ВДОСКОНАЛЕННЯ МЕТОДИКИ АКТИВНОГО АУДИТУ СЛУЖБИ ACTIVE DIRECTORY WINDOWS SERVER

Вакуленко Д.В., Добринін І.С.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: danyil.vakulenko@nure.ua,
ihor.dobrynin@nure.ua

Abstract

Active Directory is currently the most popular solution for building domain networks. This report is aimed to cover the questions related to the unique development of the methodology for active audit of Active Directory service using the newest Windows Server 2019 update. The ISO family of standards, the COBIT 2019 standard and pentest methodologies, which eventually became a kind of basis for this development, were also reviewed. This work can be used during the audit of Windows Server from the perspective of a penetration tester, to improve the security of the company that uses the domain controller.

У сучасному світі захист інформації з кожним днем стає все більшим трендом. Важливість безпеки стає особливо важливою в корпоративних мережах, які працюють під управлінням контролерів домену Active Directory Domain Services (AD DS). Контролери домену Active Directory (AD) є точкою автентифікації користувачів та єдиною точкою налаштувань групових політик безпеки корпоративної мережі [1], що викликає підвищений інтерес із боку зловмисників саме до контролерів домену Active Directory.

Безумовно, з метою запобігання потенційних зловмисних дій треба вживати певних заходів щодо забезпечення сталої роботи контролерів домену. Одним із варіантів своєчасного виявлення вразливостей є апріорне проведення аудиту як корпоративної мережі в цілому, так і контролерів домену зокрема. У доповіді пропонується підхід щодо активного аудиту контролерів домену зі встановленою службою Active Directory Domain Services.

Треба зазначити, що питанням аудиту наразі приділяється достатньо уваги. Так, наприклад, один із найкращих світових стандартів з питань забезпечення інформаційної безпеки – ISO/IEC 27001:2022 визначає, що організації повинні в заплановані терміни проводити аудити систем управління інформаційною безпекою та їхніх елементів для встановлення рівня відповідності цілей заходів безпеки нормативним вимогам [2]. Проте, проведений авторами аналіз відомих стандартів з питань аудиту [2 – 5] показав, що вони мають, як правило, декларативний характер та не надають методологічного підходу до проведення аудиту, зокрема аудиту контролерів домену Active Directory.

З метою реалізації процедури активного аудиту контролерів домену Active Directory пропонується наступний підхід, який налічує шість основних кроків.

1) Проведення розвідки, або сканування.

В запропонованому підході даний пункт передбачає сканування машин на виявлення вразливостей та у використанні інструментів для MITM-атак, якщо аудит проводиться першою стороною.

2) Побудова можливих векторів атак та експлуатація вразливостей.

Даний крок використовується після знаходження деяких вразливостей, виявлених під час попереднього кроку, або, наприклад, після отримання облікових даних користувачів, які зберігаються на контролері домену Active Directory.

3) Постексплуатаційна діяльність (Post-Exploitation).

На даному етапі використовуються інструменти та техніки, що визначені матрицею MITTRE Attack [6] для того, щоб авторизуватися на скомпрометованій машині.

4) Доступ до облікового запису адміністратора (Lateral Movement).

На даному етапі відбувається отримання більш вагомих прав за рахунок доступу до облікового запису адміністратора та отримання контролю над іншими системами корпоративної мережі.

5) Domain Dominance.

Даний етап є останнім перед створення звіту. Він включає в себе заволодіння повним контролем над доменом та отриманням якомога більшої кількості інформації.

6) Створення звіту про результати аудиту.

7) Аналіз виявлених проблем та внесення пропозицій щодо їхнього усунення.

Слід зазначити, що запропонована методика базується на підході зазначеному в [5], але доповнює та вдосконалює відомий підхід.

Запропонована методика протестована у віртуальному середовищі. Для цього використовувалась частина корпоративної мережі під управлінням контролера домена Active Directory із 3-х машини (2 Windows та одна Kali). Схема мережі, яка підлягала тестуванню, надана на рис.1.

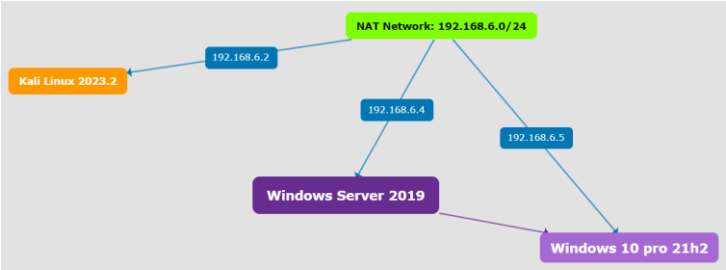

Рис. 2. Схема досліджуваного осередка корпоративної мережі

Результати активного аудиту за запропонованою методикою показали, що запропонована методика не суперечить відомим підходам до проведення активного аудиту, проте дозволяє отримати більш повні результати вразливостей контролерів домену Active Directory. Отримані в наслідок реалізації активного аудиту результати використовуватимуться для мінімізації вразливостей контролерів домену Active Directory

Результати цієї роботи доцільно використовувати під час створення та перевірки функціонування корпоративних мереж, які працюють під управлінням контролерів домену Active Directory з урахуванням вимог безпеки.

Література

1. Identity and Access documentation URL: https://learn.microsoft.com/en-us/windows-server/identity/identity-and-access (дата звернення: 07.11.2023).

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 07.11.2023).

3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/standard/75652.html (дата звернення: 10.11.2023).

4. ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing. URL: https://www.iso.org/standard/77802.html (дата звернення: 10.11.2023).

5. Windows Active Directory Audit/Assurance Program. URL: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoF8EAK (дата звернення: 31.10.2023).

6. ATTA&CK Matrix for Enterprise. URL: https://attack.mitre.org (дата звернення: 10.11.2023).

7. Вакуленко Д. В. Перспективи розвитку Інфокомунікацій та інформаційно-вимірювальних технологій. *Пропозиції щодо використання SPLUNK для аналізу функціонування інформаційних систем* : матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті» м. Харків, 10 – 12 травня 2023 р., Харків : ХНУРЕ, 2023. С. 84 – 85.