**Студент: Ганиев Р.А.**

**Группа: 11-902**

**Тема: использование бекдора протокола unrealircd 3.2.8.1**

**Содержание**

1. Развернуть виртуальные машины Kali Linux и Metasploitable
2. Убедиться в корректной настройке сети между Metasploitable и Kali Linux
3. Атака на Metasploitable
4. Оформление результатов работы

**1. Развернуть виртуальные машины Kali Linux и Metasploitable**

Постановка задачи

* развёртывание виртуальных машины Kali Linux и Metasploitable
* цель: выполнить развёртывание виртуальных машин
* средства: WMWare Workstation

Начальная ситуация

* развёртывание виртуальных машин не выполнено

Выполнение задания

* алгоритм
  + выполнить развёртывание виртуальных машин Kali Linux и Metasploitable, подготовленных в рамках выполнения лабораторных работ
* результаты
  + выполнено развёртывание виртуальных машин Kali Linux и Metasploitable

**2. Убедиться в корректной настройке сети между Metasploitable и Kali Linux**

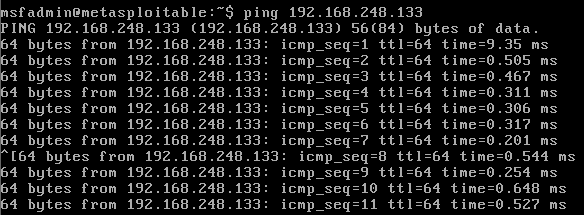
Постановка задачи

* проверка корректной настройки сети между Metasploitable и Kali Linux
* цель: убедиться в корректной настройке сети между Metasploitable и Kali Linux
* средства: ifconfig, ping

Начальная ситуация

* корректность настройки сети не проверена

Выполнение задания

* алгоритм
  + последовательное определение IP адресов машин, выданный DHCP-сервером, для Kali Linux и для Metasploitable (ifconfig | grep “inet addr”)
  + запись полученных IP-адресов как MS\_IP и KL\_IP (IP-адреса должны быть из одной подсети)
  + проверка корректности соединения: ping
* результаты
  + 
  + сеть между Metasploitable и Kali Linux настроена корректно

**3. Атака на Metasploitable**

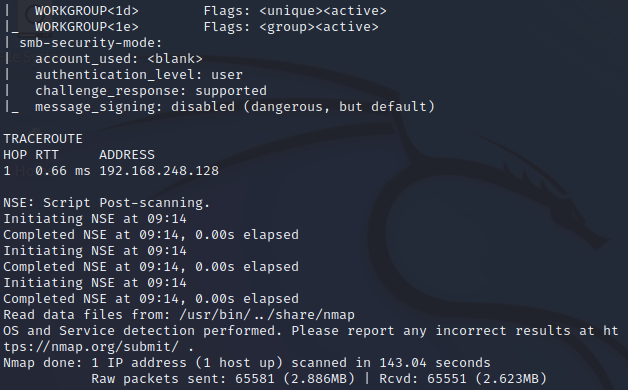
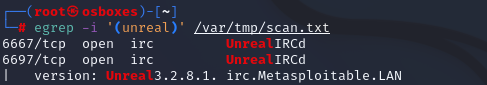
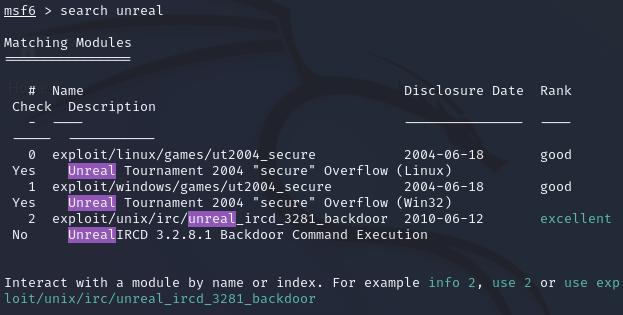
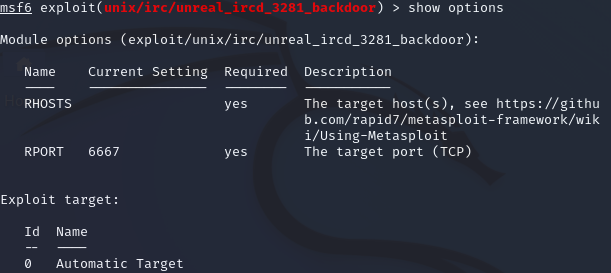
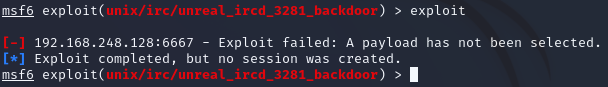
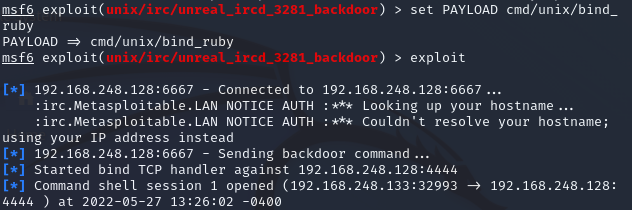
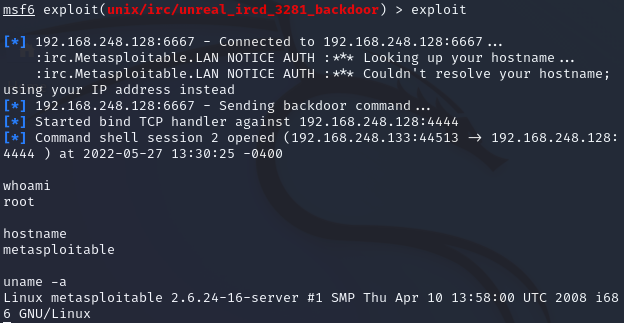
Постановка задачи

* атака на Metasploitable
* цель: произвести атаку на Metasploitable с использование уязвимости UnrealIRCD
* средства: nmap, grep, use, set, exploit

Начальная ситуация

* атака на Metasploitable с использование уязвимости UnrealIRCD не произведена

Выполнение задания

* алгоритм
  + сканирование портов Metasploitable на виртуальной машине Kali Linux (атакующая машина)
    - сканирование виртуальной машины Metasploitable (машина-жертва): nmap -p 1-65535 -T4 -A -v MS\_IP 2>&1 | tee /var/tmp/scan.txt
    - сохранение результата сканирования в файл /var/tmp/scan.txt
    - определение порта (портов), которые используются пакетом unreal, и их статуса, при помощи анализа файла, подготовленного на предыдущем шаге, с помощью команды grep
  + активация эксплоита для использования уязвимости UnrealIRCD
    - запуск консоли msfconsole в терминале атакующей машины
    - вывод списка эксплоитов по использованию уязвимостей пакета unreal, имеющихся во фреймворке metasploit: search unreal
    - запуск эксплоита: use exploit/unix/irc/unreal\_ircd\_3281\_backdoor
    - вывод списка доступных опций для эксплоита: show options
    - установка значения параметров следующим образом: set RHOST MS\_IP
    - активация эксплоита: exploit
    - проверка успешности атаки при помощи определения имени хоста (имя машины-жертвы), информации о ядре операционной системы, о системном пользователе, от чьего имени осуществлено соединение с системой
* результаты
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + произведена атака на Metasploitable с использование уязвимости UnrealIRCD

**4. Оформление результатов работы**

