



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий
искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа №5

по дисциплине: «Система для сбора событий и логов»

на тему «Threat Hunting»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

д.т.н. Козачок А.В.

Москва, 2023

Содержание

| | |
|-------------------------------|-----------|
| План работы | 3 |
| Ход работы | 4 |
| 1. Инфраструктура..... | 4 |
| 4. SNORT | 5 |
| 5. YARA | 6 |
| 6. OpenVAS..... | 9 |
| Заключение | 13 |

План работы

1. . Собрать стенд по заданию;
2. Развернуть СЗИ по одному из каждого класса;
3. SIEM (Wazuh);
4. IDS/IPS (Snort);
5. ThreatHuntingTools (YARA);
6. Scanner (OpenVAS).

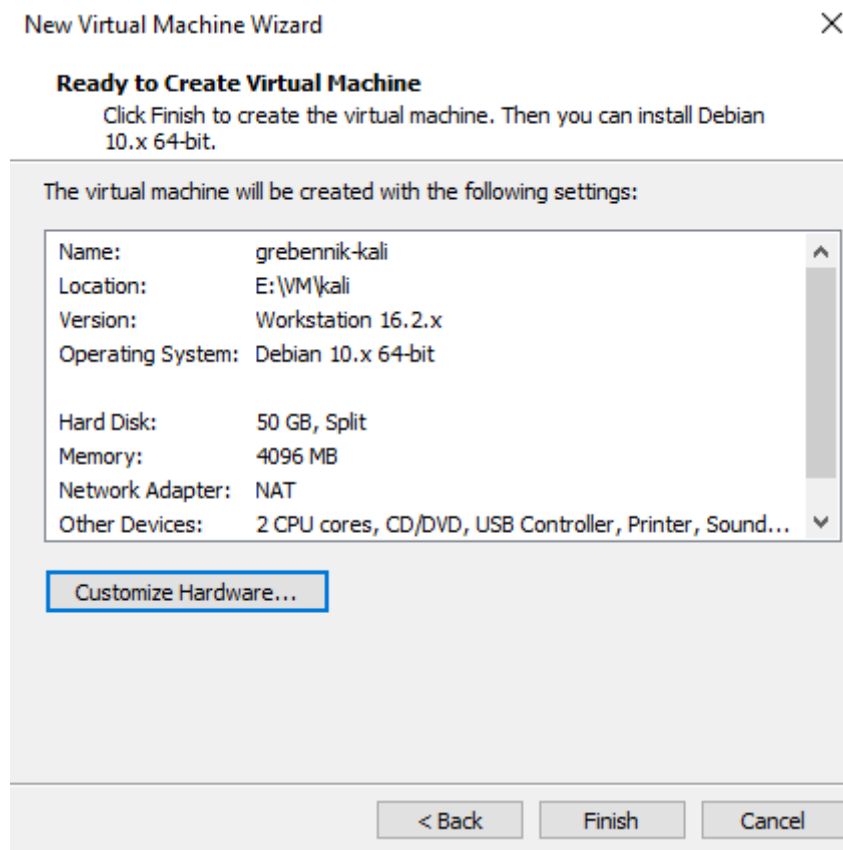
Ход работы

Threat Hunting — это процесс активного поиска и обнаружения угроз безопасности. Это практическое занятие по Threat Hunting состоит из 10 заданий, которые могут быть выполнены с использованием операционной системы Linux. GEk.y67L0SejN+8IFEkNnlo8*Oo416ta

Пункты 1, 2, 3 буду опущены, в следствие их реализации и подробном описании в практические работы №3.

1. Инфраструктура

Дополнением существующей нашей инфраструктуре будет установка Kali-Linux.

