МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТЕЙ ЦЕНТРУ СЕРТИФІКАЦІЇ В ПРОЦЕСІ ОЦІНЮВАННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр СКРИПКА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Олександр СКРИПКА
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
К.т.н. Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

а

Скрипці Олександру Володимировичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи експлуатації вразливостей центру сертифікації в процесі оцінювання безпеки корпоративних мереж”,
керівник кваліфікаційної роботи РАБЧУН Дмитро, к.т.н.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *безпека корпоративних мереж, методи оцінювання захищеності, аудит інформаційної безпеки, тестування на проникнення, Active Directory Certificate Services, вразливості центрів сертифікації, засоби усунення вразливостей, методи моніторингу та виявлення атак, міжнародні стандарти кібербезпеки.*

4. Перелік питань, які мають бути розроблені:
4.1. Виконати аналіз процесу оцінювання безпеки корпоративних мереж, визначити роль центру сертифікації у цьому процесі та розглянути будову самого центру сертифікації.
4.2. Дослідити основні вразливості центру сертифікації та методи їх експлуатації, що пов’язані з неналежними налаштуваннями шаблонів сертифікатів та центру сертифікації.
4.3. Надати рекомендації щодо усунення вразливостей центру сертифікації, а також розробити заходи щодо моніторингу та виявлення атак на центр сертифікації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз процесу оцінювання безпеки корпоративних мереж в контексті функціонування центру сертифікації.	08.04.2025	
4.	Дослідження основних вразливостей центру сертифікації та методів їх експлуатації.	15.04.2025	
5.	Надання рекомендацій щодо усунення вразливостей центру сертифікації та розробка заходів щодо виявлення атак на центр сертифікації.	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Олександр СКРИПКА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Скрипка О.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи експлуатації вразливостей центру сертифікації в процесі оцінювання безпеки корпоративних мереж"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач СКРИПКА Олександр у кваліфікаційній роботі дослідив методи оцінювання безпеки корпоративних мереж, проаналізував роль Active Directory Certificate Services, виявив типові вразливості та описав механізми їх експлуатації, надав практичні рекомендації з їх усунення та організації моніторингу загроз.

СКРИПКА Олександр продемонстрував розуміння проблеми, володіння сучасними інструментами тестування на проникнення та здатність формулювати обґрунтовані технічні рішення. У роботі успішно реалізовано як теоретичний аналіз, так і практичну частину з демонстрацією реальних сценаріїв атак на AD CS. Здобувач проявив себе як відповідальний і підготовлений виконавець, що володіє навичками дослідження в галузі кібербезпеки.

Все це дозволяє оцінити кваліфікаційну роботу здобувача СКРИПКИ Олександра на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Скрипка О.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти СКРИПКИ Олександра
на тему “Методи експлуатації вразливостей центру сертифікації в процесі оцінювання безпеки корпоративних мереж”

Актуальність. З огляду на сучасні тенденції розвитку кіберзагроз, особливої уваги заслуговують вектори атак, пов’язані з інфраструктурою відкритих ключів. Active Directory Certificate Services є критично важливим компонентом у корпоративному середовищі, і його неналежна конфігурація може призвести до повної компрометації мережі.

Тому дослідження механізмів атак на Active Directory Certificate Services та розробка рекомендацій щодо їх виявлення і запобігання є актуальним і практично значущим завданням у сфері кібербезпеки.

Позитивні сторони.

1. У роботі комплексно розглянуто сучасні методи тестування безпеки корпоративних мереж, зокрема в контексті вразливостей Active Directory Certificate Services.
2. Описано основні сценарії атак на сертифікаційну інфраструктуру з реальними прикладами використання інструментів Certipy, Certify та Impacket.
3. Структура роботи логічна й послідовна, висновки чітко сформульовані, оформлення відповідає вимогам до кваліфікаційних робіт.
4. У дослідженні наведено доцільні технічні рекомендації щодо усунення вразливостей та заходів моніторингу загроз.

Недоліки.

Доцільно було б доповнити роботу пропозиціями щодо автоматизації виявлення вразливостей та інтеграції отриманих результатів у систему управління інформаційною безпекою підприємства.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-практичному рівні та заслуговує оцінки “відмінно”. Здобувач СКРИПКА Олександр заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів експлуатації вразливостей центру сертифікації в процесі оцінювання безпеки корпоративних мереж. Робота складається зі вступу, трьох розділів, що містять 23 рисунки, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 61 аркуш, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є підвищення ефективності оцінювання безпеки корпоративних мереж.

Об'єктом дослідження є процес оцінювання безпеки корпоративних мереж у контексті функціонування центру сертифікації.

Предмет дослідження – методи експлуатації вразливостей центру сертифікації та їх застосування під час оцінювання безпеки корпоративних мереж.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, моделювання загроз, аналізу вразливостей та тестування на проникнення.

Як результат, у роботі описано підходи до проведення оцінювання безпеки корпоративних мереж, виконано аналіз основних вразливостей центру сертифікації та методів їх експлуатації, розроблено відповідні рекомендації щодо підвищення безпеки корпоративних мереж.

Галузь застосування. Досліджені методи та рекомендації можуть бути використані при проведенні тестувань на проникнення та аудиту корпоративних мереж, а також для вдосконалення політик безпеки в організаціях.

Ключові слова: ВРАЗЛИВОСТІ, ЦЕНТР СЕРТИФІКАЦІЇ, ОЦІНЮВАННЯ БЕЗПЕКИ, КОРПОРАТИВНІ МЕРЕЖІ, МЕТОДИ ЕКСПЛУАТАЦІЇ, ТЕСТУВАННЯ НА ПРОНИКНЕННЯ.

ABSTRACT

The qualification work is devoted to the study of methods of exploitation certificate authority vulnerabilities during corporate network security assessment. The work consists of an introduction, three chapters containing 23 figures, conclusions, and a list of 40 references. The total volume of the work is 61 pages, of which 6 pages are occupied by a list of abbreviations and references.

The purpose of the study is to increase the efficiency of corporate network security assessment.

The object of the study is the process of assessing corporate network security in the context of the certification authority's operation.

The subject of the study is the methods for exploiting certification authority vulnerabilities and their application in corporate network security assessment.

Research methods. To solve the mentioned higher scientific task, the methods of system analysis, threat modeling, vulnerability analysis, and penetration testing were used in the work.

As a result, the work describes the principles of corporate network security assessment, analyzes the main vulnerabilities of the certification authority and methods for their exploitation, and develops relevant recommendations for improving corporate network security.

Field of application. The discovered methods and recommendations can be used in the when conducting penetration testing and auditing corporate networks, as well as to improve security policies in organizations.

Keywords: VULNERABILITIES, CERTIFICATION AUTHORITY, SECURITY ASSESSMENT, CORPORATE NETWORKS, EXPLOITATION METHODS, PENETRATION TESTING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AD	Active Directory
AD CS	Active Directory Certificate Services
ACL	Access Control List
CA	Certification Authority
CSR	Certificate Signing Request
EKU	Enhanced Key Usage
ESC	Enterprise Security Certificates
NTLM	NT LAN Manager
PKI	Public Key Infrastructure
PKINIT	Public Key Cryptography for Initial Authentication in Kerberos
SAN	Subject Alternative Name

ВСТУП

Актуальність теми. Забезпечення безпеки корпоративної мережі є критично важливим завданням для організацій, оскільки в сучасному світі стає дедалі більше загроз кібербезпеці організацій. Під час проведення оцінювання безпеки корпоративної мережі, одним із ключових компонентів безпеки для перевірки є центр сертифікації, який відповідає за видачу, керування та перевірку цифрових сертифікатів у корпоративному середовищі.

Незважаючи на свою важливу роль у безпеці корпоративної мережі, неналежні налаштування центру сертифікації можуть призводити до появи вразливостей, зокрема до тих, що спрямовані для підвищення привілеїв. В результаті, експлуатація цих вразливостей може дозволити зловмисникам отримати несанкціонований доступ до корпоративного середовища та підвищити власні привілеї до рівня адміністратора, що в свою чергу може призвести до подальшої компрометації всієї корпоративної мережі.

З огляду на зазначене, тема кваліфікаційної роботи є актуальною, а її результати можуть сприяти покращенню оцінювання безпеки корпоративної мережі та безпосередньо дозволять підвищити рівень безпеки корпоративної мережі, що використовує центр сертифікації.

Метою роботи є підвищення ефективності оцінювання безпеки корпоративних мереж.

Об'єктом дослідження є процес оцінювання безпеки корпоративних мереж у контексті функціонування центру сертифікації.

Предмет дослідження – методи експлуатації вразливостей центру сертифікації та їх застосування під час оцінювання безпеки корпоративних мереж.

Для досягнення мети в роботі необхідно виконати наступні **завдання**:

1. Виконати аналіз процесу оцінювання безпеки корпоративних мереж, визначити роль центру сертифікації у цьому процесі та розглянути будову самого центру сертифікації.

2. Дослідити основні вразливості центру сертифікації та методи їх експлуатації, що пов’язані з неналежними налаштуваннями шаблонів сертифікатів та центру сертифікації.

3. Надати рекомендації щодо усунення вразливостей центру сертифікації, а також розробити заходи щодо моніторингу та виявлення атак на центр сертифікації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, моделювання загроз, аналізу вразливостей та тестування на проникнення.

Практичне значення одержаних результатів. Досліджені методи та рекомендації можуть бути використані при проведенні тестувань на проникнення та аудиту корпоративних мереж, а також для вдосконалення політик безпеки в організаціях.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 ПРОЦЕС ОЦІНЮВАННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Підходи до оцінювання безпеки корпоративних мереж

Сучасні корпоративні мережі є складними інформаційними системами [5], які об'єднують різні технологічні платформи, сервіси та користувачів. Їхня безпека є критичним фактором для стабільного функціонування бізнес-процесів, оскільки зростаюча кількість кіберзагроз може призвести до фінансових втрат, витоку конфіденційної інформації або компрометації всієї IT-інфраструктури.

Оцінювання безпеки корпоративних мереж є ключовим елементом стратегії кібербезпеки організації, що дозволяє своєчасно виявляти вразливості та усувати потенційні загрози. Цей процес може включати як внутрішні перевірки, так і зовнішні аудити, що проводяться незалежними експертами.

У практиці оцінювання безпеки корпоративних мереж використовуються різні підходи, які можна умовно класифікувати за трьома основними критеріями: за джерелом ініціативи (внутрішня або зовнішня оцінка), за рівнем деталізації (поверхневий аналіз або глибинне тестування), а також за методологією виконання (стандартизований аудит, експертне оцінювання, симуляція атак тощо). Така багатогранна структура дозволяє організаціям обирати найбільш релевантні механізми захисту з урахуванням масштабу мережі, галузевих особливостей та рівня загроз.

На практиці часто поєднуються формалізовані методи (наприклад, аудит відповідності політикам безпеки) із динамічними, які включають симуляцію реальних атак. Цей підхід відомий як гібридна модель оцінювання, що дозволяє одночасно і перевірити документацію, і протестувати реакцію систем на активні загрози.

Однією з поширених моделей для побудови системи оцінювання є PDCA (Plan-Do-Check-Act) — цикл безперервного вдосконалення, який дає змогу

гнучко адаптувати заходи безпеки до змін у середовищі. На етапі "Plan" організація визначає ризики та формує політику безпеки, "Do" передбачає впровадження заходів, "Check" — перевірку їх ефективності, а "Act" — коригування стратегії відповідно до результатів.

Також важливо враховувати, що сучасні мережі мають складну структуру, де поєднуються традиційні IT-середовища, хмарні сервіси, мобільні пристрої та віддалені підключення. У такому контексті зростає значення контекстно-орієнтованого оцінювання (Context-Aware Security Assessment), яке враховує особливості топології, політики доступу, взаємодії з партнерами тощо.

Ще один ефективний напрям — використання методик атаки з боку зловмисника (Adversary Emulation), що імітують дії реальних атакувальників, ґрунтуючись на відомих тактиках і техніках з фреймворку MITRE ATT&CK. Такий підхід дозволяє не лише перевірити технічну стійкість систем, а й оцінити швидкість реагування персоналу, ефективність логів, SIEM-систем та інструментів реагування.

Значного поширення набуло використання індексів безпеки — спеціалізованих метрик, що дозволяють кількісно оцінити поточний стан захищеності. Наприклад, індекс Surface Exposure Score враховує кількість відкритих портів і сервісів у зовнішній мережі, а Threat Likelihood Rating оцінює ймовірність експлуатації виявлених вразливостей. Такі підходи дозволяють краще обґрунтовувати інвестиції в кібербезпеку перед керівництвом.

У процесі оцінювання особливо важливо враховувати людський фактор. Помилки конфігурації, нехтування політиками безпеки, фішингові атаки — усе це часто стає ключовими причинами інцидентів. Саме тому сучасні підходи передбачають включення соціальної інженерії до сценаріїв тестування. Наприклад, може бути проведено контрольовану розсилку фішингових листів або симуляція телефонного шахрайства, щоб перевірити рівень обізнаності персоналу.

Слід зазначити, що правильна організація етапів оцінювання дозволяє не тільки виявляти вразливості, але й формувати стратегію їх усунення. Наприклад, після тестування на проникнення часто складається звіт з пріоритизацією ризиків: високий (потребує негайного усунення), середній (усувається протягом планових оновлень), низький (моніторинг або документування). Такий підхід дозволяє ефективно розподілити ресурси кіберзахисту.

У підсумку, підходи до оцінювання безпеки корпоративних мереж мають бути адаптивними, багаторівневими й орієнтованими на реальні загрози. Лише комбінація технічного тестування, формалізованого аудиту, поведінкових сценаріїв та стратегічного аналізу дозволяє створити дійсно стійку до загроз систему інформаційної безпеки.

Серед основних методів оцінювання безпеки можна виділити аудит інформаційної безпеки (Information Security Audit), тестування на проникнення (Penetration Testing) та проведення імітації атак (Red Teaming). Кожен з них має власні особливості, що визначають їхню доцільність використання залежно від поставлених завдань [40].

Аудит інформаційної безпеки є базовим методом оцінки рівня захищеності інформаційних систем, що дозволяє перевірити відповідність організації встановленим стандартам та нормативним вимогам, а також виявити потенційні слабкі місця у системах контролю доступу, політиках безпеки та інфраструктурі мережі.

Аудит може бути внутрішнім (проводиться співробітниками організації) або зовнішнім (виконується незалежними аудиторами чи спеціалізованими компаніями). Він може мати різну глибину: від поверхневої перевірки політик та процедур до детального аналізу конфігурацій систем і журналів подій.

