МАТЕРІАЛИ ДРУКУЮТЬСЯ УКРАЇНСЬКОЮ, АНГЛІЙСЬКОЮ, ПОЛЬСЬКОЮ МОВАМИ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

XIX Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Львів – 2024

Юрій КОПИСТИНСЬКИЙ – начальник докторантури, ад'юнктури, к.т.н.;
Андрій ТАРНАВСЬКИЙ – доцент кафедри цивільного захисту та протимінної діяльності ЛДУБЖД, к.т.н., доцент;
Олександра ПЕКАРСЬКА – викладач кафедри цивільного захисту та протимінної діяльності ЛДУБЖД;
Андрій КУШНІР – доцент кафедри наглядово-профілактичної діяльності та пожежної автоматики ЛДУБЖД, к.т.н., доцент;
Інна ОНОШКО – старший викладач кафедри наглядово-профілактичної діяльності та пожежної автоматики ЛДУБЖД;
Дмитро КОБИЛКІН – доцент кафедри права та менеджменту у сфері цивільного захисту ЛДУБЖД, к.т.н., доцент;
Ольга КОРЧАК – викладач кафедри права та менеджменту у сфері цивільного захисту ЛДУБЖД;
Роман КОНАНЕЦЬ – заступник начальника кафедри пожежної тактики та аварійно-рятувальних робіт ЛДУБЖД;
Володимир-Петро ПАРХОМЕНКО – доцент кафедри пожежної тактики та аварійно-рятувальних робіт ЛДУБЖД, к.т.н.;
Назарій БУРАК – заступник начальника кафедри інформаційних технологій та систем електронних комунікацій ЛДУБЖД, к.т.н., доцент;
Олександр ХЛЕВНОЙ – доцент кафедри інформаційних технологій та систем електронних комунікацій ЛДУБЖД, к.т.н.;
Світлана ВДОВИЧ – доцент кафедри практичної психології та педагогіки ЛДУБЖД, к.т.н., с.н.с.;
Юлія КУЛИК – викладач кафедри практичної психології та педагогіки ЛДУБЖД
Володимир МАРИЧ – старший викладач кафедри промислової безпеки та охорони праці ЛДУБЖД, к.т.н., доцент;
Наталія ІВАСІВКА – викладач кафедри промислової безпеки та охорони праці ЛДУБЖД;
Катерина СТЕПОВА – доцент кафедри екологічної безпеки ЛДУБЖД, к.т.н., доцент
Ірина КОЧМАР – викладач кафедри екологічної безпеки ЛДУБЖД;
Руслана СОДОМА – старший викладач кафедри права та менеджменту у сфері цивільного захисту ЛДУБЖД, к.е.н., доцент
Олег КОВАЛЬЧУК – викладач кафедри права та менеджменту у сфері цивільного захисту ЛДУБЖД, доктор філософії;
Галина ТЕЛЕГІНА – доцент кафедри промислової безпеки та охорони праці ЛДУБЖД, к.м.н., доцент;
Орислава ГОРНОСТАЙ – доцент кафедри промислової безпеки та охорони праці ЛДУБЖД, к.т.н., доцент
Даниїл БЕГЕН – науковий співробітник відділу науково-редакційної діяльності ЛДУБЖД
Ростислав ГРИНИК – молодший науковий співробітник відділу організації науково-дослідної діяльності ЛДУБЖД

ОРГАНІЗАТОР ТА ВИДАВЕЦЬ	Львівський державний університет безпеки життєдіяльності
Технічний редактор, комп'ютерна верстка	Беседа А.В., Беген Д.А.
Друк	Петролюк Н.І.
Відповідальний за друк	Войтович Т.М.
АДРЕСА РЕДАКЦІЇ:	ЛДУ БЖД, вул. Клепарівська, 35, м. Львів, 79007
Контактні телефони:	(032) 233-24-79, тел/факс 233-00-88

Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2024. – 906 с.