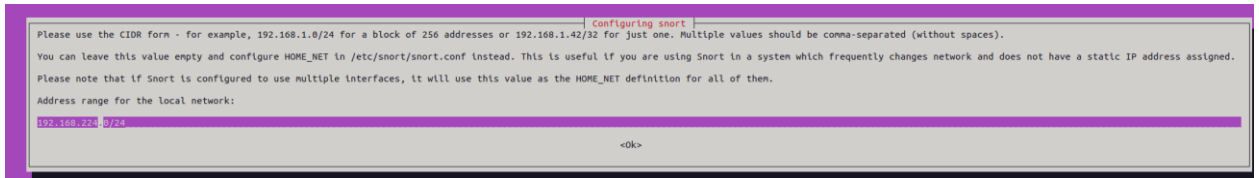


```
(gog-kali@gog-kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:1d:52:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.224.157/24 brd 192.168.224.255 scope global dynamic noprefix
route eth0
        valid_lft 1735sec preferred_lft 1735sec
    inet6 fe80::20c:29ff:fe1d:5256/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

4. SNORT

4.1. Установка Snort:

```
root@gog-agent:~# apt-get install snort -y
```



4.2. Указание домашней сети в конфиге:

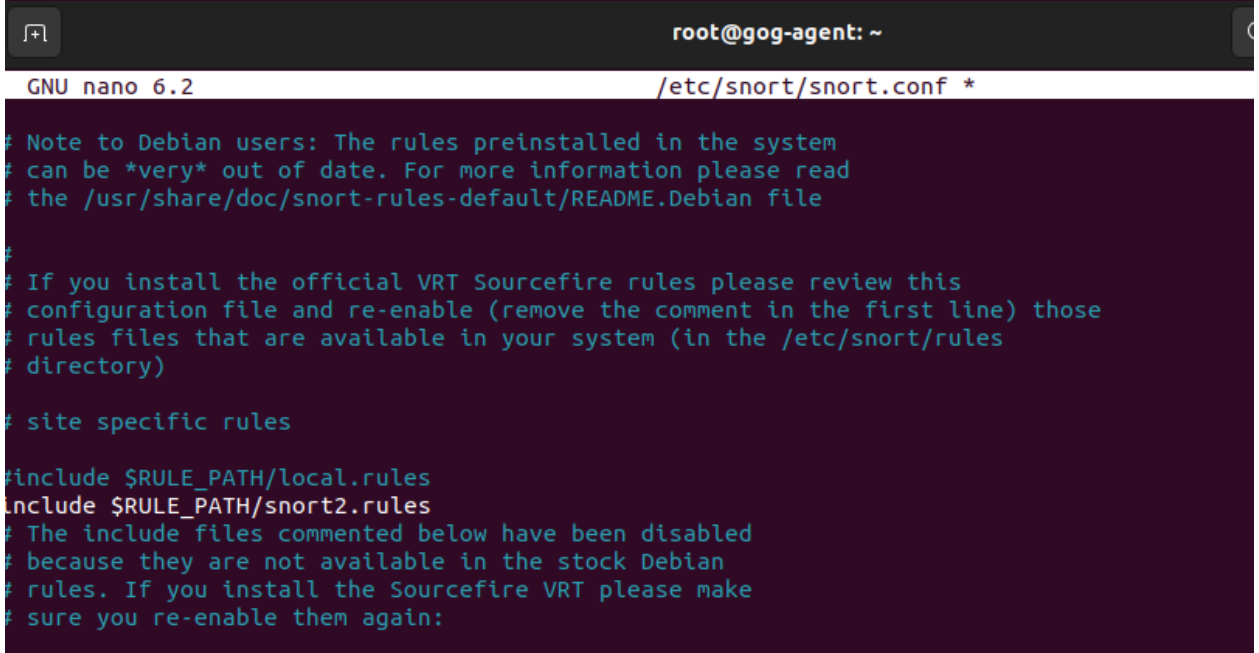
```
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.224.0/16

# Set up the external network addresses. Leave as "any" in m
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alte
```

4.3. Загрузка правил:

```
root@gog-agent:~# nano /etc/snort/snort.conf
root@gog-agent:~# git clone https://github.com/ditekshen/detection
Cloning into 'detection'...
remote: Enumerating objects: 1252, done.
remote: Counting objects: 100% (340/340), done.
remote: Compressing objects: 100% (138/138), done.
remote: Total 1252 (delta 235), reused 298 (delta 196), pack-reused 912
Receiving objects: 100% (1252/1252), 878.51 KiB | 3.57 MiB/s, done.
Resolving deltas: 100% (893/893), done.
root@gog-agent:~#
```

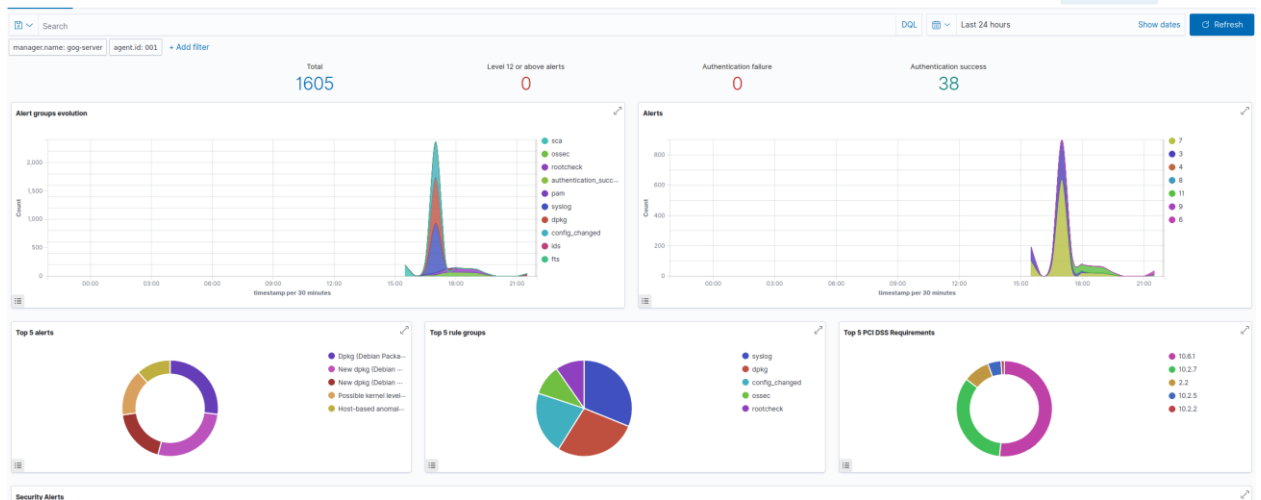
```
root@gog-agent:~# cp detection/snort/snort2.rules /etc/snort/rules/snort2.rules
```



4.4. Интеграция Wazuh и Snort

```
<apt_key>073103eade80734104097ec74030c1094cc000372313
<group>syscheck</group>
<alert_format>json</alert_format>
/integration>

<localfile>
  <log_format>snort-full</log_format>
  <location>/var/log/snort/snort.alert.fast</location>
</localfile>
```



5. YARA

5.1(Был установлен virustotal, данный пункт был опущен, но присутствует скрин интеграции, никаких проблем при установке не было обнаружено, при выполнении пунктов по инструкции, так же для регистрации на сайте самого virustotal достаточно использовать пустышку гугл. аккаунта).

5.2. 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
sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f v4.2.3.tar.gz
cd /usr/local/bin/yara-4.2.3/
sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make install && sudo make check
Hit:1 http://ru.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:3 http://ru.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 https://packages.wazuh.com/4.x/apt stable InRelease
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:6 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1 326 kB]
Get:7 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [560 kB]
Get:8 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [268 kB]
Get:9 http://ru.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1 042 kB]
Get:10 http://ru.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [686 kB]
Fetched 4 109 kB in 1s (7 310 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
```

```

Processing triggers for man-db (2.10.2-1) ...
Processing triggers for install-info (6.8-4build1) ...
  % 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 1145k     0  --:--:--  0:00:01  --:--:-- 4922k
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
=====

