Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Системи виявлення та запобігання проникненню на прикладі Wazuh

Виконав: студент IV курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Поліщук В.А. (прізвище та ініціали)

Керівник (підпис) Загородна Н.В. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль - 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«19» червня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Поліщуку Владиславу Анатолійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Системи виявлення та запобігання проникненню на прикладі Wazuh

Керівник роботи Загородна Наталія Володимирівна., к.т.н., зав. каф. КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи перелік літературних джерел та вимоги до безпеки

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Аналіз предметної області. 1.1. Аналітичний огляд. 1.2. Класифікація систем виявлення проникненнь. 1.3. Класифікація систем запобігання проникненням.
1.4. Особливості методів виявлення підозрілих подій.
1.5. Огляд найбільш поширених програмних рішень IDS / IPS і їх коротке порівняння.
2. Теоретична частина.
2.1. Огляд компонентів системи Wazuh. 2.2. Розбір основних функцій компонентів Wazuh
2.3. Вибір програмних інструментів для реалізції системи Wazuh в комп'ютерній мережі.
2.4. Обгрунтування вибору та викладення основних кроків встановлення прикладного ПЗ.
3. Практична частина. 3.1. Імітування реальної загрози безпеці в локальній мережі.
3.2. Тестування системи фіксації подій на пристроях, що моніторяться. 3.3. Налаштування системи сповіщень електронною поштою. 3.4. Налаштування системи активного реагування.
4. Безпека життєдіяльності, основи хорони праці. 5. Перелік використаних матеріалів.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Пилипець М.І., доцент кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	09.04 – 12.04	*Виконано*
2.	Підбір джерел про системи виявлення та		
	запобігання проникненню	14.04 – 17.04	*Виконано*
3.	Опрацювання джерел про системи виявлення та		
	запобігання проникненню	19.04 – 29.04	*Виконано*
4.	Розроблення системи захисту інформації	30.04 – 11.05	*Виконано*
5.	Тестування системи виявлення та запобігання		
	проникненню	12.05 – 20.05	
6.	Оформлення розділу «Аналіз технічного завдання»	20.05 – 23.05	*Виконано*
7.	Оформлення розділу «Теоретична частина»	23.05 – 28.05	*Виконано*
8.	Оформлення розділу «Практична частина»	28.05 – 05.06	*Виконано*
9.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи хорони праці»	05.06 – 07.06	*Виконано*
10.	Оформлення кваліфікаційної роботи	07.06 – 10.06	*Виконано*
11.	Нормоконтроль	11.06 – 13.06	*Виконано*
12.	Перевірка на плагіат	14.06 – 17.06	*Виконано*
13.	Захист кваліфікаційної роботи	21.06.2023	

Студент _____ Поліщук В.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Системи виявлення та запобігання проникненню на прикладі Wazuh // Поліщук Владислав Анатолійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБ–41 // Тернопіль, 2023 // С. – 66, рис. – 31, табл. – 1, слайдів – _, бібліогр. – 19.

Ключові слова: ПРОНИКНЕННЯ, ВТОРГНЕННЯ, IDS, IPS, WAZUH, ЕКСПЛОЙТ, МОНІТОРИНГ

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.

ANNOTATION

Intrusion detection and intrusion prevention systems based on Wazuh // Polishchuk Vladyslav // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2023 // P. - 66, Fig. - 31, Table - 1, Slides - _, References - 19.

Keywords: INTRUSION, PENETRATION, IDS, IPS, WAZUH, EXPLOIT, MONITORING

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.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

LOG-file – це файл системи обліку подій, який містить інформацію про одну окрему подію, включає точний час та атрибути, які були використані в обробці події.

ЕКСПЛОЙТ (exploit) – це програмне забезпечення або послідовність команд, що націлена на експлуатацію вразливості на пристрої-цілі та отримання несанкіонованого доступу або конфіденційної інформації.

SQL-подібна база даних – реляційна база даних, яка основана на таблицях, кожен рядок, яких є окремою сутністю, а стовпець – полем, яке містить дані.

SMTP – це комунікаційний протокол для пересилання електронної пошти.

ІКС – інформаційно-комунікаційна система.

СИГНАТУРА – це певний шаблон, який дозволяє технологіям кібербезпеки розпізнавати загрози.

ЗМІСТ

ВСТУП

Сучасний світ невпинно поширює інтернет-технології усіма аспектами громадського та приватного життя людей. Сьогодні кожному з нас важко уявити свої будні та вихідні без періодичною взаємодією з мережею Інтернет, шляхом пошуку потрібних відомостей для вирішення прикладних проблем, спілкування з родичами чи передавання документів держустановам або корпоративних звітів колегам та керівникам. Таким чином, присутність комп'ютерної інфраструктури, почала бути не лише опцією для модернізації свого бізнесу чи особистого життя, а і потребою бути частиною конкурентного середовища, адже інформаційні технології дають унікальні переваги в автоматизації рутинних процесів, налагодження віддаленої комунікації та ведення обліку для бізнесів.

Знаючи, що основною ціллю будь-якого бізнесу є отримання фінансової вигоди шляхом задоволення потреб споживачів, у інтернет-середовищі виникають думки про можливості отримання частини цієї вигоди незаконним шляхом. Тому для протидії спробам отримання несанкціонованого доступу до інструментів надавання благ або шляхів конвертації виконаних робіт у фінансові засоби, створюються та розвиваються програмні та апаратні рішення забезпечення інформаційної безпеки. Щорічно втрати бізнесів через зловмисний вплив кіберзлочинців досягають рекордних значень, тому інвестування у засоби виявлення та запобігання проникненням стає більш рентабельним.

Звідси, для привертання уваги бізнесів, для яких безпека їх комп'ютерних мереж має високий пріоритет, розробники програмного забезпечення постійно працюють на вдосконаленням своїх продуктів. Вони активно досліджують останні вразливості та експлойти щоб пропонувати найактуальніші засоби захисту та зменшення впливу зловмисників на ключові аспекти ІКС компанії.

Тому на сьогодні, ринок пропонує безліч програмних рішень для потреб потенційних клієнтів (які також активно вивчаються відповідними фахівцями).

І для власника бізнесу, який розглядає варіант придбання рішення безпеки в комерційної команди розробників такого програмного забезпечення, вибір може виглядати дуже заплутаним та зрівноваженим (без однозначного нахилу в бік одного ультимативного рішення, яке здатне ідеально виконати будь-яке завдання з інформаційної безпеки). Для таких випадків, компанія шукає спеціалістів-консультантів, які, маючи відповідну компетентність в питаннях підбору та доцільності використання конкретних засобі захисту інформації для конкретних проблем, що виникають в окремій комп'ютерній мережі.

Під час оцінки комп'ютерної мережі, враховуються безліч факторів та вхідних даних, які може надати власник компанії, або місцевий системний адміністратор. Проте, навіть серед широкого спектру сучасних вимог, можна виділити основні, без яких неможливо забезпечити, хоча б, базовий рівень захищеності локальної інформаційної-мережі. Такими вимогами будуть можливість виявляти ознаки зловмисного впливу на систему, та за наявності таких, оперативно вживати заходів зі зменшення такого впливу або навіть унеможливлення його завдання у майбутньому.

Для обліку подій в мережевій інфраструктурі та на окремих вузлах часто розгортають систему моніторингу, яка буде збирати інформацію про стан кожного пристрою чи служби та події, що ними обробляються. Таким чином, після факту виникнення інцидентів порушення кібербезпеки, стає можливим встановлення причинно-наслідкових зв'язків між подіями та змінами в системі.

В таких системах обліку подій, зазвичай, існує автоматична система присвоєння рейтингу серйозності інцидентів шляхом оцінки потенційно нанесеної шкоди. І для подій з достатньо високим рейтингом серйозності система моніторингу автоматично активує вбудовану програму для первинного або абсолютного зменшення загрози шляхом застосування найкращих практик з забезпечення інформаційної безпеки, що досліджуються та документуються відповідними компаніями, на кшталт MITRE.

Метою цієї кваліфікаційної роботи є демонстрація основних функцій систем виявлення та систем запобігання проникненням. А також надання

основних відомостей, якими потрібно володіти для користування такими засобами забезпечення безпеки інформації. У такий спосіб, ми зможемо знизити поріг входження для користувачів, які ніколи не працювали з подібними системами та продемонструвати їм, як за допомогою безкоштовного рішення Wazuh можна зрозуміти основні принципи роботи IDS/IPS та навіть встановити і протестувати його в умовах своєї комп’ютерної системи.

Серед завдань, які мають бути виконані для досягнення мети виділимо:

- доступне викладення основних відомостей про системи виявлення та запобігання вторгненням із наведенням конкретних прикладів програмних рішень, доступних на ринку;
- детальний опис основних функцій та принципів роботи Wazuh;
- розбір процесу встановлення необхідного серверного та вузлового програмного забезпечення Wazuh;
- демонстрація системи сповіщень про визначені підозрілі події в системі, а також налаштування системи активних реакцій на підозрілі події високої серйозності;
- проведення тестування, налаштованих систем, шляхом імітації реальних атак, спроб експлуатування вразливостей з пристрою, який виконуватиме роль потенційного зловмисника.

Так ми сформуємо чіткіше уявлення про системи виявлення та запобігання вторгненням у читача, який розглядає можливість імплементації таких систем у свою комп’ютерну мережу, але не може перейти від планування до реалізації через недостатню компетентність у питаннях вибору, встановлення та налаштування таких засобі забезпечення інформаційної безпеки.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

Згідно з новим звітом IBM, у 2022 році середня вартість витоку даних була рекордною для компаній і становила близько 4,35 млн. доларів США [6].

Це на 2.6% більше за середню вартість у 2021 році, яка становила 4,24 мільйона доларів США [6]. Враховуючи потенційно руйнівні фінансові наслідки витоку даних, компаніям важливо вжити заходів для захисту своїх даних і запобігання витоку даних. На рисунку 1.1 зображений перелік основних (найвищих) статистичних показників, які відображають вплив «крадіжок даних» на сучасні бізнеси.

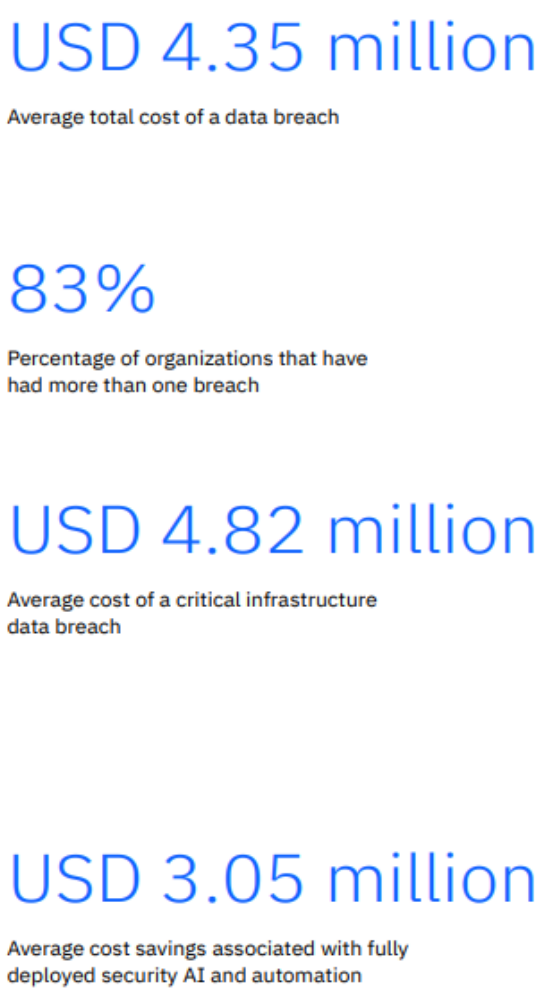


Рисунок 1.1 – Основні статистичні показники щодо оприлюднення конфіденційних даних бізнесів у 2022 році

Як бачимо, статистика ураження бізнесів сучасними кібератаками зростає

і сягає рекордних значень щорічно. Для зменшення ризиків та втрат до мінімуму, компанії застовують різноманітні засоби захисту інформації та своїх комп’ютерних мереж. Звідси, виникає потреба створення та розвитку систем, які будуть постійно відстежувати події і трафік в мережі з метою виявлення аномальних ознак поведінки пристроїв та програм.

І за виявлення фактів підозрілої активності, мета таких систем – якнайшвидше усунути причини виникнення та наслідки зловмисного впливу на систему, а також завадити отриманню несанкціонованого доступу до конфіденційної інформації.

1.1 Системи запобігання вторгненням (IPS)

IPS – система запобігання вторгненням, що відстежує мережевий трафік і не допускає зловмисників до решти вашої мережі. Системи IPS здатні розпізнавати шаблони в мережевому трафіку та негайно реагувати на них, щоб запобігти зловмисним атакам. При цьому IPS є активним ресурсом безпеки, тобто він реагує на дані в реальному часі, щоб зупинити атаки на кібербезпеку після виявлення ризику. Новіші системи IPS покладаються на заздалегідь запрограмовані правила, які дозволяють їм виконувати дії. Хоча їх основною метою є виявлення аномалій, виявивши їх, системи IPS здатні блокувати IP-адреси та обмежувати відповідний шкідливий трафік. Таким чином, вони більш активні, ніж системи виявлення вторгнень (IDS).

На рисунку 1.2 бачимо, що система запобігання вторгненням розміщена безпосередньо на шляху мережевого трафіку між відправником та одержувачем. Це саме те, що відрізняє IPS від IDS. Бо IDS є пасивною системою, яка сканує трафік і повідомляє про загрози [16].

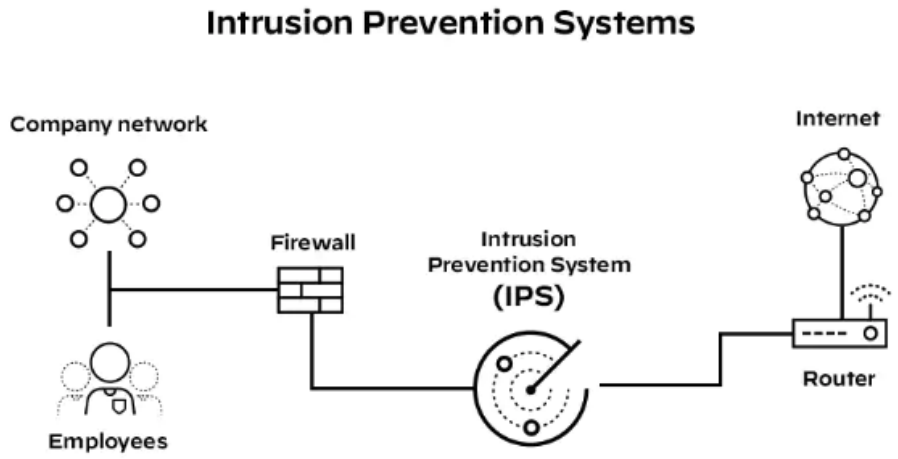


Рисунок 1.2– Схема розташування IPS як компонента комп’ютерної мережі компанії

Зазвичай, розташовуючись безпосередньо за брандмауером, IPS рішення аналізує весь мережевий трафік та вживає автоматизованих дій, коли це необхідно [16].

Цими діями можуть бути:

- надсилання сповіщення адміністратору;
- відкидання потенційно зловмисних пакетів;
- блокування джерела надходження трафіку (за IP адресою або іншими атрибутами);
- скидання з’єднання;
- конфігурування правил брандмауера для запобігання майбутніх атак.

Серед вимог до IPS як до компонента кібербезпеки:

- працювати ефективно, не створюючи додаткового навантаження на продуктивність мережі;
- працювати швидко, виявляючи експлойти у режимі реального часу;
- виявляти загрози та детально повідомляти про них, мінімізуючи хибно-позитивні (false positive) та уникати хибно-негативних (false negative) спрацювань.

Щоб успішно відповідати цим вимогам, існує кілька методів, що

використовуються для пошуку експлойтів і захисту мережі від несанкціонованого доступу. До них належать:

- виявлення на основі сигнатур (Signature-based detection) – це метод виявлення, заснований на словнику унікальних шаблонів (або сигнатур) у коді кожного експлойта. Коли експлойт виявлено, його сигнатура записується та зберігається в словнику сигнатур, що постійно поповнюється. Виявлення сигнатур для IPS поділяється на два типи:

  a) сигнатури, спрямовані на експлойти (Exploit-facing signatures), ідентифікують окремі експлойти, запускаючи унікальні шаблони конкретної спроби експлойту. IPS може ідентифікувати конкретні експлойти, знаходячи в потоці трафіку збіг із сигнатурою, що асоціюється з експлойтом;

  b) сигнатури, спрямовані на вразливість (Vulnerability-facing signatures) — це ширші сигнатури, спрямовані на основну вразливість у системі, на яку націлено атаку. Ці підписи дозволяють захищати мережі від невідомих досі експлойтів. Вони також підвищують ризик хибно-позитивних (false positive) спрацьовувань;

- виявлення на основі аномалій (Anomaly-based detection) бере вибірки мережевого трафіку випадковим чином і порівнює їх із попередньо розрахованим базовим рівнем продуктивності. Коли активність трафіку виходить за межі параметрів базової продуктивності, IPS вживає заходів;

- виявлення на основі політики (Policy-based detection) вимагає від системних адміністраторів налаштування політик безпеки на основі політик безпеки організації та мережевої інфраструктури. Якщо відбувається будь-яка дія, яка порушує визначену політику безпеки, запускається сповіщення та надсилається адміністраторам.

Крім методів роботи самих IPS, виділяють також типи таких систем, які можуть бути застосовані для різних потреб. Серед них:

- мережева система запобігання вторгненням (NIPS), яка встановлюється в стратегічних точках для моніторингу всього мережевого трафіку та сканування на наявність загроз;
- система запобігання вторгненням на хост (HIPS), яка встановлюється на робочій станції та переглядає вхідний/вихідний трафік лише з цієї машини. Часто в поєднанні з NIPS, HIPS є останньою ланкою захисту від загроз;
- аналіз поведінки мережі (NBA) аналізує мережевий трафік, щоб виявити незвичайні потоки трафіку та помітити нове зловмисне програмне забезпечення або вразливості нульового дня;
- система запобігання бездротовому вторгненню (WIPS) сканує мережу Wi-Fi на предмет несанкціонованого доступу та видаляє всі неавторизовані пристрої [17].

