МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЯРИНЮК БОГДАН ОЛЕКСАНДРОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
прикладної математики та
кібербезпеки,
д – р філософії з математики,
_____ А.В.Луценко
«__»_____20__ р.

РОЗРОБКА ТА ОЦІНКА ДОДАТКУ ДЛЯ АУДИТУ БЕЗПЕКИ В ОС WINDOWS

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
Канд. техн. наук, доцент,
старший викладач кафедри
прикладної математики та кібербезпеки
Чернов Д. В.

Оцінка:___/___/_____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК:_____
(підпис)

Вінниця - 2024

АНОТАЦІЯ

Яринюк Б. О. Розробка та оцінка додатку для аудиту безпеки в ОС Windows. Спеціальність 125 «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У бакалаврській роботі досліджується проектування та розробка програмного забезпечення для аудиту безпеки в операційній системі Windows. Основна мета полягає в аналізі та виявленні потенційних загроз безпеці, зокрема кібератак типу phishing та malware. Робота охоплює впровадження ефективних алгоритмів для виявлення вразливостей та забезпечення захисту системи. Окрема увага приділяється покращенню та оптимізації, що сприяє підвищенню ефективності аудиту безпеки в операційній системі Windows.

Ключові слова: безпека, аудит, операційна система Windows, кібератаки, вразливості.

42 с., 5 табл., 19 рис., 21 джерел.

ABSTRACT

Yarinyuk B. O. Development and evaluation of an application for security audit in Windows OS. Specialty 125 "Cybersecurity". Vasyl’ Stus Donetsk National University, Vinnytsia, 2024.

The bachelor's thesis investigates the design and development of software for security auditing in the Windows operating system. The primary goal is to analyze and identify potential security threats, particularly phishing and malware cyberattacks. The work encompasses the implementation of effective algorithms for detecting vulnerabilities and ensuring system protection. Special attention is given to improvements and optimizations that enhance the efficiency of security auditing in the Windows operating system.

Keywords: security, audit, Windows operating system, cyberattacks, vulnerabilities.

42 pp., 5 tables, 19 figures, 21 sources

ЗМІСТ

ВСТУП

У сучасному світі інформаційні технології є невід'ємною частиною діяльності будь-якої організації. Захист інформаційної інфраструктури стає критично важливим завданням, оскільки зростає кількість і складність кіберзагроз, таких як фішинг та шкідливе програмне забезпечення. Операційна система Windows, яка широко використовується в багатьох організаціях, потребує ефективного захисту від цих загроз. Проведення аудиту інформаційної безпеки, який включає використання спеціалізованого програмного та апаратного забезпечення, є важливим для забезпечення захисту даних, обробки та зберігання інформації. Актуальність дослідження полягає в необхідності розробки та впровадження ефективних методів аудиту безпеки, що дозволять вчасно виявляти і нейтралізувати загрози для ОС Windows.

Метою цього дослідження є захист операційної системи Windows від можливих кібератак, таких як фішинг та шкідливе програмне забезпечення, шляхом аналізу та впровадження програмного забезпечення для аудиту безпеки, яке підвищує ефективність використання ресурсів під час проведення аудиту.

Провести аналіз існуючих програмних засобів для аудиту безпеки операційної системи Windows.

Виявити потенційні загрози безпеці, зокрема кіберзагрози, такі як фішинг та шкідливе програмне забезпечення.

Впровадити та оцінити ефективність програмного забезпечення для аудиту безпеки.

Розробити рекомендації щодо підвищення ефективності використання ресурсів під час проведення аудиту безпеки.

Операційна система Windows та її безпека під час обробки, передачі та зберігання даних в організації.

Програмне забезпечення для аудиту безпеки операційної системи Windows, включаючи його розробку, алгоритми виявлення вразливостей та методи забезпечення захисту системи.Кваліфікаційна робота містить такі частини:

- У розділі першому представлені міжнародні стандарти, які дозволяють проводити аудит і використовувати їх в процесі аудиту. Представлені, а також порівняння конкретних стандартів використання;

- У розділі 2 розглядається принцип роботи програмного забезпечення для аудиту, що дозволяє оцінити рівень інформаційної безпеки;

- У розділі 3 прямий аудит інформаційної безпеки організації проводився з використанням програмних рішень, а також етапів і методів нейтралізації загроз в системах інформаційної безпеки.

РОЗДІЛ. 1 ОСНОВНІ ПОНЯТТЯ АУДИТУ БЕЗПЕКИ

1.1. Формулювання аудиту інформаційної безпеки та методи його виконання

Аудит інформаційної безпеки-це об'єктивне дослідження рівня безпеки в організації. Для виявлення прогалин в технічному захисті, що виникають в результаті неправильної настройки програм інформаційної безпеки в організації, при проведенні аудитів інформаційної безпеки використовуються різні методи, в тому числі різні аудити інформаційної безпеки [1].:

- Експертний аудит - цей метод аудиту враховує недоліки системи інформаційної безпеки з урахуванням досвіду експертів, що беруть участь в аудиті.

- Внутрішній аудит-оцінка механізму роботи організації, визначення філій, економічних відділів і т.д. Аудит внутрішніх компонентів організації для перевірки та оцінки управлінського аудиту.

- Зовнішній аудит-проводиться самою організацією, в тому числі фахівцями, які проводять аудит інформаційної безпеки.

- Оціночний аудит-використання цього методу включає перевірку відповідності певним стандартам сертифікації, стандартизації для поліпшення функціональної активності.

Впровадження аудиторських послуг відповідає за реалізацію важливих етапів:

- Політика безпеки;

- Особиста безпека;

- Моніторинг та перевірка відповідності міжнародним стандартам.;

- Аналіз та ідентифікація, перевірка оцінок вразливостей для прийняття відповідних заходів для мінімізації або нейтралізації наслідків.

Аудити можуть проводитися з використанням шаблонів або методів, що враховують різні політики інформаційної безпеки.

Загалом, існують стандарти, розроблені для того, щоб зовнішні та внутрішні експерти могли точно перевірити ефективність перевірок інформаційної безпеки.

Розділяючи обов'язки, ви повинні використовувати найкращі практики, які безпосередньо керують процесом аудиту, щоб забезпечити практичне здійснення аудиту.

Аудити повинні проводитися регулярно, щоб забезпечити належний захист даних. Крім того, Вам слід жовтня переглянути наступні дії:

- Змінити файл конфігурації;

- Встановіть або оновіть останнє програмне забезпечення;

- Придбання нового обладнання та програмного забезпечення, що вимагає належного післяопераційного контролю;

Аудит передбачає формування навичок використання інформаційних технологій. Крім того, аудитори безпосередньо взаємодіють із системою безпеки для забезпечення належного захисту та отримання сертифікатів, відповідальних за певні види захисту на основі інформаційних технологій.:

- Менеджер інформаційних систем (CISM);

- Управління інформаційними системами на основі управління ризиками (CRISC);

- Корпоративне управління IT (CGEIT);

- Аудитор інформаційних систем (CISA);

- Основи в області інформаційної безпеки;

- Спеціаліст з кібербезпеки Nexus (CSXP).

Таким чином, аудити вимагають комплексного підходу, і не всі заходи безпеки часто допомагають, і це може перешкодити нормальній роботі, оскільки для завершення роботи системи безпеки потрібен час. Це доставить незручності співробітникам, які тільки починають свою кар'єру [1].

1.2. Способи проведення аудиту

Найбільш поширеними методами аудиту є зовнішній і внутрішній відповідно до міжнародних стандартів на основі експертної оцінки. Зовнішній аудит

Це робиться на основі участі третіх осіб, які здійснюють прямий аудит. Внутрішні перевірки проводяться безпосередньо в організаціях, включаючи департамент безпеки [2].

Аудити, засновані на експертних оцінках, проводяться за участю експертів для оцінки відповідності ситуації з інформаційною безпекою підприємства. Використання міжнародних стандартів дозволяє оцінити відповідність організацій спеціальним стандартам, що становлять інформаційну безпеку підприємства. Виконавець аудиту виглядає наступним чином:

- Урядові установи-перш за все, їх вчать, що вони є потенційними партнерами, які проводять аудит інформаційної безпеки і регулюють всі питання аудиту.

- Внутрішні аудитори-прямі аудити проводяться під наглядом керівника організації і можуть проводитися тільки аудиторами, найнятими або створеними організацією.

- Зовнішні аудитори, як правило, є сторонніми організаціями, які можуть проводити аудити інформаційної безпеки та проводити високопрофесійні аудити.

- Спеціаліст з інформаційної безпеки - завдяки такій організації контролюється система безпеки і підтримується баланс ризиків всередині організації.

Основними завданнями, в яких бере участь аудитор інформаційної безпеки, є:

- Встановлення професійної оцінки, тобто забезпечення особистої безпеки організації, виявлення технічних проблем доступу та забезпечення безпеки шляхом їх негайного усунення відповідно до обслуговування та відповіді.

- Підготовка та планування - Аудитор може виконати цей крок на основі інформації, отриманої в результаті оцінки експертів. Завдяки такій оцінці можна скласти плани та докази для перевірки лише певних частин організації. Це дозволяє оцінити кошти, необхідні для вирішення конкретної проблеми, без проведення постійних перевірок[21].

- Мета аудиту виникає тільки тоді, коли аналізуються всі фактори або ризики, які можуть вплинути на збільшення частоти ризиків.

- Проведення перевірок - всі можливі дані збираються для виявлення можливих порушників. Це включає затвердження чітко визначених цілей аудиту.

- Підготовка аудиторських звітів-після завершення всіх аудиторських процедур створюється відповідний документ з усіма можливими змінами, поліпшеннями і рекомендаціями, які повинні бути представлені організації для участі в розробці політики інформаційної безпеки та захисту інформації в організації.

- Формування кінцевого результату-кінцевий результат пов'язаний зі складеним аудиторським висновком, містить всі розглянуті запити і пояснює, з чого складається цей аудит.

Вся ця інформація не повинна класифікуватися як дозволений доступ. Як правило, результати зазвичай вказують на рекомендації, які необхідно реалізувати для поліпшення систем інформаційної безпеки в організації.

1.3. Відповідність аудиту, міжнародним стандартам

Кожен стандарт відповідності має свої власні вимоги, але багато правил суперечать один одному. Наприклад, HIPAA захищає медичні дані, а PCI-DSS захищає фінансові дані, але обидва є подібними вимогами для шифрування даних, зберігання конфіденційної інформації та контролю доступу до запитів.Першим кроком до забезпечення відповідності є визначення стандартів, що стосуються вашого бізнесу.

Щоб розробити найефективніший дизайн, спочатку потрібно створити інфраструктуру, яка відповідає вашим потребам, але традиційні компанії, можливо, побудували існуючу інфраструктуру кілька десятиліть тому. Стандарти відповідності постійно переглядаються та оновлюються, тому необхідно створювати та аналізувати нові правила. Якщо ваша організація не застосовує нові правила відповідності до вашої існуючої інфраструктури, ви можете порушити їх і понести серйозні штрафи.

Більшість стандартів поділяються на наступні категорії в контрольному списку відповідності IT: [3]:

Контроль доступу та ідентифікації - цей стандарт визначає правила аутентифікації та авторизації.

Управління обміном даними. Організації повинні суворо контролювати дані, передані громадськістю та клієнтами.

Реакція на інцидент. Це положення наказує організаціям скорочувати, повідомляти і розслідувати кількість витоків даних.

Аварійне відновлення. Якщо ваша інфраструктура виходить з ладу, вашій організації потрібно створити резервну копію та відновити продуктивність. Стандарти аварійного відновлення скорочують час простою і гарантують, що

продуктивність і прибуток не постраждають.

Запобігання втрати даних. Це залежить від того, що вам потрібно зробити для захисту ваших ділових інтересів та продуктивності, таких як резервне копіювання, відновлення та резервне копіювання, щоб запобігти втраті даних.

Захист від шкідливих програм. Антивірусні та інші засоби захисту від шкідливих програм захищають вашу інфраструктуру від шкідливого коду, і кожен стандарт вимагає цього в різних середовищах, включаючи сервери та користувацькі пристрої.

Корпоративна політика безпеки. Організації повинні розробити політику, яку користувачі повинні дотримуватися, щоб захистити свої дані.

Моніторинг та звітність. Без моніторингу організації завжди вразливі до загроз. Створення звіту дає адміністраторам можливість перевірити продуктивність своїх систем.

Організації повинні створювати системи для захисту конфіденційності та безпеки даних клієнтів. Існує кілька основних причин для стандартів IT-безпеки:

1. Допомагають розробляти стратегії інформаційної безпеки, пропонуючи найкращі практики.

2. Недотримання може призвести до витоків даних. Інші переваги включають:

- Кращий контроль безпеки праці, менше помилок і загроз.
- Зменшення фінансових втрат від порушень даних.
- Підвищення безпеки та довіри клієнтів.

Найпоширеніші стандарти IT-безпеки включають:

- GDPR – закон ЄС про захист даних [3].
- HIPAA – федеральний закон США про медичні дані.
- PCI DSS – стандарт для захисту даних карток, створений у 2004 році.
- NIST – ресурс для технічної безпеки.
- FISMA – закон США про інформаційну безпеку, прийнятий у 2002 році.
- CIS Controls – заходи для захисту від кібератак [11].

Для визначення необхідного аудиту зверніться до адвоката або фахівця з

інформаційної безпеки. IT-відповідність орієнтована на три типи даних [4]:

1. Особиста інформація (ім'я, адреса, біометричні записи).

2. Захищена медична інформація (медичні записи).

3. Фінансові дані (номери карток, фінансова звітність).

Визначте, які стандарти необхідно дотримуватися, і призначте відповідальну особу. GDPR і PCI DSS вимагають призначення Data Protection Officer (DPO), що має багато переваг [5]:

- Спеціалізується на праві інформаційної безпеки.
- Відстежує дотримання вимог та зміни.
- Швидко повідомляє про порушення безпеки.

Для вдосконалення політики безпеки оцініть ризики, включаючи загрози, важливі активи та поточний рівень захисту. Незалежний аудит необхідний після розробки нових політик. Самоконтроль допомагає оцінити поточні рівні відповідності та виявити прогалини. Дотримуйтеся інструкцій з аудиту, таких як оцінка за стандартами NIST, GDPR та HIPAA.

Самоконтроль має високу вартість, але допомагає скласти список політик і технічних засобів для проходження аудиту інформаційної безпеки.

1.4. Програми для проведення аудиту інформаційної безпеки

Після прийняття всіх можливих рішень ви можете безпосередньо контролювати безпеку інформаційної системи за допомогою програми, яка сканує найпоширеніші вразливості в системі.:

- Burp Suite-це модульний браузер для виконання тестів безпеки у веб-програмах.
- OpenVAS-це повнофункціональний сканер вразливостей з можливістю тестування [12].
- Сканер Nmap для аналізу та аудиту мережевої безпеки.
- Nessus-це сканер вразливостей, який визначає рівень захисту інформаційної безпеки на основі виявлення поширених вразливостей та конфігурації

менеджера інформаційної безпеки.

Burp Suite - найпоширеніший інструмент, який використовується для оцінки безпеки веб-додатків. Інструмент доступний у версіях Burp Suite Community Edition, Burp Suite Professional та Burp Suite Enterprise Edition. Основними інструментами, доступними за допомогою Burp Suite, є:

- Spider - завдяки йому кінцева точка буде доступна для моніторингу її функціональності і пошуку можливих вразливостей. Основною метою використання цього модуля є пошук кінцевих точок для виявлення та нейтралізації вразливостей під час виявлення або тестування для виявлення можливих вразливостей.

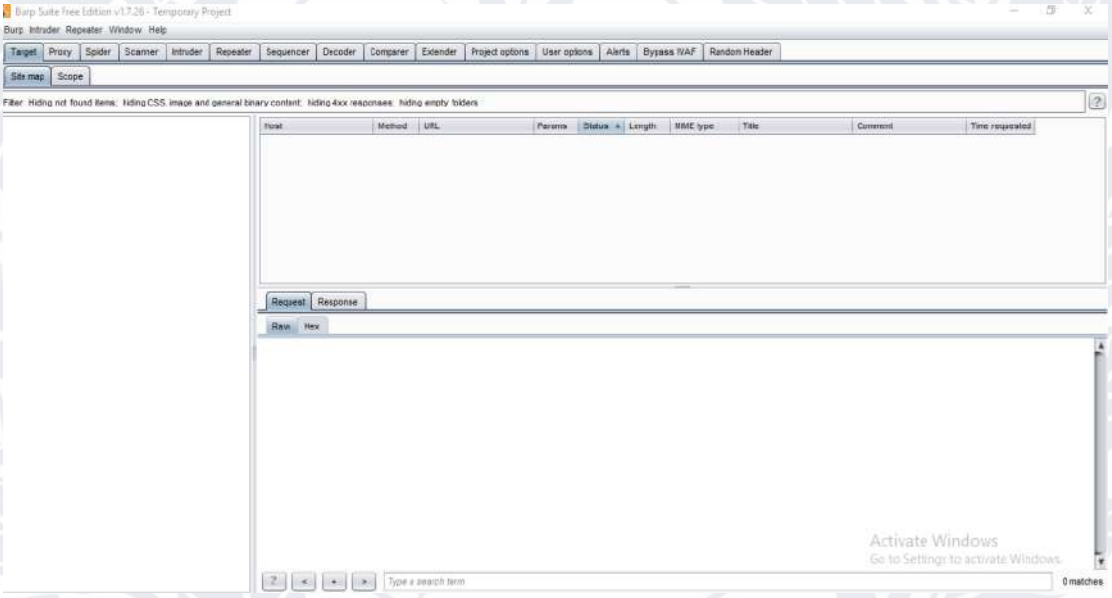


Рисунок 1.1 – Головне вікно модуля Spider

Проксі-сервер-дозволяє переглядати і змінювати вміст відповіді при його відправці. Проксі-сервер можна налаштувати для роботи із заданою зворотною IP-адресою та спортом. Проксі-сервер також можна налаштувати наступним чином

