НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2025 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему:

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-11

Ахунов Михайло Юрійович
(підпис)

Керівник доцент кафедри ІБ, к.т.н. Демчинський В.В
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Дмитро ЛАНДЕ

(підпис)

«___»_____2025 р.

ЗАВДАННЯ

на дипломну роботу здобувачу вищої освіти

Ахунову Михайлу Юрійовичу

1. Тема роботи «Автоматизація аудиту безпеки Windows за допомогою PowerShell»

керівник роботи Демчинський Володимир Васильович к.т.н., доцент, доцент кафедри інформаційної безпеки,

затверджені наказом по університету від 26 травня 2025 р. № 1761-с

2. Термін подання здобувачем вищої освіти роботи 12 червня 2025 р.

3. Вихідні дані до роботи

Літературні джерела, що висвітлюють теоретичні основи аудиту інформаційної безпеки, класифікацію типів аудиту, вимоги до безпечної конфігурації операційних систем та міжнародні стандарти безпеки

4. Зміст роботи

Огляд літературних джерел задля визначення поняття аудиту та класифікації його типів, визначення критеріїв оцінки рівня безпеки Windows систем, огляд засобів PowerShell для перевірки системної конфігурації, розробка засобу для автоматизованого аудиту інформаційної безпеки Windows систем.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.

6. Дата видачі завдання: 9 жовтня 2024 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	09.10.2024	
2	Ознайомлення з теоретичними основами аудиту інформаційної безпеки	20.01.2025	
3	Аналіз стандартів та нормативів безпеки	01.03.2025	
4	Вивчення інструментів PowerShell для аудиту систем Windows	15.03.2025	
5	Розробка структури скриптового інструменту для аудиту	28.03.2025	
6	Реалізація модулів перевірки локальних політик безпеки та параметрів брандмауера	12.04.2025	
7	Реалізація модулів контролю доступу, стану антивірусного захисту, служб і портів	26.04.2025	
8	Побудова логіки взаємодії з користувачем, меню та формування звіту	11.05.2025	
9	Тестування засобу в середовищі Windows 10	18.05.2025	
10		25.05.2025	

	Аналіз результатів тестування та формування рекомендацій		
11	Підготовка презентації до захисту	02.06.2025	
12	Остаточне оформлення дипломної роботи	12.06.2025	

Здобувач вищої освіти _____ Михайло АХУНОВ

(підпис) (власне ім'я, ПРІЗВИЩЕ)

Науковий керівник _____ Володимир ДЕМЧИНСЬКИЙ

(підпис) (власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи 161 сторінка, 55 ілюстрацій, 4 таблиці, 2 додатки, 24 джерела літератури.

Об’єкт дослідження: процес аудиту інформаційної безпеки в операційних системах Windows.

Предмет дослідження: технології автоматизації аудиту безпеки, технологія PowerShell.

Мета дослідження: розробка інструменту на основі PowerShell для автоматизованого аудиту захисту системи Windows.

Методи дослідження: Аналіз літературних джерел, моделювання алгоритму, побудова практичної моделі.

Отримані результати: реалізовано скриптовий інструмент, який здійснює перевірку основних аспектів конфігурації безпеки операційної системи Windows, таких як політики безпеки, параметри брандмауера, контроль доступу, статус антивірусного захисту, активні служби, порти. Інструмент базується на PowerShell і дозволяє проводити аудит без встановлення стороннього програмного забезпечення. Проведено тестування в умовах віртуального середовища, що підтвердило ефективність і зручність розробленого рішення. Запропоновані рекомендації для усунення виявлених порушень конфігурації.

Ключові слова: аудит інформаційної безпеки, PowerShell, Windows, критерії безпеки.

ABSTRACT

The volume of the work is 161 pages, 55 illustrations, 4 tables, 2 appendices, 24 sources of literature.

Object of research: the process of auditing information security in Windows operating systems.

Subject of research: security audit automation technologies, PowerShell technology.

Purpose of research: development of a PowerShell-based tool for automated auditing of Windows system security.

Research methods: Analysis of literary sources, algorithm modeling, construction of a practical model.

Results: A script tool was implemented that checks the main aspects of the security configuration of the Windows operating system, such as security policies, firewall settings, access control, antivirus protection status, active services, ports. The tool is based on PowerShell and allows auditing without installing third-party software. Testing was carried out in a virtual environment, which confirmed the effectiveness and convenience of the developed solution. Recommendations were proposed to eliminate the detected configuration violations.

Keywords: information security audit, PowerShell, Windows, security criteria.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

PowerShell – середовище автоматизації та мова сценаріїв, розроблена корпорацією Microsoft, яка дозволяє керувати компонентами операційної системи Windows та іншими продуктами.

ACL (Access Control List) – список контролю доступу, який визначає права користувачів і груп на об’єкти в операційній системі.

SIEM (Security Information and Event Management) – система управління інформацією та подіями безпеки, яка дозволяє аналізувати журнали, події і виявляти загрози.

OS (Operating System) – операційна система, програмне забезпечення, що керує апаратними ресурсами та забезпечує базові сервіси для прикладних програм.

Windows Defender – вбудоване антивірусне та антишпигунське програмне забезпечення Windows.

Firewall (брандмауер) – засіб мережевого захисту, що здійснює контроль вхідного та вихідного трафіку згідно з визначеними правилами.

Локальні політики безпеки – набір конфігурацій у Windows, які визначають параметри безпеки системи: паролі, права доступу, аудит тощо.

Служби Windows – служби процеси операційної системи, які запускаються автоматично або вручну та забезпечують функціонування окремих компонентів.

JSON (JavaScript Object Notation) – текстовий формат обміну даними, що використовується для зберігання та передачі структурованої інформації між системами.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 7

ВСТУП 11

1 ЗАСАДИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 14

1.1 Процес аудиту інформаційної безпеки та його цілі 14

1.2 Види аудиту інформаційної безпеки 15

1.3 Критерії оцінювання рівня безпеки в системах Windows 19

Висновки до розділу 1 41

2 АУДИТ БЕЗПЕКИ ОС WINDOWS ЗАСОБАМИ POWERSHELL 42

2.1 Особливості застосування PowerShell у сфері безпеки 42

2.2 Перевірка основних аспектів безпеки Windows 44

Висновки до розділу 2 73

3 ЗАСТОСУВАННЯ ЗАСОБІВ АУДИТУ БЕЗПЕКИ НА ОСНОВІ POWERSHELL 74

3.1 Архітектура застосунку 74

3.2 Автоматизація процесу аудиту 76

3.3 Результати тестування розроблених засобів аудиту 95

Висновки до розділу 3 108

ВИСНОВКИ 109

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 111

ДОДАТОК А ЗАСІБ ДЛЯ АВТОМАТИЗАЦІЇ АУДИТУ 114

ДОДАТОК Б КОНФІГУРАЦІЙНИЙ JSON-ФАЙЛ 153

ВСТУП

Актуальність роботи:

Сучасна ситуація в сфері цифрової безпеки характеризується зростанню кіберзагроз та підвищенню складності інформаційних атак. Організації щоденно стикаються з ризиками компрометації даних, порушення цілісності даних та можливими неполадками в критично важливих компонентах системи. Через цю причину регулярне проведення аудиту інформаційної безпеки є фундаментальним для підтримання стану безпеки системи та ефективного управління ризиками.

Операційна система Windows через свою всесвітню популярність, будучи домінуючим рішенням в корпоративному секторі, є дуже привабливою ціллю для зловмисників. Через цю причину проведення постійного моніторингу захищеності таких систем є необхідним. PowerShell, в свою чергу, є потужним інструменту для адміністрування та автоматизації, що надає можливості для створення ефективних засобів оцінки стану безпеки без залучення додаткових програмних рішень.

В сучасних умовах недостатній контроль конфігурацій безпеки систем на основі Windowsможе спричинити катастрофічні наслідки: від втрати критичних даних до повної зупинки діяльності підприємства. Традиційні підходи до аудиту часто виявляються неефективними та не забезпечують необхідної швидкості виявлення потенційних загроз.

Метою дипломної роботи є створення та тестування інструментарію автоматизації процесу аудиту інформаційної безпеки операційних систем Windows з використанням можливостей PowerShell.

Завдання дослідження:

Дослідити сучасні підходи до проведення аудиту інформаційної безпеки.

Сформулювати систему критеріїв для оцінки рівня захищеності Windows-середовища.

Вивчити функціональні можливості PowerShell в контексті завдань безпеки.

Створити засіб на основі автоматизованих скриптів для перевірки параметрів безпеки.

Провести тестування розробленого інструменту.

Об’єкт дослідження:

Методологія та процедури аудиту інформаційної безпеки в Windows.

Предмет дослідження:

Технології автоматизації аудиту інформаційної безпеки, технологія PowerShell.

Методи дослідження:

Аналіз нормативних документів та стандартів безпеки, скриптове програмування, порівняльний аналіз.

Наукова новизна одержаних результатів:

Розроблено комплексний підхід до проведення автоматизованого аудиту інформаційної безпеки Windows на основі PowerShell, що включає перевірку політик безпеки, мережевого захисту, управління доступом, конфігурації сервісів, портів та антивірусного захисту. Розроблено оригінальні команди, за допомогою яких можна провести глибокий аналіз захищеності системи без потреби в завантаженні стороннього програмного забезпечення.

Практичне значення одержаних результатів:

Створений аудиторський інструмент, що готовий до впровадження у корпоративну інфраструктуру для забезпечення регулярного контролю за станом безпеки системи. Рішення може застосовуватись у випадках внутрішнього аудиту, освітніх програмах та як компонент захисту інформаційних ресурсів без потреби у значних фінансових витратах. Ефективність та точність розробленого інструменту була протестована на платформі Windows 10.

1 ЗАСАДИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Процес аудиту інформаційної безпеки та його цілі

Аудит інформаційної безпеки – це процес проведення комплексної оцінки стану інформаційної безпеки. В свою чергу інформаційна безпека – це стан захищеності системи, який передбачає дотримання цілісності, конфіденційності та доступності інформації.

Принцип роботи аудиту полягає в перевірці того, чи відповідає система списку критеріїв безпеки, що можуть включати себе: повнота політики безпеки та відповідність їй, відповідність ISO та іншим стандартам, наявність програмних засобів захисту мережі, такі як міжмережний екран, IPS, IDS, існування правильної конфігурації NAT, VPN та протоколів шифрування, тощо

Ціль аудиту – виявити ризики, вразливості, які можуть бути як технічними, так і людськими, слабкі місця, що можуть бути експлуатовані злочинцями та стати причиною збитків, для подальшого виправлення щоб не допустити інциденти в майбутньому. Також однією з ціллю аудиту є перевірка відповідності інформаційної системи регламентам та факт того, чи слідує вона рекомендаціям безпеки.

Аудит інформаційної безпеки дозволяє крім того, що знайти слабкі місця системи, а також оцінити її рівень розвитку захисту, визначити потрібні рекомендації для покращення, а ще, не менш важливо, покращити рівень довіри від клієнтів, що є запорукою успішного бізнесу.

1.2 Види аудиту інформаційної безпеки

Внутрішній аудит безпеки полягає в використанні лише внутрішніх ресурсів підприємства для оцінки. Зазвичай ці перевірки зосереджені на відповідність політикам безпеки та справність роботи засобів безпеки. Цей тип аудиту є фінансово вигідним, оскільки наймання працівників власної компанії буде дешевшим, ніж іншої. Внутрішній аудит може дати кращий результат оцінки специфічних для вашої компанії процесів. Також є менше проблем з наданням доступу до конфіденційних та облікових даних, оскільки ці дані будуть надаватися працівникам тієї ж самої компанії. Враховуючи той факт, що працівники компанії перевіряють власний ж стан інформаційної безпеки, то для максимізації безпристрасності команду аудиторів можуть набрати з людей, які були не причасні до розробки системи інформаційної безпеки, але це не гарантує безпристрасність, що є мінусом, бо може призвести до менш об’єктивної оцінки. [1, 23]

Зовнішній аудит безпеки, на відміну від внутрішнього, залучає аудиторів з інших компаній, що нівелює головний мінус внутрішнього аудиту безпеки у відсутності безпристрасності. Аудитори за велику ціну зроблять об’єктивну оцінку захищеності системи та можуть надати рекомендації, які можливо не були очевидними для працівників компанії. Також аудитори зовнішніх компаній можуть бути більш спеціалізовані, ніж власні аудитори. Один з мінусів зовнішнього аудиту полягає в тому, що команда аудиторів може запросити доступ до конфіденційної інформації, що є більш ризиковим, ніж якби це були аудитори з вашої компанії. [1, 23]

Метою аудиту на відповідність полягає в перевірці, чи дотримується компанія нормативно-правових вимог, правил та стандартів, що регулюють її

діяльність в сфері інформаційної безпеки. Такі перевірки зазвичай стосуються дотримання деяких стандартів, критеріїв, правил та вимог, розроблених спеціально для сфери інформаційної безпеки для забезпечення захищеності системи. Відомі стандарти, до яких можуть перевірити відповідність, це ISO 27001, що є міжнародним стандартом, який позначає рекомендації та вимоги до побудови систем управління інформаційної безпеки, PCI DSS, що є стандартом для організацій, що обробляють дані платіжних карток, GDPR, що є регламентом, діючий в Європейському Союзі, та описуючий те, яким чином компанії повинні зберігати, збирати та використовувати персональні дані, та інші. Цей вид аудиту є обов'язковим з точки зору уникнення отримання штрафів та юридичних санкцій. Аудит на відповідність може бути складним в проведенні через існування великої кількості нормативних вимог та стандартів безпеки. [1, 23]

Аудит на вразливості має меті зробити перевірки системи на існування вразливостей, які потенційно можуть бути експлуатовані зловмисниками. Процес цього аудиту може включати використання спеціалізованих інструментів та методів, наприклад сканерів вразливостей, сканерів мережі, аналіз конфігурації сервісів. Також один з способів проведення аудиту на вразливості є використання PowerShell – скриптової мови Windows, оскільки вона є простим і автоматизованим рішенням збору інформації про систему. Результатом аудиту є отримання звіту з переліком виявлених вразливостей з ступенем їх критичності, з можливим використанням CVE, після аналізу якого можна зрозуміти, як покращити безпеку системи з цілю уникнення інцидентів. [1, 23]

Оцінка ризиків є одним з найважливіших компонентів аналізу безпеки системи. Задача полягає в виявлені ризиків для організації, оцінити ймовірність, потенційні репутаційні чи фінансові втрати, викликані цією подією, та шляхом аналізу цієї інформації визначити пріоритети заходів безпеки та правильно розподілити фінансування. Результатом аудиту є отримана категоризація

ризиків, згідно якої складається план реагування та зменшення. Можуть бути труднощі з тим, що план реагування та визначені пріоритети є суб'єктивними, через що можуть бути неоптимальними. В результаті це призведе до фінансових та репутаційних втрат. [1, 23]

Тестування на проникнення (Пентест) полягає в тому, що етичний хакер чи група етичних хакерів симулюють атаку на систему та таким чином визначають присутні вразливості. В результаті компанія має розуміння того, яким чином вже справжній злочинець зміг би атакувати, наскільки система безпеки готова до таких події, і якщо ні, то яким чином захиститися від подібних інцидентів в майбутньому. Серед інструментів проведення пентесту є багато інструментів, наприклад Kali Linux, Burp Suite, Metasploit, Nmap та інші. PowerShell також є одним з інструментів, за допомогою якого можна проводити симуляції атак. Оскільки такий вид аудиту є доволі нестандартним, то можна помітити такі вразливості, які непомітні при інших видах аудиту. Серед мінусів є потенційний вихід з ладу системи, так як симуляція атаки використовує такі ж самі методи, що і справжня атака. [1, 23]

Таблиця 1.1 [1, 23] – Порівняльна характеристика типів аудиту безпеки: виконавці, мета, переваги та недоліки

Тип аудиту	**Хто проводить**	**Основна мета**	**Переваги**	**Недоліки**

Кінець таблиці 1.1

Внутрішній	Власні працівники	Оцінка відповідності внутрішнім політикам	Низька вартість, знання системи	Можлива упередженість, відсутність «свіжого погляду»
Зовнішній	Незалежна організація	Об’єктивна перевірка стану безпеки	Неупередженість, професіоналізм	Висока вартість, ризик витоку конфіденційної інформації
На відповідність	Внутрішні або зовнішні аудитори	Верифікація дотримання стандартів	Законодавча відповідність, уникнення штрафів	Складність процедур, потреба в документації
На вразливості	IT-фахівці, сканери	Виявлення технічних вразливостей	Швидкість, автоматизація, CVE-ідентифікація	Можливе ігнорування людського фактору
Оцінка ризику	Аналітики, фахівці з ризиків	Аналіз ймовірностей і впливу	Стратегічне планування, пріоритетність	Суб’єктивність оцінки, ризик помилок
Пентест	Етичні хакери	Імітація реальних атак	Виявлення практичних векторів атаки	Ризик дестабілізації, складність, витрати

1.3 Критерії оцінювання рівня безпеки в системах Windows

1.3.1 Основа для оцінювання

Оцінювання рівня безпеки – процес аналізу налаштувань компонентів операційної системи, її поведінки та політик з ціллю виявлення слабких місць та впровадження відповідних дій, щоб зловмисники не мали можливості проексплуатувати їх. У випадку з системами на основі Windows оцінка рівня безпеки йде в напрямку перевірки налаштувань, створені для управління обліковими записами, мережною активністю, системними процесами та ресурсами, тощо.

В контексті аудиту інформаційної безпеки критерії безпеки – це набір перевірених практик і параметрів, які відповідають міжнародним або галузевим стандартам. Вони є орієнтирами та настановами про впровадженню інформаційно безпечної комп’ютерної системи.

У цій роботі критерії безпеки в основному будуть базуватися на основі нормативного документу CIS Microsoft Windows 10 Enterprise Benchmark, а також доповнюватися окремими положеннями з NIST SP 800-53 та NIST SP 800-41.

CIS Benchmark – це набір детально описаних рекомендацій стосовно налаштувань систем на основі Windows, що був розроблений незалежною організацією Center for Internet Security. окрема, використано CIS Microsoft Windows 10 Benchmark, що охоплює велику кількість аспектів конфігурації, таких як локальні політики безпеки, брандмауер, служби, облікові записи та інших критичних компонентів. Крім того, що цей стандарт надає інструкції по безпечній конфігурації системи, він також має обгрунтацію доцільності кожної рекомендації, а ще інформацію, як ці налаштування перевіряти в процесі аудиту

інформаційної безпеки. Для поглибленого обґрунтування критеріїв та відповідності галузевим практикам також враховувалися вимоги з NIST SP 800-53, який описує універсальні механізми управління інформаційною безпекою, та NIST SP 800-41, який надає рекомендації щодо конфігурації мережевих фільтрів.

Об’єднання критеріїв безпеки цих стандартів сприяє створенню об’єктивного та системний підхід до перевірок безпекових налаштувань Windows, що забезпечить відповідність як міжнародним стандартам, так і популярним рішенням в корпоративного середовища.

1.3.2 Параметри локальної політики безпеки

Локальні політики безпеки (Local Security Policy) – вбудований інструмент по налаштуванню політики безпеки системи з ОС Windows. За допомогою цього засобу можна налаштувати багато аспектів роботи, тому правильно налаштована конфігурація локальних політик безпеки значно покращує захищеність.

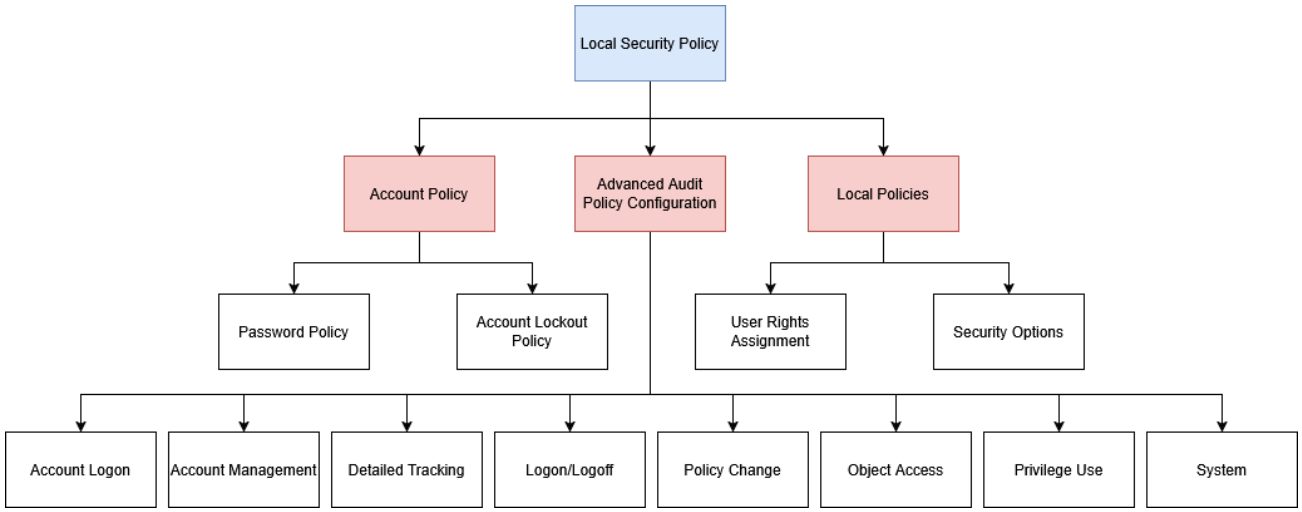

Рисунок 1.1 – Ієрархічна структура компонентів Local Security Policy в ОС Windows

На рисунку показана структура компонентів локальних політик безпеки, які будуть розглянуті в цьому розділі, серед яких присутні політики облікових записів (Account Policy), що зосереджені на налаштуваннях паролів та блокуванню облікових записів, Local Policies, що має налаштування призначення прав користувачів та параметри безпеки. Окремим елементом є Advanced Audit Policy Configuration – система аудиту, що дає можливість налаштовувати збір інформації про різні системні події.

Рекомендації стосовно політик облікових записів (Account Policy) стосуються таких напрямів як політика паролів (Password Policy) і політика блокування облікового запису (Account Lockout Policy). [2]

В політиці паролів враховуються такі критерії:

- Історія паролів (кількість попередніх паролів, які не можуть бути використані повторно): не менше 24.
- Вік паролю (мінімальний та максимальний термін дії пароля): від 1 до 60 днів.
- Довжина (мінімальна кількість символів в паролі): не менше 14 символів.
- Складність (наявність літер різного регістру, спеціальних символів та цифр): вимога увімкнена.
- Зберігання паролів з використанням зворотного шифрування: вимкнути [2]

Правильні налаштування цієї політики значно зменшує шанси несанкіонованого доступу шляхом brute-force атак.

Політика блокування облікового запису дозволяє налаштувати параметри поведінки системи у разі багаторазового невдалого входу до системи. Критерії цього розділу включають:

- Кількість невдалих спроб входу: не більше 10.
- Тривалість блокування: не менше 15 хвилин.
- Час до обнуління лічильника невдалих спроб: не менше 15 хвилин. [2]

Реалізація цієї політики ефективно захистить від brute-force атак та іншим атакам, спрямованих на підбор облікових даних

Локальні політики (Local Policies) мають такі розділи, налаштування яких впливає на безпеку системи, а саме призначення прав користувача (User Right Assignment) та параметри безпеки (Security Options). [2]

Призначення прав користувача – це розділ, який містить в собі рекомендації стосовно призначеню прав користувача. Серед критеріїв цього розділу присутні:

- Надання прав доступу до комп'ютера через мережу: доступ надається лише адміністраторам та користувачам віддаленого робочого стола.
- Обмеження доступу до критичних операцій: наприклад, права зміни системного часу чи відновлення файлів і директорій повинні бути лише у адміністраторів.
- Керування доступом до локальних політик: треба забороняти доступ до комп'ютера через мережу для гостьових облікових записів.
- Встановлення обмежень на виконання певних служб: права на “запуск як сервіс” повинні бути максимально обмежені.
- Управління доступом до файлів та об'єктів: лише адміністратори мають право взяти власність файла.

- Налаштування доступу для роботи з драйверами та пристроями: права на завантаження та вивантаження пристроїв драйверів мають лише адміністратори.
- Контроль за аудитом та введеням журналів: доступ лише адміністраторам. [2]

Налаштування з цього розділу критично важливі для забезпечення цілісності, конфіденційності та доступності, що забезпечує захист від потенційної ескалації прав та зловмисного використання важливих системних функцій.

Параметри безпеки, як підрозділ локальних політик, має такі налаштування, які контролюють поведінку системи стосовно керуванню обліковими записами, контролю доступу, а також механізми автентифікації. До критеріїв відносяться такі налаштування, як:

- Керування обліковими записами – параметри, які впливають на вимоги до паролів, обмеження облікових записів і поведінку при логіні. Наприклад, вимкнення вбудованого користувача Administrator, перейменування стандартних облікових записів, заборона використання пустих паролів, максимальний час неактивності залогіненого користувача.
- Контроль доступу – обмеження користувачів до використання системних ресурсів. Наприклад, заборона завантаження непідписаних драйверів.
- Політика інтерактивного входу, яка визначає поведінку системи під час входу користувача. Наприклад, приховування останнього користувача на екрані входу, показ попереджувального вікна на екрані входу.
- User Account Control (UAC) – компонент системи, який контролює, за яких обставин надавати адміністративні права з ціллю уникнути

несанкціонований доступ. Наприклад, увімкнення режиму Admin Approval Mode, який вимагає адміністраторів підтвердження своїх дій з підвищеними правами.

