УДК 004.056.5
СТРУКОВ Володимир Михайлович,
кандидат технічних наук, доцент,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-4722-3159
ГУДІЛІН Владислав Владиславович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

ЗАХИСТ ВІД АТАК ПІДВИЩЕННЯ ПРИВІЛЕЇВ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У більшості корпоративних інформаційних систем для швидкого адміністрування мережі використовується програмне забезпечення Active Directory – служба каталогів корпорації Microsoft для операційних систем сімейства Windows Server. Захист Active Directory є актуальним аспектом забезпечення безпеки корпоративних інформаційних систем. Реальність така, що кількість вразливих корпоративних інформаційних систем становить 73% від загального числа. У даній роботі розглянуті деякі актуальні методи атак на корпоративні інформаційні системи, пов’язані з отриманням прав адміністратора домена в Active Directory, а також сформульовані методи захисту від них.

Щоб скомпроментувати контролер домену, хакеру необхідно не тільки знайти відому вразливість, отримати реєстраційні дані користувача або знайти помилку в налаштуванні політики безпеки. Це забезпечить лише деякий мінімальний доступ з обмеженими дозволами. Тому мета атаки хакера – отримання підвищених системних привілеїв в Active Directory.

У роботі розглянуті наступні методи проведення атак для отримання привілейованих прав доступу: 1) пошук паролів в налаштуваннях SYSVOL і групових політиках, 2) атака Kerberoasting та 3) підвищення привілеїв з групової політики DNSAdmins.

Пошук паролів в налаштуваннях SYSVOL і групових політиках GPP виконується в загальнодоступній директорії SYSVOL. SYSVOL – це загальнодоменний ресурс Active Directory, до якого у всіх, хто пройшов перевірку користувачів є доступ для читання. SYSVOL містить такі дані: сценарії входу, групові політики та інші дані домену, які можуть виявитися доступними всюди, де є контролер домену, сервер, який контролює комп'ютерну мережу. Директорія SYSVOL автоматично синхронізується і використовується всіма контролерами домена. Як правило, всі групові політики домену зберігаються в файловій системі за наступним шляхом: \\<Домен>\SYSVOL\<Домен>\Policies\. Коли створюється нова групова політика, в SYSVOL створюється пов'язаний XML-файл з відповідними даними конфігурації, і якщо вказано пароль, він шифрується за допомогою алгоритму шифрування AES-256-біт. У більшості випадків наступні XML-файли будуть містити облікові дані: groups.xml, ScheduleTasks.xml та Services.xml. Але корпорація Microsoft опублікувала ключ шифрування AES, який неважко використати з метою дешифрування пароля (рис. 1):

Рис. 1. Ключ

Будь-який користувач в домені може шукати в загальному ресурсі SYSVOL файли XML, значення яких містить зашифрований пароль AES (рис. 2):

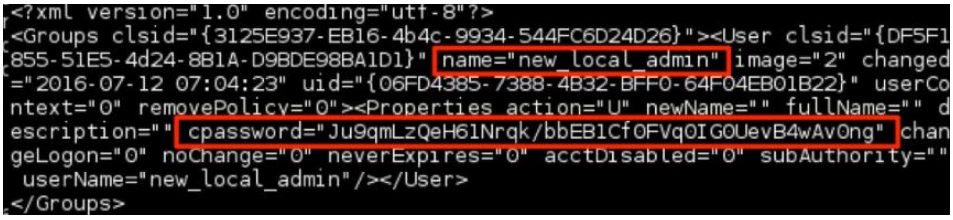

Рис. 2. Зашифрований пароль

Це відбувається через те, що авторизовані користувачі мають доступ для читання SYSVOL. Таким чином, отримавши доступ до XML-файлу, який містить пароль, хакер може використати закритий ключ AES для дешифрування пароля групової політики.

Kerberoasting – це метод, який дозволяє зловмисникові вкрасти квиток KRB_TGS, зашифрований за допомогою алгоритму RC4_HMAC_MD5, щоб зробити повний перебір хешу для отримання пароля. Мережевий протокол Kerberos використовує хеш NTLM для шифрування квитка KRB_TGS. Коли користувач домену відправляє запит на квиток TGS контролеру домену KDC для будь-якої служби, яку зареєструвала SPN, KDC генерує KRB_TGS без ідентифікації даних для авторизації користувача запитуваної служби. Зловмисник може використовувати цей квиток в автономному режимі для підбору пароля облікового запису служби, так як квиток був з використанням NTLM-хешу облікового запису служби.

Загальний план атаки виглядає наступним чином:

1. Отримання доступу до клієнтської системи доменної мережі.

2. Виявлення або сканування зареєстрованого SPN.

3. Запит на квиток TGS для виявленого SPN.

4. Отримання квитка TGS, який може бути у форматі .kirbi, ccache або бути службовим хешем (в деяких випадках).

5. Перетворення .kirby або ccache в необхідний формат для злому.

6. Перебір хеша по словнику.

Підвищення привілеїв з групової політики DNSAdmins. Microsoft не тільки реалізувала власний DNS-сервер, але і впровадила для нього протокол управління, що дозволяє інтегрувати DNS-сервер з доменами Active Directory. За замовчуванням контролери домену також є DNS-серверами, тому DNS-сервери повинні бути доступні кожному користувачеві домену. Це, в свою чергу, відкриває потенційну можливість для атаки на контролери домену: з одного боку ми маємо сам протокол DNS, а з іншого – протокол управління, заснований на RPC.