Збірник сформовано за науковими матеріалами Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів **«Проблеми та перспективи розвитку системи безпеки життєдіяльності»**.

Збірник містить матеріали таких тематичних секцій:

- Цивільна безпека.
- Пожежна та техногенна безпека.
- Менеджмент у безпеці життєдіяльності.
- Організація проведення аварійно-рятувальних робіт та гасіння пожеж.
- Інформаційні технології у безпеці життєдіяльності.
- Соціальні, психолого-педагогічні аспекти та гуманітарні засади безпеки життєдіяльності.
- Промислова безпека та охорона праці.
- Природничо-наукові та екологічні аспекти безпеки життєдіяльності.
- Організаційно-правові аспекти забезпечення безпеки життєдіяльності.
- Медицина в умовах воєнного стану.

Здано в набір 06.03.2023. Підписано до друку 28.04.2023. Формат 60x84$^{1/3}$. Папір офсетний.
Ум. друк. арк. 56,63.
Гарнітура Times New Roman.
Друк: ЛДУ БЖД
вул. Клепарівська, 35, м. Львів, 79007.
ldubzh.lviv@dsns.gov.ua

MATERIALS ARE PRINTED IN UKRAINIAN, ENGLISH AND POLISH LANGUAGES

COLLECTION OF SCIENTIFIC PAPERS

XIX International Scientific and Practical Conference of young scientists, cadets and students

PROBLEMS AND PROSPECTS FOR THE DEVELOPMENT OF THE SECURITY SYSTEM LIFE ACTIVITIES

Lviv – 2024

EDITORIAL BOARD:

Юрій KOPYSTYNSKYI – Head of the Department of Postgraduate and Postdoctoral Studies, LSULS, PhD;
Andrii TARNAVSKY – Associate Professor of the Department of Civil Protection and Mine Action, LSULS, PhD, Associate Professor;
Oleksandra PEKARSKA – Lecturer at the Department of Civil Protection and Mine Action, LSULS;
Andrii KUSHNIR – Associate Professor of the Department of supervision-preventive activity and fire automatics, LSULS, PhD, Associate Professor;
Inna ONOSHKO – Senior Lecturer of the Department of supervision-preventive activity and fire automatics, LSULS;
Dmytro KOBYLKIN – Associate Professor of the Department of Law and Management in the Field of Civil Protection, LSULS, PhD, Associate Professor;
Olha KORCHAK – Lecturer of the Department of Law and Management in the field of civil protection, LSULS;
Roman KONANETS – Deputy-head of the Department of fire tactics and emergency rescue operations, LSULS;
Volodymyr-Petro PARKHOMENKO – Associate Professor of the Department of fire tactics and emergency rescue operations, LSULS, PhD;
Nazarii BURAK – Deputy-head of the Department of Information Technologies and Systems of Electronic Communications, LSULS, PhD, Associate Professor;
Oleksandr KHLEVNOI – Associate Professor of the Department of Information Technologies and Systems of Electronic Communications, LSULS, PhD;
Svitlana VDOVYCH – Associate Professor of the Department of Applied Psychology and Pedagogy, LSULS, PhD, Senior Researcher;
Yuliia KULYK – Lecturer of the Department of Applied Psychology and Pedagogy, LSULS;
Volodymyr MARYCH – Senior Lecturer of the Department of Industrial and Occupational Safety, LSULS, PhD, Associate Professor;
Nataliia IVASIVKA – Lecturer of Department of Industrial and Occupational Safety, LSULS;
Kateryna STEPOVA – Associate Professor of the Department of Environmental Safety, LSULS, PhD, Associate Professor;
Iryna KOCHMAR – Lecturer of the Department of Environmental Safety, LSULS;
Ruslana SODOMA – Senior Lecturer of the Department of Law and Management in the Field of Civil Protection, LSULS, PhD, Associate Professor;
Oleh KOVALCHUK – Lecturer of the Department of Law and Management in the Field of Civil Protection, LSULS;
Halyna TELEHINA – Associate Professor of the Department of Industrial and Occupational Safety, LSULS, PhD, Associate Professor;
Oryslava HORNOSTAI – Associate Professor of the Department of Industrial and Occupational Safety, LSULS, PhD, Associate Professor;
Danyil BEHEN – Researcher of the Department of Scientific and Editorial Activities, LSULS;
Rostyslav HRYNYK – Junior Researcher of the Department for Organization of Scientific Research, LSULS;

