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

Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра Захист операційної системи Windows від brute-force атак
назви записувати нижнім регістром (як у реченні)

Назва (англ.): Windows operating system protection against brute-force attacks
переклад англійською

Освітній ступінь : бакалавр

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

Екзаменаційна комісія: Екзаменаційна комісія № 40
напр.: Екзаменаційна комісія №1

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

Дата захисту: 22 червня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 58

УДК: 004.56

Автор роботи
Прізвище, ім'я, по батькові (укр.): Ворона Максим Сергійович
розкривати ініціали

Прізвище, ім'я (англ.): Vorona Maksym
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.): Лечаченко Тарас Анатолійович
повністю

Прізвище, ім'я (англ.): Lechachenko Taras
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна
Вчене звання, науковий ступінь, посада: PhD доктор філософії, асистент кафедри КБ

Рецензент
Прізвище, ім'я, по батькові (укр.): Стадник Наталія Богданівна

Прізвище, ім'я (англ.): Nataliia Stadnyk

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. старший викладач кафедри КС

Ключові слова
українською: WINDOWS, RDP, FIREWALL, POWERSHELL, РОУТУР, BRUTE-FORCE,

NAT.

до 10 слів

англійською: WINDOWS, RDP, FIREWALL, POWERSHELL, РОУТУР, BRUTE-FORCE, NAT.

до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена дослідженню та захисту від brute-force атак на операційну систему Windows Server 2022. Атаки такого типу становлять серйозну загрозу для безпеки інформаційних систем, порушуючи конфіденційність та доступ до даних. У роботі розглянуті різні механізми та заходи безпеки для ефективного захисту. Аналізуються механізми політики паролів, блокування паролів після невдалих спроб та фільтрації трафіку через брандмауер. Для виявлення та блокування атак була розроблена система на базі PowerShell, яка аналізує журнал подій та автоматично блокує IP-адреси зловмисників через Windows Firewall. Моніторинг забезпечується планувальником завдань, що виконує сценарії при заданих умовах.

Розроблена система є універсальною та може бути застосована для виявлення та блокування brute-force атак на Windows Server. Результати роботи дозволять підвищити рівень безпеки операційної системи та забезпечити надійність інформаційних ресурсів. Розроблені методи можуть бути використані адміністраторами систем для покращення захисту серверів.

Кваліфікаційна робота також може бути використана в навчанні. Розроблені методи та сценарії є прикладами та практичними вправами для студентів, які вивчають безпеку операційних систем. Вона дозволяє ознайомитися з концепцією brute-force атак та навчитися захищати системи від таких загроз.

англійською:

The qualification work is devoted to the study and protection against brute-force attacks on the Windows Server 2022 operating system. Attacks of this type pose a serious threat to the security of information systems, violating confidentiality and access to data. The paper discusses various mechanisms and precautions for effective protection. The mechanisms of password policy, blocking passwords after unsuccessful attempts and filtering traffic through the firewall are analyzed. To detect and block attacks, a PowerShell-based system was developed that analyzes the event log and automatically blocks the IP addresses of intruders through Windows Firewall. Monitoring is provided by the task scheduler, which executes scripts under specified conditions.

The developed system is universal and applicable for detecting and blocking brute-force attacks on Windows Server. The results of the work will improve the security level of the operating system and ensure the reliability of information resources. The developed methods can be used by system administrators to improve server security.

Qualifying work can also be used in training. The developed methods and scenarios are examples and practical exercises for students who study the security of operating systems. It allows you to familiarize yourself with the concept of brute-force attacks and learn how to protect systems from such threats.

Бібліографічний опис:

Ворона М.С. Захист операційної системи Windows від brute-force атак: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / М. С. Ворона. – Тернопіль : ТНТУ, 2023. – 58 с.