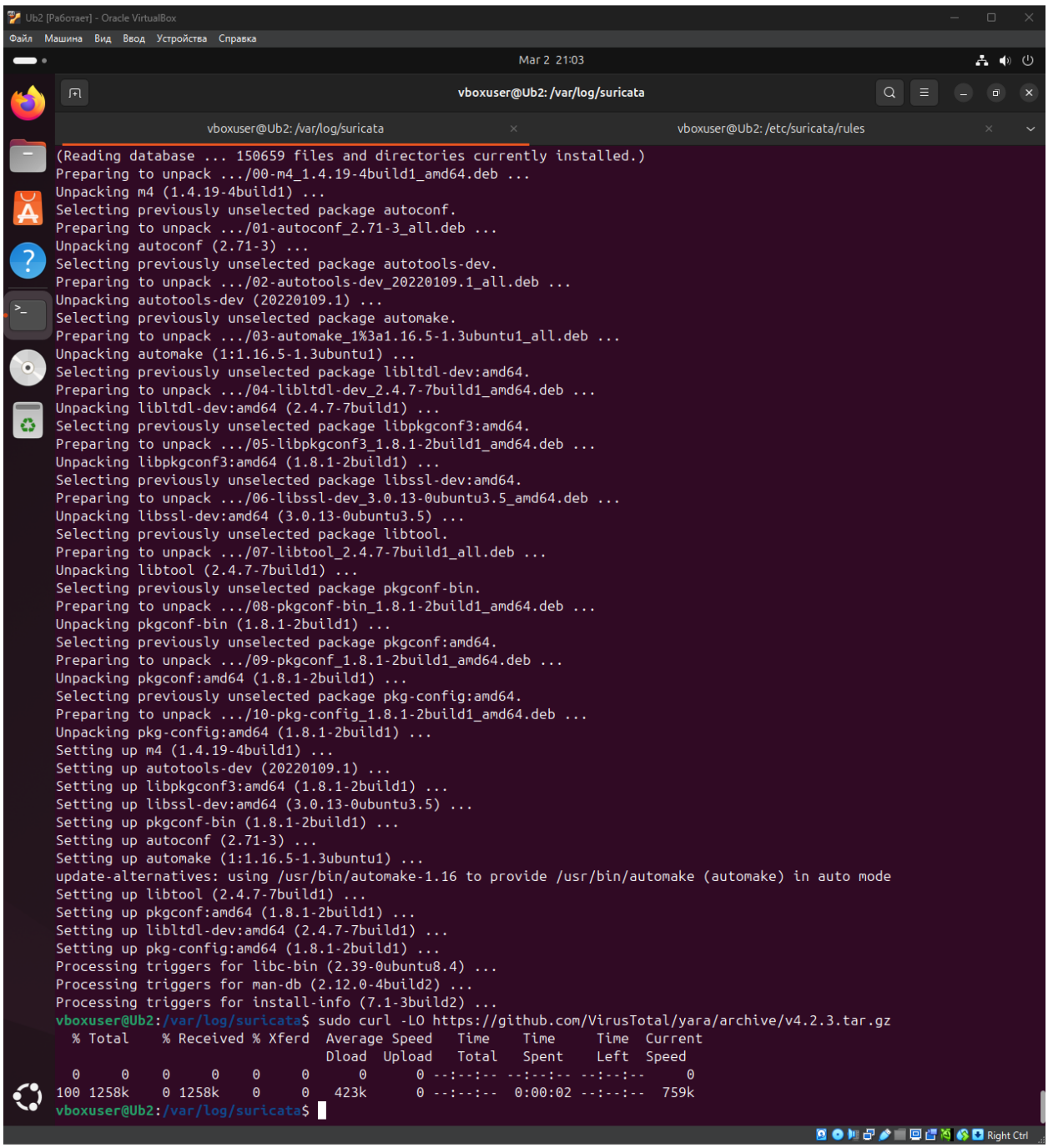

Ub1 [Работает] - Oracle VirtualBox
Файл Машина Вид Ввод Устройства Справка
Mar 2 20:53
Wazuh
Discover - Wazuh
Discover - Wazuh
https://127.0.0.1/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sc
90%
Discover
New Save Open Share Reporting Inspect
wazuh-alerts-*
Search f
Filter by type 0
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.arch
data.command
data.dpkg_status
data.dstuser
data.extra_data
data.id
data.package
data.pwd
data.srcuser
data.status
data.timestamp
data.tty
data.uid
data.version
decoder.ftscomment
decoder.name
decoder.parent
full_log
id
input.type
location
manager.name
predecoder.hostname
predecoder.program_name
predecoder.timestamp
rule.description
rule.firedtimes
rule.gdpr
rule.gpg13
rule.groups
rule.hipaa
rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 34 rule.mitre.technique: S
Mar 2, 2025 @ 20:50:41.556
input.type: log agent.ip: 192.168.31.76 agent.name: Ubuntu-agent agent.id: 001 manager.name: Ub1 data.icmp_type: 8
data.in_iface: enp0s8 data.src_ip: 192.168.31.126 data.src_port: 0 data.community_id: 1:RhCjXNjbKzhV+Ur5JE08GIdfPJQ=
data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2100366 data.alert.rev: 8
