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

КОВАЛЁВ Денис Сергеевич

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ СЕТЕЙ ОТ ПОДМЕНЫ ИНФОРМАЦИИ В ARP-ТАБЛИЦЕ

Аннотация к дипломной работе

Научный руководитель – старший преподаватель
Е.Е. Попко

Минск, 2024

РЕФЕРАТ

Дипломная работа: 44 с., 40 рис., 20 источников

МЕТОДЫ ЗАЩИТЫ, ARP-СПУФИНГ, DNS-СПУФИНГ, ВИРТУАЛЬНАЯ ЛАБОРАТОРИЯ, ИНСТРУМЕНТЫ ДЛЯ АНАЛИЗА

Целью исследования является создание виртуальной лаборатории для изучения атак типа человек посередине, изучения способов защиты и анализа трафика. В ходе исследования проведен подробный анализ сущности атаки человек посередине. Проанализированы способы выявления уязвимостей. Описаны инструменты для перехвата и анализа трафика в компьютерной сети. Реализованы сценарии атак ARP-спуфинг и DNS-спуфинг. Описаны инструменты и методы защиты от данных атак.

РЭФЕРАТ

Дыпломная праца: 44 с., 40 мал., 20 крыніц

МЕТАДЫ АБАРОНЫ, ARP-СПУФІНГ, DNS-СПУФІНГ, ВІРТУАЛЬНАЯ ЛАБАРАТОРЫЯ, ІНСТРУМЕНТЫ ДЛЯ АНАЛІЗУ

Мэтай даследавання з'яўляецца стварэнне віртуальнай лабараторыі для вывучэння нападаў тыпу чалавек пасярэдзіне, вывучэння спосабаў абароны і аналізу трафіку. У ходзе даследавання праведзены падрабязны аналіз сутнасці нападу чалавек пасярэдзіне. Прааналізаваны спосабы выяўлення ўразлівасцяў. Апісаны прылады для перахопу і аналізу трафіку ў кампутарнай сетцы. Рэалізаваны сцэнары нападаў ARP-спуфінг і DNS-спуфінг. Апісаны прылады і метады абароны ад дадзеных нападаў.

ABSTRACT

Thesis: 44 pag., 40 draw., 20 sources

PROTECTION METHODS, ARP SPOOOING, DNS SPOOOING, VIRTUAL LABORATORY, ANALYSIS TOOLS

The goal of the research is to create a virtual laboratory to study man-in-the-middle attacks, study defense methods, and analyze traffic. The study conducted a detailed analysis of the essence of a man-in-the-middle attack. Methods for identifying vulnerabilities are analyzed. Tools for intercepting and analyzing traffic on a computer network are described. ARP spoofing and DNS spoofing attack scenarios have been implemented. Tools and methods of protection against these attacks are described.