1.2 Системи виявлення вторгнень (IDS)

IDS – система виявлення вторгнень, вона відстежує вашу мережу на наявність підозрілої активності та повідомляє вас, коли виконуються попередньо сконфігуровані умови спрацювання сповіщень. Після отримання такого попередження можна вжити стратегічних заходів проти потенційної загрози незалежно від системи IDS. На відміну від системи IPS, вона не діє як посередник між відправником і отримувачем інформації. Система IDS – це скоріше закулісна система звітності, яка надає інформацію, на основі якої приймаються рішення.

Щоб ефективніше використовувати цей інструмент потрібно розуміти його основні принципи роботи. IDS повинна лише виявляти потенційну загрозу. Вона розміщена поза лінією мережевої інфраструктури і не є одним з посередників в комунікації відправника та отримувача інформації [3].

Рішення IDS часто використовують для більш ефективного використанні портів TAP або SPAN, для аналізу копії фрагмента потоку трафіку. Таким

чином гарантується відсутність впливу IDS на загальну продуктивність мережевої інфраструктури.

Система виявлення вторгнень працює, шукаючи відхилення від нормальної активності та відомі сигнатури атак. Аномальні тенденції поведінки в мережі надсилаються до стеку у вигляді вибірок, де потім перевіряються на протокольному та прикладному рівнях. Він може виявити атаку «DNS poisoning», зловмисно модифіковані пакети та Xmas сканування.

IDS може мати вигляд, як пристрою безпеки так і програмного забезпечення. А для захисту даних і систем у «хмарних» середовищах, також існують «хмарні» (cloud-based) IDS.

Виділяють п’ять типів систем виявлення вторгнень [18]:

- мережево-орієнтовані (network-based або NIDS);
- націлені на окремий хост (host-based або HIDS);
- протоколо-орієнтовані (protocol-based або PIDS);
- ті, що базуються на роботі з application protocol (application protocol-based або APIDS);
- гібридні.

Двома найпоширенішими з них є:

- мережево-орієнтовані системи виявлення вторгнень (NIDS). Такий тип IDS розгортається у всіх частинах інфраструктури та зокрема у стратегічних точках, тобто у підмережах, які зберігають або обробляють найбільш вразливу інформацію. NIDS відстежує весь трафік, що надходить до та від пристроїв у мережі, роблячи визначення на основі вмісту пакетів і метаданих.

- система виявлення вторгнень націлена на окремий хоста (HIDS). Ця IDS на основі хоста відстежує активність машини, на якій її встановлено. Іншими словами, він розгортається на певному комп’ютері, щоб допомогти фахівцям з кібербезпеки захистити його від внутрішніх і зовнішніх загроз. IDS

досягає цього, аналізуючи трафік, реєструючи зловмисну активність і повідомляючи визначених відповідальних осіб.

Три менш поширених IDS можна описати так:

- PIDS зазвичай встановлюється на веб-сервері. Вона (система виявлення вторгнень) моніторить та аналізує протокол в комунікації сервера з користувачем або пристроєм.
- APIDS – це система або агент, який зазвичай знаходиться всередині серверної частини. Вона відстежує та інтерпретує комунікацію за протоколами, що стосуються окремих програм. Наприклад, це відстежуватиме протокол SQL для програми-посередника в комунікації з веб-сервером. Тобто ця система застосовується для моніторингу комунікацій типу застосунок-застосунок.
- Гібридна система виявлення вторгнень поєднує функціонал двох або більше типів IDS. Наприклад, поєднання NIDS та HIDS дає повне уявлення про систему. Такі системи є більш потужними порівняно з іншими, більш вузькопрофільними типами IDS.

Крім типів IDS рішень, існують ще типи виявлення проникнень: на основі сигнатур та на основі аномалій, вони є спільними як для IDS, так і для IPS.

У таблиці 1.1наведені основні відмінності між системами виявлення проникнень та системами запобігання проникнень. А на рисунку 1.3 проілюстровані відмінності в розгортанні таких систем на макеті найпростішої комп’ютерної мережі [17].

Таблиця 1.1 – Порівняння основних переваг IDS та IPS

	IPS	IDS
Розташування в мережевій інфраструктурі	Є частиною прямої лінії комунікації (inline)	Поза прямою лінією комунікації (out-of-band)
Тип системи	Активна (моніторить і автоматично захищає) та/або пасивна	Пасивна (моніторить і сповіщає)

Продовження таблиці 1.1

	IPS	IDS
Механізми виявлення експлойтів	1. Виявлення на основі статистичних аномалій 2. Виявлення на основі сигнатур: – сигнатури експлойтів; – сигнатури вразливостей.	1. Виявлення на основі сигнатур: – сигнатури експлойтів; – сигнатури вразливостей.

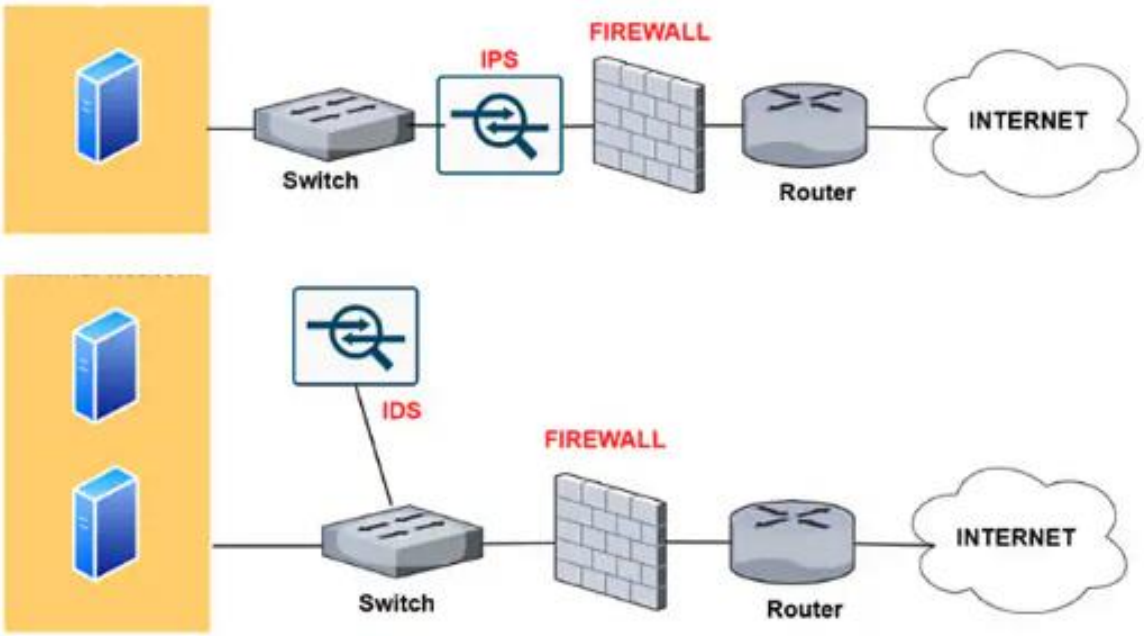


Рисунок 1.3 – Відмінності розташування IDS та IPS у найпростішій мережі

Отже, здатність IDS/IPS зупиняти зловмисників, поки вони ще збирають інформацію про мережу, є неоціненною. Водночас, універсального рішення кібербезпеки, на жаль, не існує. Зловмисники постійно знаходять нові способи використання вразливостей і обходу засобів захисту. Але наявність відповідних людей і процесів має вирішальне значення для забезпечення безпеки будь-якої організації.

1.3 Аналіз можливих рішень IDS/IPS

На сьогодні виробники систем виявлення та запобігання проникненням пропонують безліч програмних рішень. Деякі з них фокусуються лише на IPS складовій, інші ж – намагаються запропонувати максимум можливостей, які може реалізувати IDS. На противагу їм обом є і видавці, що поєднують обидві системи протидії вторгненням в одному продукті.

Щоб краще уявити, який вибір постає перед відділом кібербезпеки, коли виникає потреба впровадити IPS/IDS рішення в комп'ютерну мережу компанії, зекономивши максимум коштів – розглянемо конкретні варіанти таких рішень.

Як приклад IDS було обрано OSSEC HIDS, безкоштовна (open-source) хосто-орієнтована система виявлення проникнень, але з можливістю комерційної служби підтримки. Її користувацький веб-інтерфейс зображено на рисунку 1.4, і як бачимо, він пропонує лише обмежену кількість даних на домашній сторінці.

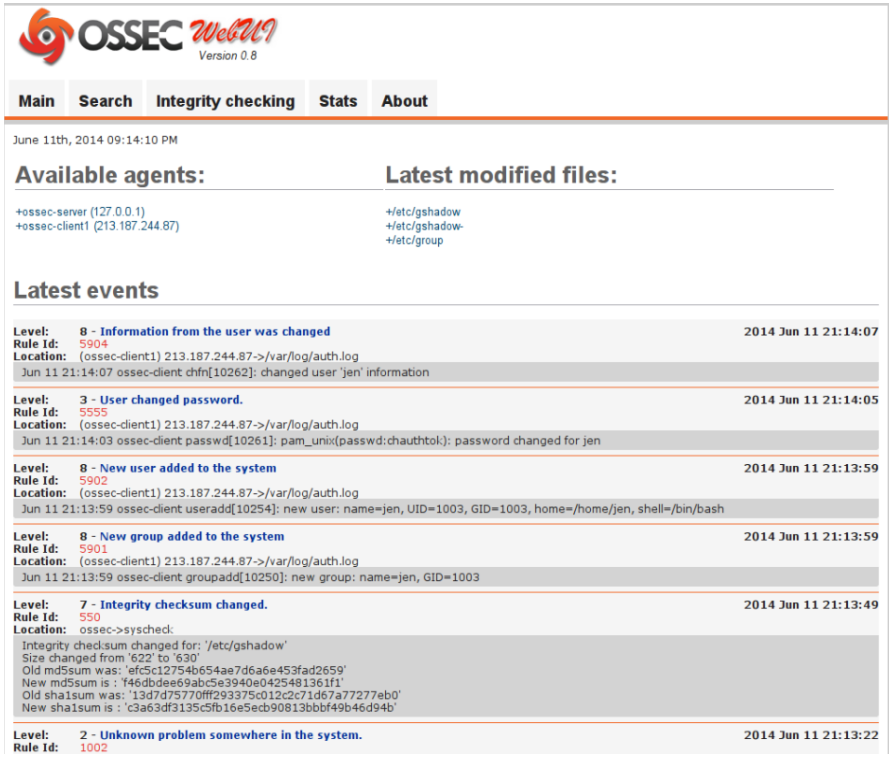


Рисунок 1.4 – Користувацький веб-інтерфейс інструменту OSSEC

Серед цих даних: список останніх подій на системах, що моніторяться, список підключених агентів (об'єктів моніторингу), та список останніх змінених файлів, аби візуально помітити чи зазнав змін вміст чутливих

каталогів на машинах. Рішення відоме своєю широкою універсальністю (сумісне з багатьма ОС) та оптимізованістю (має мінімальний вплив на загальну продуктивність системи). Його використовують великі корпорації, уряди, фінансові інституції та інші різноманітні особи, що оперують чутливою інформацією та зазнають регулярних кібератак.

У ролі IPS рішення було обрано Snort, безкоштовну NIPS (мережо-орієнтовану IPS), яка призначена для аналізу пакетів даних в комп'ютерній мережі, виявляти або блокувати спроби проникнень або атак. Дуже корисна у виявленні добре прихованих атак, таких як, наприклад, backdoor-закладки.

Для ілюстрації комплексного IDPS (Intrusion Detection & Prevention Systems) рішення, обрано Palo Alto Networks Threat Prevention.

Цей продукт встановлений у кожен новий брандмауер нового покоління, вони видаються під назвою PA-Series. На рисунку 1.5 зображений користувацький інтерфейс для роботи з даними, що надходять на сервер збору даних з підключених агентів. В цьому випадку – наведені програми, які встановлені в найбільшої кількості користувачів та загальну кількість даних, яку вони вивантажили та завантажили на робочі машини, а також рівень ризику та категорію цих програм.

Інструмент пропонує захисні компоненти на прикладному та мережевому рівнях, використовуючи власну базу сигнатур, алгоритми виявлення зловмисно модифікованих пакетів даних.

Використовуючи цю IDPS адміністратори можуть сканувати весь трафік у мережі, застосовувати правила Snort та Suricata (open-source NIDS/NIPS моніторинговий рушій), використовувати вбудовані політики безпеки, які регулярно оновлюються.

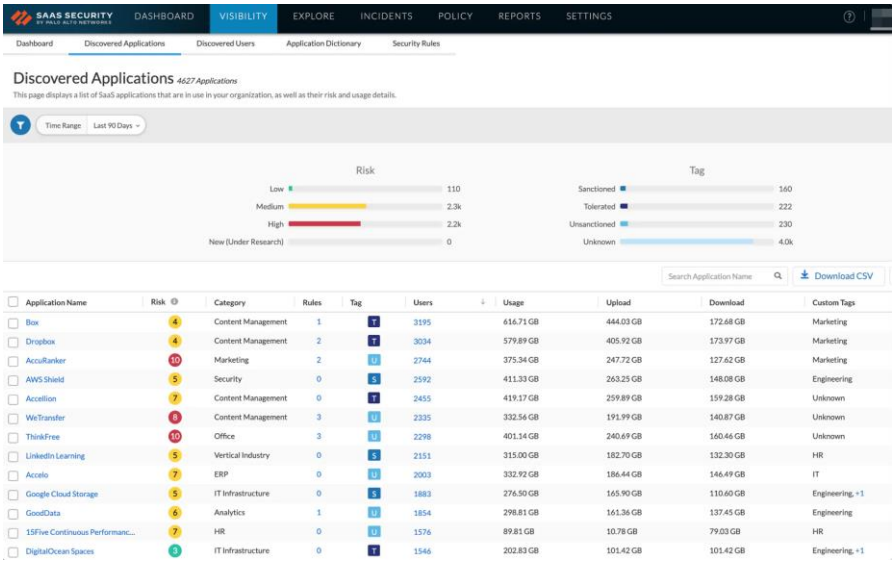


Рисунок 1.5 – Користувацький інтерфейс IDPS від Palo Alto

Як безкоштовну альтернативу Palo Alto Networks Threat Prevention розглянемо, раніше згадану, Suricata, яка є IDPS рішенням спрямованим на захист мережі. Усю зібрану інформацію система відображає за допомогою зручного користувацького інтерфейсу (рис. 1.6), який дозволяє створювати комплексні панелі з кількома видами графіків та метрик для відстеження основних тенденцій мережевої, користувацької та програмної активності в інфраструктурі. Також присутній функціонал пошуку спільних ознак одного інцидента у подіях з різних пристроїв та джерел надходження логів подій. Suricata є більш вузькопрофільним інструментом, що є цілком логічним, адже розвитком Suricata займається команда розробників з некомерційної спільноти Open Information Security Foundation (OISF). Серед основних особливостей:

- сумісність з великим переліком провідних рішень безпеки, можливість інтеграції у деякі з них (наприклад Wazuh та Elastic Stack);
- можливість реєструвати всі HTTP запити, всі DNS запити на відповіді, обміни TLS ключами та відфільтровувати файли з потоків трафіку, зберігаючи їх на цифрових носіях;
- для своїх IDP/IPS функцій використовує широку вибірку сигнатур, які відповідають відомим загрозам та зловмисній поведінці;

- здатна виявляти аномалії у досліджуваному трафіку, які можуть свідтичи про спроби експлуатувати вразливість системи;
- здатна використовувати набори правил (rulesets) ET та VRT;
- має мінімальний вплив на продуктивність системи та має зрозумілу та добре коментовану базу програмного коду;
- здатна автоматично виявляти протоколи на портах та застосовувати відповідну логіку виявлення потенційних зловмисних спроб підключення та вразливих каналів комунікації з мережею.

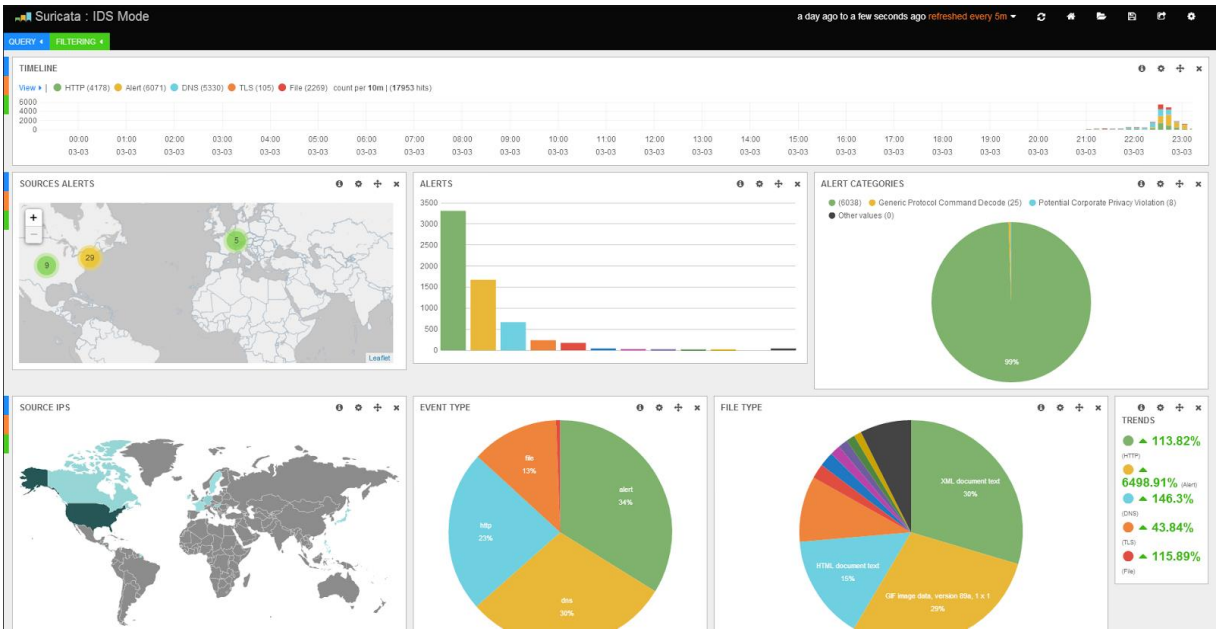


Рисунок 1.6 – Користувацький веб-інтерфейс панелі Suricata

Особливої уваги заслуговує безкоштовна open-source XDR (Extended detection and response) та SIEM (Security information and event management) платформа Wazuh. З першого погляду, вона зовсім не підходить для вимог, які мали б задовільнити IDS/IPS рішення, адже у базовій конфігурації не заявлений функціонал, який ми бачимо у інструментах безпеки, розглянутих раніше.