ORGANIZER AND PUBLISHER	Lviv State University of Life Safety
Technical editor, Computer typesetting	Beseda A.V., Danyil Behen
Printing	Petrolyuk N.I.
Responsible for printing	Voitovych T.M.
EDITORIAL OFFICE ADDRESS:	LSU LS, Kleparivska Street, 35 Lviv city, 79007
Contact telephones:	(032) 233-24-79, 233-00-88

Problems and prospects for the Development of the security system life activities: Collection of scientific papers XIX International Scientific and Practical Conference of Young Scientists, Cadets and Students. – Lviv: LSU LS, 2023. – 906 p.

The collection is based on scientific materials of XIX International Scientific and Practical Conference of Young Scientists, Cadets and Students **"Problems and Prospects for the Development of Life Safety System".**

The collection contains materials from the following thematic sections:

- Civil safety.
- Fire and technological safety.
- Management in life safety
- Organisational and legal aspects of ensuring life safety.
- Information technologies in life safety.
- Social, psychological and pedagogical aspects and humanitarian principles of life safety.
- Industrial safety and labour protection.
- Natural-scientific and ecological aspects of life safety.
- Organisation of emergency rescue operations and fire extinguishing.
- Medicine under martial law.

Sent to the set on 06.03.2023. Signed to print 28.04.2023. Format 60x841/3. Offset paper. Conditional printing of sheets. 56,63. Headset Times New Roman. Printing: LSU LS Kleparivska Street, 35, Lviv city, 79007. ldubzh.lviv@dsns.gov.ua

УДК 004.4: 004.896

РЕАГУВАННЯ НА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДАНИХ ЗАСОБАМИ ELASTIC SECURITY

Микита Купріков
Ольга Смотр, кандидат технічних наук, доцент
Львівський державний університет безпеки життєдіяльності

Робота присвячена дослідженню ефективності платформи Elastic Security у виявленні загроз, аналізу часу реагування на інциденти безпеки, а також визначенню напрямків для вдосконалення захисту даних, шляхом використання інструментарію Elastic Stack, для вирішення завдань аналізу великих обсягів даних, моніторингу систем, логування, пошуку і аналітики великих даних.

Ключові слова: Big Data, платформи моніторингу та аналізу великих даних, Elastic Stack,

RESPONDING TO DATA SECURITY THREATS WITH ELASTIC PROTECTION

Mykyta Kuprikov
Olga Smotr, Candidate of Technical Sciences, Associate Professor
Lviv State University of Life Safety

The paper investigates the effectiveness of Elastic Security in detecting threats, analyzing response times to security incidents, and identifying areas for improvement data protection by using the Elastic Stack platform tools to solve the problems of analyzing large amounts of data, monitoring systems, logging, searching, and analyzing big data.

Keywords: Big data monitoring and analysis platforms, Elastic Stack, Big Data.

У нашому сучасному взаємопов'язаному світі інформаційна безпека стала критично важливою проблемою, особливо у зв'язку з тим, що організації обробляють постійно зростаючий обсяг запитів до своїх серверів. В епоху цифрових технологій захист конфіденційних даних і підтримка цілісності систем, орієнтованих на безпеку, мають першорядне значення. Ця важливість зростає в періоди підвищених кіберзагроз, пов’язаних із повномасштабним вторгненням російських військ на територію України у 2022 році та інформаційною війною, що супроводжує цей збройний конфлікт.