```

Testsuite summary for yara 4.2.3

```

=====
# TOTAL: 15
# PASS: 15
# SKIP: 0
# XFAIL: 0
# FAIL: 0
# XPASS: 0
# ERROR: 0
=====

```

```

root@gog-server:/usr/local/bin/yara-4.2.3# yara
yara: wrong number of arguments
Usage: yara [OPTION]... [NAMESPACE:]RULES_FILE... FILE | DIR | PID

Try `--help` for more options
root@gog-server:/usr/local/bin/yara-4.2.3#

```

```

root@gog-server:~# git clone https://github.com/ditekshen/detection
Cloning into 'detection'...
remote: Enumerating objects: 1252, done.
remote: Counting objects: 100% (340/340), done.
remote: Compressing objects: 100% (138/138), done.
remote: Total 1252 (delta 235), reused 298 (delta 196), pack-reused 912
Receiving objects: 100% (1252/1252), 878.51 KiB | 3.51 MiB/s, done.
Resolving deltas: 100% (893/893), done.

```

```

GNU nano 6.2 yara_decoders.xml *
<decoder name="yara">
  <parent>yara</parent>
  <regex offsets="after_parent">into: (\$+) (\.+)</regex>
  <order>yara_rule, file_path</order>
</decoder>

```

```

root@gog-server:/var/ossec/etc/decoders# ls
local_decoder.xml  yara_decoders.xml

```

```

GNU nano 6.2 yara_rules.xml *
  <field name="error_message">\.+</field>
  <description>YARA error detected.</description>
</rule>
<rule id="100102" level="10">
  <if_sid>100100</if_sid>
  <field name="yara_rule">\.+</field>
  <description>YARA $(yara_rule) detected.</description>
</rule>
:gorup

```

```

debconf.conf      init.d
debian_version    initramfs-tools
default           inputrc
deluser.conf      insserv.conf.d
depmod.d          ipp-usb
dhcp              iproute2
dictionaries-common
dpkg              issue
                  issue.net
root@gog-server:/etc# mkdir yara
root@gog-server:/etc# ls
acpi              emacs
adduser.conf      environment
alsa              environment.d
alternatives      ethertypes
anacrontab        filebeat
apg.conf          firefox
apm               fonts
apparmor          fprintd.conf
apparmor.d        fstab
appport           fuse.conf
appstream.conf    fwupd
apt               gai.conf
avahi             gdb
bash.bashrc       gdm3
bash_completion   geoclue
bash_completion.d ghostscript
bindresvport.blacklist
binfmt.d          glvnd
bluetooth         gnome
brlapi.key        groff
brltty            group
brltty.conf       group-
ca-certificates   grub.d
ca-certificates.conf
ca-certificates.conf.dpkg-old
chatscripts       gshadow
console-setup     gshadow-
cracklib           gss
cron.d            gtk-2.0
cron.daily         gtk-3.0
cron.hourly        hdparm.conf
cron.monthly       host.conf
crontab           hostid
cron.weekly        hostname
cups              hosts
cupshelpers       hosts.allow
dbus-1            hosts.deny
dconf             hp
debconf.conf      ifplugd
debian_version    init
default           init.d
deluser.conf      initramfs-tools
depmod.d          inputrc
dhcp              insserv.conf.d
dictionaries-common
dpkg              ipp-usb
e2scrub.conf      iproute2
                  issue
                  issue.net
                  kernel
                  kernel-img.conf
netplan            kernelloops.conf
network            ldap
networkd-dispatcher
NetworkManager    ld.so.cache
networks           ld.so.conf
newt               ld.so.conf.d
nftables.conf     legal
nsswitch.conf      libao.conf
                  libaudit.conf
                  libblockdev
                  libnl-3
                  libpaper.d
                  libreoffice
                  locale.alias
                  locale.gen
                  localtime
                  logcheck
                  login.defs
                  logrotate.conf
                  logrotate.d
                  lsb-release
                  machine-id
                  magic
                  magic.mime
                  mailcap
                  mailcap.order
                  manpath.config
                  mime.types
                  mke2fs.conf
                  ModemManager
                  modprobe.d
                  modules
                  modules-load.d
                  mtab
                  nanorc
                  netconfig
                  netplan
                  network
                  networkd-dispatcher
                  NetworkManager
                  networks
                  newt
                  nftables.conf
                  nsswitch.conf
                  openvpn
                  opt
                  os-release
security           PackageKit
selinux            pam.conf
sensors3.conf     pam.d
sensors.d         papersize
services          passwd
sgml              passwd-
shadow            pcmcia
shadow-           perl
                  sudo
                  sudoers
                  sudoers.d
                  sudo_logsrvd.conf
                  sysctl.conf
                  sysctl.d
                  systemd
                  terminfo
                  thermald
                  thunderbird
                  timezone
                  tmpfiles.d
                  ubuntu-advantage
                  ucf.conf
                  udev
                  udisks2
                  ufw
                  update-manager
                  update-motd.d
                  update-notifier
                  UPower
                  usb_modeswitch.conf
                  usb_modeswitch.d
                  vim
                  vmware-tools
                  vtrgb
                  vulkan
                  wazuh-dashboard
                  wazuh-indexer
                  wgetrc
                  wpa_supplicant
                  X11
                  xattr.conf
                  xdg
                  xml
                  yara
                  zsh_command_not_found