Проте, серед основних особливостей Wazuh – її здатність до модифікації, приємний та інтуїтивний інтерфейс, зрозуміла документація та сумісність з найпоширенішими операційними системами. Таким чином, цей інструмент може не лише використовуватись як IDS/IPS а й бути чудовим додатком і

альтернативною точкою перспективи для опрацювання інцидентів у випадках, коли у інфраструктурі вже розгорнуте подібне рішення безпеки.

По черзі розглянемо яким саме чином Wazuh можна використовувати як систему виявлення вторгнень та як систему запобігання вторгненням. Основним інструментом моніторингу машин в комп'ютерній мережі є Wazuh Agent – це програмне забезпечення, яке збирає інформацію про активність на встановленому суб'єкті. Ця програма здатна виявляти:

- підозрілу активність;
- шкідливе програмне забезпечення (в тому числі, на основі сигнатур);
- приховані файли;
- факти несанкціонованого прослуховування портів;
- збирати log-файли (облікові журнали базових служб та сервісів на машині) та аналізувати їх за допомогою власного regex-рушія (допомагає відфільтровувати потрібну інформацію опираючись на джерело log-файлу і знаючи шаблон вигляду записів у таких файлах);
- сканувати програмне забезпечення на машині та сповіщати про знайдені вразливості опираючись на відкриті бази на кшталт CVE.

Однією з найважливіших функцій IDS систем є можливість сповіщати адміністратора про ознаки зловмисного впливу на мережу. Налаштування сповіщень Wazuh дозволяє створювати власні фільтри і тригери (умови спрацювання сповіщення).

Для того ж щоб використовувати Wazuh як IPS, існує Active response. Це вид програм (скриптів), який можна призначити для запуску під час спрацьовування певних сповіщень, а саме – їх тригерів. Базова комплектація містить в собі мінімально необхідний набір готових програм для адміністрування робочих станцій та невеликих серверних машин. Серед дій, на які здатні такі скрипти:

- блокування певного аккаунту в локальній мережі;

- додавання зовнішніх IP адрес до списків блокування та дроп-списків брандмауера;
- додавання IP адрес у списки блокування машин в локальній мережі;
- автоматичне перезавантаження серверних одиниць (включаючи Wazuh-сервер) після виявлення факту зміни конфігураційних файлів;

Як бачимо, завдяки функції Active response, Wazuh набуває ознак доволі варіативної системи запобігання проникненню. Ця варіативність досягається можливістю підключення різних індексів до загальної системи моніторингу, тобто джерел отримання лог-файлів та інших записів від служб та пристроїв. Таким чином, обсяг інформації, яку буде обробляти Wazuh та реагувати на неї, обмежується лише обчислювальними можливостями Wazuh Server'а (машини, за допомогою якої отримується і обробляється інформація передана Wazuh Agent'ами) і креативністю адміністратора при створенні тригерів для реагування на підозрілу активність.

2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Інфраструктура Wazuh для вирішення проблем захисту інформації в ІКС

Для збору, аналізу та обробки інформації в ІКС Wazuh використовує модель у якій одна з машин виступає Wazuh Manager'ом, а інші Wazuh Agent'ами. Тобто, Manager отримує дані зібрані Agent'ами, обробляє їх та відображає у панелі адміністратора (за замовчуванням Wazuh використовує Kibana). Таким чином, щоб приступити до роботи нам потрібно обрати машину, що буде виступати Wazuh Manager'ом та підключити до неї машини зі встановленим Wazuh Agent для збору даних. Називатимемо ці ролі менеджером та агентом відповідно, для спрощення посилання на вид програмного забезпечення встановленого на машину та функцій, які вона буде виконувати.

Отже, менеджером у нашій інфраструктурі виступатиме віртуальна машина WazuhManager1, яку буде розгорнуто у середовищі віртуалізації VMware, адже документація Wazuh містить посилання на уже готовий файл типу .OVA, що дозволить розгорнути менеджер без зайвих зусиль.

У ролі першого тестового агента обрано основну машину VLADYSLAV_POLISHCHUK з встановленою операційною системою Windows 10. Для цього ми встановимо відповідне програмне забезпечення посилаючись на офіційну документацію розробників Wazuh. На рисунку 2.1 зображені основні структурні компоненти.

Вивчаючи, схему на рисунку 2.1 можна помітити, що включає, та які функції виконує відповідне програмне забезпечення на стороні сервера та на стороні агента. Агент збирає інформацію з машини, на яку встановлений та передає її серверу, де вона обробляється та надсилається наступним суб'єктам системи моніторингу. Аналітичний рушій (Analysis engine) здатний виявляти вразливості та загрози. Крім того, дані паралельно надходять до інструменту відображення (Dashboard) та пошукового рушія (Indexer), яким виступає

Elasticsearch. Працюючи разом, ці два компонента дозволяють нам бачити, сортувати та шукати інформацію в користувацькому інтерфейсі Kibana.

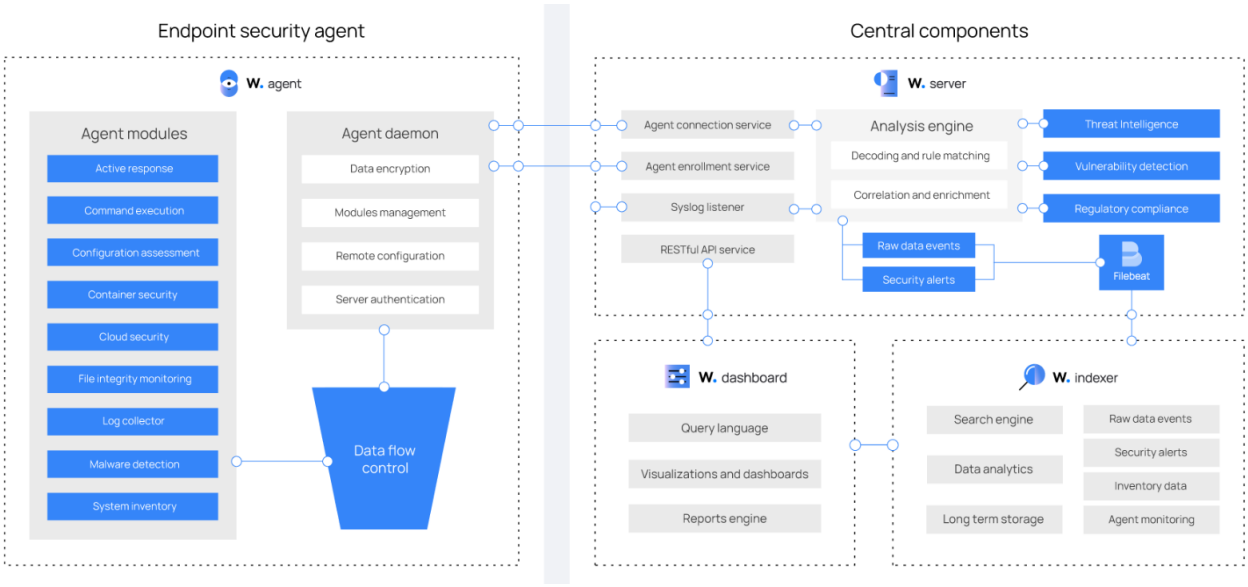


Рисунок 2.1 – Схема інфраструктури Wazuh

Розглянемо кожен з компонентів детальніше для кращого розуміння, як вони працюватимуть разом, та чим є кожен зокрема.

Wazuh Indexer (далі також – індексатор) – це система текстового пошуку та аналізу даних [19]. Індекси є основною одиницею категоризації джерел даних, зібраних сервером (Wazuh server), в моделі ELK-стаку, що включає:

- Elasticsearch – пошуковий рушій для роботи із зібраними даними з агентів;
- Kibana – інструмент відображення впорядкованих даних та взаємодії з ними шляхом пошуку і формування графіків та діаграм;
- Logstash – серверний канал даних, що дозволяє отримувати записи подій з різних джерел, фільтрувати і змінювати їх до вигляду, що придатний для читання і пошуку.

Отже, індекс – це набір, пов’язаних між собою, даних, що зберігаються та обробляються в індексаторі. Індексатор зберігає всі дані про події, як документи JSON. Кожен з цих документів містить набір ключів, що є іменами

полів, та відповідних їм значень, які можуть бути текстовими рядками, числами, булевими значеннями, датами, IP-адресами, географічними координатами та багатьма іншими типами даних. Wazuh пропонує набір індексів для збору найменш необхідних даних за замовчуванням, але також є можливість реєстрації документів і з інших джерел. Події з таких сервісів надходять у «сирому» вигляді, який часто непридатний для читання без попереднього ознайомлення з документацією відповідного сервісу. Для таких випадків є можливість налаштування користувацьких фільтрів для цих документів. За допомогою яких, ми отримаємо структурований JSON-документ, з відповідними ключами (заданими в фільтрі) та типами даних і значеннями, які є відповідниками цих ключів. Для цих цілей зручно використовувати GrokFilter, інструмент, який допомагає перетворити неструктуровані дані в лаконічний і придатний, для роботи, вигляд (рис. 2.2). Він має свій набір фільтрів для різних типів даних, серед них:

- електронна адреса;
- числові типи (десяткові, шістнадцяткові цілі та з плаваючою точкою);
- MAC-адреси;
- IP-адреси (IPv4, IPv6);
- шлях до файлу (Windows та Unix видів);
- URI шляхи;
- формати дати та часу (ISO8601, американський та європейський вид запису дат, syslog-дати та інші).

Приклад використання такого фільтру зображено на рисунку 2.1.2.

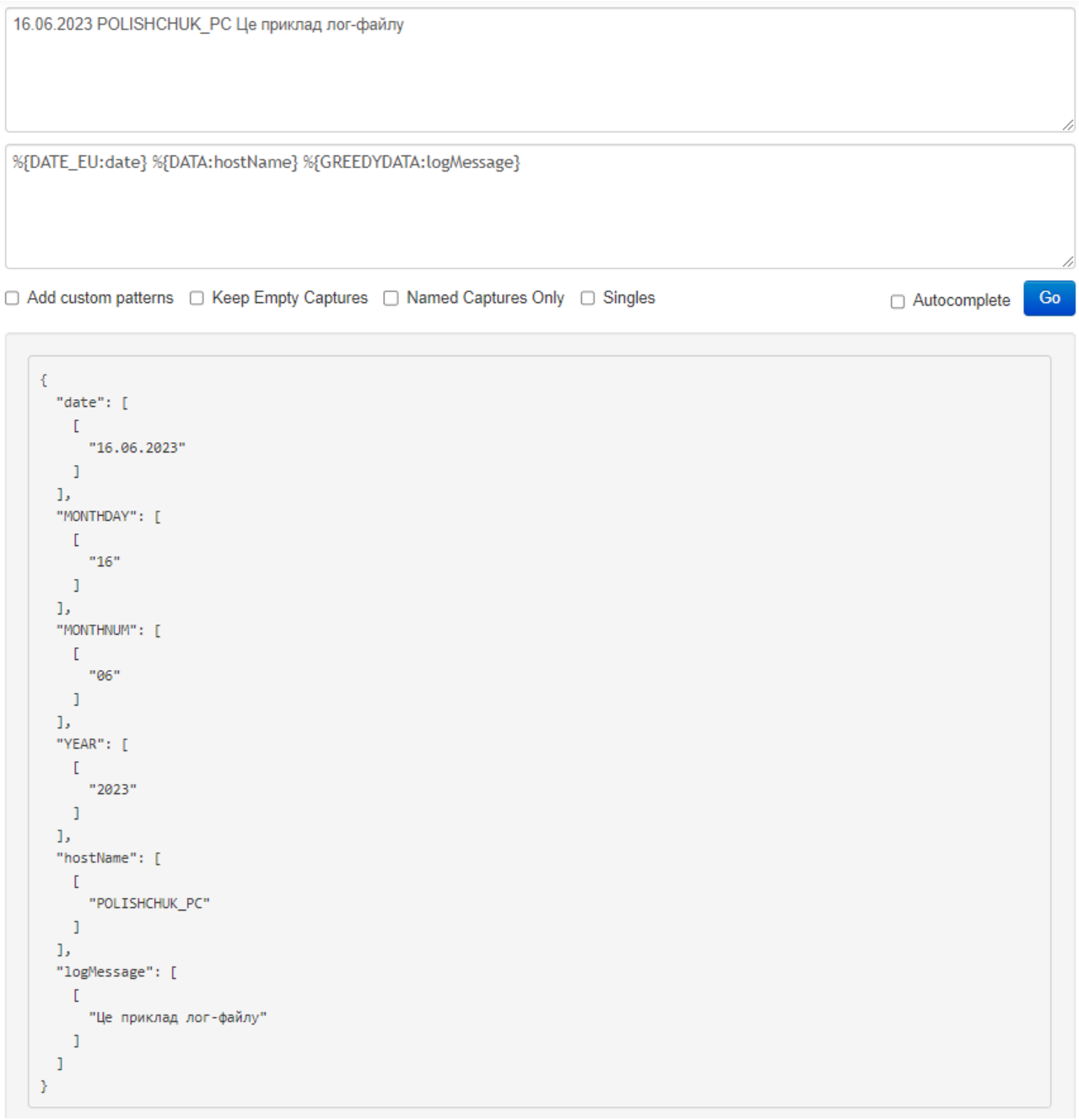


Рисунок 2.2 – Використання GrokFilter

Користуючись термінологією, яку пропонує Elasticsearch, сам Wazuh indexer є кластером (cluster), який містить в собі декілька індексів, тобто джерел або видів документів про події. Кожен кластер, а в нашому випадку – Wazuh indexer, складається з вузлів (node). Вони містять самі фрагменти документів про події, так звані, осколки (shard). Використання таких осколків дозволяє забезпечити постійну доступність та безперебійність роботи системи. Це можливо, завдяки зберіганню на кожному вузлі первинних та вторинних

осколків (осколків-реплік), первинні екземпляри яких можуть зберігатись на інших вузлах, таким чином ми отримуємо доступ до даних не залежно від того чи всі вузли одночасно є справними. Таким чином, кожен окремий вузол зберігає достатню кількість осколків (повний обсяг зібраної інформації) для безпроблемної роботи аналітика. На рисунку 2.3 зображена логічна топологія Wazuh indexer.

На практиці, індексатор реєструє документи подій надзвичайно швидко, затримка між подією та її відображенням у панелі моніторингу, зазвичай, складає одну секунду. Це дозволяє вчасно обробляти та реагувати на інциденти. Співвідносити часові мітки на документах, що відображаються в панелі та у log-файлах (журналах обліку подій в системі), що зберігаються на пристрої.

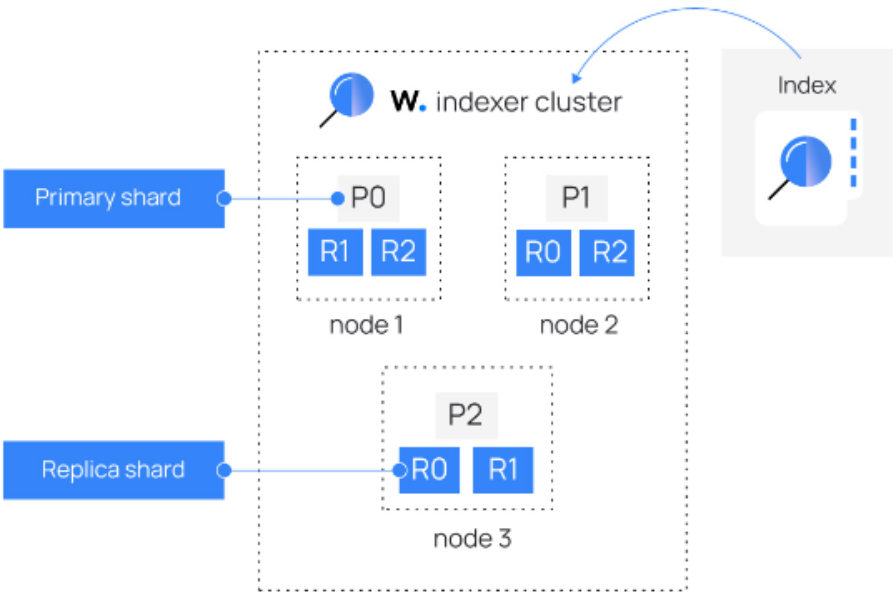


Рисунок 2.3 – Логічна топологія Wazuh indexer

Далі розглянемо компонент Wazuh Server, що аналізує дані, отримані від агентів, та активує відповідні сповіщення, коли виявляються загрози або аномалії, що є чіткою ознакою систем виявлення проникнень (IDS) [19]. Також він використовується для віддаленого керування конфігурацією агентів та моніторингу їх статусу, що, в свою чергу, є вже функцією систем запобігання

проникнень (IPS).

Сервер Wazuh використовує публічні бази відомих загроз для покращення своїх можливостей виявлення. Він також збагачує дані про умови спрацювання сповіщень, використовуючи фреймворк MITRE ATT&CK та вимоги щодо регулювання в області відповідності, такі як PCI DSS, GDPR, HIPAA, CIS та NIST 800-53, що надає корисний контекст для аналізу безпеки [19].

Архітектура сервера працює на рушії аналізу, RESTful API Wazuh, службі реєстрації агентів, службі підключення агентів, демоні кластера Wazuh та Filebeat. Сервер встановлюється на операційній системі Linux та зазвичай працює на фізичному сервері, віртуальній машині, контейнері Docker або екземплярі хмари. На рисунку 2.4 представлена архітектура сервера.

