Авторська довідка
(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Системи виявлення та запобігання проникненню на прикладі Wazuh*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Intrusion detection and intrusion prevention systems based on Wazuh*
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: 21 червня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 66

УДК:

Автор роботи
Прізвище, ім'я, по батькові (укр.): Поліщук Владислав Анатолійович
розкривати ініціали

Прізвище, ім'я (англ.): Polishchuk Vladyslav Anatoliyovych
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 Volodymyrivna
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Михалик Дмитро Михайлович
повністю

Прізвище, ім'я (англ.): Mykhalyk Dmytro
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: кандидат технічних наук, доцент. кафедри ПІ

Ключові слова:
українською: проникнення, вторгеннння, IDS, IPS, Wazuh, експлойт, моніторинг.
до 10 слів

англійською: intrusion, penetration, IDS, IPS, Wazuh, exploit, monitoring.
до 10 слів

Анотація

українською:

Кваліфікаційна роботи присвячена розгортанню системи моніторингу та її модифікації для потреб виявлення та запобігання проникненням.

Основою системи моніторингу обрана система Wazuh, яка здатна збирати дані за допомогою Wazuh Agent, обробляти їх на сервері (Wazuh Server) та відображати у веб-інтерфейсі. Інструмент також дозволяє налаштовувати умови спрацювання сповіщень та активних реакцій на події, цей функціонал було реалізовано та модифіковано шляхом імітації реальної атаки з ескалації привілеїв в системі та створення умов протидії таким загрозам.

Було розгорнуто локальний SMTP сервер, автентифікований через поштовий клієнт Gmail для надсилання листів-сповіщень про підозрілі події. Для системи активного реагування на загрози було розроблено власне правило, що забезпечує фіксує зміни конфігураційного файлу Wazuh Agent та передає цю подію для екстреного завершення роботи служби-агента з метою скидання внесених змін і, як наслідок, забезпечення цілісності файлу.

англійською:

Thesis is focused on deployment of the monitoring system and its modification for the needs of detection and prevention of intrusion.

The baseline tool of the monitoring system was chosen to be Wazuh, capable of collecting data using the Wazuh Agent, processing it on the server (Wazuh Server) and displaying it in the web interface. The tool also allows you to improve the conditions for triggering notifications and active responses to events. This functionality was implemented and modified by simulating a real attack with escalation of privileges in the system and creating conditions for countering such threats.

An on-premise SMTP server was deployed and authenticated through the Gmail mail client to reinforce suspicious event notification emails. For the system of active response to threats, a special rule was developed that ensures the capture of changes to the Wazuh Agent configuration file and transmits this event to the emergency termination of the agent service in order to reset the changes made and, as a result, ensuring the integrity of the file.

Бібліографічний опис:

Поліщук В. А. Системи виявлення та запобігання проникненню на прикладі Wazuh: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / В. А. Поліщук. – Тернопіль: ТНТУ, 2023. – 66 с.