МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

Отчет по практической работе №7

по дисциплине: «Управление информационной безопасностью»

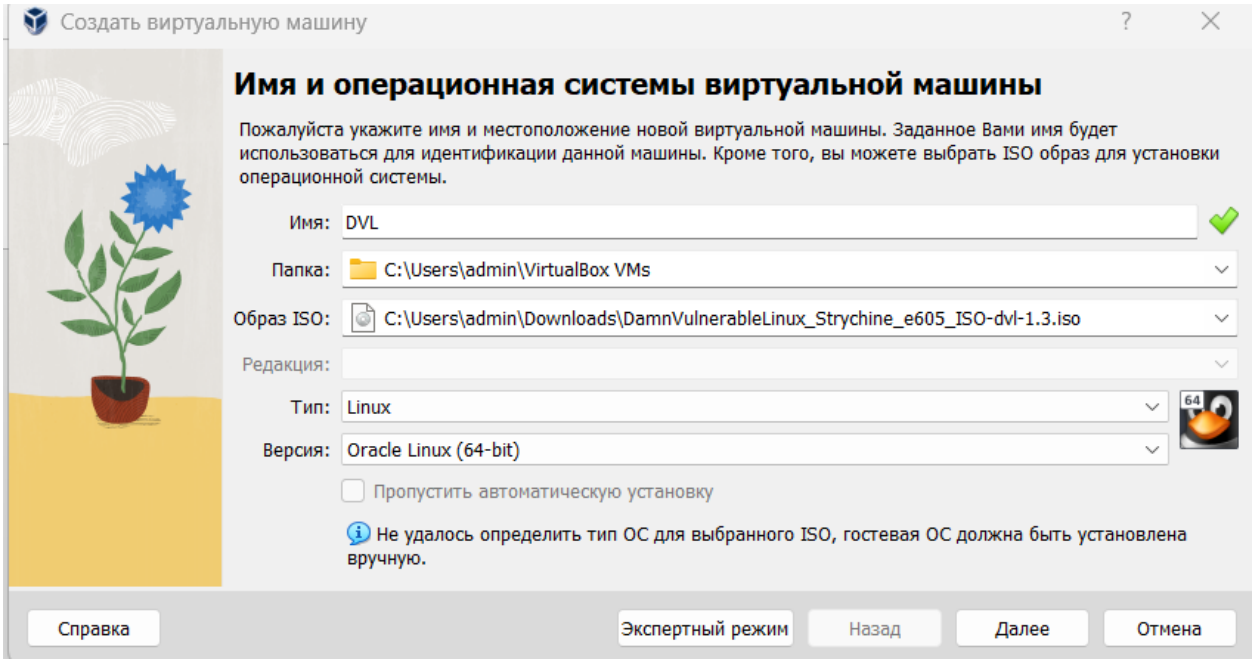
Выполнил:
Студент группы ББМО-01-22
ФИО: Карев Д.П.

