УДК 004.056
DOI: 10.33764/2618-981X-2019-6-1-187-192

МЕТОДЫ ПРОВЕДЕНИЯ АТАК ДЛЯ ПОЛУЧЕНИЯ ПРАВ АДМИНИСТРАТОРА ДОМЕНА В ACTIVE DIRECTORY

Илья Олегович Скоропупов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (909)533-12-75, e-mail: ilia.skoropupov.phsd@gmail.com

Анна Александровна Бубнова
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (913)797-92-86, e-mail: bubnova.anja@rambler.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой информационной безопасности, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

В статье рассмотрены следующие методы атаки для получения прав администратора домена в Active Directory: поиск паролей в настройках SYSVOL и групповых политиках, Kerberoast, перестановка украденных учетных данных, получение доступа к файлу базы данных AD. Сформулированы рекомендации для предотвращения атак и минимизации возможного ущерба от них.

Ключевые слова: методы атак, права администратора, active directory, групповые политики, учетные данные, минимизация ущерба.

ATTACK METHODS FOR OBTAINING DOMAIN ADMINISTRATOR RIGHTS IN ACTIVE DIRECTORY

Il'ya O. Skoropupov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone (909)533-12-75, e-mail: ilia.skoropupov.phsd@gmail.com

Anna A. Bubnova
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone. (913)797-92-86, e-mail: bubnova.anja@rambler.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Information Security, phone: (903)937-27-90, e-mail: i.n.karmanov@ssga.ru

In this article the following attack methods for obtaining domain administrator rights in Active Directory are considered: searching for passwords in the SYSVOL settings and group policies, Kerberoast, swapping of stolen credentials, getting access to AD database file. Recommendations for preventing such attacks and minimization of possible damage from them are formulated.

Key words: attack methods, administrator rights, active directory, group policies, credentials, damage minimization.

Введение

Злоумышленник может получить права администратора домена в Active Directory (AD) многими способами, например, используя известные уязвимости в программном обеспечении. Защита AD является актуальным аспектом обеспечения безопасности корпоративных информационных систем (КИС). Реальность такова, что количество уязвимых КИС составляет 73 % от общего числа [1].

Каждая компания или предприятие делит свои сети на сегменты, в число которых могут входить автоматизированные системы управления технологическими процессами (АСУ ТП) и другие технологические информационные системы. «Побег» злоумышленника из КИС в технологическую сеть может обернуться катастрофой для всего предприятия. Поэтому не стоит пренебрегать профилактикой и соблюдением простых правил безопасности. Однако появление новых методов атак на сети требует разработки новых методов защиты.

Одним из таких методов защиты является обеспечение безопасности учетной записи администратора, а также соблюдение рекомендаций для конкретного типа атак. В данной статье рассмотрены некоторые новые методы атак, а также сформулированы методы защиты от них.

Атака может начинаться с фишингового письма одному или нескольким пользователям, что позволяет злоумышленнику запустить свой код на компьютере в КИС. После запуска кода сбор информации внутри сети для обнаружения уязвимых мест с целью повышения привилегий, модификации или кражи информации.

Общие действия атаки выглядят следующим образом [2]:

– инъекция вредоносного ПО (код, эксплойты);
– сканирование сети или разведка;
– кража и использование учетных данных;
– повышение привилегий в сети;
– модификация и кража информации;
– создание скрытого запасного входа в систему.

Злоумышленнику нетрудно повысить привилегии с уровня пользователя до уровня локального администратора. Этот процесс может происходить либо с помощью уязвимости в системе, либо, путем поиска паролей администраторов в системном томе (SYSVOL) [3].

Целью исследования является описание методов проведения атак для получения прав администратора домена в AD.

Для достижения поставленной цели были обозначены следующие задачи:

– поиск и обзор литературных источников;
– разбор методов проведения атак;
– выработка рекомендаций (методов защиты).

Методы

В статье рассмотрены следующие методы проведения атак для получения прав доступа:

а) поиск паролей в настройках SYSVOL и групповых политиках;
б) Kerberoast;
в) перестановка украденных учетных данных;
г) получение доступа к файлу базы данных AD.