- Безпека мережі, яка також включає себе автентифікацію в мережному середовищі, параметри шифрування, правила взаємодії з віддаленими системами, тощо. Наприклад, заборона на підключення до іменованих каналів в анонімному режимі. [2]

Правильне налаштування цих параметрів захищає систему від несанкціонованого доступу, ескалації привілеїв, а також зловмисного доступу до критично важливих функцій.

Під час аудиту безпеки Windows важливо ретельно переглянути налаштування розширеної конфігурації політики аудиту (Advanced Audit Policy Configuration), оскільки в цьому розділі локальних політик безпеки є список різносторонніх налаштувань, пов’язаних зі збором системних логів, що є важливим механізмом безпеки. Цей розділ складається з такого списку підрозділів: Вхід до облікового запису (Account Logon), управління обліковими записами (Account Management), детальне відстеження (Detailed Tracking), вхід/вихід (Logon/Logoff), зміна політик (Policy Change), доступ до об’єктів (Object Access), використання привілеїв (Privilege Use) та система (System). Розглянемо кожний з підрозділів та логи, за які вони відповідають, окремо:

Вхід до облікового запису – це підкатегорія, яка зберігає репорти про вдалі чи невдалі входи в облікові записи. В цьому підрозділі слід перевіряти наявність цього налаштування:

- Audit Credential Validation – успішні та невдалі події.
- Управління обліковими записами відстежує всі події, що пов’язані з різноманітними змінами в облікових записах користувачів. Серед логів, існування яких треба перевіряти, присутні:

- Audit Application Group Management – успішні та невдалі події.
- Audit Computer Account Management – успішні та невдалі події.
- Audit Other Account Management Events – успішні та невдалі події.
- Audit Security Group Management – успішні та невдалі події.
- Audit User Account Management – успішні та невдалі події. [2]

Серед логів, збір яких треба включити в розділі детального відстеження, є:

- Логи PNP активності – успішні події.
- Логи створення процесів – успішні події. [2]

Вхід/вихід – це підрозділ, налаштував який можна фіксувати інформацію, пов’язану зі входом та виходом користувачів, блокуванню облікових записів та віддаленому доступу до комп’ютеру. Список логів, збір яких треба підключити в цьому підрозділі:

- Логи блокування акаунту – успішні та невдалі події.
- Логи входу/виходу користувача з системи – успішні події для виходу та успішні і невдалі події для входу.
- Логи спеціальних входів – успішні події.
- Логи інших подій входу/виходу – успішні та невдалі події. [2]

Через доступ до об’єктів треба включити збирання інформації про успішний та невдалий доступ до об’єктів файлової системи на знімних носіях. Це є важливим налаштуванням, оскільки воно може допомогти в розслідуванні, якщо зловмисник взаємодіяв зі знімними носіями, наприклад, USB-накопичувачами.

Зміна політик – розділ, через який можна налаштувати логування подій, пов’язані зі змінами в політиці безпеки. В цій підкатегорії треба підключити збір таких логів:

- Логування змін політик аудиту – успішні та невдалі події.

- Логування змін політик автентифікації – успішні події.
- Логування змін політик авторизації – успішні події. [2]

Використання привілеїв – підрозділ, через який треба включити збір інформацію про успішні та невдалі спроби надання чутливих привілеїв користувачами чи сервісам. Ці привілеї мають дуже великий вплив на систему і при несанкціонованому використанні привілеїв може призвести до поганих наслідків. Підключивши логування про надання чутливих привілеїв може допомогти при розслідуванні можливого кіберінциденту.

Система – підрозділ, який фіксує важливі системні події, такі як:

- Логування IPSec драйвера – успішні та невдалі події.
- Логування подій Windows Firewall – успішні та відхилені підключення.
- Логування порушень цілісності – успішні та невдалі події. [2]

Розширеної конфігурації політики аудиту дає можливість гнучко налаштувати збір інформації щодо різноманітних системних подій і змін, такі як дії користувачів, процесів та сервісів, доступ до об’єктів файлової системи, зміни в політиці безпеки та інші. Отримання журналів подій є ключовим фактором в розслідувані кіберінцидентів, оскільки вони є фактичною інформацією і можуть слугувати як доказ. За допомогою логів можна проаналізувати ланцюжок дій зловмисника в кіберінциденті, та на його основі зробити висновок щодо потрібних дій для покращення захисту. Також журнали подій є чудовим засобом моніторингу та допомагають в режимі реального часу провести аналіз захищеності.

1.3.3 Параметри мережевого екранування

Windows Firewall – це вбудований в ОС Windows брандмауер. Це засіб, який регулює мережну активність системи, дозволяючи чи забороняючи вхідний трафік на основі заздалегідь встановлених налаштувань. Правильна конфігурація брандмауера є дуже важливою для безпеки системи, оскільки брандмауер захищає від небажаного чи потенційно небезпечного інтернет трафіку, сканування мережі, несанкціонований віддалений доступ, DoS атака, тощо. [24]

Windows Defender брандмауер із розширеною безпекою (Windows Defender Firewall with Advanced Security) як розділ Local Security Policy – розділ з налаштуваннями безпеки брандмауера для трьох профілів: доменного (Domain), приватного (Private) та публічного (Public). Політики доменного профілю активуються в випадках, коли комп'ютер підключено до домсну Active Directory. Приватний профіль розроблений для використання, коли пристрій належить до приватної мережі (наприклад, домашня мережа). Налаштування публічного профілю з точки зору інформаційної безпеки є найважливішими, оскільки ці політики використовуються при підключенні до публічних мереж (наприклад, Wi-Fi мережа аеропорту, кав'ярні). [24]

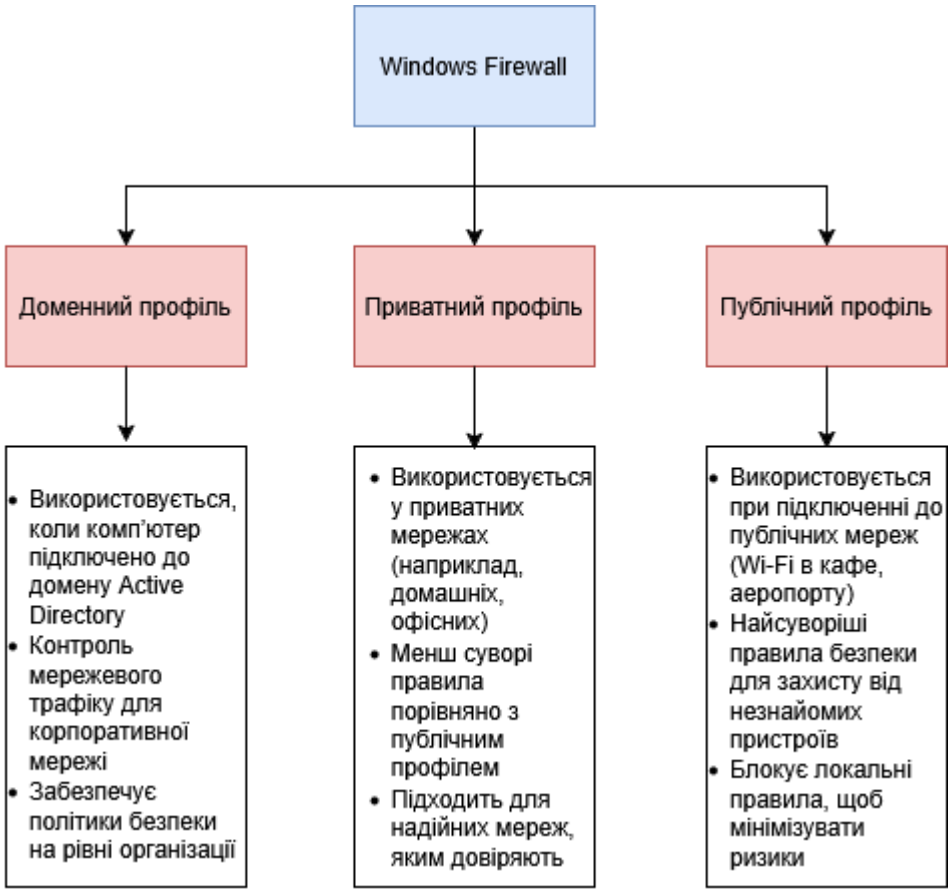

Рисунок 1.2 – Профілі Windows Firewall: доменний, приватний та публічний

Для кожного з цих профілів передбачена низка налаштувань, спрямованих на регулювання поведінки брандмауера в різних умовах. Розглянемо критерії безпеки для кожного з профілів окремо:

Доменний профіль:

- Стан брандмауера: увімкнений.
- Вхідні з'єднання: блокуються за замовчуванням.
- Вихідні з'єднання: дозволені за замовчуванням.
- Сповіщення: вимкнені.

- Журналювання: журналювати відкинуті брандмауером пакети та вдалі спроби з’єднання. Зберігати файл з логами доменного профілю, розмір якого 16384 кілобайт та більше, за розташуванням %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log. [2]

Приватний профіль:

- Стан брандмауера: увімкнений.
- Вхідні з'єднання: блокуються за замовчуванням.
- Вихідні з'єднання: дозволені за замовчуванням.
- Сповіщення: вимкнені.
- Журналювання: журналювати відкинуті брандмауером пакети та вдалі спроби з’єднання. Зберігати файл з логами приватного профілю, розмір якого 16384 кілобайт та більше, за розташуванням %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log. [2]

Публічний профіль:

- Стан брандмауера: увімкнений.
- Вхідні з’єднання: блокуються за замовчуванням.
- Вихідні з’єднання: дозволені за замовчуванням.
- Сповіщення: вимкнені.
- Застосування локальних правил брандмауера: заборонити.
- Застосування локальних правил захисту з’єднань: заборонити.
- Журналювання: журналювати відкинуті брандмауером пакети та вдалі спроби з’єднання. Зберігати файл з логами публічного профілю, розмір якого 16384 кілобайт та більше, за розташуванням %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log. [2]

Налаштування поведінки брандмауера в різних контекстах є критичними для забезпечення безпеки системи, тому під час аудиту безпеки важливе глибока

перевірка, в якій просто перевірка того, чи працює брандмауер, недостатньо. Правильна конфігурація кожного з трьох профілів дозволяє брандмауеру адаптуватися до різних умов в мережі, що в результаті покращить захист від різних видів мережних атак (включаючи сканування мережі та несанкціоновані з'єднання).

Крім цих налаштувань, політика безпеки брандмауера повинна передбачити наступне:

- Брандмауер повинен дозволяти лише потрібні IP протоколи. Серед популярних IP протоколів, які використовуються та не повинні бути заборонені, може бути ICMP, TCP та UDP. Інші протоколи, які можуть бути використані, це ESP та AH. Робота з цими протоколами повинна бути правильно налаштована згідно потреб системи. Непотрібні IP протоколи повинні бути заборонені на замовчуванням. [20]

Брандмауер також повинен бути налаштованим на потенційну роботу з протоколом IPv6, який з кожним роком набуває все більшу популярність через збільшення кількості пристроїв з IPv6. При конфігурації брандмауера треба взяти до уваги ці аспекти:

- Брандмауер повинен блокувати протоколи 6-to-4, Teredo та ISATAP у випадку, якщо вони не використовуються. Ці протоколи використовуються для інкапсуляції IPv6 пакетів у IPv4 пакети, що може бути використано для обходу контролю брандмауера, якщо його правила не розраховані на таким чином інкапсульовані пакети. [20]

TCP та UDP трафік є основними транспортними протоколами в IP-мережах, що використовуються майже всіма програмами. Для вхідного трафіку, як і для інших протоколів, повинен діяти принцип "deny by default", хоча вже для вихідного трафіку можна використовувати вже менш сурові правила, оскільки система взаємодіє з великою кількістю серверів у зовнішній мережі. [20]

Протокол ICMP часто використовується в діагностиці мережі та передачі службових повідомлень: повідомлення про помилки, тести досяжності (ping), визначення MTU, тощо. Проте, цей протокол може бути використаний зловмисниками в атаці. Наприклад, вхідні ICMP-пакети типу Echo Request можуть бути використані зловмисниками для отримання інформації про внутрішню топологію мережі, тому брандмауери часто блокують такі запити. ICMP тип 3 (Destination Unreachable) повідомлення не повинні бути відфільтровані брандмауером, оскільки ці повідомлення дуже важливі для діагностики системи. [20]

IPsec – сукупність протоколів, створених для забезпечення безпечної передачі даних IP протоколом. Організації треба визначитись, чи буде використовувати IPsec VPN. Якщо ні, протоколи ESP та AH слід заборонити. Інакше, його треба дозволити його використання лише для конкретного адресу - для шлюзу. У випадках, коли перевірка змісту IPsec трафіку необхідне, організація може вимагати використання VPN через проксі або з можливістю інспекції. [20]

1.3.4 Контроль доступу, облікові записи і групи

Одним із ключових захисних механізмів ОС Windows є контроль доступу, який реалізується через систему облікових записів користувачів, груп користувачів, прав та привілеїв. Облікові записи дають можливість ідентифікувати користувача системи, а групи, права та привілеї дозволяють визначитися з можливостями користувача, до яких ресурсів він матиме доступ, на які дії він буде здатен. Модель інформаційної безпеки ОС Windows дозволяє гнучко та легко налаштувати дозволи та обмеження на системні ресурси та файли

згідно політики безпеки, встановлених адміністратором. Тому правильне налаштування менеджменту облікових записів та контролю доступу є ключовим фактором для забезпечення конфіденційності та захисту від неправомірного доступу до ресурсів системи.

Серед важливих критеріїв безпеки, що стосуються менеджменту облікових записів, можна назвати:

- Моніторинг часу останнього входу. Слід це регулярно робити з ціллю виявити підозрілу активність та несанкціонований доступ до облікового запису.
- Блокування неактивних облікових записів. Це дозволяє запобігти ризикам, пов’язаним з використанням застарілих чи забутих облікових записів.
- Періодичний перегляд членства користувачів у групах з підвищеними привілеями, зокрема група адміністраторів, для виявлення невиправданих призначень.
- Регулярний огляд та видалення тимчасових та службових акаунтів (гостьові, технічні, для інсталяції програм). Це є необхідною умовою для забезпечення захисту від несанкціонованого доступу. [21]

При аудиті безпеки буде проводитись перевірка файлів та директорій на наявність некоректних прав доступу. Серед частих помилок, які трапляються в конфігурації прав доступу до файлів, перевірятимуться:

- Надання доступу до файлу/директорії користувачам напряму, замість надання доступу до групи користувачів. Така практика дуже сильно ускладнить менеджмент правами доступу в майбутньому, що може призвести до помилок у майбутньому.

- Не використання критеріїв для включення користувачів у групи. При правильному менеджменті при додаванні користувача до тої чи іншої групи важливо враховувати її положення та бізнес-роль.
- Відхилення від стандартів. При такій практиці менеджмент правами доступу перетвориться в хаос. Задля уникнення непорозумінь та неясності слід дотримуватись стандартів. [22]

Тепер розглянемо хороші практики, яких слід дотримуватись при управлінні правами доступу. Серед таких практик можна згадати:

- Надання прав доступу до груп, а не окремо користувачам. Такий принцип роботи, в якому права користувачам надаються не на пряму, полегшить контроль.
- З ціллю підтримання впорядкованої файлової структури системи, слід заборонити користувачам, крім адміністраторів, створювати нові папки в кореневому каталозі.
- Не надавати право Full Control для звичайних користувачів. Для більшості користувачів достатньо права Modify, які дозволяють створювати, модифікувати та видаляти файли. В той час, Full Control дає можливість змінювати права доступу до файлу, що є небажаним і ризикованим для звичайного персоналу. [22]

В аудиті інформаційної безпеки слід також перевірити слабкі, ризиковані та хибні налаштування DACL регістру, файлів та папок. Погане налаштування DACL може призвести до несанкціонованого доступу, підвищення привілеїв, втрати цілісності або конфіденційності критичних даних.

Таблиця 1.2 [3, с. 563-564] – Права доступу ключів реєстру Windows та їх вплив на безпеку

Назва права доступу	**Опис впливу при наданні ненадійному або частково довіреному користувачу**
KEY_SET_VALUE	Можливе підвищення привілеїв. Дозволяє змінювати значення ключа реєстру на довільне.
KEY_CREATE_SUB_KEY	Можливе підвищення привілеїв. Дозволяє створювати підключі з будь-якими значеннями.
WRITE_DAC	Можливе підвищення привілеїв. Дозволяє змінювати DACL ключа, надаючи собі або іншим права KEY_SET_VALUE або KEY_CREATE_SUB_KEY.
WRITE_OWNER	Можливе підвищення привілеїв. Дозволяє змінювати власника ключа. Власник може змінювати DACL (має право WRITE_DAC) і надавати собі додаткові права.
GENERIC_WRITE	Можливе підвищення привілеїв. Включає права KEY_SET_VALUE і KEY_CREATE_SUB_KEY.
GENERIC_ALL	Можливе підвищення привілеїв. Включає права KEY_SET_VALUE і KEY_CREATE_SUB_KEY (повний контроль)

Кінець таблиці 1.2

DELETE	Можливе підвищення привілеїв. Дозволяє видаляти ключ, що фактично еквівалентно можливості його змінити, створивши заново з потрібними значеннями
KEY_QUERY_VALUE, KEY_ENUMERATE_SUB_KEYS	Можливе розкриття конфіденційної інформації. Дозволяє читати значення ключів і перелічувати їх підключі. Це може надати зловмиснику інформацію про встановлене ПЗ, шляхи до файлів, налаштування системи тощо
GENERIC_READ	Можливе розкриття інформації. Включає в себе KEY_QUERY_VALUE та KEY_ENUMERATE_SUB_KEYS, що дозволяє читати як вміст, так і структуру реєстру

Таблиця 1.3 [3, с 565-567] – Права доступу директорій Windows та їх вплив на безпеку

Назва права доступу	**Опис впливу при наданні ненадійному або частково довіреному користувачу**
FILE_ADD_FILE	Дозволяє створювати файли в папці. Файли належатимуть зловмиснику

Кінець таблиці 1.3

FILE_ADD_SUBDIRECTORY	Дозволяє створювати підкаталоги. Можна заздалегідь створити структуру з успадковуваними правами доступу
FILE_DELETE_CHILD	Дозволяє видаляти файли в папці. Потім зловмисник може підставити власні файли
WRITE_DAC	Дозволяє змінити DACL, тобто дати собі будь-які права
GENERIC_WRITE	Дає сукупність прав: створення файлів, підкаталогів, видалення вмісту
GENERIC_ALL	Повний контроль: включає всі небезпечні дії над директорією
DELETE	Дозволяє видаляти директорію, а потім створювати нову з успадковуваними правами
FILE_LIST_DIRECTORY, FILE_READ_ATTRIBUTES, FILE_READ_EA	Можливе розкриття конфіденційної інформації. Дозволяє перегляд метаданих файлів у каталозі. Назви файлів можуть містити чутливі відомості, а також імена користувачів або інші дані, що можуть бути використані у багатостадійній атаці
GENERIC_READ	Можливе розкриття інформації. Це право включає FILE_LIST_DIRECTORY, FILE_READ_ATTRIBUTES та FILE_READ_EA, що дозволяє читати вміст і структуру каталогу

Таблиця 1.4 [3, с 572] – Права доступу файлів Windows та їх вплив на безпеку

Назва права доступу	**Опис впливу при наданні ненадійному або частково довіреному користувачу**
FILE_WRITE_DATA	Можливе підвищення привілеїв. Дозволяє перезаписувати вміст файлу
FILE_APPEND_DATA	Можливе підвищення привілеїв. Дозволяє додавати довільні дані в кінець файлу
WRITE_DAC	Можливе підвищення привілеїв. Дозволяє змінювати DACL файлу, надаючи собі будь-які права доступу до файлу
WRITE_OWNER	Можливе підвищення привілеїв. Дозволяє ставати власником об’єкта. Власник може змінювати DACL (має право WRITE_DAC), що дає повний контроль над файлом
GENERIC_WRITE	Можливе підвищення привілеїв. Включає право FILE_WRITE_DATA
GENERIC_ALL	Можливе підвищення привілеїв. Включає право FILE_WRITE_DATA (повний контроль)
DELETE	Можливе підвищення привілеїв. Дозволяє видаляти файл і потенційно замінювати його на інший, контрольований зловмисником
FILE_READ_DATA	Можливе розкриття конфіденційної інформації. Дозволяє переглядати вміст файлу

Кінець таблиці 1.4

FILE_READ_ATTRIBUTES, FILE_READ_EA	Можливе розкриття інформації. Дозволяє читати метадані файлу, які можуть містити чутливу інформацію, наприклад імена файлів чи налаштування
GENERIC_READ	Можливе розкриття інформації. Включає FILE_READ_DATA, FILE_READ_ATTRIBUTES і FILE_READ_EA, що дає повний доступ до вмісту файлу і його метаданих

1.3.5 Оновлення системи та антивірусний захист

У контексті аудиту інформаційної безпеки вкрай важливо перевірити, чи належно перевірені механізми оновлення Windows, а також чи правильно конфігурований вбудований антивірусний захист, а саме Windows Defender, оскільки відсутність цих засобів створюють потенційні точки входу для зловмисників, неможливість виявлення та нейтралізації загрози, які вже проникли в систему та активні.

Розглянемо критерії безпеки, пов’язані з оновленнями системи та антивірусним захистом:

- Включити захист Windows Defender проти потенційно небажаних програм. Такі програми теоретично можуть бути дуже небезпечні та приховувати в собі шкідливе програмне забезпечення.

- Включити засіб Windows Defender SmartScreen. З його допомогою система захищає користувачів від запуску потенційно шкідливих програм та переходу на небезпечні вебсайти.
- Заборонити користувачам ігнорувати попередження Windows Defender SmartScreen для файлів та сайтів.
- Включити сканування в реальному часі для Windows Defender. Це налаштування є дуже важливим, оскільки антивірус сканує ресурси в момент взаємодії з ними та блокує активність шкідливого програмного забезпечення.
- Включити оновлення визначення вірусів. Визначення вірусів – це файли, які Windows Defender використовує для сканування системи та визначення шкідливого програмного забезпечення. Періодичне оновлення цих файлів забезпечить захист від нещодавно відкритих вразливостей. [2]

1.3.6 Порти, служби та автозапуск

Один з ключових аспектів забезпечення захищеного стану системи з ОС Windows – це контроль за активними сервісами, службами та елементами автозавантаження. Непотрібні або шкідливі сервіси та процеси здатні створити потенційні точки входу для зловмисників.

Одна з найкращих рекомендацій стосовно менеджменту портів полягає в тому, що мають бути відкриті тільки необхідні порти. Для забезпечення безпечної конфігурації системи слід залишити відкритими лише ті порти, які використовуються в бізнес-процесах або службах. В першу чергу слід перевіряти на факт відкритості саме ці порти, оскільки вони є найбільш вразливими до атак:

21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 53 (DNS), 137 та 139 (NetBIOS over TCP), 445 (SMB), 80, 443, 8080, 8443 (HTTP, HTTPS), 1433, 1434, 3006 (порти, що використовуються базами даних) та 3389 (Remote Desktop). [4]

Рекомендації для менеджменту служб:

- Вимкнути сервіс Bluetooth. Сама технологія вважається не дуже безпечною і при своїй роботі не завжди використовує шифрування, тому цей сервіс бажано вимкнути.
- Вимкнути сервіс геолокації. З точки зору безпеки, це погана ідея розкривати своє місцезнаходження, тому цей сервіс треба вимкнути.
- Вимкнути Windows Mobile Hotspot Service. Можливість запуску мобільної точки доступу робить мережу дуже вразливою для хакерів та іншого роду зловмисників.
- Вимкнути Computer Browser Service. Цей сервіс є застарілим та може використовувати небезпечні протоколи, що генерують забагато зайвого трафіку, що в свою чергу підвищує ризик атаки.
- Вимкнути Infrared Monitor Service. Даний сервіс не є безпечним та його з’єднання можуть стати причиною витоку данних.
- Вимкнути FTP Server Service. Якщо комп’ютер відкритий як FTP сервер, то це створює величезний ризик для безпеки.
- Xbox Game Monitoring Service. Цей сервіс не має нічого спільного з підприємствами, тому повинен бути вимкнений. [2]

Основна рекомендація, що стосується автозапуску – за замовчуванням не виконувати жодних команд автозапуску. При виконання команди автозапуску, система Windows не буде питати дозвіл користувача на виконання, що створює великий ризик для безпеки. [2]

Висновки до розділу 1

У цьому розділі було проведено аналіз теоретичного підґрунтя аудиту інформаційної безпеки, зокрема визначення основних критеріїв оцінки безпеки систем Windows.

Встановлено, що аудит інформаційної безпеки – це процес комплексної оцінки захищеності систем з метою виявлення вразливостей, оцінки ризиків та визначення рекомендацій щодо покращення рівня безпеки. Разом з цим було класифіковано шість основних типів аудиту інформаційної безпеки: внутрішній та зовнішній аудит, аудит на відповідність, аудит на вразливості, оцінка ризиків та тестування на проникнення.

Визначено п’ять основних компонентів безпеки Windows для аудиту та критерії безпеки для кожного з них: локальні політики безпеки, Windows Firewall, контроль доступу, антивірусний захист та менеджмент служб та портів.

2 АУДИТ БЕЗПЕКИ ОС WINDOWS ЗАСОБАМИ POWERSHELL

2.1 Особливості застосування PowerShell у сфері безпеки

PowerShell – це універсальне середовище командного рядка і скриптова мова, за допомогою якої можна забезпечити автоматизоване керування різними компонентами систем на основі Windows. Вона поєднує інтерфейс командного рядка разом з елементами об’єктно-орієнтованого програмування, що робить PowerShell хорошим та зручним засобом адміністрування. [8, 19]

На відміну від традиційних оболонок, наприклад Bash, які працюють переважно з текстовими даними, PowerShell оперує об'єктами .NET. Це означає, що вхідні та вихідні дані командлетів є об’єктами, що дозволяє легко отримувати доступ до їх властивостей та методів, в той час коли зі звичайними текстовими даними такий підхід був би значно складніший. Наприклад, команда Get-Process повертає об'єкти процесів, з яких можна безпосередньо отримати необхідну інформацію. PowerShell інтегрований в Windows та може отримати доступ до компонентів системи – файлової системи, реєстру, служб, мережеві інтерфейси, журнали подій, та засобів, таких як Windows Management Instrumentation (WMI) та Common Information Model (CIM). Мова PowerShell підтримує підключення зовнішніх модулів, що дає змогу додавати підтримку специфічних технологій (наприклад, Active Directory, Windows Defender або брандмауера). PowerShell дає змогу створювати сценарії, які можуть запускатися вручну, за розкладом або при виконанні певних встановлених умов. За допомогою цього механізму можна реалізувати постійний моніторинг безпеки, щоденне сканування критичних налаштувань або реагування на ті чи інші зміни. Сукупність цих особливостей

дає можливість застосувати PowerShell для аудиту інформаційної безпеки, ефективно перевіряючи налаштування безпеки системи. [8, 19]

PowerShell може працювати з такими рівнями доступу:

- User – звичайний користувацький рівень доступу з обмеженим функціоналом.
- Administrator – повний доступ до системних ресурсів. Важливо не надавати такий рівень доступу невповноваженим особам.
- System - найвищий рівень доступу до системних ресурсів. Якщо команди запускаються від імені служб, вони можуть отримати доступ до критичних компонентів ОС.

Політика виконання PowerShell – це захисний механізм, створений для контролювання умов роботи PowerShell скриптів, в результаті чого захищає від запуску шкідливих скриптів і несанкціонованого доступу. Існують такі політики виконання:

- AllSigned - дозволяє запуск скрипта, але лише у випадку підписання довіреною особою, а також запитує дозвіл для запуску скриптів від видавників, які ще не були визначені як надійні чи ненадійні.
- Bypass – нічого не блокується і нема ніяких попереджень.
- Default – політика виконання за замовчуванням. Зазвичай це політика RemoteSigned для клієнтів та серверів Windows.
- RemoteSigned – скрипти можуть виконуватись, але завантажені з інтернету скрипти та файли конфігурації потребують цифрового підпису для роботи.
- Restricted – скрипти не дозволяються для запуску, на відміну від окремих команд.
- Undefined – політика виконання не задана.

- Unrestricted – запуск скриптів дозволено, буде запит на дозвіл для запуску скриптів. [5]

Отже, PowerShell є універсальним інструментом для виконання адміністративних задач у системах на основі Windows завдяки можливостям взаємодіяти з внутрішніми елементами операційної системи, об’єктної моделі та можливості реалізації автоматизації. Однією з адміністративних задач може бути аудит інформаційної безпеки.

2.2 Перевірка основних аспектів безпеки Windows

2.2.1 Перевірка політик безпеки

secedit /export /cfg C:\audit.txt – команда, яка робить експорт налаштувань локальної політики Windows у вигляді текстового файлу. [17]

Secedit – системна утиліта Windows, створена для імпорту та експорту політик безпеки, застосувань шаблонів безпеки та аналізу відповідності конфігурації системи стандартам.

/export – ключ, що вказує на те, що треба експортувати поточні налаштування безпеки.

/cfg C:\audit.txt – шлях до файлу, в якому буде збережена конфігурація.

Після виконання цієї команди дані зчитуємо за допомогою Get-Content C:\audit.txt

```
PS C:\Windows\system32> secedit /export /cfg C:\audit.txt

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.

PS C:\Windows\system32> Get-Content C:\audit.txt
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 0
MaximumPasswordAge = -1
MinimumPasswordLength = 0
PasswordComplexity = 0
PasswordHistorySize = 0
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
NewAdministratorName = "Administrator"
NewGuestName = "Guest"
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableAdminAccount = 0
EnableGuestAccount = 0
[Event Audit]
AuditSystemEvents = 0
AuditLogonEvents = 0
AuditObjectAccess = 0
AuditPrivilegeUse = 0
AuditPolicyChange = 0
AuditAccountManage = 0
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 0
```

Рисунок 2.1 – Створення конфігураційного файлу безпеки через secedit /export

```
[Privilege Rights]
SeNetworkLogonRight = *S-1-1-0,*S-1-5-32-544,*S-1-5-32-545,*S-1-5-32-551
SeBackupPrivilege = *S-1-5-32-544,*S-1-5-32-551
SeChangeNotifyPrivilege = *S-1-1-0,*S-1-5-19,*S-1-5-20,*S-1-5-32-544,*S-1-5-32-545,*S-1-5-32-551
SeSystemtimePrivilege = *S-1-5-19,*S-1-5-32-544
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-544
SeAuditPrivilege = *S-1-5-19,*S-1-5-20
SeIncreaseQuotaPrivilege = *S-1-5-19,*S-1-5-20,*S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544,*S-1-5-90-0
SeLoadDriverPrivilege = *S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-559
SeServiceLogonRight = *S-1-5-80-0
SeInteractiveLogonRight = Guest,*S-1-5-32-544,*S-1-5-32-545,*S-1-5-32-551
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544,*S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420
SeAssignPrimaryTokenPrivilege = *S-1-5-19,*S-1-5-20
SeRestorePrivilege = *S-1-5-32-544,*S-1-5-32-551
SeShutdownPrivilege = *S-1-5-32-544,*S-1-5-32-545,*S-1-5-32-551
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeDenyNetworkLogonRight = Guest
SeDenyInteractiveLogonRight = Guest
SeUndockPrivilege = *S-1-5-32-544,*S-1-5-32-545
SeManageVolumePrivilege = *S-1-5-32-544
SeRemoteInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-555
SeImpersonatePrivilege = *S-1-5-19,*S-1-5-20,*S-1-5-32-544,*S-1-5-6
SeCreateGlobalPrivilege = *S-1-5-19,*S-1-5-20,*S-1-5-32-544,*S-1-5-6
SeIncreaseWorkingSetPrivilege = *S-1-5-32-545
SeTimeZonePrivilege = *S-1-5-19,*S-1-5-32-544,*S-1-5-32-545
SeCreateSymbolicLinkPrivilege = *S-1-5-32-544
SeDelegateSessionUserImpersonatePrivilege = *S-1-5-32-544
```

Рисунок 2.2 – Створення конфігураційного файлу безпеки через secedit /export (продовження)

Вивід має розділ System Access, в якому є велика кількість змінних, які зберігають системні налаштування, описані в Local Security Policy в підрозділах Password Policy, Account Lockout Policy та Security Options:

- Password Policy
  - PasswordHistorySize – історія паролів (кількість попередніх паролів, які не можна повторити).
  - MaximumPasswordAge – максимальний вік паролю (днів).
  - MinimumPasswordAge – мінімальний вік паролю (днів).
  - MinimumPasswordLength – мінімальна довжина паролю.
  - PasswordComplexity – увімкнення складності паролю (1 – увімкнено, 0 - вимкнено).
  - ClearTextPassword – увімкення зберігання пароля з використанням зворотного шифрування (0 - паролі не зберігаються зворотно зашифрованими, 1 - паролі зберігаються у форматі, який можна розшифрувати)
- Account Lockout Policy
  - LockoutBadCount – максимальна кількість невдалих спроб входу.
  - LockoutDuration – тривалість блокування (хв).
  - ResetLockoutCount – час до обнулення лічильника (хв).
  - AllowAdministratorLockout – чи дозволено блокування адміністратора (1 – дозволено, 0 – не дозволено).
- Security Options
  - EnableAdminAccount – увімкнення вбудованого облікового запису адміністратора (1 – увімкнено, 0 - вимкнено).
  - EnableGuestAccount - увімкнення вбудованого облікового запису гостя (1 – увімкнено, 0 - вимкнено).

- NewAdministratorName – назва вбудованого облікового запису адміністратора.
- NewGuestName – назва вбудованого облікового запису гостя.

Для перевірки налаштувань цих розділів в аудиті безпеки достатньо дістати значення налаштувань і порівняти їх з еталонними.

Вивід команди також має розділ Privilege Rights, в якому, аналогічно з розділом System Access, зберігає змінні, в яких зберігається інформація про те, яким користувачам та групам за їх значенням SID надаются привілеї:

- SeRemoteInteractiveLogonRight – доступ до системи через віддалений робочий стіл (RDP).
- SeSystemtimePrivilege – зміна системного часу.
- SeTakeOwnershipPrivilege – взяття володіння об’єктами.
- SeServiceLogonRight – вхід у систему як служба.
- SeSecurityPrivilege – керування аудитом і журналами подій.
- SeDenyNetworkLogonRight – заборона входу через мережу.
- SeLoadDriverPrivilege – дозволяє завантаження драйверів.

В цьому розділі, аналогічно як з минулим, треба дістати відповідні значення налаштувань, але оскільки значення зберігають SID користувача чи групи користувачів, до яких відноситься те чи інше налаштування, треба реалізувати визначення типу облікового запису за його SID, щоб вже отриманні значення порівняти з еталонними.

$obj = New-Object System.Security.Principal.SecurityIdentifier("S-1-5-32-544")

$obj.Translate([System.Security.Principal.NTAccount])

```
PS C:\Windows\system32> $obj = New-Object System.Security.Principal.SecurityIdentifier("S-1-5-32-544")
PS C:\Windows\system32> $obj.Translate([System.Security.Principal.NTAccount])
Value
-----
BUILTIN\Administrators
```

Рисунок 2.3 – Визначення групи "Administrators" за SID у PowerShell

Цей фрагмент PowerShell коду можна використати для перетворення SID у читабельне ім’я користувача чи групи.

New-Object – стандартна PowerShell-команда для створення .Net об’єктів.

System.Security.Principal.SecurityIdentifier – це .NET-клас, який представляє SID в об'єктному вигляді.

("S-1-5-32-544") – це SID користувача чи групи користувачів, в даному випадку це група Адміністраторів.

В результаті ми отримуємо об’єкт SID, який зберігається у змінній $obj.

.Translate(...) - це команда, яка перетворює SID у звичну людині назву користувача або групи.

[System.Security.Principal.NTAccount] — вказує, що ми хочемо перетворити SID в тип NTAccount, тобто в іменовану форму: BUILTIN\Administrators.

В результаті отримаємо назву облікового запису або групи у форматі Джерело\Назва

Для перевірки стану політики, пов’язаною з дозволом на завантаження непідписаних драйверів, доцільно використати утиліту bcdedit, яка виводить інформацію про конфігурацію завантажувача операційної системи.

Щоб перевірити, чи дозволено завантаження непідписаних драйверів, можна використати наступну команду PowerShell:

bcdedit | Select-String -Pattern "testsigning" [7]

```
PS C:\Windows\system32> bcdedit | Select-String -Pattern "testsigning"

testsigning             No


PS C:\Windows\system32>
```

Рисунок 2.4 – Перевірка значення параметра testsigning

bcdedit – утиліта, що виводить усі параметри конфігурації завантаження системи (Boot Configuration Data).

Select-String -Pattern "testsigning" - виконує пошук у виводі наявності параметра testsigning.

В результаті ми отримаємо значення параметра testsigning, значення якого вказує на дозвіл завантаження непідписаних драйверів (при значенні “yes” система дозволяє завантаження непідписаних драйверів, при значенні “no” або відсутності цього параметра забороняє).

Політики інтерактивного входу налаштовують інформацію, яка буде показуватися на екрані входу в систему Windows, наприклад певні попередження. Інші важливі політики – це політики пов’язані з UAC. Дані налаштування зберігаються в розділі реєстру HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. За допомогою команди Get-ItemProperty можна отримати значення реєстру Windows.

Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"

```
PS C:\Windows\system32> Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"


ConsentPromptBehaviorAdmin   : 5
ConsentPromptBehaviorUser    : 3
DSCAutomationHostEnabled     : 2
EnableCursorSuppression      : 1
EnableFullTrustStartupTasks  : 2
EnableInstallerDetection     : 1
EnableLUA                    : 1
EnableSecureUIAPaths         : 1
EnableUIADesktopToggle       : 0
EnableUwpStartupTasks        : 2
EnableVirtualization         : 1
PromptOnSecureDesktop        : 1
SupportFullTrustStartupTasks : 1
SupportUwpStartupTasks       : 1
ValidateAdminCodeSignatures  : 0
dontdisplaylastusername      : 0
legalnoticecaption           :
legalnoticetext              :
scforceoption                : 0
shutdownwithoutlogon         : 1
undockwithoutlogon           : 1
PSPath                       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curren
                               tVersion\Policies\System
PSParentPath                 : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curren
                               tVersion\Policies
PSChildName                  : System
PSDrive                      : HKLM
PSProvider                   : Microsoft.PowerShell.Core\Registry
```

Рисунок 2.5 – Отримання параметрів з реєстру HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Команда, яка виводить налаштування відповідного реєстру. Параметри, які нас будуть цікавити у виводі команди, це:

- DontDisplayLastUserName – чи показувати останього користувача на екрані входу (якщо значення 1 – ім’я не показуєтсья, якщо значення 0 - показується).
- LegalNoticeCaption – заголовок попереджувального повідомлення.
- LegalNoticeText – текст попереджувального повідомлення.
- EnableLUA – включати UAC (1 – увімкнено, 0 - вимкнено).
- ConsentPromptBehaviorAdmin – поведінка запиту для адміністратора (рекомендоване значення 5 - Запит на підтвердження з можливістю натиснути "Так/Ні").
- InactivityTimeoutSecs – час неактивності залогіненого користувача, після якого завершиться сеанс.

В аудиті безпеки достатньо дістати значення цих параметрів та порівняти з еталонними значеннями.

Одними з найважливіших політик безпеки є політики мережевої безпеки. Налаштування цих політик зберігаються в реєстрі HKLM\SYSTEM\CurrentControlSet\Control\Lsa і він аналогічно може бути прочитаним за допомогою Get-ItemProperty.

Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"

```
PS C:\Windows\system32> Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"


auditbasedirectories      : 0
auditbaseobjects          : 0
Bounds                    : {0, 48, 0, 0...}
crashonauditfail          : 0
fullprivilegeauditing     : {0}
LimitBlankPasswordUse     : 1
NoLmHash                  : 1
Security Packages         : {""}
Notification Packages     : {scecli}
Authentication Packages   : {msv1_0}
LsaPid                    : 584
LsaCfgFlagsDefault        : 0
SecureBoot                : 1
ProductType               : 6
disabledomaincreds        : 0
everyoneincludesanonymous : 0
forceguest                : 0
restrictanonymous         : 0
restrictanonymoussam      : 1
SamConnectedAccountsExist : 1
PSPath                    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Ls
PSParentPath              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
PSChildName               : Lsa
PSDrive                   : HKLM
PSProvider                : Microsoft.PowerShell.Core\Registry
```

Рисунок 2.6 – Отримання параметрів з реєстру HKLM:\SYSTEM\CurrentControlSet\Control\Lsa

Поле з виводу команди, яке нас цікавить в аудиті інформаційної безпеки це RestrictAnonymous, що забороняє анонімний доступ до ресурсів через мережу (1 – заборона, 0 - дозвіл), та LimitBlankPasswordUse – що забороняє дозвіл на використання пустих паролів (1 – заборона, 0 - дозвіл).

Для отримання інформації про вбудований аудит Windows можна скористатися командою PowerShell auditpol.

*auditpol /get /category:**

```
>> auditpol /get /category:*
System audit policy
Category/Subcategory                        Setting
System
  Security System Extension                 No Auditing
  System Integrity                          Success and Failure
  IPsec Driver                              No Auditing
  Other System Events                       Success and Failure
  Security State Change                     Success
Logon/Logoff
  Logon                                     Success and Failure
  Logoff                                    Success
  Account Lockout                           Success
  IPsec Main Mode                           No Auditing
  IPsec Quick Mode                          No Auditing
  IPsec Extended Mode                       No Auditing
  Special Logon                             Success
  Other Logon/Logoff Events                 No Auditing
  Network Policy Server                     Success and Failure
  User / Device Claims                      No Auditing
  Group Membership                          No Auditing
Object Access
  File System                               No Auditing
  Registry                                  No Auditing
  Kernel Object                             No Auditing
  SAM                                       No Auditing
  Certification Services                    No Auditing
  Application Generated                     No Auditing
  Handle Manipulation                       No Auditing
  File Share                                No Auditing
  Filtering Platform Packet Drop            No Auditing
  Filtering Platform Connection             No Auditing
  Other Object Access Events                No Auditing
  Detailed File Share                       No Auditing
  Removable Storage                         No Auditing
  Central Policy Staging                    No Auditing
Privilege Use
  Non Sensitive Privilege Use               No Auditing
  Other Privilege Use Events                No Auditing
  Sensitive Privilege Use                   No Auditing
Detailed Tracking
  Process Creation                          No Auditing
  Process Termination                       No Auditing
  DPAPI Activity                            No Auditing
  RPC Events                                No Auditing
  Plug and Play Events                      No Auditing
  Token Right Adjusted Events               No Auditing
Policy Change
  Audit Policy Change                       Success
  Authentication Policy Change              Success
  Authorization Policy Change               No Auditing
  MPSSVC Rule-Level Policy Change           No Auditing
  Filtering Platform Policy Change          No Auditing
  Other Policy Change Events                No Auditing
Account Management
  Computer Account Management               No Auditing
  Security Group Management                 Success
  Distribution Group Management             No Auditing
  Application Group Management              No Auditing
  Other Account Management Events           No Auditing
  User Account Management                   Success
DS Access
  Directory Service Access                  No Auditing
  Directory Service Changes                 No Auditing
  Directory Service Replication             No Auditing
  Detailed Directory Service Replication    No Auditing
Account Logon
  Kerberos Service Ticket Operations        No Auditing
  Other Account Logon Events                No Auditing
  Kerberos Authentication Service           No Auditing
  Credential Validation                     No Auditing
```

Рисунок 2.7 – Отримання налаштувань політик вбудованого аудиту

Ця команда дозволяє вивести весь перелік аудиту та його статус, чи він увімкнений. Завдяки цьому можна швидко перевірити, які саме події безпеки зараз фіксуються системою. [6]

Вивід цієї команди фіксує основі категорії аудиту, такі як вхід та вихід до облікового запису, доступ до ресурсів файлової системи, використання привілеїв, зміна політик безпеки, та інші, що необхідні для моніторингу активності та аналізу безпеки системи. В колонці Settings вказується поточний стан відповідної категорії аудиту. Цих станів може бути всього чотири:

- No Auditing – аудит цієї події вимкнений.
- Success – фіксуються тільки вдалі події в системі (наприклад, вдалий логін).
- Failure – фіксуються тільки невдалі події в системі (наприклад, невдалий логін).
- Success and Failure – фіксуються як вдалі, так і невдалі події.

В аудиті інформаційної безпеки треба перевірити чи увімкнений збір важливої інформації. Це буде реалізовано за допомогою порівняння значення з виводу цієї команди з еталонними значеннями, що відповідають критеріям безпеки.

2.2.2 Перевірка конфігурації брандмауера

Для перевірки налаштувань Windows Firewall, використовується команда PowerShell *Get-NetFirewallProfile.* Цей командлет надає повну інформацію щодо основних параметрів брандмауера, які належать до відповідних профілів мережевого підключення. [14]

```
PS C:\Windows\system32> Get-NetFirewallProfile


Name                            : Domain
Enabled                         : True
DefaultInboundAction            : NotConfigured
DefaultOutboundAction           : NotConfigured
AllowInboundRules               : NotConfigured
AllowLocalFirewallRules         : NotConfigured
AllowLocalIPsecRules            : NotConfigured
AllowUserApps                   : NotConfigured
AllowUserPorts                  : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen                  : True
EnableStealthModeForIPsec       : NotConfigured
LogFileName                     : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes             : 4096
LogAllowed                      : False
LogBlocked                      : False
LogIgnored                      : NotConfigured
DisabledInterfaceAliases        : {NotConfigured}

Name                            : Private
Enabled                         : True
DefaultInboundAction            : NotConfigured
DefaultOutboundAction           : NotConfigured
AllowInboundRules               : NotConfigured
AllowLocalFirewallRules         : NotConfigured
AllowLocalIPsecRules            : NotConfigured
AllowUserApps                   : NotConfigured
AllowUserPorts                  : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen                  : True
EnableStealthModeForIPsec       : NotConfigured
LogFileName                     : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes             : 4096
LogAllowed                      : False
LogBlocked                      : False
LogIgnored                      : NotConfigured
DisabledInterfaceAliases        : {NotConfigured}

Name                            : Public
Enabled                         : True
DefaultInboundAction            : NotConfigured
DefaultOutboundAction           : NotConfigured
AllowInboundRules               : NotConfigured
AllowLocalFirewallRules         : NotConfigured
AllowLocalIPsecRules            : NotConfigured
AllowUserApps                   : NotConfigured
AllowUserPorts                  : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen                  : True
EnableStealthModeForIPsec       : NotConfigured
LogFileName                     : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes             : 4096
LogAllowed                      : False
LogBlocked                      : False
LogIgnored                      : NotConfigured
DisabledInterfaceAliases        : {NotConfigured}
```

Рисунок 2.8 – Отримання конфігурації профілів брандмауера

Команда виводить налаштування безпеки для кожного з трьох профілів брандмауера: Domain, Private, Public. Серед параметрів конфігурації, які будуть розглядатися в аудиті безпеки, присутні:

- Enabled – відображає, чи увімкнено брандмауер для відповідного профілю (True або False).
- DefaultInboundAction – вказує дію за замовчуванням для вхідних з’єднань (Block або Allow).
- DefaultOutboundAction – вказує дію за замовчуванням для вихідних з’єднань (Block або Allow).
- AllowLocalFirewallRules – чи дозволено застосування локальних правил брандмауера (True або False).
- AllowLocalIPsecRules – чи дозволено локальні IPsec-правила (True або False).
- LogFileName – шлях до файлу, в який здійснюється журналювання подій брандмауера.
- LogAllowed – чи ведеться журналювання дозволених з’єднань (True або False).
- LogBlocked – чи ведеться журналювання заблокованих з’єднань (True або False).

Отримані дані можна зберегти для порівняння з еталонними значеннями відповідно до стандартів.

За допомогою команди *Get-NetIPsecRule | Where-Object { $_.Enabled -eq 'True' },* аналогічно як з минулою командою, можна вивести активні правила IpSec протоколів. Оскільки цей протокол в нашій системі використовуватися не буде, то в аудиті безпеки ми будемо дивитись, чи вивід команди пустий. [14]

Одним з критеріїв безпеки є заборона на вхідний Echo Request трафік. За допомогою цієї команди Powershell можна перевірити наявність правила, яке дозволяє цей трафік:

```
Get-NetFirewallRule -Direction Inbound | Where-Object {
    $_.Enabled -eq $true -and
    $_.Action -eq "Allow" -and
    ($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and
    $_.Name -match "EchoRequest|ERQ"
}| Select-Object Name, DisplayName, Enabled, Direction, Action, Profile
```

Get-NetFirewallRule -Direction Inbound – команда, що отримує всі правила брандмауера для вхідного трафіку.

Where-Object { ... } – командлет, який фільтрує отриманий масив за умовами, які знаходяться в блоці.

$_.Enabled -eq $true – фільтруємо лише увімкнені правила.

$_.Action -eq "Allow" – відбираємо правила, які дозволяють трафік.

($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") – перевіряємо в назві правила рядок з назвою ICMP протоколу.

$_.DisplayName -match "EchoRequest|ERQ" – перевіряємо в назві правила рядок EchoRequest чи ERQ.

Якщо змінна $icmpEchoInboundAllowed не буде пустою, то у команди буде вивід, що означає, що вхідний Echo Request трафік дозволений.

Аналогічно до минулої команди, можна записати команду для пошуку активного правила, що дозволяє вхідні Destionation Unreachable ICMP пакети, наявність якого треба перевіряти в аудиті безпеки:

Get-NetFirewallRule -Direction Inbound | Where-Object {

$_.Enabled -eq $true -and

$_.Action -eq "Allow" -and

($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and

($_.Name -match "DU|DestinationUnreachable")

} | Select-Object Name, DisplayName, Enabled, Direction, Action, Profile

```
PS C:\Windows\system32> Get-NetFirewallRule -Direction Inbound | Where-Object {
    $_.Enabled -eq $true -and
    $_.Action -eq "Allow" -and
    ($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and
    ($_.Name -match "DU|DestinationUnreachable")
} | Select-Object Name, DisplayName, Enabled, Direction, Action, Profile


Name        : CoreNet-ICMP6-DU-In
DisplayName : Core Networking - Destination Unreachable (ICMPv6-In)
Enabled     : True
Direction   : Inbound
Action      : Allow
Profile     : Any

Name        : CoreNet-ICMP4-DUFRAG-In
DisplayName : Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)
Enabled     : True
Direction   : Inbound
Action      : Allow
Profile     : Any
```

Рисунок 2.9 – Перевірка наявності активних правил дозволу вхідниxDestionation Unreachable ICMP пакетів

На відміну від минулої команди, в цій ми шукаємо рядки DU чи DestinationUnreachable в назві правила. Нашим критерієм безпеки є наявність

цього активного правила, тому при виконанні команди, якщо вона матиме вивід, можна зробити висновок про те, що критерій дотримано.