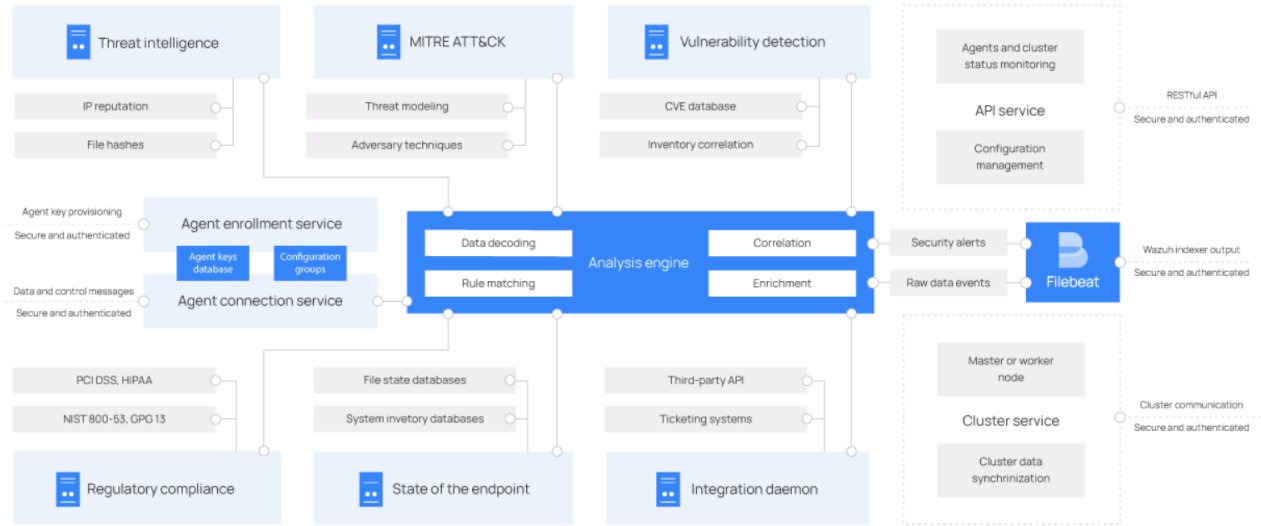


Рисунок 2.4 – Схема архітектури сервера Wazuh

Сервер Wazuh складається з кількох компонентів, перерахованих нижче, які мають різні функції, такі як реєстрація нових агентів, перевірка ідентичності кожного агента та шифрування зв'язку між агентом Wazuh та сервером Wazuh:

- служба реєстрації агентів: вона використовується для реєстрації нових агентів. Ця служба надає та розподіляє унікальні ключі автентифікації для

кожного агента. Процес виконується як мережева служба та підтримує аутентифікацію через сертифікати TLS/SSL або надання фіксованого пароля;

- служба підключення агентів: ця служба отримує дані від агентів. Вона використовує ключі, якими діляться служба реєстрації, для перевірки ідентичності кожного агента та шифрування зв'язку між агентом Wazuh та сервером Wazuh. Крім того, ця служба надає централізоване керування конфігурацією, що дозволяє віддалено надсилати нові налаштування агента;
- рушій для аналізу: це серверний компонент, який виконує аналіз даних. Він використовує декодери для визначення типу оброблюваних даних (події Windows (event log), журнали SSH (ssh log), журнали (log) веб-сервера та інші). Ці декодери також витягують важливі елементи даних з повідомлень журналу, такі як IP-адреса джерела запиту, ідентифікатор події або ім'я користувача. Потім, за допомогою правил, двигун визначає певні шаблони в розшифрованих подіях, які можуть спричинити спрацювання відповідних сповіщень і, можливо, навіть вдатись до автоматичних заходів захисту (наприклад, блокування IP-адреси, зупинка виконання процесу або видалення шкідливого програмного забезпечення).
- RESTful API Wazuh: ця служба надає інтерфейс для взаємодії з інфраструктурою Wazuh. Вона використовується для керування налаштуваннями агентів та серверів, моніторингу загального стану інфраструктури, керування та редагування декодерів та правил Wazuh, а також запитування стану конкретних користувацьких машин, що відстежуються;
- демон кластера Wazuh: ця служба використовується для горизонтального масштабування серверів Wazuh, розгортання їх у вигляді кластера. Такий тип конфігурації, спільно з балансувальником навантаження мережі, забезпечує високу доступність та балансування навантаження. Демон кластера Wazuh використовується для забезпечення комунікації між серверами Wazuh та для їх синхронізації;
- Filebeat: він використовується для надсилання подій та тривог

індексатору Wazuh. Він зчитує вивід рушія аналізу Wazuh та надсилає події в реальному часі. Крім того, він забезпечує балансування навантаження при підключенні до кластера індексаторів Wazuh з кількома вузлами (nodes).

Наступним розглянемо Wazuh Dashboard. Інтерфейс користувача Wazuh є гнучким та інтуїтивно зрозумілим веб-інтерфейсом для перегляду, аналізу та візуалізації даних про події та тривоги в галузі безпеки (рис. 2.5). Він також використовується для управління та моніторингу платформи Wazuh. Крім того, він надає функції контролю доступу на основі ролей (RBAC) та одноразового входу (SSO) [19].

Візуалізація та аналіз даних. Веб-інтерфейс допомагає користувачам навігувати через різні типи даних, зібраних агентом Wazuh, а також через безпекові тривоги, що генеруються сервером Wazuh. Користувачі також можуть генерувати звіти та створювати власні візуалізації та панелі інструментів. Налаштування таких сторінок дозволяють додавати таблиці, діаграми та інші елементи візуалізації.

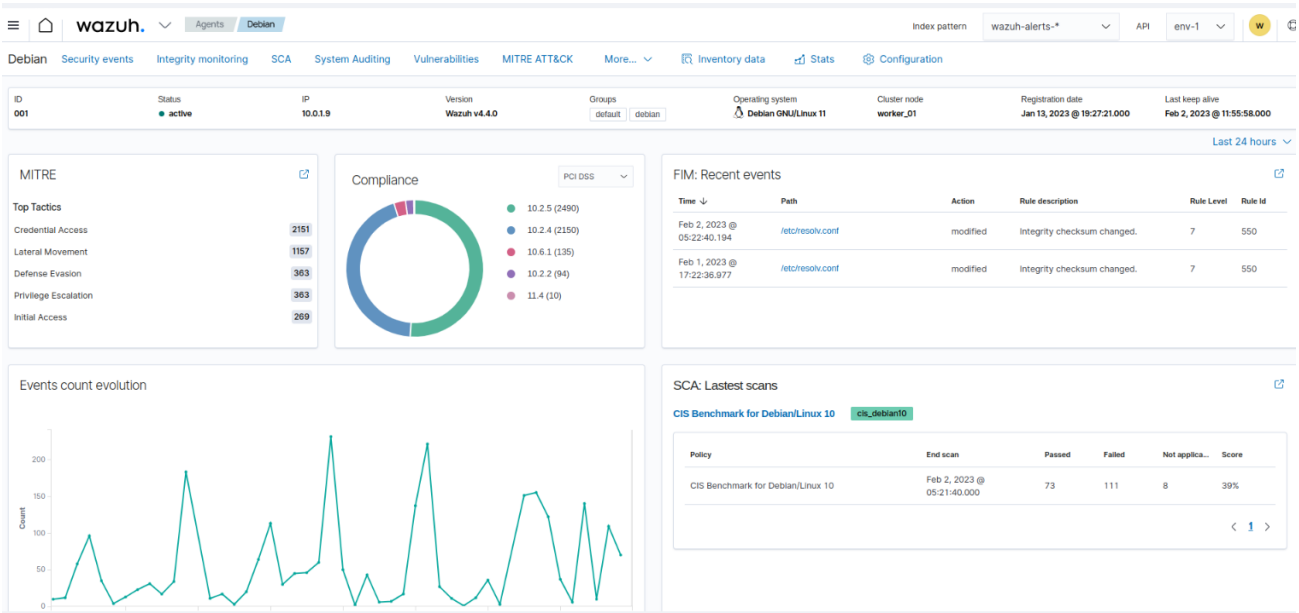


Рисунок 2.5– Користувацький інтерфейс сторінки візуалізації з інформацією про один конкретний агент

На приклад, Wazuh надає готові панелі інструментів для відповідності до

регуляторних вимог, таких як PCI DSS, GDPR, HIPAA та NIST 800-53. Також надається інтерфейс для навігації по фреймворку MITRE ATT&CK та пов'язаних тривог (рис. 2.6) [19].

Моніторинг та конфігурація агентів. Інтерфейс користувача Wazuh дозволяє користувачам керувати конфігурацією агентів та моніторити їх статус. Наприклад, для кожної кінцевої точки, яку моніторять, користувачі можуть визначити, які модулі агента будуть активовані, які журнали будуть прочитані, які файли будуть моніторитися на зміни цілісності або які перевірки конфігурації будуть виконуватися.

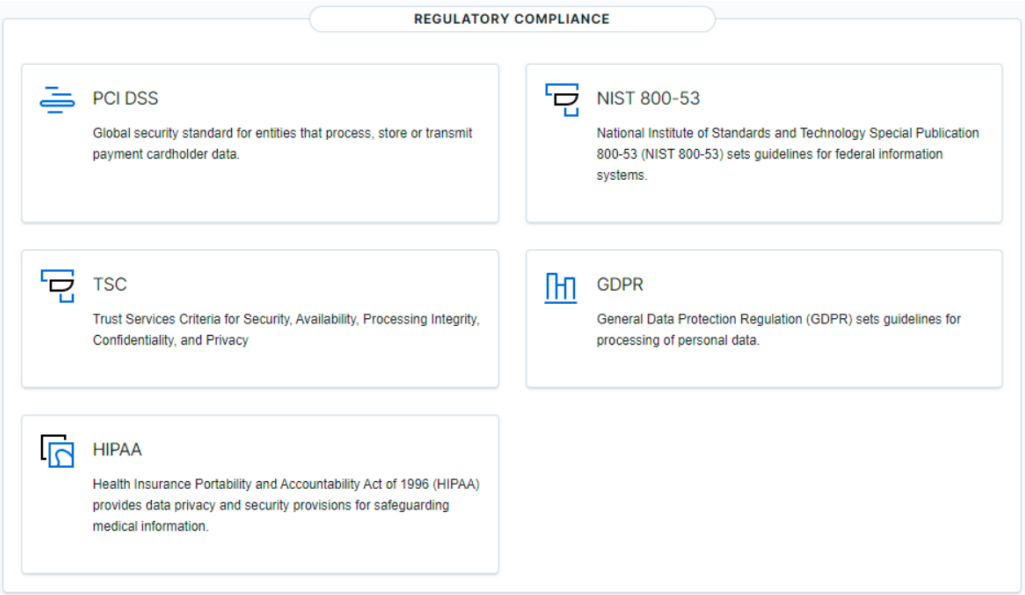


Рисунок 2.6 – Регуляторні вимоги в панелі керування Wazuh Dashboard

Останній компонентом слід розглянути Wazuh Agent. Агент Wazuh сумісний з Linux, Windows, macOS, Solaris, AIX та іншими операційними системами. Він може бути розгорнутий на ноутбуках, робочих станціях, серверах, хмарних інстанціях, Docker-контейнерах або віртуальних машинах. Агент допомагає захистити систему, забезпечуючи можливості запобігання, виявлення та реагування на загрози, що ознаками IDS/IPS. Він також використовується для збору різних типів даних про систему та додатки, які він передає на сервер Wazuh через зашифрований та автентифікований канал.

Агент Wazuh має модульну архітектуру. Кожен компонент відповідає за свої завдання, включаючи моніторинг файлової системи, читання журналів (log-файлів), збір даних інвентаризації, сканування конфігурації системи та пошук шкідливих програм. Користувачі можуть керувати модулями агента за допомогою налаштувань конфігурації, пристосовуючи рішення до своїх конкретних випадків використання [19]. Діаграма на рисунку 2.7 зображує архітектуру та компоненти агента.

Рисунок 2.7 – Схема архітектури агента Wazuh

Всі модулі агента налаштовувані і виконують різні безпекові завдання. Ця модульна архітектура дозволяє вам увімкнути або вимкнути кожен компонент залежно від ваших потреб у безпеці. Нижче наведені різні цілі всіх модулів агента:

- збиральник логів (Log collector): Цей компонент агента може читати облікові журнали подій встановлених служб та події Windows (Event log), збираючи повідомлення логів операційної системи та додатків. Він підтримує фільтри XPath для подій Windows та розпізнає багаторядкові формати, такі як логи Linux Audit;
- виконання команд (Command execution): Агенти періодично виконують авторизовані команди, збирають їх вивід та повідомляють про це на

сервер Wazuh для подальшого аналізу. Можна використовувати цей модуль для різних цілей, таких як моніторинг вільного місця на жорсткому диску або отримання списку останніх ввійшовших користувачів;

- моніторинг цілісності файлів (File Integrity Management або FIM): Цей модуль моніторить файлову систему та повідомляє про створення, видалення або зміни файлів. Він відстежує зміни атрибутів файлів, дозволів, власності та вмісту. Коли відбувається подія, він фіксує деталі "хто, що і коли" в реальному часі. Крім того, модуль FIM будує та підтримує базу даних із станом моніторованих файлів, що дозволяє виконувати запити віддалено;
- оцінка конфігурації безпеки (Security configuration assessment або SCA): Цей компонент забезпечує постійну оцінку конфігурації, використовуючи вбудовані методи перевірки на основі стандартів Центру Безпеки інтернету (CIS). Користувачі також можуть створювати власні перевірки SCA для моніторингу та забезпечення своїх політик безпеки;
- інвентаризація системи (System Inventory): Цей модуль агента періодично запускає сканування, збираючи дані інвентаризації, такі як версія операційної системи, мережеві інтерфейси, активні процеси, встановлені програми та список відкритих портів. Результати сканування зберігаються в локальних базах даних SQLite, до яких можна отримати доступ віддалено;
- виявлення шкідливих програм (Malware Detection): За допомогою підходу, не основаного на сигнатурах, цей компонент може виявляти аномалії та можливу наявність rootkit-ів. Він також виявляє приховані процеси, приховані файли та захищені порти під час моніторингу системних викликів;
- активне реагування (Active Response): Цей модуль автоматично виконує дії при виявленні загроз, викликаючи реакції для блокування мережевого з'єднання, зупинки виконання процесу або видалення шкідливого файлу. Користувачі також можуть створювати власні реакції за потреби та налаштовувати, наприклад, реакції на виконання бінарного файлу у «пісочниці» (ізольованому середовищі для тестування), захоплення мережевого трафіку та

сканування файлу з антивірусом;

- моніторинг безпеки контейнерів (Container Security Monitoring): Цей модуль агента інтегрований з API Docker Engine для моніторингу змін в середовищі контейнерів. Наприклад, він виявляє зміни в образах контейнерів, конфігурації мережі або обсягах даних. Крім того, він попереджує про контейнери, що працюють у привілейованому режимі, і про користувачів, що виконують команди у працюючому контейнері;
- моніторинг безпеки хмари (Cloud Security Monitoring): Цей компонент моніторить машини, що орендуються на хмарних платформах, такі як Amazon AWS, Microsoft Azure або Google GCP. Він взаємодіє з їх API. Може виявляти зміни в інфраструктурі хмари (наприклад, створення нового користувача, зміна групи безпеки, успішний доступ до привілейованого режиму, використання користувачами команд від імені адміністратора тощо) та збирати логи цих хмарних сервісів (наприклад, AWS Cloudtrail, AWS Macie, AWS GuardDuty, Azure Active Directory тощо).

Агент Wazuh комунікує з сервером Wazuh для надсилання зібраних даних та подій, пов'язаних з безпекою. Крім того, агент надсилає оперативні дані, повідомляючи про свою конфігурацію та статус. Після підключення агента можна оновлювати, моніторити та налаштовувати віддалено з сервера Wazuh.

Зв'язок агента з сервером відбувається через безпечний канал (TCP або UDP), забезпечуючи шифрування та стиснення даних в режимі реального часу. Крім того, він включає механізми контролю потоку даних, щоб уникнути переповнення, чергуючи події при необхідності та захищаючи пропускну здатність мережі.

Перед підключенням агента до сервера вам потрібно зареєструвати агента, що надасть йому унікальний ключ для аутентифікації та шифрування даних.

2.2 Налаштування системи Wazuh для виявлення та запобігання проникнень

Для подальшого тестування нашої системи на спроможність успішно виявляти та сповіщати адміністратора ІКС про проникнення в мережу, нам потрібні машини, на які ми встановимо Wazuh Agent та Wazuh Server.

Спершу встановимо сервер Wazuh щоб мати готову платформу, до якої вже потім можна буде підключати довільну кількість агентів, хоча в рамках цього дослідження, буде достатньо і одного агента.

Wazuh Server можна встановити кількома способами, основний з яких це встановлення його як пакету на вже функціонуючу операційну систему Linux. Для цього потрібно проводити процес встановлення та конфігурації усіх служб власноруч. Але є і альтернативні способи встановлення, одним з яких, є встановлення Wazuh Server на віртуальну машину за допомогою завантаженого OVA-файлу на дистрибутиві CentOS 7. Цей файл можна розгорнути в середовищі віртуалізації як вже налаштовану систему готову для роботи.

Як середовище віртуалізації було обрано VMware Workstation 17 Player. Воно не має кардинальних відмінностей від альтернатив, на кшталт VirtualBox, але все ж має достатній функціонал для ілюстрування основних особливостей віртуальних машин, які будуть встановлюватись в рамках цього дослідження.

Для встановлення OVA-образу, спершу завантажимо його за посиланням в документації Wazuh. Далі в користувацькому інтерфейсі середовища віртуалізації обираємо «Відкрити віртуальну машину», даємо їй ім’я та директорію, в якій будуть зберігатись файли нової віртуальної машини. Після запуску нас зустрічає інтерфейс командної строки та запитує дані для входу, які можна знайти в документації.

Після вводу даних для входу ми потрапляємо в термінал керування сервером, де можна перевірити IP-адресу веб-панелі керування, яку ми будемо використовувати для роботи з агентами, сповіщеннями та зібраними даними. У виводі команди «ip a» бачимо, що на інтерфейсі eth0 налаштована IP-адреса

192.168.110.128, за якою ми і отримаємо доступ до панелі. На рисунку 2.8 зображено вивід цієї команди.