Важливим аспектом аудиту є відповідність міжнародним стандартам кібербезпеки, які регламентують вимоги до захисту інформаційних активів. Серед найважливіших стандартів можна виділити [1, 28]:

- ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою (СУІБ), що встановлює вимоги до створення, впровадження, підтримки та вдосконалення СУІБ.
- NIST SP 800-53 – набір рекомендацій Національного інституту стандартів і технологій США, який містить вимоги щодо безпеки інформаційних систем.
- GDPR (General Data Protection Regulation) – європейський регламент захисту персональних даних, що встановлює жорсткі вимоги до їх обробки та зберігання.
- CIS Controls – набір базових рекомендацій для забезпечення кібербезпеки організацій.
- PCI DSS (Payment Card Industry Data Security Standard) – стандарт для компаній, що працюють із платіжними картками, який визначає вимоги до захисту фінансових даних.

Дотримання цих стандартів є важливим кроком у забезпеченні кіберстійкості організації, оскільки дозволяє не лише знизити ризики кібератак, а й виконати регуляторні вимоги та здійснювати відповідну діяльність.

Доволі часто проведення тестування на проникнення є у вимогах та рекомендаціях стандартів, зокрема PCI DSS. Згідно цього стандарту, проведення регулярного тестування на проникнення є однією з обов’язкових вимог для організацій, що працюють із банківськими картками.

Тестування на проникнення є активним методом оцінки захищеності системи, що передбачає імітацію реальних атак на інформаційну інфраструктуру з метою виявлення вразливостей та перевірки можливості їх експлуатації [15, 33].

На відміну від аудиту, який зазвичай зосереджений на перевірці політик і процесів безпеки, тестування на проникнення дозволяє оцінити стійкість системи до реальних атак та виявити існуючі вразливості.

Існує кілька підходів до тестування на проникнення, що визначають рівень початкової обізнаності тестувальників про систему [15, 21]:

- Black Box – тестувальники не мають жодної попередньої інформації про корпоративну інфраструктуру, що імітує реальні атаки зловмисника.
- Gray Box – тестування проводиться з обмеженим доступом до певних внутрішніх даних, наприклад, з використанням облікового запису звичайного користувача.
- White Box – тестувальники мають повний доступ до внутрішньої документації та конфігурацій системи, що дозволяє максимально точно ідентифікувати вразливості та оцінити загальний рівень безпеки.

На рис. 1.1 зображено етапи проведення тестування на проникнення, які відображають послідовний процес аналізу безпеки інформаційних систем.

Рис. 1.1. Схема етапів проведення тестування на проникнення

Першим етапом є розвідка та збір інформації, під час якого тестувальники використовують відкриті джерела (OSINT), сканування мережі та інші методи для отримання інформації про цільову систему. Цей етап дозволяє зрозуміти архітектуру мережі, ідентифікувати відкриті порти, використовувані сервіси та потенційні вразливості.

Другим етапом є пошук та ідентифікація вразливостей, на якому проводиться глибший аналіз виявлених сервісів та конфігурацій, що можуть

містити слабкі місця. Використовуються автоматизовані інструменти для сканування вразливостей, а також ручні методи для їх виявлення.

Третій етап – експлуатація вразливостей, що передбачає використання знайдених слабких місць для отримання несанкціонованого доступу до системи. Це може включати віддалене виконання коду, підвищення привілеїв, отримання облікових даних або розширення контролю над інфраструктурою.

Четвертим етапом є пост-експлуатація, коли тестувальники оцінюють масштаби отриманого доступу, з'ясовують, наскільки глибоко можна проникнути в систему, та визначають потенційний вплив атаки.

Останній етап – аналіз результатів та формування звіту, що включає документування знайдених вразливостей, методів їх експлуатації та можливих наслідків компрометації. Також у звіті надаються рекомендації щодо усунення вразливостей та підвищення рівня безпеки системи.

Ця структура забезпечує системний підхід до оцінювання рівня кібербезпеки організації та дозволяє виявити й усунути потенційні загрози до того, як ними скористаються реальні зловмисники.

Також можна виділити метод оцінювання безпеки Red Teaming, який не обмежується лише технічним аналізом вразливостей, а включає імітацію складних атак, що можуть включати методи соціальної інженерії, експлуатацію внутрішніх загроз та складні сценарії проникнення.

На відміну від тестування на проникнення, яке зазвичай має чітко визначені межі та проводиться з метою виявлення вразливостей, Red Teaming орієнтований на оцінку здатності команди безпеки протидіяти реальним атакам.

У цьому процесі зазвичай задіяні дві команди:

- Red Team – команда атакуючих, яка імітує дії реальних зловмисників, використовуючи сучасні техніки обходу засобів безпеки.
- Blue Team – команда захисту, яка відповідає за виявлення, аналіз та запобігання атакам.

У деяких організаціях використовується підхід Purple Teaming, коли команди Red Team та Blue Team співпрацюють для вдосконалення процесів

виявлення та реагування на атаки.

Red Teaming дозволяє організації оцінити не лише технічну безпеку, а й здатність команди безпеки до оперативного виявлення та реагування на загрози. Однак цей метод є складним у реалізації, потребує значних ресурсів та зазвичай використовується великими організаціями, що мають розвинену систему кіберзахисту.

Таким чином, оцінювання безпеки корпоративних мереж є комплексним процесом, що включає аналіз політик безпеки, перевірку відповідності нормативним стандартам, тестування на проникнення та імітацію складних атак. Залежно від потреб організації можуть застосовуватися різні підходи, які доповнюють один одного та дозволяють отримати всебічну картину стану кібербезпеки.

1.2 Роль центру сертифікації у корпоративній безпеці

У сучасних корпоративних мережах використання сертифікатів відіграє критичну роль у забезпеченні захисту даних, аутентифікації користувачів і пристроїв, а також у реалізації механізмів шифрування. Без належного управління цифровими сертифікатами ризики несанкціонованого доступу та компрометації даних значно зростають. Центром сертифікації (Certificate Authority, CA) називається довірена сторона, яка випускає, підтверджує та відкликає цифрові сертифікати, гарантуючи їхню автентичність і цілісність. Основою цього процесу є інфраструктура відкритих ключів (PKI), яка дозволяє організаціям забезпечувати довірені відносини між користувачами, серверами та сервісами. Тому нерідко саме інфраструктура відкритих ключів є ціллю не тільки аудиторів безпеки, а й зловмисників, які використовують її у своїх кампаніях.

Для впровадження PKI у корпоративних середовищах широко використовується Active Directory Certificate Services (AD CS) – серверний компонент Windows Server, який дозволяє централізовано керувати

сертифікатами всередині корпоративної мережі. Інтеграція AD CS з Active Directory забезпечує автоматичну видачу сертифікатів користувачам, пристроям, серверним сервісам та іншим елементам IT-інфраструктури. Впровадження PKI у корпоративному середовищі дозволяє реалізовувати такі механізми безпеки, як безпечна аутентифікація користувачів, підписання документів, шифрування електронної пошти, забезпечення довіри між мережевими пристроями та реалізація багатофакторної аутентифікації.

AD CS складається з кількох основних компонентів, кожен із яких виконує свою специфічну функцію в рамках PKI [7, 17, 23, 27, 34]:

- Certification Authority (CA) – центр сертифікації, який є основним компонентом, видає та керує цифровими сертифікатами. У середовищі AD CS може бути реалізована ієрархія центрів сертифікації, що включає Root CA (кореневий центр сертифікації) та Subordinate CAs (підлеглі центри сертифікації).
- Certificate Templates – шаблони сертифікатів, які визначають налаштування сертифікатів, зокрема права на їх видачу, термін дії, призначення тощо.
- Certificate Enrollment Web Service (CES) – дозволяє пристроям та користувачам отримувати та оновлювати сертифікати за допомогою HTTPS.
- Certificate Enrollment Policy Web Service (CEP) – забезпечує доступ до політик видачі сертифікатів, що визначають правила отримання сертифікатів у корпоративному середовищі.
- CA Web Enrollment – веб-інтерфейс для запиту та оновлення сертифікатів, особливо корисний у випадках, коли пристрої не є частиною домену.
- Network Device Enrollment Service (NDES) – надає можливість отримання сертифікатів для мережевих пристроїв, таких як маршрутизатори та комутатори.

Однією з основних характеристик цифрового сертифіката є його

призначення, яке визначає, для яких цілей цей сертифікат може бути використаний. В шаблоні сертифіката це визначається розширеним використанням ключа (Enhanced Key Usage, EKU), яке задає конкретні політики для кожного сертифіката. Наприклад, сертифікати можуть бути призначені для аутентифікації користувачів (Client Authentication), підтвердження сервера (Server Authentication), підписання програмного коду (Code Signing) або шифрування електронної пошти (Secure Email).

Табл. 1.1 містить найпоширеніші OIDs (Object Identifiers), які визначають призначення сертифікатів у корпоративному середовищі [7, 27, 30].

Таблиця 1.1.

Призначення сертифікатів в корпоративному середовищі

OID	**Призначення**	**Опис**
1.3.6.1.5.5.7.3.2	Client Authentication	Використовується для аутентифікації користувачів
1.3.6.1.5.5.7.3.1	Server Authentication	Застосовується для ідентифікації серверів, наприклад, у HTTPS
1.3.6.1.4.1.311.20.2.2	Smart Card Logon	Використовується для аутентифікації через смарт-картки
1.3.6.1.5.5.7.3.3	Code Signing	Призначений для підписування виконуваних файлів та скриптів

Продовження таблиці 1.1.

OID	**Призначення**	**Опис**
1.3.6.1.5.5.7.3.4	Secure Email	Використовується для шифрування та підписування електронної пошти (S/MIME)
1.3.6.1.4.1.311.10.3.4	Encrypting File System	Дозволяє шифрувати та дешифрувати файли і директорії на системі

Відповідно, сертифікати можуть використовуватися не лише для аутентифікації користувачів та серверів, а й для реалізації розширених механізмів безпеки, таких як аутентифікація в мережі на основі смарт-карток, підписування PowerShell-скриптів, а також шифрування електронної пошти.

Видача сертифікатів у AD CS базується на запитах на сертифікати (Certificate Signing Requests, CSR), які формуються користувачами або системами і відправляються до CA для перевірки запиту та видачі сертифікату [2, 27]. Цей процес проходить такі етапи (Рис. 1.2):

1) Користувач або пристрій формує CSR, включаючи свій відкритий ключ та мета-відомості.

2) Запит надсилається до центру сертифікації (CA), який перевіряє його відповідність політикам.

3) Якщо перевірка успішна, CA підписує сертифікат своїм приватним ключем і видає його користувачу.

4) Користувач отримує сертифікат і може використовувати його для визначеної мети (аутентифікація, шифрування тощо).

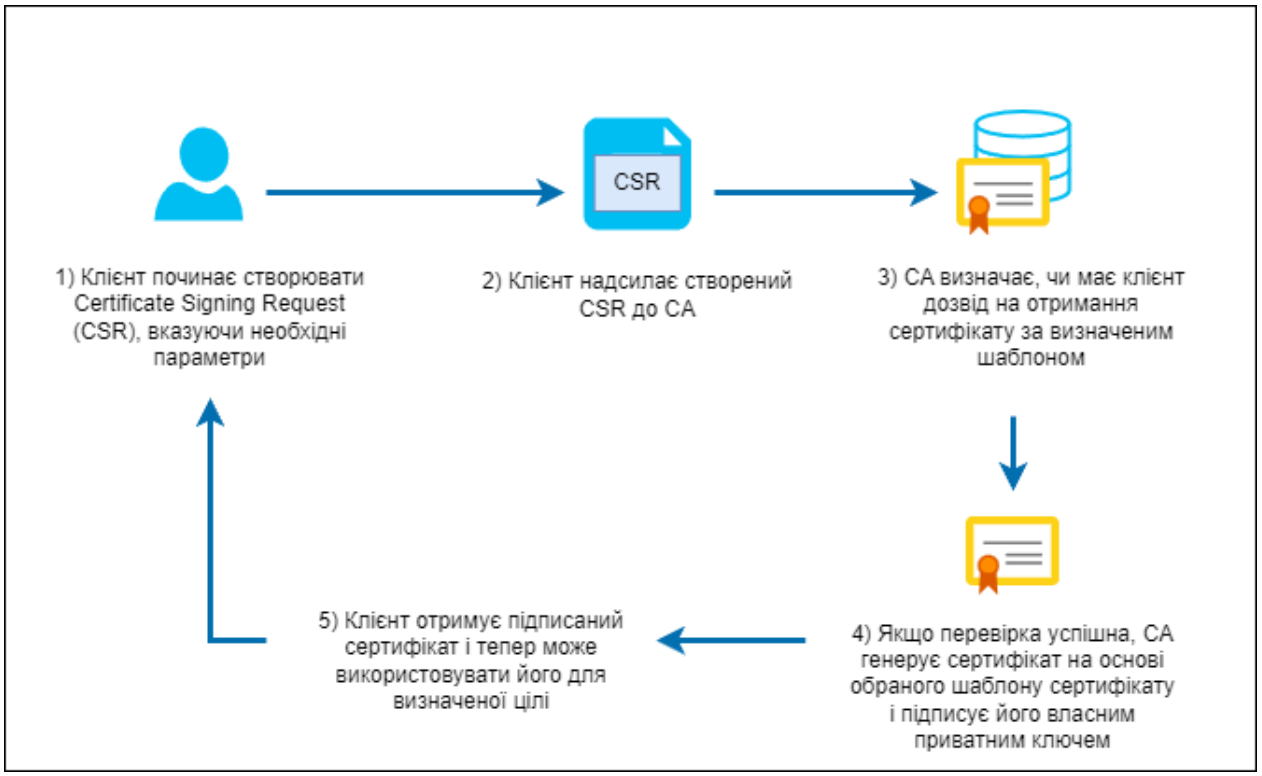

Рис 1.2 Процес отримання сертифіката в AD CS

Однією з важливих особливостей AD CS є інтеграція з Kerberos-аутентифікацією через механізм PKINIT (Public Key Cryptography for Initial Authentication in Kerberos). Це розширення дозволяє використовувати сертифікати для отримання Kerberos TGT (Ticket Granting Ticket), що значно підвищує безпеку корпоративної аутентифікації [17]. Використання PKINIT у поєднанні зі смарт-картками або токенами дозволяє впроваджувати безпарольний вхід у систему (passwordless authentication) та підвищувати рівень безпеки за рахунок відмови від традиційних паролів.

Ще одним важливим аспектом роботи AD CS є механізм відкликання сертифікатів, який дозволяє забезпечити безпеку PKI шляхом оперативного відключення скомпрометованих або більше не потрібних сертифікатів. Для цього використовуються такі технології [16, 17, 23]:

- Certificate Revocation List (CRL) – список відкликаних сертифікатів, який регулярно оновлюється та розповсюджується серед клієнтів.
- Online Certificate Status Protocol (OCSP) – сервіс, що дозволяє перевіряти статус сертифікатів у реальному часі.

Таким чином, AD CS є ключовим компонентом корпоративної безпеки, який забезпечує управління цифровими сертифікатами, аутентифікацію користувачів і пристроїв, а також шифрування даних. Впровадження PKI дозволяє організаціям реалізовувати довірену взаємодію між серверами, користувачами та службами, мінімізуючи ризики компрометації даних.

Ще одним важливим аспектом роботи AD CS є управління життєвим циклом сертифікатів, зокрема їх своєчасна ротація, моніторинг термінів дії та автоматизація процесів відкликання. У великих організаціях тисячі сертифікатів можуть бути активними одночасно, і навіть один прострочений або скомпрометований сертифікат може призвести до критичних наслідків, зокрема зупинки сервісів або створення можливості для атак типу “Man-in-the-Middle”.

У практиці безпеки AD CS відіграє ключову роль у впровадженні архітектури Zero Trust, де кожна спроба доступу перевіряється, а автентичність користувача чи пристрою засвідчується за допомогою сертифікатів. У цьому контексті використання короткострокових сертифікатів (наприклад, на кілька годин або днів) і автоматичного відкликання вразливих екземплярів є критичним фактором стійкості до атак.

Крім того, відомі приклади використання слабких налаштувань AD CS у реальних атаках. Наприклад, під час досліджень безпеки, команда SpecterOps виявила, що в багатьох організаціях залишаються активними шаблони сертифікатів з небезпечними параметрами, які дозволяють запитувати сертифікати від імені будь-якого користувача (наприклад, з параметром CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT). Такі конфігурації активно використовувалися під час Red Team-операцій та були визнані критично небезпечними.

Також важливим компонентом є аудит доступу до об’єктів AD CS, зокрема шаблонів сертифікатів і об’єктів CA в Active Directory. Без належного контролю прав доступу до цих об’єктів навіть звичайні користувачі можуть отримати можливість модифікувати політики або ініціювати запити на сертифікати з

підвищеними правами. Це відкриває шлях до атак на основі делегування, зокрема використання механізму Resource-Based Constrained Delegation (RBCD), який дозволяє зловмиснику діяти від імені адміністратора.

З огляду на вищезазначене, роль AD CS в екосистемі безпеки не обмежується видачею сертифікатів — він стає одним із критичних вузлів управління доступом та автентифікацією в доменній інфраструктурі, що вимагає постійного контролю, аудиту та оновлення політик.

Відомо, що багато організацій мають неналежні налаштування AD CS, що дозволяє зловмисникам експлуатувати ці вразливості для проведення атак на внутрішню мережу. Тому AD CS є важливим об’єктом тестування на проникнення, особливо під час перевірки захищеності інфраструктури Active Directory. У наступному розділі буде розглянуто ключові вразливості центру сертифікації та способи їх експлуатації.

Висновки до розділу 1

У цьому розділі було розглянуто основні підходи до оцінювання безпеки корпоративних мереж, включаючи аудит інформаційної безпеки, тестування на проникнення та Red Teaming. Було визначено, що аудит дозволяє оцінити відповідність організації нормативним вимогам та стандартам кібербезпеки, тестування на проникнення використовується для виявлення вразливостей у корпоративній інфраструктурі, а Red Teaming спрямований на перевірку ефективності заходів кіберзахисту та здатності організації до виявлення й протидії загрозам.

Також було розглянуто роль центру сертифікації у корпоративній безпеці. Було визначено, що AD CS є ключовим компонентом інфраструктури відкритих ключів (PKI) у корпоративних середовищах. Він забезпечує управління цифровими сертифікатами, що використовуються для аутентифікації, шифрування даних та контролю доступу. Основними компонентами AD CS є центр сертифікації (CA), шаблони сертифікатів, механізми видачі та

відкликання сертифікатів, а також служби реєстрації та політик сертифікації.

Було розглянуто механізм видачі сертифікатів у AD CS, що базується на запитах CSR, а також інтеграцію з Kerberos через PKINIT, яка дозволяє використовувати сертифікати для аутентифікації користувачів. Особливу увагу було приділено розширеному використанню ключів (EKU), яке визначає можливості використання сертифікатів у корпоративному середовищі.

Хоча AD CS є потужним інструментом для забезпечення безпеки корпоративної мережі, його неналежні налаштування можуть призвести до серйозних ризиків. Неправильна конфігурація центру сертифікації або слабкі шаблони сертифікатів можуть стати вектором атак, що дозволяє зловмисникам отримати несанкціонований доступ до критичних ресурсів. У наступному розділі буде детально проаналізовано відомі вразливості центру сертифікації та методи їх експлуатації.

Розділ 2 ВРАЗЛИВОСТІ ЦЕНТРУ СЕРТИФІКАЦІЇ ТА МЕТОДИ ЇХ ЕКСПЛУАТАЦІЇ

2.1 Вектори атак на центр сертифікації

У процесі тестування на проникнення корпоративних мереж особливу увагу приділяють аналізу захищеності Active Directory, оскільки це рішення є основним механізмом управління ідентифікацією та доступом у корпоративному середовищі. Active Directory містить критичні компоненти, компрометація яких дозволяє зловмисникам отримати контроль над усією мережею. Саме тому тестування на проникнення Active Directory є одним із основних напрямків оцінювання безпеки корпоративних мереж. Взявши за основу етапи проведення тестування на проникнення (рис 1.1), для Active Directory тестування на проникнення та Red Teaming може передбачати наступний шлях компрометації цільового середовища (Kill Chain) [4, 15, 16, 31, 33]:

1. Розвідка та збір інформації (Reconnaissance).

На цьому етапі проводиться отримання інформації про цільову інфраструктуру. В межах тестування на проникнення Active Directory це може включати пасивний збір даних через OSINT, аналіз DNS-записів, взаємодію з мережею через запити NetBIOS, SMB, LDAP або використання внутрішніх джерел інформації. Метою є ідентифікація облікових записів, групових політик, мережевих ресурсів та сервісів, які можуть бути корисними на наступних етапах атаки.

2. Пошук та експлуатація вразливостей (Vulnerability Identification & Exploitation). Після збору базової інформації виконується аналіз наявних вразливостей, які можуть бути використані для початкового доступу до системи. Це може включати атаки на слабкі або повторно використані паролі, експлуатацію неправильно налаштованих дозволів на доступ, використання публічно відомих вразливостей у службах домену, атак на механізми

аутентифікації та політики безпеки.

3. Підвищення привілеїв (Privilege Escalation). Після отримання початкового доступу атакувальники прагнуть розширити свої привілеї у домені. Це може відбуватися через експлуатацію конфігураційних помилок, наприклад, неправильних прав у політиках груп (GPO), небезпечних механізмів делегування привілеїв або використання вразливостей локального та доменного контролю доступу. Отримання привілеїв адміністратора домену відкриває можливості для повного контролю над мережею.

4. Горизонтальне переміщення (Lateral Movement). Після підвищення привілеїв атакувальники шукають способи переміщення мережею та отримання доступу до інших систем. Це може здійснюватися через повторне використання зламаних облікових даних, сеанси RDP, використання WinRM, WMI або інших внутрішніх механізмів аутентифікації для отримання контролю над іншими хостами.

5. Зловживання доменними довірчими відносинами (Cross Trust Attacks). У випадках, коли в корпоративній мережі налаштовані довірчі відносини між різними доменами або навіть лісами Active Directory, зловмисники можуть використовувати це для компрометації інших частин інфраструктури. Це може включати переміщення між доменами, використання наявних облікових даних або сертифікатів, що мають довіру між системами.

На рис. 2.1 наведено схему процесу Kill Chain:

Рис. 2.1. Схема процесу Kill Chain

Тестування AD зазвичай зосереджується на таких аспектах, як слабкі паролі, неправильно налаштовані політики доступу, використання застарілих механізмів аутентифікації та помилки у налаштуванні групових політик (GPO). Проте одним із найбільш недооцінених, але критичних компонентів AD є Active Directory Certificate Services – механізм управління цифровими сертифікатами, що інтегрується з Active Directory та використовується для аутентифікації, шифрування і контролю доступу.

Через те, що AD CS часто не розглядається як основний вектор атак, його налаштування можуть містити вразливості, які дозволяють зловмисникам підвищувати привілеї, пересуватися мережею та закріплюватися в ній. Якщо зловмисник зможе експлуатувати вразливості AD CS, він може: підвищити свої привілеї у домені, отримавши сертифікати для адміністраторських облікових записів; просуватися мережею, використовуючи сертифікати як засіб аутентифікації до різних систем; закріпитися в мережі, створюючи довготривалі методи доступу, які важко виявити. Зважаючи на ці ризики, AD CS є важливим компонентом тестування на проникнення.

Загалом, існує низка векторів атак на Active Directory Certificate Services, які можуть бути використані зловмисниками для компрометації корпоративної мережі. Найбільш дослідженими та поширеними є вразливості підвищення привілеїв, що отримали назву ESC (Enterprise Security Certificates) атаки. Окрім цього, AD CS також може використовуватися для закріплення в мережі (PERSIST), крадіжки облікових даних (THEFT), а також для збереження доступу в домені (DPERSIST). Нижче наведено табл. 2.1, в якій наведено існуючі та працюючі на момент проведення дослідження вектори та вразливості шаблонів сертифікатів та центру сертифікації [4, 6, 12, 14, 36, 38].

Таблиця 2.1.

Вектори атак та вразливості AD CS

Назва вектору	**Призначення**	**Короткий опис**
THEFT1	Крадіжка сертифікатів	Експорт сертифікатів та їхніх закритих ключів за допомогою API Crypto від Windows
THEFT2	Крадіжка сертифікатів	Витягування сертифікатів користувача та закритих ключів за допомогою DPAPI
THEFT3	Крадіжка сертифікатів	Витягування сертифікатів комп'ютера та закритих ключів за допомогою DPAPI
THEFT4	Крадіжка сертифікатів	Крадіжка існуючих сертифікатів на диску

Продовження таблиці 2.1.

Назва вектору	**Призначення**	**Короткий опис**
PERSIST1	Закріплення (Persistence)	Закріплення від імені користувача за допомогою нових запитів на отримання сертифікату
PERSIST2	Закріплення (Persistence)	Закріплення від імені комп’ютера за допомогою нових запитів на отримання сертифікату
PERSIST3	Закріплення (Persistence)	Закріплення від імені користувача або комп’ютера шляхом поновлення сертифіката до закінчення терміну його дії
DPERSIST1	Закріплення в домені (Domain Persistence)	Підробка будь-якого сертифікату в домені, використовуючи вкрадений сертифікат CA Root та приватні ключі
DPERSIST2	Закріплення в домені (Domain Persistence)	Підробка будь-якого сертифікату в домені, використовуючи вкрадений зовнішній Trusted Root сертифікат і приватні ключі
DPERSIST3	Закріплення в домені (Domain Persistence)	Створення Backdoor на CA у вигляді встановлення зловмисних неправильних конфігурацій

Продовження таблиці 2.1.

Назва вектору	**Призначення**	**Короткий опис**
ESC1	Підвищення привілеїв в домені (Domain Privilege Escalation)	Вразливий шаблон сертифікату дозволяє запитувати сертифікат для будь-якого користувача (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT + Client Authentication/Smart Card Logon EKU)
ESC2	Підвищення привілеїв в домені (Domain Privilege Escalation)	Вразливий шаблон сертифікату дозволяє запитувати сертифікат для будь-якого користувача (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT + Any Purpose EKU or no EKU)
ESC3	Підвищення привілеїв в домені (Domain Privilege Escalation)	Запитувач може отримати сертифікат enrollment agent certificate (Application Policy - Certificate Request Agent) і використати його для запиту сертифіката від імені будь-якого користувача (Certificate Request Agent EKU)
ESC4	Підвищення привілеїв в домені (Domain Privilege Escalation)	Вразливі права доступу (ACL – GenericWrite) у шаблонів сертифікатів
ESC5	Підвищення привілеїв в домені (Domain Privilege Escalation)	Вразливі права доступу у центра сертифікації

Продовження таблиці 2.1.

Назва вектору	**Призначення**	**Короткий опис**
ESC7	Підвищення привілеїв в домені (Domain Privilege Escalation)	Вразливі налаштування ролей Certificate Authority Access Control Roles (ManageCA та ManageCertificate) у центрі сертифікації. Дозволяє схвалювати невдалі запити сертифікатів для будь-якого користувача (ESC7 Case 1), або дозволяє зловживати CRL для отримання веб-оболонок віддаленого виконання коду на CA (ESC7 Case 2)
ESC8	Підвищення привілеїв в домені (Domain Privilege Escalation)	Можливість виконувати атаки NTLM Relay до кінцевих точок AD CS HTTP Endpoints, що дозволяє скомпрометувати контролер домену.
ESC11	Підвищення привілеїв в домені (Domain Privilege Escalation)	Можливість виконувати атаки NTLM Relay до кінцевих точок AD CS ICertPassage Remote Protocol (ICPR) RPC Endpoints, що дозволяє скомпрометувати контролер домену

Дані вразливості демонструють, що AD CS може стати критичним вектором атаки, якщо він налаштований неналежним чином. Частина вразливостей, що не була згадана в таблиці, вже була усунена оновленнями безпеки. Наприклад, ESC15 було виправлено останніми оновленнями, тому розглядати його детально недоцільно.

У рамках цього дослідження основний акцент буде зроблено саме на ESC-вразливостях, які безпосередньо пов’язані з неправильною конфігурацією центрів сертифікації та шаблонів сертифікатів. Вразливості AD CS можуть бути поділені на дві основні групи:

- Вразливості шаблонів сертифікатів (ESC1 – ESC4) – виникають через неналежно налаштовані шаблони сертифікатів, які дозволяють зловмисникам отримати сертифікати з підвищеними привілеями.
- Вразливості центру сертифікації (ESC5, ESC7, ESC8, ESC11) – спричинені неправильним налаштуванням прав доступу до служби сертифікації, що дозволяє зловмисникам видавати собі довірені сертифікати або скомпрометувати CA.

Для виявлення всіх вище зазначених вразливостей використовуються інструменти Certify (для OS Windows) або Certipy (для OS Linux), які аналізують наявну інфраструктуру AD CS, зокрема шаблони сертифікатів та центри сертифікації, на наявність неналежних конфігурацій.

Незважаючи на наявність спеціалізованих інструментів для виявлення вразливостей AD CS, практичне виявлення їх експлуатації зловмисниками залишається складним завданням. Це зумовлено тим, що використання сертифікатів у мережі виглядає як легітимна діяльність і рідко викликає підозру з боку засобів виявлення атак. Наприклад, автентифікація через Kerberos PKINIT або доступ до служб із використанням сертифікатів не генерує критичних подій безпеки в журналах, якщо не налаштовано спеціалізованого моніторингу.

