Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та систем електронних комунікацій

«Допущено до захисту»
Начальник кафедри ІТтаСЕК
кандидат технічних наук,
доцент
_____Олександр ПРИДАТКО
“____” _____ 20___ року

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему **«Дослідження та розробка системи моніторингу та аналізу великих обсягів даних за допомогою платформи Elastic Stack»**

Виконав:
здобувач VI курсу, групи КНм61
спеціальності 122 «Комп’ютерні науки»
(шифр і назва спеціальності)
Купріков М.П.
(прізвище та ініціали)
Керівник Смотр О.О.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)

Львів – 2024 року

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та систем електронних комунікацій

Освітнього ступеня магістр
Спеціальність 122 “Комп’ютерні науки”

ЗАТВЕРДЖУЮ
Начальник кафедри ІТтаСЕК
кандидат технічних наук,
доцент
_____Олександр ПРИДАТКО
“____” _____ 20___ року

ЗАВДАННЯ
на кваліфікаційну роботу

Здобувачу Купрікову Микиті Павловичу
(прізвище, ім’я, по батькові)
1. Тема Дослідження та розробка системи моніторингу та аналізу великих обсягів даних за допомогою платформи Elastic Stack
керівник роботи Смотр О.О.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЛДУ БЖД від “__” _____ _____ року № _____
2. Термін подання здобувачем роботи _____
3. Початкові дані до роботи
1. Morgan S. Top 10 Cybersecurity Predictions and Statistics For 2023. Cybercrime Magazine. URL: https://cybersecurityventures.com/top-5- cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ (date of access: 16.06.2023).
2. Chuvakin A. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress, 2012. 460 p.
3. Kali Linux. Тестування на проникнення і безпеку / А. Замм та ін. ; ред. Н. Гринчик ; пер. з англ. А. Герасименко. 4-те вид. Packt Publishing, 2018. 528 с.
4. Зміст роботи/проекту (перелік питань, які потрібно розробити)
Вступ
Розділ 1. Теоретичні аспекти аналізу лог-файлів та системи ELK
Розділ 2. Аналіз загроз безпеки інформації
Розділ 3. Впровадження системи для аналізу лог-файлів з використанням ELK
Висновки
Список використаних джерел
Додатки

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

6. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання кваліфікаційної роботи/проекту	Термін виконання етапів роботи	Примітка
1.	Аналіз загроз безпеки інформації		
2.	Досліжження теоретичних аспектів аналізу лог-файлів та систем ELK		
3.	Впровадження системи для аналізу лог-файлів з використанням ELK		

Здобувач _____ Микита КУПРІКОВ
(підпис) (прізвище та ініціали)

Керівник роботи _____ Ольга СМОТР
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Метою кваліфікаційної роботи є дослідження можливостей використання стеку ELK для аналізу лог-файлів з метою виявлення потенційних загроз в безпеці.

Для досягнення поставленої мети потрібно вирішити такі завдання:

– зібрати лог-файли з різних джерел та джерел зберігання даних;

– завантажити та індексувати ці лог-файли в ELK стек;

– налаштувати систему відслідковування лог-файлів та збір метрик з ELK;

– розробити та застосувати алгоритми аналізу лог-файлів для виявлення потенційних загроз безпеці;

– візуалізувати результати аналізу за допомогою інструментів візуалізації даних в ELK.

Об’єктом дослідження є лог-файли, які збираються з різних джерел.

Предметом дослідження є алгоритми аналізу даних для виявлення потенційних загроз безпеці та їх візуалізація, а також процес автоматичного сповіщення та плани дій щодо вирішення виявлених проблем.

Практична вагомість. Аналіз лог-файлів є важливою складовою безпеки комп'ютерних систем. Зловмисники можуть скористатися вразливостями системи, щоб отримати незаконний доступ до конфіденційної інформації. Виявлення потенційних загроз безпеці та реагування на них є надзвичайно важливим для забезпечення безпеки та збереження даних. Використання ELK для аналізу лог-файлів дозволяє автоматизувати процес виявлення загроз та спрощує процес реагування на них, що робить цю технологію незамінною для практичного застосування в сфері безпеки комп'ютерних систем.