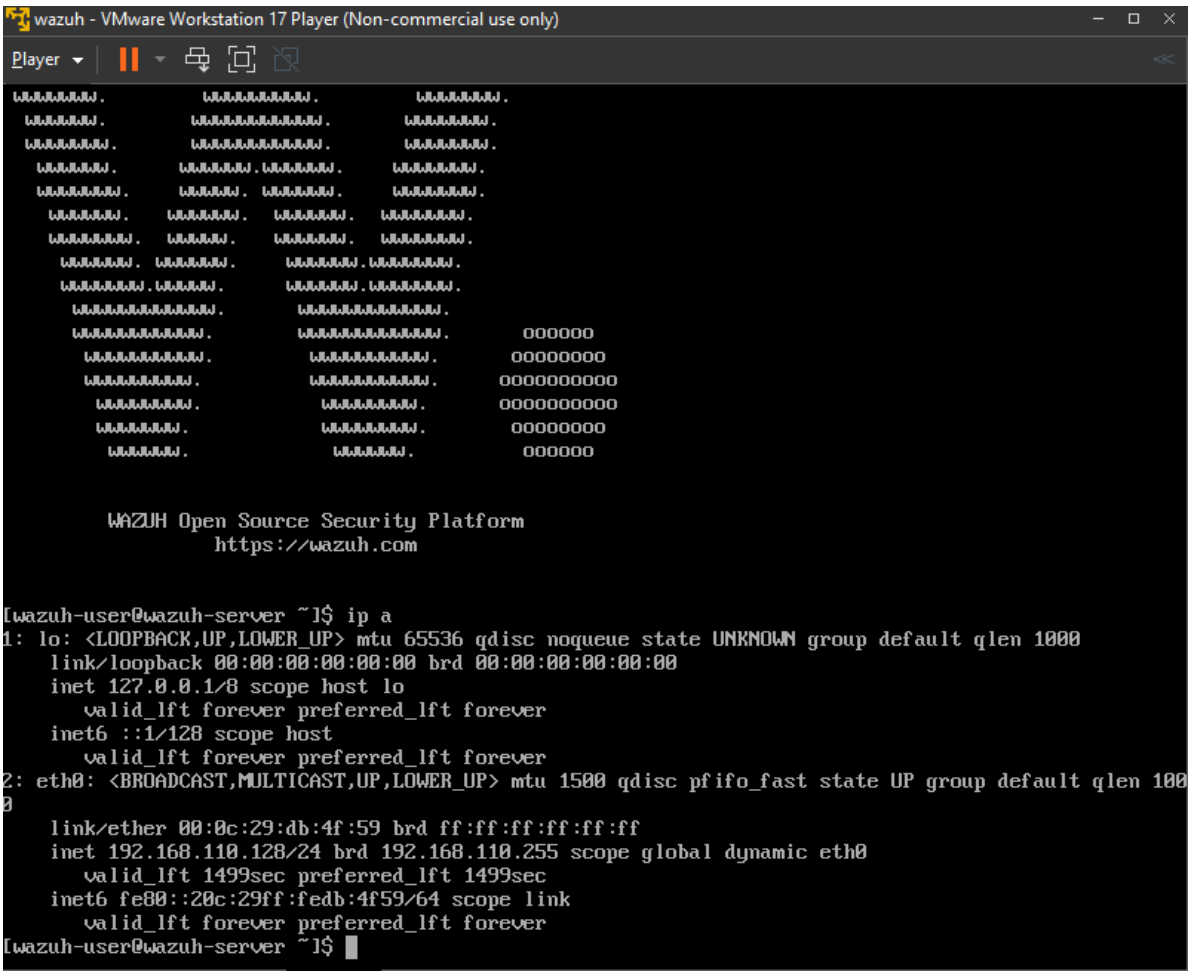


Рисунок 2.8 – Командний рядок для роботи з Wazuh Server

Отже, щоб перейти до панелі керування введемо 192.168.110.128 у адресне поле веб-браузера (в даному випадку був використаний Google Chrome). Тільки важливо перед IP-адресою вказати протокол HTTPS, адже спроби використати HTTP будуть невдалими, це ми можемо довести, перевіривши TCP-з’єднання на портах цих служб у командному рядку PowerShell (рис. 2.9).

```
PS C:\Users\Admin> Test-NetConnection 192.168.110.128 -port 80
WARNING: TCP connect to (192.168.110.128 : 80) failed


ComputerName            : 192.168.110.128
RemoteAddress           : 192.168.110.128
RemotePort              : 80
InterfaceAlias          : VMware Network Adapter VMnet8
SourceAddress           : 192.168.110.1
PingSucceeded           : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False



PS C:\Users\Admin> Test-NetConnection 192.168.110.128 -port 443


ComputerName     : 192.168.110.128
RemoteAddress    : 192.168.110.128
RemotePort       : 443
InterfaceAlias   : VMware Network Adapter VMnet8
SourceAddress    : 192.168.110.1
TcpTestSucceeded : True
```

Рисунок 2.9 – Перевірка з’єднання на портах служб HTTP та HTTPS відповідно

Таким чином, панель керування Wazuh, в нашому випадку, доступна за «https://192.168.110.128». Перейшовши за цьою URL-адресою ми потрапляємо на форму для входу в адмін-панель. Ім’я користувача та пароль вказані в документації та обидва дорівнюють «admin». Після успішної автентифікації ми потрапляємо на домашню сторінку панелі (рис. 2.10), де нам одразу пропонується підключити агентів для моніторингу, а також продемонстровані основні функції, та сконфігуровані заздалегідь запити до бази зібраних даних, за якими можн відфільтувати бажану категорію подій, наприклад – вразливості (за категоризацією MITRE) або події про зміну, додавання, видалення та іншої взаємодії з файлами в системі агента.

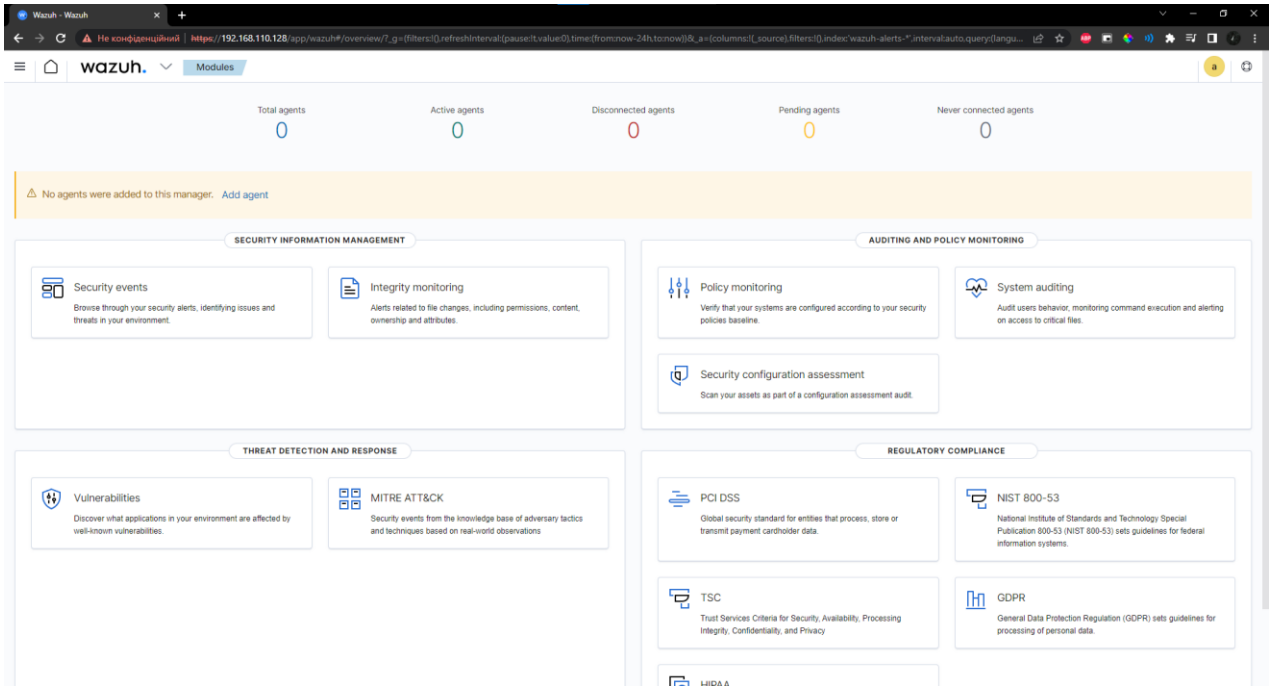


Рисунок 2.10 – Адміністративна панель керування Wazuh

Далі перейдемо до встановлення Wazuh Agent на мою основну систему. Для цього потрібно встановити відповідне програмне забезпечення для Windows, посилання для завантаження можна знайти в документації з встановлення Wazuh.

Встановлення займає декілька хвилин та реалізується через зручну утиліту з графічним інтерфейсом. Після вставовлення треба запустити графічний інтерфейс самого агента, і вказати IP-адресу Wazuh Manager’a (яка і є адресою нашого Wazuh Server, тобто 192.168.110.128) і автентифікаційний ключ. Але є і простіший спосіб підключення агентів до панелі. Якщо перейти за гіпер-покликанням «Add agent», яке зображене на рисунку 2.2.3, можна потрапити на сторінку підключення, де після надання усіх потрібних відомостей про агента та його пристрій, буде згенерована команда, яку потрібно виконати у терміналі PowerShell, а після цього запустити відопвідний сервіс. На рисунку 2.11 зображена сторінка підключення з вже наданими даними про агента.

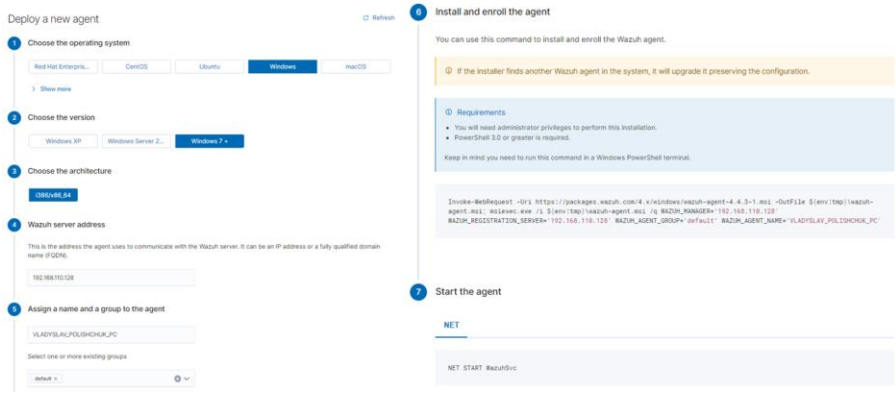


Рисунок 2.11 – Форма для надання відомостей про агента для подальшого підключення

І після слідування всім крокам в згаданій сторінці підключенн, ми бачимо нашу машину у списку агентів, як активну (рис. 2.12).

У цій панелі також можна переглядати список підключених агентів, бачити їх статус підключення, експортувати список цих агентів (у форматі .csv) для подання звітності та перегляду детальнішої інформації про останні події на агенті натисканням на його назву в таблиці підключених агентів або на іконку ока в стовпці дій.

Серед цих дій можна переглядати налаштування моніторингу політик безпеки, лог-файлів, реєстрація подій Windows (Event log) та інші аспекти, інформацію про які здатний збирати Wazuh Agent.

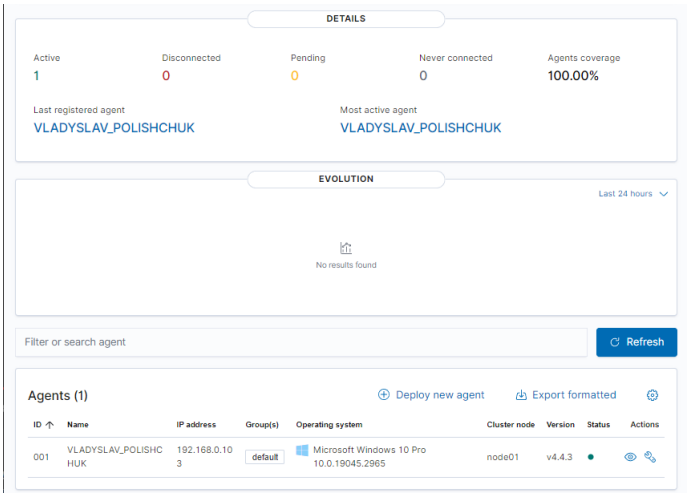


Рисунок 2.12 – Список та статус підключених агентів

Проте для ролі жертви (цілі тестових атак) було обрано віртуальну машину на Windows 10, яка дуже подібна до основної системи, але більш ізольована та буде знаходитись у одній підмережі (192.168.110.0/24) з потенційним зловмисником, що імітуватиме реальні умови.

2.3 Налаштування системи потенційного зловмисника

Тепер налаштуємо машину, яка буде відігравати роль системи потенційного зловмисника для імітації реальних кібератак. У такий спосіб, ми зможемо протестувати систему сповіщення та реагування на інциденти в умовах, наближених до реальних. Операційною системою для таких цілей була обрана Kali Linux.

Kali Linux – це спеціалізована операційна система, розроблена для забезпечення тестування на проникнення і безпеку комп'ютерних систем. Вона базується на дистрибутиві Debian Linux і має вбудований набір інструментів для проведення аудиту безпеки, тестування вразливостей, відновлення паролів та багато іншого.

Система надає доступ до більш як 600 інструментів для виконання різноманітних завдань, пов'язаних з безпекою і проникненням. Ці інструменти охоплюють різні аспекти, такі як сканування портів, виявлення вразливостей, злам паролів, перехоплення пакетів, аналіз безпеки мережі, сканування веб-застосунків та інші.

Kali Linux стала дуже популярною серед фахівців з безпеки і етичних хакерів, оскільки він надає потужні інструменти та ресурси для тестування та оцінки безпеки систем. Він також використовується у навчальних цілях, де студенти можуть отримати практичний досвід роботи з різними аспектами безпеки.

Крім того, Kali Linux також має велику спільноту користувачів і розробників, яка надає підтримку, оновлення та розширення системи. Вона постійно оновлюється з новими інструментами та допрацюваннями в цілях

безпеки, що робить її потужним і актуальним інструментом для безпекових досліджень.

Важливо відзначити, що використання Kali Linux повинно здійснюватися з дозволу власника системи або з уповноваження в рамках етичного хакінгу та безпекового аудиту. Використання цієї системи без дозволу може бути незаконним і порушувати приватність та безпеку інших систем.

Щоб встановити цю операційну систему, як віртуальну машину потрібно перейти в розділ завантажень офіційного сайту Kali Linux. Обираємо спеціалізований образ для VMware та додаємо його у середовище віртуалізації за допомгою вже знайомої функції «Open a Virtual Machine», яку було використано для додавання Wazuh Server'а. Конфігурація автоматично виділяє під систему 2 ГБ оперативної пам'яті та 80 ГБ пам'яті жорсткого диску, що є цілком достатнім для виконання термінальних команд. Також автоматично налаштовано користувача, ім'я та пароль якого дорівнюють «kali».

Отже, після встановлення віртуальної машини-зловмисника ми підготували всіх суб'єктів для проведення тестування системи Wazuh на спроможність спростити процедуру аналізу, виявлення та реагування на спроби сканування та проникнення в пристрій, що моніториться.

3 ПРАКТИЧНА ЧАСТИНА

У цьому розділі буде розглянуте практичне застосування Wazuh, як системи виявлення та запобігання проникненням. Зокрема, буде описаний процес роботи з документами та аналіз інцидентів за допомогою них. Також буде детально викладений процес налаштування сповіщень та активних відповідей (active response) на події, що визначені як потенційно зловмисні або підозрілі. Для наочного прикладу проектуватимуться найпростіші атаки та спроби сканування пристрою на відомі вразливості за допомогою віртуальної машини потенційного зловмисника.

3.1 Тестування фіксації подій в панелі Wazuh

Для початку, проведемо найпростіше сканування мережі з перспективи зловмисника. Таким чином, ми проектуємо ситуацію, коли зловмисник знаходиться в межах однієї локальної мережі з жертвою, це часто може трапитись з користувачами, підключеними до громадської Wi-Fi мережі у кафе, бібліотеках або коворкінгах.

Спершу, дізнаємось яку IP-адресу, яку маршрутизатор роздав зловмиснику, і одразу ж побачимо маску підмережі для розуміння скільки адрес виділено в цій локальній мережі, відповідно – який діапазон нам потрібно сканувати, щоб виявити кількість та види пристроїв в цій мережі. Для цього проробимо дії, проілюстровані на рисунку 3.1.1. Команда для виводу IP-адреси показала, що адреса машини зловмисника – 192.168.110.129, а маска підмережі – /24. Це означає, що під пристрої в мережі було виділено адреси в діапазоні від 192.168.110.1 по 192.168.110.254, адже 192.168.110.0 зарезервована під IP-адресу мережі, а 192.168.110.255 – під широкомовну (broadcast) адресу.

Для сканування, як бачимо, було використано інструмент для аудиту безпеки мережі NMAP з прапором «-O», який додасть у інформацію про пристрої, операційну систему кожного з них (якщо це можливо) (рис. 3.1) [14].

Вивід команди було експортовано у текстовий файл щоб не засмічувати вікно виводу, а також – окремо зберегти результати сканування, адже вони є статичними і, таким чином, цим файлом можна послуговуватись під час подальшого сканування систем на предмет вразливості.

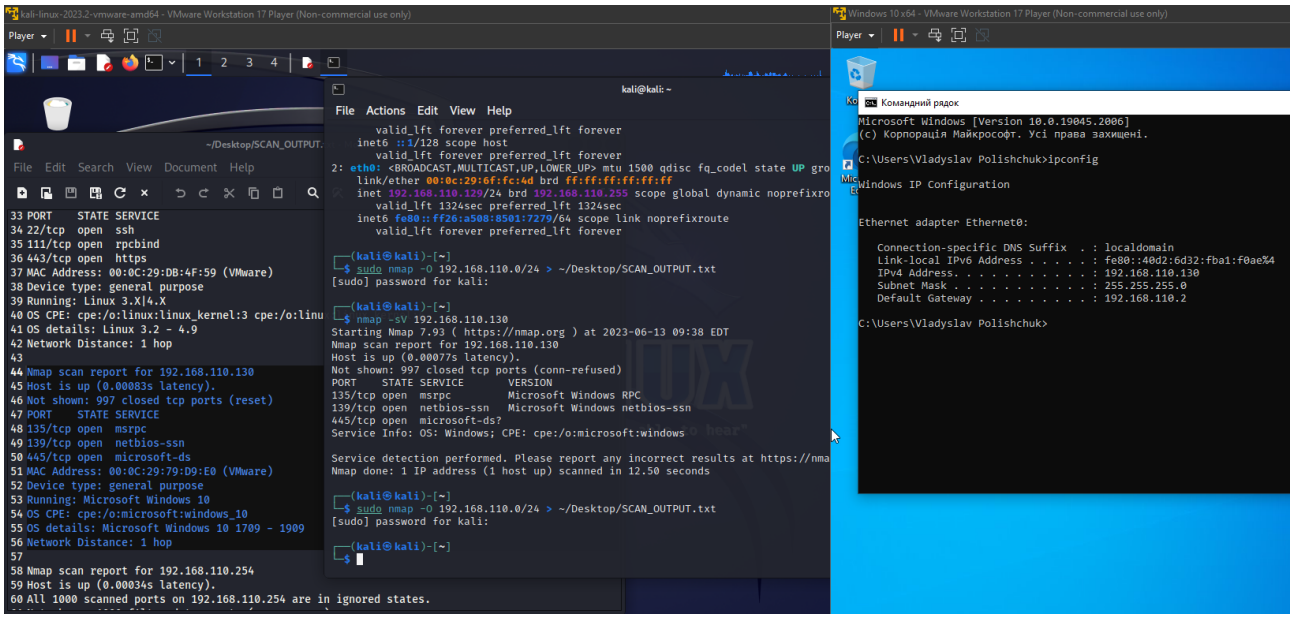


Рисунок 3.1 – Сканування пристроїв в локальній мережі та виявлення IP-адерси жертви

Так як, Wazuh є більш наближеною до HIDS (Host based IDS), звідси – агенти збирають інформацію в першу чергу на вузлі, тобто фіксують зміни файлів, даних входу користувачів, додавання користувачів до адміністративних груп, відкриття TCP / UDP та інші зміни в конфігурації системи, які можуть спричинити послаблення будь-якої зі сторін захищеності.