Давайте заглибимося в те, чому інформаційна безпека важлива, і дослідимо її значення в контексті великомасштабних серверних взаємодій і кібератак. Інформаційна безпека захищає особисті та конфіденційні дані від несанкціонованого доступу. Незалежно від того, чи це записи про клієнтів,

фінансові транзакції або інтелектуальна власність, захист цієї інформації має вирішальне значення. Тож очевидно, що із зростанням кількості атак розшифрування та порушень даних, надійні заходи із кібербезпеки вже не є вибором — вони є необхідністю. Це охоплює захист вашої IT-системи, мереж та даних від цифрових атак. Таким чином, інформаційна безпека - це не просто технічна проблема, це стратегічний імператив.

Критично важливим для повсякденної діяльності будь-якої компанії, а тим паче безпеко-орієнтованих структур держави, є конфіденційна інформація про продукти, процеси, клієнтів та постачальників. 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.

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 відповідних систем, може допомогти в розробці такого плану та його впровадженні на практиці. Адже з розвитком інформаційних технологій та збільшенням кількості даних, що обробляються, аналіз лог-файлів з використанням стеку ELK (ELK - ElasticSearch, Logstash, Kibana) для виявлення потенційних загроз безпеці стає все більш актуальним [1].

Відповідно, аналіз лог-файлів та виявлення аномалій у поведінці системи може допомогти вчасно виявити потенційні загрози та забезпечити кібербезпеку організації.

Перш за все, лог-файли - це файли, які містять записи про події, які відбуваються в операційній системі або програмному забезпеченні. Вони зберігають інформацію про те, як користувачі взаємодіють з системою, що відбувається під час виконання програм, які процеси запущені та інші дії, які відбуваються в системі.

Огляд лог-файлів допомагає розуміти, як функціонує система та виявляти аномальну поведінку, що може свідчити про зловживання доступом або зловмисну діяльність. Це може бути корисно при розслідуванні інцидентів безпеки та при виявленні вразливостей, які можуть бути використані для атак на систему.

Однак, аналіз лог-файлів може бути трудомістким і складним завданням, оскільки лог-файли можуть бути великими та недоступними для ручного аналізу. У таких випадках використання системи збору та аналізу лог-файлів, ми пропонуємо використовувати саме ELK систему, яка дозволяє автоматизувати цей процес та зробити його більш ефективним [2].

Найпоширеніші види лог-файлів, які зустрічаються у більшості операційних систем і додатків, такі:

• системні лог-файли: містять інформацію про події, що сталися на рівні операційної системи, такі як старт/стоп служб, помилки ядра тощо;

• лог-файли додатків: містять інформацію про події, що сталися у програмах та додатках. Наприклад, лог-файли баз даних містять інформацію про запити до бази даних, а лог-файли веб-серверів містять інформацію про запити до веб-сайту;

• лог-файли мережевої активності: містять інформацію про мережеву активність, таку як інформацію про з'єднання, трафік, аутентифікацію, авторизацію тощо.

Крім того, існують різні спеціалізовані лог-файли, які зберігають інформацію про певні типи подій, такі як лог-файли антивірусного програмного забезпечення, які містять інформацію про виявлені загрози безпеки.

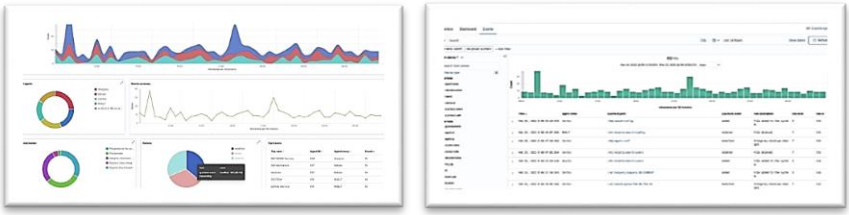
Для кожного типу лог-файлів існують спеціальні інструменти для їхнього збору, обробки та аналізу. ELK став дуже популярним інструментом для збору, обробки та аналізу лог-файлів, особливо в контексті забезпечення безпеки інформації. А для ефективного аналізу загроз безпеці інформації, їх необхідно розрізняти, та діяти відповідно до класу атаки. Один з можливих способів класифікації загроз безпеці інформації - це відповідно до виду атаки, яку вони викликають. Тож, атаки можуть бути активними та пасивними.