2.2.3 Аналіз облікових записів і прав доступу

Для перевірки часу останнього логіну можна використати наступний код:

```
Get-LocalUser | Where-Object { $_.Enabled -eq $true } | ForEach-Object {
    [PSCustomObject]@{
        User = $_.Name
        LastLogon = $_.LastLogon
    }
}
```

```
PS C:\Windows\system32> Get-LocalUser | Where-Object { $_.Enabled -eq $true } | ForEach-Object {
    [PSCustomObject]@{
        User = $_.Name
        LastLogon = $_.LastLogon
    }
}

User       LastLogon
----       ---------
seemsgucci 09.06.2025 16:43:05
```

Рисунок 2.10 – Отримання списку користувачів разом з часов останнього логіну

Get-LocalUser – отримує список локальних користувачів системи.

Where-Object { $_.Enabled -eq $true } – фільтрує лише активні аккаунти.

ForEach-Object { ... } – для кожного користувача виконуємо дію.

В результаті отримуємо список активних користувачів разом з датою останнього логіну. Це може бути корисним для відслідковування несанкціонованого доступу до аккаунту та знаходження забутих і застарілих облікових записів. [12]

Для отримання списку користувачів, що належать групі адміністраторів, можна використати код:

Get-LocalGroupMember -Group "Administrators" [11]

```
PS C:\Windows\system32> Get-LocalGroupMember -Group "Administrators"

ObjectClass Name                          PrincipalSource
----------- ----                          ---------------
User        DESKTOP-U5DQAB1\Administrator Local
User        DESKTOP-U5DQAB1\user2         Local


PS C:\Windows\system32>
```

Рисунок 2.11 – Отримання списку користувачів-адміністраторів

В аудиті інформаційної безпеки слід переконатися, що до групи адміністраторів не належать користувачі, що не повинні.

Для отримання списку тимчасових та технічних акаунтів можна використати наступний код:

Get-LocalUser | Where-Object { $_.Name -match "temp|test|guest|install" } [12]

```
PS C:\Windows\system32> Get-LocalUser | Where-Object { $_.Name -match "temp|test|guest|install" }

Name  Enabled Description
----  ------- -----------
Guest False   Built-in account for guest access to the computer/domain


PS C:\Windows\system32>
```

Рисунок 2.12 – Отримання списку тимчасових та службових акаунтів

В аудиті інформаційної безпеки такі акаунти слід знаходити та, зазвичай, видаляти.

Для отримання прав доступу об'єкта файлової системи існує команда:

Get-Acl -Path "шлях до файлу" [10]

```
PS C:\Windows\system32> $acl = Get-Acl -Path "C:\Users\lab3m\Desktop\test.txt"
PS C:\Windows\system32> $acl | Format-List -Force
>>


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\lab3m\Desktop\test.txt
Owner  : DESKTOP-U5DQAB1\user2
Group  : DESKTOP-U5DQAB1\None
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         DESKTOP-U5DQAB1\user2 Allow  FullControl
Audit  :
Sddl   : O:S-1-5-21-1777076922-1185462647-3778723286-1001G:S-1-5-21-1777076922-1185462647-3778723286-513D:(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5
         -21-1777076922-1185462647-3778723286-1001)
```

Рисунок 2.13 – Отримання списку ACL файлу

В процесі перевірки конфігурації DACL слід перевіряти на наявність потенційно небезпечних прав.

Важливою частиною аудиту безпеки є перевірка на те, чи не надаються права до файлів чи папок окремим користувачам. Для цього можна використати код:

$path = "C:\Users\Public"

Get-ChildItem -Path $path -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {

try {

$acl = Get-Acl $_.FullName -ErrorAction Stop

```
            foreach ($ace in $acl.Access) {
                $identity = $ace.IdentityReference.Value

                $sid =
([System.Security.Principal.NTAccount]$identity).Translate([System.Security.Princip
al.SecurityIdentifier])
                if ($sid.Value -match "^S-1-5-21") {
                    [PSCustomObject]@{
                        FilePath = $_.FullName
                        User     = $identity
                        Rights   = $ace.FileSystemRights
                    }
                }
            }
        } catch {

        }
        }
```

```
PS C:\Windows\system32> $path = "C:\Users\Public"

Get-ChildItem -Path $path -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
    try {
        $acl = Get-Acl $_.FullName -ErrorAction Stop
        foreach ($ace in $acl.Access) {
            $identity = $ace.IdentityReference.Value

            $sid = ([System.Security.Principal.NTAccount]$identity).Translate([System.Security.Principal.S
            if ($sid.Value -match "^S-1-5-21") {
                [PSCustomObject]@{
                    FilePath = $_.FullName
                    User     = $identity
                    Rights   = $ace.FileSystemRights
                }
            }
        }
    } catch {

    }
}


FilePath
--------
C:\Users\Public\AccountPictures
C:\Users\Public\AccountPictures
C:\Users\Public\Documents
C:\Users\Public\Downloads
C:\Users\Public\Libraries
```

Рисунок 2.14 – Перевірка чи не надаються права до файлів чи папок окремим користувачам

Get-ChildItem -Path $path -Recurse -Force -ErrorAction SilentlyContinue – рекурсивно отримуємо список елементів папки C:\Users\Public.

ForEach-Object { ... } – для кожного знайденого елементу буде виконуватися дія в блоці.

Get-Acl $_.FullName -ErrorAction Stop – отримує список ACL для файла чи папки.

foreach ($ace in $acl.Access) { ... } – перебирає кожен ACE в ACL.

$identity = $ace.IdentityReference.Value – отримуємо назву, якій адресовано право.

$sid = ([System.Security.Principal.NTAccount]$identity).Translate([System.Security.Principal.SecurityIdentifier]) – код, що перетворює ім'я в SID.

if ($sid.Value -match "^S-1-5-21") – шаблон SID, який притаманний саме обліковим записам користувача.

В результаті дії коду отримуємо список файлів, в яких є записи ACE, що надані тільки окремим користувачам. В аудиті безпеки треба вказувати на такі файли, оскільки вони мають неоптимально встановлені права. [10]

Однією з інших важливих політик є перевірка прав на кореневий каталог, а саме те, чи можуть інші користувачі, крім адміністраторів, створювати в ньому файли і каталоги. Це можна перевірити за допомогою кода:

```
$acl = Get-Acl -Path "C:\"


foreach ($ace in $acl.Access) {
    $identity = $ace.IdentityReference
    $rights = $ace.FileSystemRights.ToString()


    if ($rights -match "CreateDirectories|Modify|FullControl") {
        if ($identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
            [PSCustomObject]@{
                UserOrGroup = $identity
                Rights      = $rights
                Path        = "C:\"
```

```
        }
      }
    }
  }
```

```
PS C:\Windows\system32> $acl = Get-Acl -Path "C:\"

foreach ($ace in $acl.Access) {
    $identity = $ace.IdentityReference
    $rights = $ace.FileSystemRights

    if ($rights -match "CreateDirectories|Modify|FullControl") {
        if ($identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
            [PSCustomObject]@{
                UserOrGroup = $identity
                Rights      = $rights
                Path        = "C:\"
            }
        }
    }
}


PS C:\Windows\system32>
```

Рисунок 2.15 – Перевірка наявності прав на зміну змісту кореневого каталогу в недовірених користувачів

$acl = Get-Acl -Path "C:\" – отримуємо записи ACL кореневого каталога.

foreach ($ace in $acl.Access) { - перебирає кожен ACE з ACL.

$identity = $ace.IdentityReference та $rights = $ace.FileSystemRights – для кожного ACE витягується назва користувача/групи та права доступу до кореневого каталогу

if ($rights -match "CreateDirectories|Modify|FullControl") { та if ($identity -notmatch "Administrators|SYSTEM|TrustedInstaller") { у випадку, якщо в записі ACE є правило, що дає доступ до створення файлів чи каталогів в кореневому каталозі і це право має не довірена особа (в нашому випадку це адміністратори,

система та TrustedInstaller), то команда виведе цей запис ACE, що свідчить про можливість недовіреної особи створювати файли і каталоги в кореневому каталозі. В аудиті безпеки треба перевіряти права кореневого каталогу та повідомляти про цю проблему у разі наявності. [10]

Іншою важливою перевіркою в аудиті безпеки є перевірка на наявність небезпечних прав доступу у файлів і каталогів, а саме Full Control. Такі файли можна знайти за допомогою коду:

```
$path = "C:\Users\Public"


Get-ChildItem -Path $path -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
    try {
        $acl = Get-Acl $_.FullName -ErrorAction Stop
        foreach ($ace in $acl.Access) {
            $identity = $ace.IdentityReference.Value
            $rights = $ace.FileSystemRights.ToString()

            if ($rights -match "FullControl" -and
                $identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
                [PSCustomObject]@{
                    FilePath = $_.FullName
                    User     = $identity
```

Rights = $rights

}

}

}

} catch {

}

}

```
PS C:\Windows\system32> $path = "C:\Users\Public"

Get-ChildItem -Path $path -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
    try {
        $acl = Get-Acl $_.FullName -ErrorAction Stop
        foreach ($ace in $acl.Access) {
            $identity = $ace.IdentityReference.Value
            $rights = $ace.FileSystemRights.ToString()

            if ($rights -match "FullControl" -and
                $identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
                [PSCustomObject]@{
                    FilePath = $_.FullName
                    User     = $identity
                    Rights   = $rights
                }
            }
        }
    } catch {

    }
}


FilePath
--------
C:\Users\Public\AccountPictures
C:\Users\Public\AccountPictures
C:\Users\Public\AccountPictures
C:\Users\Public\Documents
C:\Users\Public\Documents
C:\Users\Public\Downloads
C:\Users\Public\Downloads
```

Рисунок 2.16 – Перевірка наявності права Full Control у недовірених користувачів

Get-ChildItem -Path $path -Recurse -Force -ErrorAction SilentlyContinue – рекурсивно отримуємо список елементів папки C:\Users\Public.

ForEach-Object { ... } – для кожного знайденого елементу буде виконуватися дія в блоці.

Get-Acl $_.FullName -ErrorAction Stop – отримує список ACL для файла чи папки.

foreach ($ace in $acl.Access) { ... } – перебирає кожен ACE в ACL.

$identity = $ace.IdentityReference та $rights = $ace.FileSystemRights – для кожного ACE витягується назва користувача/групи та права доступу.

If ($rights -match "FullControl" та $identity -notmatch "Administrators|SYSTEM|TrustedInstaller" – ACE перевіряється на наявність права Full Control у не довіреної особи (в нашому випадку це адміністратори, система та TrustedInstaller).

В результаті код робить вивід всіх файлів та каталогів, що мають записи з небезпечним правом Full Control для звичайного користувача. В аудиті безпеки треба повідомляти про такі файли чи каталоги. [10]

2.3.4 Перевірка антивірусного захисту

Для перевірки налаштувань Windows Defender можна скористатися командлетом *Get-MpPreference,* який виведе низку налаштувань антивірусного сканування системи. [9]

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>
PS C:\Windows\system32> Get-MpPreference


AllowDatagramProcessingOnWinServer                    : False
AllowNetworkProtectionDownLevel                       : False
AllowNetworkProtectionOnWinServer                     : False
AllowSwitchToAsyncInspection                          : True
ApplyDisableNetworkScanningToIOAV                     : False
AttackSurfaceReductionOnlyExclusions                  :
AttackSurfaceReductionRules_Actions                   :
AttackSurfaceReductionRules_Ids                       :
AttackSurfaceReductionRules_RuleSpecificExclusions    :
AttackSurfaceReductionRules_RuleSpecificExclusions_Id :
BruteForceProtectionAggressiveness                    : 0
BruteForceProtectionConfiguredState                   : 0
BruteForceProtectionExclusions                        :
BruteForceProtectionLocalNetworkBlocking              : False
BruteForceProtectionMaxBlockTime                      : 0
BruteForceProtectionSkipLearningPeriod                : False
CheckForSignaturesBeforeRunningScan                   : False
CloudBlockLevel                                       : 0
CloudExtendedTimeout                                  : 0
ComputerID                                            : 3F4029CE-F19E-4186-97DE-E32B55A9C5F3
ControlledFolderAccessAllowedApplications             :
ControlledFolderAccessDefaultProtectedFolders         : {N/A: Controlled Folder Access is disabled}
ControlledFolderAccessProtectedFolders                :
DefinitionUpdatesChannel                              : 0
DisableArchiveScanning                                : False
DisableAutoExclusions                                 : False
DisableBehaviorMonitoring                             : False
DisableBlockAtFirstSeen                               : False
DisableCacheMaintenance                               : False
DisableCatchupFullScan                                : True
DisableCatchupQuickScan                               : True
DisableCoreServiceECSIntegration                      : False
DisableCoreServiceTelemetry                           : False
DisableCpuThrottleOnIdleScans                         : True
DisableDatagramProcessing                             : False
DisableDnsOverTcpParsing                              : False
DisableDnsParsing                                     : False
DisableEmailScanning                                  : True
DisableFtpParsing                                     : False
DisableGradualRelease                                 : False
```

Рисунок 2.17 – Отримання конфігурації брандмауера

Серед параметрів, значення яких будуть розглядатися в аудиті безпеки, присутні:

- PUAProtection – увімкнення захисту від потенційно небажаних програм (0 – вимкнено, 1 – режим блокування, 2 – режим аудиту)
- DisableRealtimeMonitoring – вимкнути сканування в реальному часі (False – сканування увімкнене, True - вимкнене)

Іншим критерієм безпеки є робота Windows Defender SmartScreen, налаштування якого зберігаються в реєстрі HKLM:\SOFTWARE\Policies\Microsoft\Windows\System. За допомогою наступної команди можна подивитися параметри цього захисного механізму.

Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System"

В виводі команди будемо розглядати налаштування двох полів:

EnableSmartScreen – чи увімкнений SmartScreen (1 – увімкнено, 0 - вимкнено)

PreventOverride - заборона ігнорування попереджень SmartScreen (1 – увімкнено, 0 - вимкнено)

Для перевірки дати останього оновлення визначення вірусів, можна скористатися командлетом *Get-MpComputerStatus* [9]

```
PS C:\Windows\system32>  Get-MpComputerStatus


AMEngineVersion                  : 1.1.25040.1
AMProductVersion                 : 4.18.25030.2
AMRunningMode                    : Normal
AMServiceEnabled                 : True
AMServiceVersion                 : 4.18.25030.2
AntispywareEnabled               : True
AntispywareSignatureAge          : 0
AntispywareSignatureLastUpdated  : 5/16/2025 2:29:37 PM
AntispywareSignatureVersion      : 1.429.34.0
AntivirusEnabled                 : True
AntivirusSignatureAge            : 0
AntivirusSignatureLastUpdated    : 5/16/2025 2:29:37 PM
```

Рисунок 2.18 – Отримання дати останього оновлення визначення вірусів

Поля, які зберігають дати останнього оновлення, це AntispywareSignatureLastUpdated та AntivirusSignatureLastUpdated. Останнє оновлення, очевидно, не повинно бути застарілим.

2.3.5 Аналіз портів, служб та автозапуску

З перевіркою відкритих портів дуже допоможе утиліта netstat. Передивитись відкриті порти можна за допомогою команди:

netstat -ano | Select-String "LISTENING" [15]

```
PS C:\Windows\system32> netstat -ano | Select-String "LISTENING"
>>

  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       816
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       584
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4996
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1004
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1092
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1748
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       588
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       816
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:7680              [::]:0                 LISTENING       4996
  TCP    [::]:49664             [::]:0                 LISTENING       600
  TCP    [::]:49665             [::]:0                 LISTENING       496
  TCP    [::]:49666             [::]:0                 LISTENING       1004
  TCP    [::]:49667             [::]:0                 LISTENING       1092
  TCP    [::]:49668             [::]:0                 LISTENING       1748
  TCP    [::]:49669             [::]:0                 LISTENING       588
```

Рисунок 2.19 – Отримання списку відкритих портів

В аудиті безпеки слід подивитись, чи використовуються непотрібні порти та звернути увагу на використання потенційно вразливих портів.

Для перевірки роботи сервіса можна скористатися командою:

Get-Service -Name <назва сервіса> [13]

Серед сервісів, які будемо перевіряти в аудиті безпеки, присутні:

- Bthserv – Bluetooth.
- Lfsvc – Geolocation Service.
- Icssvc - Windows Mobile Hotspot Service.
- Browser - Computer Browser Service.
- irmon - Infrared Monitor Service.
- FTPSVC - FTP Server Service.
- xbgm - Xbox Game Monitoring Service. [2]

Налаштування автозапуску зберігаються в наступних розділах реєстру:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run – запускає Запускає програми для всіх користувачів при вході в систему.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce – запускає програми один раз для всіх користувачів, після запуску запис видаляється.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run – запускає програми для поточного користувача при вході.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce – запускає програми один раз для поточного користувача, після запуску запис видаляється. [16]

В аудиті інформаційної безпеки треба перевіряти, щоб ці реєстри були пустими.

Висновки до розділу 2

У другому розділі було розглянуто можливості PowerShell для проведення аудиту інформаційної безпеки в середовищі Windows. PowerShell завдяки об'єктно-орієнтованій архітектурі та інтеграції з ОС Windows надає адміністраторам чудовий засіб для перевірки безпечності конфігурації системи. Іншими важливими перевагами цього інструменту є комплексність охоплення – можливість перевірити усі критично важливі аспекти безпеки системи, а також автоматизація процесів, що значно підвищує ефективність роботи адміністратора та зменшує шанс людської помилки.

Розглянуті засоби для проведення аудиту безпеки охоплюють такі аспекти безпеки системи:

- Перевірка політик безпеки, включаючи парольні політики, політики блокування облікових записів та привілеї користувачів
- Аналіз конфігурації Windows Firewall та активних правил фільтрації трафіку.
- Оцінка правильності налаштування прав доступу до файлів та каталогів.
- Контроль стану антивірусного захисту та системи SmartScreen.
- Моніторинг відкритих портів та активних служб.

3 ЗАСТОСУВАННЯ ЗАСОБІВ АУДИТУ БЕЗПЕКИ НА ОСНОВІ POWERSHELL

3.1 Архітектура застосунку

На основі критеріїв безпеки, описаних в розділі 1.3, та засобів, описаних в розділі 2.2, розробимо скрипт для автоматизації аудиту безпеки.

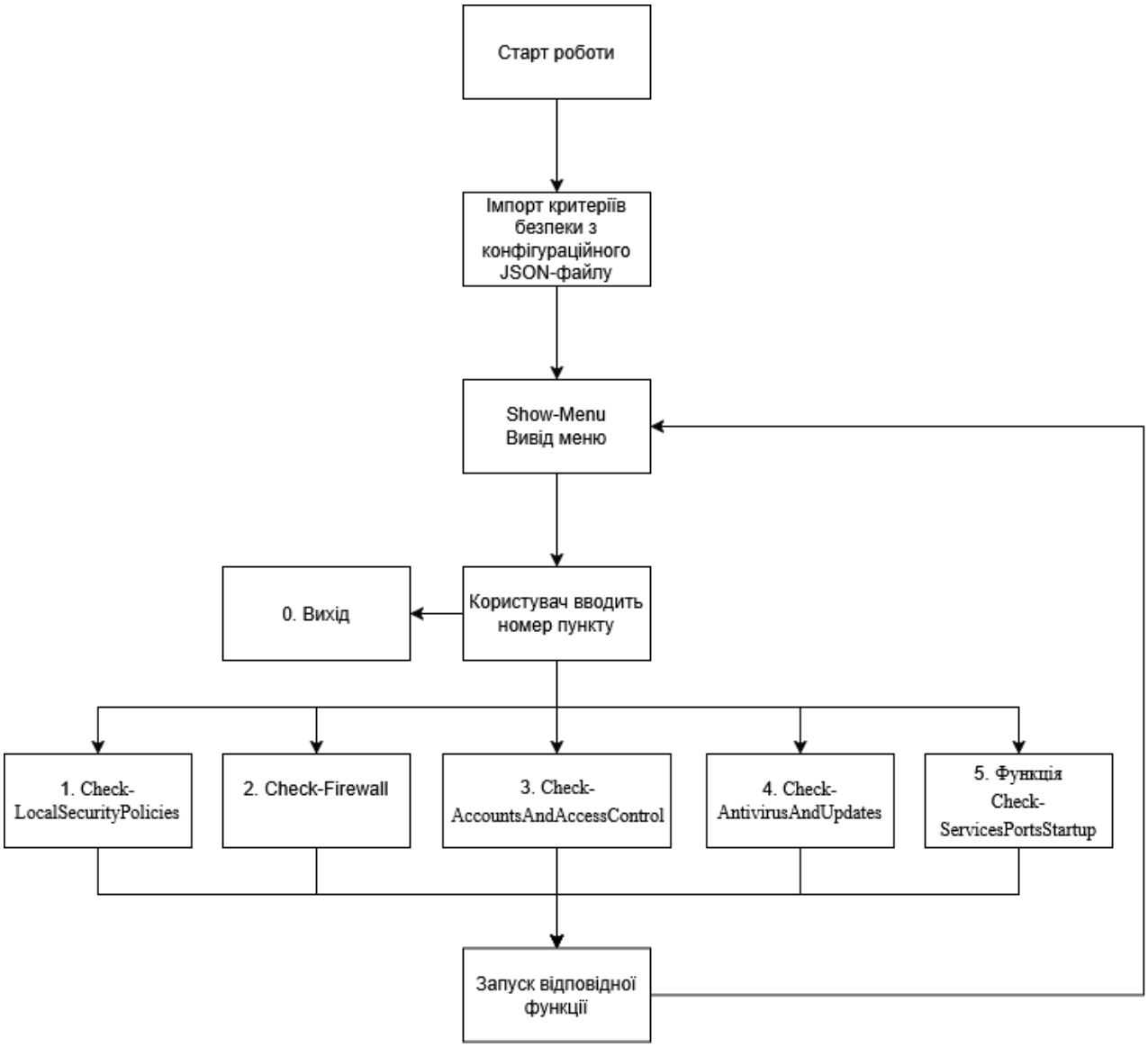

Рисунок 3.1 – Схема роботи програми для автоматизації аудиту безпеки

Як видно на схемі, робота програми полягає в координації основної функції меню роботи інших 5 функцій, що проводять автоматизований аудит безпеки:

- Check-LocalSecurityPolicies – проводить аналіз налаштувань локальних політик безпеки.
- Check-Firewall – виконує детальну перевірку стану Windows Defender Firewall для всіх мережевих профілів та перевіряє активні правила фільтрації трафіку.
- Check-AccountsAndAccessControl – функція для перевірки налаштувань прав доступу до файлової системи.
- Check-AntivirusAndUpdates – здійснює перевірку стану антивірусного програмного забезпечення та актуальність встановлених антивірусних сигнатур.
- Check-ServicesPortsStartup – функція для знаходження вразливих активних сервісів та відкритих портів.

Логіка роботи додатку полягає в тому, що користувачу дається вибір однієї з опцій аудиту. Після вибору користувачем певного конкретного напрямку, виконується відповідна функція. Далі за допомогою засобів PowerShell виконується збір інформації про стан системи. Ця інформація порівнюється з еталонними значеннями та результат перевірки виводиться у консоль у зрозумілому користувачу вигляді з виділенням проблем в налаштуваннях та рекомендаціями щодо їх усунення.

Структура звіту інструменту проста та зосереджена на наочності результатів перевірки. Звіт формується з категорії перевірки (брандмауер, контроль доступу, тощо) та статусу налаштування (еталон, відхилення). У консоль виводиться список перевірених налаштувань безпеки з їхніми поточними значеннями та

коротким коментарем щодо відповідності еталонному значенню. У випадку відповідності, рядок з підтвердженням правильності налаштування виведеться зеленим кольором. Інакше, якщо значення відхиляється від еталону, інструмент виводить відповідне повідомлення червоним кольором разом з інформацією стосовно того, яке налаштування є очікуваним. Такий формат виводу дуже інтуїтивно зрозумілий, дає загальне розуміння стану безпечності системи та допомагає прийняти рішення стосовно коригування конфігурації системи.

```
=== ПЕРЕВІРКА НАЛАШТУВАНЬ РЕЄСТРУ (POLICIES\SYSTEM) ===
DontDisplayLastUserName [0] — НЕ ВІДПОВІДАЄ! Очікується: 1
EnableLUA (UAC) [1] — OK
ConsentPromptBehaviorAdmin [5] — OK
InactivityTimeoutSecs [600] — OK
```

Рисунок 3.2 – Формат звіту

З ціллю зручності, масштабованості та зручності підтримки було прийнято рішення зберігати еталонні значення критеріїв безпеки в окремому JSON-файлі. Під час запуску користувач самостійно вводить шлях до цього файлу, після чого проводиться імпорт даних.

3.2 Автоматизація процесу аудиту

3.2.1 Структура головного меню

Було розроблено функцію, що реалізовувало інтерфейс консольного меню, в якому користувачу дається вибір з 5 основних напрямків перевірок: Local Security Policies, Windows Firewall, Облікові записи та контроль доступу, Антивірусний захист та оновлення, Порти служби та автозапуск. У разі

неправильного вводу від користувача з'являється повідомлення з проханням ввести правильне значення.

```
$exitScript = $false

function Show-Menu {
    Clear-Host
    Write-Host "Оберіть категорію аудиту безпеки Windows:`n"
    Write-Host "1. Local Security Policies"
    Write-Host "2. Windows Firewall"
    Write-Host "3. Облікові записи та контроль доступу"
    Write-Host "4. Антивірусний захист та оновлення"
    Write-Host "5. Порти, служби та автозапуск"
    Write-Host "0. Вийти"
}

do {
    Show-Menu
    $choice = Read-Host "Введіть номер пункту"
    switch ($choice) {
        '1' { Check-LocalSecurityPolicies }
        '2' { Check-Firewall }
        '3' { Check-AccountsAndAccessControl }
        '4' { Check-AntivirusAndUpdates }
        '5' { Check-ServicesPortsStartup }
        '0' {
            Write-Host "Вихід із скрипту..." -ForegroundColor Yellow
            $exitScript = $true
        }
        default { Write-Host "Невірний вибір. Спробуйте ще раз." -ForegroundColor Red }
    }

    if (-not $exitScript) {
        Write-Host "`nНатисніть Enter для продовження..."
        Read-Host
    }
} while (-not $exitScript)
```

Рисунок 3.3 – Код інтерфейсу

3.2.2 Імпорт критеріїв безпеки з конфігураційного JSON-файлу

В рамках розробки інструменту аудиту безпеки було вирішено зберігати конфігураційні дані у окремому JSON-файлі. Це допомагає розділити логіку самого додатку і дані, з якими він працює, що в свою чергу робить використання більш гнучким.

