Маркеєв Б.В., магістрант
Фальковський І. Г., ст. викладач
Державний університет «Житомирська політехніка»

ТИПИ АТАК НА ДОМЕННИЙ КОНТРОЛЕР ТА ШЛЯХИ ЇХ ЗАПОБІГАННЯ

Доменний контролер (DC) – це ключовий елемент інфраструктури Active Directory (AD), що забезпечує автентифікацію, авторизацію та централізоване управління доступом. Через критичну роль у мережі він є головною мішенню для зловмисників, а його компрометація може призвести до повного контролю над IT-інфраструктурою організації.

Серед поширених атак на DC виділяють Pass-the-Hash, Golden Ticket, DCSync, Kerberoasting. Наприклад, Golden Ticket дозволяє створювати квитки Kerberos із повними правами адміністратора, а DCSync використовує привілеї "Replicating Directory Changes" для імітації реплікації AD, що дозволяє зловмиснику отримати хеші паролів користувачів, зокрема адміністраторів. Інструменти на кшталт Mimikatz значно спрощують отримання паролів і хешів навіть у захищених середовищах. Реальні випадки атак на корпорації свідчать про необхідність впровадження комплексних заходів захисту.

Основні методи безпеки включають мінімізацію привілеїв, ізоляцію DC у сегментованих VLAN, регулярне оновлення ПЗ та багатофакторну автентифікацію (MFA). Обмеження доступу до реплікації Active Directory мінімізує ризик DCSync атак. Важливим є моніторинг активності за допомогою Microsoft Defender for Identity, Advanced Threat Analytics (ATA), що дозволяє виявляти загрози на ранніх стадіях.

Серед сучасних рішень виділяється Credential Guard, який ізолює облікові дані від несанкціонованого доступу, ефективно захищаючи від Pass-the-Hash атак. Для запобігання Golden Ticket атак необхідно регулярно оновлювати пароль облікового запису KRBTGT. Додаткові заходи, такі як аудит адміністраторських облікових записів та обмеження доступу до критичних даних, суттєво знижують ризики компрометації.

Сучасні підходи до безпеки, зокрема Zero Trust, передбачають перевірку кожного запиту на доступ незалежно від його джерела. Використання штучного інтелекту (AI) в системах безпеки, як-от Microsoft Sentinel, дозволяє аналізувати великий обсяг логів та виявляти підозрілі взаємозв’язки. Інструменти PingCastle та BloodHound стали стандартом для виявлення вразливостей та аналізу можливих векторів атак.

Ефективний захист доменних контролерів вимагає комплексного підходу, що включає контроль облікових записів, моніторинг трафіку, застосування сучасних технологій на кшталт AI та Zero Trust моделі. Використання спеціалізованих інструментів аналізу дозволяє виявляти та блокувати загрози на ранніх етапах, що критично важливо для забезпечення кібербезпеки корпоративної інфраструктури.

Список використаних джерел:

1. Active Directory Security Best Practices. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers (дата звернення: 21.03.2025).
2. Pass-the-Hash (PtH) Attacks and Mitigation Strategies. *Microsoft.* URL: https://www.microsoft.com/en-us/download/details.aspx?id=36036 (дата звернення: 21.03.2025).
3. Microsoft Defender for Identity. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/defender-for-identity/ (дата звернення: 21.03.2025).
4. Credential Guard Overview. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard (дата звернення: 21.03.2025).
5. Zero Trust Security Model. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/security/zero-trust/ (дата звернення: 21.03.2025).
6. Golden Ticket and DCSync Attacks on Active Directory. *Mandiant Threat Intelligence.* URL: https://www.mandiant.com/resources/blog/active-directory-attacks (дата звернення: 21.03.2025).
7. PingCastle – Active Directory Security Assessment. *PingCastle.* URL: https://www.pingcastle.com/ (дата звернення: 21.03.2025).
8. Mimikatz and DCSync Attacks. *AdSecurity.* URL: https://adsecurity.org/?page_id=1821 (дата звернення: 21.03.2025).
9. Microsoft Sentinel Documentation. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/azure/sentinel/ (дата звернення: 21.03.2025).
10. BloodHound – Active Directory Analysis Tool. *BloodHound Docs.* URL: https://bloodhound.readthedocs.io/en/latest/ (дата звернення: 21.03.2025).