о пользе своевременных патчей Microsoft AD / Хабр

habr.com/ru/companies/bastion/articles/724966

secm3n

secm3n 27 мар 2023 в 15:15

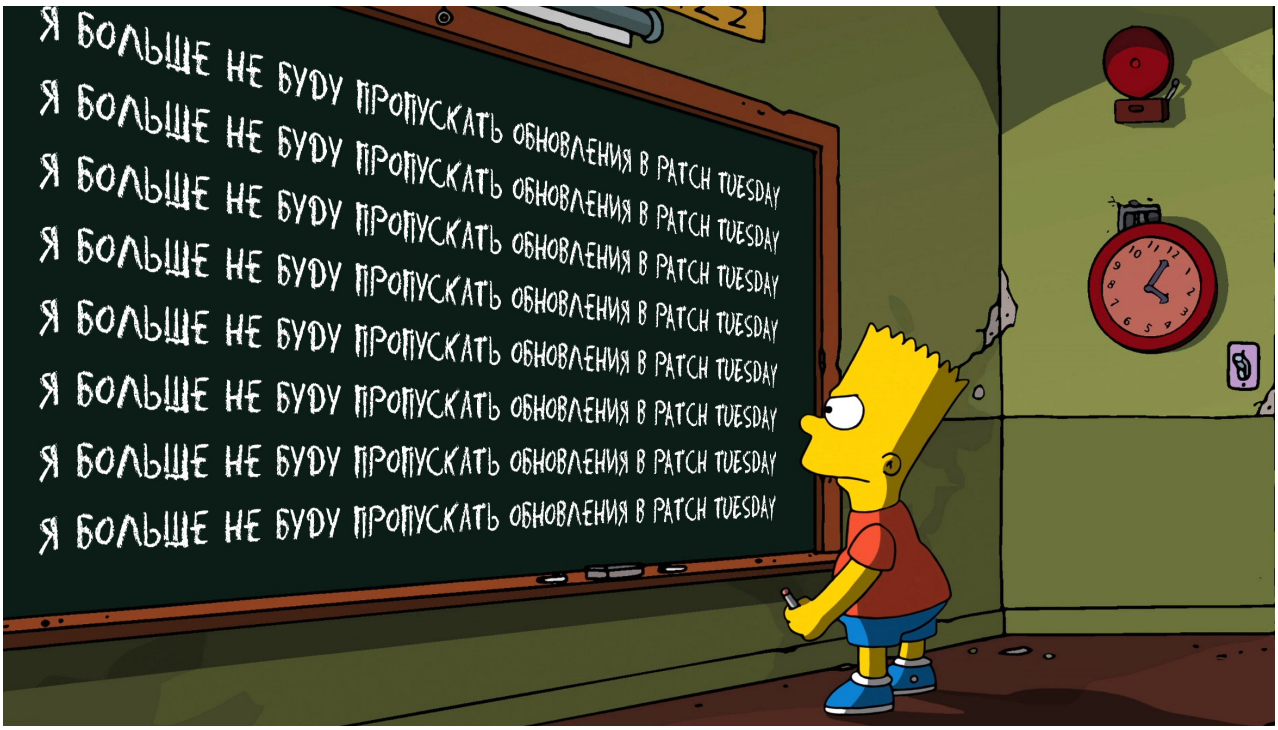
Пентест корпоративной сети: о пользе своевременных патчей Microsoft AD

Средний

8 мин

12K

Кейс



Сегодня поделюсь с вами историей из практики, которая наглядно покажет, к каким быстрым и катастрофическим последствиям может привести задержка с установкой патчей для серверного ПО.

В работе я нередко сталкиваюсь с уязвимостями, связанными с важнейшим компонентом корпоративных версий Microsoft Windows Server — средой службы каталогов Active Directory (AD). Весной прошлого года я убедился, насколько быстро основной механизм, обеспечивающий разграничение прав пользователей в AD, может превратиться в главную дыру в обороне.

Одна телекоммуникационная компания обратилась к нам с просьбой протестировать корпоративную сеть на проникновение с внутреннего периметра. Была поставлена простая, но глобальная задача — попытаться получить максимальные привилегии для рядового пользователя. Основной целью был домен. Дальнейших вредоносных действий, таких как захват контроля над финансами или базами данных от нас не требовалось.