Користувач, що входить до групи DNSAdmins або має права на запис в об'єкти DNS-сервера, може завантажити на DNS-сервер довільну DLL. Це дуже небезпечно, оскільки багато корпоративних мереж використовують контролер домену в якості DNS-сервера (рис. 3):

Рис. 3. Параметри користувача

Таким чином, для реалізації атаки ми можемо просто завантажити на DNS-сервер довільну бібліотеку за допомогою команди dnscmd (шлях \\ops-build\dll повинен бути доступний для читання DC). Щоб перевірити, чи була завантажена DLL, можна використати наступну команду: Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters\-Name ServerLevelPluginDll.

Так як користувач – член групи DNSAdmins, можливо перезапустити службу DNS:

sc \\ops-dc stop dns

sc \\ops-dc start dn

Після перезапуску DNS-сервера буде виконано код з завантаженої бібліотеки. Така бібліотека може містити скрипт PowerShell для зворотного підключення (рис. 4):

Рис. 4. Код бібліотеки

Після успішного виконання скрипта буде отримано зворотне підключення з правами system (рис. 5):

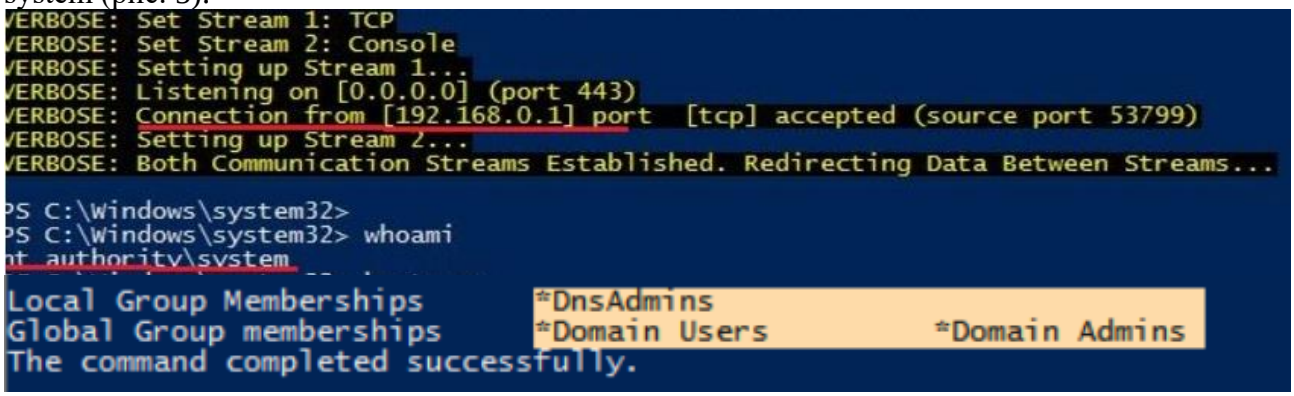

Рис. 5. Зворотне підключення

Для запобігання атак, заснованих на пошуку паролів в налаштуваннях SYSVOL, потрібно керуватися наступними рекомендаціями: розмежовувати доступ до файлів, що містять паролі, видалити існуючі XML-файли групових політик в SYSVOL, які містять паролі, своєчасно встановлювати останні оновлення з центру оновлень Windows.

Оскільки в атаці Kerberoasting протокол автентифікації Kerberos використовується звичайним чином, найкраща міра захисту від атаки – використання складних паролів для службових облікових записів, пов'язаних з Kerberos та SPN. Крім того, слід налаштувати MS SQL-сервер або будь-яку іншу службу без використання облікових записів із системними привілеями, а також доцільне використання спеціального захисного програмного забезпечення для зберігання паролів.

Щоб запобігти атаці підвищення привілеїв з групової політики DNSAdmins, слід перевірити список управління доступом ACL щодо відсутності привілеїв на запис об'єктів в DNS-сервер та членство в групі DNSAdmins. Очевидні показники в log-файлах DNS-сервера, такі як перезапуск служби DNS, події DNS-сервера з ідентифікатором 150 для помилки та 770 для успішного виконання можуть слугувати для детектування атаки. Моніторинг змін реєстру HKLM:\SYSTEM\CurrentControlSet\services\DNS\Parameters \ServerLevelPluginDll також допоможе детектувати спробу несанкціонованого отримання системних прав.

Таким чином, були розглянуті деякі з актуальних можливих методів проведення атак на корпоративні інформаційні системи, які засновані на використанні служби каталогів Active Directory і метою яких є отримання прав адміністратора домену, а також було надано практичні рекомендації із захисту та детектування проаналізованих видів атак.

Список використаних джерел

1. Metcalf S. Finding passwords in SYSVOL and exploiting group policy preferences // Active Directory Security : вебсайт. 28.12.2015. URL: https://adsecurity.org/?p=2288 (дата звернення: 15.04.2021).

2. Medin T. Attacking Kerberos: Kicking the Guard Dog of Hades // Red Siege Information Security. 08.2008. URL: https://www.redsiege.com/wp-content/uploads/2020/08/Kerberoastv4.pdf (дата звернення: 19.04.2021).

3. Metcalf S. Cracking Kerberos TGS tickets using Kerberoast – exploiting Kerberos to compromise the Active Directory Domain // Active Directory Security : вебсайт. 31.12.2015. URL: https://adsecurity.org/?p=2293 (дата звернення: 20.04.2021).

4. Metcalf S. Detecting Kerberoasting activity. // Active Directory Security : вебсайт. 05.02.2017. URL: https://adsecurity.org/?p=3458 (дата звернення: 23.04.2021).

Одержано 28.04.2021