Крім того, зловмисники можуть залишатися в мережі протягом тривалого часу, використовуючи видані сертифікати як засіб постійного доступу (persistence), що ускладнює процес реагування на інциденти. Відомі випадки, коли після видалення зламаних облікових записів атакувальники продовжували мати доступ до середовища через збережені сертифікати, що були видані із шаблонів з недостатнім рівнем контролю. У зв’язку з цим, важливим завданням для фахівців з безпеки є налаштування збору та аналізу логів, пов’язаних із виданими сертифікатами, змінами в шаблонах і діями адміністраторів CA.

Особливу небезпеку становлять ті випадки, коли вразливі шаблони дозволяють користувачам самостійно задавати поля сертифікату (наприклад, параметр Subject Alternative Name), що відкриває шлях до підробки особи

іншого користувача, зокрема адміністратора. Якщо при цьому EKU шаблону дозволяє автентифікацію (наприклад, Client Authentication), зловмисник отримує фактично повний доступ до цільових ресурсів від імені привілейованого облікового запису.

Також слід звернути увагу на небезпеку розширених сценаріїв атак, які комбінують вразливості AD CS із іншими компонентами Active Directory. Наприклад, за допомогою атаки типу "Resource-Based Constrained Delegation" (RBCD), зловмисник може налаштувати делегування прав до CA-сервера, якщо має права GenericWrite до об'єкта CA в Active Directory. У поєднанні з ESC5 це відкриває можливості для отримання Kerberos-квитків від імені будь-якого користувача, включно з адміністраторами домену.

З огляду на це, ефективне тестування на проникнення повинно включати не лише ідентифікацію вразливих шаблонів, а й аналіз пов’язаних об'єктів у AD, делегувань прав, логів подій і політик безпеки. Лише комплексний підхід дозволяє оцінити реальний ризик для доменної інфраструктури, пов’язаний із центром сертифікації.

2.2 Вразливості шаблонів сертифікатів

Вразливості шаблонів сертифікатів AD CS є наслідком неправильних налаштувань, що можуть дозволяти низькопривілейованим користувачам запитувати сертифікати від імені інших облікових записів або з розширеними можливостями. Найпоширенішими з них є ESC1, ESC2, ESC3 та ESC4 [8, 10, 25, 31, 37, 39].

ESC1 та ESC2 виникають у випадках, коли шаблон сертифіката має параметр CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT, що дозволяє користувачеві самостійно задавати Subject Alternative Name (SAN). Також зловмиснику необхідно мати права на отримання сертифікату (Enrollment Rights) для вразливого шаблону.

У випадку ESC1, якщо цей параметр комбінується з EKU Client

Authentication або EKU Smart Card Logon, то користувач може запитати сертифікат на ім’я будь-якого іншого облікового запису в домені, включаючи адміністратора. У випадку ESC2, для успішної експлуатації вразливості, у шаблоні не повинно бути встановлено його призначення (Any EKU). Тобто, таким чином, зловмисник також може запитати сертифікат на ім’я будь-якого іншого облікового запису в домені, при цьому вказуючи будь-яке призначення сертифікату. Приклади вразливих шаблонів сертифікатів до ESC1 та ESC2 наведені на рис 2.2 та рис 2.3 відповідно.

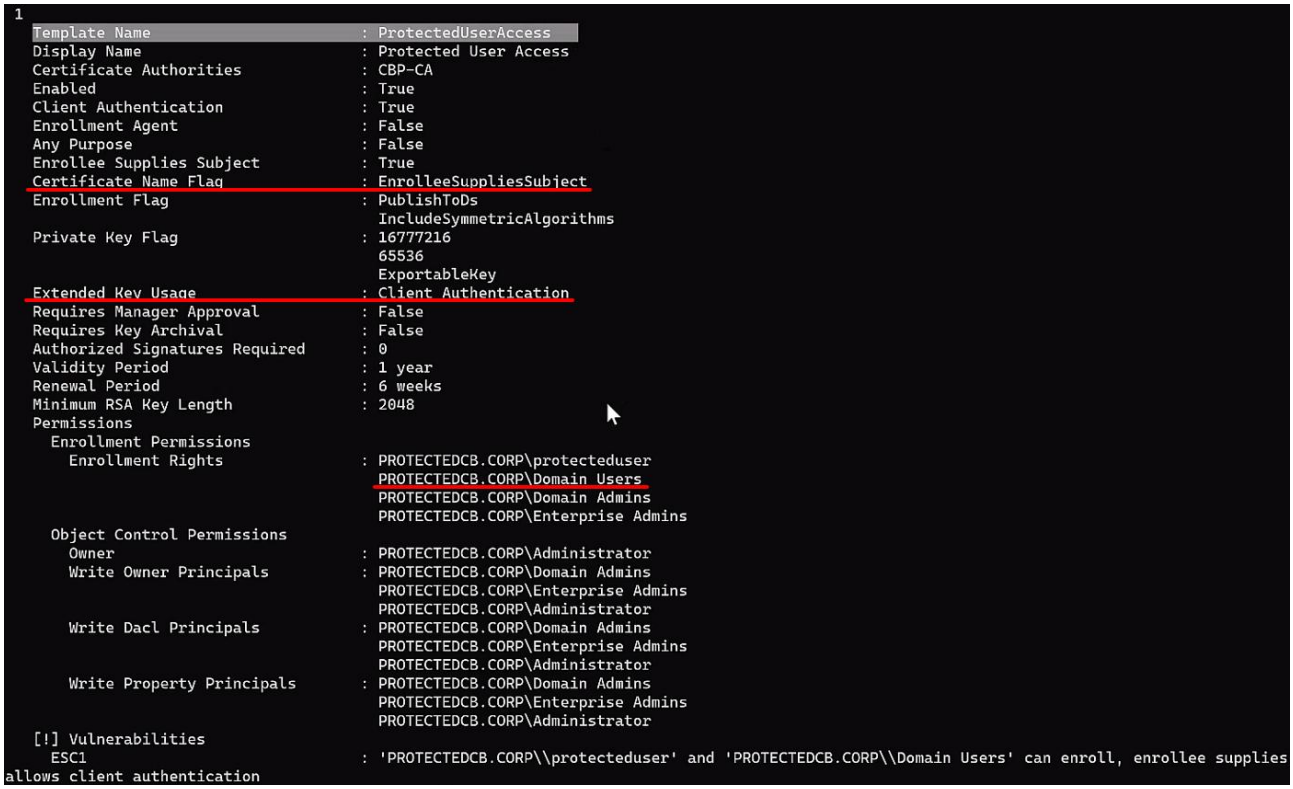

Рис. 2.2. Вразливі конфігурації шаблону до ESC1, які дозволяють отримати сертифікат від імені будь-якого користувача

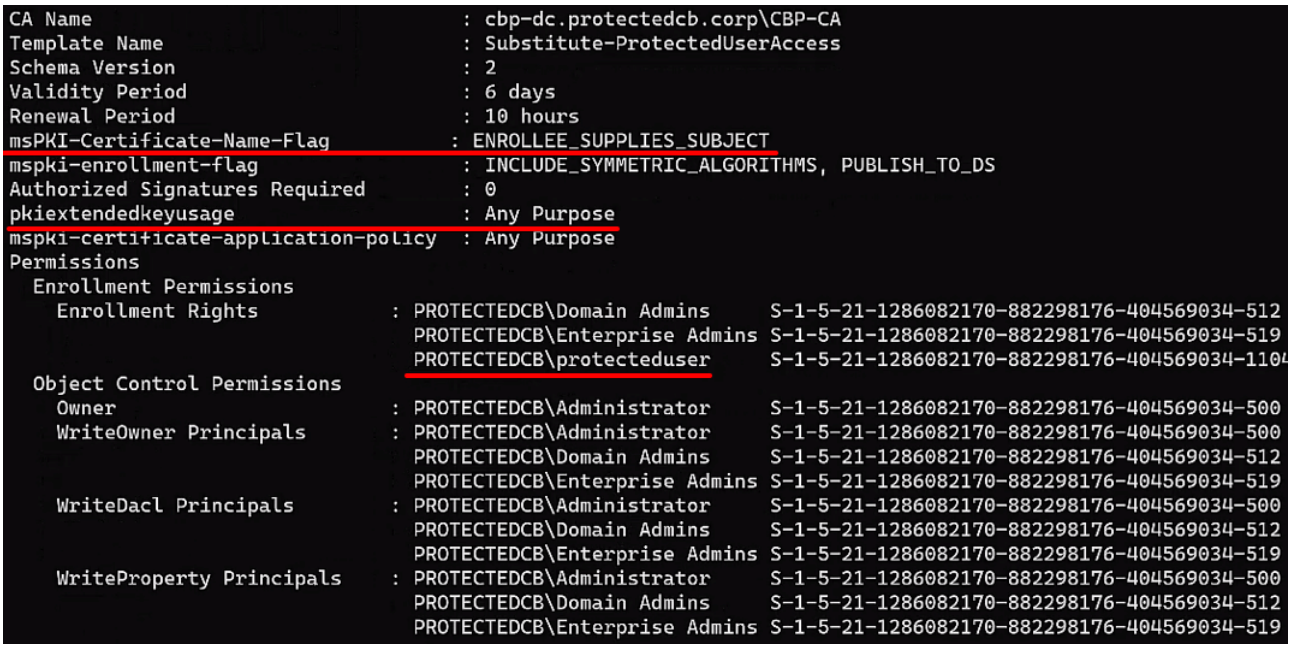

Рис. 2.3. Вразливі конфігурації шаблону до ESC2, які дозволяють отримати сертифікат від імені будь-якого користувача

Для проведення експлуатації даних та подальших вразливостей було використано утиліти Certipy та Certify, що дозволило виконати CSR запити від імені звичайного непривілейованого користувача, в яких було вказано альтернативне ім’я у вигляді імені адміністратора домену.

Команда для експлуатації ESC1 (Certipy):

certipy req -u "ім'я користувача" -hashes "хеш пароля" -dc-ip "IP контролера домену" -target "FQDN CA" -ca "назва CA" -template "назва вразливого шаблону" -upn "альтернативне ім'я користувача, якого необхідно скомпрометувати" -out "місце зберігання сертифікату"

Команда для експлуатації ESC2 (Certify):

Certify.exe request /ca:"FQDN CA"\"назва CA" /template:"вразливий шаблон" /altname:"альтернативне ім'я користувача, якого необхідно скомпрометувати" /domain:"назва домену"

В результаті, було отримано сертифікати адміністраторів домену (рис 2.4, рис 2.5), які зловмисник може використати для проходження аутентифікації через Kerberos PKINIT та виконання подальших атак на домен.

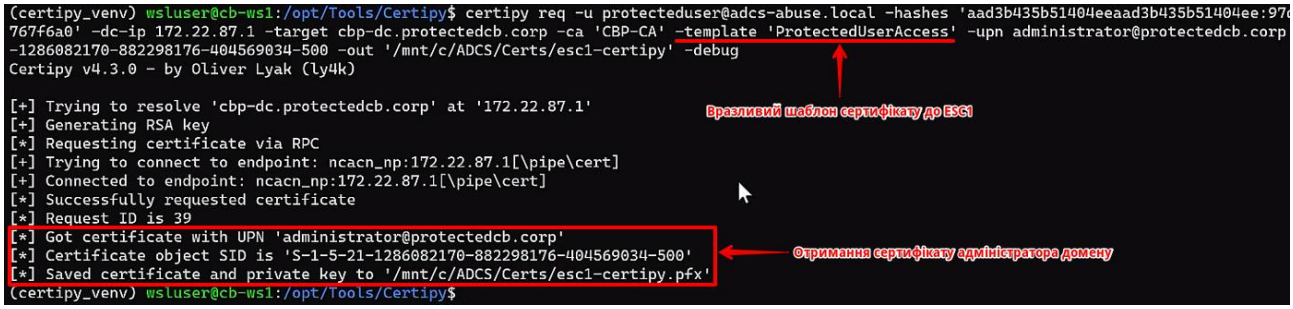

Рис. 2.4. Результат експлуатації вразливості ESC1

Рис. 2.5. Результат експлуатації вразливості ESC2

Вразливість ESC3 пов’язана з можливістю отримання сертифіката Certificate Request Agent, який дозволяє в свою чергу отримувати сертифікати для інших користувачів. Якщо у шаблоні сертифікату встановлено EKU

Certificate Request Agent та для параметру Authorized Signatures Required встановлено значення “0”, зловмисник, отримавши такий сертифікат, може створити новий запит (CSR) на ім’я будь-якого користувача, наприклад, адміністратора домену. Для цього зловмиснику також потрібно знайти інший шаблон сертифікату, який дозволяє використати сертифікат Certificate Request Agent. Такий шаблон сертифікату повинен мати EKU Client Autentciation, а також увімкнений параметр Application Policy Issuance Requirement зі значенням Authorized Signatures Required.

Як і попередні вразливості, це дозволяє зловмиснику отримати сертифікати від імені привілейованих облікових записів та використовувати їх для проходження аутентифікації в домені.

Приклади необхідних шаблонів сертифікатів до експлуатації ESC3 наведений на рис 2.6 та рис 2.7.