Проверил:

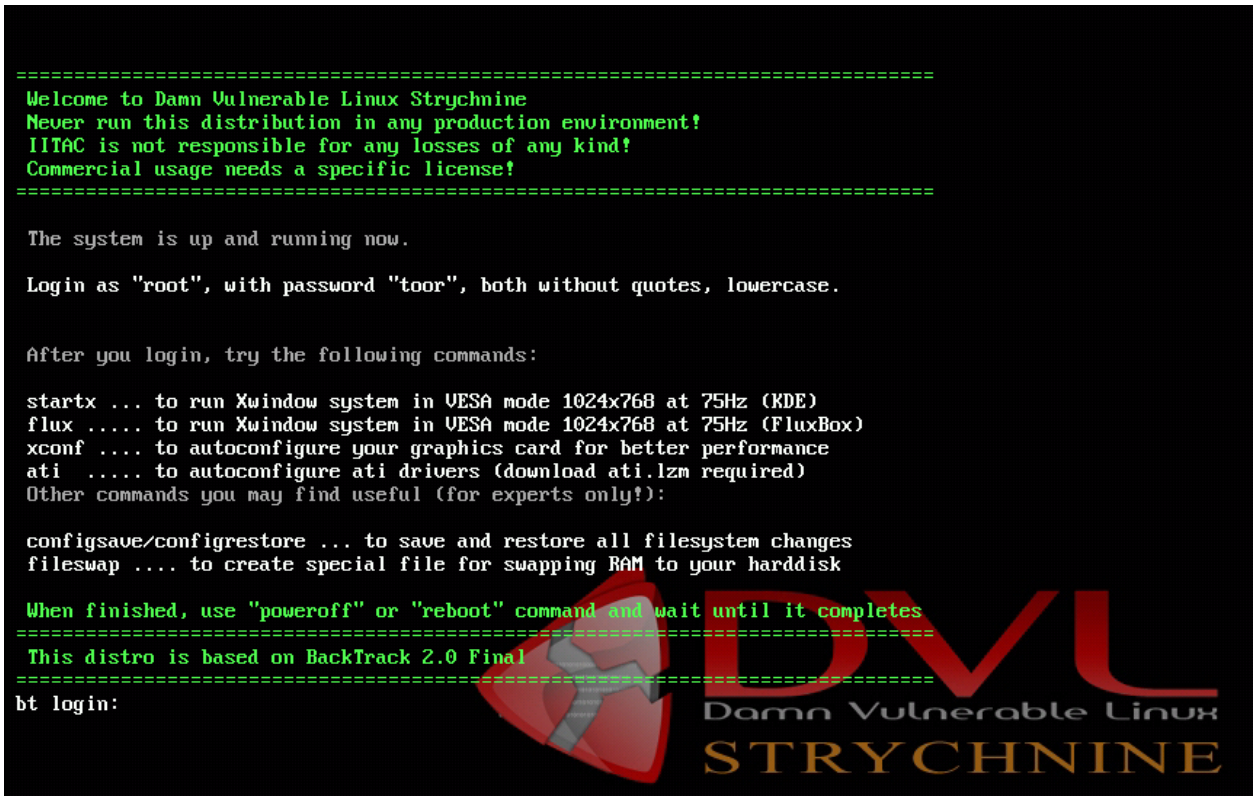
Р.В. Пимонов

Москва 2023

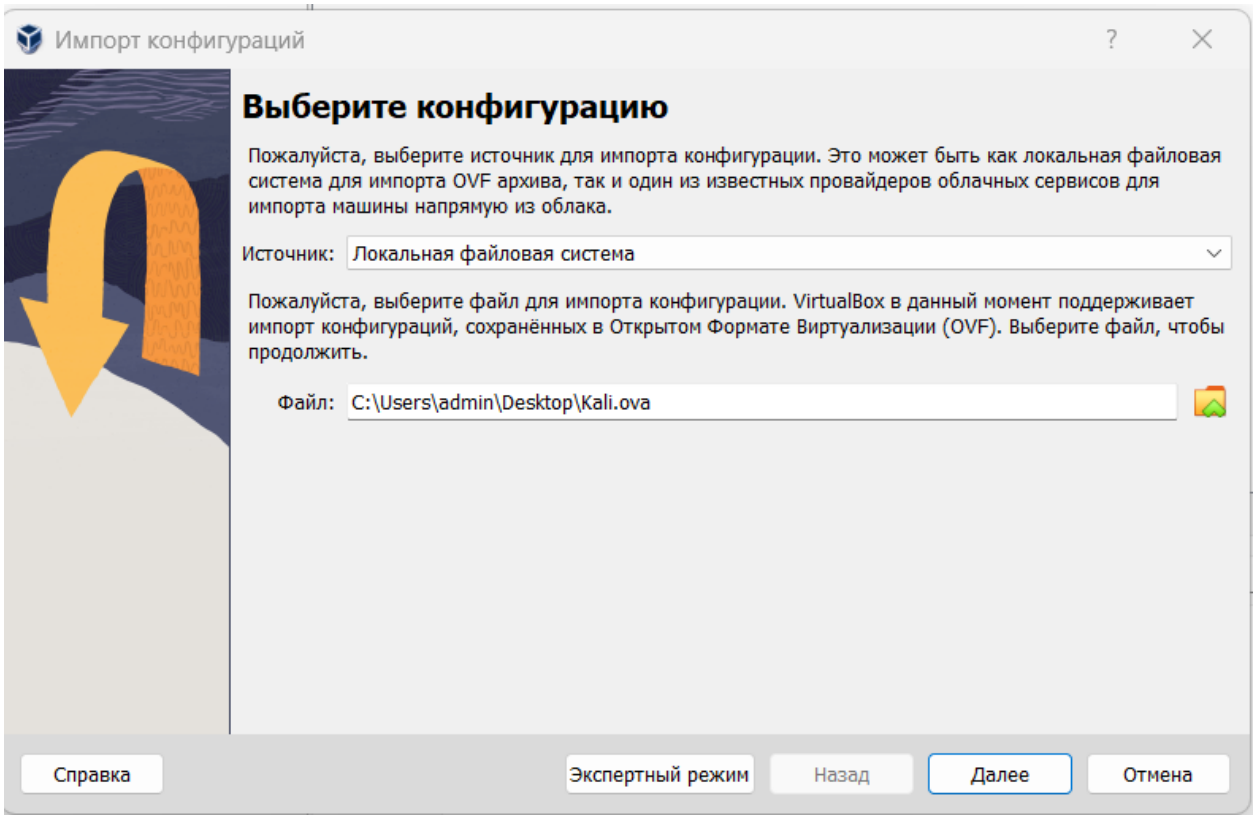
Начнем с установки ОС DVL



После установки, войдем по логину root и паролю toor.



После успешной установки ОС, приступим к установки Kali, также будем ставить в среде виртуализации VirtualBox.



Посмотрим, какой ip адрес у наших систем(для начала поставим сетевой мост)

```
┌──(root㉿kali)-[/home/kali]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault 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 pfifo_fast state U
P group default qlen 1000
    link/ether 08:00:27:95:bd:54 brd ff:ff:ff:ff:ff:ff
    inet 10.0.7.49/24 brd 10.0.7.255 scope global dynamic noprefixroute eth0
       valid_lft 42898sec preferred_lft 42898sec