```
{
  "PasswordPolicies": {
    "PasswordHistorySize": 24,
    "MaximumPasswordAge": 60,
    "MinimumPasswordAge": 1,
    "MinimumPasswordLength": 14,
    "PasswordComplexity": 1,
    "ClearTextPassword": 0
  },

  "LockoutPolicies": {
    "LockoutBadCount": 10,
    "LockoutDuration": 15,
    "ResetLockoutCount": 15
  },

  "AccountPolicies": {
    "EnableAdminAccount": 0,
    "EnableGuestAccount": 0,
    "NewAdministratorName": "Administrator",
    "NewGuestName": "Guest"
  },

  "PrivilegeRights": {
    "SeRemoteInteractiveLogonRight": ["S-1-5-32-544", "S-1-5-32-555"],
    "SeSystemtimePrivilege": ["S-1-5-32-544", "S-1-5-19"],
    "SeTakeOwnershipPrivilege": ["S-1-5-32-544"],
    "SeSecurityPrivilege": ["S-1-5-32-544"],
    "SeDenyNetworkLogonRight": ["S-1-5-32-546", "S-1-2-0"],
    "SeLoadDriverPrivilege": ["S-1-5-32-544"],
    "SeServiceLogonRight": ["S-1-5-32-544"]
  },

  "BootSettings": {
    "TestSigning": "no"
  },

  "RegistrySettings": {
    "DontDisplayLastUserName": 1,
    "EnableLUA": 1,
    "ConsentPromptBehaviorAdmin": 5,
    "InactivityTimeoutSecs": 900
  },

  "LsaSettings": {
    "RestrictAnonymous": 1,
    "LimitBlankPasswordUse": 1
  },
```


Рисунок 3.4 – Конфігураційний JSON-файл

```
"AuditPolicy": {
  "Credential Validation": "Success and Failure",
  "Application Group Management": "Success and Failure",
  "Computer Account Management": "Success and Failure",
  "Other Account Management Events": "Success and Failure",
  "Security Group Management": "Success and Failure",
  "User Account Management": "Success and Failure",
  "Plug and Play Events": "Success",
  "Process Creation": "Success",
  "Account Lockout": "Success and Failure",
  "Group Membership": "Success",
  "Logoff": "Success",
  "Logon": "Success and Failure",
  "Other Logon/Logoff Events": "Success and Failure",
  "Special Logon": "Success",
  "Removable Storage": "Success and Failure",
  "Audit Policy Change": "Success and Failure",
  "Authentication Policy Change": "Success",
  "Authorization Policy Change": "Success",
  "Sensitive Privilege Use": "Success and Failure",
  "IPsec Driver": "Success and Failure",
  "Other System Events": "Success and Failure",
  "Security State Change": "Success",
  "Security System Extension": "Success and Failure",
  "System Integrity": "Success and Failure"
},
```

Рисунок 3.5 – Конфігураційний JSON-файл (продовження)

```
"FirewallSettings": {
  "Domain": {
      "Enabled": true,
      "DefaultInboundAction": "Block",
      "DefaultOutboundAction": "Allow",
      "AllowLocalFirewallRules": true,
      "AllowLocalIPsecRules": true,
      "LogFileName": "%SystemRoot%\\System32\\logfiles\\firewall\
        \domainfw.log",
      "LogAllowed": true,
      "LogBlocked": true,
      "LogFileSizeKB": 16384
  },
  "Private": {
      "Enabled": true,
      "DefaultInboundAction": "Block",
      "DefaultOutboundAction": "Allow",
      "AllowLocalFirewallRules": true,
      "AllowLocalIPsecRules": true,
      "LogFileName": "%SystemRoot%\\System32\\logfiles\\firewall\
        \privatefw.log",
      "LogAllowed": true,
      "LogBlocked": true,
      "LogFileSizeKB": 16384
  },
  "Public": {
      "Enabled": true,
      "DefaultInboundAction": "Block",
      "DefaultOutboundAction": "Allow",
      "AllowLocalFirewallRules": false,
      "AllowLocalIPsecRules": false,
      "LogFileName": "%SystemRoot%\\System32\\logfiles\\firewall\
        \publicfw.log",
      "LogAllowed": true,
      "LogBlocked": true,
      "LogFileSizeKB": 16384
  }
},
```

Рисунок 3.6 – Конфігураційний JSON-файл (продовження)

```
"FirewallRules": {
  "ICMPEchoRequest": "Block",
  "ICMPDestUnreachable": "Allow",
  "BlockedTunnelProtocols": ["6to4", "Teredo", "ISATAP"]
},

"DangerousPermissions": {
  "Registry": [
    "SetValue",
    "CreateSubKey",
    "WriteDac",
    "WriteOwner",
    "GenericWrite",
    "GenericAll",
    "Delete",
    "QueryValue",
    "EnumerateSubKeys"
  ],
  "File": [
    "WriteData",
    "AppendData",
    "WriteDac",
    "WriteOwner",
    "GenericWrite",
    "GenericAll",
    "Delete",
    "ReadData",
    "ReadAttributes",
    "ReadExtendedAttributes"
  ],
  "Folder": [
    "CreateFiles",
    "CreateDirectories",
    "DeleteSubdirectoriesAndFiles",
    "WriteDac",
    "GenericWrite",
    "GenericAll",
    "Delete",
    "ListDirectory",
    "ReadAttributes",
    "ReadExtendedAttributes"
  ]
},
```

Рисунок 3.7 – Конфігураційний JSON-файл (продовження)

```
  "Services": [
      "BthServ",
      "lfsvc",
      "icssvc",
      "Browser",
      "irmon",
      "FTPSVC",
      "xbgm"
  ],

  "VulnerablePorts": [21, 22, 23, 25, 53, 80, 137, 139, 1433, 1434, 3006, 3389,
    443, 8080, 8443, 445],
  "AutorunExpectedEmpty": true
}
```

Рисунок 3.8 – Конфігураційний JSON-файл (продовження)

Разом з цим була розроблена функція Load-ConfigFile, яка пропонує користувачеві ввести шлях до конфігураційного файлу та перевіряє правильність вводу. Функція в результаті зберігає зміст цього файлу в змінній, який має інформацію про еталонні значення критеріїв безпеки, які потім будуть використані функціями перевірок конфігурацій.

```
function Load-ConfigFile {
    do {
        $configPath = Read-Host "Введіть шлях до конфігураційного файлу (JSON)"
        if (Test-Path $configPath) {
            try {
                $config = Get-Content $configPath | ConvertFrom-Json
                Write-Host "[+] Конфігурація завантажена успішно!" -ForegroundColor Green
                return $config
            } catch {
                Write-Host "[-] Помилка при читанні файлу. Перевірте його формат!" -ForegroundColor Red
            }
        } else {
            Write-Host "[-] Файл не знайдено. Спробуйте ще раз!" -ForegroundColor Red
        }
    } while ($true)
}

$baseline = Load-ConfigFile
```

Рисунок 3.9 – функція Load-ConfigFile

3.2.3 Функція Check-LocalSecurityPolicies

Функція була реалізована для перевірки основних параметрів локальних політик безпеки. Вона робить експорт налаштувань політик до конфігураційного файлу та подальший аналіз цих значень, та перевірка значень з реєстру.

```
function Check-LocalSecurityPolicies {
    Write-Host "`n[+] Експорт локальних політик безпеки..." -ForegroundColor Cyan

    $exportPath = "C:\audit.txt"

    try {
        secedit /export /cfg $exportPath | Out-Null
        Write-Host "[+] Конфігурацію експортовано до $exportPath" -ForegroundColor Green
    } catch {
        Write-Host "[-] Помилка під час експорту конфігурації." -ForegroundColor Red
        return
    }

    #Отримання конфігурації
    $config = Get-Content $exportPath

    function Get-ConfigValue($param) {
        $line = $config | Where-Object { $_ -like "$param =*" }
        if ($line) {
            return ($line -split "=")[1].Trim()
        } else {
            return "NOT SET"
        }
    }

    function Check-Setting($name, $value, $expected, $comparison) {
        if ($value -eq "NOT SET") {
            $result = $false
        } else {
            switch ($comparison) {
                "ge" { $result = ([int]$value -ge [int]$expected) }
                "eq" { $result = ([int]$value -eq [int]$expected) }
                "le" { $result = ([int]$value -le [int]$expected) }
                default { $result = $false }
            }
        }

        if ($result) {
            Write-Host "$name [$value] - OK" -ForegroundColor Green
        } else {
            Write-Host "$name [$value] - НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
        }
    }

    function Translate-SIDToName($sid) {
        try {
            $obj = New-Object System.Security.Principal.SecurityIdentifier($sid)
            return $obj.Translate([System.Security.Principal.NTAccount]).Value
        } catch {
            return $sid
        }
    }

    function Check-PrivilegeRight($name, $expectedSids) {
    $line = $config | Where-Object { $_ -match "^\s*$name\s*=" }
    if (-not $line) {
        Write-Host "$name - НЕ ЗНАЙДЕНО!" -ForegroundColor Red
        return
    }

    $rawValue = ($line -split "=")[1].Trim()
    $rawSids = $rawValue.Split(",") | ForEach-Object { $_.Trim().TrimStart('*') }

    $translatedNames = $rawSids | ForEach-Object { Translate-SIDToName $_ }
    $expectedNames = $expectedSids | ForEach-Object {
        if ($_ -match "^S-1-") { Translate-SIDToName $_ } else { $_ }
    }

    Write-Host "`n${name}:"
    Write-Host "  Фактичні акаунти: $($translatedNames -join ', ')"
    Write-Host "  Очікувані акаунти: $($expectedNames -join ', ')"

    $diff = Compare-Object -ReferenceObject $expectedNames -DifferenceObject $translatedNames

    if ($diff) {
        Write-Host "  НЕ ВІДПОВІДАЄ!" -ForegroundColor Red
    } else {
        Write-Host "  OK." -ForegroundColor Green
    }
    }
```

Рисунок 3.10 – Функція Check-LocalSecurityPolicies

```
#Парольні політики
Write-Host "`n=== ПЕРЕВІРКА ПАРОЛЬНОЇ ПОЛІТИКИ ===" -ForegroundColor Cyan
Check-Setting "Історія паролів (PasswordHistorySize)" (Get-ConfigValue "PasswordHistorySize") $baseline.PasswordPolicies.PasswordHistorySize "ge"
Check-Setting "Максимальний вік паролю (MaximumPasswordAge)" (Get-ConfigValue "MaximumPasswordAge") $baseline.PasswordPolicies.MaximumPasswordAge "le"
Check-Setting "Мінімальний вік паролю (MinimumPasswordAge)" (Get-ConfigValue "MinimumPasswordAge") $baseline.PasswordPolicies.MinimumPasswordAge "ge"
Check-Setting "Мінімальна довжина паролю (MinimumPasswordLength)" (Get-ConfigValue "MinimumPasswordLength") $baseline.PasswordPolicies.MinimumPasswordLength "ge"
Check-Setting "Складність паролю (PasswordComplexity)" (Get-ConfigValue "PasswordComplexity") $baseline.PasswordPolicies.PasswordComplexity "eq"
Check-Setting "Зворотно зашифровані паролі (ClearTextPassword)" (Get-ConfigValue "ClearTextPassword") $baseline.PasswordPolicies.ClearTextPassword "eq"

Write-Host "`n=== ПЕРЕВІРКА ПОЛІТИКИ БЛОКУВАННЯ ===" -ForegroundColor Cyan
Check-Setting "Кількість невдалих спроб (LockoutBadCount)" (Get-ConfigValue "LockoutBadCount") $baseline.LockoutPolicies.LockoutBadCount "le"
Check-Setting "Тривалість блокування (LockoutDuration)" (Get-ConfigValue "LockoutDuration") $baseline.LockoutPolicies.LockoutDuration "ge"
Check-Setting "Обнулення лічильника (ResetLockoutCount)" (Get-ConfigValue "ResetLockoutCount") $baseline.LockoutPolicies.ResetLockoutCount "ge"

Write-Host "`n=== ПЕРЕВІРКА ОБЛІКОВИХ ЗАПИСІВ ===" -ForegroundColor Cyan
Check-Setting "Вбудований адміністратор (EnableAdminAccount)" (Get-ConfigValue "EnableAdminAccount") $baseline.AccountPolicies.EnableAdminAccount "eq"
Check-Setting "Вбудований гість (EnableGuestAccount)" (Get-ConfigValue "EnableGuestAccount") $baseline.AccountPolicies.EnableGuestAccount "eq"

Write-Host "`n=== ПЕРЕВІРКА НАЗВ ВБУДОВАНИХ ОБЛІКОВИХ ЗАПИСІВ ===" -ForegroundColor Cyan
$newAdminName = Get-ConfigValue "NewAdministratorName"
$newGuestName = Get-ConfigValue "NewGuestName"

if ($newAdminName -and $newAdminName -ne $baseline.AccountPolicies.NewAdministratorName) {
    Write-Host "NewAdministratorName [$newAdminName] - OK" -ForegroundColor Green
} else {
    Write-Host "NewAdministratorName [$newAdminName] - НЕ ВІДПОВІДАЄ! Має бути НЕ '$($baseline.AccountPolicies.NewAdministratorName)'." -ForegroundColor Red
}

if ($newGuestName -and $newGuestName -ne $baseline.AccountPolicies.NewGuestName) {
    Write-Host "NewGuestName [$newGuestName] - OK" -ForegroundColor Green
} else {
    Write-Host "NewGuestName [$newGuestName] - НЕ ВІДПОВІДАЄ! Має бути НЕ '$($baseline.AccountPolicies.NewGuestName)'." -ForegroundColor Red
}

Write-Host "`n=== ПЕРЕВІРКА ПРАВ ПРИВІЛЕІВ ===" -ForegroundColor Cyan

foreach ($privilege in $baseline.PrivilegeRights.PSObject.Properties.Name) {
    Check-PrivilegeRight $privilege $baseline.PrivilegeRights.$privilege
}

Write-Host "`n=== ПЕРЕВІРКА РЕЖИМУ ЗАВАНТАЖЕННЯ НЕПІДПИСАНИХ ДРАЙВЕРІВ ===" -ForegroundColor Cyan

try {
    $bcdOutput = bcdedit | Select-String -Pattern "testsigning"
    $expectedValue = $baseline.BootSettings.TestSigning

    if ($bcdOutput) {
        if ($bcdOutput -match $expectedValue) {
            Write-Host "Testsigning [$bcdOutput] - OK" -ForegroundColor Green
        } else {
            Write-Host "Testsigning [$bcdOutput] - НЕ ВІДПОВІДАЄ! Очікується: $expectedValue" -ForegroundColor Red
        }
    } else {
        Write-Host "Testsigning відсутній - за замовчуванням ВИМКНЕНО." -ForegroundColor Yellow
    }
} catch {
    Write-Host "[-] Не вдалося виконати перевірку параметра Testsigning." -ForegroundColor Red
}

Write-Host "`n=== ПЕРЕВІРКА НАЛАШТУВАНЬ РЕЄСТРУ (POLICIES\SYSTEM) ===" -ForegroundColor Cyan
```

Рисунок 3.11 – Функція Check-LocalSecurityPolicies (продовження)

```
Write-Host "`n=== ПЕРЕВІРКА НАЛАШТУВАНЬ РЕЄСТРУ (POLICIES\SYSTEM) ===" -ForegroundColor Cyan

try {
    $regPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
    $regValues = Get-ItemProperty -Path $regPath

    function Check-RegistrySetting($name, $actual, $expected, $condition = "equal") {
        if ($condition -eq "eq" -and $actual -eq $expected) {
            Write-Host "$name [$actual] - OK" -ForegroundColor Green
        } elseif ($condition -eq "le" -and $actual -lt $expected -and $actual -ne 0) {
            Write-Host "$name [$actual] - OK" -ForegroundColor Green
        } else {
            Write-Host "$name [$actual] - НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
        }
    }

    Check-RegistrySetting "DontDisplayLastUserName" $regValues.DontDisplayLastUserName $baseline.RegistrySettings.DontDisplayLastUserName "eq"
    Check-RegistrySetting "EnableLUA (UAC)" $regValues.EnableLUA $baseline.RegistrySettings.EnableLUA "eq"
    Check-RegistrySetting "ConsentPromptBehaviorAdmin" $regValues.ConsentPromptBehaviorAdmin $baseline.RegistrySettings.ConsentPromptBehaviorAdmin "eq"
    Check-RegistrySetting "InactivityTimeoutSecs" $regValues.InactivityTimeoutSecs $baseline.RegistrySettings.InactivityTimeoutSecs "le"

    Write-Host "`n=== Перевірка попереджувального повідомлення ===" -ForegroundColor Cyan

    $caption = $regValues.LegalNoticeCaption
    $text = $regValues.LegalNoticeText

    if ($caption) {
        Write-Host "LegalNoticeCaption: [$caption]" -ForegroundColor Green
    } else {
        Write-Host "LegalNoticeCaption - ВІДСУТНЄ!" -ForegroundColor Red
    }

    if ($text) {
        Write-Host "LegalNoticeText: [$text]" -ForegroundColor Green
    } else {
        Write-Host "LegalNoticeText - ВІДСУТНЄ!" -ForegroundColor Red
    }
}
catch {
    Write-Host "[-] Не вдалося прочитати ключі реєстру $regPath" -ForegroundColor Red
}

Write-Host "`n=== ПЕРЕВІРКА ПОЛІТИКИ МЕРЕЖЕВОЇ БЕЗПЕКИ (LSA) ===" -ForegroundColor Cyan

try {
    $lsaPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
    $lsaValues = Get-ItemProperty -Path $lsaPath

    function Check-LsaSetting($name, $actual, $expected) {
        if ($actual -eq $expected) {
            Write-Host "$name [$actual] - OK" -ForegroundColor Green
        } else {
            Write-Host "$name [$actual] - НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
        }
    }

    Check-LsaSetting "RestrictAnonymous" $lsaValues.RestrictAnonymous $baseline.LsaSettings.RestrictAnonymous
    Check-LsaSetting "LimitBlankPasswordUse" $lsaValues.LimitBlankPasswordUse $baseline.LsaSettings.LimitBlankPasswordUse
    }
catch {
    Write-Host "[-] Не вдалося прочитати ключі реєстру $lsaPath" -ForegroundColor Red
}
```

Рисунок 3.12 – Функція Check-LocalSecurityPolicies (продовження)

```
    #Налаштування аудиту

    function Check-AuditSubcategory($subcategoryName, $expectedSetting, $displayName) {
    $line = $auditLines | Where-Object { $_ -match "^\s*$subcategoryName\s{2,}" }
    if (-not $line) {
        Write-Host "$displayName - НЕ ЗНАЙДЕНО!" -ForegroundColor Red
        return
    }

    $columns = $line -split '\s{2,}'
    $setting = $columns[-1].Trim()

    if ($setting -eq $expectedSetting) {
        Write-Host "$displayName [$setting] - OK" -ForegroundColor Green
    } else {
        Write-Host "$displayName [$setting] - НЕ ВІДПОВІДАЄ! Очікується: $expectedSetting" -ForegroundColor Red
    }
    }


    Write-Host "`n=== ПЕРЕВІРКА AUDIT POLICY ===" -ForegroundColor Cyan

    $auditSettings = auditpol /get /category:* | Out-String
    $auditLines = $auditSettings -split "`r?`n"

    foreach ($subcategory in $baseline.AuditPolicy.PSObject.Properties.Name) {
        $expected = $baseline.AuditPolicy.$subcategory
        Check-AuditSubcategory $subcategory $expected "Перевірка Audit '$subcategory'"
    }

    Write-Host "`nАналіз завершено.`n" -ForegroundColor Cyan

}
```

Рисунок 3.13 – Функція Check-LocalSecurityPolicies (продовження)

3.2.4 Функція Check-Firewall

Дана функція робить здійснює перевірку налаштувань брандмауера Windows включаючи статус захисту для різних мережевих профілів та аналіз правил фільтрації трафіку.

```
function Check-Firewall {
    Write-Host "`n=== ПЕРЕВІРКА БРАНДМАУЕРА ===" -ForegroundColor Cyan

    $profiles = Get-NetFirewallProfile

    foreach ($profile in $profiles) {
        $name = $profile.Name
        Write-Host ""
        Write-Host "=== Профіль: $name ===" -ForegroundColor Cyan

        if ($baseline.FirewallSettings.$name) {
            $expected = $baseline.FirewallSettings.$name
        } else {
            Write-Host "Не знайдено конфігурацію для профілю $name! Перевірте baseline.json" -ForegroundColor Yellow
            continue
        }

        function Compare-Setting($desc, $actual, $expected) {
            if ($actual -eq $expected) {
                Write-Host "$desc [$actual] - OK" -ForegroundColor Green
            } else {
                Write-Host "$desc - НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
            }
        }

        # Основні налаштування
        Compare-Setting "Стан брандмауера (Enabled)" $profile.Enabled $expected.Enabled
        Compare-Setting "Вхідні з'єднання (DefaultInboundAction)" $profile.DefaultInboundAction $expected.DefaultInboundAction
        Compare-Setting "Вихідні з'єднання (DefaultOutboundAction)" $profile.DefaultOutboundAction $expected.DefaultOutboundAction
        Compare-Setting "Застосування локальних правил брандмауера (AllowLocalFirewallRules)" $profile.AllowLocalFirewallRules $expected.AllowLocalFirewallRules
        Compare-Setting "Застосування локальних IPsec-правил (AllowLocalIPsecRules)" $profile.AllowLocalIPsecRules $expected.AllowLocalIPsecRules

        # Журналювання
        Compare-Setting "Шлях до файлу логу" $profile.LogFileName $expected.LogFileName
        Compare-Setting "Журналювання дозволених з'єднань" $profile.LogAllowed $expected.LogAllowed
        Compare-Setting "Журналювання заблокованих з'єднань" $profile.LogBlocked $expected.LogBlocked

        if ($profile.LogMaxSizeKilobytes -ge $expected.LogFileSizeKB) {
            Write-Host "Максимальний розмір файлу журналу [$($profile.LogMaxSizeKilobytes) KB] - OK" -ForegroundColor Green
        } else {
            Write-Host "Максимальний розмір файлу журналу [$($profile.LogMaxSizeKilobytes) KB] - НЕ ВІДПОВІДАЄ! Очікується: не менше $($expected.LogFileSizeKB) KB" -ForegroundColor Red
        }
    }

    Write-Host "`n=== АКТИВНІ ПРОТОКОЛИ ТА ПОРТИ У ВВІМКНЕНИХ ПРАВИЛАХ ===" -ForegroundColor Cyan

    $expectedFirewallRules = $baseline.FirewallRules

    $activeIpSecRules = Get-NetIPsecRule | Where-Object { $_.Enabled -eq $true }
    if ($activeIpSecRules) {
        Write-Host "Активні правила IPsec (повинні бути відсутні):" -ForegroundColor Red
        $activeIpSecRules | Format-Table Name, Enabled, Action, Direction
    } else {
        Write-Host "Активних правил IPsec нема - OK" -ForegroundColor Green
    }
```

Рисунок 3.14 – Функція Check-Firewall

```
    # ICMP Echo Request
    $icmpEchoInboundAllowed = Get-NetFirewallRule -Direction Inbound | Where-Object {
        $_.Enabled -eq $true -and
        $_.Action -eq $expectedFirewallRules.ICMPEchoRequest -and
        ($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and
        $_.Name -match "EchoRequest|ERQ"
    }

    Write-Host "`n=== Вхідний ICMP Echo Request ===" -ForegroundColor Cyan
    if ($icmpEchoInboundAllowed) {
        Write-Host "Вхідний ICMP Echo Request [$($expectedFirewallRules.ICMPEchoRequest)] - OK" -ForegroundColor Green
    } else {
        Write-Host "Вхідний ICMP Echo Request - НЕ ВІДПОВІДАЄ! Очікується: $($expectedFirewallRules.ICMPEchoRequest)" -ForegroundColor Red
    }

    # ICMP Destination Unreachable
    $icmpDestUnreachAllowed = Get-NetFirewallRule -Direction Inbound | Where-Object {
        $_.Enabled -eq $true -and
        $_.Action -eq $expectedFirewallRules.ICMPDestUnreachable -and
        ($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and
        ($_.Name -match "DU|DestinationUnreachable")
    }

    Write-Host "`n=== Вхідні ICMP Destination Unreachable ===" -ForegroundColor Cyan
    if ($icmpDestUnreachAllowed) {
        Write-Host "Вхідні ICMP Destination Unreachable [$($expectedFirewallRules.ICMPDestUnreachable)] - OK" -ForegroundColor Green
    } else {
        Write-Host "Вхідні ICMP Destination Unreachable - НЕ ВІДПОВІДАЄ! Очікується: $($expectedFirewallRules.ICMPDestUnreachable)" -ForegroundColor Red
    }

    Write-Host "`n=== ПЕРЕВІРКА БЛОКУВАННЯ ТУНЕЛЬНИХ ПРОТОКОЛІВ (6to4, Teredo, ISATAP) ===" -ForegroundColor Cyan

    foreach ($proto in $baseline.FirewallRules.BlockedTunnelProtocols) {
        $rule = Get-NetFirewallRule -Enabled True | Where-Object {
            $_.Direction -eq "Inbound" -and
            $_.Action -eq "Block" -and
            $_.DisplayName -match $proto
        }

        if ($rule) {
            Write-Host "Правило блокування $proto знайдено - OK" -ForegroundColor Green
        } else {
            Write-Host "Правило блокування $proto ВІДСУТНЄ! Очікується: Block" -ForegroundColor Red
        }
    }

    Write-Host "`nПеревірка брандмауера завершена.`n" -ForegroundColor Cyan
}
```

Рисунок 3.15 – Функція Check-Firewall (продовження)

3.2.5 Фукнція Check-AccountsAndAccessControl

Функція для перевірки налаштувань контролю доступу до системних ресурсів.