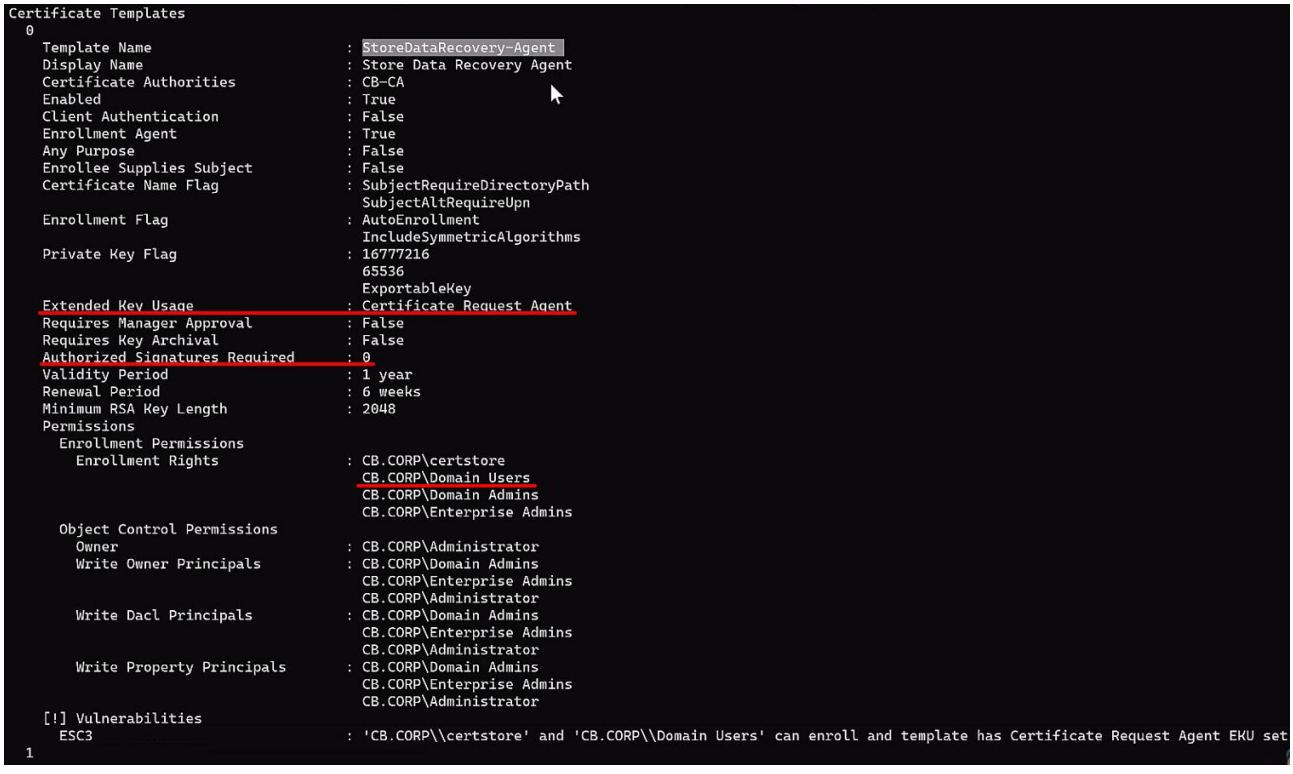

Рис. 2.6. Шаблон сертифікату Certificate Request Agent, який необхідний для експлуатації ESC3

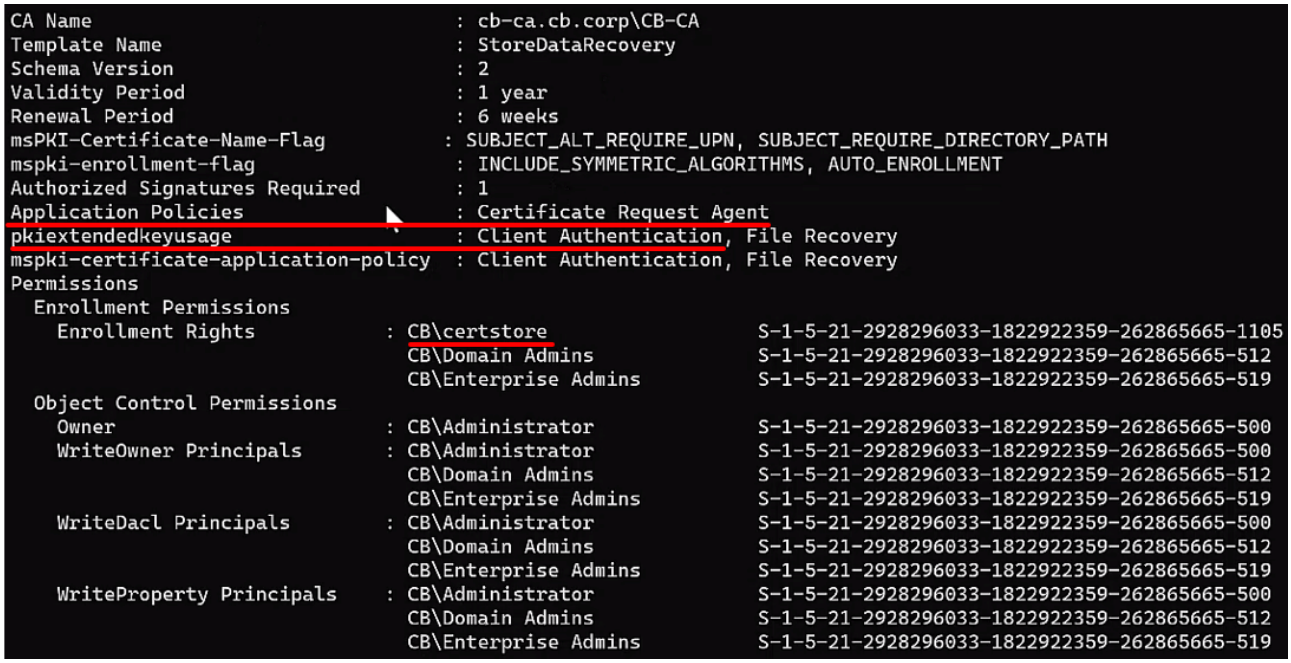

Рис. 2.7. Шаблон сертифікату, який необхідний для використання сертифікату Certificate Request Agent та експлуатації ESC3

Для початку виконаємо запит на отримання сертифікату Certificate Request Agent (рис 2.8).

Команда для отримання сертифікату Certificate Request Agent (Certipy):

certipy req -u "ім'я користувача" -hashes "хеш пароля" -dc-ip "IP контролера домену" -target "FQDN CA" -ca "назва CA" -template "назва шаблону сертифікату Certificate Request Agent" -upn "альтернативне ім'я користувача, якого необхідно скомпрометувати" -out "місце зберігання сертифікату"

Рис. 2.8. Отримання сертифікату Certificate Request Agent

Після цього необхідно використати отриманий сертифікат для запиту нового сертифікату від імені адміністратора домену (рис 2.9).

Команда для отримання сертифікату адміністратора домену (Certipy):

certipy req -u "ім'я користувача" -hashes "хеш пароля" -dc-ip "IP контролера домену" -target "FQDN CA" -ca "назва CA" -template "назва необхідного шаблону сертифікату" -on-behalf-of "домен\ім'я користувача, якого необхідно скомпрометувати" -pfx "шлях до розташування сертифікату Certificate Request Agent" -out "місце зберігання сертифікату" -timeout 30

Рис. 2.9. Результат експлуатації вразливості ESC3

Вразливість ESC4 стосується неправильно налаштованих прав доступу ACLs (Access Control Lists) на шаблонах сертифікатів. Якщо низькопривілейований користувач має право GenericWrite або FullControl на шаблон сертифіката, він може змінити його конфігурацію. Ця вразливість дозволяє зловмиснику редагувати наявні вразливі шаблони сертифікатів та зробити їм вразливими до інших вразливостей, зокрема таких як ESC1, ESC2 та ESC3.

Приклад вразливого шаблону до ESC4 наведено на рис 2.10.

Рис. 2.10. Вразливі конфігурації шаблону до ESC4, які дозволяють низькопривілейованому користувачу вносити зміни в шаблон

Утиліта Certipy дозволяє в автоматичному режимі виконати модифікацію шаблону та зробити його вразливим до ESC1 (рис 2.11).

Команда для автоматичної модифікації вразливого шаблону до ESC4 (Certipy):

certipy template -u "ім'я користувача" -hashes "хеш пароля" -template "вразливий шаблон до ESC4"

Рис. 2.11. Експлуатація вразливості ESC4 для отримання вразливого шаблону до ESC1

Після цього відкривається можливість експлуатація вразливості ESC1 через модифікований шаблон сертифікату, що в результаті дозволяє отримати сертифікат адміністратора домену (рис 2.12).

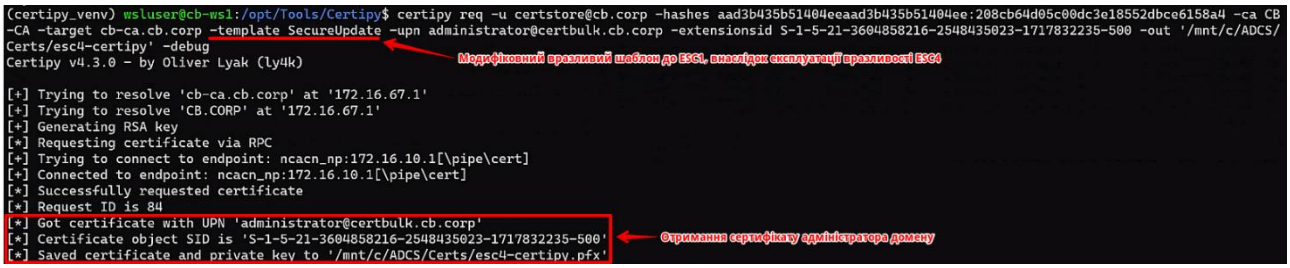

Рис. 2.12. Експлуатація вразливості ESC1, внаслідок модифікації вразливого шаблону до ESC4

2.3 Вразливості центру сертифікації

Окрім проблем із шаблонами сертифікатів, існує низка критичних вразливостей, пов’язаних із самим центром сертифікації.

Наприклад, вразливість ESC5 пов’язана з неналежними налаштуваннями прав доступу на об’єкті сервера сертифікації (CA Server Object) в Active Directory. Якщо зловмисник має права GenericWrite або GenericAll на об’єкті сервера CA, він може змінювати його атрибути, що відкриває можливості для атак на делегування прав доступу. Одним із поширених сценаріїв є використання атрибуту msDS-AllowedToActOnBehalfOfOtherIdentity, що дозволяє налаштувати ресурсно-обмежене делегування (RBCD) та видавати квитки Kerberos від імені будь-якого користувача. У випадку компрометації сервера CA це дозволяє зловмиснику отримати повний контроль над AD CS і виконати подальшу компрометацію домену. Оскільки сервери сертифікації

часто мають підвищені привілеї у домені, компрометація CA може слугувати точкою подальшого просування зловмисника мережею. Приклад наявності у звичайного користувача привілеїв GenericWrite до об'єкта CA наведено на рис. 2.13.

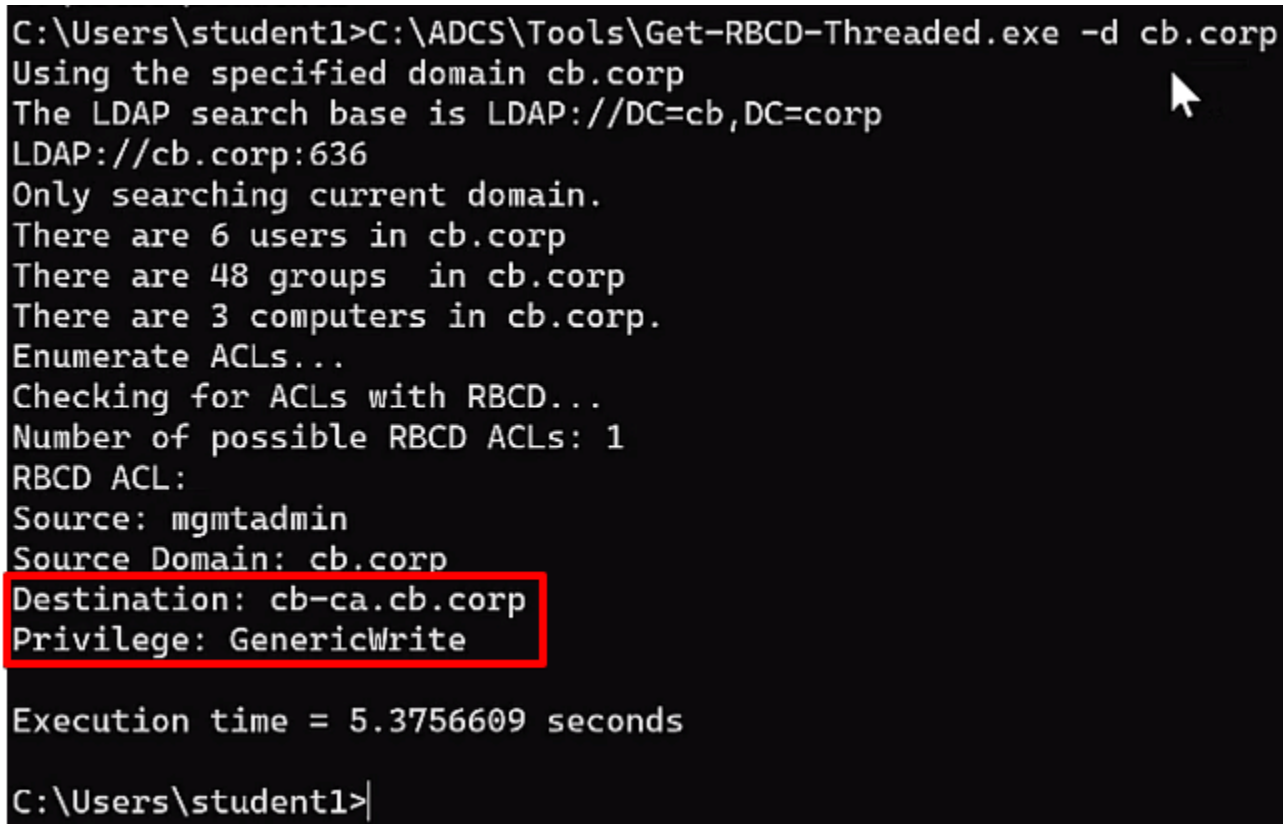

Рис. 2.13. Вразливі конфігурації CA до ESC5

Для експлуатації даної вразливості також необхідно попередньо створити обліковий запис машини (рис 2.14), що може бути реалізовано за допомогою утиліти Impacket.

Рис. 2.14. Створення облікового запису машини для подальшої експлуатації ESC5

Далі, для зловживання функцією RBCD та експлуатації ESC5, необхідно записати SID новоствореного облікового запису в атрибуті msDS-AllowedToActOnBehalfOfOtherIdentity центру сертифікації (рис. 2.15).

Команда для експлуатації вразливості ESC5 (Impacket):

python3 /opt/Tools/rbcdattack/rbcd.py -dc-ip "IP контролера домену" -t "назва CA" -f "назва облікового запису машини" -hashes "хеш паролю користувача, котрий має права ESC5" "домен\ім'я користувача, користувача, котрий має права ESC5

Рис. 2.15. Експлуатація вразливості ESC5

В результаті, за рахунок зловживання функції RBCD, зловмисник матиме змогу отримати віддалене виконання команд на сервері центру сертифікації від імені адміністратора (рис 2.16).

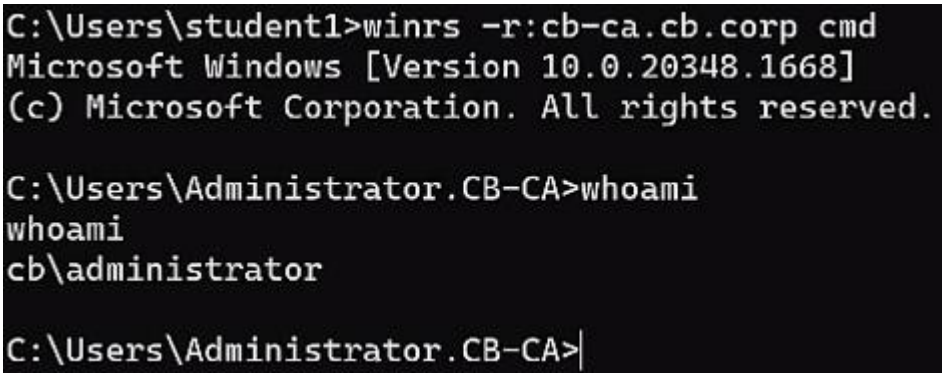

Рис. 2.16. Отримання RCE на центрі сертифікації від імені адміністратора

Вразливість ESC7 виникає через неправильні налаштування ролей доступу до центру сертифікації та дозволяє зловмиснику отримати контроль над процесом видачі сертифікатів або навіть виконати віддалений код на сервері CA.