    inet6 fe80::a00:27ff:fe95:bd54/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali]
└─#
```

```
bt ~ # ip a
1: lo: <LOOPBACK,UP,10000> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,NOTRAILERS,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ba:7f:cb brd ff:ff:ff:ff:ff:ff
    inet 10.0.7.50/24 brd 10.0.7.255 scope global eth0
bt ~ #
```

Приступим к анализу нашей ОС DVL с помощью команды nmap.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 10.0.7.50
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-18 05:08 EST
Nmap scan report for 10.0.7.50
Host is up (0.00073s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
631/tcp  open  ipp     CUPS 1.1
|_http-title: 403 Forbidden
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 08:00:27:BA:7F:CB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.73 ms 10.0.7.50

OS and Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
```

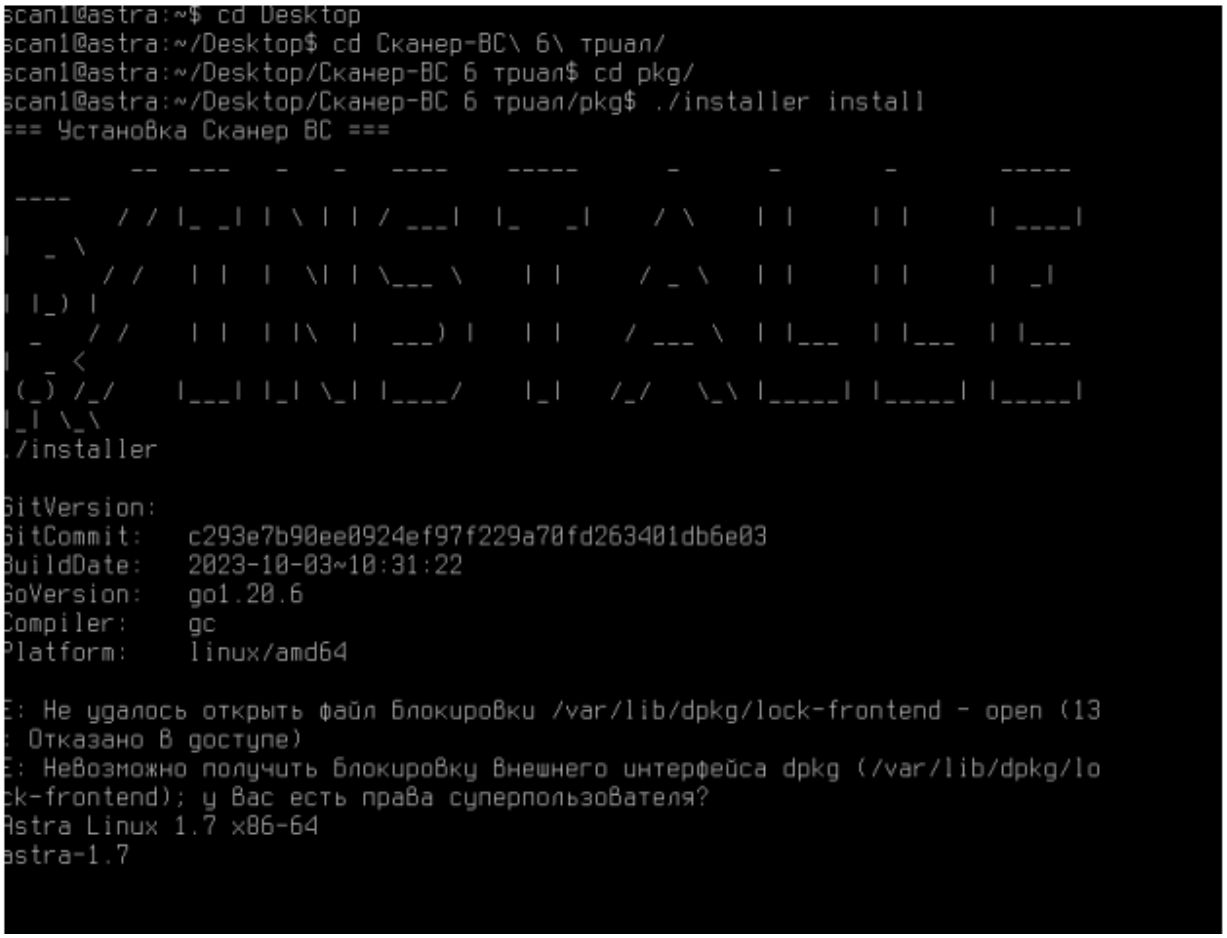
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 10.0.7.50
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-18 05:11 EST
Nmap scan report for 10.0.7.50
Host is up (0.00025s latency).
Not shown: 98 closed tcp ports (reset)
PORT     STATE SERVICE
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: 08:00:27:BA:7F:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Нам показаны все открытые порты. Для понимания их уязвимостей воспользуемся средством анализи защищенности Сканер-ВС.

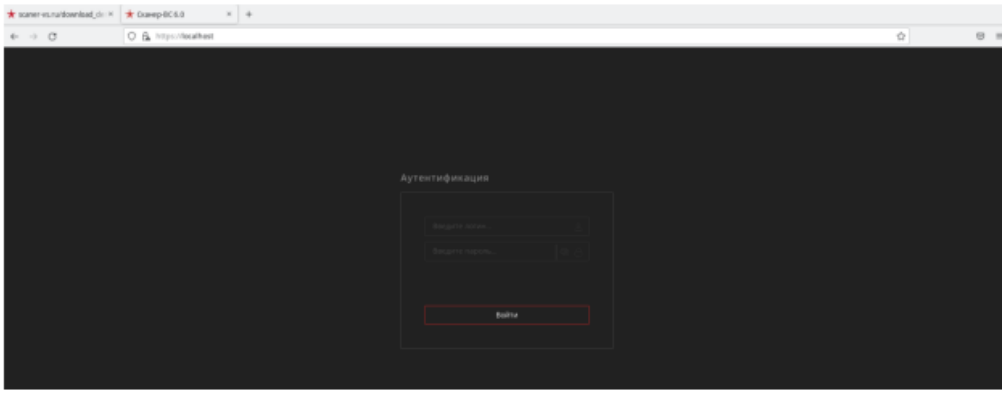
Для установки Сканер-ВС 6 скачен файл и лицензия:
https://disk.yandex.com.am/d/yHA2DFrphWd_fQ

Далее мы переходим на ОС Astra linux 1.7 и начинаем установку.

