ВЗЛОМ

Разбираем атаки на Microsoft Active Directory. Техники проникновения и детекта

Антон Тюрин , 13.06.2018 4 комментария 49,106 Добавить в закладки

Содержание статьи

01. Шесть атак на AD, которые нельзя не заметить
02. Семь заклинаний атакующих для захвата Active Directory
02.1 Стадия 1. Разведка
02.2 Стадия 2. Продвижение по AD
02.3 Стадия 3. Эксплуатация
02.4 Рекомендации к стадиям 1–3
02.5 Стадия 4. Захват домена
03. Заключение

За последние четыре года ни один Black Hat или DEF CON не обошелся без докладов на тему атак на Microsoft Active Directory. Участники рассказывают о новых векторах и своих изобретениях, но не забывают и о советах, как можно их обнаружить и предотвратить. В этой статье мы рассмотрим популярные способы атак на AD и приведем рекомендации, которые помогут от них защититься.

Шесть атак на AD, которые нельзя не заметить

Многие производители программного обеспечения для мониторинга ИБ уже поддерживают в своих продуктах разнообразные техники атак злоумышленников. Рассмотрим некоторые из них.

Pass-the-Hash

Эта техника возможна благодаря архитектурным особенностям протокола аутентификации NTLM, разработанного Microsoft в девяностых годах прошлого века. Для того чтобы залогиниться на удаленном хосте, используется хеш пароля, хранящийся в памяти компьютера, с которого происходит аутентификация. Соответственно, его оттуда можно извлечь.

Как называются таблицы для выполнения быстрого перебора паролей Windows по их хешам?

- Распределенные
- Радужные
- Рандомные

Mimikatz

Для удобной эксплуатации Pass-the-Hash французский исследователь Бенжамен Делпи (Benjamin Delpy) в 2014 году разработал утилиту mimikatz. Она позволяет дампить из памяти clear-text-пароли и NTLM-хеши.

Brute Force

Если злоумышленнику недостаточно тех учетных данных, которые он извлек с одного хоста, он может прибегнуть к грубой, но действенной технике подбора паролей.

net user /domain

Откуда взять словарь имен пользователей для того, чтобы провести атаку Brute Force? Любому члену домена доступно выполнение команды `net user /domain` , которая возвращает полный список имен пользователей из AD.

Kerberoasting

Если же в домене в качестве протокола аутентификации используется Kerberos, то злоумышленник может прибегнуть к атаке Kerberoasting. Любой аутентифицированный в домене пользователь может запросить Kerberos-билет для доступа к сервису (Ticket Granting Service). TGS зашифрован хешем пароля учетной записи, от которой запущен целевой сервис. Злоумышленник, получив таким образом TGS, теперь может расшифровать его, подбирая пароль и не боясь блокировки, поскольку делает это офлайн. В случае успеха он получает пароль от ассоциированной с сервисом учетной записи, которая зачастую бывает привилегированной.

PsExec

После того как злоумышленник получил нужные учетные данные, перед ним встает задача удаленного исполнения команд. Для этого отлично подходит утилита PsExec из набора Sysinternals. Она хорошо себя зарекомендовала как среди IT-администраторов, так и среди атакующих.

Как UAC проверяет действия пользователя в домене?

- Все команды удаленных пользователей, а локально — за исключением админов
- Проверяются действия всех пользователей, кроме администраторов домена
- UAC не проверяет действия удаленного пользователя, если он локальный админ

Семь заклинаний атакующих для захвата Active Directory

Сейчас мы переходим к семи заклинаниям, благодаря которым атакующие могут получить полный контроль над Active Directory. Разделим их на четыре стадии:

1. Разведка.
2. Продвижение по AD.
3. Эксплуатация.
4. Захват домена.

На схеме можно увидеть все четыре, а также техники, которые на них применяются. Рассмотрим каждую детально.

Семь заклинаний атакующих, разделенные на четыре стадии

Стадия 1. Разведка

Начнем с разведки.

PowerView

Этот инструмент входит в популярный PowerShell-фреймворк для проведения тестирований на проникновение — PowerSploit. Также на него опирается инструмент BloodHound, строящий граф связей объектов внутри AD.

Граф связей объектов Active Directory

BloodHound сразу предоставляет такие возможности:

- найти аккаунты всех доменных администраторов;
- найти хосты, на которых залогинены доменные администраторы;
- построить кратчайший путь от хоста атакующего до хоста с сессией доменного админа.

Последний пункт дает ответ на вопрос, какие хосты нужно взломать атакующему, чтобы добраться до учетки доменного админа. Такой подход сильно сокращает время на получение полного контроля над доменом.