У першому випадку, якщо зловмисник має роль ManageCertificates, він може затверджувати запити на видачу сертифікатів, навіть якщо вони не були схвалені автоматично. Це дозволяє зловмиснику погодити власний запит на отримання сертифікату для будь-якого облікового запису у домені, включно з

адміністраторами.

У другому випадку, якщо зловмисник має роль ManageCA, він може маніпулювати списками відкликаних сертифікатів (CRL), зловживаючи можливістю завантажувати або змінювати файли на сервері сертифікації. Це відкриває шлях до завантаження шкідливих файлів або створення веб-оболонок, що забезпечують виконання довільного коду (RCE) без необхідності отримання локального доступу до сервера CA. Вразливість ESC7 є критичною, оскільки дозволяє зловмиснику отримати контроль над сервером CA, що може спричинити масштабні наслідки для безпеки всієї корпоративної мережі. Приклад наявності у звичайного користувача ролей ManageCertificates та ManageCA та наведено на рис. 2.17.

```
Certificate Authorities
  0
    CA Name                             : CB-CA
    DNS Name                            : cb-ca.cb.corp
    Certificate Subject                 : CN=CB-CA, DC=cb, DC=corp
    Certificate Serial Number           : 51F5AA83C01B57B34635410A3738E79D
    Certificate Validity Start          : 2023-01-11 12:46:01+00:00
    Certificate Validity End            : 2028-01-11 12:56:01+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : INTERNALCB.CORP\Administrators
      Access Rights
        Enroll                          : INTERNALCB.CORP\Authenticated Users
                                          INTERNALCB.CORP\internaluser
        ManageCertificates              : S-1-5-21-2928296033-1822922359-262865665-512
                                          S-1-5-21-2928296033-1822922359-262865665-519
                                          INTERNALCB.CORP\Administrators
                                          INTERNALCB.CORP\internaluser
        ManageCa                        : S-1-5-21-2928296033-1822922359-262865665-512
                                          S-1-5-21-2928296033-1822922359-262865665-519
                                          INTERNALCB.CORP\Administrators
                                          INTERNALCB.CORP\internaluser
    [!] Vulnerabilities
      ESC7                              : 'INTERNALCB.CORP\\internaluser' has dangerous permissions
```

Рис. 2.17. Вразливі конфігурації CA до ESC7

Для прикладу, було розглянуто експлуатацію вразливості ESC7 Case 1, яка полягала у створенні невдалого запиту на отримання сертифікату від імені адміністратора домену (рис 2.18) та його погодженні.

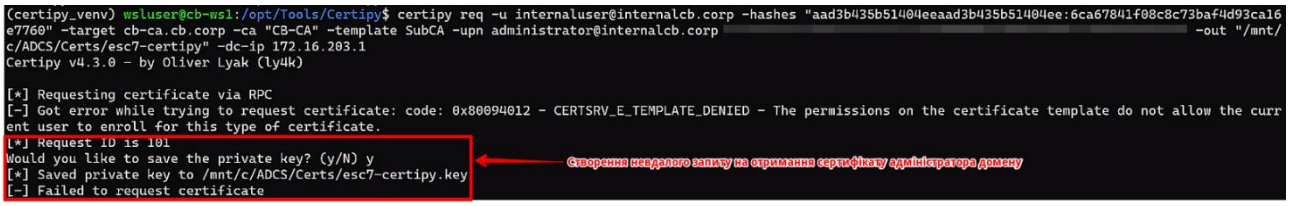

Рис. 2.18. Створення невдалого запиту на отримання сертифікату адміністратора домену

В подальшому, через наявність у низькопривілейованого користувача прав ManageCertificates, було погоджено невдалий запит та отримано сертифікат адміністратора домену (рис 2.19).

Команда для погодження невдалого запиту на отримання сертифікату адміністратора домену (Certipy):

certipy ca -u "ім'я користувача з правами ManageCertificates" -hashes "хеш паролю користувача" -ca "назва CA" -issue-request "ID невдалого запиту" -dc-ip "IP контролера домену" -target "FQDN CA"

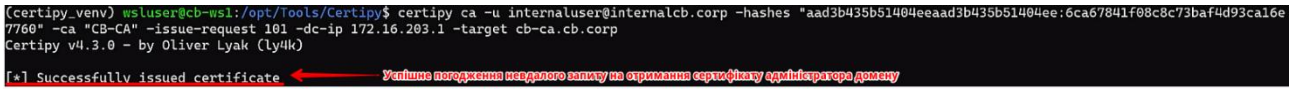

Рис. 2.19. Експлуатація вразливості ESC7.1

Вразливості ESC8 та ESC11 пов’язані з можливістю виконання NTLM Relay-атак на різні компоненти Active Directory Certificate Services, що дозволяє зловмиснику отримати підвищені привілеї або навіть повний контроль над доменом.

ESC8 виникає через можливість виконання NTLM Relay-атаки на веб-служби AD CS, зокрема на Certificate Enrollment Web Services (CES) та Certificate Enrollment Policy Web Services (CEP), які працюють по HTTP. Якщо ці служби не використовують розширені механізми захисту такі як підтримка підпису NTLM, зловмисник може використовувати Coerce-атаки для виконання примусової аутентифікації високопривілейованого облікового запису до вразливого сервісу. Це дозволяє зловмиснику видавати собі сертифікат цього облікового запису, зокрема контролера домену. Успішна експлуатація цієї

вразливості призводить до можливості аутентифікації в мережі від імені високопривілейованого користувача, отримання доступу до критичних ресурсів та подальшого горизонтального переміщення мережею.

ESC11 є подібною до ESC8, але вона використовує інший механізм атаки – NTLM Relay на ICertPassage Remote Protocol (ICPR), який обробляється через інтерфейси RPC. Вразливість полягає у тому, що функція “Enforce Encryption for Requests”, яка вимагає використання підпису для пакетів (шифрування запитів), є вимкненою (по замовчуванню увімкнена). В результаті, служба не вимагає підпису та не запобігає повторному використанню NTLM-хешів, що дозволяє зловмиснику виконати атаку типу relay та отримати сертифікат облікового запису контролера домену, як і під час експлуатації вразливості ESC8.

У випадку обох вразливостей успішна експлуатація може призвести до компрометації всієї доменної інфраструктури. Приклади наявності вразливих конфігурацій центрів сертифікації до ESC8 та ESC11 наведено на рис 2.20.

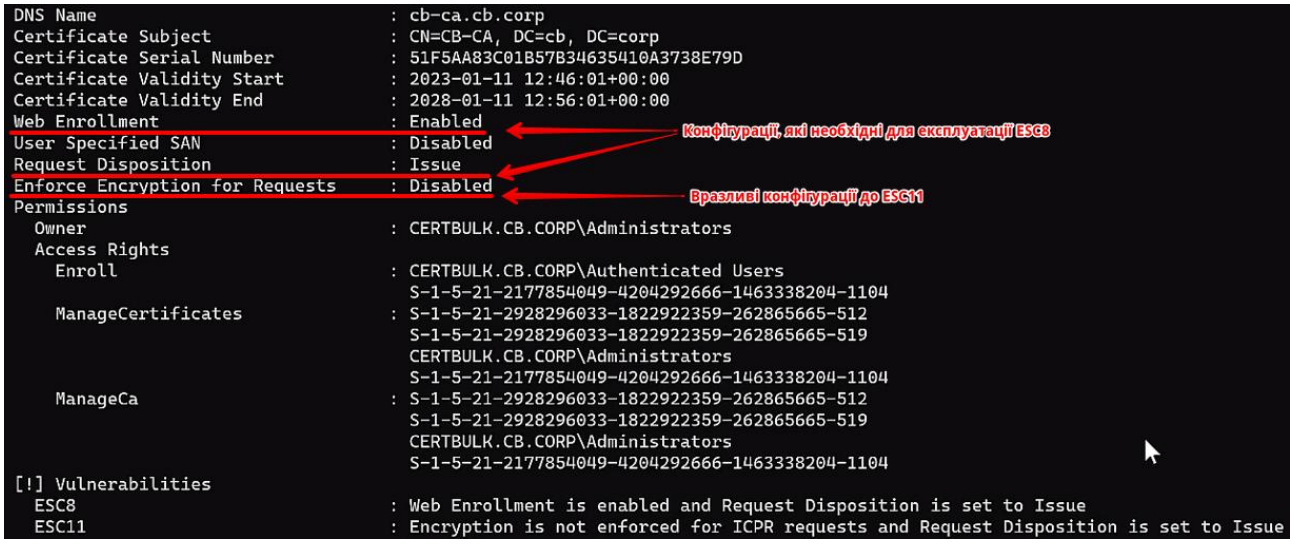

Рис. 2.20. Вразливі конфігурації CA до ESC8 та ESC11

Для експлуатації даних вразливостей необхідно виконати Coerce-атаку на контролер домену (рис 2.21), що дозволяє виконати його примусову аутентифікацію на системі зловмисника, де в свою чергу, за допомогою утиліти ntlmrelayx, буде виконано NTLM Relay атаку, яка в свою чергу дозволяє

передати облікові дані контролеру домену до вразливих кінцевих точок на центрі сертифікації. В результаті, було отримано сертифікат контролеру домену (рис 2.22).

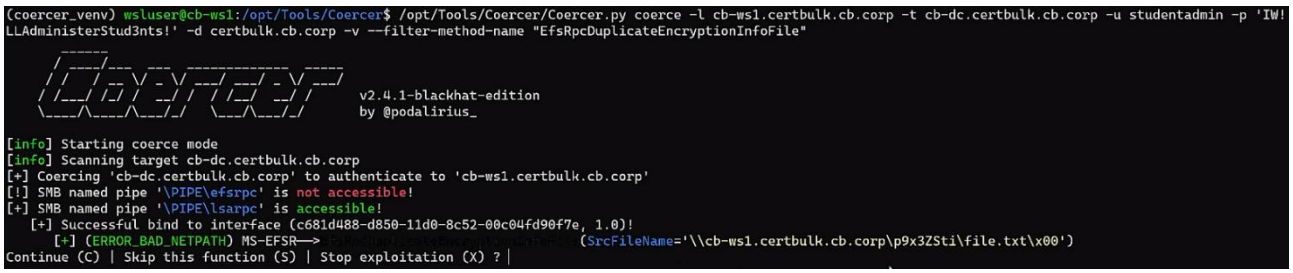

Рис. 2.21. Виконання Coerce-атаки на контролер домену

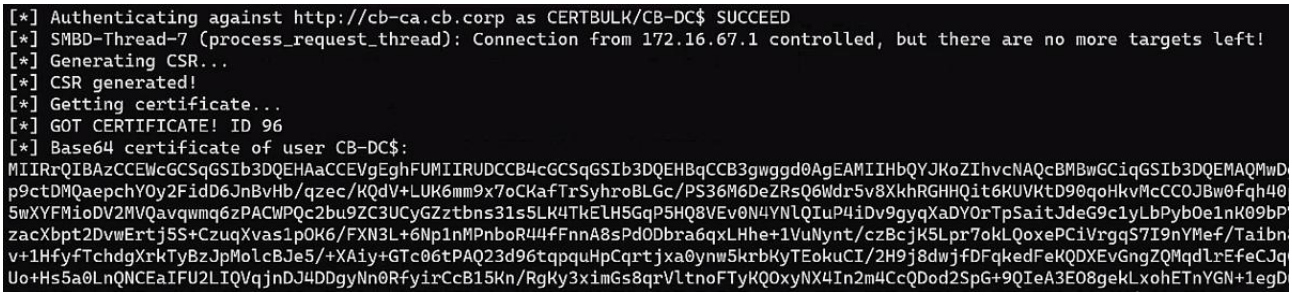

Рис. 2.22. Отримання сертифікату контролера домену внаслідок NTLM Relay атаки

Висновки до розділу 2

У цьому розділі було проведено детальний аналіз вразливостей Active Directory Certificate Services, що можуть використовуватися зловмисниками для підвищення привілеїв у домені, переміщення мережею та закріплення в середовищі. Було розглянуто основні вектори атак, включаючи ESC (Enterprise Security Certificates), PERSIST, THEFT та DPERSIST, які зловмисники можуть використовувати для компрометації корпоративної інфраструктури.

Було встановлено, що AD CS може стати критичною точкою у безпеці корпоративних мереж через неналежні налаштування шаблонів сертифікатів та прав доступу до центрів сертифікації. Найбільш небезпечні вразливості належать до двох категорій: вразливості шаблонів сертифікатів (ESC1 – ESC4), що дозволяють низькопривілейованим користувачам отримувати сертифікати від імені привілейованих облікових записів, та вразливості центрів сертифікації

(ESC5, ESC7, ESC8, ESC11), що можуть призвести до повного компрометування AD CS [10, 19, 20, 21, 31, 35, 39].

Для кожної з виявлених вразливостей було розглянуто механізми їх експлуатації, включаючи використання інструментів Certipy та Certify, які дозволяють виконувати аналіз конфігурацій AD CS, автоматично отримувати сертифікати та здійснювати атаки на центр сертифікації. Було продемонстровано, що неправильні налаштування центрів сертифікації та їхніх компонентів можуть дозволити зловмисникам отримати доступ до облікових записів адміністраторів домену, виконувати NTLM Relay-атаки, маніпулювати списками сертифікатів та навіть досягати віддаленого виконання коду на сервері центру сертифікації.

Особливу увагу було приділено вразливостям ESC1 – ESC4, які стосуються шаблонів сертифікатів. Було показано, що внаслідок їхньої експлуатації зловмисники можуть запитувати сертифікати для будь-яких облікових записів у домені та аутентифікуватися через Kerberos PKINIT. Також увагу було приділено вразливостям ESC5, ESC7, ESC8 та ESC11, які пов’язані з неналежними налаштуваннями самого центру сертифікації, що відкриває можливості для атак на делегування доступу, компрометації серверів сертифікації та NTLM Relay-атак на контролери домену.

У результаті дослідження було встановлено, що експлуатація вразливостей AD CS може бути критичною для безпеки корпоративних мереж.

Розділ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ЦЕНТРУ СЕРТИФІКАЦІЇ

3.1 Рекомендації щодо усунення вразливостей центру сертифікації

Усунення вразливостей в Active Directory Certificate Services є критично важливим для забезпечення безпеки корпоративної інфраструктури. Основні заходи щодо захисту включають належну конфігурацію центрів сертифікації, аудит налаштувань шаблонів сертифікатів, обмеження доступу та оновлення програмного забезпечення [1, 2, 3, 9, 11, 18, 20, 22, 23, 26, 29, 32, 35].