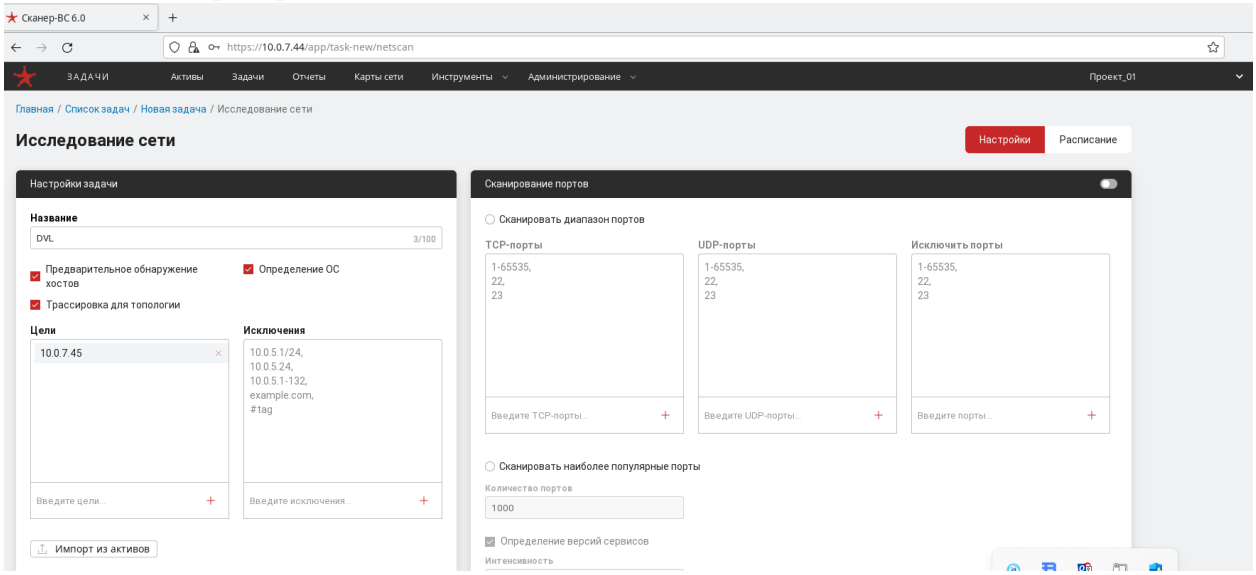


Установка прошла успешно.

