САНКТ-ПЕТЕРБУРГСИЙ ГОСУДАРСТВЕННЫЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра Компьютерных Систем и Программных Технологий

ОТЧЕТ

по лабораторной работе №5
Тема: «Инструмент тестов на проникновение Metaspoit»
Дисциплина: «Методы и средства защиты информации»

Выполнил: студент гр. 53501/2
Пономарев М.А.

Преподаватель
Вылегжанина К.Д.

Санкт-Петербург
2015

Содержание

1 Задание

а) Подключиться к VNC-серверу, получить доступ к консоли

б) Получить список директорий в общем доступе по протоколу SMB

в) Получить консоль используя уязвимость в vsftpd

г) Получить консоль используя уязвимость в irc

д) Armitage Hail Mary

е) Изучить три файла с исходным кодом эксплойтов или служебных скриптов на ruby и описать, что в них происходит

2 Выполнение

2.1 Подключиться к VNC-серверу, получить доступ к консоли

2.2 Получить список директорий в общем доступе по протоколу SMB

2.3 Получить консоль используя уязвимость в vsftpd

2.4 Получить консоль используя уязвимость в irc

2.5 Armitage Hail Mary

2.6 Изучить три файла с исходным кодом эксплойтов или служебных скриптов на ruby и описать, что в них происходит