Выбор инструмента

Так как заказчик не ограничивал нас в способах проникновения, я решил попробовать нечто новое — использовать уязвимость CVE-2022–26923, о которой подробно расскажу ниже. На момент проведения пентеста, она была совсем недавно обнаружена и пропатчена. Чтобы первым узнавать о подобных «новинках», я мониторю сообщения в Facebook и Twitter-аккаунтах узкопрофильных специалистов по ИБ. Подчас такая осведомленность дает серьезное преимущество.

На тот момент CVE-2022–26923 нельзя было идентифицировать каким-либо сканером. Но чтобы найти ее и использовать, нужен был минимум дополнительных хакерских инструментов. Фактически, я использовал только mimikatz и Rubeus. Однако, главная особенность этой уязвимости, повлиявшая на мой выбор, — результат можно было получить крайне быстро, уже на ранних этапах работы.

CVE-2022–26923 — история вопроса

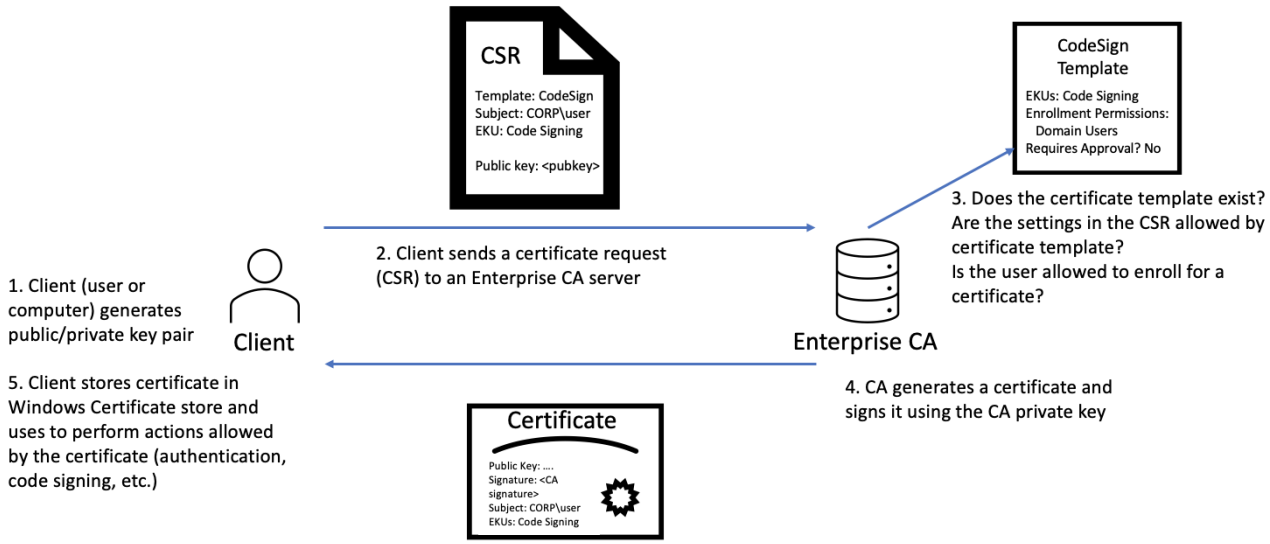
Прежде, чем переходить к описанию этапов самого пентеста, хотелось бы подробнее остановиться на самой уязвимости, иначе вам может быть сложно понять смысл моих действий.

Обнаружение

Уязвимость повышения привилегий AD домена CVE-2022–26923 (Certified) была обнаружена сотрудником датского Института исследования кибер-угроз (Institute For Cyber Risk) Оливером Ляком (ly4k) в рамках проекта Zero Day Initiative (ZDI). Основой для находки Оливера стало исследование уровня уязвимости служб сертификатов в корпоративных реализациях Microsoft Active Directory Public Key Infrastructure, которое провели Will Schroeder и Lee Christensen в июле 2021 года.

Механизм действия

CVE-2022–26923 позволяет пользователю с низким уровнем привилегий в среде Active Directory (с ролью сервера AD CS) повысить их до уровня администратора домена.



Раздача сертификатов в Active Directory

Уязвимость CVE-2022–26923 связана с особенностью аутентификации на основе сертификатов в средах AD DS — при запросе сертификата система берет значение принципала, указывающее на авторизованного пользователя, только из поля «dnsHostName», не учитывая данные в поле «SamAccountName».

