Шитов Є.А., магістрант
Фальковський І. Г., старший викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ АТАК НА АКТИВНІ ДОМЕННІ КОНТРОЛЕРИ ТА ПІДХОДІВ ДО ЇХ ЗАХИСТУ

В умовах сучасних кіберзагроз доменні контролери (DC), які є ключовим компонентом інфраструктури Active Directory (AD), залишаються однією з основних цілей кіберзлочинців. Атаки на доменні контролери можуть призводити до повної компрометації мережі організації, тому аналіз методів атак і механізмів захисту має критичне значення для забезпечення безпеки інформаційної інфраструктури.

У ході дослідження проведено класифікацію основних методів атак на доменні контролери. Одним із ключових напрямів є атаки на облікові записи з високими привілеями, як-от облікові записи адміністраторів домену. Зловмисники часто застосовують методи Pass-the-Hash та Pass-the-Ticket [2] для отримання несанкціонованого доступу до ресурсів, обходячи механізми автентифікації.

Другий напрямок атак включає компрометацію NTLM-хешів і Kerberos-квитків. Особливо небезпечними є атаки Golden Ticket та Silver Ticket,[1] які дозволяють тривалий час залишатися в мережі з найвищими привілеями.

Ще одним важливим методом атак є експлуатація механізмів реплікації каталогів, коли інструменти на кшталт DCSync дозволяють зловмисникам отримати доступ до хешів паролів усіх користувачів, зокрема адміністраторів.

Дослідження також охопило вплив людського фактора на безпеку доменних контролерів. Виявлено, що неналежне управління обліковими записами, відсутність складних політик паролів та низький рівень обізнаності персоналу про сучасні кіберзагрози можуть сприяти успішній реалізації атак. Тому значна увага приділяється створенню культури безпеки в організації через навчання співробітників та розробку чітких процедур реагування на інциденти.[3]

Аналіз ефективності методів захисту показав, що регулярна ротація облікових записів із високими привілеями із застосуванням Kerberos Authentication Policies and Silos значно знижує ризики атак. Впровадження багатофакторної автентифікації (MFA) забезпечує додатковий рівень безпеки, а використання систем моніторингу, таких як Audit Policy і Advanced Threat Analytics (ATA), дозволяє своєчасно виявляти підозрілі дії в мережі. Крім того, регулярне оновлення операційних систем і компонентів Active Directory є ефективним способом запобігання атакам, що експлуатують вразливості програмного забезпечення.[5]

Таким чином, результати дослідження підкреслюють необхідність комплексного підходу до захисту активних доменних контролерів, який включає управління привілейованими обліковими записами, впровадження багатофакторної автентифікації, постійний моніторинг аномальної активності та регулярне оновлення програмного забезпечення. Розроблені рекомендації відповідають міжнародним стандартам інформаційної безпеки, таким як ISO/IEC 27001, і можуть бути адаптовані для потреб різних організацій.[4]

Список використаних джерел

1. Active Directory Kerberos Attacks: Golden Tickets & Silver Tickets. [Електронний ресурс] / LinkedIn Mohammad Abdur Rahim.S. – 2024. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/active-directory-kerberos-attacks-golden-tickets-silver-sarker
2. Top 10 Active Directory Attack Methods. [Електронний ресурс] / Lepide Philip Robinson – 2024. – Режим доступу до ресурсу: https://www.lepide.com/blog/top-10-active-directory-attack-methods/
3. A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises [Електронний ресурс] / ScienceDirect. – 2020. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S157401372300059X
4. Як стандарт ISO/IEC 27001 допомагає розвиватися сучасному бізнесу [Електронний ресурс] / IT Specialist – 2023. – Режим доступу до ресурсу: https://my-itspecialist.com/standard-iso/iec-27001-for-business
5. Best Practices for Securing Active Directory. [Електронний ресурс] / Microsoft – 2023. – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory