**Фахрутдинов Булат Загфярович**

**11-902**

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

**Цели и задачи:** научиться получать доступ к root атакуемого устройства

**Ход работ:**

1. Был скачан образ OC Kali Linux с разрешением «.iso» и установлен на виртуальную машину VMWare
2. Были проверены технические характеристики виртуальной машины: архитектура процессора – х64, количество процессоров – 1, объем ОЗУ – 512 MB, размер жесткого диска – 16 GB, тип сетевого подключения – сетевой мост.
3. Был выполнен вход в систему и запрос ip-адреса
   1. Выполнена команда “ip a” для просмотра адреса виртуальной ОС в сети. Адрес был локальным, поэтому было необходимо получить DHCP адрес, для связи с хостовым ПК
      1. Выполнена команда “dhclient” – для получения публичного адреса
   2. Адрес был записан для дальнейшей работы с хостовым ПК
4. Запуск nmap
   1. Выполнил команду “ nmap -p 1-65535 -T4 -A –v MS\_IP 2>&1 | tee /var/tmp/scan.txt”
   2. Убедился в том, что все успешно запущено
5. Определение портов rpcinfo, nfs и ssh
   1. Выполнил команду egrep –i ‘(rpcinfo|nfs|ssh)’ /var/tmp/scan.txt и нашел порт 2049
6. Оценка NFS сервера
   1. Установил все параметры по инструкции и выполнил ‘explot’
   2. Подключился к удаленной машине и выполнил whoami – получил
7. Открытие NETCAT сессии
   1. Выполнил «rpcinfo –p 192.168.244.129»
   2. Определил состояние NFS сервиса на машине жертвы
8. Сгенерировал SSH ключи (пункт 1.4.1), после чего смонтировал файловую систему и изменил authorized\_keys. Выполнил подключение по SSH
9. Сбор статистики
   1. Выполнил команды: showmount -a для просмотра статистики
   2. Командой sudo umount -a -t nfs размонтировал систему