Манипулируя свойством «dnsHostName», потенциальный злоумышленник может отождествить имя учетной записи своего компьютера с контроллером домена через выпуск соответствующего сертификата из центра сертификации AD. В дальнейшем полученный сертификат можно использовать для запроса TGT билета Kerberos, повышения привилегий до администратора домена и проведения дополнительных атак, таких как DCSync.

Реализовать уязвимость можно с помощью 3 конфигураций, имеющихся в шаблонах сертификата сервера AD CS:

- Allow Enroll («разрешить регистрацию») — позволяет любому аутентифицированному пользователю или компьютеру самостоятельно подать заявку на получение сертификата с административными привилегиями. Включенная сюда функция Allow Full Control permission («разрешить полный доступ») дает полный контроль над шаблоном сертификата.

- Client Authentication EKU (Extended/Enhanced Key Usage) — группа идентификаторов объектов (OID), которые определяют, как можно использовать сертификат.

- msPKI-Certificate-Name-Flag (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT) — флаг, управляющий значением альтернативного имени субъекта (SAN) сертификата. Изменив значение SAN (параметр SanType), можно послать запрос на выдачу сертификата с более высокими разрешениями домена.

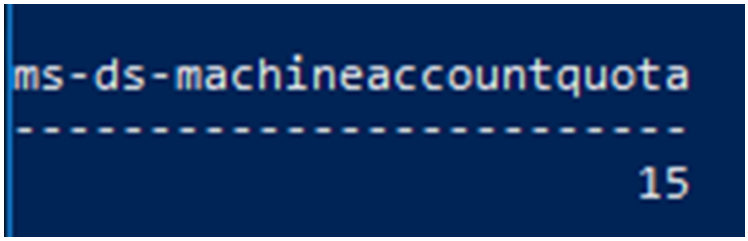
Вектор атаки

В нашем случае основной вектор атаки реализовывался через рабочие станции, подключенные к корпоративной сети. Для эксплуатации CVE-2022–26923 нужно было поэтапно выполнить несколько операций:

1. Создать или получить контроль над объектом «компьютер» во внутренней сети, чтобы изменить некоторые атрибуты этого объекта.
2. Найти подходящий шаблон сертификата для запроса.
3. Запросить сертификат от имени контроллера домена и получить с его помощью TGT билет Kerberos.
4. С помощью атаки DCSync получить хеши паролей администраторов домена и захватить административный контроль.

Захват объекта «компьютер»

В домене Active Directory заказчика (в атрибуте «MachineAccountQuota») было разрешено создавать до 15 подобных учетных записей типа «компьютер».



Значение атрибута «MachineAccountQuota»

Однако, согласно политике, установленной на контроллерах домена, делать это могли только администраторы. Обойти этот барьер позволили имеющиеся в системе так называемые «пресозданные» (pre-created) учетные записи компьютеров, которые еще ни разу не использовались или долгое время были неактивны. У таких машин пароль от учетной записи по умолчанию — ее имя, только строчными буквами. Например, если имя компьютера «Test» то, дефолтный пароль к нему будет «test».

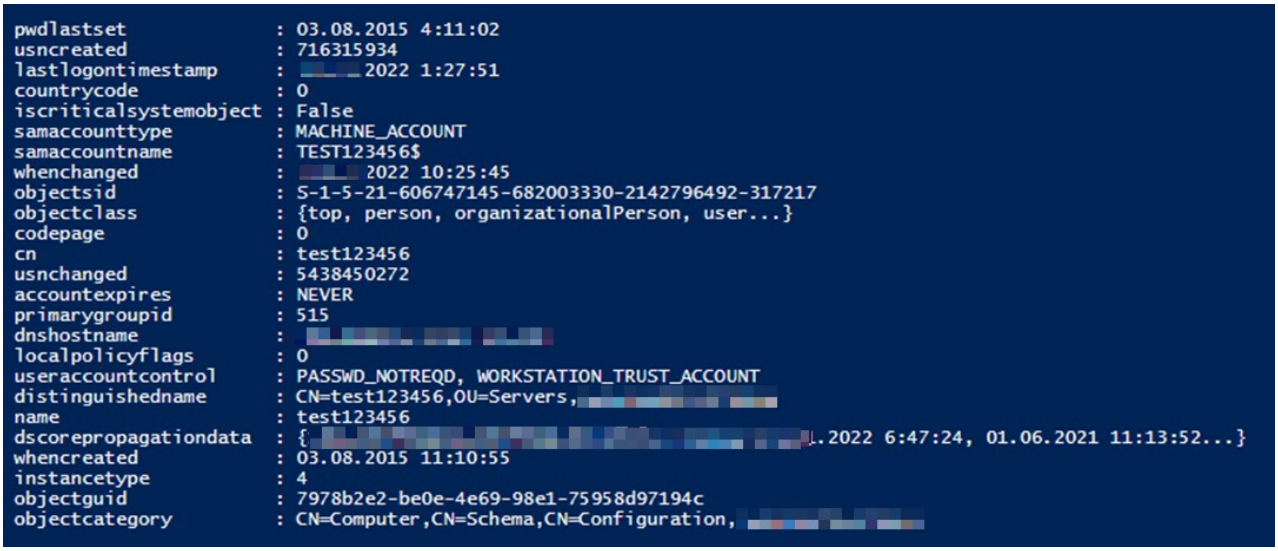
Объясняется этот казус технологическим наследованием. Такая особенность установки имен и паролей рабочих станций характерна для Windows 2000. По мере обновления сетей обновлялись и операционные системы, и, чтобы обеспечить обратную совместимость при создании учетной записи, разработчики добавили в настройки галочку «Assign this computer account as a pre-Windows 2000 computer». Поэтому в «старых» сетях даже с новейшими системами можно встретить такой артефакт, но он отсутствует в тех, которые строились с нуля относительно недавно.