```
function Check-AccountsAndAccessControl {
    Write-Host "`n=== Аудит контролю доступу ===" -ForegroundColor Cyan

    Write-Host "`n=== Моніторинг часу останнього входу ===" -ForegroundColor Cyan

    $users = Get-LocalUser | Where-Object { $_.Enabled -eq $true }

    foreach ($user in $users) {
        Write-Host "$($user.Name) - Останній логін: $($user.LastLogon)" -ForegroundColor Yellow
    }

    Write-Host "`n=== Виявлення неактивних облікових записів ===" -ForegroundColor Cyan

    $inactiveUsers = Get-LocalUser | Where-Object { $_.Enabled -eq $true -and $_.LastLogon -lt (Get-Date).AddDays(-90) }

    if ($inactiveUsers) {
        Write-Host "Неактивні облікові записи виявлено!" -ForegroundColor Red
        $inactiveUsers | Format-Table Name, LastLogon -AutoSize
    } else {
        Write-Host "Неактивних облікових записів не виявлено." -ForegroundColor Green
    }

    Write-Host "`n=== Перевірка членства користувачів у групі адміністраторів ===" -ForegroundColor Cyan

    $adminUsers = Get-LocalGroupMember -Group "Administrators"

    if ($adminUsers) {
        Write-Host "Список користувачів у групі адміністраторів:" -ForegroundColor Yellow
        $adminUsers | Format-Table Name, ObjectClass -AutoSize
    } else {
        Write-Host "Група адміністраторів порожня!" -ForegroundColor Red
    }

    Write-Host "`n=== Перевірка тимчасових та службових акаунтів ===" -ForegroundColor Cyan

    $temporaryAccounts = Get-LocalUser | Where-Object { $_.Name -match "temp|test|guest|install" }

    if ($temporaryAccounts) {
        Write-Host "Виявлено тимчасові акаунти!" -ForegroundColor Yellow
        $temporaryAccounts | Format-Table Name, Enabled -AutoSize
    } else {
        Write-Host "Тимчасових акаунтів не виявлено." -ForegroundColor Green
    }

    #Введення шляху користувачем
    $PathToCheck = Read-Host "`nВведіть шлях до об'єкта (файл, директорія або ключ реєстру), який потрібно перевірити"

    if (-not (Test-Path $PathToCheck)) {
        Write-Host "Помилка: вказаний шлях не існує." -ForegroundColor Red
        exit
    }

    Write-Host "`n=== Перевірка прав доступу ===" -ForegroundColor Cyan

    $expectedPermissions = $baseline.DangerousPermissions

    #Визначення типу об'єкта
    $objectType = if ((Get-Item $PathToCheck).PSIsContainer) { "Folder" } else { "File" }
    if ($PathToCheck -match "^HKLM|HKCU|HKCR|HKU|HKCC") { $objectType = "Registry" }

    Write-Host "`nПеревірка прав доступу для об'єкта типу: $objectType" -ForegroundColor Cyan
```

Рисунок 3.16 – Функція Check-AccountsAndAccessControl

```
#Аналіз прав доступу відповідно до типу
try {
    $acl = Get-Acl -Path $PathToCheck -ErrorAction Stop
    $dangerousRights = $expectedPermissions.$objectType

    foreach ($ace in $acl.Access) {
        $identity = $ace.IdentityReference.Value
        $rights = $ace.FileSystemRights.ToString()

        foreach ($dangerousRight in $dangerousRights) {
            if ($rights -match $dangerousRight) {
                Write-Host "`nПотенційно небезпечне право виявлено!" -ForegroundColor Red
                Write-Host "Об'єкт: $PathToCheck" -ForegroundColor Yellow
                Write-Host "Користувач/Група: $identity" -ForegroundColor Yellow
                Write-Host "Права доступу: $rights" -ForegroundColor Yellow
                Write-Host "----------------------------------------"
            }
        }
    }
} catch {
    Write-Host "[-] Не вдалося отримати ACL для $PathToCheck" -ForegroundColor Yellow
}
```

Рисунок 3.17 – Функція Check-AccountsAndAccessControl (продовження)

```
#Отримання шляху до перевірки від користувача
$DirToCheck = Read-Host "Введіть шлях до директорії, яку потрібно перевірити"
if (-not (Test-Path $DirToCheck)) {
    Write-Host "Помилка: вказаний шлях не існує." -ForegroundColor Red
    return
}

$RootPath = "C:\"

#Права напряму користувачам
Write-Host "`n=== Перевірка прав, наданих безпосередньо користувачам ===" -ForegroundColor Cyan
$directUserAccess = Get-ChildItem -Path $DirToCheck -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
    try {
        $acl = Get-Acl $_.FullName -ErrorAction Stop
        foreach ($ace in $acl.Access) {
            $identity = $ace.IdentityReference.Value
            $sid = ([System.Security.Principal.NTAccount]$identity).Translate([System.Security.Principal.SecurityIdentifier])
            if ($sid.Value -match "^S-1-5-21") {
                [PSCustomObject]@{
                    FilePath = $_.FullName
                    User     = $identity
                    Rights   = $ace.FileSystemRights
                }
            }
        }
    } catch {}
}

if ($directUserAccess) {
    Write-Host "Прямі права користувачам виявлено" -ForegroundColor Red
    $directUserAccess | Format-Table -AutoSize
} else {
    Write-Host "Прямих прав користувачам не виявлено" -ForegroundColor Green
}

#Створення файлів у кореневому каталозі
Write-Host "`n=== Перевірка прав створення файлів/каталогів у кореневому каталозі ===" -ForegroundColor Cyan
$rootAcl = Get-Acl -Path $RootPath
$unwantedRootRights = @()

foreach ($ace in $rootAcl.Access) {
    $identity = $ace.IdentityReference.Value
    $rights = $ace.FileSystemRights.ToString()

    if ($rights -match "CreateDirectories|Modify|FullControl") {
        if ($identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
            $unwantedRootRights += [PSCustomObject]@{
                UserOrGroup = $identity
                Rights      = $rights
                Path        = $RootPath
            }
        }
    }
}

if ($unwantedRootRights.Count -gt 0) {
    Write-Host "Небажані права створення в кореневому каталозі виявлено" -ForegroundColor Red
    $unwantedRootRights | Format-Table -AutoSize
} else {
    Write-Host "Небажаних прав створення в кореневому каталозі не виявлено." -ForegroundColor Green
}
```

Рисунок 3.18 – Функція Check-AccountsAndAccessControl (продовження)

```
    #Наявність Full Control
    Write-Host "`n=== Перевірка наявності небезпечних прав Full Control ===" -ForegroundColor Cyan
    $fullControlIssues = Get-ChildItem -Path $DirToCheck -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
        try {
            $acl = Get-Acl $_.FullName -ErrorAction Stop
            foreach ($ace in $acl.Access) {
                $identity = $ace.IdentityReference.Value
                $rights = $ace.FileSystemRights.ToString()

                if ($rights -match "FullControl" -and
                    $identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
                    [PSCustomObject]@{
                        FilePath = $_.FullName
                        User     = $identity
                        Rights   = $ace.FileSystemRights
                    }
                }
            }
        } catch {}
    }

    if ($fullControlIssues) {
        Write-Host "Файли з небезпечними правами Full Control виявлено" -ForegroundColor Red
        $fullControlIssues | Format-Table -AutoSize
    } else {
        Write-Host "Файлів з небезпечними правами Full Control не виявлено." -ForegroundColor Green
    }

    Write-Host "`nАудит завершено." -ForegroundColor Cyan
}
```

Рисунок 3.19 – Функція Check-AccountsAndAccessControl (продовження)

3.2.6 Функція Check-AntivirusAndUpdates

Функція здійснює моніторинг стану антивірусного захисту системи, перевіряє актуальність антивірусних баз даних та статус системних оновлень Windows.

```
function Check-AntivirusAndUpdates {
    Write-Host "`n=== ПЕРЕВІРКА АНТИВІРУСНОГО ЗАХИСТУ ТА ОНОВЛЕНЬ WINDOWS DEFENDER ===" -ForegroundColor Cyan

    $expected = $baseline.AntivirusSettings
    $mpPrefs = Get-MpPreference

    function Compare-Setting($desc, $actual, $expected) {
        if ($actual -eq $expected) {
            Write-Host "$desc [$actual] — OK" -ForegroundColor Green
        } else {
            Write-Host "$desc [$actual] — НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
        }
    }

    Compare-Setting "PUAProtection" $mpPrefs.PUAProtection $expected.PUAProtection
    Compare-Setting "Сканування в реальному часі" $mpPrefs.DisableRealtimeMonitoring $expected.DisableRealtimeMonitoring

    try {
        $ss = Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System"
        Compare-Setting "SmartScreen" $ss.EnableSmartScreen $expected.EnableSmartScreen
        Compare-Setting "SmartScreen PreventOverride" $ss.PreventOverride $expected.PreventOverride
    } catch {
        Write-Host "SmartScreen — НЕ ВІДПОВІДАЄ! Не вдалося зчитати налаштування з реєстру" -ForegroundColor Red
    }

    # Перевірка актуальності сигнатур
    $status = Get-MpComputerStatus
    $now = Get-Date
    $avDelta = ($now - $status.AntivirusSignatureLastUpdated).Days
    $asDelta = ($now - $status.AntispywareSignatureLastUpdated).Days

    if ($avDelta -le $expected.MaxSignatureAgeDays) {
        Write-Host "Антивірусні сигнатури [$($status.AntivirusSignatureLastUpdated)] — OK" -ForegroundColor Green
    } else {
        Write-Host "Антивірусні сигнатури [$($status.AntivirusSignatureLastUpdated)] — НЕ ВІДПОВІДАЮТЬ! Оновлено $avDelta дн. тому" -ForegroundColor Red
    }

    if ($asDelta -le $expected.MaxSignatureAgeDays) {
        Write-Host "Антишпигунські сигнатури [$($status.AntispywareSignatureLastUpdated)] — OK" -ForegroundColor Green
    } else {
        Write-Host "Антишпигунські сигнатури [$($status.AntispywareSignatureLastUpdated)] — НЕ ВІДПОВІДАЮТЬ! Оновлено $asDelta дн. тому" -ForegroundColor Red
    }
}
```

Рисунок 3.20 – Функція Check-AntivirusAndUpdates

3.2.7 Функція Check-ServicesPortsStartup

Функція аналізує активні мережеві порти та стан системних служб, виявляючи потенційні загрози безпеці.

```
function Check-ServicesPortsStartup {
    Write-Host "`n=== Перевірка служб, портів та автозапуску ===" -ForegroundColor Cyan

    $blockedServices = $baseline.Services
    $expectedPorts = $baseline.VulnerablePorts
    $expectedAutorunStatus = $baseline.AutorunExpectedEmpty

    Write-Host "`n=== Перевірка служб ===" -ForegroundColor Cyan

    foreach ($serviceName in $blockedServices) {
        $service = Get-Service -Name $serviceName -ErrorAction SilentlyContinue

        if ($service) {
            if ($service.Status -eq 'Stopped') {
                Write-Host "$serviceName - Disabled - OK" -ForegroundColor Green
            } else {
                Write-Host "$serviceName - Enabled! Очікується: Disabled" -ForegroundColor Red
            }
        } else {
            Write-Host "$serviceName - НЕ ЗНАЙДЕНО (можливо відсутній у системі)" -ForegroundColor Yellow
        }
    }


    #Перевірка портів
    Write-Host "`n=== Перевірка відкритих портів ===" -ForegroundColor Cyan
    $netstatOutput = netstat -ano | Select-String "LISTENING"
    $openVulnerablePorts = @()

    foreach ($port in $expectedPorts) {
        if ($netstatOutput -match "[:\.]$port\s") {
            $openVulnerablePorts += $port
        }
    }

    if ($openVulnerablePorts.Count -eq 0) {
        Write-Host "Потенційно вразливі порти не відкриті - OK" -ForegroundColor Green
    } else {
        Write-Host "ВІДКРИТІ потенційно вразливі порти: $($openVulnerablePorts -join ', ')" -ForegroundColor Yellow
    }
```

Рисунок 3.21 – Функція Check-ServicesPortsStartup

```
    #Перевірка автозапуску
    Write-Host "`n=== Перевірка автозапуску ===" -ForegroundColor Cyan
    $runKeys = @(
        "HKLM:\Software\Microsoft\Windows\CurrentVersion\Run",
        "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce",
        "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run",
        "HKCU:\Software\Microsoft\Windows\CurrentVersion\RunOnce"
    )

    $hasAutorunEntries = $false

    foreach ($key in $runKeys) {
        try {
            $values = Get-ItemProperty -Path $key -ErrorAction Stop
            $props = $values.PSObject.Properties | Where-Object {
                $_.Name -notmatch "^PS"
            }

            if ($props.Count -gt 0) {
                Write-Host "Знайдено записи в $key" -ForegroundColor Red
                foreach ($entry in $props) {
                    Write-Host " - $($entry.Name): $($entry.Value)" -ForegroundColor Yellow
                }
                $hasAutorunEntries = $true
            }
        } catch {}
    }

    if ($expectedAutorunStatus -and (-not $hasAutorunEntries)) {
        Write-Host "Автозапуск вимкнений - OK" -ForegroundColor Green
    }
}
```

Рисунок 3.22 – Функція Check-ServicesPortsStartup (продовження)

3.3 Результати тестування розроблених засобів аудиту

Для перевірки функціональності розробленого засобу було проведено його тестування на операційній системі Windows 10. Тестування полягало в перевірці роботи п’яти основних функцій та їх взаємодії з системними компонентами.

```
PS C:\Users\lab3m\Desktop> .\1.ps1
Введіть шлях до конфігураційного файлу (JSON): C:\Users\lab3m\Desktop\baseline.json
```

Рисунок 3.23 – Ввід шляху до конфігураційного JSON-файлу

Спочатку користувачу треба ввести шлях до конфігураційного JSON-файлу, в якому зберігаються еталонні значення.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту:
```

Рисунок 3.24 – Інтерфейс консольного меню

Перевірка інтерфейсу користувача показала справну роботу консольного меню. Функція показує інформацію щодо п’яти основних напрямів аудиту.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту: 9
Невірний вибір. Спробуйте ще раз.

Натисніть Enter для продовження...
```

Рисунок 3.25 – Реакція на неправильний ввід користувача

Система правильно реагує на неправильний вхідні данні користувача – при неочікуваному вводі виводиться відповідне повідомлення.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту: 1

[+] Експорт локальних політик безпеки...
[+] Конфігурацію експортовано до C:\audit.txt

=== ПЕРЕВІРКА ПАРОЛЬНОЇ ПОЛІТИКИ ===
Історія паролів (PasswordHistorySize) [0] — НЕ ВІДПОВІДАЄ! Очікується: 24
Максимальний вік паролю (MaximumPasswordAge) [42] — OK
Мінімальний вік паролю (MinimumPasswordAge) [0] — НЕ ВІДПОВІДАЄ! Очікується: 1
Мінімальна довжина паролю (MinimumPasswordLength) [0] — НЕ ВІДПОВІДАЄ! Очікується: 14
Складність паролю (PasswordComplexity) [0] — НЕ ВІДПОВІДАЄ! Очікується: 1
Зворотно зашифровані паролі (ClearTextPassword) [0] — OK

=== ПЕРЕВІРКА ПОЛІТИКИ БЛОКУВАННЯ ===
Кількість невдалих спроб (LockoutBadCount) [0] — OK
Тривалість блокування (LockoutDuration) [NOT SET] — НЕ ВІДПОВІДАЄ! Очікується: 15
Обнулення лічильника (ResetLockoutCount) [NOT SET] — НЕ ВІДПОВІДАЄ! Очікується: 15

=== ПЕРЕВІРКА ОБЛІКОВИХ ЗАПИСІВ ===
Вбудований адміністратор (EnableAdminAccount) [0] — OK
Вбудований гість (EnableGuestAccount) [0] — OK

=== ПЕРЕВІРКА НАЗВ ВБУДОВАНИХ ОБЛІКОВИХ ЗАПИСІВ ===
NewAdministratorName ["Administrator"] — OK
NewGuestName ["Guest"] — OK

=== ПЕРЕВІРКА ПРАВ ПРИВІЛЕЇВ ===

SeRemoteInteractiveLogonRight:
  Фактичні акаунти: BUILTIN\Administrators, BUILTIN\Remote Desktop Users
  Очікувані акаунти: BUILTIN\Administrators, BUILTIN\Remote Desktop Users
  OK.

SeSystemtimePrivilege:
  Фактичні акаунти: NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators
  Очікувані акаунти: BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
  OK.

SeTakeOwnershipPrivilege:
  Фактичні акаунти: BUILTIN\Administrators
  Очікувані акаунти: BUILTIN\Administrators
  OK.

SeSecurityPrivilege:
  Фактичні акаунти: BUILTIN\Administrators
  Очікувані акаунти: BUILTIN\Administrators
  OK.

SeDenyNetworkLogonRight:
  Фактичні акаунти: Guest
  Очікувані акаунти: BUILTIN\Guests, LOCAL
  НЕ ВІДПОВІДАЄ!

SeLoadDriverPrivilege:
  Фактичні акаунти: BUILTIN\Administrators
  Очікувані акаунти: BUILTIN\Administrators
  OK.

SeServiceLogonRight:
  Фактичні акаунти: NT SERVICE\ALL SERVICES
  Очікувані акаунти: BUILTIN\Administrators
  НЕ ВІДПОВІДАЄ!
```

Рисунок 3.26 – Вивід функції Check-LocalSecurityPolicies

```
=== ПЕРЕВІРКА РЕЖИМУ ЗАВАНТАЖЕННЯ НЕПІДПИСАНИХ ДРАЙВЕРІВ ===
Testsigning [testsigning             No] — OK

=== ПЕРЕВІРКА НАЛАШТУВАНЬ РЕЄСТРУ (POLICIES\SYSTEM) ===
DontDisplayLastUserName [0] — НЕ ВІДПОВІДАЄ! Очікується: 1
EnableLUA (UAC) [1] — OK
ConsentPromptBehaviorAdmin [5] — OK
InactivityTimeoutSecs [600] — OK

=== Перевірка попереджувального повідомлення ===
LegalNoticeCaption — ВІДСУТНЄ!
LegalNoticeText: []

=== ПЕРЕВІРКА ПОЛІТИКИ МЕРЕЖЕВОЇ БЕЗПЕКИ (LSA) ===
RestrictAnonymous [0] — НЕ ВІДПОВІДАЄ! Очікується: 1
LimitBlankPasswordUse [1] — OK

=== ПЕРЕВІРКА AUDIT POLICY ===
Перевірка Audit 'Credential Validation' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Application Group Management' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Computer Account Management' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Other Account Management Events' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Fail
Перевірка Audit 'Security Group Management' [Success] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'User Account Management' [Success] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Plug and Play Events' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success
Перевірка Audit 'Process Creation' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success
Перевірка Audit 'Account Lockout' [Success] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Group Membership' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success
Перевірка Audit 'Logoff' [Success] — OK
Перевірка Audit 'Logon' [Success and Failure] — OK
Перевірка Audit 'Other Logon/Logoff Events' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Special Logon' [Success] — OK
Перевірка Audit 'Removable Storage' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Audit Policy Change' [Success] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Authentication Policy Change' [Success] — OK
Перевірка Audit 'Authorization Policy Change' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success
Перевірка Audit 'Sensitive Privilege Use' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'IPsec Driver' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'Other System Events' [Success and Failure] — OK
Перевірка Audit 'Security State Change' [Success] — OK
Перевірка Audit 'Security System Extension' [No Auditing] — НЕ ВІДПОВІДАЄ! Очікується: Success and Failure
Перевірка Audit 'System Integrity' [Success and Failure] — OK

Аналіз завершено.


Натисніть Enter для продовження...
```

Рисунок 3.27 – Вивід функції Check-LocalSecurityPolicies (продовження)

Функція Check-LocalSecurityPolicies успішно виконує експорт налаштувань локальних політик безпеки до тимчасового конфігураційного файлу, дістає потрібні значення з реєстрів та коректно аналізує ключові параметри безпеки, вказуючи на відповідність критеріям безпеки.

На виводу функції видно, що в моїй системі найбільше відхилень у парольних політик та політик блокування облікових записів. Також доволі погана

ситуація стосовно налаштувань вбудованого аудиту безпеки, оскільки велика кількість важливих категорій аудиту просто не ведуться. В моїй системі також відсутнє налаштування попереджувального повідомлення, виводиться інформація стосовно останнього залогіненого користувача, дозволено анонімне підключення до іменованих каналів, що створює потенційні вразливості для системи.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту: 2

=== ПЕРЕВІРКА БРАНДМАУЕРА ===

=== Профіль: Domain ===
Стан брандмауера (Enabled) [True] — OK
Вхідні з'єднання (DefaultInboundAction) — НЕ ВІДПОВІДАЄ! Очікується: Block
Вихідні з'єднання (DefaultOutboundAction) — НЕ ВІДПОВІДАЄ! Очікується: Allow
Застосування локальних правил брандмауера (AllowLocalFirewallRules) [True] — OK
Застосування локальних IPsec-правил (AllowLocalIPsecRules) [True] — OK
Шлях до файлу логу — НЕ ВІДПОВІДАЄ! Очікується: %SystemRoot%\System32\logfiles\firewall\domainfw.log
Журналювання дозволених з'єднань — НЕ ВІДПОВІДАЄ! Очікується: True
Журналювання заблокованих з'єднань [True] — OK
Максимальний розмір файлу журналу [4096 KB] — НЕ ВІДПОВІДАЄ! Очікується: не менше 16384 KB

=== Профіль: Private ===
Стан брандмауера (Enabled) [True] — OK
Вхідні з'єднання (DefaultInboundAction) — НЕ ВІДПОВІДАЄ! Очікується: Block
Вихідні з'єднання (DefaultOutboundAction) — НЕ ВІДПОВІДАЄ! Очікується: Allow
Застосування локальних правил брандмауера (AllowLocalFirewallRules) — НЕ ВІДПОВІДАЄ! Очікується: True
Застосування локальних IPsec-правил (AllowLocalIPsecRules) — НЕ ВІДПОВІДАЄ! Очікується: True
Шлях до файлу логу — НЕ ВІДПОВІДАЄ! Очікується: %SystemRoot%\System32\logfiles\firewall\privatefw.log
Журналювання дозволених з'єднань [True] — OK
Журналювання заблокованих з'єднань — НЕ ВІДПОВІДАЄ! Очікується: True
Максимальний розмір файлу журналу [16384 KB] — OK

=== Профіль: Public ===
Стан брандмауера (Enabled) [True] — OK
Вхідні з'єднання (DefaultInboundAction) — НЕ ВІДПОВІДАЄ! Очікується: Block
Вихідні з'єднання (DefaultOutboundAction) — НЕ ВІДПОВІДАЄ! Очікується: Allow
Застосування локальних правил брандмауера (AllowLocalFirewallRules) [False] — OK
Застосування локальних IPsec-правил (AllowLocalIPsecRules) [False] — OK
Шлях до файлу логу — НЕ ВІДПОВІДАЄ! Очікується: %SystemRoot%\System32\logfiles\firewall\publicfw.log
Журналювання дозволених з'єднань [True] — OK
Журналювання заблокованих з'єднань [True] — OK
Максимальний розмір файлу журналу [16384 KB] — OK

=== АКТИВНІ ПРОТОКОЛИ ТА ПОРТИ У ВВІМКНЕНИХ ПРАВИЛАХ ===
Активних правил IPsec нема — OK

=== Вхідний ICMP Echo Request ===
Вхідний ICMP Echo Request — НЕ ВІДПОВІДАЄ! Очікується: Block

=== Вхідні ICMP Destination Unreachable ===
Вхідні ICMP Destination Unreachable [Allow] — OK

=== ПЕРЕВІРКА БЛОКУВАННЯ ТУНЕЛЬНИХ ПРОТОКОЛІВ (6to4, Teredo, ISATAP) ===
Правило блокування 6to4 ВІДСУТНЄ! Очікується: Block
Правило блокування Teredo ВІДСУТНЄ! Очікується: Block
Правило блокування ISATAP ВІДСУТНЄ! Очікується: Block

Перевірка брандмауера завершена.