data.alert.metadata.updated_at: 2019_07_26 data.alert.metadata.confidence: Medium data.alert.metadata.created_at: 2010_09_23
data.alert.metadata.signature_severity: Informational data.alert.gid: 1 data.alert.signature: GPL ICMP PING *NIX
Expanded document
View surrounding documents
View single document
Table JSON
t _index wazuh-alerts-4.x-2025.03.02
t agent.id 001
t agent.ip 192.168.31.76
t agent.name Ubuntu-agent
data.alert.action allowed
data.alert.category Misc activity
data.alert.gid 1
data.alert.metadata.confidence Medium
data.alert.metadata.created_at 2010_09_23
data.alert.metadata.signature_severity Informational
data.alert.metadata.updated_at 2019_07_26
data.alert.rev 8
data.alert.severity 3
data.alert.signature GPL ICMP PING *NIX
data.alert.signature_id 2100366
data.community_id 1:RhCjXNjbKzhV+Ur5JE08GIdfPJQ=
data.dest_ip 192.168.31.76
data.dest_port 0
data.direction to_server
data.event_type alert
data.flow.bytes_toclient 1078
data.flow.bytes_toserver 1176
data.flow.dest_ip 192.168.31.76
data.flow.pkts_toclient 11
Right Ctrl



Установка yara

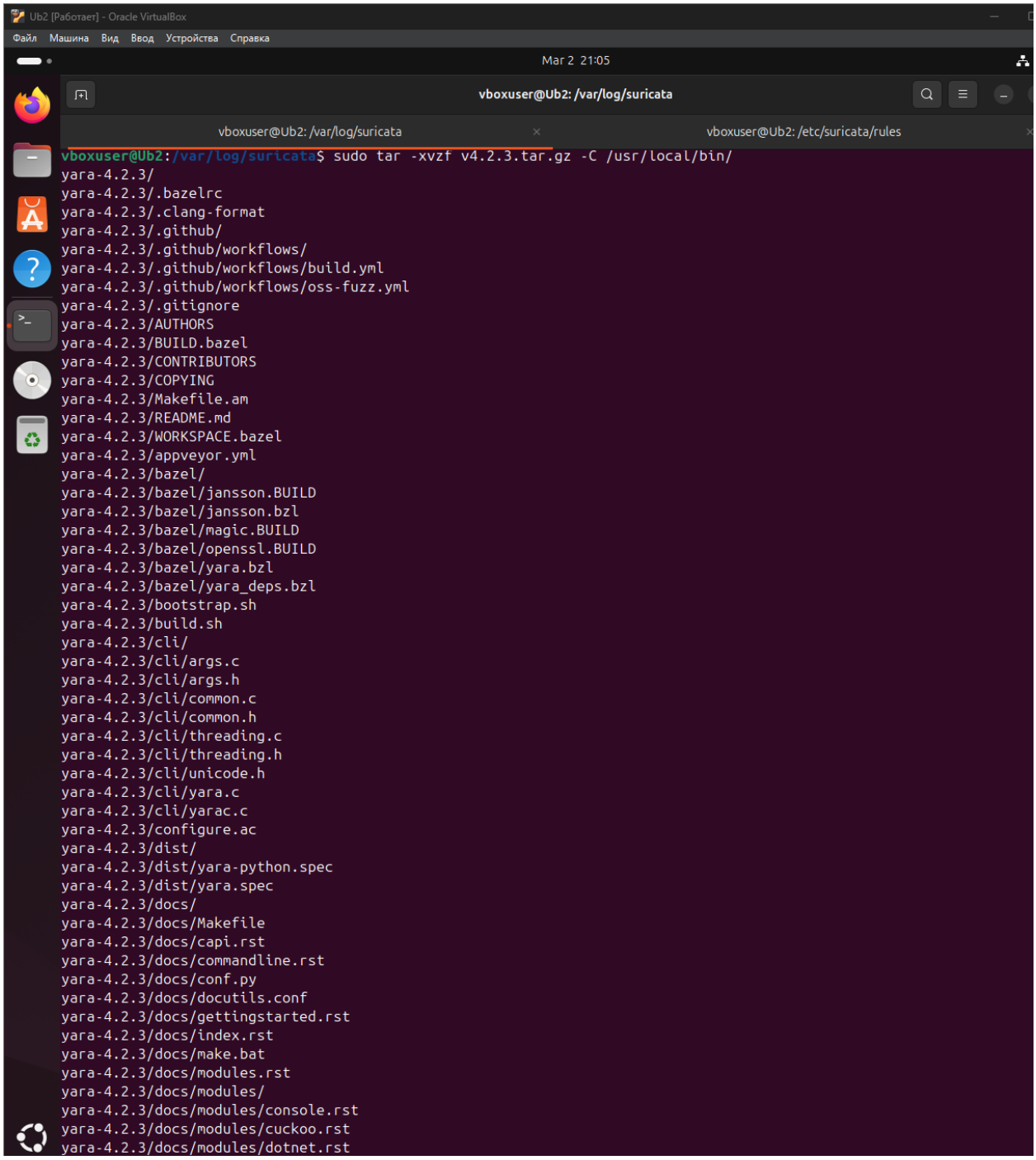
sudo apt install -y make gcc autoconf libtool libssl-dev pkg-config

sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz

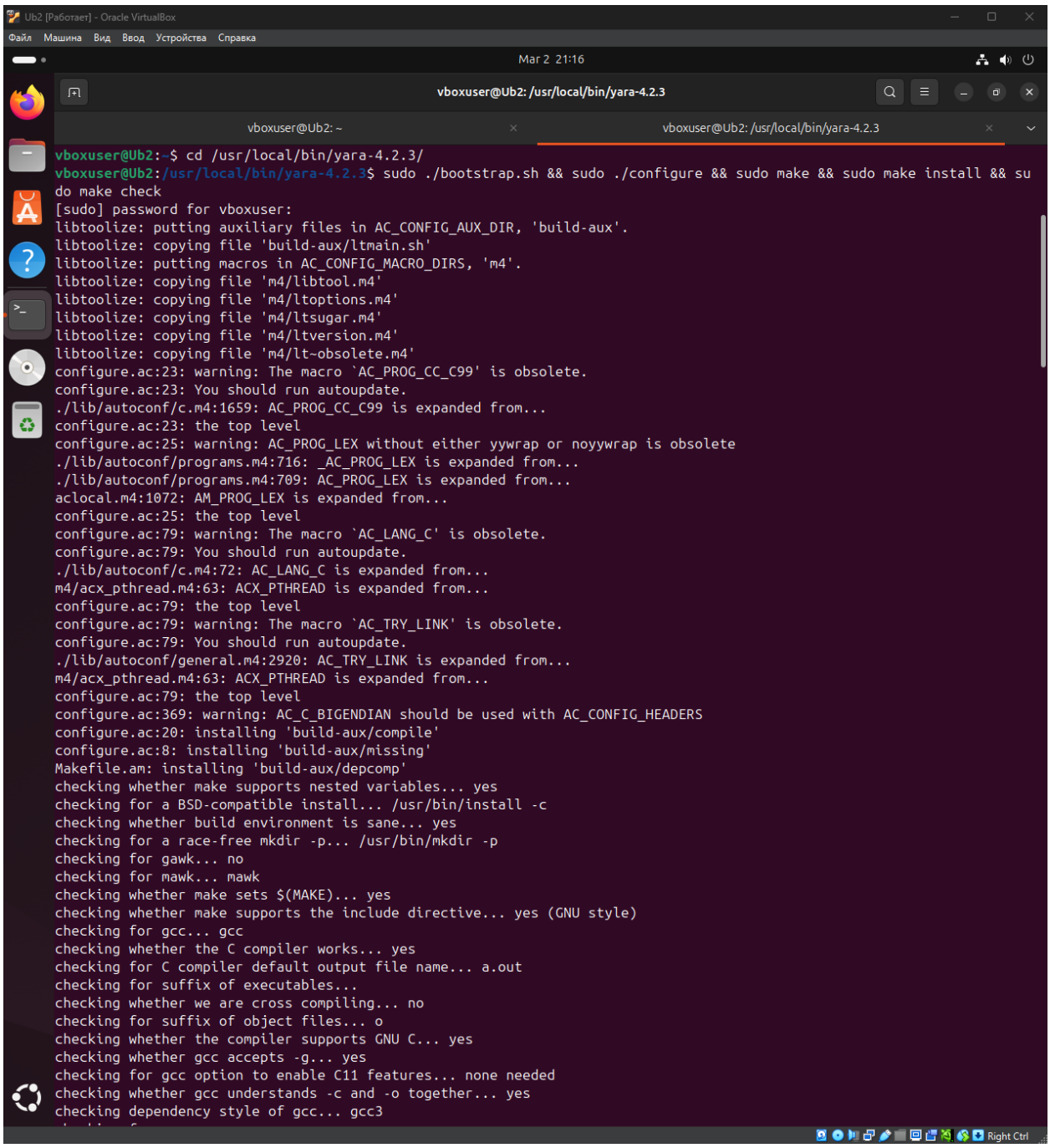

Ub2 [Работает] - Oracle VirtualBox
Файл Машина Вид Ввод Устройства Справка
Mar 2 21:03
vboxuser@Ub2: /var/log/suricata
vboxuser@Ub2: /var/log/suricata
vboxuser@Ub2: /etc/suricata/rules
(Reading database ... 150659 files and directories currently installed.)
Preparing to unpack .../00-m4_1.4.19-4build1_amd64.deb ...
Unpacking m4 (1.4.19-4build1) ...
Selecting previously unselected package autoconf.
Preparing to unpack .../01-autoconf_2.71-3_all.deb ...
Unpacking autoconf (2.71-3) ...
Selecting previously unselected package autotools-dev.
Preparing to unpack .../02-autotools-dev_20220109.1_all.deb ...
Unpacking autotools-dev (20220109.1) ...
Selecting previously unselected package automake.
Preparing to unpack .../03-automake_1%3a1.16.5-1.3ubuntu1_all.deb ...
Unpacking automake (1:1.16.5-1.3ubuntu1) ...
Selecting previously unselected package libltdl-dev:amd64.
Preparing to unpack .../04-libltdl-dev_2.4.7-7build1_amd64.deb ...
Unpacking libltdl-dev:amd64 (2.4.7-7build1) ...
Selecting previously unselected package libpkgconf3:amd64.
Preparing to unpack .../05-libpkgconf3_1.8.1-2build1_amd64.deb ...
Unpacking libpkgconf3:amd64 (1.8.1-2build1) ...
Selecting previously unselected package libssl-dev:amd64.
Preparing to unpack .../06-libssl-dev_3.0.13-0ubuntu3.5_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Selecting previously unselected package libtool.
