Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0411U002567

Особливі позначки: відкрита

Дата реєстрації: 31-05-2011

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Тимошик Назар Петрович
2. Tymoshyk Nazar Petrovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 29-04-2011

Спеціальність за освітою: 7.160102

Місце роботи здобувача: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: 79013, Україна, м.Львів, вул. С.Бандери, 12

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 35.052.08

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. С. Бандери, 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: 79013, Україна, м.Львів, вул. С.Бандери, 12

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.39.17

Тема дисертації:

1. Вдосконалення принципів побудови та функціонування приманок в задачах захисту комп'ютерних систем та мереж

2. Improving the principles of construction of honeypot systems for protection of computer systems and networks

Реферат/анотація:

1. Дисертація присвячена питанням вдосконалення повно-інтерактивних приманок із забезпеченням стійкої до виявлення та блокування зловмисником систем реєстрації подій та знімання інформації з каналів взаємодії зловмисника та приманки. Розроблено нові підходи до розв'язання поставлених задач на основі бінарної реконструкції команд віртуального процесора на гіпервізорі Qemu. Досліджено та розроблено нові методи реєстрації та моніторингу зламу комп'ютерних систем. Розроблено математичну модель та підсистему протидії атакам на доступність та функціональність приманок. Запропоновані та розроблені методи дозволили програмно реалізувати систему захисту та моніторингу приманок під назвою "Система збору інформації та аналізу приманок" (СЗІАП). Розроблено поведінкову модель взаємодії між зловмисником та приманкою яка дозволила обирати параметри моніторингу подій у приманці.

2. The dissertation is devoted to research on improving the height interactive honeypots with providing proof to identify and block registration and event monitoring systems by malicious. New approaches to solve that problem

based on the virtualization approach and binary reconstruction of system calls passed thought virtual processor. Researched and developed new methods of registration and monitoring of fracture of computer systems, algorithms and mathematical model subsystem against attacks on the availability and functionality of honeypots. Proposed and developed methods have allowed the program to realize system protection and monitoring honeypots called "System of information gathering and analysis of Honeypots (SoIGAH). A behavioural model of interaction between the attacker and the honeypot is allowed to choose options for monitoring events in the honeypot. Based on this method was possible to identify and introduce ways of access attempts, allowing us to automate analysing attacks. By using equivalent parameters (as in Sebek v.3) our system show lower workload at monitoring system that confirms the efficacy, which made gains in productivity by 15%.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Піскозуб Андріан Збігневич
2. Piskozub Andrian Zbihnievych

Кваліфікація: к.т.н., 05.13.08

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Русин Богдан Павлович

2. Русин Богдан Павлович

Кваліфікація: д.т.н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Браіловський Микола Миколайович

2. Браіловський Микола Миколайович

Кваліфікація: к.т.н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Яремчук Юрій Євгенович

2. Яремчук Юрій Євгенович

Кваліфікація: к.т.н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Стадник Богдан іванович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Стадник Богдан іванович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.