Такие «пресозданные» учетные записи можно найти по атрибуту «UserAccountControl» с параметрами «PASSWD_NOTREQD» и «WORKSTATION_TRUST_ACCOUNT». Одна из них и позволила мне обойти запрет

на создание новых учетных записей.

Смена DNS-имени

Захваченная учетка «Test123456» имела право выполнять запросы в Active Directory и изменять свои атрибуты. Для получения максимальных привилегий мне оставалось лишь заменить атрибут «dnshostname» нашего компьютера на DNS-имя контроллера домена.



Изменение атрибута dnshostname для test123456

Для этого можно использовать любой специализированный инструмент, способный вести разведку в среде Microsoft Active Directory, например, PowerView. Сгодятся даже штатные средства PowerShell, хотя выполнить подмену с их помощью будет сложнее.

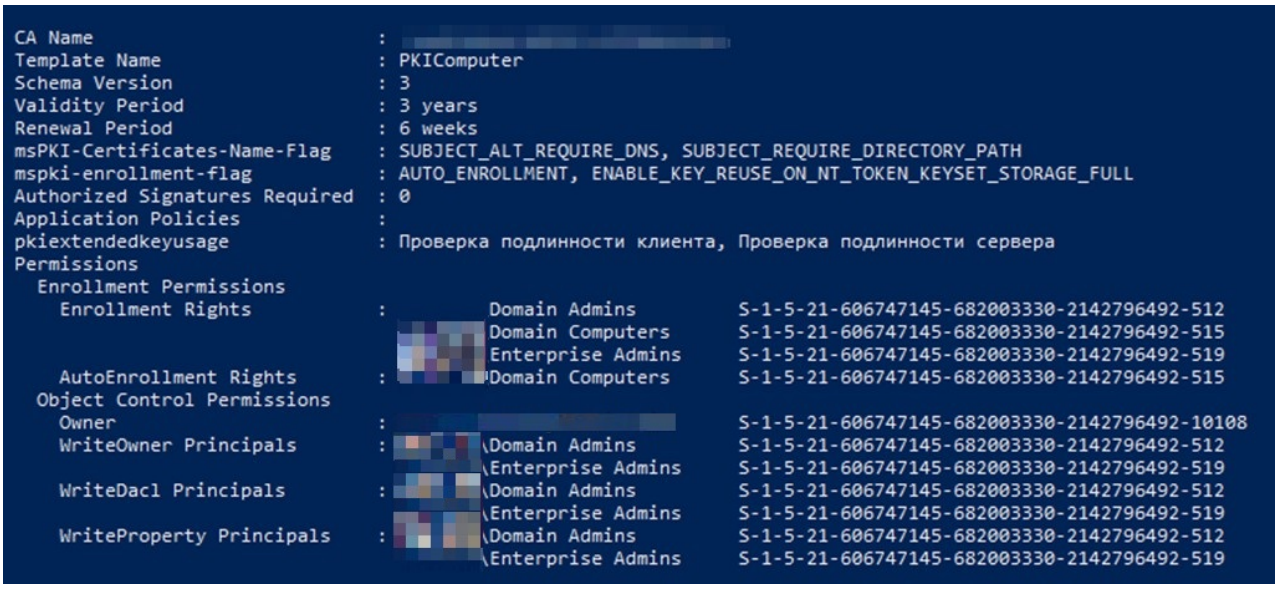
Поиск шаблона сертификата

На следующем этапе требовалось найти подходящий шаблон сертификата (PKI Certificate Template) для создания запроса на прохождение аутентификации в домене. Шаблоны хранятся в домене Active Directory и доступны для каждого авторизованного пользователя или субъекта (домена).

