



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.

```
=====
Welcome to Damn Vulnerable Linux Strychnine
Never run this distribution in any production environment!
IITAC is not responsible for any losses of any kind!
Commercial usage needs a specific license!
=====

The system is up and running now.

Login as "root", with password "toor", both without quotes, lowercase.

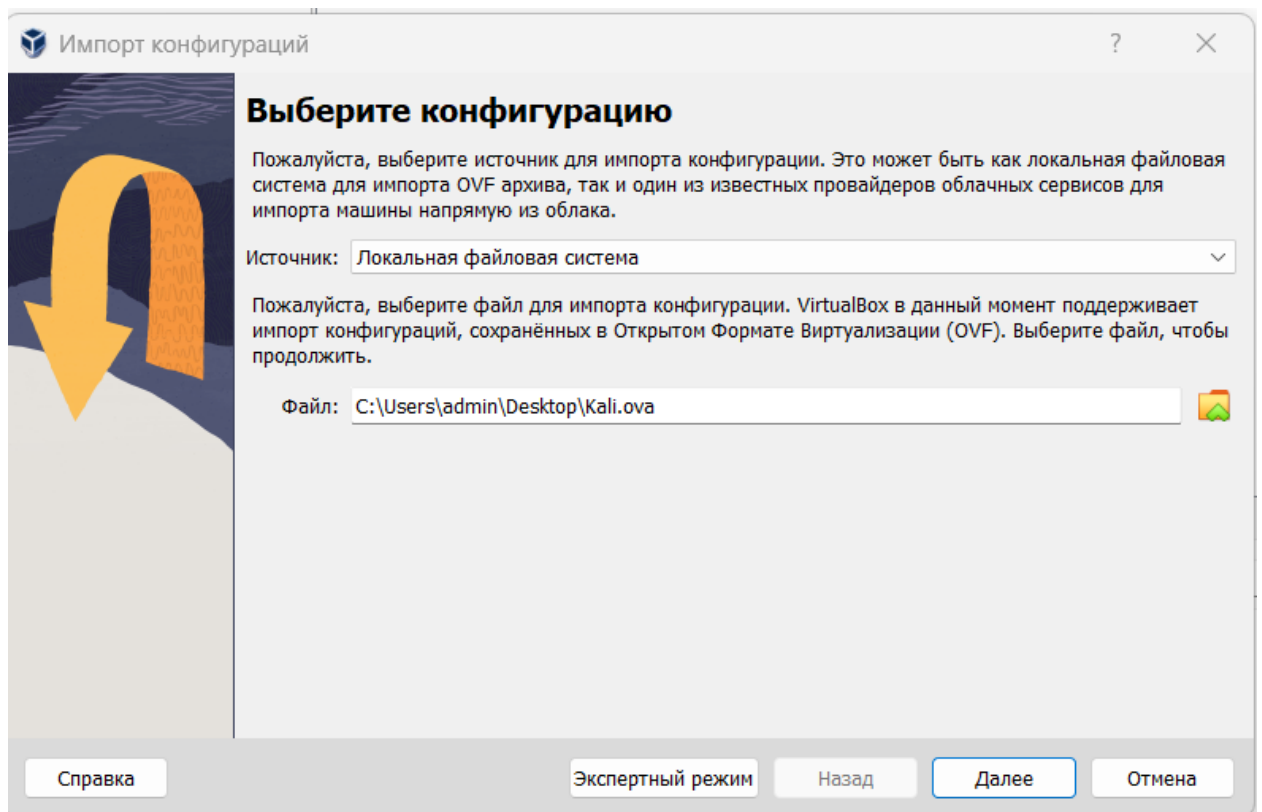
After you login, try the following commands:

startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)
flux .... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)
xconf ... to autoconfigure your graphics card for better performance
ati .... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only!):

configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk

When finished, use "poweroff" or "reboot" command and wait until it completes
=====
This distro is based on BackTrack 2.0 Final
=====
bt login:
```

После успешной установки ОС, приступим к установке 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 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP 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 https://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 анализа защищенности Сканер-ВС.

https://disk.yandex.com/am/d/yHA2DFrphWd_fQ

```
scanl@astra:~$ cd Desktop  
scanl@astra:~/Desktop$ cd Сканер-BC\ 6\ trueal/  
scanl@astra:~/Desktop/Сканер-BC 6 trueal$ cd pkg/  
scanl@astra:~/Desktop/Сканер-BC 6 trueal/pkg$ ./installer install  
=== Установка Сканер BC ===  
  
-----  
---- / / | _ | | \ | | / ___| | _ | | / \ | | | | | ____|  
_ \ / / | | | | \ | | \__ \ | | / _ \ | | | | | _|  
|_) | / / | | | | \ | | ___) | | | / __ \ | | | | |___  
_ < / / | | | | \ | | ___) | | | / __ \ | | | | |___  
( ) /_/ |_____| | | \ | | _____/ | | /_/ \_\ |_____||_____  
|_ | \_\  
./installer
```

```
GitVersion:  
GitCommit: c293e7b90ee0924ef97f229a70fd263481db6e03  
BuildDate: 2023-10-03~10:31:22  
GoVersion: go1.20.6  
Compiler: gc  
Platform: linux/amd64
```

```
E: Не удалось открыть файл блокировки /var/lib/dpkg/lock-frontent - open (13  
E: Отказано в доступе)  
E: Невозможно получить блокировку внешнего интерфейса dpkg (/var/lib/dpkg/lo  
ck-frontent); у вас есть права суперпользователя?  
Astra Linux 1.7 x86-64  
astra-1.7
```

Установка прошла успешно.

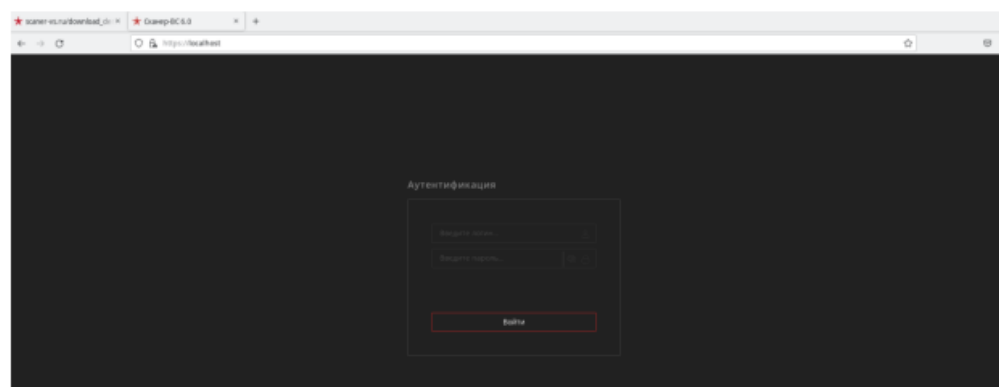
```
Конфигурации успешно изменены.
=====
ЗАВЕРШЕН этап: установка основного пакета сканера
=====

НАЧИНАЕТСЯ этап: установка данных Базы данных сканера
=====
ожидание применения миграций postgres
Восстановление данных vulndb. Это займет некоторое время.
Ok
Восстановление данных scanner-asset.
Ok
Обновление views
=====
ЗАВЕРШЕН этап: установка данных Базы данных сканера
=====

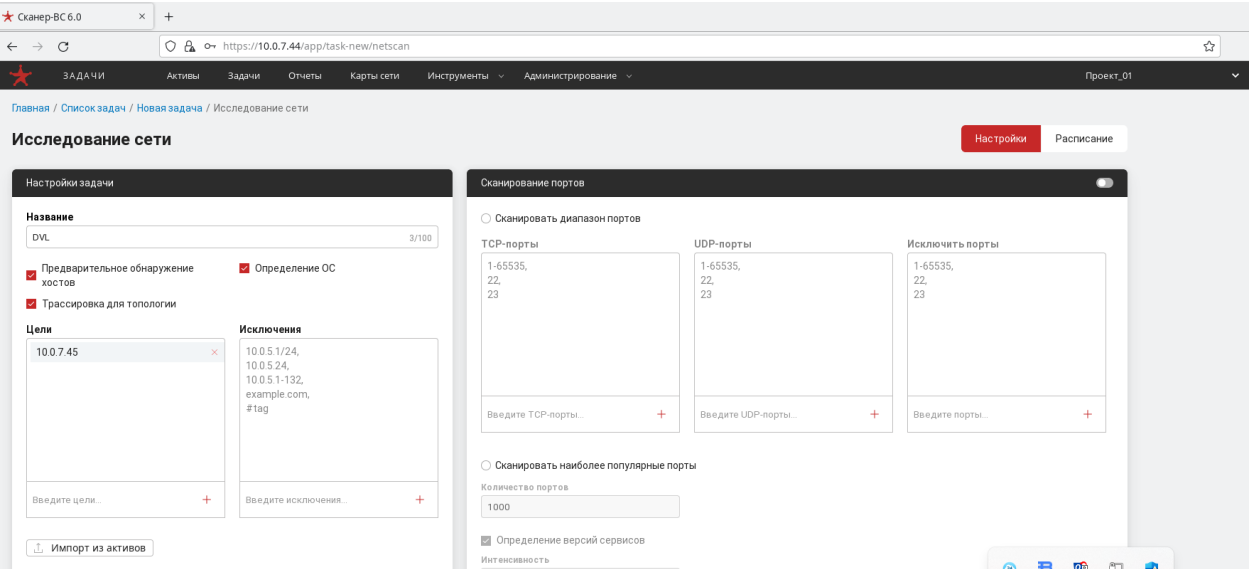
.d0000b .d0000b 0000b. 00000b. 00000b. .d00b. 000d000
00K d00P" "00b 000 "00b 000 "00b d0P Y0b 000P"
"Y0000b 000 .d000000 000 000 000 000 000X000 000
X00 Y00b. 000 000 000 000 000 000 Y0b. 000
00000P" "Y0000P "Y000000 000 000 000 000 "Y0000 000

=== Установка завершена ===
root@astra:/hone/scan1/Desktop/Сканер-BC 6 trial/pkg#
```