Ключові слова: ELK, ЛОГ-ФАЙЛИ, БЕЗПЕКА, ЗАГРОЗИ, АНАЛІЗ ДАНИХ.

Додано примітку [au1]: Перенесіть вниз після анотації

ABSTRACT

The purpose of the graduation project is to investigate the possibilities of using the ELK stack to analyze log files in order to identify potential security threats.

To achieve this goal, it is necessary to solve the following tasks:

- collect log files from various sources and data storage sources;
- upload and index these log files to the ELK stack;
- set up a system for tracking log files and collecting metrics from ELK;
- develop and apply algorithms for analyzing log files to identify potential security threats;
- visualize the results of the analysis using data visualization tools in ELK;

The object of the study is the log files collected from various sources.

The subject of the study is data analysis algorithms for identifying potential security threats and their visualization, as well as the process of automatic notification and action plans to address the identified problems.

Practical significance. Analyzing log files is an important component of computer system security. Attackers can exploit system vulnerabilities to gain illegal access to confidential information. Detecting and responding to potential security threats is crucial to ensure the security and safety of data. Using ELK to analyze log files automates the process of detecting threats and simplifies the process of responding to them, making this technology indispensable for practical use in the field of computer system security.

Keywords: ELK, LOG FILES, SECURITY, THREATS, DATA ANALYSIS.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ELK - ElasticSearch, Logstash, Kibana

FIM (File Integrity Monitoring) - моніторинг цілісності файлів
МСБ - малий та середній бізнес
DoS (Denial of Service) - відмова у обслуговуванні

DDoS (Distributed Denial of Service) - розподілена відмова у обслуговуванні
США - Сполучені Штати Америки
ФБР - Федеральне Бюро Розслідувань

API (Application Programming Interface) - інтерфейс програмування додатків rps - запитів за секунду
MD5 (Message Digest Algorithm 5) - алгоритм гешування повідомлень 5 SHA1 (Secure Hash Algorithm 1) - безпечний алгоритм хешування 1
SHA256 (Secure Hash Algorithm 256-bit) - безпечний алгоритм хешування 256-бітний
ПЗ - програмне забезпечення

IP (Internet Protocol) - інтернет-протокол
CBD-списки - списки центральної бази даних
TCP (Transmission Control Protocol) - протокол контролю передачі RST - скидання
AFM/DHD (Advanced Firewall Manager / Distributed Denial of Service Hybrid Defender) - розширений менеджер брандмауера / гібридний захисник від розподілених відмов у обслуговуванні
VS/PO (Virtual Server / Protected Object) - віртуальний сервер / захищений об'єкт
IPI (Intelligent Platform Interface) - інтелектуальний платформенний інтерфейс
PPS - пакетів за секунду
DNS (Domain Name System) - система доменних імен

TLS (Transport Layer Security) - безпека транспортного рівня

HTTP (HyperText Transfer Protocol) - протокол передачі гіпертексту

HTTPS (HyperText Transfer Protocol Secure) - безпечний протокол передачі гіпертексту

ЗМІСТ

ВСТУП

Розвиток інформаційних технологій та комп'ютерних мереж значно збільшив можливості обміну та обробки інформації для сучасних компаній. Завдяки цьому виникли нові методи ведення бізнесу та співпраці з клієнтами, партнерами та постачальниками. Однак, зростання залежності від інформаційних технологій призвело до збільшення числа потенційних загроз безпеки, що можуть мати катастрофічні наслідки для компаній.

У останні роки інформаційні технології відіграють все більшу роль в нашому житті, стаючи невід'ємною складовою повсякденної діяльності і розвитку. Цифрова трансформація впливає на всі аспекти нашого життя, від особистого спілкування і розваг до роботи та управління ресурсами компаній. Такий стрімкий розвиток IT став можливим завдяки неперервним інноваціям, що відбуваються в галузі, а також різноманітним можливостям, що відкриваються перед нами.