```



```

GNU nano 6.2 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 -----#

# Response
FILENAME=$0
LOCAL="dirname $0"
#EXTRA arg
YARA_PATH=
YARA_RULES=
while [ "$1" != "" ]; do
    case $1 in
        -yara_path) shift
            YARA_PATH=$2
            ;;
        -yara_rules) shift
            YARA_RULES=$2
            ;;
        *) shift
    esac
done
cd $LOCAL
cd ../
# Set LOG_FILE path
PWD=$(pwd)
LOG_FILE="$PWD/../logs/active-responses.log"
#----- Analyze parameters -----#

if [[ ! $YARA_PATH ]] || [[ ! $YARA_RULES ]]; then
    echo "wazuh-yara: ERROR: Yara path and rules parameters are mandatory." >> $LOG_FILE
    exit 1
fi

#----- Main workflow -----#

# Execute Yara scan on the specified filename
yara_output=$(("$YARA_PATH"/yara -w -r "$YARA_RULES" "$FILENAME"))

if [[ $yara_output != "" ]]; then
    # Iterate every detected rule and append it to the LOG_FILE
    while read -r line; do
        echo "wazuh-yara: info: $line" >> $LOG_FILE
    done << "$yara_output"
fi

exit 1;

```

```

root@gog-server:/var/ossec/active-response/bin/yara.sh# touch yara.sh
root@gog-server:/var/ossec/active-response/bin/yara.sh# nano yara.sh
root@gog-server:/var/ossec/active-response/bin/yara.sh# nano yara.sh
root@gog-server:/var/ossec/active-response/bin/yara.sh# ls
yara.sh
root@gog-server:/var/ossec/active-response/bin/yara.sh# sudo chmod 750 /var/ossec/active-response/bin/yara.sh
root@gog-server:/var/ossec/active-response/bin/yara.sh# chown root:wazuh /var/ossec/active-response/bin/yara.sh
root@gog-server:/var/ossec/active-response/bin/yara.sh#