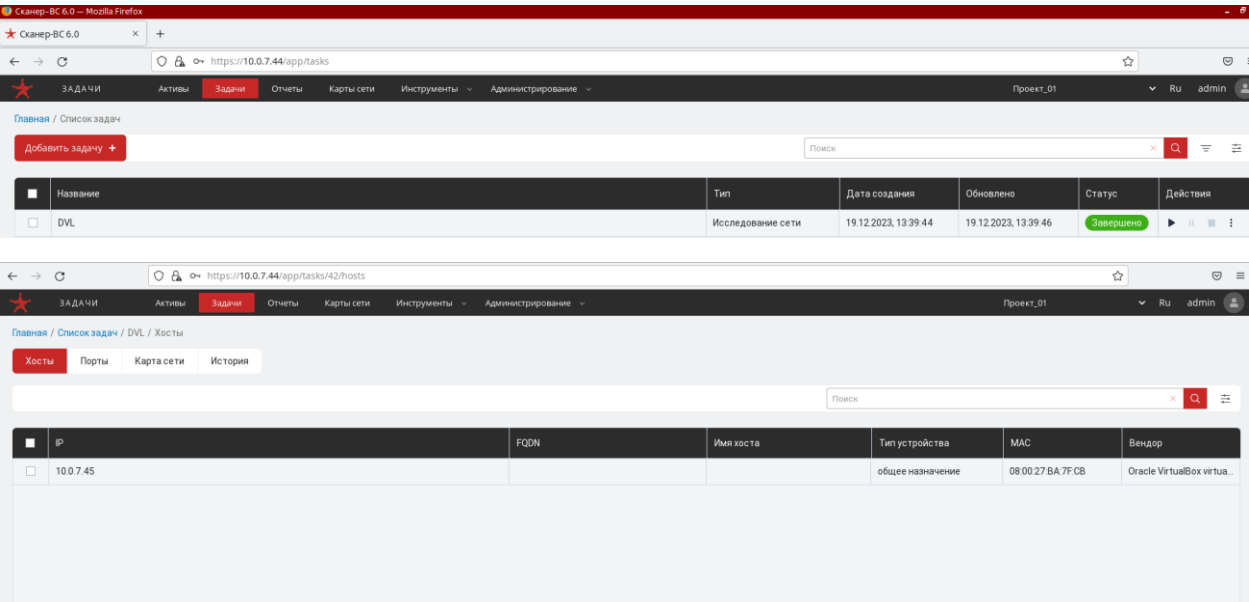
Перейдем в веб-интерфейс логин и пароль по умолчанию: admin admin



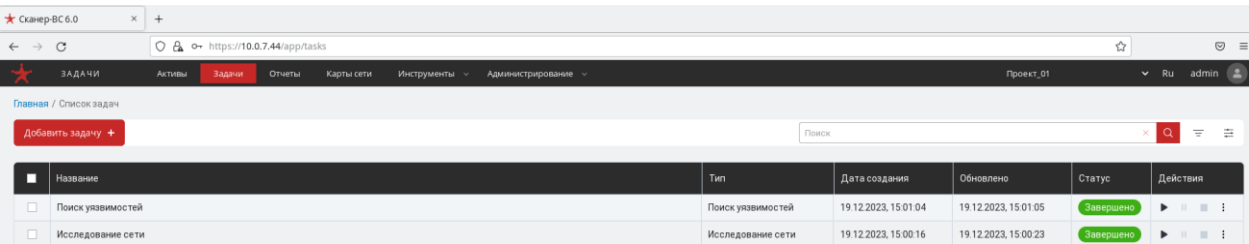
Мы попали на наш веб интерфейс, приступим к исследованию сети, записываем ip адрес ОС DVL



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.