Зміцнення інфраструктури AD CS та центру сертифікації базується на рекомендаціях Microsoft, зокрема:

- Securing PKI – офіційні рекомендації з безпеки для інфраструктури відкритих ключів (PKI) Microsoft PKI Security.
- AD Security Guidance – специфічні рекомендації щодо захисту AD CS AD CS Security Guidance.

Перш за все, сервери сертифікації повинні розглядатися як активи рівня Tier 0, аналогічно до контролерів домену, оскільки компрометація CA може призвести до повного захоплення домену. Це передбачає суворе обмеження доступу до CA та його конфігурації, використання окремих привілейованих облікових записів для адміністрування, а також мінімізацію кількості користувачів, які можуть взаємодіяти з CA.

Одним із найважливіших заходів є належна конфігурація шаблонів сертифікатів. Вразливості ESC1, ESC2 та ESC3 виникають через можливість низькопривілейованих користувачів запитувати сертифікати від імені інших облікових записів. Для усунення цих проблем необхідно провести повний аудит шаблонів сертифікатів, перевіривши їхні параметри на наявність критичних налаштувань, таких як CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT, який дозволяє запитувачу самостійно задавати Subject Alternative Name (SAN). Якщо цей параметр увімкнено у шаблонах, що містять EKU Client Authentication або

Smart Card Logon, необхідно або змінити їхні права доступу, або видалити ці шаблони.

Окрему увагу слід приділити шаблонам з EKU Any Purpose або тим, у яких взагалі відсутні обмеження на використання сертифіката. Вони створюють загрозу, оскільки дозволяють видачу сертифікатів для будь-якого користувача без додаткових перевірок. Для усунення цих ризиків рекомендується видалити небезпечні шаблони або змінити їхню конфігурацію таким чином, щоб лише довірені групи могли їх використовувати. Ще однією вразливістю є ESC3, яка виникає, коли у шаблоні сертифіката встановлено EKU Certificate Request Agent без вимоги до цифрового підпису авторизованого підписанта. Це дозволяє зловмиснику отримати сертифікат, який у свою чергу може бути використаний для запиту інших сертифікатів від імені будь-якого користувача. Усунути цю вразливість можна, додавши вимогу про обов'язковий цифровий підпис при видачі таких сертифікатів або повністю заборонивши використання шаблонів Certificate Request Agent без відповідного контролю. Окрім цього, необхідно перевірити права доступу до шаблонів сертифікатів. Якщо звичайний користувач має права GenericWrite або FullControl до шаблону, він може змінювати його параметри та зробити вразливим до інших атак, таких як ESC1, ESC2 або ESC3. Це створює ризик несанкціонованої ескалації привілеїв, тому такі права необхідно прибрати. Для цього слід переглянути список дозволів через властивості кожного шаблону та обмежити їх лише адміністраторам або спеціальним групам користувачів, яким дійсно необхідно отримувати ці сертифікати.

Ще одним важливим напрямом зміцнення безпеки є впровадження регулярного процесу ревізії всіх налаштувань центрів сертифікації. Ревізія має охоплювати не лише параметри шаблонів сертифікатів, а й відповідність ключовим політикам безпеки, таким як мінімальний набір прав доступу, принцип найменших привілеїв (Least Privilege), обмеження видимості шаблонів у каталозі (Publication Settings), використання криптографічно стійких алгоритмів (наприклад, RSA 4096 біт або ECDSA) та актуальність термінів дії

сертифікатів. Забезпечення коротших термінів дії сертифікатів дозволяє зменшити потенційне вікно для експлуатації скомпрометованого сертифіката.

Також важливо впровадити політику періодичного ротаційного оновлення ключів (Key Rollover) для центра сертифікації, що дає змогу уникнути тривалого використання одного й того ж ключа, який у разі компрометації може стати вектором широкомасштабної атаки. Ротація ключів повинна супроводжуватись обов'язковим оновленням відповідних сертифікатів, переконфігурацією шаблонів та синхронізацією з NtAuthCertificates у лісі Active Directory.

Крім того, однією з потенційних загроз, які варто враховувати, є неконтрольоване делегування адміністрування центру сертифікації. У деяких організаціях адміністратори можуть надавати додаткові ролі або розширені повноваження без належного аудиту. Рекомендується розробити й затвердити чітку політику доступу, що регламентує, хто саме має право змінювати конфігурації CA, а також вести облік змін у складі адміністраторських груп (Audit Trail), використовуючи засоби централізованого моніторингу та журналювання (наприклад, через SIEM-системи).

Окрім проблем із шаблонами сертифікатів, велике значення мають вразливості, що пов'язані з самим центром сертифікації. Вразливість ESC5 виникає через неналежні налаштування прав доступу до об'єкта сервера сертифікації (CA Server Object) в Active Directory. Якщо зловмисник має права GenericWrite або GenericAll на цей об'єкт, він може змінювати його атрибути, зокрема додавати записи у msDS-AllowedToActOnBehalfOfOtherIdentity. Це дозволяє налаштувати ресурсно-обмежене делегування (RBCD) та видавати квитки Kerberos від імені будь-якого користувача, що може призвести до повного компрометування сервера сертифікації та домену. Щоб запобігти цьому, слід переглянути права доступу до об'єкта CA в Active Directory, видаливши всі зайві записи та залишивши лише необхідні адміністраторські привілеї. Іншою критичною вразливістю є ESC7, яка виникає через неналежні налаштування ролей доступу в центрі сертифікації. Якщо зловмисник має роль

ManageCertificates, він може затверджувати невдалі запити на видачу сертифікатів, що дозволяє йому отримати сертифікат від імені будь-якого користувача, зокрема адміністратора домену. Якщо ж зловмисник має роль ManageCA, він може маніпулювати списками відкликаних сертифікатів (CRL), зловживаючи можливістю завантажувати або змінювати файли на сервері сертифікації. Це відкриває шлях до завантаження шкідливих файлів або створення веб-оболонок, що забезпечують виконання довільного коду (RCE) на сервері. Усунути цю вразливість можна, переглянувши ролі доступу в CA та прибравши зайві дозволи у користувачів, яким вони не потрібні. Особливо слід звернути увагу на те, щоб звичайні користувачі не мали можливості схвалювати запити на отримання сертифікатів.

Окрему категорію складають вразливості, пов’язані з атаками NTLM Relay. Вразливості ESC8 та ESC11 використовують можливість виконання NTLM Relay-атак на веб-служби AD CS та інтерфейси RPC, що дозволяє зловмиснику отримати підвищені привілеї або навіть повний контроль над доменом. Захист від таких атак включає кілька заходів. По-перше, слід встановити оновлення KB5014754 від Microsoft, яке посилює перевірку аутентифікації на основі сертифікатів та запобігає атакам relay через веб-сервіси AD CS. Після встановлення цього оновлення необхідно налаштувати параметр StrongCertificateBindingEnforcement у режимі Full Enforcement, щоб забезпечити максимальний рівень захисту. По-друге, слід вимкнути підтримку NTLM-аутентифікації в AD CS, використовуючи NTLM Blocking або застосовуючи Extended Protection Authentication (EPA). Якщо веб-служби AD CS (CEP та CES) не є критично важливими, їх слід вимкнути. Якщо ж вони необхідні, слід перевести їх на використання виключно HTTPS та увімкнути розширений захист аутентифікації. Для усунення вразливості ESC11 необхідно повністю вимкнути інтерфейси RPC, які вважають застарілими. Додатково рекомендується налаштувати фільтрацію трафіку таким чином, щоб доступ до AD CS мав лише обмежений список серверів і користувачів.

Крім того, можна використовувати техніки PREVENT, представлені в

дослідженні Certified Pre-Owned від SpecterOps, які структуровано охоплюють різні аспекти безпеки AD CS (табл. 3.1) [12, 25, 36].

Таблиця 3.1.

Вектори запобігання вразливостей AD CS

Вектор запобігання	**Короткий опис**
PREVENT1	Трактування серверів CA як Tier 0 активів та обмеження доступу лише для адміністраторів. Це запобігає можливості компрометації CA низькопривілейованими користувачами.
PREVENT2	Захист налаштувань CA шляхом обмеження прав Manage CA та Manage Certificates, а також вимкнення небезпечних параметрів у реєстрі.
PREVENT3	Проведення аудиту всіх опублікованих шаблонів сертифікатів, видалення небезпечних та зайвих шаблонів.
PREVENT4	Посилення налаштувань шаблонів сертифікатів: вимкнення CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT, обмеження прав Enrollment, додавання адміністративного затвердження запитів.

Продовження таблиці 3.1.

Вектор запобігання	Короткий опис
PREVENT5	Перевірка NtAuthCertificates, що містять довірені сертифікати, оскільки вони можуть використовуватись для видачі нових сертифікатів зловмисниками.
PREVENT6	Захист приватних ключів CA шляхом використання HSM (Hardware Security Modules) або апаратних токенів, що унеможливлює їх крадіжку.
PREVENT7	Строгий контроль відповідності користувачів їхнім сертифікатам, зокрема обмеження на мапування сертифікатів до облікових записів AD.
PREVENT8	Захист HTTP Enrollment Endpoint: вимкнення NTLM, увімкнення SSL/TLS, впровадження захисту від NTLM Relay-атак.

3.2 Заходи щодо моніторингу та виявлення атак на центр сертифікації

Забезпечення безпеки Active Directory Certificate Services неможливе без ефективного моніторингу та своєчасного виявлення атак [24, 25]. Оскільки компрометація AD CS може призвести до повного контролю над корпоративною мережею, важливо використовувати журнали подій Windows, інструменти аналізу та спеціалізовані механізми спостереження за активністю у системі. Основу моніторингу становить аудиту подій у Windows Event Log. Першочергово слід активувати відповідні журнали за допомогою Group Policy: *Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Object Access → Audit Certification Services*, встановивши параметри Success та Failure. Це дозволить фіксувати події, що можуть свідчити про спроби зловживання AD CS.

Для детектування атак рекомендується відстежувати ключові події в журналах безпеки Windows [11, 13, 19, 22, 29]:

- ID 4886 – запит на сертифікат;
- ID 4887 – видача сертифіката;
- ID 4898 – завантаження нового шаблону сертифікатів;
- ID 4899 – модифікація шаблону сертифікатів;
- ID 4900 – зміна прав доступу до шаблону сертифікатів;
- ID 4768 – запит квитка аутентифікації Kerberos (PKINIT);
- ID 4769 – запит сервісного квитка Kerberos;
- ID 4624 – успішна аутентифікація з використанням сертифікатів;
- ID 4648 – спроба входу в систему із зазначенням облікових даних

Особливо важливим є виявлення аномальної активності, яка може вказувати на атаку. Наприклад, потрібно перевіряти запити сертифікатів із підозрілими атрибутами, такими як Subject Alternative Name (SAN), що використовується для отримання сертифікатів від імені інших облікових записів (ESC1, ESC2). Для цього застосовується команда *Get-CertRequest -HasSAN* у PSPKIAudit.

Іншим важливим напрямком моніторингу є контроль за змінами в налаштуваннях CA. Наприклад, події ID 4890, 4891, 4892 сигналізують про зміну конфігурації центру сертифікації, що може вказувати на компрометацію або спробу впровадження бекдору. Також слід контролювати ID 5058, 5061, 5059, які можуть свідчити про спроби експортування закритих ключів сертифікатів (крадіжка ключів DPAPI).

Моніторинг аутентифікації за допомогою сертифікатів є критичним компонентом виявлення атак. Для цього необхідно контролювати використання PKINIT (4768) та Schannel (4769, 4648, 4624). Аномальні входи, такі як використання сертифікатів високопривілейованих облікових записів на нових пристроях або швидке використання сертифіката після видачі, можуть вказувати на атаку Pass-the-Cert або використання викрадених сертифікатів (THEFT5).

Ще одним ключовим аспектом є виявлення змін у сертифікатах, що використовуються для входу в систему. Наприклад, якщо адміністратор або високопривілейований користувач несподівано отримує новий сертифікат, це може бути спроба закріплення у системі (PERSIST1, PERSIST2). Для цього рекомендується порівнювати видані сертифікати з використаними для аутентифікації (EID 4768, 4624).

Додатково можна впровадити методи активного виявлення, такі як DETECT-техніки, рекомендовані в дослідженні Certified Pre-Owned від SpecterOps (табл. 3.2) [12, 25, 36].

Таблиця 3.2.

Вектори виявлення атак на AD CS

Вектор виявлення	**Короткий опис**
DETECT1	Моніторинг реєстрації сертифікатів для користувачів та машин. Дозволяє виявити підозрілі запити сертифікатів.
DETECT2	Виявлення аутентифікації за допомогою сертифікатів. Використовується для аналізу підозрілих логонів через PKINIT або Schannel.
DETECT3	Контроль подій резервного копіювання CA. Відстежує спроби збереження критичних даних CA (ID 4876, 4877).
DETECT4	Виявлення змін у шаблонах сертифікатів. Використовується для моніторингу подій 4899 та 4900, що вказують на зміну політик видачі сертифікатів.
DETECT5	Виявлення доступу до зашифрованих ключів DPAPI. Дозволяє знайти спроби зловмисників отримати доступ до закритих ключів користувачів або CA.

Продовження таблиці 3.2.

Вектор виявлення	Короткий опис
DETECT6	Використання honey credentials. Створення підроблених сертифікатів у критичних директоріях дозволяє виявити зловмисників при спробах використання.
DETECT7	Моніторинг змін у конфігурації AD CS, включаючи модифікацію ACL CA, що може вказувати на атаку.

Висновки до розділу 3

У цьому розділі було розглянуто заходи щодо підвищення безпеки корпоративних мереж шляхом усунення вразливостей Active Directory Certificate Services (AD CS) та впровадження механізмів моніторингу і виявлення атак. Детальний аналіз методів захисту підтвердив, що ефективна безпека AD CS можлива лише за умови комплексного підходу, що включає як превентивні заходи, так і системи активного моніторингу. Рекомендації щодо усунення вразливостей AD CS були спрямовані на виправлення помилок у налаштуваннях шаблонів сертифікатів та самого центру сертифікації. Основними заходами було виділено аудит та модифікацію шаблонів сертифікатів для усунення потенційних шляхів ескалації привілеїв, таких як ESC1, ESC2 та ESC3. Було наголошено на важливості обмеження доступу до шаблонів, видалення небезпечних конфігурацій та застосування вимоги до цифрового підпису сертифікатів. Для підвищення захисту центрів сертифікації розглянуто усунення ESC5 та ESC7 шляхом обмеження прав доступу до CA Server Object, а також посилення контролю над процесом видачі сертифікатів. Особливу увагу приділено захисту від атак NTLM Relay, які можуть використовувати вразливості ESC8 та ESC11, для чого рекомендовано впровадження StrongCertificateBindingEnforcement та розширеної

аутентифікації EPA. Для системного підходу до безпеки AD CS було використано методику PREVENT, розроблену SpecterOps. Запропоновані техніки охоплюють критичні аспекти захисту: трактування серверів CA як Tier 0 активів, аудит та посилення конфігурацій шаблонів сертифікатів, обмеження доступу до критичних компонентів інфраструктури та впровадження апаратного захисту ключів. Другий напрямок підвищення безпеки AD CS стосувався моніторингу та виявлення атак. Було розглянуто критичні журнали подій Windows, які дозволяють ідентифікувати зловживання механізмами сертифікації, включаючи підозрілі запити сертифікатів (ID 4886, 4887), модифікацію шаблонів (ID 4898–4900), зміну конфігурацій CA (ID 4890–4892) та несанкціоноване використання сертифікатів (ID 4768, 4624). Моніторинг PKINIT та Schannel аутентифікації дозволяє виявити потенційне використання викрадених сертифікатів або атаки Pass-the-Cert. Додатково запропоновано виявлення аномальних змін у шаблонах сертифікатів, використання honey credentials та контроль змін у конфігураціях AD CS. Таким чином, впровадження запропонованих заходів дозволяє значно зменшити ризики компрометації AD CS, запобігти атакам на центр сертифікації та своєчасно ідентифікувати потенційні загрози. Комплексний підхід до усунення вразливостей у поєднанні з активним моніторингом є ключовим фактором захисту інфраструктури відкритих ключів у корпоративному середовищі.

