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

**Касаткин Александр Денисович  
11-902**

**Запуск эксплоита distcc используя Metasploit**

1. Сканируем открытые порты с помощью NMAP
2. Открываем консоль Metasploit и выполняем:  
    use exploit/unix/misc/distcc\_exec
3. Настраиваем эксплоит

В нашем случае это cmd/unix/bind\_ruby и 192.168.109.134

1. Выполняем exploit

Теперь получили доступ к консоли

**Получение доступа к Metasploitable.**

1. Прослушиваем порт 4444 в новой консоли командой

netcat -vlp 4444

1. Скачиваем эксплоит
2. Компилируем эксплоит командой

gcc exploit-8572.c -o exploit-8572

1. Создадим скрипт для предоставления консоли по netcat

**Форезинка**

1. Выявление аномальной активности. Привязываем сетевые подключения к идентификаторам процессов.

netstat –noap | less;

192.168.109.132, использующие порт 4444

SH\_PID 5501

RUBY\_PID 5467

1. ps -eaf | grep RUBY\_PID | grep -v grep;

RUBY\_PID выполняет скрипт

## ps -eaf | grep SH\_PID | grep -v grep

## найдем P\_SH\_PID – pid родительского процесса SH\_PID

ps -eaf | grep P\_SH\_PID | grep -v grep

1. lsof –p RUBY\_PID

От Metasploitable до Kali Linux.

lsof –p SH\_PID;

root, идущие от Metasploitable до Kali Linux

## cat /tmp/run

## Клиент netcat подключился к серверу 192.168.109.132:4444 и предоставил ему /bin/sh

## **Создание дампа памяти с помощью LiME**

1. Подготовка директории.

## Создадим каталог /var/www/distcc командой mkdir –p /var/www/distcc

## Сменим владельца директории командой chown www-data:www-data /var/www/distcc

* 1. измените права доступа командой chmod 755 /var/www/distcc;

## Изменим права доступа командой chmod 755 /var/www/distcc

## Создадим дамп оперативной памяти Metasploitable c помощью команды insmod ./lime-2.6.24-16-server.ko "path=/var/www/distcc/distcc\_memory.lime format=lime"

## Сохраним  сведений о состоянии сетевых соединений и слушаемых на данном компьютере портах командой netstat -naop > /var/www/distcc/distcc\_netstat.txt

## Сохраним вывод информации о том, какие файлы используются теми или иными процессами в системе командой lsof > /var/www/distcc/distcc\_lsof.txt

1. Сохраним отчёт о работающих процессах командой ps -eaf > /var/www/distcc/distcc\_pseaf.txt

**Создание MD5 хеш-суммы.**

1. перейти в каталог /var/www/distcc/ командой cd /var/www/distcc/;
2. выполнить создание MD5 хеш-сумм командой md5sum \* | tee distcc\_md5.txt.

**Результаты:**