Тому у тестових атаках увага буде зосереджена на отримання доступу до оболонки системи (CMD або PowerShell) і подальшої ескалації привілеїв. Приступимо до аналізу отриманої інформації після першого сканування за допомогою NMAP. На пристрої жертви бачимо відкриті порти 139 та 445, ці порти можуть бути вразливими до вразливості MS08-067. Ця вразливість, при експлуатації може надати зловмиснику віддалений контроль над пристроєм та можливість виконувати зловмисні команди на ньому. Важливо, навіть якщо

зловмисникові не вдасться експлуатувати вразливість, його спроби можуть спричинити екстрене завершення процесу Svchost.exe, який є невід'ємним компонентом для стабільної роботи операційної системи та її сервісів. Його раптове припинення може призвести до серйозних наслідків для системи, зокрема її вимкнення та скидання усіх активних служб без збереження попереднього стану.

Щоб перевірити, чи вразливі, знайдені порти, до MS08-67 скористаємось Metasploit Framework. Даний інструмент є одним з найвідоміших і найпотужніших наборів інструментів для тестування на проникнення та експлуатації вразливостей. Це відкрите програмне забезпечення, яке надає широкі можливості для проведення аудиту безпеки, розробки експлойтів та керування уразливими системами.

Metasploit містить понад 2000 модулів, зокрема експлойти, payload-и (модуль зловмисного програмного забезпечення, який використовується для налагодження зв'язку між пристроєм жертви і комп'ютером або сервером зловмисника), сканери тощо. Ці модулі дозволяють проводити тестування на проникнення, використовуючи різні методики та підходи, і допомагають виявляти та використовувати вразливості в цільових системах.

Цей фреймворк надає гнучкість і зручний інтерфейс для виконання атак. Він пропонує як графічний (Metasploit Community Edition та Metasploit Pro), так і командний (msfconsole) інтерфейси. За допомогою цих інтерфейсів користувачі можуть використовувати модулі, налаштовувати параметри атаки, виконувати експлойти та аналізувати результати.

Metasploit також підтримує розробку власних модулів та експлойтів. Це дозволяє розробникам створювати власні атаки, налаштовувати їх для конкретних потреб і спільно використовувати їх з іншими користувачами. Ця можливість робить Metasploit Framework гнучким і розширюваним інструментом для випробування безпеки.

Для використання цього інструменту потрібно виконати команду msfconsole, тоді після підвантаження всіх компонентів ми потрапляємо у

консоль взаємодії з базою експлойтів, payload-ів та інших компонентів фреймворку. Щоб почати тестування, ми обрали відповідний експлойт для можливої вразливості з бази експлойтів, а на роль payload-а обрали meterpreter, який є зловмисною програмою для віддаленого управління пристроями-цілями. Далі задаємо IP-адресу цілі і наш експлойт готовий до виконання, яке ми реалізуємо через команду «exploit» (рис 3.2). Але, на жаль, нам не вдалось отримати віддалений доступ цього разу, це сталось через те, що на машині встановлена версія Windows 10 22H2 (збірки 19045.2965), яка не є вразливою до цього експлойту, адже в зоні ризику знаходяться, здебільшого, системи на Windows XP та Windows Server 2003.

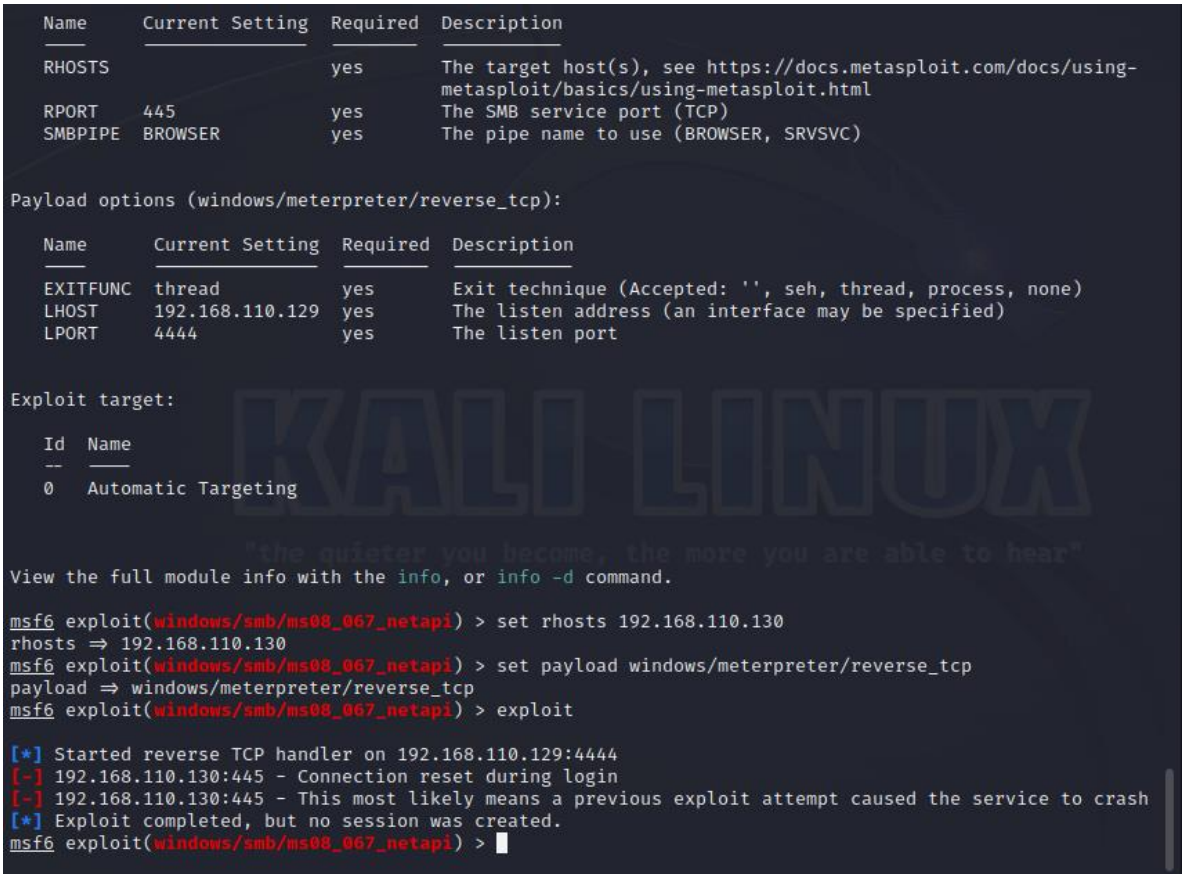


Рисунок 3.2 – Спроба експлуатації вразливості MS08-067

Проте, існує інший спосіб провести meterpreter на машину-жертву. Це можливо завдяки зловмисному файлу, який ми створили за допомогою інструменту створення файлів з вбудованими payload-ами – msfvenom. Як параметри задаємо IP-адресу машини зловмисника, до якої буде під’єднуватись

жертва (адже payload базується за зворотному з’єднанні), порт, тип файлу та його назву (рис. 3.3).

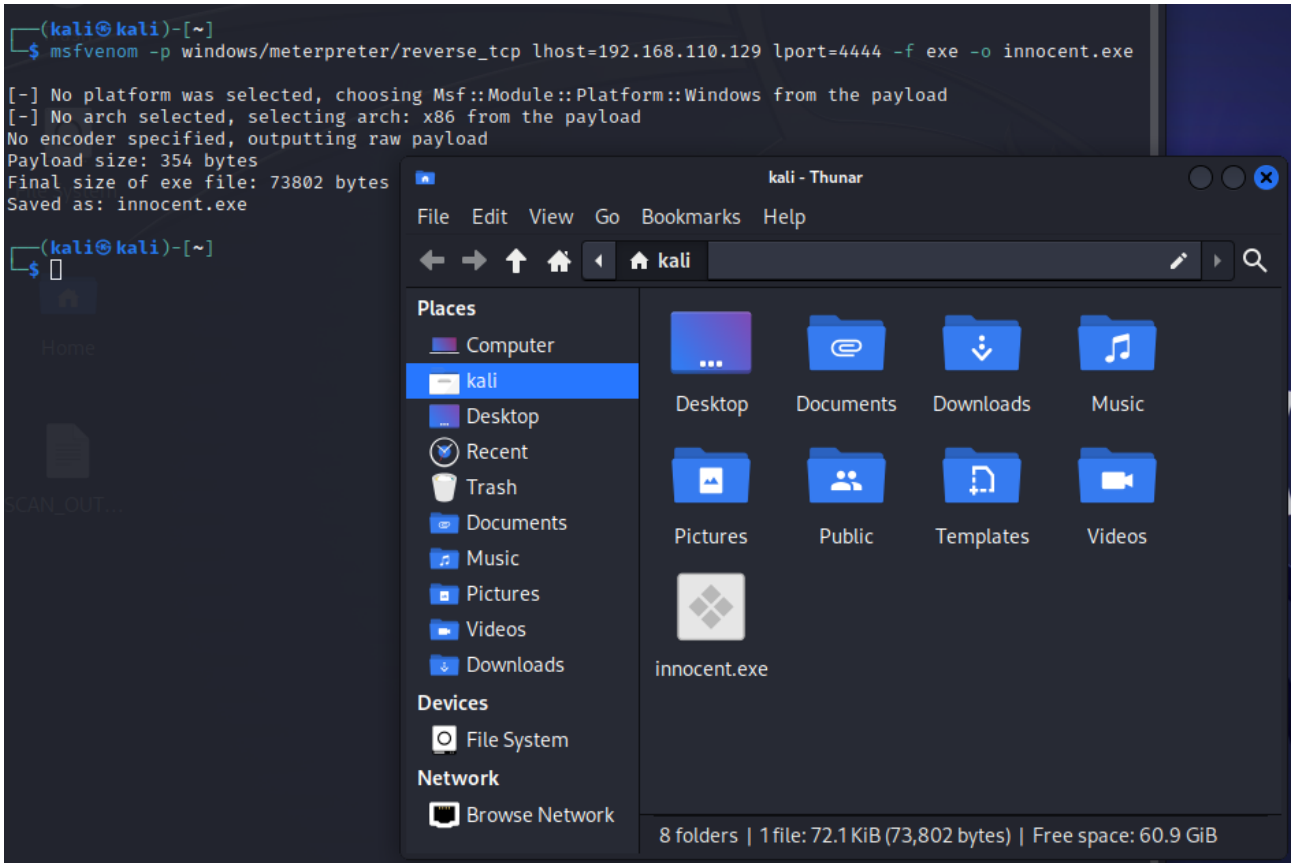


Рисунок 3.3 – Створення зловмисного exe-файлу

Після створення такого файлу, потенційний зловмисник повинен змусити жертву виконати цей файл у своїй системі, для цього він може передати його їй електронною поштою або через взаємодію зі зловмисним веб-застосунком (які є двома найпоширенішими способами розповсюдження зловмисного ПЗ), замаскувавши цей файл під невинний або навіть корисний. Як наслідок, після виконання цього файлу в системі зловмисник отримує доступ до пристрою жертви через інтерфейс командного рядка CMD (рис. 3.4) [1]. Крім того, meterpreter дозволяє збирати інформацію про ввід символів з клавіатури користувача (key logger), спостерігати за екраном користувача в реальному часі, робити знімки екрану, управляти веб-камерою та багато інших дій для збору інформації.

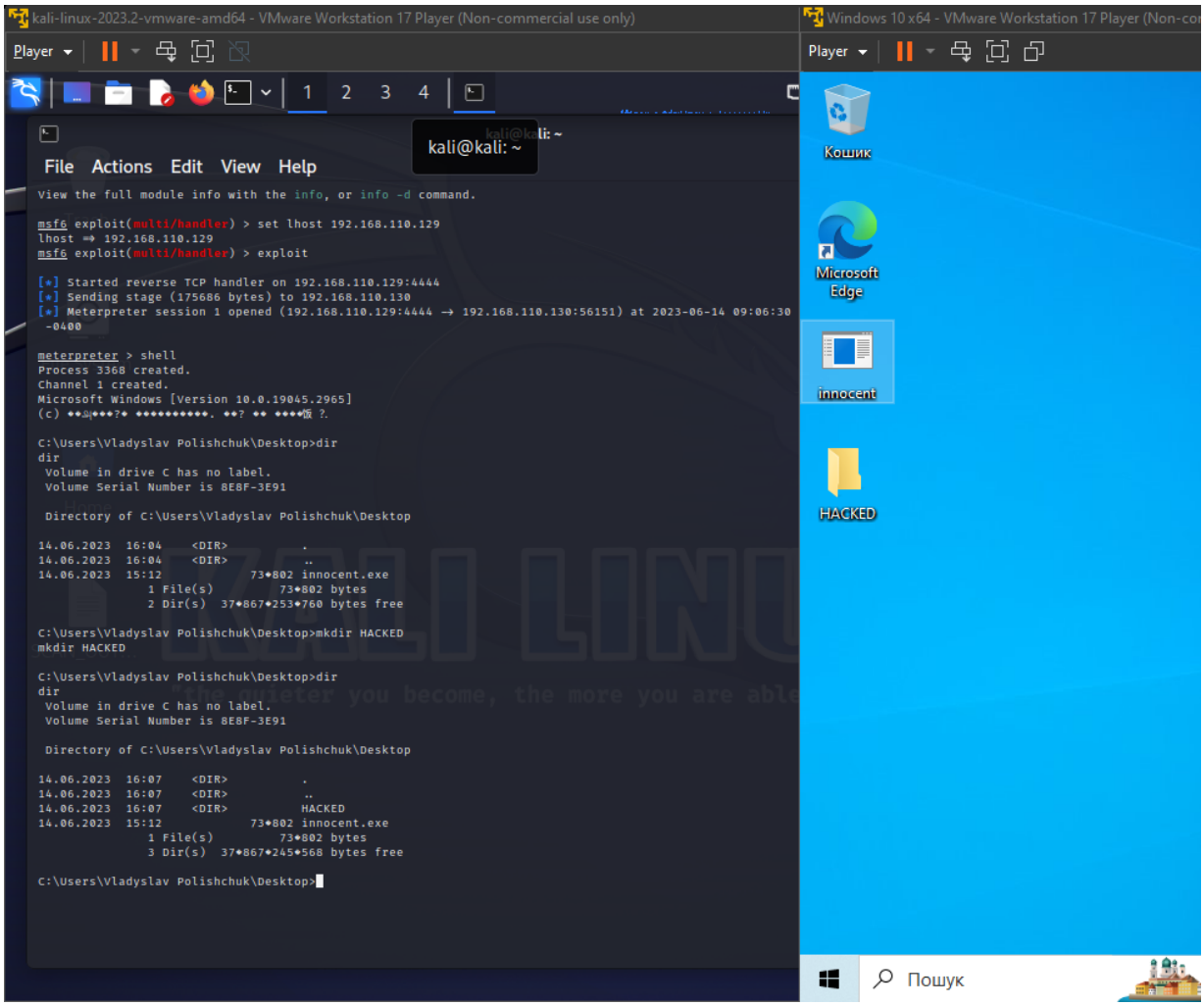


Рисунок 3.4 – Приклад доступу до CMD жертви

Коли ми отримали користувацький віддалений доступ, потрібно знайти спосіб ескалації привілеїв до адміністративних. Це можна реалізувати за допомогою іншого експлойту з бібліотеки Metasploit – bypassuac-fodhelper. Цей експлойт допомагає обійти UAC (User Account Controll), який надсилатиме запит підтвердження усіх дій, які виконуються в системі від імені адміністратора. Використємо сесію meterpreter-a для обходу UAC та запуску CMD а адміністративному режимі (про це свідчитиме директорія «system32» в стрічці вводу команд) (рис. 3.5). Одразу ж спробуємо створити користувача «hackerVlad» та додати його до адміністративної групи користувачів. На рисунку 3.5зображені відповідні дії для ескалації привілеїв в системі до рівня локального адміністратора.

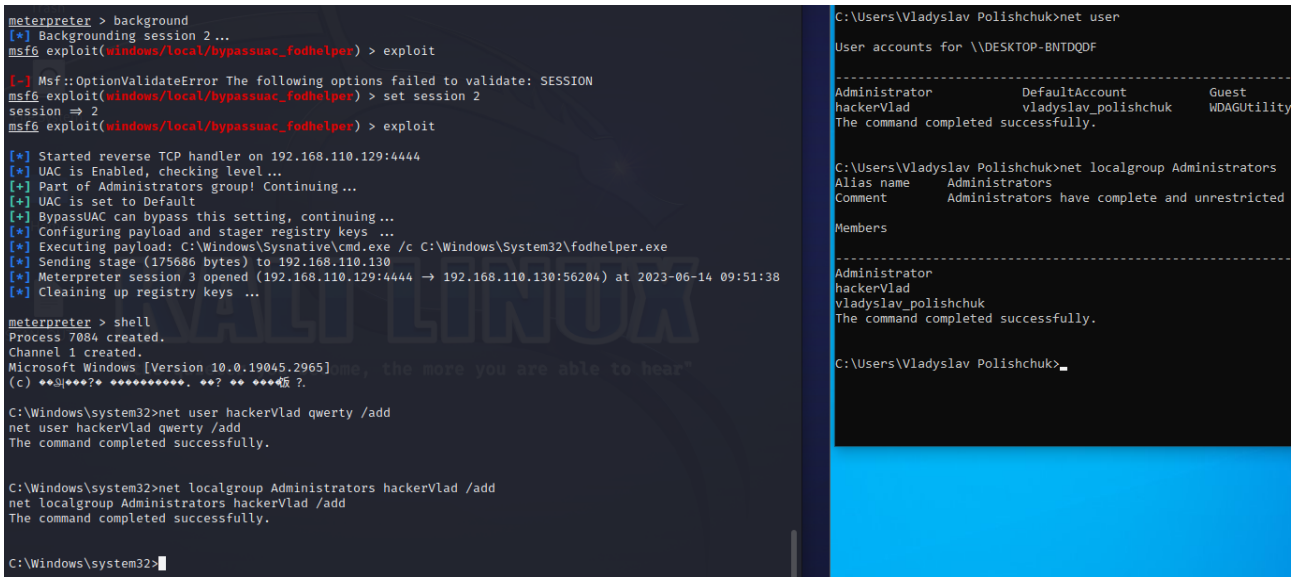


Рисунок 3.5 – Ескалація привілеїв в системі

Після ескалації привілеїв ми спробували знайти відповідні події, як задокументовані в панелі Kibana. Для цього потрібно зайти в режим перегляду усіх документів подій під назвою «Discover». А далі – відфільтрувати документи про окремі події додавання нового користувача та включення його до групи, для цього існують ідентифікатори подій (EventID) і для цих подій вони дорівнюють 4720 і 4728 відповідно. На рисунку 3.6 зображені дві шукані події у панелі Kibana, також виділені SecurityID новоствореного користувача та адміністративної групи.

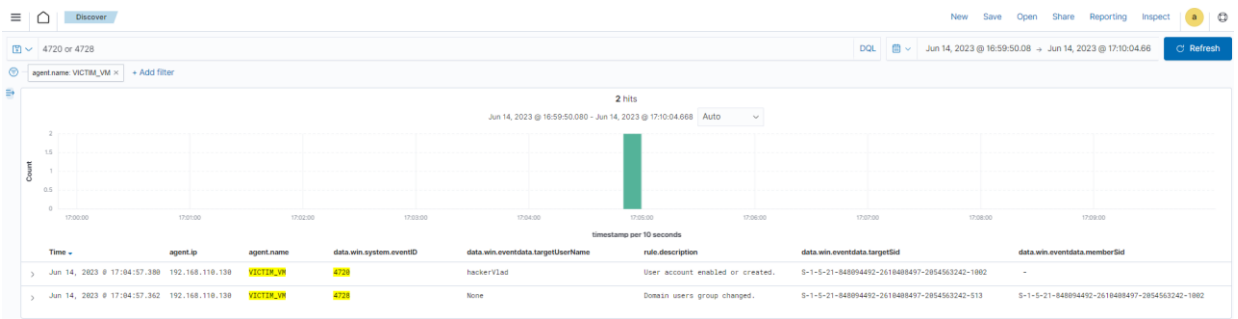


Рисунок 3.6 – Події ескалації привілеїв зафіксовані Wazuh Agent та відображені в панелі Kibana

Агент успішно зафіксував обидві події та відобразив їх у панелі для

роботи з лог-файлами подій Kibana.

3.2 Налаштування сповіщень про зловмисні події

Коли фіксація подій Wazuh Agent-ом працює як слід, можна встановити певні умови за яких Wazuh буде не тільки реєструвати важливі події в системі, а і сповіщати адміністратора про їх виникнення.

У Wazuh є опція відправки сповіщень за допомогою електронної пошти, але для цього нам потрібно налаштувати локальний SMTP сервер (спеціалізований сервер для відправки електронних листів). Для цього ми створили ще одну віртуальну машину з операційною системою Linux, дистрибутив – Ubuntu 22.04.2. Такий вибір був зроблений через згадку цього дистрибутиву, як рекомендованого в документації Wazuh, для розгортання SMTP сервера. Для функціонування такого сервера спершу потрібно встановити такі пакети (використавши пакетний менеджер apt-get):

- postfix – безкоштовний агент для доставки електронної пошти (Mail Trasfer Agent або MTA) та за сумісністю – основа нашого SMTP сервера;
- mailutils;
- libsasl2-2;
- ca-certificates;
- libsasl2-modules.

Як бачимо, основним компонентом є агент Postfix, а усі інші – це, рекомендовані документацією, пакети-додатки для його стабільної роботи. Надсилати листи ми будемо за допомогою Gmail, найвідомішого поштового сервісу, але для цього потрібно автентифікувати наш сервер для нього за допомогою паролю застосунку, який можна отримати, підключивши другий фактор автентифікації до свого Google-акаунту.

Тому після змін у конфігуративному файлі Postfix, серед яких:

- налаштування даних для автентифікації на smtp.gmail.com (для

автоматичної відправки електронних листів від імені автентифікованого користувача);

- активація параметрів, що відповідають за роботу TLS та підключення сертифікатів зі встановленого пакета ca-certificates;
- важливо додати IP-адресу Wazuh Server-а до значень змінної «my_networks», якщо цього не зробити, то Postfix не зможе обробляти листи отримані від системи сповіщень Wazuh.

Далі записуємо свої дані, як відправника, у потрібний файл директорії агента, щоб він міг ним користуватись під час відправки електронних листів. Також ми файл для паролів штатною командою postmap і робимо його недоступним для усіх крім адміністратора root та усіх програм, які виконуються в системі від його імені.

Далі ми вказали потрібні атрибути у конфігурації нашого Wazuh Server, а саме:

- активація сповіщень електронною поштою;
- IP-адресу SMTP-сервера;
- електронна пошта відправника;
- електронна пошта отримувача (що дорівнює адресі відправника в нашому випадку).

На рисунку 3.7 зображені рядки файлу конфігурації /var/ossec/etc/ossec.conf.

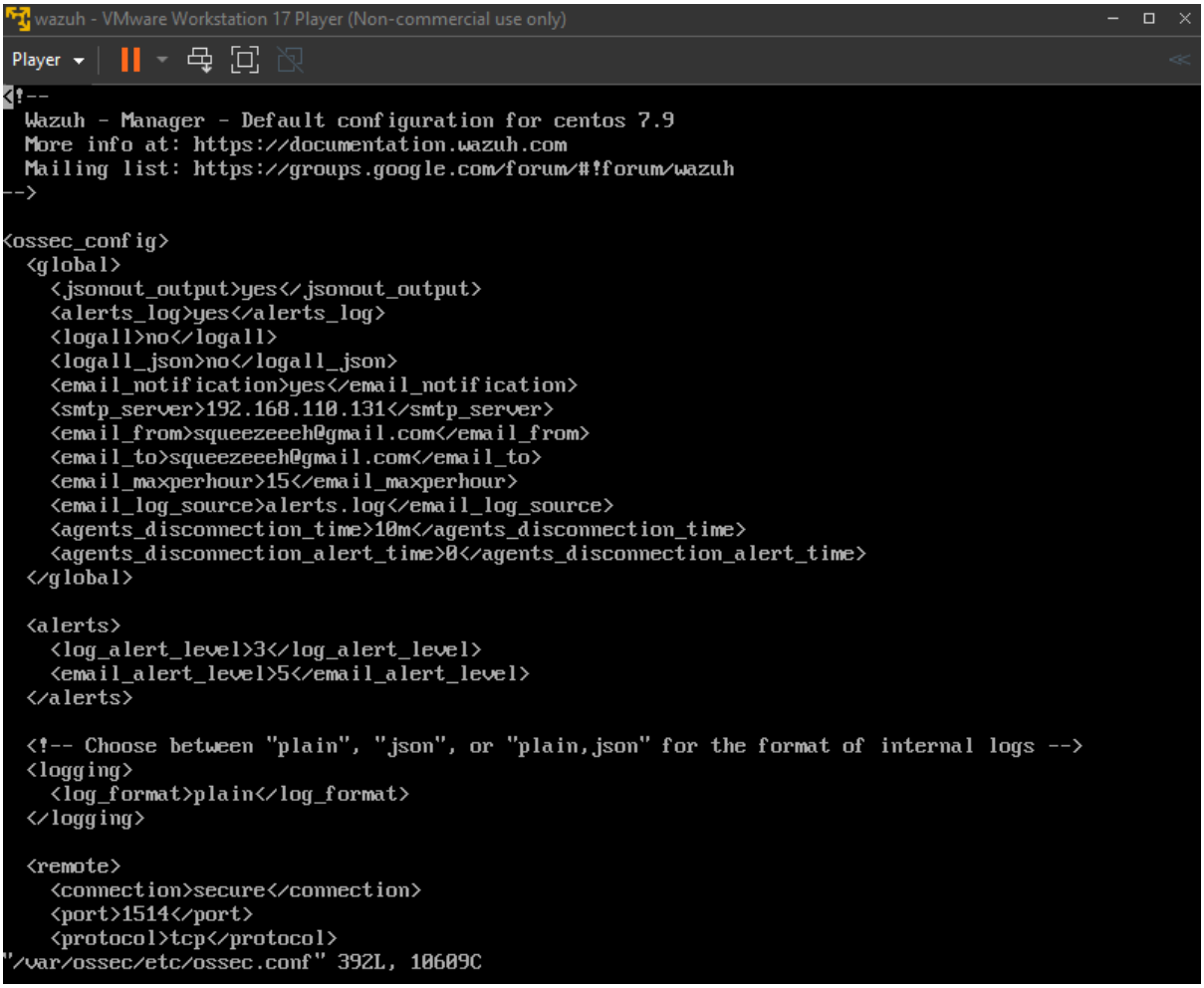


Рисунок 3.7 – Змінений файл конфігурації Wazuh Server для сповіщень електронною поштою

І після перезапуску служби wazuh-manager на сервері, ми готові до невеликого тестування отримання сповіщень про події, які ми раніше фіксували у панелі Kibana. Зокрема, створення користувача та додання його до користувацької групи. Після чого ми, одразу ж, отримали два листи-сповіщення (рис. 3.8) різного рівня ризику за 16-бальною шкалою Wazuh (8 – для додавання користувача та 12 – для включення користувача до групи локальних адміністраторів).

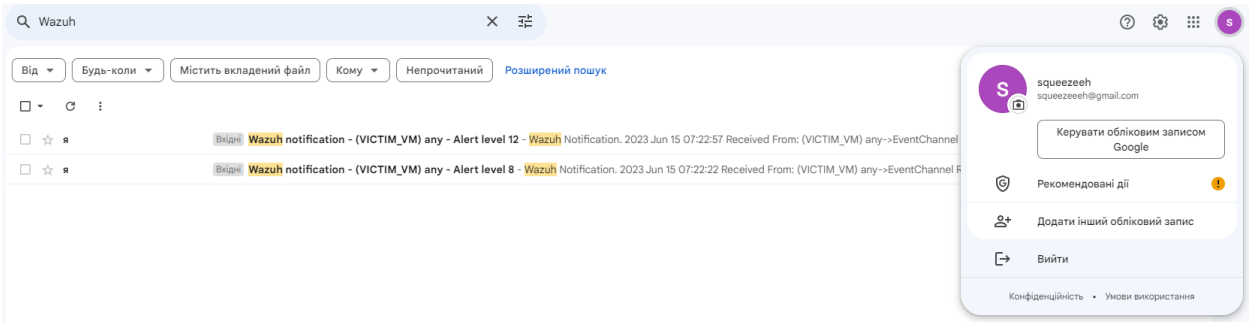


Рисунок 3.8– Отримані листи сповіщень про зроблені зміни в конфігурації користувачів системи

Ці листи місять список полів та значень, які допоможуть адміністратору розслідувати інцидент та оперативно вжити потрібних заходів для мінімізації впливу на мережу. Роглянемо вміст на прикладі сповіщення про додавання нового користувача в систему, пропустивши лог події у необробленому форматі, адже далі викладені ті самі дані, тільки розкладені на змінні для зручнішого читання та розуміння (рис. 3.9).

Бачимо, що поля в тексті сповіщення пістять набір інформації про ім’я користувача, якого було створено, пристрій на, якому було внесено зміни, точний час та EventID конкретної події. Це дозволяє адміністратору оперативно співставити дані зі сповіщення з документами подій в панелі Kibana і, як наслідок, отримати більше інформації про інцидент для прийняття відповідних рішень.

Після активації сповіщень про інциденти електронною поштою, наша Wazuh-система набула атрибутів IDS. Авжеж, це не максимум її функціоналу, адже, як зазначалось в теоретичному розділі, Wazuh дає можливість підключати не обмежену кількість модулів та індексів, як джерел збору інформації у вигляді лог-файлів подій.

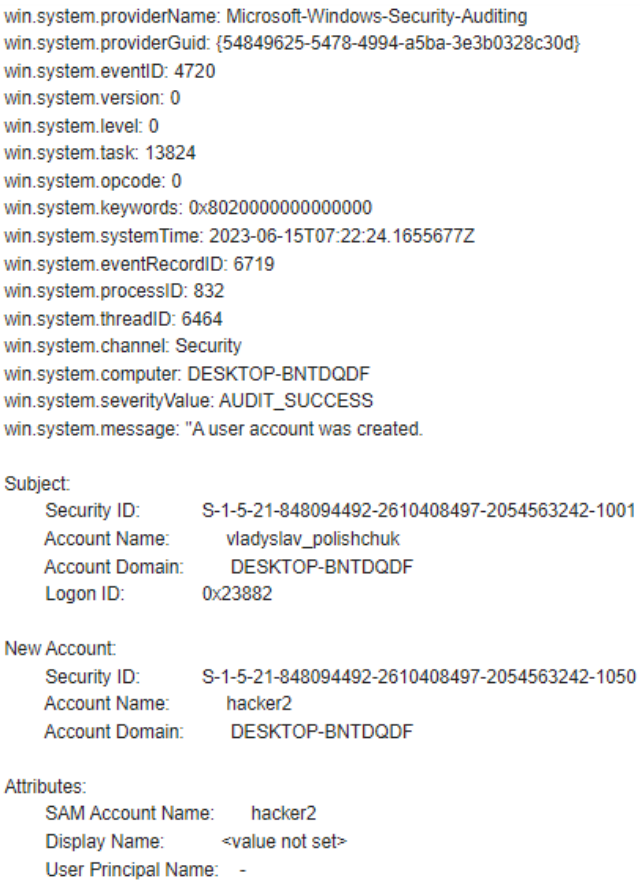


Рисунок 3.9 – Зміст сповіщення про додаваня нового користувача

3.3 Активне реагування на інциденти

Для надання нашій системі Wazuh властивостей і можливостей IPS-рішення ми задамо в конфігурації агентів умову, за виконання якої, буде спрацьовувати відповідна дія, як відповідь на підозрілу активність. Такий функціонал досягається завдяки особливості Wazuh під назвою Active Response, що налаштовується шляхом створення блоків в конфігураційному файлі сервера Wazuh та має свій синтаксис.

Для тестування активної реакції на інцидент ми вирішили продемонструвати, як Wazuh може забезпечувати цілісність файлів. І в першу чергу він має бути здатним вберегти власні конфігураційні файли від несанкціонованих спроб модифікації. Для таких випадків існує правило під ідентифікатором 550 під назвою «Integrity checksum changed.», тобто він напряму відповідає за цілісність файлів і фіксує усі факти змін в них. Тому

перш ніж тестувати Active Response нам потрібно створити для нього спеціальне правило, яке буде стосуватись лише головного файла конфігурації агента, його ми виділили завдяки оператору «match», який спрацьовує, коли в змісті події включає в себе задане значення. Також ми додали невеликий опис, щоб відрізнити це правило від інших правил, що стосуються цілісності різних типів файлів не лише за числовим ідентифікатором. На рисунку 3.10 зображений запис цього правила у конфігураційному файлі для додавання локальних користувацьких правил [20].

```
<group name="restart,">

  <!-- RULE FOR ACTIVE RESPONSE DIPLOMA PROJECT -->
  <rule id="100002" level="7">
    <if_sid>550</if_sid>
    <match>ossec.conf</match>
    <description>Wazuh Agent configuration file was changed. Restarting...</description>
  </rule>

</group>
```

Рисунок 3.10 – Новостворене правило для фіксації змін в головному конфігураційному файлі Wazuh Agent

Після перезапуску wazuh-manager з метою актуалізації списку правил, ми протестували роботу цього правила, додавши один символ до випадкового коментаря всередині конфігураційного файлу, що ніяк не вплине на його виконання але кардинально вплине на його хеш-суму. І ми одразу ж отримали сповіщення про зміну файлу, на який націлене правило (рис. 3.11).

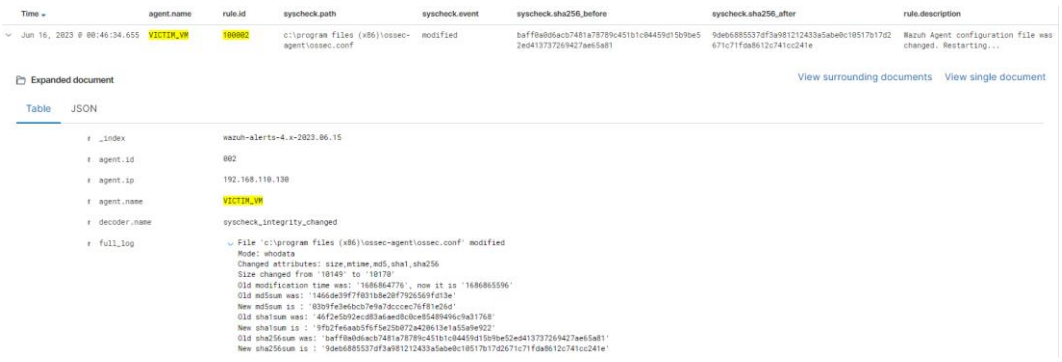
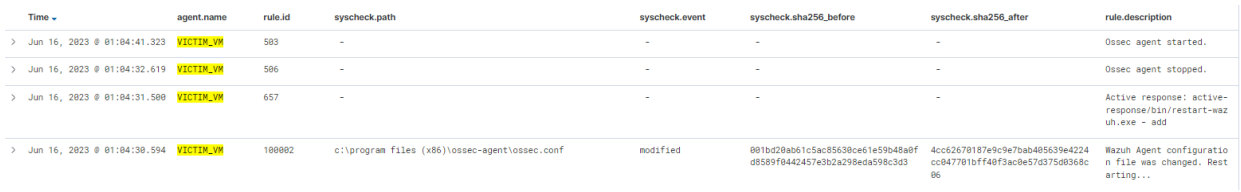


Рисунок 3.11 – Сповіщення про зміну файлу конфігурації Wazuh Agent

Тепер нам потрібно додати блок Active Response в головну конфігурацію

Wazuh Server, аби при спрацьовуванні правила виконувалась програма «restart-wazuh», яка перезавантажуватиме Wazuh Agent на пристрої, скинувши усі потенційно зловмисні зміни (рис. 3.12) [20].