Крім стандартного аудиту Windows, рекомендується інтеграція AD CS із системами SIEM (Security Information and Event Management), такими як Microsoft Sentinel, Splunk, ArcSight або QRadar. Ці системи дозволяють не лише централізувати збір логів, але й реалізовувати правила кореляції подій, виявляючи складні шаблони поведінки, що вказують на компрометацію. Наприклад, комбінація подій видачі сертифікатів (ID 4887), запитів PKINIT (ID 4768) та входу адміністратора (ID 4624) за короткий проміжок часу може сигналізувати про використання вкраденого або зловживаного сертифіката.

Також важливо впровадити поведінковий аналіз користувачів (User and Entity Behavior Analytics, UEBA), який дозволяє виявляти нетипову активність, наприклад, коли звичайний користувач раптово отримує доступ до критичних ресурсів або часто запитує сертифікати протягом короткого часу. Поведінкові моделі можуть допомогти ідентифікувати lateral movement – переміщення атакувальника мережею за допомогою сертифікатів, що складно виявити за допомогою тільки традиційного логування.

Додатково рекомендується налаштувати моніторинг дій адміністраторів AD CS, зокрема операцій із керування ролями, завантаженням CRL та резервного копіювання. Це дає змогу вчасно виявити внутрішні загрози або компрометацію облікових записів з високими привілеями.

Іншим корисним заходом є створення honey-користувачів або honey-сертифікатів — приманок, що ніколи не повинні використовуватись у реальних сценаріях. Їх доступ чи активація однозначно свідчать про зловмисну активність у мережі. Такі техніки дозволяють швидко виявляти розвідку або спроби ескалації привілеїв у сертифікаційній інфраструктурі.

Усі описані методи, як класичні (журнали подій), так і сучасні (SIEM, UEBA, honey-техніки), створюють багаторівневу систему виявлення атак, яка підвищує загальну стійкість PKI до компрометацій. Їхнє комбіноване застосування дозволяє виявляти не лише відомі техніки, але й нові, ще не задокументовані способи зловживання службою сертифікації.

ВИСНОВКИ

Досліджено основні підходи до оцінювання безпеки корпоративних мереж, зокрема аудит інформаційної безпеки, тестування на проникнення та Red Teaming. Встановлено, що ефективне оцінювання кібербезпеки передбачає комплексний підхід, що поєднує відповідність стандартам та здатність організації виявляти й запобігати атакам. Проаналізовано роль Active Directory Certificate Services у корпоративній безпеці та встановлено, що AD CS є критичним елементом інфраструктури відкритих ключів, який забезпечує керування сертифікатами для аутентифікації та шифрування. Визначено, що неналежна конфігурація AD CS створює ризики, які можуть бути використані для компрометації домену.

Виокремлено основні вразливості AD CS, зокрема пов’язані з шаблонами сертифікатів (ESC1 – ESC4) та налаштуванням центрів сертифікації (ESC5, ESC7, ESC8, ESC11). Встановлено, що їхня експлуатація дозволяє зловмисникам отримувати підвищені привілеї, обходитись без паролів, переміщуватися мережею та закріплюватися у системі. Обґрунтовано небезпеку атак на AD CS, які можуть призвести до компрометації всієї мережі.

Розроблено рекомендації щодо усунення вразливостей, які включають аудит та посилення конфігурацій шаблонів сертифікатів, обмеження доступу до CA, впровадження захисту від NTLM Relay-атак. Визначено, що усунення ESC1 – ESC3 можливе шляхом заборони CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT та обмеження прав доступу до критичних шаблонів. Запропоновано заходи для мінімізації ризиків ESC5 шляхом обмеження прав доступу до CA Server Object. Доведено необхідність впровадження Extended Protection Authentication для захисту від атак NTLM Relay.

Проаналізовано методи моніторингу AD CS, виокремлено ключові події Windows Event Log, що дозволяють виявляти загрози. Встановлено, що моніторинг критичних подій дозволяє своєчасно реагувати на спроби

компрометації. Обґрунтовано важливість аналізу PKINIT та Schannel для виявлення атак на сертифікати.

Визначено, що ефективний захист AD CS можливий лише за умови поєднання превентивних заходів та активного моніторингу. Обґрунтовано доцільність використання методик PREVENT та DETECT, які охоплюють основні аспекти захисту та моніторингу. Запропоновано практичні рекомендації щодо регулярного аудиту AD CS, використання сучасних методів моніторингу та автоматизованого аналізу загроз. Впровадження запропонованих заходів дозволяє значно знизити ризики компрометації AD CS, запобігти атакам на центр сертифікації та своєчасно виявляти потенційні загрози, забезпечуючи безпеку корпоративної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. iIT Distribution Україна. Найкращі практики ефективного управління вразливостями. iIT Distribution Україна. URL: https://iitd.ua/najkrashhi-praktiki-efektivnogo-upravlinnya-vrazlivostyami/ (дата звернення: 21.04.2025).

2. My IT Specialist. Максимальний захист Active Directory з Tenable Identity Exposure. My IT Specialist. URL: https://my-itspecialist.com/safeguarding-active-directory-with-tenable-identity-exposure (дата звернення: 21.04.2025).

3. Microsoft. Огляд Microsoft Defender for Identity та його можливості. Microsoft Learn. URL: https://learn.microsoft.com/uk-ua/defender-for-identity/what-is (дата звернення: 21.04.2025).

4. Artur Marzano. ADCS Attack Techniques Cheatsheet. URL: https://docs.google.com/spreadsheets/d/1E5SDC5cwXWz36rPP_TXhhAvTvqz2RGnMYXieu4ZHx64 (date of access: 21.04.2025).

5. CSO Online. Active Directory Certificate Services a big security blindspot. CSO Online. URL: https://www.csoonline.com/article/570879/report-active-directory-certificate-services-a-big-security-blindspot-on-enterprise-networks.html (date of access: 21.04.2025).

6. Cybersensus. Active Directory Certificate Services— Part 1. Medium. URL: https://medium.com/@yury.xisto/active-directory-certificate-services-part-1-53cdec63961e (date of access: 21.04.2025).

7. Encryption Consulting. Understanding Active Directory Certificate Services. Encryption Consulting. URL: https://www.encryptionconsulting.com/understanding-active-directory-certificate-services/ (date of access: 21.04.2025).

8. Encryption Consulting. Mitigating ESC1 and ESC8 Vulnerability in Active Directory. Encryption Consulting Blog. URL: https://www.encryptionconsulting.com/mitigating-esc1-and-esc8-vulnerability-in-active-directory/ (date of access: 21.04.2025).

9. GitHub. Certify. GitHub Repository. URL: https://github.com/GhostPack/Certify (date of access: 21.04.2025).

10. GitHub. Certipy: Tool for Exploiting Active Directory Certificate Services. GitHub Repository. URL: https://github.com/ly4k/Certipy (date of access: 21.04.2025).

11. GitHub. PSPKIAudit: Security Auditing for Active Directory Certificate Services. GitHub Repository. URL: https://github.com/GhostPack/PSPKIAudit (date of access: 21.04.2025).

12. GlobalSign. Active Directory Certificate Services: What Is It & Why Should I Use It? GlobalSign Blog. URL: https://www.globalsign.com/en/blog/what-is-active-directory-certificate-services (date of access: 21.04.2025).

13. Google Cloud. Defend Against the Latest Active Directory Certificate Services Threats. Google Cloud Blog. URL: https://cloud.google.com/blog/topics/threat-intelligence/defend-ad-cs-threats (date of access: 21.04.2025).

14. Gradenegger U. Limits of Microsoft Active Directory Certificate Services. Uwe Gradenegger's Blog. URL: https://www.gradenegger.eu/en/limits-of-the-microsoft-active-directory-certificate-services/ (date of access: 21.04.2025).

15. HackTheBox. Active Directory Pentesting: Cheatsheet and Beginner Guide. HackTheBox Blog. URL: https://www.hackthebox.com/blog/active-directory-penetration-testing-cheatsheet-and-guide (date of access: 21.04.2025).

16. Microsoft. Active Directory Certificate Services Documentation. Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/ (date of access: 21.04.2025).

17. Microsoft. Active Directory Certificate Services Overview. Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview (date of access: 21.04.2025).

18. Microsoft. Best Practices for Securing Active Directory. Microsoft Docs. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory (date of access: 21.04.2025).

19. Microsoft. Configure sensors for AD FS, AD CS, and Microsoft Entra Connect. Microsoft Learn. URL: https://learn.microsoft.com/en-us/defender-for-identity/deploy/active-directory-federation-services (date of access: 21.04.2025).

20. Microsoft. Identify insecure AD CS certificate enrollment IIS endpoints (ESC8). Microsoft Learn. URL: https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-insecure-adcs-certificate-enrollment (date of access: 21.04.2025).

21. Microsoft. KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS). Microsoft Support. URL: https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429 (date of access: 21.04.2025).

22. Microsoft. Microsoft Defender for Identity now detects suspicious certificate usage. Microsoft Tech Community. URL: https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/microsoft-defender-for-identity-now-detects-suspicious-certificate-usage/3743335 (date of access: 21.04.2025).

23. Microsoft. Securing PKI: Best Practices for Implementing a Microsoft Windows Server 2022 Public Key Infrastructure. Microsoft Docs. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/pki-design-considerations (date of access: 21.04.2025).

24. Microsoft. What is Microsoft Defender for Identity? Microsoft Tech Community. URL: https://techcommunity.microsoft.com/t5/microsoft-threat-protection-blog/microsoft-defender-for-identity-expands-its-coverage-with-new-ad/ba-p/3894215 (date of access: 21.04.2025).

25. NCC Group. Defending Your Directory: An Expert Guide to Fortifying Active Directory Certificate Services (ADCS) Against Exploitation. NCC Group. URL: https://www.nccgroup.com/us/research-blog/defending-your-directory-an-expert-guide-to-fortifying-active-directory-certificate-services-adcs-against-exploitation/ (date of access: 21.04.2025).

26. Netwrix. Active Directory Certificate Services: Risky Settings and How to Remediate Them. Netwrix Blog. URL: https://blog.netwrix.com/2021/08/24/active-directory-certificate-services-risky-settings-and-how-to-remediate-them/ (date of access: 21.04.2025).

27. NinjaOne. Active Directory Certificate Services: AD CS Explanation & Configuration. NinjaOne Blog. URL: https://www.ninjaone.com/blog/active-directory-certificate-services-definition-configuration/ (date of access: 21.04.2025).

28. NIST. Guidelines for Public Key Infrastructure (PKI) Implementation. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-32.pdf (date of access: 21.04.2025).

29. Palo Alto Networks. Detecting Active Directory Certificate Services Abuse with Cortex XDR. Palo Alto Networks Blog. URL: https://www.paloaltonetworks.com/blog/security-operations/detecting-active-directory-certificate-services-abuse-with-cortex-xdr/ (date of access: 21.04.2025).

30. Raj Chandel's Blog. Active Directory Pentesting Using Netexec Tool: A Complete Guide. URL: https://www.hackingarticles.in/active-directory-pentesting-using-netexec-tool-a-complete-guide/ (date of access: 21.04.2025).

31. RedFox Security. Exploiting Active Directory Certificate Services (AD CS). RedFox Security Blog. URL: https://redfoxsec.com/blog/exploiting-active-directory-certificate-services-ad-cs/ (date of access: 21.04.2025).

32. Redmond Magazine. Microsoft Defender for Identity Adds More Certificate Abuse Detections. Redmond Magazine. URL: https://redmondmag.com/Articles/2023/08/16/Microsoft-Defender-for-Identity-Certificate-Abuse.aspx (date of access: 21.04.2025).

33. SecureLayer7. Exploring, Exploiting Active Directory Pen Test. SecureLayer7 Blog. URL: https://blog.securelayer7.net/exploring-exploiting-active-directory-pen-test/ (date of access: 21.04.2025).

34. SecureW2. Active Directory Certificate Services (AD CS): Explained. SecureW2 Blog. URL: https://www.securew2.com/blog/active-directory-certificate-services-ad-cs-explained (date of access: 21.04.2025).

35. Sectigo. Navigating the complexities: challenges in Microsoft AD CS and the role of automation. Sectigo Resource Library. URL: https://www.sectigo.com/resource-library/navigating-the-complexities-challenges-in-microsoft-ad-cs-and-the-role-of-automation (date of access: 21.04.2025).

36. SpecterOps. Certified Pre-Owned: Abusing Active Directory Certificate Services. SpecterOps Whitepaper. URL: https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf (date of access: 21.04.2025).

37. TAC Security. Understanding and Mitigating Active Directory Certificate Services (AD CS) Vulnerabilities. TAC Security Blog. URL: https://tacsecurity.com/understanding-and-mitigating-active-directory-certificate-services-ad-cs-vulnerabilities/ (date of access: 21.04.2025).

38. The Hacker Recipes. Certificate Services (AD-CS). The Hacker Recipes. URL: https://www.thehacker.recipes/ad/movement/adcs/ (date of access: 21.04.2025).

39. TrustFoundry. Understanding Active Directory Certificate Services: A Focus on ESC1 and ESC8. TrustFoundry Blog. URL: https://trustfoundry.net/2024/08/19/understanding-active-directory-certificate-services-a-focus-on-esc1-and-esc8/ (date of access: 21.04.2025).

40. Vaadata. Active Directory (AD) Pentesting: Objective & Methodology. Vaadata Blog. URL: https://www.vaadata.com/blog/active-directory-pentesting-objective-methodology-black-box-and-grey-box-tests/ (date of access: 21.04.2025).