Preparing to unpack .../07-libtool_2.4.7-7build1_all.deb ...
Unpacking libtool (2.4.7-7build1) ...
Selecting previously unselected package pkgconf-bin.
Preparing to unpack .../08-pkgconf-bin_1.8.1-2build1_amd64.deb ...
Unpacking pkgconf-bin (1.8.1-2build1) ...
Selecting previously unselected package pkgconf:amd64.
Preparing to unpack .../09-pkgconf_1.8.1-2build1_amd64.deb ...
Unpacking pkgconf:amd64 (1.8.1-2build1) ...
Selecting previously unselected package pkg-config:amd64.
Preparing to unpack .../10-pkg-config_1.8.1-2build1_amd64.deb ...
Unpacking pkg-config:amd64 (1.8.1-2build1) ...
Setting up m4 (1.4.19-4build1) ...
Setting up autotools-dev (20220109.1) ...
Setting up libpkgconf3:amd64 (1.8.1-2build1) ...
Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Setting up pkgconf-bin (1.8.1-2build1) ...
Setting up autoconf (2.71-3) ...
Setting up automake (1:1.16.5-1.3ubuntu1) ...
update-alternatives: using /usr/bin/automake-1.16 to provide /usr/bin/automake (automake) in auto mode
Setting up libtool (2.4.7-7build1) ...
Setting up pkgconf:amd64 (1.8.1-2build1) ...
Setting up libltdl-dev:amd64 (2.4.7-7build1) ...
Setting up pkg-config:amd64 (1.8.1-2build1) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for install-info (7.1-3build2) ...
vboxuser@Ub2:/var/log/suricata$ 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 423k 0 --:--:-- 0:00:02 --:--:-- 759k
vboxuser@Ub2:/var/log/suricata$
Right Ctrl

sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/

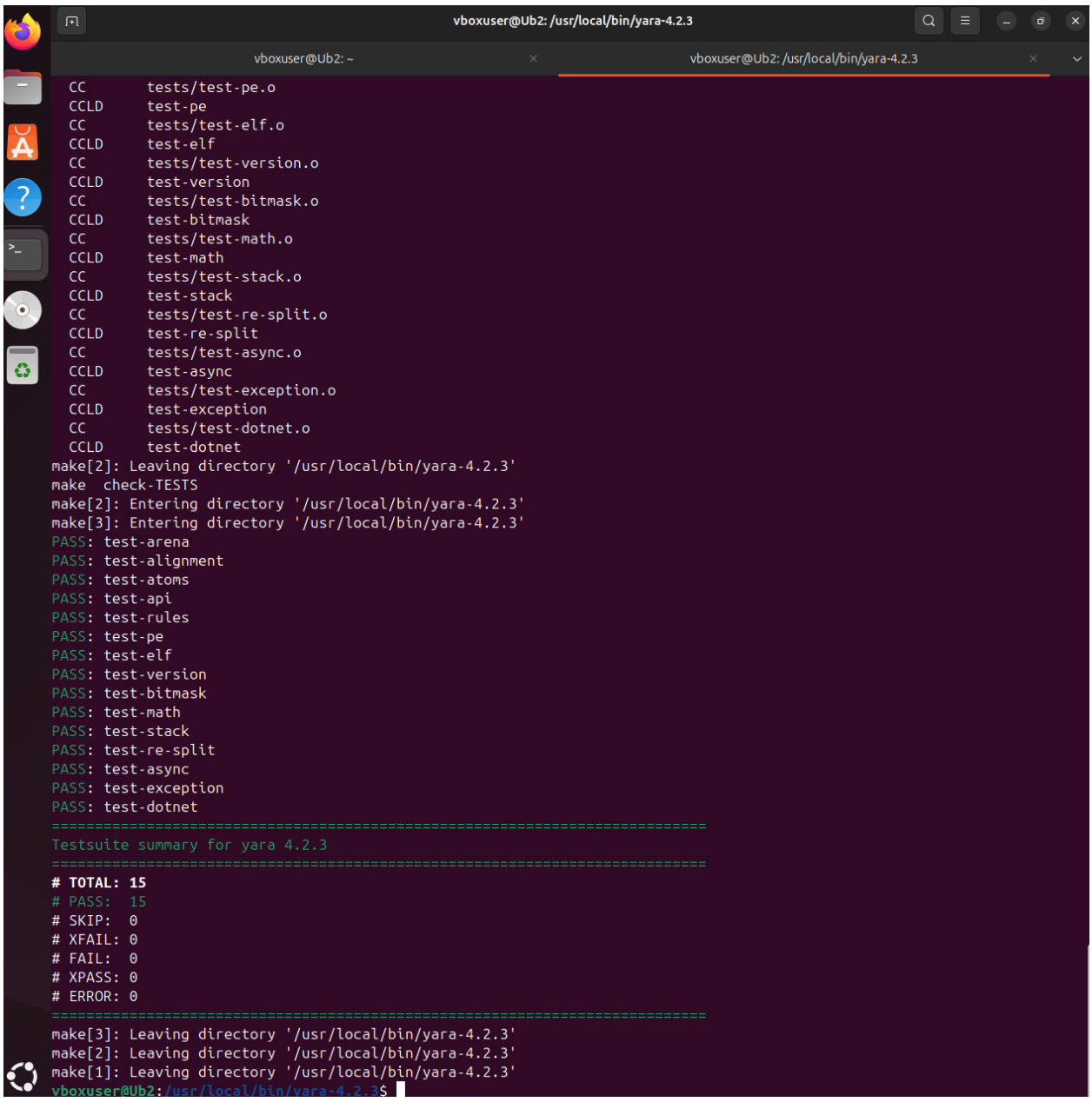
sudo rm -f v4.2.3.tar.gz



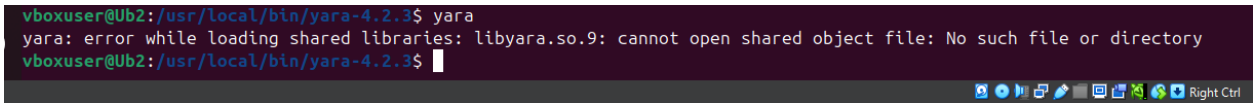
sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make install && sudo make check