Однак, разом з тим, як інформаційні технології все більше переплітаються з нашим життям, збільшуються й потенційні ризики, пов'язані з ними. Це стосується, зокрема, зберігання та обробки персональних даних, безпеки корпоративних мереж і захисту від злому. З цієї причини компаніям дедалі важливіше стає розуміти, як забезпечити високий рівень безпеки та контролю над своїми інформаційними ресурсами.

У цьому контексті аналіз лог-файлів відіграє важливу роль у виявленні та відстеженні потенційних загроз безпеки. Стек ELK (Elasticsearch, Logstash, Kibana) є сучасним та потужним інструментом для аналізу та моніторингу лог-файлів, що дозволяє фахівцям з кібербезпеки швидко виявляти аномалії та забезпечувати захист інформаційних систем.

ELK стек, як згадувалось раніше, є одним з інструментів, що допомагає компаніям ефективно вирішувати проблеми безпеки. Але важливо зазначити, що успішна реалізація стратегії безпеки залежить не тільки від використання

відповідних технічних рішень, а й від розуміння корпоративною культурою значення інформаційної безпеки та відповідального підходу до управління даними.

Критично важливим бізнес-активом для повсякденної діяльності будь-якої компанії та її виживання є конфіденційна інформація про продукти, процеси, клієнтів та постачальників. З розвитком інформаційних технологій та збільшенням кількості даних, що обробляються, аналіз лог-файлів з використанням стеку ELK для виявлення потенційних загроз безпеці стає все більш актуальним.

Найбільш поширеною загрозою в мережній системі є несанкціонований доступ до інформаційних та обчислювальних ресурсів компанії. Це може призвести до втрати конфіденційності, цілісності та доступності інформації, яка є технологічним активом. Відповідно, аналіз лог-файлів та виявлення аномалій у поведінці системи може допомогти вчасно виявити потенційні загрози та забезпечити кібербезпеку організації.

Несанкціонований доступ до даних через компрометування комп'ютерної безпеки також відомий як злом. В ідеалі будь-яка організація повинна мати якийсь план реагування на інциденти для боротьби зі зломами локальної мережі, але дослідження показують, що цьому моменту приділяється мало уваги. Застосування аналізу лог-файлів з використанням ELK може допомогти в розробці такого плану та його впровадженні на практиці.

Метою даної магістерської роботи є дослідження можливостей використання стеку ELK для аналізу лог-файлів з метою виявлення потенційних загроз в безпеці. Для досягнення цієї мети, будуть вивчені основні принципи роботи стеку ELK, його архітектура та можливості в контексті аналізу лог-файлів. Також будуть розглянуті методи застосування стеку ELK для виявлення аномалій та атак на інформаційні системи.

Виявлення потенційних загроз безпеці та запобігання їх реалізації є

критично важливим завданням, особливо у сфері інформаційної безпеки. Використання системи ELK для аналізу лог-файлів дозволяє швидко та ефективно виявляти потенційні загрози безпеці та приймати необхідні заходи для їх запобігання.

ВИСНОВКИ

У даній роботі було проведено детальний аналіз важливості та значення лог-файлів в контексті інформаційної безпеки. Метою роботи була розробка методу аналізу лог-файлів для виявлення потенційних загроз безпеки з використанням системи ELK.

Метою магістерської роботи було дослідження можливостей використання стеку ELK для аналізу лог-файлів з метою виявлення потенційних загроз в безпеці. Дослідження обгрунтовує актуальність використання стеку ELK у сфері інформаційної безпеки та вплив цієї технології на якість та ефективність аналізу лог-файлів.

В процесі роботи над темою було розглянуто основні види лог-файлів та особливості їх зберігання та аналізу. Було проведено порівняльний аналіз систем журналювання подій Windows та Linux, що дозволило більш точно визначитиїх відмінності та спільні риси.

Важливу частину роботи складає розгляд принципів збору та аналізу лог-файлів з використанням ELK. Було досліджено основні компоненти цієї системи - Elasticsearch, Logstash та Kibana, та розглянуто їх взаємодію та особливості використання.

Робота містить детальний аналіз загроз безпеки інформації, включаючи класифікацію активних та пасивних атак. Окрім того, було розглянуто, як система ELK може допомогти в аналізі та виявленні цих загроз.