Натисніть Enter для продовження...
```

Рисунок 3.28 – Вивід функції Check-Firewall

Функція Check-Firewall продемонструвала високу ефективність у перевірці стану Windows Defender Firewall для кожного з профілів, вказуючи на правильність налаштування різних аспектів. Функція також показала можливість перевірки активних мережних правил фільтрації трафіку. Функція успішно відображає детальну інформацію про налаштування брандмауера у структурованому вигляді.

В моїй системі є критичне відхилення стосовно налаштувань брандмауера – усі профілі брандмауера некоректно налаштовані стосовно дозволу на вхідні та вихідні з’єднання. У випадку вихідних з’єднань це не є критичним, в той час як неправильне налаштування вхідних з’єднань створює критичні загрози для системи, збільшуючи ризик несанкціонованого віддаленого доступу до комп’ютера. Іншим відхиленням є відсутність правила, що блокує вхідні ICMP Echo Request трафік, що може призвести до DoS/DDoS атаки чи скануванню топології мережі зловмисником. Також в нашій системі відсутні правила блокування 6to4, Teredo, ISATAP трафіку. Ці протоколи дозволяють інкапсуляцію IPv6-пакетів у IPv4 та можуть бути використані для обходу існуючих фільтрів безпеки.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту: 3

=== Аудит контролю доступу ===

=== Моніторинг часу останнього входу ===
user1 — Останній логін:
user2 — Останній логін: 06/13/2025 20:45:25

=== Виявлення неактивних облікових записів ===
Неактивні облікові записи виявлено!

Name  LastLogon
----  ---------
user1



=== Перевірка членства користувачів у групі адміністраторів ===
Список користувачів у групі адміністраторів:

Name                          ObjectClass
----                          -----------
DESKTOP-U5DQAB1\Administrator User
DESKTOP-U5DQAB1\user2         User



=== Перевірка тимчасових та службових акаунтів ===
Виявлено тимчасові акаунти!

Name  Enabled
----  -------
Guest   False
```

Рисунок 3.29 – Вивід функції Check-AccountsAndAccessControl

```
Введіть шлях до об'єкта (файл, директорія або ключ реєстру), який потрібно перевірити: C:\Users\Public

=== Перевірка прав доступу ===

Перевірка прав доступу для об'єкта типу: Folder

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\BATCH
Права доступу: DeleteSubdirectoriesAndFiles, Modify, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\BATCH
Права доступу: DeleteSubdirectoriesAndFiles, Modify, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\BATCH
Права доступу: CreateFiles, AppendData, ReadAndExecute, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\INTERACTIVE
Права доступу: DeleteSubdirectoriesAndFiles, Modify, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\INTERACTIVE
Права доступу: DeleteSubdirectoriesAndFiles, Modify, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\INTERACTIVE
Права доступу: CreateFiles, AppendData, ReadAndExecute, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\SERVICE
Права доступу: CreateFiles, AppendData, ReadAndExecute, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\SERVICE
Права доступу: DeleteSubdirectoriesAndFiles, Modify, Synchronize
----------------------------------------

Потенційно небезпечне право виявлено!
Об'єкт: C:\Users\Public
Користувач/Група: NT AUTHORITY\SERVICE
Права доступу: DeleteSubdirectoriesAndFiles, Modify, Synchronize
----------------------------------------
```

Рисунок 3.30 – Вивід функції Check-AccountsAndAccessControl (продовження)

```
Введіть шлях до директорії, яку потрібно перевірити: C:\Users\Public

=== Перевірка прав, наданих безпосередньо користувачам ===
Прямі права користувачам виявлено

FilePath                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                User
--------                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
C:\Users\Public\AccountPictures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Desktop                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Documents                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Downloads                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Libraries                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Music                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Pictures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Videos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\1.txt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\1.txt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\desktop.ini                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\desktop.ini                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image1080.jpg DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image192.jpg  DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image208.jpg  DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image240.jpg  DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image32.jpg   DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image40.jpg   DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image424.jpg  DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image448.jpg  DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image48.jpg   DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image64.jpg   DESKTOP-U5DQAB1...
C:\Users\Public\AccountPictures\S-1-5-21-1777076922-1185462647-3778723286-1001\{C62893DE-7005-44A2-904A-EDC86BEB193C}-Image96.jpg   DESKTOP-U5DQAB1...
C:\Users\Public\Desktop\Microsoft Edge.lnk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Documents\tets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Documents\tets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DESKTOP-U5DQAB1...
C:\Users\Public\Documents\tets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Desktop-U5DQAB1...


=== Перевірка прав створення файлів/каталогів у кореневому каталозі ===
Небажаних прав створення в кореневому каталозі не виявлено.
```

Рисунок 3.31 – Вивід функції Check-AccountsAndAccessControl (продовження)

```
=== Перевірка наявності небезпечних прав Full Control ===
Файли з небезпечними правами Full Control виявлено

FilePath                                                
```

наданих прав доступу до папки C:\Users\Public, ці записи слід уважно перевірити на те, чи не надано надлишкові права неочікуваним та недовіреним користувачам. Далі виводиться інформація про некоректне надання прав користувачам напряму, що є поганою практикою в менеджменті контролю доступу. Такі записи бажано видаляти та в майбутньому давати права доступу саме групі користувачів. Інструмент потім виводить інформацію про права на модифікацію змісту кореневого каталогу недовіреним користувачам. В моїй системі нема відхилень від еталону в цьому критерії.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту: 4

=== ПЕРЕВІРКА АНТИВІРУСНОГО ЗАХИСТУ ТА ОНОВЛЕНЬ WINDOWS DEFENDER ===
PUAProtection [0] — НЕ ВІДПОВІДАЄ! Очікується: 1
Сканування в реальному часі [False] — OK
SmartScreen [] — НЕ ВІДПОВІДАЄ! Очікується: 1
SmartScreen PreventOverride [] — НЕ ВІДПОВІДАЄ! Очікується: 1
Антивірусні сигнатури [06/13/2025 16:24:06] — OK
Антишпигунські сигнатури [06/13/2025 16:24:06] — OK

Натисніть Enter для продовження...
```

Рисунок 3.33 – Вивід функції Check-AntivirusAndUpdates

Функція Check-AntivirusAndUpdates продемонстрував надійну роботу в перевірці стану систем антивірусного захисту. Було перевірено правильність налаштування сканування в реальному часі, SmartScreen та антивірусних і антишпигунських сигнатур.

Під час перевірки антивірусного захисту було помічено ряд відхилень від критеріїв безпеки. В моїй системі нема PUA, що захищає від запуску небажаних додатків, що може створювати ризики для безпеки. Також нема правильного налаштування SmartScreen, що збільшує ризик використання шкідливого програмного забезпечення, фішингу та інших загроз.

```
Оберіть категорію аудиту безпеки Windows:

1. Local Security Policies
2. Windows Firewall
3. Облікові записи та контроль доступу
4. Антивірусний захист та оновлення
5. Порти, служби та автозапуск
0. Вийти
Введіть номер пункту: 5

=== Перевірка служб, портів та автозапуску ===

=== Перевірка служб ===
BthServ — Disabled — OK
lfsvc — Enabled! Очікується: Disabled
icssvc — Disabled — OK
Browser — Enabled! Очікується: Disabled
irmon — НЕ ЗНАЙДЕНО (можливо відсутній у системі)
FTPSVC — НЕ ЗНАЙДЕНО (можливо відсутній у системі)
xbgm — НЕ ЗНАЙДЕНО (можливо відсутній у системі)

=== Перевірка відкритих портів ===
ВІДКРИТІ потенційно вразливі порти: 139, 445

=== Перевірка автозапуску ===
Знайдено записи в HKLM:\Software\Microsoft\Windows\CurrentVersion\Run
 - SecurityHealth: C:\Windows\system32\SecurityHealthSystray.exe
 - VBoxTray: C:\Windows\system32\VBoxTray.exe
Знайдено записи в HKCU:\Software\Microsoft\Windows\CurrentVersion\Run
 - OneDrive: "C:\Users\lab3m\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

Натисніть Enter для продовження...
```

Рисунок 3.34 – Вивід функції Check-ServicesPortsStartup

Функція Check-ServicesPortsStartup успішно виконала перевірку наявності вразливих активних сервісів та відкритих портів.

Інформація, отримана в результаті виконання цієї функції, свідчить про потенційні ризики. В системі присутні активні сервіси геолокації (lfsvc) та computer browser (Browser) – це є відхиленням від стандартів безпеки, такі сервіси

слід відключити. Також в моїй системі є відкриті 139 та 445 порти, що відовідає NetBIOS over TCP та SMB сервісам. У випадку, якщо їх робота не є очікуваною, то відповідні порти слід закрити. Також були помічені записи в автозапуску. У випадку моєї системи, програми, що запускаються з автозапуску, є безпечними, але загалом автозапуск є популярним способом запуску шкідливого програмного забезпечення, тому його слід регулярно перевіряти.

Висновки до розділу 3

В процесі розробки та тестування засобу автоматизації аудиту безпеки Windows було розроблено структуру застосунку на основі п’яти функцій, що координуються через консольне меню, кожна з яких відповідає за один з основних напрямків перевірок аудиту: локальні політики безпеки, Windows Firewall, система контролю доступу, антивірусний захист та оновлення, служби та порти. В ході роботи проведено тестування розробленого застосунку на системі Windows 10, в результаті якого було перевірено справність та точність роботи разом зі зручністю використання.

ВИСНОВКИ

В процесі дипломного проектування було успішно виконано поставлені задачі шляхом вивчення теоретичних основ та практичних методів проведення аудиту інформаційної безпеки в середовищі Windows з використанням технології PowerShell. Розроблено новий інструмент для автоматизованої перевірки системи безпеки.

Дослідження охопило ключові компоненти захисту систем на основі Windows: локальні політики безпеки, конфігурацію брандмауера, система контролю доступу, системи антивірусного захисту, а також контроль мережевих портів та програм автозавантаження. Результатом стала розробка автоматизованої системи аудиту на основі PowerShell, здатної ідентифікувати порушення стандартів безпечної конфігурації.

Практичні результати включають структурований набір команд PowerShell для всебічної оцінки системної безпеки та функціональний інструмент.

Розроблений інструмент демонструє системний підхід до аудиту безпеки завдяки врахуванню великої кількості аспектів безпеки та інтегруванню широкого спектру безпекових критеріїв. Серед інших переваг цього засобу є простота експлуатації, на відміну від засобів як SCAP чи OpenSCAP, які потребують складного налаштування та завантаження додаткового програмного забезпечення, що робить розроблений засіб кращим вибором для систем, де використання стороннього програмного забезпечення є небажаним.

Наукова цінність роботи полягає в практичній реалізації комплексного підходу до аудиту інформаційної безпеки систем Windows засобами PowerShell, що раніше не мало системного наукового обґрунтування.

Напрямки подальшого розвитку проекту є:

- Інтеграція з SIEM системами для покращення моніторингу безпеки.
- Розробка веб-інтерфейсу для спрощення взаємодії з розробленою системою аудиту.

Створений засіб може дієво використовуватися в корпоративному секторі на підприємствах різного масштабу для проведення бюджетного внутрішнього аудиту безпеки без залучення зовнішніх консультантів, у освітній сфері з метою демонстрації практичного застосування скриптових технологій у сфері інформаційної безпеки, та державному секторі для проведення попередньої оцінки рівня захищеності системи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. 6 Types of Security Audits (Електронний ресурс) // Спосіб доступу: URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/types-of-security-audits/

2. CIS Microsoft Windows 10 Enterprise (Release 1703) Benchmark (Електронний ресурс) // Спосіб доступу: URL: https://community.mis.temple.edu/mis5170sec001sec701sp2018/files/2018/02/CIS_Microsoft_Windows_10_Enterprise_Release_1703_Benchmark_v1.3.0.pdf

3. Gray Hat Hacking, The Ethical Hacker's Handbook (Електронний ресурс) // Спосіб доступу: URL: https://pages.cs.wisc.edu/~ace/media/gray-hat-hacking.pdf

4. Identifying Common Open Port Vulnerabilities in Your Network (Електронний ресурс) // Спосіб доступу: URL: https://blog.netwrix.com/open-ports-vulnerability-list

5. Microsoft Learn: about_Execution_Policies (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.5

6. Microsoft Learn: auditpol (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol

7. Microsoft Learn: bcdedit (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/bcdedit

8. Microsoft Learn: Chapter 1 - Getting started with PowerShell (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/scripting/learn/ps101/01-getting-started?view=powershell-7.5

9. Microsoft Learn: Defender (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/module/defender/?view=windowsserver2025-ps

10. Microsoft Learn: Get-Acl (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/ru-ru/powershell/module/microsoft.powershell.security/get-acl?view=powershell-7.5

11. Microsoft Learn: Get-LocalGroupMember (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/get-localgroupmember?view=powershell-5.1&viewFallbackFrom=powershell-7.5

12. Microsoft Learn: Get-LocalUser Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/get-localuser?view=powershell-5.1&viewFallbackFrom=powershell-7.5

13. Microsoft Learn: Get-Service (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-service?view=powershell-7.5

14. Microsoft Learn: NetSecurity (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/module/netsecurity/?view=windowsserver2025-ps

15. Microsoft Learn: netstat (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

16. Microsoft Learn: Run and RunOnce Registry Keys (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys

17. Microsoft Learn: secedit commands (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/secedit

18. Microsoft Learn: User Rights Assignment (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/user-rights-assignment

19. Microsoft Learn: What is PowerShell? (Електронний ресурс) // Спосіб доступу: URL: https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.5

20. NIST Special Publication 800-41 Revision 1 (Електронний ресурс) // Спосіб доступу: URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

21. NIST Special Publication 800-53 Revision 5 (Електронний ресурс) // Спосіб доступу: URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

22. NTFS Permissions Management Best Practices and Guide (Електронний ресурс) // Спосіб доступу: URL: https://www.lepide.com/blog/ntfs-permissions-management-guide-and-best-practices/

23. Security Audits: A Comprehensive Overview (Електронний ресурс) // Спосіб доступу: URL: https://auditboard.com/blog/what-is-security-audit/

24. Wikipedia: Windows Firewall (Електронний ресурс) // Спосіб доступу: URL: https://en.wikipedia.org/wiki/Windows_Firewall

ДОДАТОК А ЗАСІБ ДЛЯ АВТОМАТИЗАЦІЇ АУДИТУ

```
function Check-LocalSecurityPolicies {
    Write-Host "`n[+] Експорт локальних політик безпеки..." -ForegroundColor Cyan

    $exportPath = "C:\audit.txt"

    try {
        secedit /export /cfg $exportPath | Out-Null
        Write-Host "[+] Конфігурацію експортовано до $exportPath" -ForegroundColor Green
    } catch {
        Write-Host "[-] Помилка під час експорту конфігурації." -ForegroundColor Red
        return
    }

    #Отримання конфігурації
    $config = Get-Content $exportPath

    function Get-ConfigValue($param) {
```

```
    $line = $config | Where-Object { $_ -like "$param =*" }
    if ($line) {
        return ($line -split "=")[1].Trim()
    } else {
        return "NOT SET"
    }
}

function Check-Setting($name, $value, $expected, $comparison) {
    if ($value -eq "NOT SET") {
        $result = $false
    } else {
        switch ($comparison) {
            "ge" { $result = ([int]$value -ge [int]$expected) }
            "eq" { $result = ([int]$value -eq [int]$expected) }
            "le" { $result = ([int]$value -le [int]$expected) }
            default { $result = $false }
        }
    }

    if ($result) {
```

```
        Write-Host "$name [$value] — OK" -ForegroundColor Green
    } else {
        Write-Host "$name [$value] — НЕ ВІДПОВІДАЄ! Очікується: $expected" -
ForegroundColor Red
    }
}

function Translate-SIDToName($sid) {
    try {
        $obj = New-Object System.Security.Principal.SecurityIdentifier($sid)
        return $obj.Translate([System.Security.Principal.NTAccount]).Value
    } catch {
        return $sid
    }
}

function Check-PrivilegeRight($name, $expectedSids) {
$line = $config | Where-Object { $_ -match "^\s*$name\s*=" }
if (-not $line) {
    Write-Host "$name — НЕ ЗНАЙДЕНО!" -ForegroundColor Red
    return
```

```
    }

    $rawValue = ($line -split "=")[1].Trim()
    $rawSids = $rawValue.Split(",") | ForEach-Object { $_.Trim().TrimStart('*') }

    $translatedNames = $rawSids | ForEach-Object { Translate-SIDToName $_ }
    $expectedNames = $expectedSids | ForEach-Object {
        if ($_ -match "^S-1-") { Translate-SIDToName $_ } else { $_ }
    }

    Write-Host "`n${name}:"
    Write-Host "  Фактичні акаунти: $($translatedNames -join ', ')"
    Write-Host "  Очікувані акаунти: $($expectedNames -join ', ')"

    $diff = Compare-Object -ReferenceObject $expectedNames -DifferenceObject
$translatedNames

    if ($diff) {
        Write-Host "  НЕ ВІДПОВІДАЄ!" -ForegroundColor Red
    } else {
        Write-Host "  ОК." -ForegroundColor Green
```

```
}
}

#Парольні політики
Write-Host "`n=== ПЕРЕВІРКА ПАРОЛЬНОЇ ПОЛІТИКИ ===" -ForegroundColor Cyan
Check-Setting "Історія паролів (PasswordHistorySize)" (Get-ConfigValue "PasswordHistorySize") $baseline.PasswordPolicies.PasswordHistorySize "ge"
Check-Setting "Максимальний вік паролю (MaximumPasswordAge)" (Get-ConfigValue "MaximumPasswordAge") $baseline.PasswordPolicies.MaximumPasswordAge "le"
Check-Setting "Мінімальний вік паролю (MinimumPasswordAge)" (Get-ConfigValue "MinimumPasswordAge") $baseline.PasswordPolicies.MinimumPasswordAge "ge"
Check-Setting "Мінімальна довжина паролю (MinimumPasswordLength)" (Get-ConfigValue "MinimumPasswordLength") $baseline.PasswordPolicies.MinimumPasswordLength "ge"
Check-Setting "Складність паролю (PasswordComplexity)" (Get-ConfigValue "PasswordComplexity") $baseline.PasswordPolicies.PasswordComplexity "eq"
Check-Setting "Зворотно зашифровані паролі (ClearTextPassword)" (Get-ConfigValue "ClearTextPassword") $baseline.PasswordPolicies.ClearTextPassword "eq"
```

```
Write-Host "`n=== ПЕРЕВІРКА ПОЛІТИКИ БЛОКУВАННЯ ===" -ForegroundColor Cyan

Check-Setting "Кількість невдалих спроб (LockoutBadCount)" (Get-ConfigValue "LockoutBadCount") $baseline.LockoutPolicies.LockoutBadCount "le"

Check-Setting "Тривалість блокування (LockoutDuration)" (Get-ConfigValue "LockoutDuration") $baseline.LockoutPolicies.LockoutDuration "ge"

Check-Setting "Обнулення лічильника (ResetLockoutCount)" (Get-ConfigValue "ResetLockoutCount") $baseline.LockoutPolicies.ResetLockoutCount "ge"


Write-Host "`n=== ПЕРЕВІРКА ОБЛІКОВИХ ЗАПИСІВ ===" -ForegroundColor Cyan

Check-Setting "Вбудований адміністратор (EnableAdminAccount)" (Get-ConfigValue "EnableAdminAccount") $baseline.AccountPolicies.EnableAdminAccount "eq"

Check-Setting "Вбудований гість (EnableGuestAccount)" (Get-ConfigValue "EnableGuestAccount") $baseline.AccountPolicies.EnableGuestAccount "eq"


Write-Host "`n=== ПЕРЕВІРКА НАЗВ ВБУДОВАНИХ ОБЛІКОВИХ ЗАПИСІВ ===" -ForegroundColor Cyan

$newAdminName = Get-ConfigValue "NewAdministratorName"

$newGuestName = Get-ConfigValue "NewGuestName"
```

```
if ($newAdminName -and $newAdminName -ne $baseline.AccountPolicies.NewAdministratorName) {
    Write-Host "NewAdministratorName [$newAdminName] — OK" -ForegroundColor Green
} else {
    Write-Host "NewAdministratorName [$newAdminName] — НЕ ВІДПОВІДАЄ! Має бути НЕ '$($baseline.AccountPolicies.NewAdministratorName)'." -ForegroundColor Red
}

if ($newGuestName -and $newGuestName -ne $baseline.AccountPolicies.NewGuestName) {
    Write-Host "NewGuestName [$newGuestName] — OK" -ForegroundColor Green
} else {
    Write-Host "NewGuestName [$newGuestName] — НЕ ВІДПОВІДАЄ! Має бути НЕ '$($baseline.AccountPolicies.NewGuestName)'." -ForegroundColor Red
}

Write-Host "`n=== ПЕРЕВІРКА ПРАВ ПРИВІЛЕЇВ ===" -ForegroundColor Cyan

foreach ($privilege in $baseline.PrivilegeRights.PSObject.Properties.Name) {
```

```
        Check-PrivilegeRight $privilege $baseline.PrivilegeRights.$privilege
    }

    Write-Host "`n=== ПЕРЕВІРКА РЕЖИМУ ЗАВАНТАЖЕННЯ НЕПІДПИСАНИХ ДРАЙВЕРІВ ===" -ForegroundColor Cyan

    try {
        $bcdOutput = bcdedit | Select-String -Pattern "testsigning"
        $expectedValue = $baseline.BootSettings.TestSigning

        if ($bcdOutput) {
            if ($bcdOutput -match $expectedValue) {
                Write-Host "Testsigning [$bcdOutput] — OK" -ForegroundColor Green
            } else {
                Write-Host "Testsigning [$bcdOutput] — НЕ ВІДПОВІДАЄ! Очікується: $expectedValue" -ForegroundColor Red
            }
        } else {
            Write-Host "Testsigning відсутній — за замовчуванням ВИМКНЕНО." -ForegroundColor Yellow
        }
    } catch {
```

```
    Write-Host "[-] Не вдалося виконати перевірку параметра Testsigning." -ForegroundColor Red
  }

  Write-Host "`n=== ПЕРЕВІРКА НАЛАШТУВАНЬ РЕЄСТРУ (POLICIES\SYSTEM) ===" -ForegroundColor Cyan

  try {
    $regPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
    $regValues = Get-ItemProperty -Path $regPath

    function Check-RegistrySetting($name, $actual, $expected, $condition = "equal") {
      if ($condition -eq "eq" -and $actual -eq $expected) {
        Write-Host "$name [$actual] — OK" -ForegroundColor Green
      } elseif ($condition -eq "le" -and $actual -lt $expected -and $actual -ne 0) {
        Write-Host "$name [$actual] — OK" -ForegroundColor Green
      } else {
        Write-Host "$name [$actual] — НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
      }
```

```
}

Check-RegistrySetting "DontDisplayLastUserName" $regValues.DontDisplayLastUserName $baseline.RegistrySettings.DontDisplayLastUserName "eq"
Check-RegistrySetting "EnableLUA (UAC)" $regValues.EnableLUA $baseline.RegistrySettings.EnableLUA "eq"
Check-RegistrySetting "ConsentPromptBehaviorAdmin" $regValues.ConsentPromptBehaviorAdmin $baseline.RegistrySettings.ConsentPromptBehaviorAdmin "eq"
Check-RegistrySetting "InactivityTimeoutSecs" $regValues.InactivityTimeoutSecs $baseline.RegistrySettings.InactivityTimeoutSecs "le"

Write-Host "`n=== Перевірка попереджувального повідомлення ===" -ForegroundColor Cyan

$caption = $regValues.LegalNoticeCaption
$text = $regValues.LegalNoticeText

if ($caption) {
    Write-Host "LegalNoticeCaption: [$caption]" -ForegroundColor Green
} else {
```

```
        Write-Host "LegalNoticeCaption — ВІДСУТНЄ!" -ForegroundColor Red
    }

    if ($text) {
        Write-Host "LegalNoticeText: [$text]" -ForegroundColor Green
    } else {
        Write-Host "LegalNoticeText — ВІДСУТНЄ!" -ForegroundColor Red
    }
}
catch {
    Write-Host "[-] Не вдалося прочитати ключі реєстру $regPath" -ForegroundColor Red
}

Write-Host "`n=== ПЕРЕВІРКА ПОЛІТИКИ МЕРЕЖЕВОЇ БЕЗПЕКИ (LSA) ===" -ForegroundColor Cyan

try {
    $lsaPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
    $lsaValues = Get-ItemProperty -Path $lsaPath
```

```
    function Check-LsaSetting($name, $actual, $expected) {
        if ($actual -eq $expected) {
            Write-Host "$name [$actual] — OK" -ForegroundColor Green
        } else {
            Write-Host "$name [$actual] — НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
        }
    }

    Check-LsaSetting "RestrictAnonymous" $lsaValues.RestrictAnonymous $baseline.LsaSettings.RestrictAnonymous
    Check-LsaSetting "LimitBlankPasswordUse" $lsaValues.LimitBlankPasswordUse $baseline.LsaSettings.LimitBlankPasswordUse
    }
  catch {
    Write-Host "[-] Не вдалося прочитати ключі реєстру $lsaPath" -ForegroundColor Red
  }

  #Налаштування аудиту
```

```
function Check-AuditSubcategory($subcategoryName, $expectedSetting, $displayName) {
    $line = $auditLines | Where-Object { $_ -match "^\s*$subcategoryName\s{2,}" }
    if (-not $line) {
        Write-Host "$displayName — НЕ ЗНАЙДЕНО!" -ForegroundColor Red
        return
    }

    $columns = $line -split '\s{2,}'
    $setting = $columns[-1].Trim()

    if ($setting -eq $expectedSetting) {
        Write-Host "$displayName [$setting] — OK" -ForegroundColor Green
    } else {
        Write-Host "$displayName [$setting] — НЕ ВІДПОВІДАЄ! Очікується: $expectedSetting" -ForegroundColor Red
    }
}



Write-Host "`n=== ПЕРЕВІРКА AUDIT POLICY ===" -ForegroundColor Cyan
```

```
    $auditSettings = auditpol /get /category:* | Out-String
    $auditLines = $auditSettings -split "`r?`n"

    foreach ($subcategory in $baseline.AuditPolicy.PSObject.Properties.Name) {
        $expected = $baseline.AuditPolicy.$subcategory
        Check-AuditSubcategory $subcategory $expected "Перевірка Audit '$subcategory'"
    }