	IP	FQDN	Название	Версия	Количество уязвимостей	Уровень критичности	Дата обнаружения
<input type="checkbox"/>	10.0.7.45		cups	1.1	55	Критический	19.12.2023, 15:01:05

Сразу виден критический уровень угроз. (около 40 угроз)

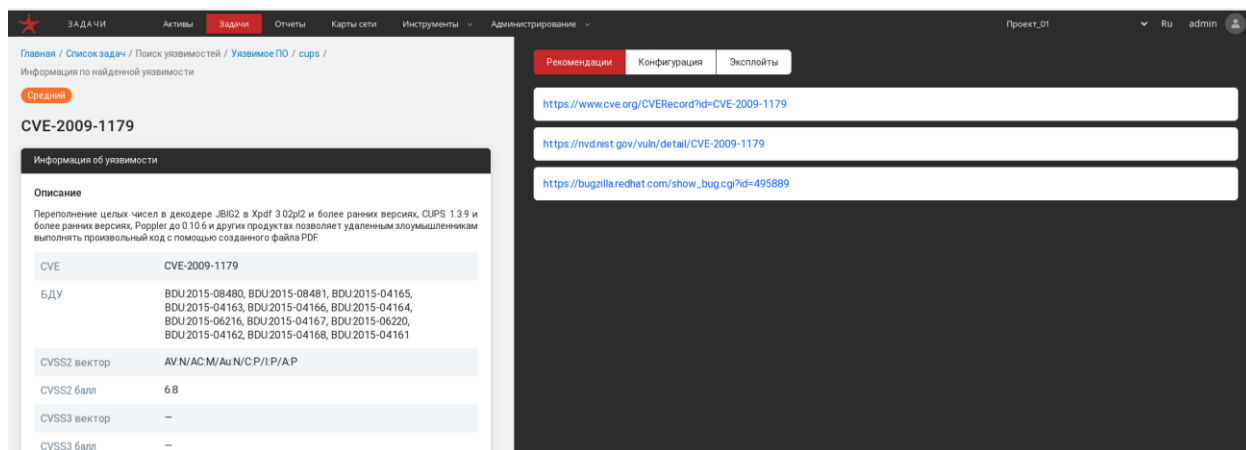
	CVE	БДУ	CVSS2 балл	CVSS3 балл	Уровень критичности
<input type="checkbox"/>	CVE-2008-3940	BDU 2015-09353	9.9	—	Средний
<input type="checkbox"/>	CVE-2007-0720	BDU 2015-09555	5	—	Средний
<input type="checkbox"/>	CVE-2009-0146	BDU 2015-06220, BDU 2015-08480, BDU 2015-0416...	6.8	—	Средний
<input type="checkbox"/>	CVE-2007-4045	BDU 2015-09592	5	—	Средний
<input type="checkbox"/>	CVE-2007-3387	BDU 2015-03567, BDU 2015-03565, BDU 2015-03566	6.8	—	Средний
<input type="checkbox"/>	CVE-2009-0147	BDU 2015-09375, BDU 2015-08481, BDU 2015-0416...	6.8	—	Средний
<input type="checkbox"/>	CVE-2009-0163	BDU 2015-04162, BDU 2015-04163, BDU 2015-0416...	6.8	—	Средний
<input type="checkbox"/>	CVE-2009-0164	BDU 2015-09375	6.4	—	Средний
<input type="checkbox"/>	CVE-2009-0166	BDU 2015-04167, BDU 2015-08481, BDU 2015-0848...	4.3	—	Средний
<input type="checkbox"/>	CVE-2009-0799	BDU 2015-08481, BDU 2015-08480, BDU 2015-0416...	4.3	—	Средний
<input type="checkbox"/>	CVE-2008-5183	BDU 2015-07185, BDU 2015-08466, BDU 2015-0846...	4.3	—	Средний

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

Рекомендации	Конфигурация	Эксплойты
https://www.cve.org/CVERecord?id=CVE-2009-0800		
https://nvd.nist.gov/vuln/detail/CVE-2009-0800		
https://bugzilla.redhat.com/show_bug.cgi?id=495887		

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 скриншотах 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
```