Параметры имени шаблона, подходящего для атаки:

- Атрибут назначения сертификата AD в поле «pKIExtendedKeyUsage» должен содержать в идентификаторе объекта (OID) сведения, что основное назначение (Key Usage) сертификата — проверка подлинности клиента. Это идентифицирует нас для PKI как полноправного клиента.
- Следующий важный параметр отражен в поле «Enrollment Rights» (права на выпуск сертификата). Там, помимо прочего, должно значиться «Domain Computers».

С помощью этих параметров мне удалось найти подходящий шаблон «PKIComputer» и создать на его основе запрос на выпуск сертификата.



Подходящий шаблон сертификата

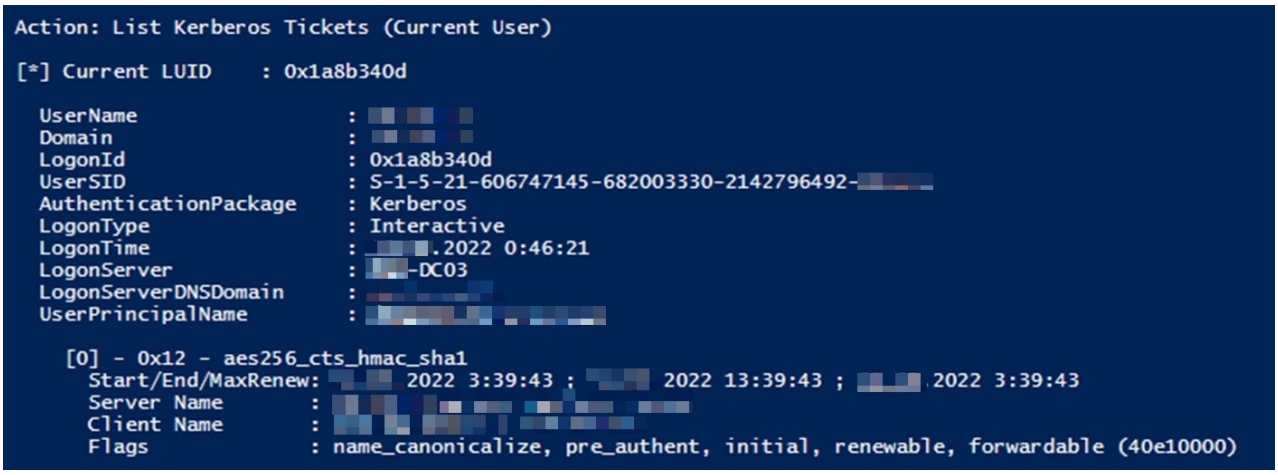
Запрос сертификата

Это можно сделать двумя методами:

- с помощью хакерского инструмента Certify;
- с помощью штатной утилиты Certutil.exe, входящей в службы сертификатов Windows.

Первый вариант, естественно, легче, но повышает риск обнаружения. Второй сложнее — нужно вручную подготовить файл запроса и вообще уверенно владеть Certutil. Зато подобный запрос вызывает меньше подозрений.