Ретранслятор-використовується для перевірки введених значень, оцінки виконання, перевірки параметрів запиту, перевірки чистоти даних сервера, виявлення несподіваних значень і помилок під час передачі даних, перевірки реалізації захисту CSRF і перевірки можливості повторної відправки запитів з

ручними змінами

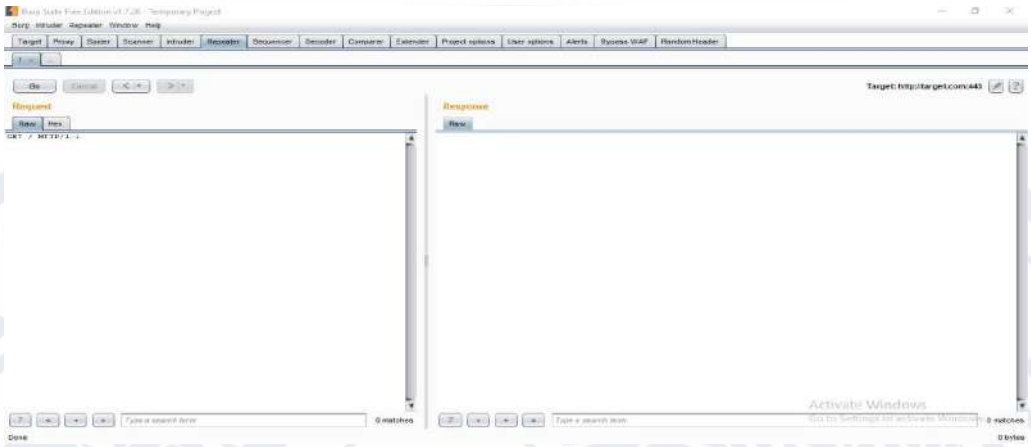


Рисунок 1.2 – Головне вікно модуля Repeater

Sequencer -це перевірка ентропії, яка перевіряє випадковість маркерів, що генеруються веб-сервером. Ці маркери використовуються для автентифікації в конфіденційних транзакціях, прикладами таких маркерів є файли cookie та маркери анти-CSRF

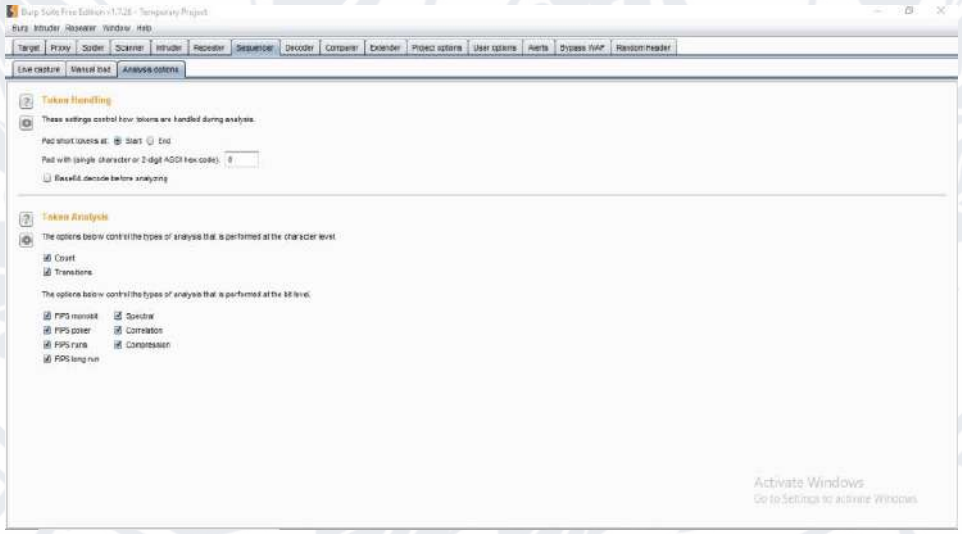


Рисунок 1.3 – Головне вікно Sequencer

Декодер, який може розшифровувати URL, HTML, Base64, Hex тощо, включає список розповсюджених методів кодування. Цей інструмент корисний при аналізі даних у значеннях параметрів або заголовках, допомагаючи виявити фрагменти інформації. Він також використовується для створення корисних пейлоадів для різних класів вразливостей.:

Рисунок 1.4 – Головне вікно Decoder

Extender – модулі завдяки яким розширюються можливості як використанняBurp Suite, проведення аудитів, тестів, різноманітних компонентів

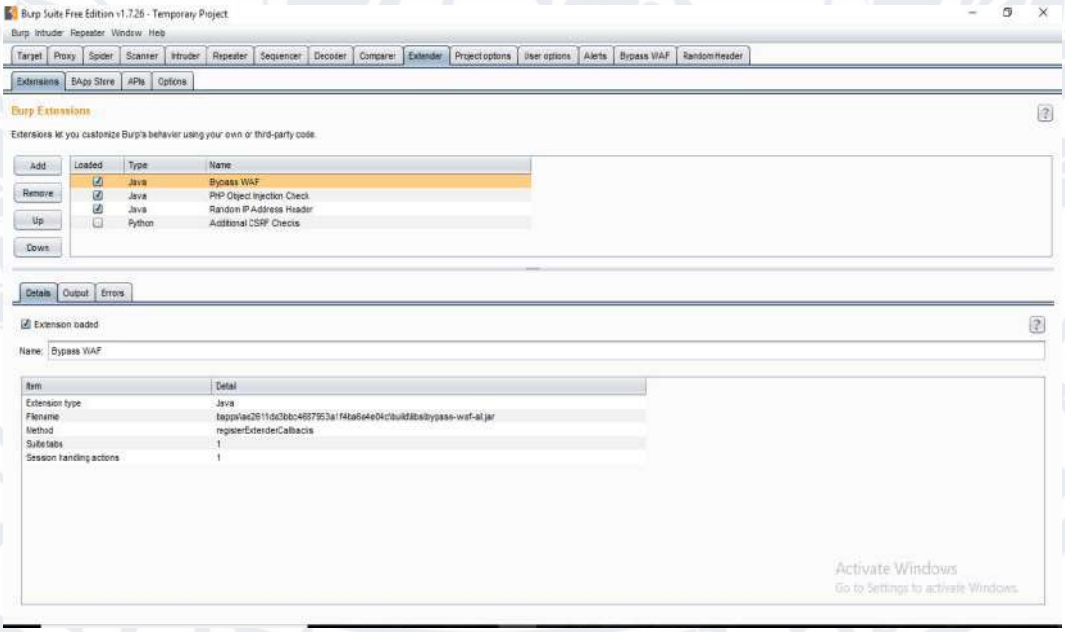


Рисунок 1.5 – Головне вікно Extender

Браузер-автоматично сканує веб-сайти на наявність безлічі поширених вразливостей і перераховує інформацію про надійність кожної помилки і

складності її використання. Однак браузер недоступний у версії Community Edition[21].

Nmap-це інструмент, який використовується для сканування IP-адрес, що працюють в мережі, виявлення відкритих портів і служб, а також для виявлення вразливостей. Основними функціями Nmap є:

Допомагає ідентифікувати служби, що працюють в мережі;
nmap може знайти інформацію про операційну систему, що працює на пристрої. Зберіть статистику про мережевий трафік.

Nmap також пропонує гнучкі функції призначення та порту, сканування, сканування SunRPC. Більшість платформ Unix та Windows підтримуються як у графічному інтерфейсі, так і в режимі командного рядка.