Активні атаки - це атаки, при яких зловмисники активно взаємодіють з цільовою системою з метою її порушення або отримання доступу до конфіденційної інформації. Ці атаки можуть включати напади на мережевий протокол, експлойти вразливостей програмного забезпечення, злам паролів та багато іншого. Активні атаки можуть мати на меті викрадення, внесення змін або знищення даних, завдання шкоди роботі системи або злам безпеки мережі. Пасивні атаки - це атаки, при яких зловмисники не взаємодіють з системою, а лише збирають інформацію, що передається по мережі. Такі атаки можуть включати перехоплення мережевого трафіку, аналіз вмісту пакетів, викрадення файлів локальних систем та інші. Ці атаки можуть бути складнішими у виявленні, оскільки зловмисники не змінюють стан системи, а лише збирають інформацію.

Оскільки активні та пасивні атаки мають різні характеристики та можуть використовувати різні методи, виявлення цих атак вимагає використання різних методик та інструментів. Важливо також розуміти, що залежно від цілей та мети зловмисника, можуть використовуватись як активні, так і пасивні атаки.

Активні атаки є більш складними в реалізації порівняно з пасивними атаками, але водночас можуть бути більш ефективними. Вони спрямовані на зміну даних або заборону доступу до них.

Щоб спостерігати активні атаки в ELK використовується компонент контролю цілісності файлів (File Integrity Monitoring, FIM) [1-2]. Він генерує сповіщення, коли він виявляє зміну в файловій системі. Метадані включають контрольні суми MD5, SHA1 та SHA256, розміри файлів (до та після зміни), права на файли, власника файлу, зміни вмісту та користувача, який зробив ці зміни (who-data). Для прикладу на рисунку 1 відображено інформаційні панелі ELK, на яких користувачі можуть бачити всі деталі спрацьованих сповіщень та знайти повний звіт про виявлені зміни. За це в ELK відповідає модуль FIM (File Integrity Monitoring – модуль моніторингу цілісності файлів) проводить періодичні скани на конкретних шляхах та контролює конкретні каталоги на предмет змін в реальному часі. Тож користувач можете встановити, які шляхи слід контролювати, в налаштуваннях агентів та менеджера.



а) б)

Рисунок 1 – Вигляд розділу інформаційної панелі де користувачі можуть переглядати деталі сповіщень щодо звернень до даних у вигляді:
а) графіків; б) у вигляді окремих випадків

Окрім того за допомогою ELK, ми можемо спостерігати несподівані та підозрілі спроби входу, наприклад, що це за техніка взлому, результат входу, категорія події, IP-адреса джерела, місцезнаходження джерела, повідомлення про помилку та інші. Приклад відображення атаки на автентифікацію у ELK показано на рисунку 2.

Time (@timestamp)	threat.technique.name	event.login.outco...	event.cate...	source.ip	source.local...	error.message
Jun 13, 2023 @ 17:09:58.450	Brute Force	failure	authentication	77.244.187.75	Kyiv	authentication failed for [bruno.pianetti@planetel.it], invalid password
Jun 13, 2023 @ 17:09:45.955	Brute Force	failure	authentication	77.244.187.75	Kyiv	authentication failed for [bruno.pianetti@planetel.it], invalid password
Jun 13, 2023 @ 17:09:43.936	Brute Force	failure	authentication	77.244.187.75	Kyiv	authentication failed for [bruno.pianetti@planetel.it], invalid password
Jun 13, 2023 @ 17:09:33.737	Brute Force	failure	authentication	77.244.187.75	Kyiv	authentication failed for [bruno.pianetti@planetel.it], invalid password
Jun 13, 2023 @ 17:08:58.400	Brute Force	failure	authentication	77.244.187.74	Kyiv	authentication failed for [bruno.pianetti@planetel.it], invalid password

Рисунок 2 – Приклад відображення атаки на автентифікацію у ELK

Пасивні атаки, хоча менш складні в реалізації, все ж можуть мати серйозні наслідки для інформаційної безпеки. Оскільки вони не змінюють інформацію, а лише перехоплюють її, то часто їх важко виявити [3].