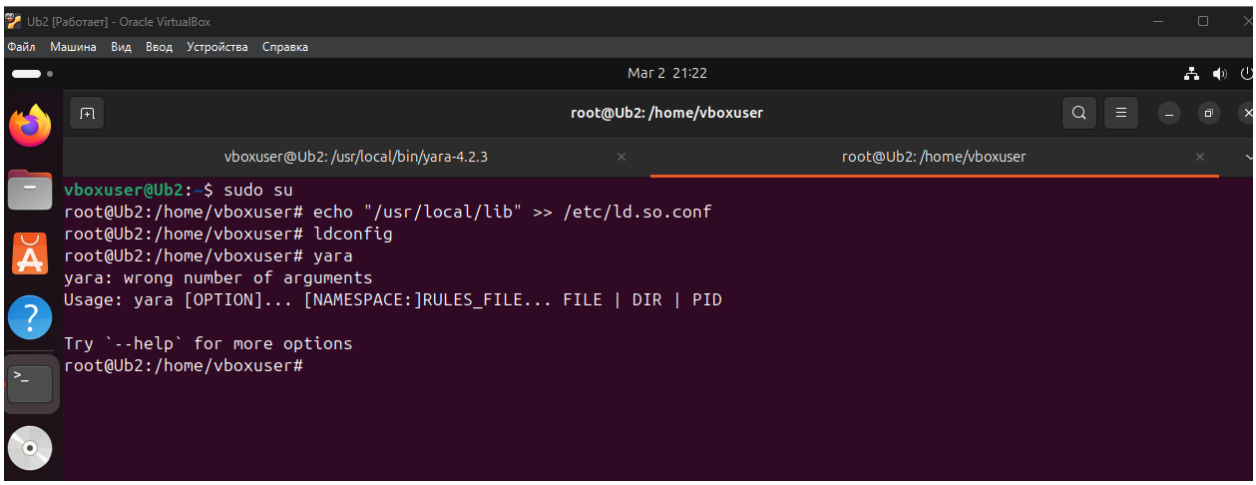
Установка завершена

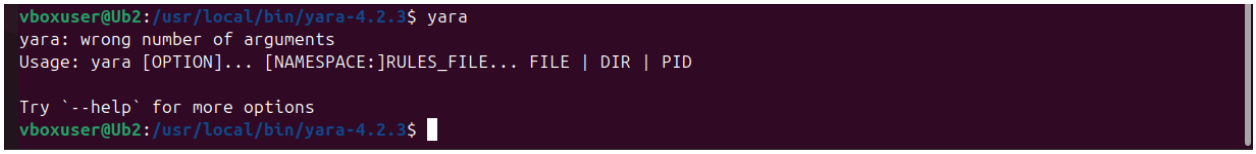


Ошибка при проверки yara



echo "/usr/local/lib" >> /etc/ld.so.conf
ldconfig

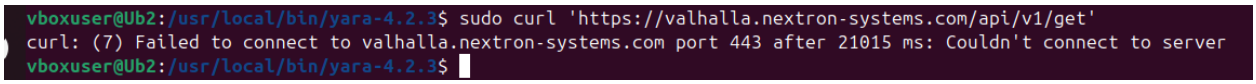




Создание директории под рулы

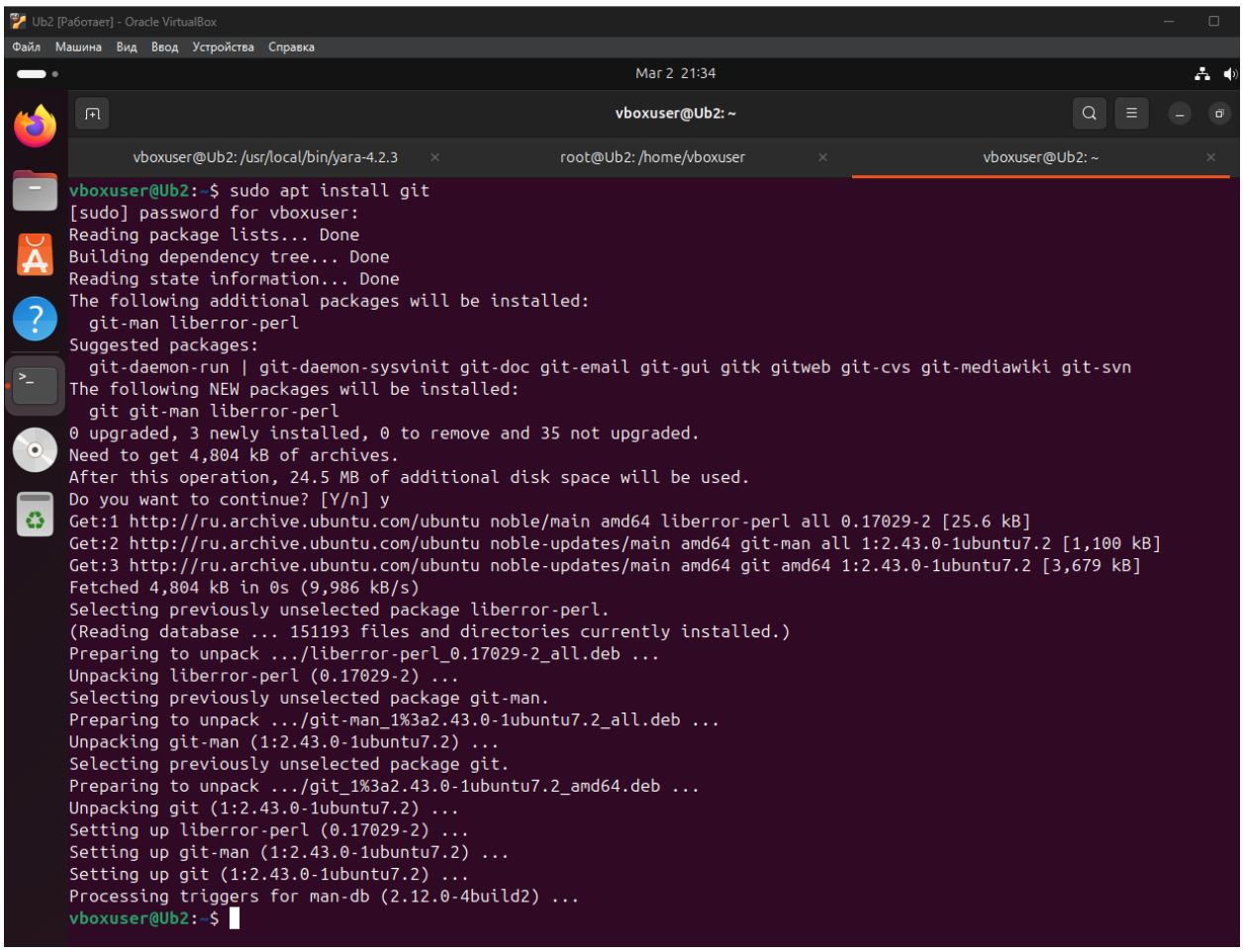
sudo mkdir -p /tmp/yara/rules

Через sudo curl 'https://valhalla.nextron-systems.com/api/v1/get' не удалось скачать