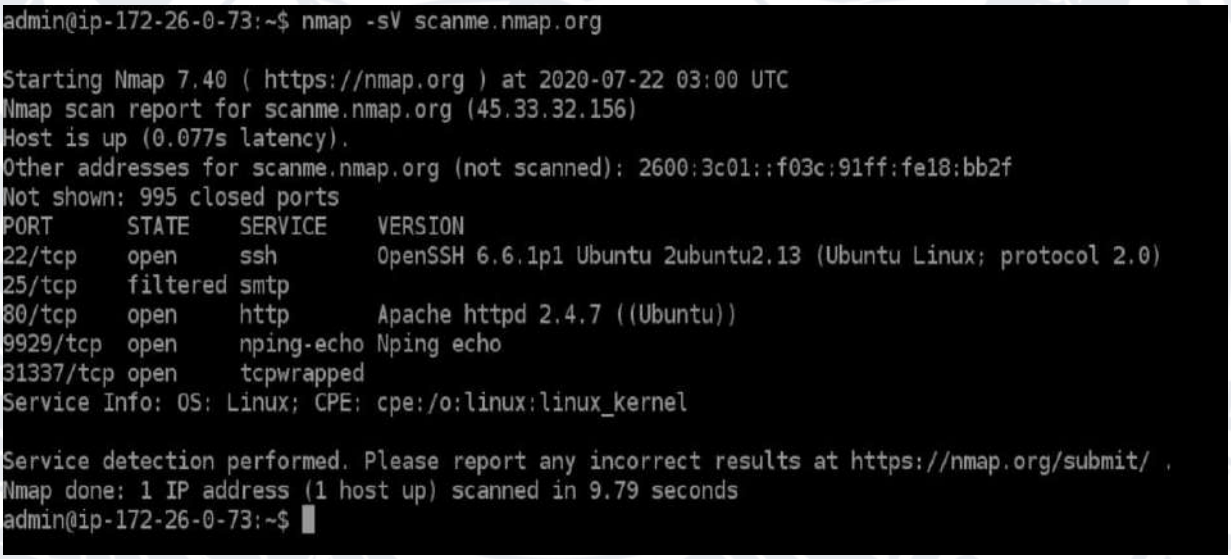


Рисунок 1.6 – Інтерфейс командного рядка nmap

OpenVAS-це повнофункціональний сканер вразливостей, який виявляє застарілі мережеві служби, відсутні виправлення безпеки, погано налаштовані сервери та інші вразливості. жовтень. Він також інтегрується з багатьма іншими популярними платформами безпеки, такими як OSSEC та Snort. Особливості включають [12] :

- Підтримка сканування вразливостей для 26 000 CVE;

- Доступний веб-інтерфейс;

- Експорт звітів про вразливості у формати Html, PDF та CSV;

Nessus-це інструмент, який використовується для перевірки вразливостей, які хакери можуть використовувати для отримання конфіденційної інформації.

Nessus перевіряє кожен порт на комп'ютері, щоб визначити, яка служба запущена, а потім перевіряє цю службу, щоб хакери могли здійснювати шкідливі атаки. Функції програми полягають в наступному::

- Сканування на наявність вразливостей в системі безпеки, які можуть дозволити несанкціонований контроль або доступ до конфіденційних даних;

- Виявлення несанкціонованих конфігурацій системи безпеки.

- Сканування тимчасових кінцевих точок, які не завжди підключені до локальної мережі.

- Підвищення загальної продуктивності сканування: агент сканування мережі дозволяє сканувати віддалену мережу, щоб прискорити час завершення сканування.

Nessus використовує надбудову, яка працює на всіх хостах мережі, для сканування та виявлення вразливостей.

1.5. Висновки до розідлу 1

У першому розділі бакалаврської роботи було проведено огляд основних понять аудиту інформаційної безпеки. Зокрема, було визначено різні методи проведення аудиту, включаючи експертний, внутрішній, зовнішній та аудит на основі оцінки. Були розглянуті ключові етапи проведення аудиту, серед яких політики безпеки, управління і перевірка відповідності міжнародним стандартам, а також аналіз і виявлення вразливостей. Проведений огляд акцентував увагу на важливості регулярного проведення аудиту для підтримання високого рівня захисту даних і відповідності новітнім стандартам безпеки.

РОЗДІЛ 2. МЕХАНІЗМ ФУНКЦІОНУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АУДИТУ

2.1. Логування у Windows

Аудит безпеки Windows-це функція Windows, яка допомагає захистити безпеку вашого комп'ютера та корпоративної мережі. Аудит Windows призначений для моніторингу активності користувачів, аналізу та розслідування інцидентів безпеки, а також усунення загроз. Аудити безпеки дозволяють застосовувати політику безпеки у вашому середовищі відповідно до корпоративних, державних або промислових вимог.

Аудит безпеки є одним з найбільш ефективних інструментів, що пропонує операційна система Windows для збереження цілісності системи. Ви можете активувати перевірку безпеки Windows за допомогою групової політики або локальної політики безпеки. Відкрийте панель керування Windows, оберіть "Адміністрування", після чого запустіть "Локальні політики безпеки". Відкрийте розділ локальної політики та виберіть політику аудиту. На правій панелі вікна Локальні політики безпеки відобразиться перелік політик аудиту. [13].

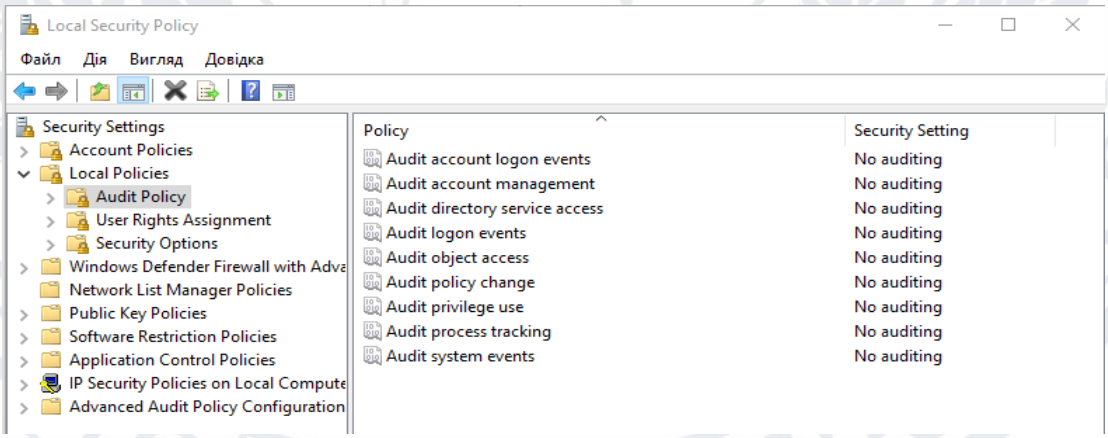


Рисунок 2.1 — Налаштування політики аудиту

Політика аудиту повинна розглядатися як частина загальної стратегії безпеки, а рівні аудиту повинні визначатися індивідуально для кожного середовища. Аудит

виявляє атаки, які становлять загрозу для IT-інфраструктури (успіх чи невдача), а також атаки на ресурси, які були визначені як цінні при оцінці ризиків.

2.2. Методи оцінки рівня інформаційної безпеки

Саме параметри політики аудиту визначають, які події слід реєструвати в журналі подій. Додаткові параметри політики аудиту безпеки, доступні для операційних систем Windows у Windows Server2008R2 та Windows 7 та новіших версіях, ви можете дізнатися, як вони працюють.

Загалом 53 параметри політики аудиту безпеки допомагають організаціям застосовувати критичні правила щодо бізнес-процесів та безпеки, виконуючи чітко визначені дії, такі як адміністратор групи змінив налаштування та дані на сервері. Певна група співробітників отримала доступ до важливих файлів. Правильний список контролю доступу до системи (SACL) - це надійний захист від невиявленого доступу [13], який включає всі файли, папки або файли на комп'ютері.

Ці 53 параметри дозволяють вибирати лише поведінку, яку потрібно відстежувати (відображається у списку реєстру подій), і виключати результати аудиту для поведінки, яка не представляє особливого інтересу або не має значення для повного імені. Крім того, політики аудиту безпеки Windows 7 і Windows Server2008R2 можуть застосовуватися з використанням групових політик домену, що дозволяє відносно легко змінювати, тестувати і розгортати параметри політики аудиту для обраних користувачів і груп. Налаштування політики аудиту параметри політики доступні в наступних категоріях:

2.3. Журнали подій Windows

Журнал подій Windows призначений для фіксації та зберігання важливих даних про апаратні та програмні події.

- Додаток: зберігає події, зареєстровані програмою. Наприклад, додаток

для роботи з базами даних може фіксувати помилки файлів. Розробник визначає, які саме події слід записувати.

- Безпека: фіксує спроби входу з правильними та неправильними обліковими даними, а також події, пов'язані з видаленням, переміщенням або відкриттям файлів та інших об'єктів. Адміністратори можуть ініціювати аудит та реєструвати події в журналі безпеки.

- Система: містить події, що стосуються драйверів системних пристроїв.