Метод поиска паролей является самым простым, так как не требует специальных инструментов взлома, а осуществляется злоумышленником при помощи проводника Windows. Поиск выполняется в общей папке SYSVOL DFS. В большинстве случаев следующие XML-файлы будут содержать учетные данные: groups.xml, scheduletasks.xml и & Services.xml. SYSVOL – это общедоменный ресурс AD, к которому у всех прошедших проверку пользователей есть доступ для чтения. SYSVOL содержит в себе следующие данные: сценарии входа, групповые политики и другие данные домена, которые могут оказаться доступными везде, где есть контроллер домена (сервер, контролирующий область компьютерной сети). Это вызвано тем, что SYSVOL автоматически синхронизируется и используется всеми контроллерами домена. Как правило, все групповые политики домена хранятся в файловой системе по следующему пути: \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\, где DOMAIN это название текущего домена.

Когда создается новая групповая политика, в SYSVOL создается связанный XML-файл с соответствующими данными конфигурации, и, если указан пароль, он шифруется с помощью AES-256-бит. Корпорация Microsoft опубликовала ключ шифрования AES [4], который можно использовать для расшифровки пароля. Любой пользователь в домене может искать в общем ресурсе SYSVOL файлы XML, значение которого содержит зашифрованный пароль AES. Это происходит из-за того, что аутентифицированные пользователи имеют доступ для чтения SYSVOL.

Таким образом, получив доступ к XML-файлу, содержащему пароль, злоумышленник может использовать закрытый ключ AES для расшифровки пароля групповой политики.

Следующий метод называется Kerberoast. Kerberoast – эффективный метод извлечения учетных данных обычного пользователя из AD без отправки каких-либо пакетов в атакуемую злоумышленником систему. Причина, по которой эта атака эффективна, заключается в том, что большинство паролей учетных записей имеют ту же длину, что и минимальный пароль домена, например, 10 символов. Большинство учетных записей могут иметь пароли, которые не изменялись в течение долгого времени. Это негативно сказывается на их защите, так как пароли могли быть скомпрометированы ранее. Кроме того, большинство учетных записей имеют избыточные привилегии и часто входят в группы администраторов домена.

Атака Kerberoast начинается с отправки запроса в службу TGS Kerberos от имени пользователя. Данная служба отвечает за аутентификацию пользователей, так как она хранит криптографические ключи. Запрос использует валидный тикет проверки подлинности пользователя домена. Контроллер домена не отслеживает подключение пользователя к службе TGS Kerberos. Контроллер домена ищет SPN (основные имена службы – уникальные идентификаторы) в Active Directory и шифрует тикет, используя учетную запись службы TGS Kerberos, связанную с SPN, чтобы служба TGS Kerberos могла проверить доступ пользователя. Тип шифрования у запрошенного тикета Kerberos – RC4_HMAC_MD5. Для шифрования тикета используется хэш пароля протокола сетевой аутентификации учетной записи. Это означает, что Kerberoast может открыть тикет Kerberos, попробовав разные хэши протокола сетевой аутентификации, и, когда тикет успешно открыт, обнаруживается правильный пароль учетной записи [5].

Название метода перестановки украденных учетных данных говорит само за себя.

Для повышения привилегий до уровня администратора происходит компрометация одного автоматизированного рабочего места (АРМ) и эксплуатация уязвимостей. Из-под учетной записи администратора осуществляется попытка пройти аутентификацию на других АРМ. Далее происходит сбор информации об учетных записях, которую необходимо поменять местами.

Путем простой замены проводится перестановка учетных данных или любое другое действие, направленное на дестабилизацию работы КИС [6–7].

Получение доступа к базе данных AD является еще одним методом проведения атак для получения прав администратора.

База данных AD (файл ntds.dit) содержит информацию обо всех объектах в домене, включая хэши паролей для всех учетных записей пользователей. Данные из этой базы копируются на все контроллеры домена. Файл ntds.dit доступен только тем, кто может войти в контроллер. Защита данного файла крайне важна, поскольку доступ к нему может привести к полной компрометации домена.

