Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи бакалавра *Розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на IMAP сервер*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Development, Integration, and Evaluation of the Effectiveness of Protection Against Slow and Fast Brute-Force Attacks on an IMAP Server*
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 41
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 27 грудня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 58

УДК: 004.42

Автор роботи
Прізвище, ім'я, по батькові (укр.): Бекер Іван Миколайович
розкривати ініціали

Прізвище, ім'я (англ.): Beker Ivan
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м. Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Загородна Наталія Володимирівна
повністю

Прізвище, ім'я (англ.): Zagorodna Nataliya
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки Тернопіль, Україна
Вчене звання, науковий ступінь, посада: : к.т.н., доцент, завідувач кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Никитюк Вячеслав Вячеславович
повністю

Прізвище, ім'я (англ.): Nikityuk Vyacheslav
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: к. т. н., доцент, заступник завідувача кафедри комп'ютерних наук

Ключові слова
українською: FreeBSD, IMAP, PF, brute-force, bash, dovecot
до 10 слів

англійською: FreeBSD, IMAP, PF, brute-force, bash, dovecot

до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена дослідженню методів захисту IMAP сервера від brute-force атак. Було проведено аналіз повільних та швидких brute-force атак та методів їх виявлення. Розроблено та застосовано політику паролів для збільшення безпеки облікових записів користувачів. Розроблено та реалізовано методику захисту від швидких brute-force атак за допомогою PF в операційній системі FreeBSD.

Також у результаті дослідження було розроблено програмний модуль для аналізу лог-файлів IMAP сервера Dovecot з метою виявлення та блокування повільних brute-force атак за допомогою PF. Було розроблено та налаштовано систему автоматичного сповіщення адміністратора про інциденти безпеки через корпоративний Jabber.

Отримані результати підтвердили, що розроблений захист працює коректно та успішно блокує спроби атак в реальному часі. Реалізація заходів захисту та автоматичного інформування адміністратора дозволяє оперативно реагувати на потенційні загрози.

англійською:

The qualification work is devoted to the study of methods for protecting an IMAP server from brute-force attacks. An analysis of slow and fast brute-force attacks and methods for their detection was carried out. Developed and implemented a password policy to increase the security of user accounts. A method of protecting against fast brute-force attacks using PF in the FreeBSD operating system has been developed and implemented.

Also, as a result of the research, a software module was developed for analyzing Dovecot server IMAP log files in order to detect and block slow attacks using PF. A system for automatically notifying the administrator about security incidents via corporate Jabber was developed and configured.

The results obtained confirmed that the developed protection works correctly and successfully blocks attack attempts in real time. The implementation of protection measures and automatic notification of the administrator allows you to quickly respond to potential threats.

Бібліографічний опис:

Бекер І.В. Розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на IMAP сервер: кваліфікаційна робота магістра за спеціальністю 125 — Кібербезпека / Бекер Іван Миколайович . – Тернопіль : ТНТУ, 2023. – С. 66