- CustomLog: особистий журнал додатків, що зберігає події, записані розробником програми. Використовуючи ці журнали, ваша програма може контролювати розмір файлів журналу та підвищувати рівень безпеки, не впливаючи на інші програми.

Централізована служба журналу використовується програмами та компонентами операційної системи для запису завершених операцій через інтерфейс програмування (API). Події з усіх джерел зберігаються в єдиному журналі подій, і користувачі можуть використовувати переглядач подій для доступу до потрібної інформації:

- Ідентифікатор події (EventID);
- Типи подій;
- Категорія події;
- Масив рядків;
- Двійкові дані.

Кожне джерело подій має власний файл повідомлень, який містить ідентифікатори повідомлень, параметри та описи категорій. Система використовує EventID для унікальної ідентифікації подій, що можуть статися в Windows.

Цей журнал є критично важливим інструментом для адміністраторів та розробників, дозволяючи їм відслідковувати та аналізувати різні події для підтримки стабільності та безпеки системи.

Таблиця 2.1 Типи подій

Тип події	**Опис події**
Успішний аудит	Подія безпеки, яка створюється при успішному доступі до ресурсу і перевіряється відповідно до параметрів локальної політики аудиту. Наприклад, успішний Користувач вийшов із системи або успішно видалив файл.
Не успішний аудит	Подія безпеки, яка створюється при успішному доступі до ресурсу і перевіряється відповідно до параметрів локальної політики аудиту. Наприклад, логін користувача, зазнав невдачі.
Помилка	Події, які генеруються якщо зафіксована некоректна подія що ймовірно призведе до втрати даних або спричинить припинення функціонування частини системи. Наприклад збій роботи драйверів.
Попередження	Цей тип інциденту вказує на те, що вам не потрібно негайно втручатися, але ігнорування проблеми може призвести до помилок і збоїв. Наприклад Переповнення жорсткого диска.
Інформація	Цей тип події вказує на успішне виконання з важливих рідкісних операцій.

2.4. Структура Zabbix

Архітектура системи моніторингу Zabbix складається з двох найважливіших частин: агента та сервера. Сервер Zabbix лежить в основі програмного процесу zabbix. Сервер опитує та фіксує дані, обчислює тригери та надсилає сповіщення користувачам. Це центральний компонент, за допомогою якого агенти та проксі-сервери Zabbix повідомляють про доступність та цілісність системи. Сам сервер може дистанційно керувати мережевими службами (такими як веб-сервери та поштові сервери) за допомогою простого елемента керування[6].

Сервер виступає як центральне сховище, де зберігаються усі конфігураційні, статистичні та операційні дані. Він не лише надає можливість адміністратору вчасно виявляти проблеми в будь-якій системі, яку він контролює, але й активно повідомляє про ці проблеми. Робота серверів на базі Zabbix складається з трьох окремих компонентів: самого сервера Zabbix, веб-інтерфейсу та зберігання бази даних.

Сервер Zabbix звертається до агентів для отримання різноманітних даних, таких як завантаження процесора. Отримані від агента дані потім зберігаються в базі даних.

Активний режим моніторингу в реальному часі відрізняється своєю поведінкою. Спочатку агент отримує від сервера Zabbix список елементів, які потрібно відстежувати. Після цього агент надсилає нові дані на сервер у визначений період часу.Виконання пасивної або активної перевірки налаштовується шляхом вибору відповідного типу контрольного елемента. Агент Zabbix обробляє такі елементи, як" агент zabbix "та"агент zabbix (увімкнено)".

Вся інформація про конфігурацію Zabbix зберігається в базі даних, з якою взаємодіють як сервер, так і веб-інтерфейс. Наприклад, при створенні нового Елементи додаються до таблиці елементів у базі даних через веб-інтерфейс (або API). Потім приблизно 1 раз на 1 хвилину сервер zabbix запитує список активних елементів у таблиці елементів і зберігає їх у кеші на сервері Zabbix

Агент Zabbix може обробляти локальні ресурси та програми (жорсткі диски, пам'ять, статистику процесора тощо).) був розгорнутий для цілей моніторингу, щоб активно відстежувати.).). Агент збирає дані від клієнта та надсилає зібрану інформацію на сервер Zabbix для подальшої обробки. У разі збою (наприклад, при переповненні жорсткого диска або в процесі аварійного обслуговування) Zabbix server завчасно повідомляє адміністратора конкретної машини про збої.

Агент Zabbix дуже ефективний, оскільки використовує вбудовані системні виклики для збору статистики. Пасивний та активний контроль агенти Zabbix можуть виконувати пасивний та активний контроль. При пасивній перевірці агент відповідає після того, як сервер надсилає агенту запит [7].

2.5. Висновки до розділу 2

У другому розділі було розглянуто принципи роботи програмного забезпечення для аудиту інформаційної безпеки. Проведено огляд різних інструментів, таких як Burp Suite, OpenVAS, Nmap і Nessus, які використовуються для моніторингу та аудиту інформаційних систем. Детально описано структуру Zabbix, включаючи його функціональні можливості та принципи роботи. Було показано, як ці інструменти можуть бути використані для оцінки рівня безпеки та виявлення вразливостей, що дозволяє підвищити загальний рівень інформаційної безпеки системи.

РОЗДІЛ. 3. ІНТЕГРАЦІЯ СИСТЕМИ МОНІТОРИНГУ

3.1. Відстеження та керування обліковимм записом користувача

У постанові Ради Міністрів України “від 2019-6-6 рр. № 518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" в пунктах 19-23 [15] йдеться про архітектуру IT-інфраструктури та політику безпеки організації, а також про перелік засобів, необхідних для забезпечення безпеки. перевірка подій проводиться Міністерством критичної інфраструктури. Проаналізувавши вищевказані вимоги до реєстрації подій на об'єкті La. Незважаючи ні на що, була створена система моніторингу.:

- Аудит управління обліковими записами
- Аудит доступу до об'єктів файлової системи
- Аудит цілісності системи

Щоб реєструвати події входу / виходу користувача в журнал подій Windows, необхідно включити відповідні параметри системного аудиту

Перевірка облікових даних для аудиту подій аудиту за допомогою облікових даних, які операційна система надсилає для запиту входу в обліковий запис Користувача. Ці події відбуваються на комп'ютерах, яким дозволено використовувати облікові дані (локальному комп'ютеру дозволено локальний обліковий запис).

Служба автентифікації Kerberos визначає, чи слід генерувати події автентифікації для запитів, які надають запити автентифікації Kerberos (tgts).Під час налаштування цього параметра політики подія аудиту генерується після запиту автентифікації kerberos (TGT). Аудит успіху реєструє успішні спроби, а аудит невдачі - невдалі спроби[8].

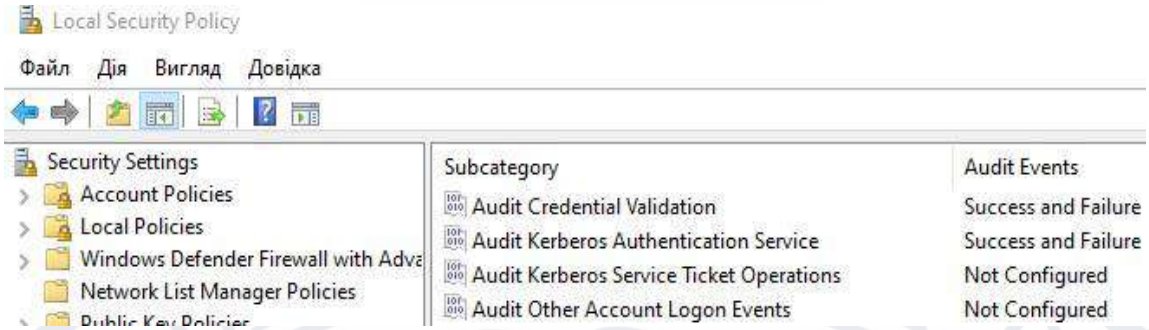


Рисунок 3.1 — Політика аудиту для реєстрації подій входу / виходу з облікового запису Користувача.

Щоб зберегти дії щодо видалення, блокування та збереження облікових записів користувачів, перейдіть на вкладку Керування обліковими записами комп'ютерів та обліковими записами користувачів у розділі категорії.

Аудит управління обліковими записами комп'ютерів-це параметр політики, який допомагає відстежувати зміни, пов'язані з обліковим записом, на комп'ютерах, що належать домену, на яких операційна система генерує події аудиту під час створення, зміни або видалення облікового запису комп'ютера.