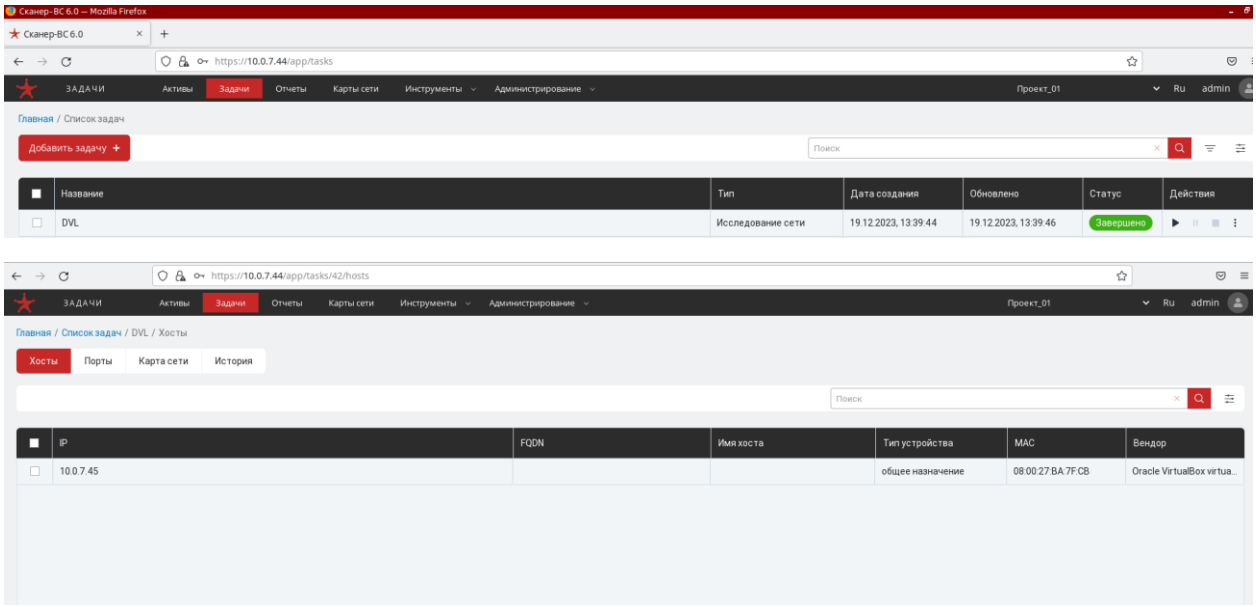
Перейдем в веб-интерфейс логин и пароль по умолчанию: admin admin



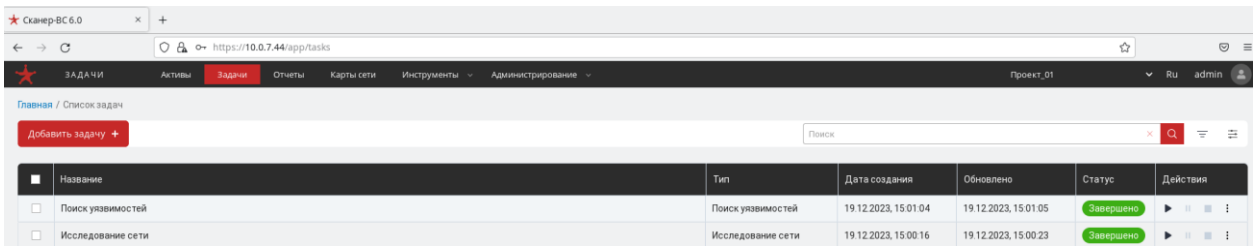
Мы попали на наш веб интерфейс, приступим к исследованию сети, записываем ip адрес ОС DVL



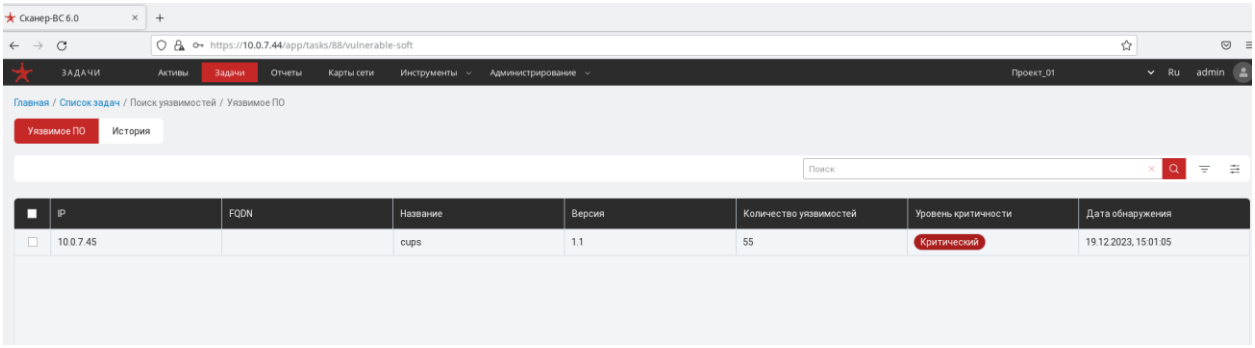