Практична частина роботи включає встановлення Elasticsearch, Logstash і Kibana, а також налаштування цих компонентів для обробки лог-файлів. Особлива увага приділена розробці фільтрів для Logstash та шаблонів для Elasticsearch, що є ключовим елементом ефективного аналізу лог-файлів.

Таким чином, можна зробити висновок, що стек ELK є потужним інструментом для аналізу лог-файлів та виявлення потенційних загроз безпеки. Він дозволяє компаніям ефективно виявляти, відстежувати та

аналізувати можливі проблеми, що забезпечує високий рівень захисту від несанкціонованого доступу."

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Turnbull J. The Logstash Book / James Turnbull., 2013. - 262 c.
2. Gormley C., Tong Z. Elasticsearch: The Definitive Guide: A Distributed Real-Time Search and Analytics Engine. 2015. 724 p.
3. Srivastava A. Mastering Kibana 6.x: Visualize your Elastic Stack data with histograms, maps, charts, and graphs. Packt Publishing, 2018. 365 p.
4. Aggarwal M. Network Security with pfSense: Architect, deploy, and operate enterprise-grade firewalls. Packt Publishing, 2018. 152 p.
5. Elasticsearch Guide [8.8] | Elastic. *Elasticsearch Platform - Find real-time answers at scale | Elastic*. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html (date of access: 01.04.2023).
6. Event Logging (Event Logging) - Win32 apps. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging (date of access: 05.05.2023).
7. Vulnerability detection - Use cases Â· Wazuh documentation. *Wazuh documentation*. URL: https://documentation.wazuh.com/current/getting-started/use-cases/vulnerability-detection.html (date of access: 11.06.2023).
8. Антон П. Советы и рекомендации по преобразованию неструктурированных данных из логов в ELK Stack используя GROK в LogStash. *Хабр*. URL: https://habr.com/ru/articles/509632/ (дата звернення: 14.06.2023).
9. Chuvakin A. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress, 2012. 460 p.
10. Kali Linux. Тестування на проникнення і безпеку / А. Замм та ін. ; ред. Н. Гринчик ; пер. з англ. А. Герасименко. 4-те вид. Packt Publishing, 2018. 528 с.

11. Kurose J., Ross K. Computer Networking: A Top-Down Approach. 7th ed. Pearson, 2016. 864 p.

12. Speciner M., Perlman R., Kaufman C. Network Security: Private Communications in a Public World. 2nd ed. Pearson, 2002. 1103 p.

13. Зеркалов Д.В. Безпека життєдіяльності та основи охорони праці. Навчальний посібник. К.: «Основа». 2016. - 267 с.

14. Яремко З. М. Безпека життєдіяльності: Навч. посіб. — Львів., 2005. - 301 с.

15. Желібо Є. П. Заверуха Н.М., Зацарний В.В. Безпека життєдіяльності. Навчальний посібник. - К.; Каравела, 2004. -328 с.

16. Morgan S. Cybercrime To Cost The World 8 Trillion Annually In 2023. Cybercrime Magazine. URL: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/ (date of access: 16.06.2023).

17. Morgan S. 2022 Official Cybercrime Report. 83 Main Street, 2nd Flr., Northport, N.Y. 11768 : eSentire, 2022. 32 p. URL: https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf.

18. Cyber Heatmap: CyberRisk Is Rising Across 70 Global. www.moodys.com. URL: https://www.moodys.com/research/Moodys-Cyber-Heatmap-Cyber-Risk-Is-Rising-Across-70-Global--PBC_1343021.

19. McLean E. Managing Cyber Risk. 2022 Cybercrime Report. Erin McLean, CMO & Tia Hopkins, Field CTO, eSentire. SoundCloud. URL: https://soundcloud.com/cybercrimemagazine/managing-cyber-risk-2022-cybercrime-report-erin-mclean-cmo-tia-hopkins-field-cto-esentire (date of access: 16.06.2023).

20. Morgan S. Top 10 Cybersecurity Predictions and Statistics For 2023. Cybercrime Magazine. URL: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ (date of access: 16.06.2023).