Елемент керування обліковими записами користувачів дозволяє переглядати зміни в облікових записах користувачів. Події включають наступне:

- Обліковий запис Користувача було створено, змінено, видалено, перейменовано, деактивовано, увімкнено, заблоковано або розблоковано;

- Пароль облікового запису Користувача встановлено або змінено;

- Ідентифікатор безпеки (SID) був доданий або не доданий до історії Sid облікового запису Користувача;[21]

- Настроюваний пароль для режиму відновлення служби каталогів;

- Змінено дозволи для облікового запису адміністратора;

- У списку відображається членство користувачів в локальній групі;

- Облікові дані адміністратора облікового запису були створені або відновлені.

Нижче описані події ідентифікатора події, які повинні бути зареєстровані

під час аудиту облікового запису[8].

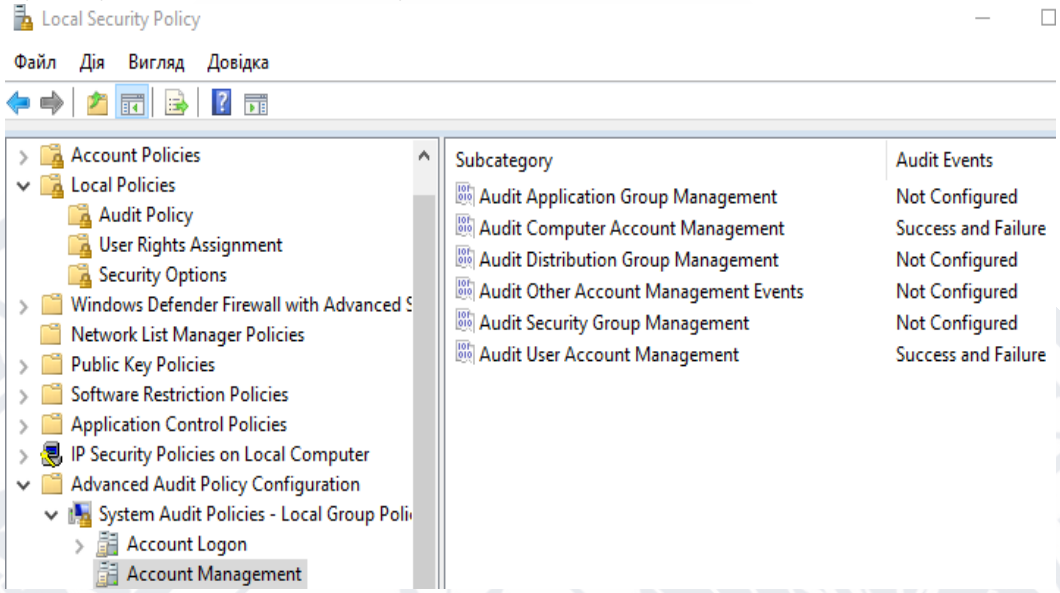


Рисунок 3.2 — Політика аудиту для ведення журналу подій видалення та створення облікових записів користувачів.

3.2. Аудит доступу до елементів системи

Для забезпечення аудиту доступу до об'єктів файлової системи система моніторингу повинна взаємодіяти з параметрами аудиту файлової системи для цих об'єктів. Події аудиту генеруються тільки для об'єктів, що мають спеціальний системний список контролю доступу (System Access Control List), і лише тоді, коли тип запитуваного доступу та обліковий запис, що надсилає запит, відповідають параметрам, заданим у Sacl.

Системний список контролю доступу (System Access Control List) визначає, як перевіряється доступ до файлів і папок і є механізмом делегування подій. Sacl використовується для встановлення загальносистемної політики безпеки, зокрема для ведення журналу та аудиту доступу до ресурсів. Об'єкти, що мають Sacl, являють собою системні каталоги або файли, які перевіряють принципи безпеки (користувачів, груп, комп'ютерів) під час доступу до них.Як правило, списки контролю доступу налаштовуються для важливих об'єктів файлової системи. Можна генерувати події політики файлової системи аудиту в масштабах всієї системи, але на практиці це призводить до виникнення занадто

великої кількості подій, тому неможливо згенерувати подію політики файлової системи аудиту для всієї системи.

Таблиця 3.1 Події роботи з файловою системою[21]

ID	Опис
4656	Розпізнає момент ініціації роботи з файлом.
4663	Визначає проведену дію з об'єктом.
4660	Визначає операцію видалення.
4658	Визначає завершення взаємодії з файлом.
4670	Була здійснена зміна режиму контролю доступу.

3.3. Аудит цілісності системи

Для забезпечення цілісності даних і програмного забезпечення використовуйте параметр цілісності системи аудиту. Цілісність системи аудиту визначає, чи перевіряє операційна система події, що порушують цілісність підсистеми безпеки. До числа дій, що порушують цілісність підсистеми безпеки, відносяться::

- Збій системи аудиту призводить до втрати перевіряються подій;

-Цей процес може бути використаний для уособлення клієнта, відповіді на запити адресного простору клієнта, читання в адресному просторі клієнта або читання адресного простору клієнта.;

- Порушення цілісності віддаленого виклику процедури (RPC);

- Порушення цілісності коду з неприпустимим значенням хешу виконуваного файлу;

- Виконання операцій шифрування [20].

Таблиця 3.2 Події що входять до Audit System Integrity

EventID	**Опис**
4612	Внутрішні ресурси, виділені для черги аудиторських повідомлень, були вичерпані, що призвело до втрати деяких аудитів.
4615	Недійсне використання порту LPC (Local Procedure Call).
4618	Був зафіксований події безпеки за відстеженим шаблоном.
4816	Під час розшифрування вхідного повідомлення RPC (Remote Procedure Call) виявлено порушення цілісності.
5038	Перевірка цілісності коду виявила недійсний хеш-зображення файлу. Це може бути наслідком несанкціонованих змін у файлі або вказувати на можливість помилки пристрою, що призвела до недійсного хеш-диска.
5056	Було проведено криптографічне самотестування.
5057	Під час криптографічної маніпуляції сталася помилка у виконанні операції.
5060	В процесі перевірки виник збій.
5061	Криптографічна операція.
6281	Запис на цілісність коду сигналізує про те, що хеш сторінки у файлі зображення недійсний. Така невідповідність може виникнути через неправильну підписку файлу без відповідного хешу або пошкодження в результаті несанкціонованих змін. Помилковий хеш також може свідчити про можливу несправність дискового пристрою.
6410	Виявлено, що файл не відповідає встановленим стандартам безпеки для безпечного завантаження в процес.
5062	Було проведено криптографічне самотестування у ядрі системи.

3.4. Конфігурація системи відстеження подій

Zabbix-це рішення для розподіленого моніторингу серверів

корпоративного класу з відкритим кодом. Це корисне програмне забезпечення, що використовується розробниками для моніторингу продуктивності і цілісності серверів, віртуальних машин, додатків, служб, баз даних, веб-сайтів, хмар і т.д., а також великої кількості мережевих параметрів. Zabbix використовує гнучкий механізм сповіщень, який сповіщає користувачів про проблеми через безліч платформ, таких як електронна пошта, Slack, Jira та Brevis.One і т.д. [9].

1. Однією з його головних переваг є те, що це програмне забезпечення з відкритим кодом.Це означає, що програма повністю безкоштовна, а також дозволяє візуалізувати ваші дані.

Сервер Zabbix збирає і аналізує дані від усіх агентів і забезпечує коректне представлення даних. Він також надає Настроюваний і простий спосіб інтерпретації веб-інтерфейсів / панелей інструментів за допомогою різних графіків, мережевих карт, слайд-шоу та звітів.

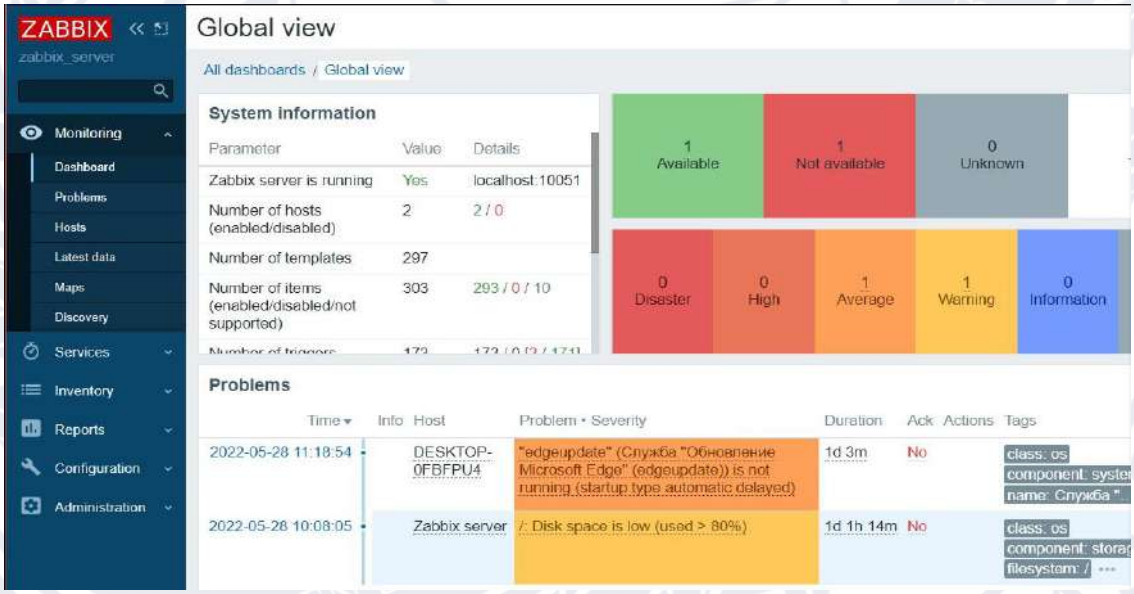


Рисунок — 3.3 Web-інтерфейс Zabbix

З точки зору користувача, Zabbix розділений на дві великі частини: сервер та агент. Сервер знаходиться на одному комп'ютері, який збирає та зберігає статистичні дані, а агенти на цих комп'ютерах збирають дані для подальшої передачі на сервер.