Задача создана и выполнена успешно



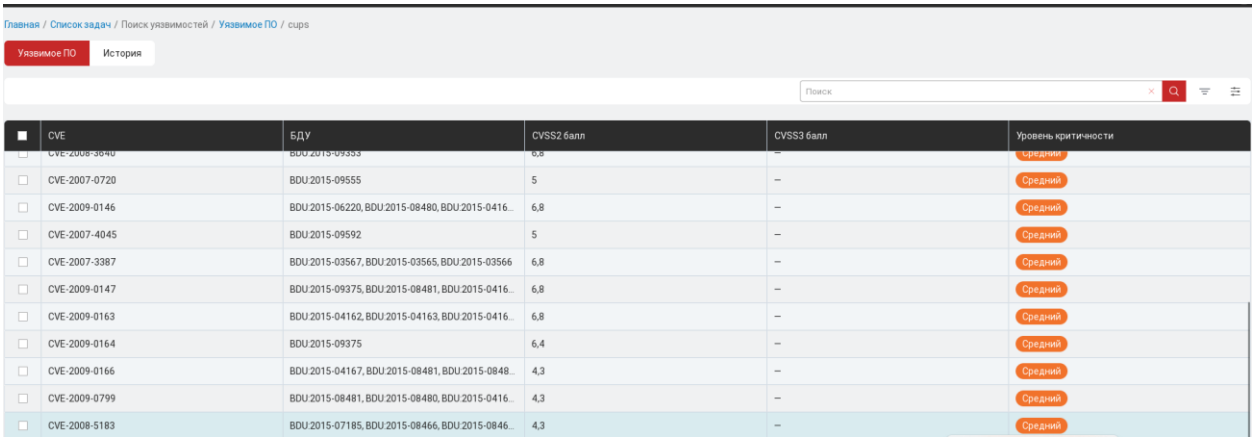
Приступим к поиску уязвимостей, для этого используем задачу исследования сети, подбираем нужно конфигурации поиска уязвимостей.



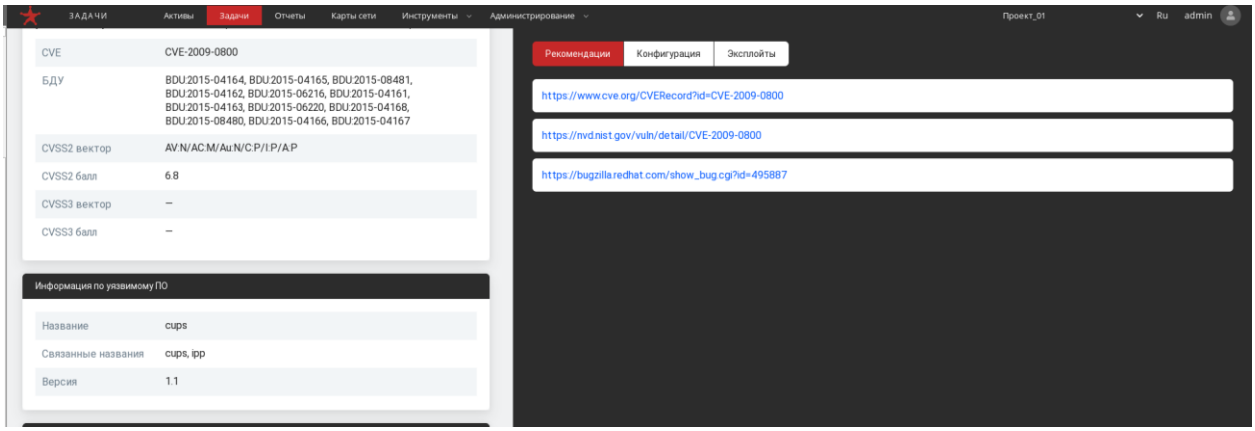
Задача выполнена успешно, посмотрим, что выводит данный сканер.