```

6. OpenVAS

6.1 Установка openvas согласно инструкции на Kali:

```

(root@ gog-kali)-[/home/gog-kali]
# sudo apt install -y openvas
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Заметьте, вместо «openvas» выбирается «gvm»
Следующий пакет устанавливался автоматически и больше не требуется:
cython3 debtags gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gir1.2-webkit2-4.0 gobject-introspection
gobject-introspection-bin kali-debtags king-phisher libarmadillo11 libblkid-dev libblockdev-crypto2 libblockdev-fs2
libblockdev-loop2 libblockdev-part-err2 libblockdev-part2 libblockdev-swap2 libblockdev-utils2 libblockdev2
libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgdal32 libgeos3.11.1 libglib2.0-dev libglib2.0-dev-bi
libgumbo1 libgupnp-igd-1.0-4 libjavascriptcoregtk-4.0-18 libjim0.81 libmount-dev libmujs2 libncurses5 libnfs13 libobjc-1
libpcre2-32-0 libpcre2-dev libpcre2-posix3 librtlsdr0 libselinux1-dev libsepol-dev libsoup-gnome2.4-1 libspatialite7
libsuperlu5 libtexluajit2 libtinfo5 libucl1 libutf8proc2 libwebkit2gtk-4.0-37 libwebsockets17 libyara9 libzxing2 lua-lpe
python3-advancedhttpserver python3-aioredis python3-apscheduler python3-backcall python3-boltons python3-cairo-dev
python3-cryptography37 python3-debian python3-flask-security python3-future python3-geoip2 python3-geojson python3-graph
python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay python3-icalendar python3-jaraco.classes python3-j
python3-maxminddb python3-pickleshare python3-promise python3-py python3-pyminifier python3-pytz-deprecation-shim
python3-quamash python3-rfc3986 python3-rule-engine python3-rx python3-smoke-zephyr python3-texttable python3-tzlocal
python3-unicodesv tftp uuid-dev

```

6.2. MOpenVAS поставляется с собственной службой Redis для Kali GNU/Linux. Убедимся, что сервис Redis настроен для корректной работы с OpenVAS командой «systemctl status redisserver@openvas.service».

```
(root@gog)~[/home/gog]
# systemctl start redis-server@openvas.service

(root@gog)~[/home/gog]
# systemctl status redis-server@openvas.service
● redis-server@openvas.service - Advanced key-value store (openvas)
   Loaded: loaded (/usr/lib/systemd/system/redis-server@.service; disabled; preset: disabled)
   Active: active (running) since Tue 2024-01-19 12:22:42 MSK; 29s ago
     Docs: http://redis.io/documentation,
           man:redis-server(1)
   Main PID: 331139 (redis-server)
   Status: "Ready to accept connections"
     Tasks: 5 (limit: 14374)
    Memory: 8.9M (peak: 9.3M)
       CPU: 118ms
    CGroup: /system.slice/system-redis\x2dservice.slice/redis-server@openvas.service
            └─331139 */usr/bin/redis-server unixsocket:/run/redis-openvas/redis-server.sock

янв 19 12:22:42 gog redis-server[331139]: Supervised by systemd. Please make sure you set appropriate values for TimeoutStartSec and TimeoutStopSec in your service unit.
янв 19 12:22:42 gog redis-server[331139]: o000o000o000o Redis is starting o000o000o000o
янв 19 12:22:42 gog redis-server[331139]: Redis version=7.0.15, bits=64, commit=00000000, modified=0, pid=331139, just started
янв 19 12:22:42 gog redis-server[331139]: Configuration loaded
янв 19 12:22:42 gog redis[331139]: monotonic clock: POSIX clock_gettime
янв 19 12:22:42 gog redis[331139]:

Redis 7.0.15 (00000000/0) 64 bit
Running in standalone mode
Port: 0
PID: 331139

https://redis.io
```