    Write-Host "`nАналіз завершено.`n" -ForegroundColor Cyan

}

function Check-Firewall {
    Write-Host "`n=== ПЕРЕВІРКА БРАНДМАУЕРА ===" -ForegroundColor Cyan

    $profiles = Get-NetFirewallProfile

    foreach ($profile in $profiles) {
        $name = $profile.Name
```

```
Write-Host ""
Write-Host "=== Профіль: $name ===" -ForegroundColor Cyan

if ($baseline.FirewallSettings.$name) {
    $expected = $baseline.FirewallSettings.$name
} else {
    Write-Host "Не знайдено конфігурацію для профілю $name! Перевірте baseline.json" -ForegroundColor Yellow
    continue
}

function Compare-Setting($desc, $actual, $expected) {
    if ($actual -eq $expected) {
        Write-Host "$desc [$actual] — OK" -ForegroundColor Green
    } else {
        Write-Host "$desc — НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
    }
}

# Основні налаштування
```

```
Compare-Setting "Стан брандмауера (Enabled)" $profile.Enabled $expected.Enabled

Compare-Setting "Вхідні з’єднання (DefaultInboundAction)" $profile.DefaultInboundAction $expected.DefaultInboundAction

Compare-Setting "Вихідні з’єднання (DefaultOutboundAction)" $profile.DefaultOutboundAction $expected.DefaultOutboundAction

Compare-Setting "Застосування локальних правил брандмауера (AllowLocalFirewallRules)" $profile.AllowLocalFirewallRules $expected.AllowLocalFirewallRules

Compare-Setting "Застосування локальних IPsec-правил (AllowLocalIPsecRules)" $profile.AllowLocalIPsecRules $expected.AllowLocalIPsecRules


# Журналювання

Compare-Setting "Шлях до файлу логу" $profile.LogFileName $expected.LogFileName

Compare-Setting "Журналювання дозволених з’єднань" $profile.LogAllowed $expected.LogAllowed

Compare-Setting "Журналювання заблокованих з’єднань" $profile.LogBlocked $expected.LogBlocked


if ($profile.LogMaxSizeKilobytes -ge $expected.LogFileSizeKB) {

  Write-Host "Максимальний розмір файлу журналу [$($profile.LogMaxSizeKilobytes) KB] — OK" -ForegroundColor Green
```

```
    } else {
        Write-Host "Максимальний розмір файлу журналу [$($profile.LogMaxSizeKilobytes) KB] — НЕ ВІДПОВІДАЄ! Очікується: не менше $($expected.LogFileSizeKB) KB" -ForegroundColor Red
    }
}

Write-Host "`n=== АКТИВНІ ПРОТОКОЛИ ТА ПОРТИ У ВВІМКНЕНИХ ПРАВИЛАХ ===" -ForegroundColor Cyan

$expectedFirewallRules = $baseline.FirewallRules

$activeIpSecRules = Get-NetIPsecRule | Where-Object { $_.Enabled -eq $true }
if ($activeIpSecRules) {
    Write-Host "Активні правила IPsec (повинні бути відсутні):" -ForegroundColor Red
    $activeIpSecRules | Format-Table Name, Enabled, Action, Direction
} else {
    Write-Host "Активних правил IPsec нема — OK" -ForegroundColor Green
}

# ICMP Echo Request
```

```
$icmpEchoInboundAllowed = Get-NetFirewallRule -Direction Inbound | Where-Object {
    $_.Enabled -eq $true -and
    $_.Action -eq $expectedFirewallRules.ICMPEchoRequest -and
    ($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and
    $_.Name -match "EchoRequest|ERQ"
}

Write-Host "`n=== Вхідний ICMP Echo Request ===" -ForegroundColor Cyan
if ($icmpEchoInboundAllowed) {
    Write-Host "Вхідний ICMP Echo Request [$($expectedFirewallRules.ICMPEchoRequest)] — OK" -ForegroundColor Green
} else {
    Write-Host "Вхідний ICMP Echo Request — НЕ ВІДПОВІДАЄ! Очікується: $($expectedFirewallRules.ICMPEchoRequest)" -ForegroundColor Red
}

# ICMP Destination Unreachable
$icmpDestUnreachAllowed = Get-NetFirewallRule -Direction Inbound | Where-Object {
    $_.Enabled -eq $true -and
    $_.Action -eq $expectedFirewallRules.ICMPDestUnreachable -and
```

```
        ($_.DisplayName -match "ICMP4|ICMPv4|ICMP6|ICMPv6") -and
        ($_.Name -match "DU|DestinationUnreachable")
    }

    Write-Host "`n=== Вхідні ICMP Destination Unreachable ===" -ForegroundColor Cyan
    if ($icmpDestUnreachAllowed) {
        Write-Host "Вхідні ICMP Destination Unreachable [$($expectedFirewallRules.ICMPDestUnreachable)] — OK" -ForegroundColor Green
    } else {
        Write-Host "Вхідні ICMP Destination Unreachable — НЕ ВІДПОВІДАЄ! Очікується: $($expectedFirewallRules.ICMPDestUnreachable)" -ForegroundColor Red
    }

    Write-Host "`n=== ПЕРЕВІРКА БЛОКУВАННЯ ТУНЕЛЬНИХ ПРОТОКОЛІВ (6to4, Teredo, ISATAP) ===" -ForegroundColor Cyan

    foreach ($proto in $baseline.FirewallRules.BlockedTunnelProtocols) {
        $rule = Get-NetFirewallRule -Enabled True | Where-Object {
            $_.Direction -eq "Inbound" -and
            $_.Action -eq "Block" -and
```

```
        $_.DisplayName -match $proto
    }

    if ($rule) {
        Write-Host "Правило блокування $proto знайдено — OK" -ForegroundColor Green
    } else {
        Write-Host "Правило блокування $proto ВІДСУТНЄ! Очікується: Block" -ForegroundColor Red
    }
  }

  Write-Host "`nПеревірка брандмауера завершена.`n" -ForegroundColor Cyan
}

function Check-AccountsAndAccessControl {
  Write-Host "`n=== Аудит контролю доступу ===" -ForegroundColor Cyan

  Write-Host "`n=== Моніторинг часу останнього входу ===" -ForegroundColor Cyan

  $users = Get-LocalUser | Where-Object { $_.Enabled -eq $true }
```

```
foreach ($user in $users) {
    Write-Host "$($user.Name) — Останній логін: $($user.LastLogon)" -ForegroundColor Yellow
}

Write-Host "`n=== Виявлення неактивних облікових записів ===" -ForegroundColor Cyan

$inactiveUsers = Get-LocalUser | Where-Object { $_.Enabled -eq $true -and $_.LastLogon -lt (Get-Date).AddDays(-90) }

if ($inactiveUsers) {
    Write-Host "Неактивні облікові записи виявлено!" -ForegroundColor Red
    $inactiveUsers | Format-Table Name, LastLogon -AutoSize
} else {
    Write-Host "Неактивних облікових записів не виявлено." -ForegroundColor Green
}

Write-Host "`n=== Перевірка членства користувачів у групі адміністраторів ===" -ForegroundColor Cyan
```

```
$adminUsers = Get-LocalGroupMember -Group "Administrators"

if ($adminUsers) {
    Write-Host "Список користувачів у групі адміністраторів:" -ForegroundColor Yellow
    $adminUsers | Format-Table Name, ObjectClass -AutoSize
} else {
    Write-Host "Група адміністраторів порожня!" -ForegroundColor Red
}

Write-Host "`n=== Перевірка тимчасових та службових акаунтів ===" -ForegroundColor Cyan

$temporaryAccounts = Get-LocalUser | Where-Object { $_.Name -match "temp|test|guest|install" }

if ($temporaryAccounts) {
    Write-Host "Виявлено тимчасові акаунти!" -ForegroundColor Yellow
    $temporaryAccounts | Format-Table Name, Enabled -AutoSize
} else {
    Write-Host "Тимчасових акаунтів не виявлено." -ForegroundColor Green
```

```
}

#Введення шляху користувачем
$PathToCheck = Read-Host "`nВведіть шлях до об'єкта (файл, директорія або ключ реєстру), який потрібно перевірити"

if (-not (Test-Path $PathToCheck)) {
    Write-Host "Помилка: вказаний шлях не існує." -ForegroundColor Red
    exit
}

Write-Host "`n=== Перевірка прав доступу ===" -ForegroundColor Cyan

$expectedPermissions = $baseline.DangerousPermissions

#Визначення типу об'єкта
$objectType = if ((Get-Item $PathToCheck).PSIsContainer) { "Folder" } else { "File" }
if ($PathToCheck -match "^HKLM|HKCU|HKCR|HKU|HKCC") { $objectType = "Registry" }
```

```
Write-Host "`nПеревірка прав доступу для об'єкта типу: $objectType" -ForegroundColor Cyan


#Аналіз прав доступу відповідно до типу
try {
    $acl = Get-Acl -Path $PathToCheck -ErrorAction Stop
    $dangerousRights = $expectedPermissions.$objectType


    foreach ($ace in $acl.Access) {
        $identity = $ace.IdentityReference.Value
        $rights = $ace.FileSystemRights.ToString()


        foreach ($dangerousRight in $dangerousRights) {
            if ($rights -match $dangerousRight) {
                Write-Host "`nПотенційно небезпечне право виявлено!" -ForegroundColor Red
                Write-Host "Об'єкт: $PathToCheck" -ForegroundColor Yellow
                Write-Host "Користувач/Група: $identity" -ForegroundColor Yellow
                Write-Host "Права доступу: $rights" -ForegroundColor Yellow
                Write-Host "----------------------------------------"
            }
```

```
        }
    }
} catch {
    Write-Host "[-] Не вдалося отримати ACL для $PathToCheck" -ForegroundColor Yellow
}


#Отримання шляху до перевірки від користувача
$DirToCheck = Read-Host "Введіть шлях до директорії, яку потрібно перевірити"
if (-not (Test-Path $DirToCheck)) {
    Write-Host "Помилка: вказаний шлях не існує." -ForegroundColor Red
    return
}


$RootPath = "C:\"


#Права напряму користувачам
Write-Host "`n=== Перевірка прав, наданих безпосередньо користувачам ===" -ForegroundColor Cyan
$directUserAccess = Get-ChildItem -Path $DirToCheck -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
```

```
        try {
            $acl = Get-Acl $_.FullName -ErrorAction Stop
            foreach ($ace in $acl.Access) {
                $identity = $ace.IdentityReference.Value
                $sid =
([System.Security.Principal.NTAccount]$identity).Translate([System.Security.Princip
al.SecurityIdentifier])
                if ($sid.Value -match "^S-1-5-21") {
                    [PSCustomObject]@{
                        FilePath = $_.FullName
                        User     = $identity
                        Rights   = $ace.FileSystemRights
                    }
                }
            }
        } catch {}
    }

    if ($directUserAccess) {
        Write-Host "Прямі права користувачам виявлено" -ForegroundColor Red
        $directUserAccess | Format-Table -AutoSize
```

```
} else {
    Write-Host "Прямих прав користувачам не виявлено" -ForegroundColor Green
}

#Створення файлів у кореневому каталозі
Write-Host "`n=== Перевірка прав створення файлів/каталогів у кореневому каталозі ===" -ForegroundColor Cyan
$rootAcl = Get-Acl -Path $RootPath
$unwantedRootRights = @()

foreach ($ace in $rootAcl.Access) {
    $identity = $ace.IdentityReference.Value
    $rights = $ace.FileSystemRights.ToString()

    if ($rights -match "CreateDirectories|Modify|FullControl") {
        if ($identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
            $unwantedRootRights += [PSCustomObject]@{
                UserOrGroup = $identity
                Rights      = $rights
                Path        = $RootPath
            }
```

```
            }
        }
    }

    if ($unwantedRootRights.Count -gt 0) {
        Write-Host "Небажані права створення в кореневому каталозі виявлено" -ForegroundColor Red
        $unwantedRootRights | Format-Table -AutoSize
    } else {
        Write-Host "Небажаних прав створення в кореневому каталозі не виявлено." -ForegroundColor Green
    }

    #Наявність Full Control
    Write-Host "`n=== Перевірка наявності небезпечних прав Full Control ===" -ForegroundColor Cyan
    $fullControlIssues = Get-ChildItem -Path $DirToCheck -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
        try {
            $acl = Get-Acl $_.FullName -ErrorAction Stop
            foreach ($ace in $acl.Access) {
                $identity = $ace.IdentityReference.Value
```

```
            $rights = $ace.FileSystemRights.ToString()

            if ($rights -match "FullControl" -and
               $identity -notmatch "Administrators|SYSTEM|TrustedInstaller") {
               [PSCustomObject]@{
                  FilePath = $_.FullName
                  User     = $identity
                  Rights   = $ace.FileSystemRights
               }
            }
         }
      } catch {}
   }

   if ($fullControlIssues) {
      Write-Host "Файли з небезпечними правами Full Control виявлено" -
ForegroundColor Red
      $fullControlIssues | Format-Table -AutoSize
   } else {
      Write-Host "Файлів з небезпечними правами Full Control не виявлено." -
ForegroundColor Green
```

```
    }

    Write-Host "`nАудит завершено." -ForegroundColor Cyan
}

function Check-AntivirusAndUpdates {
    Write-Host "`n=== ПЕРЕВІРКА АНТИВІРУСНОГО ЗАХИСТУ ТА ОНОВЛЕНЬ WINDOWS DEFENDER ===" -ForegroundColor Cyan

    $expected = $baseline.AntivirusSettings
    $mpPrefs = Get-MpPreference

    function Compare-Setting($desc, $actual, $expected) {
        if ($actual -eq $expected) {
            Write-Host "$desc [$actual] — OK" -ForegroundColor Green
        } else {
            Write-Host "$desc [$actual] — НЕ ВІДПОВІДАЄ! Очікується: $expected" -ForegroundColor Red
        }
    }
```

```
Compare-Setting "PUAProtection" $mpPrefs.PUAProtection $expected.PUAProtection
Compare-Setting "Сканування в реальному часі" $mpPrefs.DisableRealtimeMonitoring $expected.DisableRealtimeMonitoring


try {
    $ss = Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System"
    Compare-Setting "SmartScreen" $ss.EnableSmartScreen $expected.EnableSmartScreen
    Compare-Setting "SmartScreen PreventOverride" $ss.PreventOverride $expected.PreventOverride
} catch {
    Write-Host "SmartScreen — НЕ ВІДПОВІДАЄ! Не вдалося зчитати налаштування з реєстру" -ForegroundColor Red
}


# Перевірка актуальності сигнатур
$status = Get-MpComputerStatus
$now = Get-Date
$avDelta = ($now - $status.AntivirusSignatureLastUpdated).Days
$asDelta = ($now - $status.AntispywareSignatureLastUpdated).Days
```

```
    if ($avDelta -le $expected.MaxSignatureAgeDays) {
        Write-Host "Антивірусні сигнатури [$($status.AntivirusSignatureLastUpdated)] — OK" -ForegroundColor Green
    } else {
        Write-Host "Антивірусні сигнатури [$($status.AntivirusSignatureLastUpdated)] — НЕ ВІДПОВІДАЮТЬ! Оновлено $avDelta дн. тому" -ForegroundColor Red
    }

    if ($asDelta -le $expected.MaxSignatureAgeDays) {
        Write-Host "Антишпигунські сигнатури [$($status.AntispywareSignatureLastUpdated)] — OK" -ForegroundColor Green
    } else {
        Write-Host "Антишпигунські сигнатури [$($status.AntispywareSignatureLastUpdated)] — НЕ ВІДПОВІДАЮТЬ! Оновлено $asDelta дн. тому" -ForegroundColor Red
    }
}

function Check-ServicesPortsStartup {
    Write-Host "`n=== Перевірка служб, портів та автозапуску ===" -ForegroundColor Cyan
```

```
$blockedServices = $baseline.Services
$expectedPorts = $baseline.VulnerablePorts
$expectedAutorunStatus = $baseline.AutorunExpectedEmpty

Write-Host "`n=== Перевірка служб ===" -ForegroundColor Cyan

foreach ($serviceName in $blockedServices) {
    $service = Get-Service -Name $serviceName -ErrorAction SilentlyContinue

    if ($service) {
        if ($service.Status -eq 'Stopped') {
            Write-Host "$serviceName — Disabled — OK" -ForegroundColor Green
        } else {
            Write-Host "$serviceName — Enabled! Очікується: Disabled" -
ForegroundColor Red
        }
    } else {
        Write-Host "$serviceName — НЕ ЗНАЙДЕНО (можливо відсутній у
системі)" -ForegroundColor Yellow
    }
```

```
}



#Перевірка портів
Write-Host "`n=== Перевірка відкритих портів ===" -ForegroundColor Cyan
$netstatOutput = netstat -ano | Select-String "LISTENING"
$openVulnerablePorts = @()


foreach ($port in $expectedPorts) {
    if ($netstatOutput -match "[:\.]$port\s") {
        $openVulnerablePorts += $port
    }
}


if ($openVulnerablePorts.Count -eq 0) {
    Write-Host "Потенційно вразливі порти не відкриті — OK" -ForegroundColor
Green
} else {
    Write-Host "ВІДКРИТІ потенційно вразливі порти: $($openVulnerablePorts -
join ', ')" -ForegroundColor Yellow
}
```

```
#Перевірка автозапуску
Write-Host "`n=== Перевірка автозапуску ===" -ForegroundColor Cyan
$runKeys = @(
    "HKLM:\Software\Microsoft\Windows\CurrentVersion\Run",
    "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce",
    "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run",
    "HKCU:\Software\Microsoft\Windows\CurrentVersion\RunOnce"
)

$hasAutorunEntries = $false

foreach ($key in $runKeys) {
    try {
        $values = Get-ItemProperty -Path $key -ErrorAction Stop
        $props = $values.PSObject.Properties | Where-Object {
            $_.Name -notmatch "^PS"
        }

        if ($props.Count -gt 0) {
            Write-Host "Знайдено записи в $key" -ForegroundColor Red
```

```
            foreach ($entry in $props) {
                Write-Host " - $($entry.Name): $($entry.Value)" -ForegroundColor Yellow
            }
            $hasAutorunEntries = $true
        }
    } catch {}
  }

  if ($expectedAutorunStatus -and (-not $hasAutorunEntries)) {
    Write-Host "Автозапуск вимкнений — OK" -ForegroundColor Green
  }
}

function Load-ConfigFile {
  do {
    $configPath = Read-Host "Введіть шлях до конфігураційного файлу (JSON)"
    if (Test-Path $configPath) {
      try {
        $config = Get-Content $configPath | ConvertFrom-Json
```

```
            Write-Host "[+] Конфігурація завантажена успішно!" -ForegroundColor Green
            return $config
        } catch {
            Write-Host "[-] Помилка при читанні файлу. Перевірте його формат!" -ForegroundColor Red
        }
    } else {
        Write-Host "[-] Файл не знайдено. Спробуйте ще раз!" -ForegroundColor Red
    }
  } while ($true)
}

$baseline = Load-ConfigFile

$exitScript = $false

function Show-Menu {
  Clear-Host
  Write-Host "Оберіть категорію аудиту безпеки Windows:`n"
  Write-Host "1. Local Security Policies"
```

```
    Write-Host "2. Windows Firewall"
    Write-Host "3. Облікові записи та контроль доступу"
    Write-Host "4. Антивірусний захист та оновлення"
    Write-Host "5. Порти, служби та автозапуск"
    Write-Host "0. Вийти"
}

do {
    Show-Menu
    $choice = Read-Host "Введіть номер пункту"
    switch ($choice) {
        '1' { Check-LocalSecurityPolicies }
        '2' { Check-Firewall }
        '3' { Check-AccountsAndAccessControl }
        '4' { Check-AntivirusAndUpdates }
        '5' { Check-ServicesPortsStartup }
        '0' {
            Write-Host "Вихід із скрипту..." -ForegroundColor Yellow
            $exitScript = $true
        }
```

```
        default { Write-Host "Невірний вибір. Спробуйте ще раз." -ForegroundColor
Red }
    }


    if (-not $exitScript) {
        Write-Host "`nНатисніть Enter для продовження..."
        Read-Host
    }
} while (-not $exitScript)
```

ДОДАТОК Б КОНФІГУРАЦІЙНИЙ JSON-ФАЙЛ


```
{
 "PasswordPolicies": {
  "PasswordHistorySize": 24,
  "MaximumPasswordAge": 60,
  "MinimumPasswordAge": 1,
  "MinimumPasswordLength": 14,
  "PasswordComplexity": 1,
  "ClearTextPassword": 0
 },

 "LockoutPolicies": {
  "LockoutBadCount": 10,
  "LockoutDuration": 15,
  "ResetLockoutCount": 15
 },

 "AccountPolicies": {
  "EnableAdminAccount": 0,
  "EnableGuestAccount": 0,
```

```
  "NewAdministratorName": "Administrator",
  "NewGuestName": "Guest"
},

"PrivilegeRights": {
  "SeRemoteInteractiveLogonRight": ["S-1-5-32-544", "S-1-5-32-555"],
  "SeSystemtimePrivilege": ["S-1-5-32-544", "S-1-5-19"],
  "SeTakeOwnershipPrivilege": ["S-1-5-32-544"],
  "SeSecurityPrivilege": ["S-1-5-32-544"],
  "SeDenyNetworkLogonRight": ["S-1-5-32-546", "S-1-2-0"],
  "SeLoadDriverPrivilege": ["S-1-5-32-544"],
  "SeServiceLogonRight": ["S-1-5-32-544"]
},

"BootSettings": {
  "TestSigning": "no"
},

"RegistrySettings": {
  "DontDisplayLastUserName": 1,
  "EnableLUA": 1,
```

"ConsentPromptBehaviorAdmin": 5,
"InactivityTimeoutSecs": 900
},

"LsaSettings": {
"RestrictAnonymous": 1,
"LimitBlankPasswordUse": 1
},

"AuditPolicy": {
"Credential Validation": "Success and Failure",
"Application Group Management": "Success and Failure",
"Computer Account Management": "Success and Failure",
"Other Account Management Events": "Success and Failure",
"Security Group Management": "Success and Failure",
"User Account Management": "Success and Failure",
"Plug and Play Events": "Success",
"Process Creation": "Success",
"Account Lockout": "Success and Failure",
"Group Membership": "Success",
"Logoff": "Success",

```
  "Logon": "Success and Failure",
  "Other Logon/Logoff Events": "Success and Failure",
  "Special Logon": "Success",
  "Removable Storage": "Success and Failure",
  "Audit Policy Change": "Success and Failure",
  "Authentication Policy Change": "Success",
  "Authorization Policy Change": "Success",
  "Sensitive Privilege Use": "Success and Failure",
  "IPsec Driver": "Success and Failure",
  "Other System Events": "Success and Failure",
  "Security State Change": "Success",
  "Security System Extension": "Success and Failure",
  "System Integrity": "Success and Failure"
},

"FirewallSettings": {
  "Domain": {
    "Enabled": true,
    "DefaultInboundAction": "Block",
    "DefaultOutboundAction": "Allow",
    "AllowLocalFirewallRules": true,
```

```
    "AllowLocalIPsecRules": true,
    "LogFileName": "%SystemRoot%\\System32\\logfiles\\firewall\\domainfw.log",
    "LogAllowed": true,
    "LogBlocked": true,
    "LogFileSizeKB": 16384
  },
  "Private": {
    "Enabled": true,
    "DefaultInboundAction": "Block",
    "DefaultOutboundAction": "Allow",
    "AllowLocalFirewallRules": true,
    "AllowLocalIPsecRules": true,
    "LogFileName": "%SystemRoot%\\System32\\logfiles\\firewall\\privatefw.log",
    "LogAllowed": true,
    "LogBlocked": true,
    "LogFileSizeKB": 16384
  },
  "Public": {
    "Enabled": true,
    "DefaultInboundAction": "Block",
    "DefaultOutboundAction": "Allow",
```

```
      "AllowLocalFirewallRules": false,
      "AllowLocalIPsecRules": false,
      "LogFileName": "%SystemRoot%\\System32\\logfiles\\firewall\\publicfw.log",
      "LogAllowed": true,
      "LogBlocked": true,
      "LogFileSizeKB": 16384
  }
},

"FirewallRules": {
  "ICMPEchoRequest": "Block",
  "ICMPDestUnreachable": "Allow",
  "BlockedTunnelProtocols": ["6to4", "Teredo", "ISATAP"]
},

"DangerousPermissions": {
  "Registry": [
      "SetValue",
      "CreateSubKey",
      "WriteDac",
      "WriteOwner",
```

"GenericWrite",
"GenericAll",
"Delete",
"QueryValue",
"EnumerateSubKeys"
],
"File": [
"WriteData",
"AppendData",
"WriteDac",
"WriteOwner",
"GenericWrite",
"GenericAll",
"Delete",
"ReadData",
"ReadAttributes",
"ReadExtendedAttributes"
],
"Folder": [
"CreateFiles",
"CreateDirectories",

"DeleteSubdirectoriesAndFiles",
"WriteDac",
"GenericWrite",
"GenericAll",
"Delete",
"ListDirectory",
"ReadAttributes",
"ReadExtendedAttributes"
]
},

"AntivirusSettings": {
"PUAProtection": 1,
"DisableRealtimeMonitoring": false,
"EnableSmartScreen": 1,
"PreventOverride": 1,
"MaxSignatureAgeDays": 1
},

"Services": [
"BthServ",

"lfsvc",
"icssvc",
"Browser",
"irmon",
"FTPSVC",
"xbgm"
],

"VulnerablePorts": [21, 22, 23, 25, 53, 80, 137, 139, 1433, 1434, 3006, 3389, 443, 8080, 8443, 445],
"AutorunExpectedEmpty": true
}