Для ефективного виявлення потенційних загроз безпеці необхідно проводити аналіз лог-файлів, що збираються системою моніторингу безпеки, та визначати надзвичайні події. При цьому потрібно звертати увагу на різноманітність атак та можливі шляхи їх реалізації, щоб мати можливість діяти вчасно та ефективно у разі виявлення загроз. В даному випадку дуже важливою є інформація про те, які служби (IP-адреси) зазнали атаки і які контексти або захищені об'єкти були задіяні. На рисунку 3 відображено інформаційну панель ELK, щодо служб, які зазанли атаки та які вектори використовує зловмисник. На двох лівих графіках ви отримуєте цю інформацію для втрачених пакетів. На двох правих графіках ви бачите цю інформацію для пакетів, що перевищують поріг виявлення, але не досягають рівня усунення загрози.

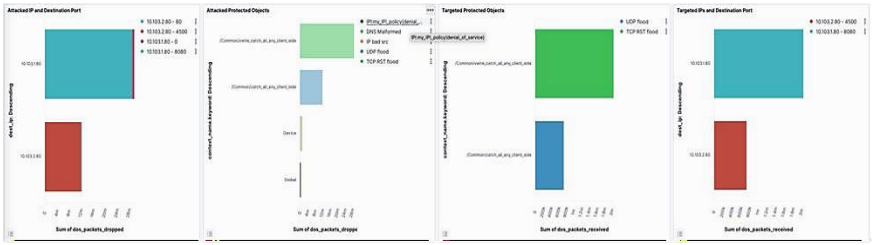


Рисунок 3 – Інформація про ціль атаки

Аналіз загроз безпеки інформації є критичним для забезпечення цілісності та безпеки інформаційних систем. Статистика та аналіз атак дозволяють отримати уявлення про типи загроз і їх частоту, що допомагає у визначенні стратегій захисту. Класифікація загроз допомагає у систематизації потенційних атак, що спрощує їх розпізнавання та управління ризиками. Практичні приклади використання аналізу лог-файлів, зокрема застосування ElasticSearch та Kibana для моніторингу DDoS-атак, свідчать про ефективність інструментів ELK у виявленні та реагуванні на загрози безпеки. Такий аналіз дозволяє не лише вчасно реагувати на потенційні загрози, а й попереджати їх виникнення шляхом аналізу та вдосконалення захисних стратегій.

За результатами даної роботи 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 літератури

1. Elastic N.V. "Elastic Stack Documentation". URL: https://www.elastic.co/guide/index.html.

2. Купріков М, Смотр О. Моніторинг та аналіз великих обсягів даних засобами платформи elastic stack. Інформаційна безпека та інформаційні технології ІБІТ-2023: збірних тез доповідей VI Всеукраїнсь-кої науково-практичної конференції, 30 листопада 2023 року. – Львів, ЛДУ БЖД, 2023. – С.341-343

3. Radu, Marius, "Elastic Stack for Monitoring, Logs and Metrics." Apress, 2017.

References

1. Elastic N.V., "Elastic Stack Documentation". URL: https://www.elastic.co/guide/index.html.

2. Kuprikov M, Smotr O. Monitoring and analysis of large amounts of data using the elastic stack platform. Information security and information technologies IBIT-2023: collection of abstracts of the VI All-Ukrainian scientific and practical conference, November 30, 2023. - Lviv, LSU of Life Safety, 2023. - P.341-343.

3. Radu, Marius, "Elastic Stack for Monitoring, Logs and Metrics." Apress, 2017.

Секція 5 / Section 5

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У БЕЗПЕЦІ ЖИТТЄДІЯЛЬНОСТІ