6.3. При попытке запустить настройку сервиса, получаем ошибку о версии СУБД. Для решения данной проблемы необходимо заменить порт текущей версии СУБД на 5433, а порт необходимой версии заменить на 5432, после перезапустим postgresql:

```
(root@gog)~[/home/gog]
# gvm-setup

[>] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (15) is not 16 that is required by libgvm
[-] ERROR: libgvm needs PostgreSQL 16 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster

(root@gog)~[/home/gog]
#listen_addresses = 'localhost' # what IP address(es) to listen on;
                                # comma-separated list of addresses;
                                # defaults to 'localhost'; use '*' for all
                                # (change requires restart)
port = 5433 # (change requires restart)
max_connections = 100 # (change requires restart)
#superuser_reserved_connections = 3 # (change requires restart)
unix_socket_directories = '/var/run/postgresql' # comma-separated list of directories
                                                # (change requires restart)
#unix_socket_group = '' # (change requires restart)
```

```

(root@gog)-[/home/gog]
# nano /etc/postgresql/15/main/postgresql.conf

(root@gog)-[/home/gog]
# nano /etc/postgresql/16/main/postgresql.conf

(root@gog)-[/home/gog]
# systemctl restart postgresql

(root@gog)-[/home/gog]
#

```

- 6.4. Запускаем настройки сервиса и после проверяем успешность установки

```

(root@gog)-[/home/gog]
# gvm-setup

[>] Starting ...
[>] Creating ...
[>] Creating ...
[*] Creating ...
[*] Creating ...
[*] Creating ...
CREATE ROLE
[*] Applying ...
GRANT ROLE
[*] Creating ...
CREATE EXTENSION
[*] Creating ...
CREATE EXTENSION
[*] Creating ...

```

```

(root@gog)-[/home/gog]
# gvm-check-setup
gvm-check-setup 23.11.0
Test completeness and readiness of GVM-23.11.0
Step 1: Checking OpenVAS (Scanner)...
OK: OpenVAS Scanner is present in version 22.7.9.
OK: Notus Scanner is present in version 22.6.2.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
OK: _gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket: /va
sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 88018 NVTs.
OK: The notus directory /var/lib/notus/products contains 453 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting ospd-openvas service
Waiting for ospd-openvas service
OK: ospd-openvas service is active.
OK: ospd-OpenVAS is present in version 22.6.2.
Step 2: Checking GVM Manager ...
OK: GVM Manager (gvm) is present in version 23.1.0.
Step 3: Checking Certificates ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CERT data found in /var/lib/gvm/cert-data.

```

```

[root@gog]~[/home/gog]
# gvm-check-setup
gvm-check-setup 23.11.0
Test completeness and readiness of GVM-23.11.0
Step 1: Checking OpenVAS (Scanner) ...
OK: OpenVAS Scanner is present in version 22.7.9.
OK: Notus Scanner is present in version 22.6.2.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
OK: _gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket: /va
sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 88018 NVTs.
OK: The notus directory /var/lib/notus/products contains 453 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting ospd-openvas service
Waiting for ospd-openvas service
OK: ospd-openvas service is active.
OK: ospd-OpenVAS is present in version 22.6.2.
Step 2: Checking GVM Manager ...
OK: GVM Manager (gvm) is present in version 23.1.0.
Step 3: Checking Certificates ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CERT data found in /var/lib/gvm/cert-data.

