????? ??????????

Каталог (Directory, хранилище данных) — в контексте компьютерной сети, иерархическая структура, хранящая информацию об объектах в сети. Объекты - это серверы, общие тома и принтеры, учетные записи пользователей, рабочие станции, домены, приложения, службы, политики безопасности и почти все остальное в вашей сети.

Служба каталогов (Directory Service) — является как источником информации каталога, так и службой, делающей информацию доступной и полезной для администраторов, пользователей, сетевых служб и приложений. Active Directory™, служба каталогов, которая хранит информацию о сетевых объектах, а также реализует службы, которые делают эту информацию доступной и полезной для пользователей, компьютеров и приложений.

Объекты (Objects) — это сущности, составляющие сеть, отдельный именованный набор атрибутов, представляющий что-то конкретное, например, пользователя, принтер или приложение.

Схема (Schema) — это описание классов объектов (различных типов объектов) и атрибутов для этих классов объектов. Для каждого класса объектов схема определяет атрибуты, которые должен иметь этот класс объектов, дополнительные атрибуты, которые он может иметь, и класс объектов, который может быть его родителем. Каждый объект Active Directory является экземпляром класса объекта. Каждый атрибут определяется только один раз и может использоваться в нескольких классах. Например, атрибут Description определяется один раз, но используется во многих различных классах.

Домены — это объекты-контейнеры, или набор административно определенных объектов, которые имеют общую базу данных каталога, политики безопасности и доверительные отношения с другими доменами. Таким образом, каждый домен является административной границей для объектов. Один домен может охватывать несколько физических мест или сайтов, и содержать миллионы объектов.

Дерево домена (Domain Tree) — состоит из нескольких доменов, которые имеют общую схему и конфигурацию, образуя непрерывное пространство имен. Домены в дереве также связаны между собой доверительными отношениями. Active Directory представляет собой набор из одного или нескольких деревьев.

Лес (Forest) — это набор из одного или нескольких деревьев доменов, которые не образуют непрерывное пространство имен. Все деревья в лесу имеют общую схему, конфигурацию и глобальный каталог. Все деревья в данном лесу обмениваются доверием в соответствии с транзитивными иерархическими отношениями доверия Kerberos. В отличие от деревьев, лес не требует отдельного имени. Лес существует как набор объектов перекрестных ссылок и доверительных отношений Kerberos, распознаваемых входящими в него деревьями. Деревья в лесу образуют иерархию для целей доверия Kerberos. Имя дерева в корне дерева доверия

относится к данному лесу.

Доверительные отношения (Trust Relationship) — это отношения, установленные между двумя доменами, которые позволяют пользователям одного домена быть распознанными контроллером домена в другом домене. Доверительные отношения позволяют пользователям получать доступ к ресурсам в другом домене, а также позволяют администраторам управлять правами пользователей в другом домене. На уровне леса доверительные отношения создаются автоматически между корневым доменом леса и корневым доменом каждого дерева доменов, добавленного в лес, в результате чего между всеми доменами в лесу Active Directory существует полное доверие.

Захват домена - получение уровня доступа управления контроллером домена из под учетной записи, которая имеет соответствующие права.

Способы захвата контроллер домена

- Эксплуатация уязвимости в контроллере домена.
- Кража учетных данных, токенов и сессий привилегированных учетных записей.
- Эксплуатация мисконфигураций сервисов в AD, предоставляющих доступ от имени привилегированных учетных записей.

По умолчанию наивысшие права в домене имеет учетная запись из группы Enterprise Admins.

Администраторы предприятия (Enterprise Admins) — это встроенная группа, находится в контейнере Users корневого домена леса, которая по умолчанию имеет административный доступ ко всем доменам в лесу. Enterprise Admins представляет полный доступ к конфигурации всех контроллеров домена. Существует очень мало задач, требующих использования учетной записи Enterprise Admins.

Администраторы (Administrators) – находится в контейнере Builtin каждого домена. Эта группа имеет полный доступ ко всем контроллерам домена и данным в контексте именования домена. Она может изменять членство во всех административных группах домена, а группа Администраторы (Administrators) в корневом домене леса может изменять членство в группах Администраторы предприятия (Enterprise Admins), Администраторы Схемы (Schema Admins) и Администраторы домена (Domain Admins).

Администраторы домена (Domain Admins) – находятся в контейнере Users каждого домена. Эта группа входит в группу Администраторы своего домена. Поэтому она наследует все полномочия группы Администраторы. Кроме того, она по умолчанию входит в локальную группу Администраторы каждого рядового компьютера домена, в результате чего администраторы домена получают в свое распоряжение все компьютеры домена.

Возможности групп Администраторов

Получив права доступа в одной из этих групп, мы можем управлять конфигурацией Домена или даже Леса. Мы можем получить доступ или изменить любые данные учетных записей, машин, сервисов и пр. А также управлять любой машиной в домене и любой учетной

записью.

Также можем выгрузить все секреты, ключи, хеши пользователей и пр. учетных записей из контроллера домена и пользоваться ими для создания токенов доступа или входа в машины.

Для эксплуатации такой возможности зачастую используется утилита SecretsDump.py пакета Impacket, выполняющая атаку под названием DCSync Attack.

DCSync Attack

Разрешение DCSync подразумевает наличие таких разрешений на сам домен: DS-Replication-Get-Changes, Replicating Directory Changes All и Replicating Directory Changes In Filtered Set.

Важные замечания о DCSync:

Атака DCSync имитирует поведение контроллера домена и просит другие контроллеры домена реплицировать информацию с помощью протокола Directory Replication Service Remote Protocol (MS-DRSR). Поскольку MS-DRSR является действительной и необходимой функцией Active Directory, его нельзя отключить или деактивировать.
По умолчанию только администраторы домена, администраторы предприятия, администраторы и группы контроллеров домена имеют необходимые привилегии.

SecretsDump

Утилита secretsdump выполняет атаку DCSync Attack и выполняет различные техники для извлечения хэшей с удаленной машины без выполнения на ней какого-либо агента. Для SAM и LSA Secrets (включая кэшированные учетные данные) утилита пытается прочитать как можно больше из реестра, затем сохраняет хэши в целевой системе (%SYSTEMROOT%\\\Temp dir) и читает остальные данные оттуда.

Для NTDS.dit:

- Получает список пользователей домена и получает его хэши и ключи Kerberos, используя вызов [MS-DRDS] DRSGetNCChanges() , реплицируя только нужные нам атрибуты.
- Извлекает NTDS.dit через vssadmin, выполненный с помощью smbexec. Он копируется на temp dir и разбирается удаленно.

Пример выполнения команды:

```
python3 secretsdump.py test.local/john:password123@10.10.10.1
```

Файл ntds.dit представляет собой базу данных, в которой хранится информация Active Directory, такая, как сведения о пользователях, группах и членстве в группах. База также включает хеши паролей для всех пользователей в домене.

Revision #2
Created 11 October 2025 16:25:21 by Admin
Updated 11 October 2025 17:16:34 by Admin