Вот неполный список методов для получения информации из базы данных ntds.dit:

– получение доступа к резервным копиям домена и создание бэкдора с помощью файла ntds.dit из общей резервной копии, к которой имеют доступ все пользователи;

– клонирование виртуальных данных контроллера домена с использованием учетной записи администратора и копирование связанных данных. Полученный доступ к виртуальным хранилищам можно использовать для подмены информации. Также, с правами администратора можно копировать данные на локальный жесткий диск, извлекая их из памяти виртуальной машины, когда виртуальная машина приостановлена;

– компрометация учетной записи с правами на вход в контроллер домена.

Результаты

Для предотвращения атак, основанных на поиске паролей в настройках SYSVOL, нужно руководствоваться следующими рекомендациями:

– своевременно устанавливать последние обновления из центра обновлений Windows;

– удалить существующие XML-файлы групповых политик в SYSVOL, содержащие пароли;

– разграничить доступ к файлам, содержащим пароли [8].

Для предотвращения атак Kerberoast нужно руководствоваться следующими рекомендациями:

– пароли служебных учетных записей должны быть длиннее 25 символов;

– необходимо использовать специальное защитное программное обеспечение для хранения паролей.

Для предотвращения атак, использующих перестановку украденных учетных данных, необходимо, чтобы:

– администраторы имели отдельные АРМ для административной деятельности;

– учетные записи администраторов никогда не регистрировались на обычных рабочих станциях;

– все пароли локальных учетных записей администраторов на АРМ и серверах были длинными, сложными и генерировались случайным образом;

– групповые политики были настроены так, чтобы аутентификация администратора осуществлялась только на доверенных устройствах, а локальная учетная запись администратора была отключена.

Групповая политика может включать следующие параметры:

а) запрет доступа к компьютеру из сети;

б) запрет входа через службы удаленного рабочего стола [9–10].

Для предотвращения несанкционированного доступа к файлу базы данных AD нужно:

– ограничить число учетных записей, которые имеют права на вход в контроллеры домена;

– ограничить число учетных записей с полными правами AD, особенно учетных записей служб;

– ограничить доступ к каждой копии базы данных AD и ввести запрет на размещение ее копий в системах с уровнем доверия более низким, чем у контроллеров домена [11].

Заключение

В данной статье были рассмотрены некоторые из возможных методов проведения атак на AD для получения прав администратора домена, а также были предложены методы защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Positive Technologies. Исследования. Промышленные компании: векторы атак [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/?sphrase_id=62183.

2. Penetration testing. A hands-on introduction to Hacking. / Georgia Weidman. // No starch press. – San Francisco. – 2014. – P. 113.

3. Служба поддержки Microsoft. Как переместить дерева SYSVOL, служба FRS используется для репликации [Электронный ресурс]. – Режим доступа: https://support.microsoft.com/ru-ru/help/842162/how-to-relocate-a-sysvol-tree-that-uses-frs-for-replication.

4. Docs Microsoft. Password Encryption [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.

5. Attacking Kerberos. Kicking the guard dog of hades. [Электронный ресурс]. – Режим доступа: https://files.sans.org/summit/hackfest2014/PDFs/Kicking %20the %20Guard %20Dog %20of %20Hades %20- %20Attacking %20Microsoft %20Kerberos %20 %20- %20Tim %20Medin(1).pdf.

6. Mimikatz DCSync Usage, Exploitation, and Detection [Электронный ресурс]. – Режим доступа: https://adsecurity.org/?p=1729.

7. Sneaky Active Directory Persistence Tricks [Электронный ресурс]. – Режим доступа: https://adsecurity.org/?p=1929.

8. Finding Passwords in SYSVOL & Exploiting Group Policy Preferences. [Электронный ресурс]. – Режим доступа: https://adsecurity.org/?p=2288.

9. Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain [Электронный ресурс]. – Режим доступа: https://adsecurity.org/?p=2293.

10. Detecting Kerberoasting Activity [Электронный ресурс]. – Режим доступа: https://adsecurity.org/?p=3458.

11. Accidental Sabotage: Beware of CredSSP [Электронный ресурс]. – Режим доступа: https://www.powershellmagazine.com/2014/03/06/accidental-sabotage-beware-of-credssp/.