Відповідно до вимог, викладених у пункті 19-23 постанови Кабінету

Міністрів України № 518 від жовтня 2019-6-19 "Про затвердження Загальних вимог до кібербезпеки критично важливих об'єктів інфраструктури", аудиторські дані збираються з додаткових хостів на серверах Zabbix [15][17].

Реєстрація події містить інформацію про дату та час реєстрації події, тип та ступінь досягнення. Тут більш докладно описані такі відомості, як імена користувачів, імена систем, ідентифікатори процесів і мережеві об'єкти.

Система моніторингу Zabbix реалізує систему, яка збирає, зберігає та аналізує журнали подій програмного та апаратного забезпечення вузлів IT-інфраструктури. Для зручності перегляду адміністратору необхідно створити шаблон відстеження.

Результати моніторингу обладнання IT-інфраструктури зберігаються в базі даних Zabbix server. Щоб заархівувати дані трасування, потрібно скинути базу даних на інший носій.

Якщо у вас є елементи збору даних та тригери, які винятково переходять у стан "проблема", корисно мати механізм оповіщення, який сповіщає про важливі події, коли ви не можете безпосередньо вивчити веб-інтерфейс[9].

Сповіщення електронною поштою - найпоширеніший спосіб надсилання повідомлень. Тому налаштуйте їх спеціально. Для цього перейдіть на панель "адміністрування" – "тип носія" і виберіть "пошта" зі списку попередньо налаштованих методів повідомлення.

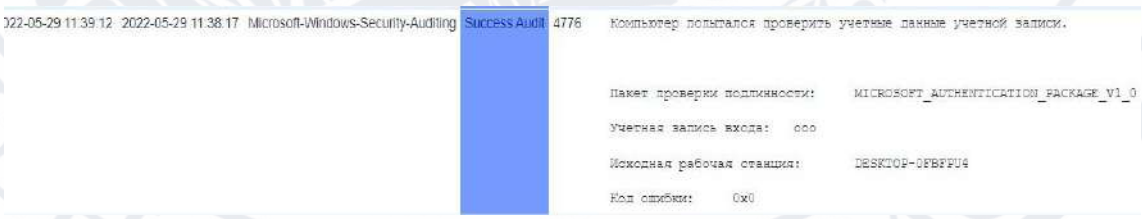


Рисунок 3.4 — Запис даних аудиту з хостів Zabbix

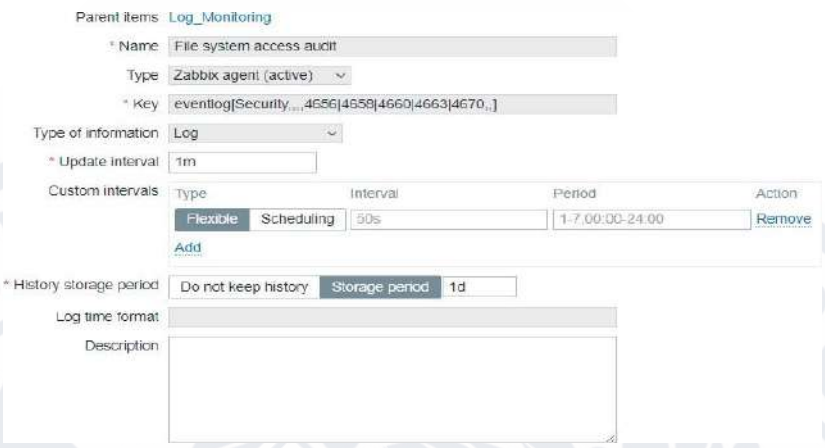
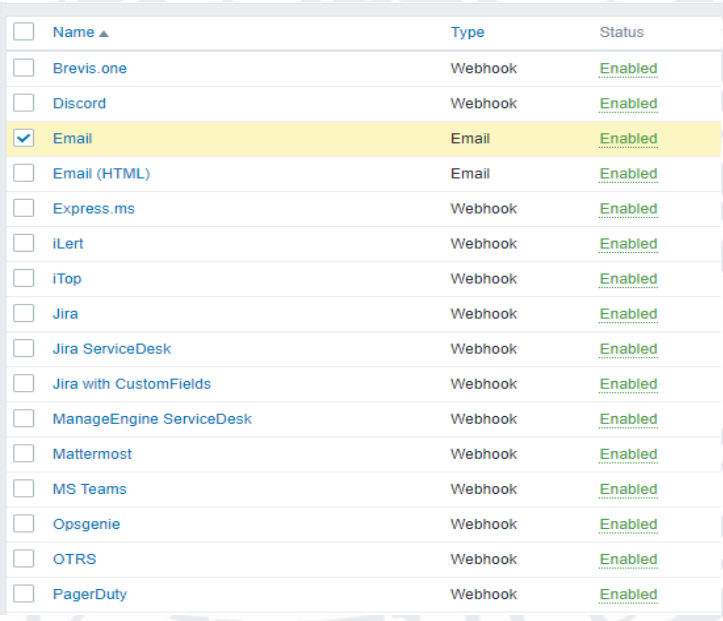


Рисунок 3.5 — Створення шаблону моніторингу

Name ▲	Triggers	Key	Interval	History	Trends	Type
Audit of account management		eventlog[Security,,,,4624|4625|4648|4672|4647|4776|4771| 4720|4722|4723|4724|4725|4726|4738|4740|4767|4781|4794|4741|4742|4743,,]	1m	1d		Zabbix agent (active)
Audit system integrity		eventlog[Security,,,,4612|4615|4618|4816|5038|5036|5057|5060|5061|6281|6410|5062,,]	1m	1d		Zabbix agent
File system access audit		eventlog[Security,,,,4656|4658|4660|4663|4670,,]	1m	1d		Zabbix agent (active)

Рисунок 3.6 — Список шаблонів моніторингу



Name ▲	Type	Status
Brevis.one	Webhook	Enabled
Discord	Webhook	Enabled
Email	Email	Enabled
Email (HTML)	Email	Enabled
Express.ms	Webhook	Enabled
iLert	Webhook	Enabled
iTop	Webhook	Enabled
Jira	Webhook	Enabled
Jira ServiceDesk	Webhook	Enabled
Jira with CustomFields	Webhook	Enabled
ManageEngine ServiceDesk	Webhook	Enabled
Mattermost	Webhook	Enabled
MS Teams	Webhook	Enabled
Opsgenie	Webhook	Enabled
OTRS	Webhook	Enabled
PagerDuty	Webhook	Enabled

Рисунок 3.7 — Список варіантів сповіщення

Zabbix дозволяє вам вибрати більшість доступних вам медіа та соціальних сервісів або підключити свої власні, використовуючи опцію Створити тип

Мультимедіа. Zabbix забезпечує повний робочий процес, включаючи можливість відправляти оповіщення, переглядати отриману інформацію, передавати її іншим користувачам і застосовувати дії. Натисніть на електронний лист, щоб відкрити вікно налаштувань. У стовпці електронна пошта SMTP введіть адресу відправника повідомлення та параметри мережевого протоколу. Давайте збережемо зміни.[21]

Тепер можна застосувати ці зміни до тригера. Перейдіть на панель дій і створіть дію, яка реагує на подію з певним унікальним ідентифікатором, яка сталася під час роботи вашого персонального комп'ютера. В рамках цієї роботи я розділив наступні події на 3 логічні блоки: перевірка цілісності системи за допомогою ідентифікаторів 4612, 4615, 4618, 4816, 5038, 5056, 5057, 5060,

5061, 5062, 6281, 6410, Id4656, 4658, 4660, 4663, 4670 файлова система аудиту, ID4656, 4658, 4660, 4663, 4670 управління обліковими записами користувачів аудиту 4624, 4648, 4672, 4625, 4647, 4776, 4771, 4720, 4722, 4723, 4724, 4725, 4726, 4738 рік,

4740, 4767, 4781, 4794, 4741, 4742, 4743[21].