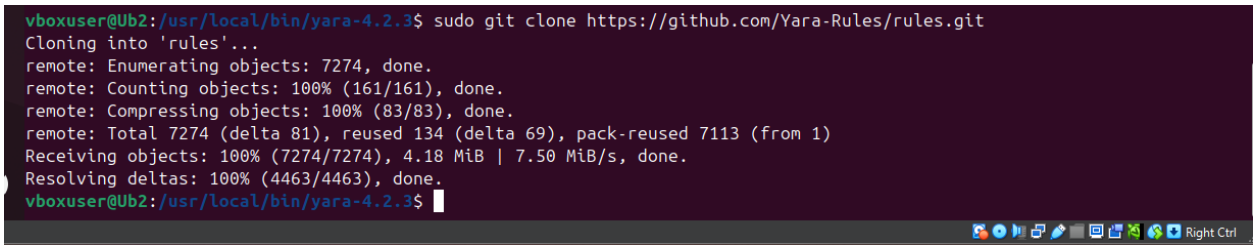
Установка через гит

sudo apt install git



Установка рулов с гита

sudo git clone https://github.com/Yara-Rules/rules.git



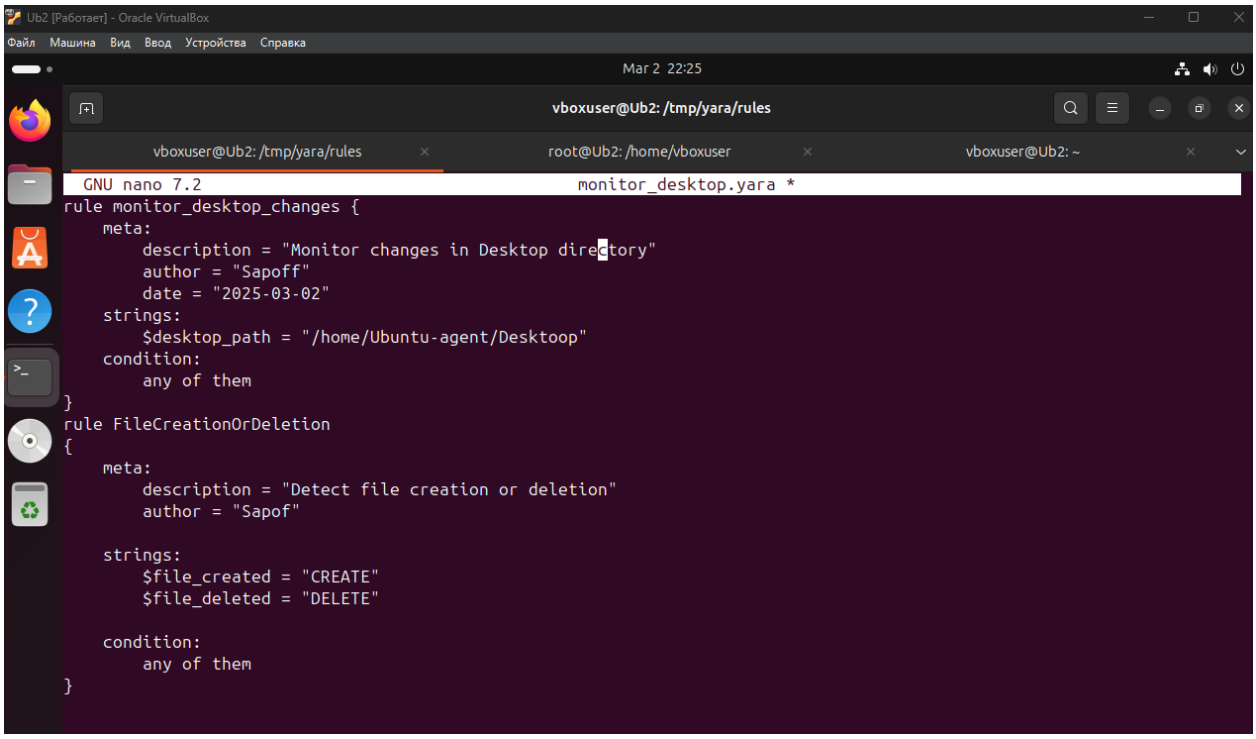
Создаю правило для с изменением файла (установка/удаление)

cd /tmp/yara/rules

sudo nano monitor_desktop.yara

```
rule monitor_desktop_changes {

    meta:

        description = "Monitor changes in Desktop directory"

        author = "Sapoff"

        date = "2025-03-02"

    strings:
```