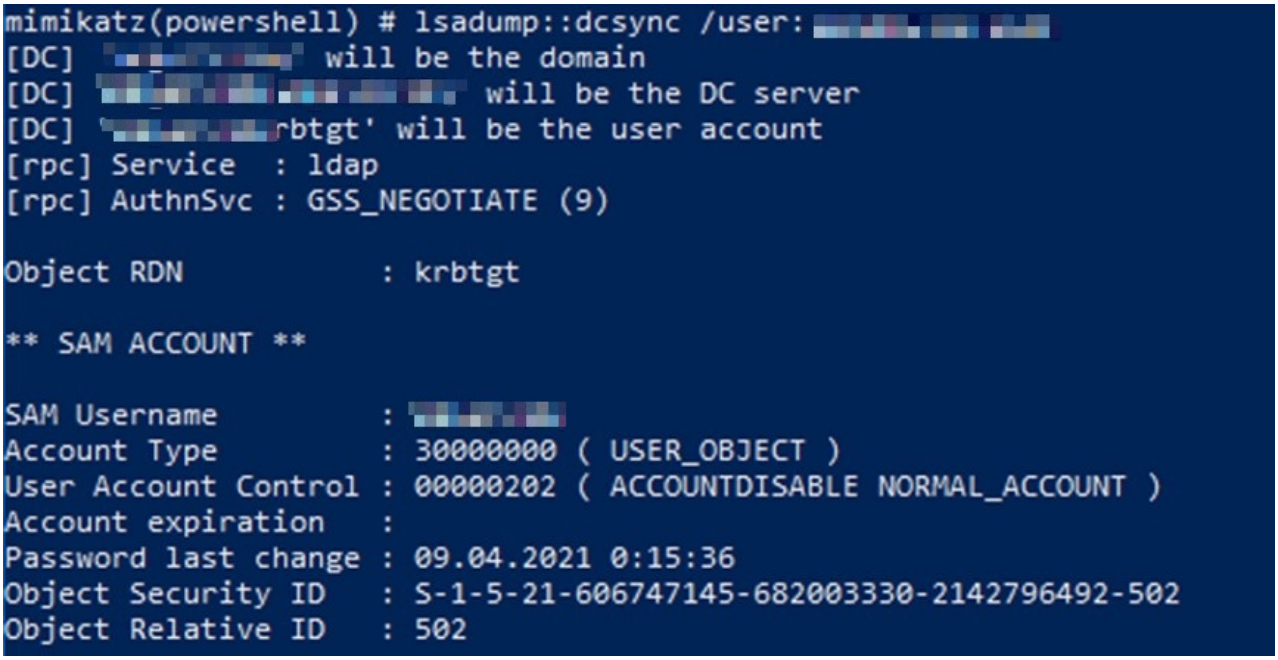
Еще одним важным моментом на этом этапе был запрос билета на доступ к другим ресурсам домена (Ticket-Granting Ticket, TGT) в центре распространения ключей (Key Distribution Center, KDC). Именно здесь на помощь пришел упомянутый выше Rubeus, который помог успешно пройти аутентификацию в домене AD.