```

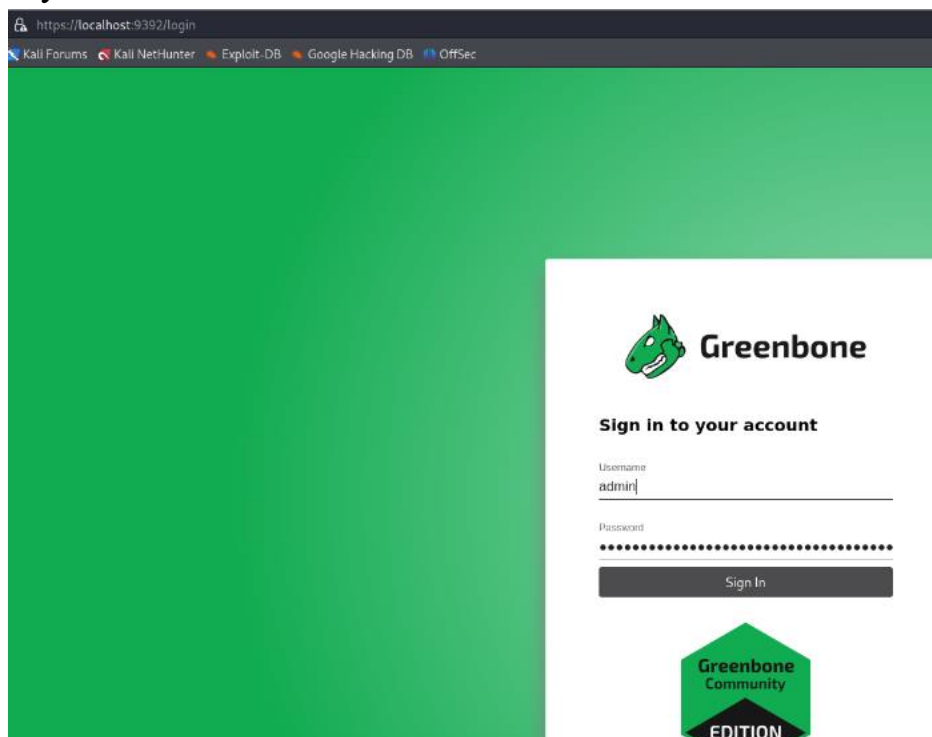
6.5 Настроим сервис gvm и обновим базу OpenVAS, включим сервис gvm:

```

[root@gog]~[/home/gog]
# greenbone-feed-sync
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
+ Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to
/var/lib/notus
+ Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to
/var/lib/openvas/plugins


```

6.6 Переходим в веб-интерфейс по адресу <https://localhost:9392/>. Вводим учетные данные пользователя admin и сразу попадаем на главную страницу:



6.7 Запускаем Task Wizard для сканирования узла(была проанализирована в м с накатаной Damn Vulnerable Linux)

Task Wizard



Quick start: Immediately scan an IP address


IP address or hostname:

The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.


The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

Cancel

Start Scan

6.8. Результаты сканирования:

| Information | Results (2 of 17) | Hosts (1 of 1) | Ports (0 of 2) | Applications (4 of 4) | Operating Systems (1 of 1) |
|--|----------------------|-------------------|-------------------|--------------------------|-------------------------------|
| Application CPE | | | | | |
| cpe:/a:apple:cups:1.1 | | | | | |
| cpe:/a:openprinting:cups:1.1 | | | | | |
|  cpe:/a:mysql:mysql | | | | | |

| Information | Results (2 of 17) | Hosts (1 of 1) | Ports (0 of 2) | Applications (4 of 4) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0) |
|--|----------------------|-------------------|-------------------|--------------------------|-------------------------------|---|-------------------------|------------------------------|----------------------------|------------------|
| CVE | | | | | | NVT | | | | |
| CVE-1999-0524 | | | | | | ICMP Timestamp Reply Information Disclosure | | | | |
| (Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse=severity) | | | | | | | | | | |
| 1 - 1 | | | | | | | | | | |
| Severity | | High | Medium | Low | Log | False Pos. | Ac | | | |
| 9.9 (High) | | 13 | 20 | 3 | 34 | 0 | | | | |
| Apply to page contents | | | | | | | | | | |

Закключение

В рамках данной практической работы были развернуты и настроены СЗИ разных классов, которые при совместном использовании на информационной системе и должной пред настройке могут обеспечить высокий уровень защиты. Благодаря данной работе были получены навыки полезные практические навыки, как по настройке средств мониторинга, так и понимания организации защиты информации.