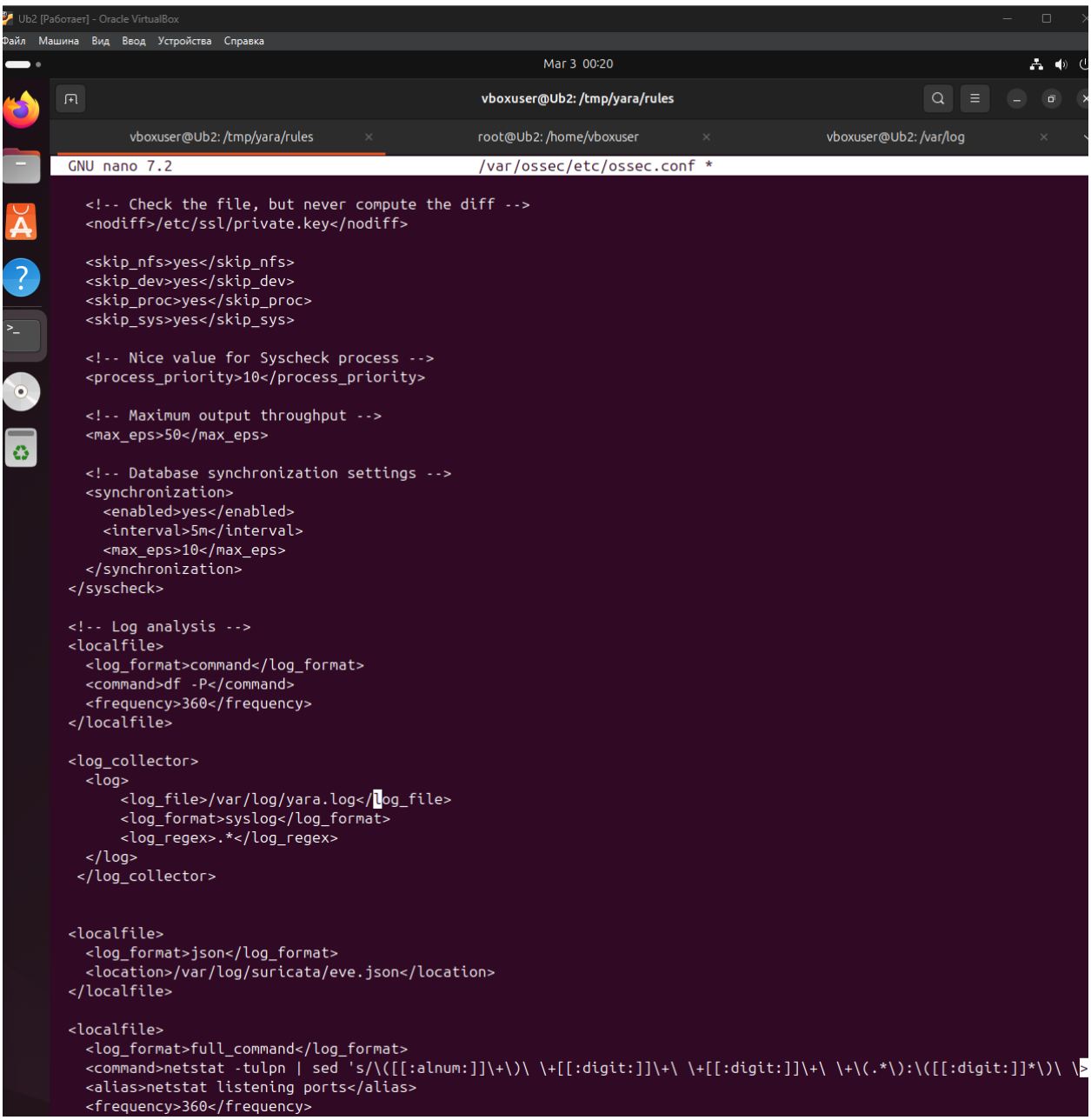
```
        $desktop_path = "/home/Ubuntu-agent/Desktoop"

    condition:

        any of them

}

rule FileCreationOrDeletion

{

    meta:

        description = "Detect file creation or deletion"

        author = "Sapof"


    strings:

        $file_created = "CREATE"

        $file_deleted = "DELETE"


    condition:

        any of them

}
```



Указываю логи в конфиге агента

sudo nano /var/ossec/etc/ossec.conf

```
 <log_collector>
   <log>
      <log_file>/var/log/yara.log</log_file>
      <log_format>syslog</log_format>
      <log_regex>.*</log_regex>
   </log>
 </log_collector>
```



Проверка правила