Time	agent.name	rule.id	syscheck.path	syscheck.event	syscheck.sha256_before	syscheck.sha256_after	rule.description
Jun 16, 2023 @ 01:04:41.323	VICTIM_VM	503	-	-	-	-	Ossec agent started.
Jun 16, 2023 @ 01:04:32.619	VICTIM_VM	506	-	-	-	-	Ossec agent stopped.
Jun 16, 2023 @ 01:04:31.500	VICTIM_VM	657	-	-	-	-	Active response: active-response/bin/restart-wazuh.exe - add
Jun 16, 2023 @ 01:04:30.594	VICTIM_VM	100002	c:\program files (x86)\ossec-agent\ossec.conf	modified	001bd20ab61c5ac85630ce61e59b48a0fd8589f0442457e3b2a298eda598c3d3	4cc62670187e9c9e7bab405639e4224cc047701bff40f3ac0e57d375d0368c06	Wazuh Agent configuration file was changed. Restarting...

Рисунок 3.12 – Робота Active Response відображена у історії подій

Таким чином, ми продемонстрували, що Wazuh може не лише збирати і відображати інформацію, а й сповіщати про зловмисні події, та навіть вживати певних заходів, у випадках визначених адміністратором (що є ознакою IPS).

Проте, Active Response не обмежується лише перезавантаженням агентів, за наявності підключеного джерела лог-файлів з брандмауерів, Unix-серверів, антивірусів або фільтрів електронної пошти він здатний керувати і їх конфігураціями, якщо розробити відповідні правила і активні реакції.

Отже, попри увесь вбудований в Wazuh функціонал, він залишає безмежний простір для надбудов та модифікацій, а також інтеграцій з іншими рішеннями моніторингу і безпеки. Це робить його одним з найбільш гнучких та приємних в роботі, інструментом для фахівців різних підгалузей кібербезпеки.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Шляхи підвищення життєдіяльності людини

Повномасштабне вторгнення, яке розпочала росія 24 лютого 2022 року на території України, має неабиякий негативний вплив на психічне й фізичне здоров'я людини. Уже понад півтори роки українці живуть із відчуттям страху, що нагадує про себе з кожним сповіщенням про повітряну тривогу та звуком сирени. Щодня велика кількість новини про зруйновані будинки від обстрілів та число загиблих морально пригнічують українці, а економічні труднощі спричиняють емоційні страждання. Ті, хто перебувають у виснаженому стані, а також ті, хто залишаються у форматі самомобілізації повинні усвідомити, що їхній стан – це наслідок психологічної травми. Відтак в умовах війни підвищення життєдіяльності людини є надзвичайно складним, але водночас важливим завданням для підтримки морального стану і збереження фізичних сил. Однак, навіть у таких реаліях, є кілька методів, які можуть сприяти збереженню працездатності людей.

Основні методи підвищення життєдіяльності можна умовно розділити на два типи: активні – ті, що напряму впливають на трудові можливості людини, та пасивні – мають лише дотичний вплив на продуктивність (рис. 4.1).

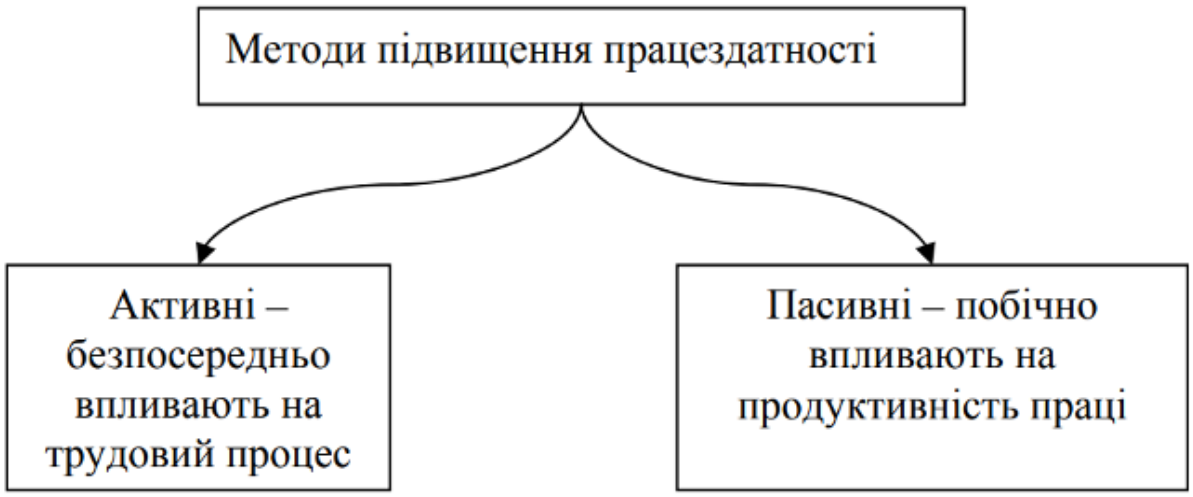


Рисунок 4.1 – Методи підвищення працездатності

До активних методів належать розподіл і кооперація праці; оптимізація ритму праці; раціональна організація робочого місця; удосконалення режиму праці й відпочинку; раціональне застосування засобів фізичної культури й спорту. [7] До кожного аспекту активного методу застосовують різні шляхи покращення працездатності:

- делегування праці або командна робота – цей шлях базується на взаємодії між людьми з метою досягнення спільної мети. Розподіл завдань та кооперація покращують ефективність використання наявних ресурсів, зокрема людських, фінансових і матеріальних. Учасники команди мають виконувати ту роботу, в якій можуть бути найбільш продуктивними, а їхня праця – результативною. Люди можуть навчатися один від одного, передавати знання та навички, що дозволяє кожному зростати як професіоналу, і разом сприяти подоланню спільних труднощів;
- оптимізація темпу праці – такий спосіб передбачає ефективність робочих процесів та використання сучасних технологій. Автоматизація рутинних завдань та застосування програмного забезпечення можуть допомогти зменшити необхідний час для виконання певних робіт. Наприклад, використання спеціалізованого програмного забезпечення для обліку або автоматичного розсилання електронних листів може суттєво зекономити час працівнику. Також ефективне планування робочого дня, встановлення пріоритетів та використання технік управління часом (метод Pomodoro), допоможуть зосередитися на найважливіших завданнях і уникнути розсіяності;
- організація робочого місця – це один із шляхів покращення життєдіяльності, що передбачає оптимізацію освітлення, простору, ергономіку меблів та обладнання, і, безпосередньо, зручність та безпеку. Робоче місце розташовують у найкраще природно освітлювальній частині кімнати. У разі нестачі природного світла використовують приємне та регульоване штучне освітлення, яке не спричиняє надмірного напруження очей. Належне розташування столу, стільця, монітора комп’ютера, клавіатури та миші

допомагає уникнути перенапруження м'язів, що може спровокувати проблеми з поставою.

- покращення режиму праці та відпочинку – цей спосіб передбачає баланс між роботою та вільним часом. Наприклад, складання розкладу чи графіку на кілька днів або тижнів, де буде запланований час для відпочинку та розваг. До того ж створення режиму задля якісного сну відновлює фізичну і психологічну енергію, покращує когнітивні функції і загальний стан здоров'я людини;
- раціональне використання засобів фізичної культури й спорту – здоровий спосіб життя є ключовим аспектом підвищення життєдіяльності. Регулярні перерви, фізична активність, здоровий сон і налагоджені відносини в робочому оточенні можуть позитивно вплинути на продуктивність і загальний стан працівника не лише в умовах війни, але й загалом.

До пасивних методів, що побічно впливають на працездатність і продуктивність праці, можна віднести оздоровлення умов зовнішнього середовища, тобто поліпшення метеорологічних умов, зниження шуму, вібрації, зменшення запиленості й загазованості повітря тощо [7].

Кліматичні умови можуть суттєво впливати на самопочуття та працездатність людини. Підтримка комфортної температури та вологості повітря сприяє зниженню фізичного напруження, покращує концентрацію та сприйняття інформації.

Щодо основних організаційних методів зниження шуму та відбрації, то до них належать: захист часом (обмеження часу перебування людини в умовах підвищеного шуму); захист відстанню (віддалення робочих місць від джерел шуму) [7]. Також для зниження рівня шуму і вібрації використовують індивідуальні засоби захисту, а саме: вушні вкладиші, навушники, шоломофони тощо. Під час їхнього застосування отримують зниження рівня звукового тиску на 10–15 дБ. Навушники знижують рівень звукового тиску на 7–35 дБ в середньому діапазоні частот. Шоломофони захищають вушну область і знижують рівень звукового тиску на 30–40 дБ у середньому діапазоні частот.

Повітря, яке містить багато шкідливих речовин, може мати негативний вплив на дихальну систему, спричиняти алергічні реакції та погіршувати загальний стан здоров'я. Застосування ефективної системи вентиляції, використання фільтрів повітря та забезпечення чистоти приміщень можуть допомогти зменшити запиленість та забезпечити свіжий і безпечний для дихання повітря.

Отже, всі проаналізовані шляхи щодо покращення життєдіяльності людини в умовах воєнного стану можуть бути застосовані і як загальні поради задля удосконалення. Сприятливі умови праці забезпечують комфорт та безпеку працівників, а також сприяють підвищенню їх продуктивності та загального самопочуття, що є надважливо станом на сьогодні.

4.2 Естетичне оформлення робочого місця оператора ПК, верстату, установки

Ефективність та продуктивність праці користувача ПК залежить не лише від правильно організованого робочого місця з урахуванням всіх технічних та безпекових вимог, але й від естетичного оформлення. Комфортні умови для роботи сприяють не тільки кращій працездатності, а й загальному самопочуттю виконавця робіт.

Естетичне оформлення робочого місця оператора складається з таких аспектів, як-от:ретельно спланованого розташування засобів і предметів праці задля зручності користування; дотримання санітарних і гігієнічних вимог; підбору доцільної кольорової гами кабінету; музичного чи інструментального супроводу; окремої зони для відпочинку; озеленення простору з оздоровчою метою.

Водночас естетичні аспекти планування кабінету не повинні перешкоджати ергономічному розташуванню габаритних меблів та наявних технічних засобів для праці. Використання робочої площі повинно бути ефективним та економним водночас.

Робоче місце оператора ПК, верстату чи установки не має чітких естетичних вимог, то ж працівник може організувати робочий простір відповідно до власних уподобань і потреб. Наприклад, більшість операторів надають перевагу мінімалістичному стилю. Серед його переваг виокремлюються такі як спрощеність і лаконічність. Враховуючи цей аспект, місце виглядає організовано та приємно для очей. Мінімалістичний дизайн характеризується простими лініями, використанням нейтральних кольорів і невеликою кількістю декоративних елементів не лише з естетичною метою, але й безпековою.

Мінімалістичний стиль передбачає наявність чистої робочої поверхні, без надмірного забруднення чи нагромадження сміттям. Необхідні засоби для виконання праці, такі як комп'ютер, монітор, клавіатура та миша, розташовані таким чином, щоб забезпечити зручність і ергономіку для оператора. Кабелі можуть бути приховані або організовані, щоб уникнути непотрібного візуального скупчення. Дотримання чистоти, порядку та належної організації дозволяють зменшити рівень стресу та забезпечити зручний доступ до необхідних матеріалів і ресурсів для праці. Використання органайзерів, шухляд, полиць та інших засобів для розподілу робочих матеріалів дають змогу підтримувати візуальну чистоту та створити естетичну атмосферу на робочому місці.

Для мінімалістичного робочого простору важливо обрати меблі та аксесуари, які мають прості форми і лінії. Матеріали можуть бути натуральними, зокрема надають перевагу дереву чи металу, або сучасними, такими як скло. Важливо обмежити кількість декоративних елементів і зосередитися на практичності та функціональності робочого місця.

Кольорове оформлення поверхонь технологічного обладнання, транспортних засобів та інвентарю повинні відповідати обраній кольоровій гамі. Кольори мають великий вплив на настрій і емоційний стан людини. Зокрема це може бути поєднання різних кольорів у інтер'єрі або лише на організованому робочому місці. Кольорова палітра мінімалістичного робочого

місця, як правило, базується на нейтральних тонах, таких як білий, сірий, чорний або бежевий. Це допомагає зробити простір візуально спокійним і чистим. Якщо оператор бажає додати акцентів, то це можна створити за допомогою яскравого кольору або одного вибраного предмета. Тому варто обрати ту палітру, що стимулюватиме концентрацію уваги.

Не менш важливим аспектом естетичного оформлення робочого місця оператора ПК, верстату чи установки є додавання особистого шарму. Фотографії, картини, рослини або мотивуючі цитати можуть стати додатковими елементами, які відображають індивідуальність та надихають під час робочого процесу. Такі деталі створюють приємну атмосферу та допомагають оператору ПК відчувати себе комфортно й зосереджено. У кабінеті може бути встановлений кондиціонер, вентилятор, жалюзі задля забезпечення санітарних та гігієнічних вимог та приємного перебування оператора на робочому місці.

Отже, естетичне оформлення робочого місця оператора ПК вимагає комплексного підходу, у якому буде поєднуватися кольорова гама, ергономіка, особистий стиль та засоби безпеки. Мінімалістичний стиль на робочому місці допомагає зосередитися на самій роботі і уникнути візуального шуму. Він створює спокійну і організовану атмосферу, що сприяє продуктивності і концентрації. Цей стиль може бути ідеальним вибором для тих операторів, що цінують простоту, ефективність і чистоту у своєму робочому просторі.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи були виконані завдання з доступного викладення основних відомостей про системи виявлення та запобігання вторгненням, їх види та категоризація. Також були названі конкретні програмні рішення IDS / IPS з коротким порівнянням з найближчим, за функціоналом, інструментом.

Наступним були детально описані основні функції і принципи роботи Wazuh. Як невід'ємний компонент розгортання, був детально розібраний процес встановлення необхідного серверного та вузлового програмного забезпечення Wazuh.

Після налаштування базових функцій Wazuh, як системи моніторингу елементів системи, ми описали конфігурацію системи сповіщень про визначені підозрілі події в системі, а також налаштували систему активних реакцій на підозрілі події високої серйозності.

Після реалізації функцій сповіщення і Active Response, які надали Wazuh ознак IDPS, ми провели тестування, налаштованих систем, шляхом імітації реальних атак, спроб експлуатування вразливостей з пристрою, який виконував роль потенційного зловмисника, що знаходиться в одній локальній мережі з жертвою.

В результаті успішного виконання поставлених завдань, ми можемо вважати мету досягнутою. А отже, ця кваліфікаційна робота може слугувати джерелом отримання базових знань для формування чіткого уявлення про IDS / IPS для читачів, які розглядають можливість впровадження системи виявлення та запобігання вторгненням у свою комп'ютерну систему.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Metasploit. How to use a reverse shell in Metasploit. URL: https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html

2. Axelsson S. Intrusion Detection Systems: A Survey and Taxonomy: технічний посібник. G¨oteborg, Sweden. 2000. 27 с.

3. ДСН 3.3.6.037 – 99 Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку. [Чинний від 01.12.99]. Київ. URL: https://zakon.rada.gov.ua/rada/show/va037282-99#Text

4. ДСН 3.3.6.039 – 99 Державні санітарні норми виробничої загальної та локальної вібрації. [Чинний від 01.12.99]. Київ. URL: https://zakon.rada.gov.ua/rada/show/va039282-99#Text

5. ДБН В.2.5-28 : 2018. Природне і штучне освітлення – Київ: ТОВ «КИЇВПРОЕЛЕКТРОПРОЕКТ», 2018. 133 с. URL: https://ledeffect.com.ua/images/__branding/dbn2018.pdf

6. IBM Corporation, Cost of a Data Breach Report 2022: статистичний звіт. Нью-Йорк: IBM Corporation, 2022. 59 с.

7. Стиценко Т.Є., Пронюк Г.В., Сердюк Н.М., Хондак І.І. «Безпека життєдіяльності»: навч. посібник / Т.Є Стиценко, Г.В. Пронюк, Н.М. Сердюк, І.І. Хондак. – Харків: ХНУРЕ, 2018. – 336 с.

8. Система безпеки комп’ютерної мережі з використанням пристроїв CISCO IDS I PIX / М. Карпінський, М. Гіжицкі, А. Брандис, Н. Герила, З. Рута // Вісник ТДТУ. — Т. : ТНТУ, 2006. — Том 11. — № 3. — С. 101–108.

9. Ребуха А. М. Порівняльний аналіз інформаційних систем виявлення вторгнень у роботу комп'ютерних систем: дипломна робота магістра за спеціальністю „126 — інформаційні системи та технології“ / А. М. Ребуха. — Тернопіль : ТНТУ, 2020. — 120 с.

10. Романчук В. О. Розробка програмного модуля для виявлення вторгнень методами машинного навчання: кваліфікаційна робота бакалавра за

спеціальністю 125 — Кібербезпека / В. О. Романчук. – Тернопіль : ТНТУ, 2022. – 53 с.

11. Santiago Ti. Configure Postfix to Send Email Using External SMTP Servers. URL: https://www.linode.com/docs/guides/postfix-smtp-debian7/

12. VMware Inc. VMware Workstation 17.0.2 Player Release Notes. URL: https://docs.vmware.com/en/VMware-Workstation-Player/17.0.2/rn/vmware-workstation-1702-player-release-notes/index.html

13. OffSec Services Limited. PRIVILEGE ESCALATION. URL: https://www.offsec.com/metasploit-unleashed/privilege-escalation/

14. Nmap Network Scanning, Chapter 8. Remote OS Detection, Usage and Examples. URL: https://nmap.org/book/osdetect-usage.html

15. Palo Alto Networks. What is an Intrusion Prevention System? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

16. Palo Alto Networks. What is an Intrusion Detection System? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids

17. Wazuh Inc. Documentation Wazuh, User manual. URL: https://documentation.wazuh.com/current/user-manual/index.html

18. Wazuh Inc. Documentation Wazuh, Getting started, Components. URL: https://documentation.wazuh.com/current/getting-started/components/index.html

19. Wazuh Inc. Active Response. URL: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html