It дуже важливо правильно згрупувати та обробити існуючі журнали, щоб їх можна було легко розбити на логічні та практичні частини.

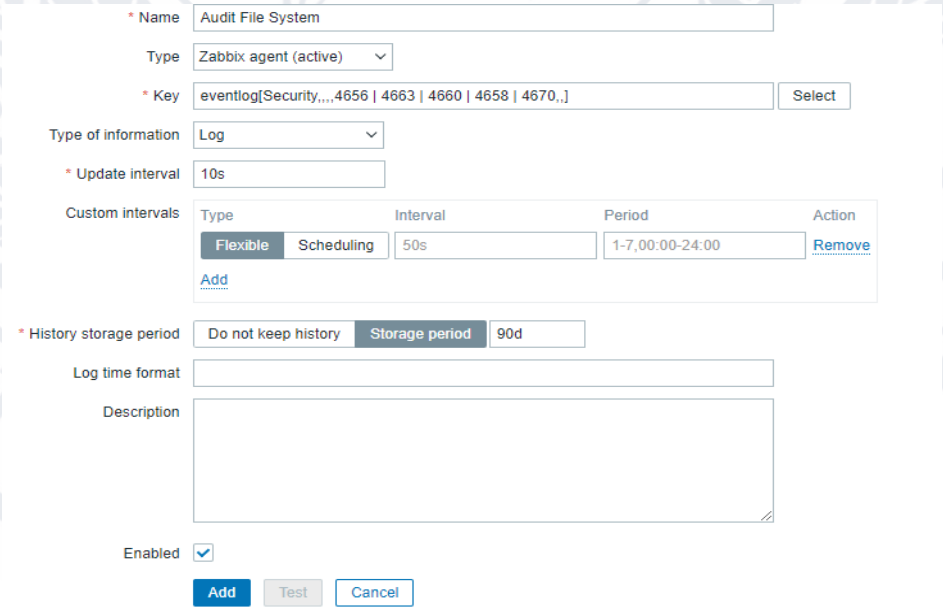


Рисунок 3.8 — Фільтр подій для *Audit System Integrity*

Це меню також дозволяє встановлювати умови для скасування виняткових ситуацій, з різними умовами і ланцюжками перевірок. Розглянемо механізми сповіщень для різних груп користувачів. Перейдіть на панель "конфігурація–дія–тригер" і додайте групу користувачів, які отримують повідомлення про помилки або попередження.

Для адміністраторів встановимо попередження про помилку електронною поштою. Натисніть "Створити дію", введіть ім'я та критерії, щоб додати групу користувачів, які отримуватимуть сповіщення. Групи користувачів можна створювати або редагувати в меню адміністрування-групи користувачів / ролі користувачів / Користувач.

Система моніторингу Zabbix включає визначення аудиту управління обліковими записами, запису аудиту, доступу об'єктів до файлової системи та аудиту цілісності системи. Ці вимоги є мінімально необхідними відповідно до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 "Про затвердження Загальних вимог до кібербезпеки критично важливих об'єктів інфраструктури"[21].

3.5. Висновки до розділу 3

У третьому розділі роботи було описано процес впровадження системи моніторингу Zabbix для проведення аудиту інформаційної безпеки в організації. Розглянуто налаштування політик аудиту для управління обліковими записами, доступу до об’єктів файлової системи та перевірки цілісності системи. Було налаштовано систему моніторингу для збору, збереження та аналізу даних аудиту. Описано процес налаштування оповіщень і створення шаблонів моніторингу для забезпечення оперативного реагування на інциденти безпеки. Це впровадження дозволяє організації своєчасно виявляти та нейтралізувати загрози, підтримуючи високий рівень інформаційної безпеки [18].

ВИСНОВКИ

У цьому дослідженні ми проаналізували практичні аспекти використання систем моніторингу для реєстрації, зберігання та аналізу інцидентів безпеки на державних підприємствах. Використання таких систем стає все більш важливим в сучасному цифровому середовищі, особливо на критично важливих об'єктах інфраструктури.

Результати дослідження показали, що правильно налаштована система моніторингу може ефективно виявляти і усувати проблеми безпеки, що виникають в режимі реального часу. Процес створення аудиту інформаційної безпеки починається з детального планування та аналізу, при якому послуги, що використовуються в процесі обробки, ретельно перевіряються та оцінюються ризики, пов'язані з їх використанням. На основі цього аналізу вживаються відповідні заходи для мінімізації впливу або повного усунення виявлених вразливостей.

У дослідженні були враховані мінімальні законодавчі вимоги для реєстрації подій у системі з урахуванням вимог Постанови Кабінету Міністрів України № 6-19 від 2019 р.та рекомендовано встановити політику аудиту.Показано використання, можливості та обмеження програмного рішення Zabbix для 518 записів мережевого моніторингу та аудиту.

Основними недоліками Zabbix були необхідність встановлення серверного розділу в системі Linux та обмежене зберігання журналів. Однак, враховуючи можливість інтеграції з іншими системами моніторингу та аналізу журналів, Zabbix є багатообіцяючим інструментом для забезпечення інформаційної безпеки на критично важливих об'єктах інфраструктури.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Campusetic. Auditorías De Ciberseguridad. 2022 [Електронний ресурс]. Режим доступу: https://campusetic.com/auditorias-de-ciberseguridad/

2. ISACA Journal. Holistic IT Governance, Risk Management, Security and Privacy Needed for Effective Implementation. 2016 [Електронний ресурс]. Режим доступу: https://www.isaca.org/resources/isacajournal/issues/2016/volume-5/holistic-it-governance-risk-management-security-and-privacy-needed-for-effective-implementation-and

3. Proofpoint. What is IT Compliance? [Електронний ресурс]. Режим доступу: https://www.proofpoint.com/us/threat-reference/it-compliance

4. SeaGlass Technology. What Are The IT Security Compliance Standards? [Електронний ресурс]. Режим доступу: https://www.seaglasstechnology.com/what-are-the-it-security-compliance-standards/

5. Ekran System. How to Pass an IT Compliance Audit? [Електронний ресурс]. Режим доступу: https://www.ekransystem.com/en/blog/how-to-pass-it-compliance-audit

6. Overview of Zabbix. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: https://www.zabbix.com/documentation/1.8/en/manual/about/overview_of_zabbix#:~:text=Zabbix%20is%20an%20enterprise-class,alerts%20for%20virtually%20any%20event

7. Nagios – Overview. Online Tutorials Library. URL: https://www.tutorialspoint.com/nagios/nagios_overview.htm#:~:text=Nagios%20is%20an%20open%20source,IT%20infrastructure%20and%20its%20performance

8. Garman, J.. Kerberos: The Definitive Guide. O'Reilly Media. ISBN:

0596004036. 2003

9. Stankowicz, S. (Stankowic, S.). Zabbix Network Monitoring Essentials. Packt Publishing. pp.1-20. 2015

10. Eventlog Key – Win32 apps. Developer tools, technical documentation and coding examples | Microsoft Docs. URL: https://docs.microsoft.com/en-us/windows/win32/eventlog/eventlog-key.

11. Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. "Аудит та управління інцидентами інформаційної безпеки". Київ: Центр навч.- наук. та наук.-пр. видань НА СБ України. 2014 URL:[https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf]

12. OpenVAS. (2018). OpenVAS Protocol Specification. Архівовано з [https://web.archive.org/web/20180624105954/https://www.openvas.org/protocol-doc.html]

13 Auditing Security and Controls of Windows Domains von Derek Melber [https://beckassets.blob.core.windows.net/product/readingsample/350956/9780894135637_excerpt_001.pdf].

14 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

15 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Офіційний веб портал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text

16 Про основні засади забезпечення кібербезпеки України. Офіційний веб портал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

17 Про затвердження Загальних вимог до кіберзахисту об'єктів

критичної інфраструктури. Офіційний веб портал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

18 Davis, H. (2017). "Security Event Logging and Analysis in Public Sector". *Journal of Government Information Systems*, pp. 95-120.

19 Wang, T., & Liu, P. (2020). "Effective Use of Monitoring Systems in State Infrastructure". *IT Management Journal*, pp. 85-105.

20 NIST про NIST SP 800-53 (версія Rev. 5) URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

21 Аудит інформаційної безпеки ТОВ “Се Броднетце-Україна” URL: https://elartu.tntu.edu.ua/bitstream/lib/38302/1/Dyplom_Voitso_O_M_2022.pdf