Получение TGT билета Kerberos

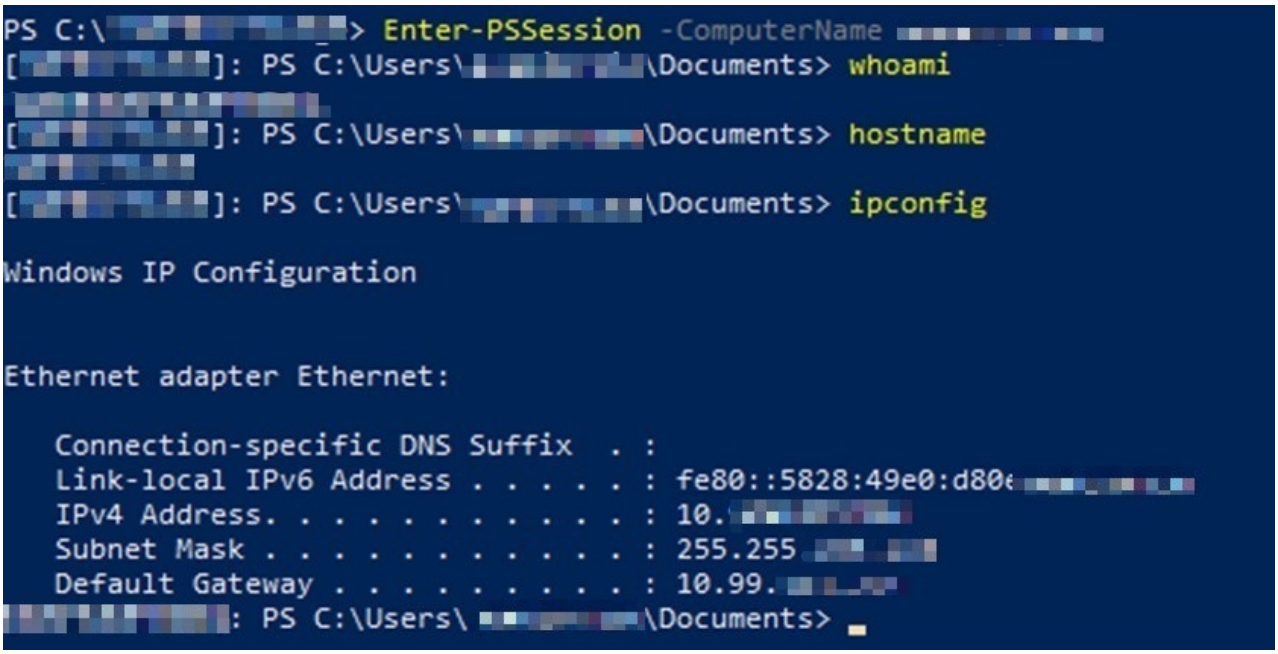
Получение административных прав

Полученный с помощью Rubeus тикет (TGT) я использовал для проведения атаки DCSync, направленной на дамп хешей паролей администраторов домена.



Результат атаки DCSync

Имея на руках действующие пароли, я получил прямой доступ к контроллеру домена «msk-hq-dc01». Задача была выполнена.



Получение доступа к контроллеру домена

Само собой, после получения сертификата и подготовки отчета для заказчика, я вернул «dnshostname» в дефолтное состояние и устранил все следы своей работы.

Почему это стало возможным

CVE-2022–26923 была исправлена в рамках обновлений безопасности от Microsoft за май 2022 года, через добавление в пользовательские шаблоны сертификатов на контроллере домена нового идентификатора объекта (OID) — szOID_NTDS_CA_SECURITY_EXT, содержащего специальный маркер пользователя Object-Sid (SID). Пентест проводился вскоре после того, как Microsoft выпустила патч и опубликовала сведения об уязвимости. Несмотря на это, патч в корпоративной сети компании не был установлен.

По нашей практике видно, что между публикацией информации об уязвимости и установкой патча на корпоративных ресурсах обычно проходит от недели до месяца. И это при том, что Microsoft выпускает патчи во второй вторник каждого месяца. Это и есть тот самый Patch Tuesday.

В крупных компаниях задержки вызваны размерами ИТ-инфраструктуры, которые подразумевают более длительный процесс выкатывания патчей, включающий предварительную обкатку на «тестовом» контроллере домена.

Другая вероятная причина в том, что патчи применяются только после перезагрузки контроллера домена. Но на практике системные администраторы стараются перезагружать контроллеры постепенно, чтобы не прерывать рабочие процессы. В итоге обновления устанавливаются неодновременно и в сети компании нет-нет, да и найдется пара-тройка непропатченных машин.

В данном случае задержку в установке патча могли вызвать еще и слухи о том, что он вызывает сбои в работе механизма аутентификации пользователей. Но, какими ни были бы причины, по которым установка патчей задерживается, это создает окно возможностей для хакеров.

Заключение

По итогам проведенного тестирования мы составили отчет для заказчика, куда был включен ряд практических рекомендаций по закрытию обнаруженной уязвимости:

- Провести аудит и удалить все неиспользуемые объекты типа «компьютер».
- Установить обновления, исправляющие уязвимость CVE-2022–26923.
- Изменить пароли для учетной записи krbtgt (дважды, чтобы гарантированно перезаписать историю и исключить работоспособность старых TGT).
- Изменить пароли администраторов домена.

Для полной гарантии устранения этой уязвимости, помимо установки патча, следует пересоздать старые шаблоны сертификатов. Но главный вывод, который мы сделали из ситуации и попытались донести до руководства компании, оказался простым — в условиях постоянно растущего числа угроз ИБ временной фактор может стать решающим. Достаточно на несколько дней затянуть с установкой патчей и киберпреступники получат отличную возможность завладеть важнейшей частью цифровой инфраструктуры компании.

Конечно, скорость установки обновлений серверного ПО сильно зависит от размеров компании. Крупные предприятия с обширной ИТ-инфраструктурой в основном не практикуют накатывание патчей «день в день», но порой риски столь велики, что ситуация требует немедленных действий.

Мы рекомендуем системным администраторам и специалистам по ИБ следить за выходящими патчноутами серверного ПО и оценивать степень риска, который несут новые угрозы. Иногда лучше оперативно выкатить обновление, нарушив привычную процедуру предварительной обкатки, чем столкнуться с перспективой полной потери контроля над корпоративной инфраструктурой.