Сразу виден критический уровень угроз. (около 40 угроз)

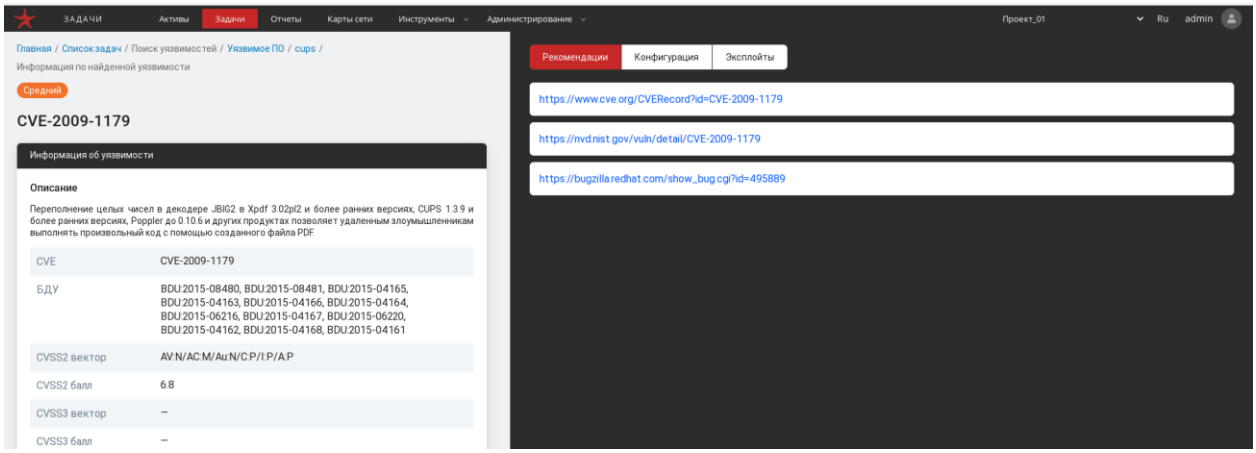


Для наглядности зайдем в несколько уязвимостей и посмотрим, что нам предлагает сканер.



Отображена CVE, БДУ ФСТЭК и балл критичности угрозы, нам также предложено рекомендации по устранению данной угрозы:

https://www.cve.org/CVERecord?id=CVE-2009-0800



Во второй угрозе нам также отображено описание, балл угрозы и рекомендации по устранению уязвимости:

https://nvd.nist.gov/vuln/detail/CVE-2009-1179

Сканирование Metasploit

С помощью программы Metasploit также можно совершать сканирование, пример такого сканирования. На дальнейших сриншотах можно увидеть работу (заранее было сделано статический маршрут)

Для проведения сканирования хоста на наличие и определение сервисов и какие там могут быть уязвимости необходимо использовать команду.

```
[-] Failed to load module: db_nmap
msf6 auxiliary(scanner/mysql/mysql_version) > db_nmap -sV -p 3306,631 192.168.31.143
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 13:28 EST
[*] Nmap: Nmap scan report for 192.168.31.143
[*] Nmap: Host is up (0.00s latency).
[*] Nmap: PORT     STATE SERVICE VERSION
[*] Nmap: 631/tcp  open  ipp     CUPS 1.1
[*] Nmap: 3306/tcp open  mysql   MySQL (unauthorized)
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

```
msf6 auxiliary(scanner/mysql/mysql_version) > db_nmap -sV -A -p 3306,631 192.168.31.143
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 13:29 EST
[*] Nmap: Nmap scan report for 192.168.31.143
[*] Nmap: Host is up (0.00s latency).
[*] Nmap: PORT     STATE SERVICE VERSION
[*] Nmap: 631/tcp  open  ipp     CUPS 1.1
[*] Nmap: |_http-title: 403 Forbidden
[*] Nmap: |_http-server-header: CUPS/1.1
[*] Nmap: | http-methods:
[*] Nmap: |_  Potentially risky methods: PUT
[*] Nmap: 3306/tcp open  mysql   MySQL (unauthorized)
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 6.46 seconds
```