МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра телекоммуникаций и информационных технологий

Аннотация к дипломной работе

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯ

ДУДИНСКИЙ Даниил Александрович

Научный руководитель – старший преподаватель,
Е.Е. Попко

Минск, 2025

РЕФЕРАТ

Дипломная работа: 62 с., 26 рис., 13 источников

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯ

Цель работы – исследование методов использования уязвимостей операционных систем для повышения привилегий пользователя, анализ реальных случаев эксплуатации таких уязвимостей и разработка виртуальной лаборатории, представляющей интерфейс для изучения и демонстрации типовых сценариев атак.

В ходе работы проанализированы техники повышения привилегий, рассмотрено для каких платформ и как эти техники могут быть использованы. Построена карта возможных под-техник повышения привилегий в Linux. Сформулирован сценарий поиска уязвимостей информации о системе.

В практической части была создана виртуальная лаборатория, состоящая из трех виртуальных машин. Каждая из машин выполняет свою роль. Первая машину предоставляет возможность пользователю, собрав информацию о системе, обнаружить следы атаки с повышением привилегий. Вторая машина представляет собой еще не взломанную, но уязвимую систему (уязвимости созданы в ходе выполнения дипломной работы). Что позволяет пользователю, используя сформулированный сценарий поиска информации о системе, найти и устранить созданные уязвимости. Третья машина на данный момент уязвимостями, которые могут эксплуатироваться.

Сформулированный сценарий и созданная виртуальная лаборатория могут быть использованы в качестве учебного материала для будущих специалистов по безопасности.

РЭФЕРАТ

Дыпломная праца: 62 с., 26 мал., 13 крыніц

ВЫКАРЫСТАННЕ УРАНЛІВАСЦЯЎ АПЕРАЦЫЙНЫХ СІСТЭМ ДЛЯ ПАВЫШЭННЯ ПРЫВІЛЕЯЎ КАРЫСТАЛЬНІКА

Мэта працы – даследаванне метадаў выкарыстання ўразлівасцяў аперацыйных сістэм для павышэння прывілеяў карыстальніка, аналіз рэальных выпадкаў эксплуатацыі такіх уразлівасцяў і распрацоўка віртуальнай лабараторыі, якая прадстаўляе інтэрфейс для вывучэння і дэманстрацыі тыпавых сцэнарыяў атак.

У ходзе працы прааналізаваны тэхнікі павышэння прывілеяў, разгледжана, для якіх платформ і як гэтыя тэхнікі могуць быць выкарыстаны. Пабудавана карта магчымых падтэхнік павышэння прывілеяў у Linux. Сфармуляваны сцэнар пошуку ўразлівасцяў і інфармацыі пра сістэму.

У практычнай частцы была створана віртуальная лабараторыя, якая складаецца з трох віртуальных машын. Кожная з машын выконвае сваю ролю. Першая машына дае магчымасць карыстальніку, сабраўшы інфармацыю пра сістэму, выявіць сляды атакі з павышэннем прывілеяў. Другая машына ўяўляе сабой яшчэ не ўзламаную, але ўразлівую сістэму (уразлівасці створаны ў ходзе выканання дыпломнай працы), што дазваляе карыстальніку, выкарыстоўваючы сфармуляваны сцэнар пошуку інфармацыі пра сістэму, знайсці і ліквідаваць створаныя ўразлівасці. Трэцяя машына на дадзены момант мае ўразлівасці, якія могуць быць эксплуатаваныя.Сфармуляваны сцэнар і створаная віртуальная лабараторыя могуць быць выкарыстаныя ў якасці навучальнага матэрыялу для будучых спецыялістаў па бяспецы.

ABSTRACT

Thesis: 62 p., 26 fig., 13 sources

EXPLOITING OPERATING SYSTEM VULNERABILITIES TO ENHANCE USER PRIVILEGES

The purpose of the work is to study methods of exploiting operating system vulnerabilities to increase user privileges, analyze real–world cases of exploiting such vulnerabilities, and develop a virtual laboratory that provides an interface for studying and demonstrating typical attack scenarios.

In the course of the work, privilege enhancement techniques are analyzed, which platforms are considered and how these techniques can be used. A map of possible privilege escalation techniques in Linux has been built. A scenario for finding vulnerabilities in information about the system is formulated.

In the practical part, a virtual laboratory was created, consisting of three virtual machines. Each of the machines performs its own role. The first machine provides an opportunity for the user, having collected information about the system, to detect traces of a privilege escalation attack. The second machine is not yet hacked, but a vulnerable system (vulnerabilities were created during the completion of the thesis). This allows the user, using a formulated scenario for searching information about the system, to find and eliminate the created vulnerabilities. The third machine currently has vulnerabilities that can be exploited.

The formulated scenario and the created virtual laboratory can be used as educational material for future security specialists.