PowerView отличает от встроенных утилит для получения данных об объектах AD (например, `net.exe`) то, что он работает по протоколу LDAP, а не SAMR. Для обнаружения этой активности подойдет событие 1644 с контроллера домена. Логирование данного события включается добавлением соответствующего значения в реестре:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostic\\15 Field Engineeri
```

Включение логирования LDAP Event 1644

Событие 1644 с параметрами LDAP-запроса

Стоит обратить внимание на то, что таких событий может быть довольно много, и хорошей альтернативой детекту по событию будет детект по трафику, поскольку LDAP — это clear-text-протокол, соответственно, все запросы в трафике отлично видны.

LDAP SearchRequest

Еще одна важная особенность этого фреймворка — он написан на чистом PowerShell и не имеет зависимостей. И здесь для детектирования нам поможет появившаяся в PowerShell версии 5 возможность расширенного аудита. Событие 4104 показывает тело скрипта, в котором мы можем поискать характерные для PowerView названия функций.

SPN Scan

Эта техника может заменить атакующему запуск Nmap. После того как атакующий разобрался, какие пользователи и группы есть внутри AD, для полноты картины ему понадобится информация, какие есть сервисы.

Обычно это решается сканированием портов утилитой Nmap. Но теперь эту информацию можно получить и из AD — она там хранится в виде так называемых SPN (Service Principal Names). SPN состоит из serviceclass, он уникален для каждого типа сервиса, затем идет hostname в форме FQDN и для некоторых сервисов — port.

Примеры SPN

WWW
Полный список Service Principal Names

Обнаружить SPN Scan также поможет аудит событий LDAP.

Важно отметить, что SPN scan имеет явное преимущество перед сканом Nmap: он менее шумный. При использовании Nmap тебе нужно подключаться к каждому узлу и отправлять сотни пакетов на тот диапазон портов, который ты указал. А для получения списка SPN нужно отправить всего один запрос.

Remote Sessions Enumeration

Важной задачей перед атакующим на этапе lateral movement становится определение, какой пользователь на какой машине залогинен. Либо у него уже есть учетные данные пользователя (хеш или Kerberos-тикет) и он ищет хосты, куда можно беспрепятственно залогиниться. Либо он в поисках хоста, где есть живая сессия доменного администратора.

Тогда срабатывает сценарий: охота -> компрометация любого хоста -> залив mimikatz -> профит.

Для обнаружения данной техники можно использовать два события. 4624 — это успешный логон на удаленной системе с логон тайпом 3, а также события доступа к сетевой шаре IPC$, и нюанс: название пайпа — srvsvc. Почему пайп так называется, можно понять из трафика.

В левой части в красных рамках обращения к SMB, затем обращения к пайпу — `srvsvc`. Вот этот пайп позволяет взаимодействовать по специальному протоколу Server Service Remote Protocol. Конечным хостам он позволяет получать от него различную административную информацию, в том числе среди запросов есть такой, который называется NetSessEnum. В результате этого запроса возвращается полный список залогиненных на удаленной системе пользователей с IP и именами пользователей.

INFO

В MaxPatrol SIEM мы сделали детект на основе связки этих двух событий с учетом srvsvc. И аналогичный детект по трафику в PT Network Attack Discovery.

Стадия 2. Продвижение по AD

Overpass-the-Hash

Реинкарнация Pass-the-Hash. Что атакующий может сделать, если у него есть NTLM-хеш? Он может провести атаку Pass-the-Hash — но на нее уже есть детекты. Поэтому был найден новый вектор — атака Overpass-the-Hash.

Протокол Kerberos был разработан специально для того, чтобы пароли пользователей в том или ином виде не передавались по сети. Для этого на своей машине пользователь хешем своего пароля шифрует запрос на аутентификацию. В ответ Key Distribution Center (специальная служба, которая хостится на контроллере домена) выдает ему билет на получение других билетов — так называемый Ticket-Granting Ticket (TGT). Теперь клиент считается аутентифицированным, и в течение десяти часов он может обращаться за билетами для доступа к другим сервисам. Соответственно, если атакующий сдампил хеш пользователя, который входит в доверенную группу интересующего его сервиса, например ERP-системы или базы данных, атакующий может выпустить пропуск для себя и успешно авторизоваться на этом сервисе.

Как детектить. Если атакующий использует PowerShell-версию mimikatz для этой атаки, то здесь на помощь приходит логирование тела скрипта, потому что «Invoke-Mimikatz» — весьма примечательная строчка.

Или же 4688 — событие запуска процесса с расширенным аудитом командной строки. Даже если бинарь будет переименован, то по командной строке мы обнаружим очень характерную для mimikatz команду.

По трафику Overpass-the-Hash можно детектить на основе аномалии, которая возникает в результате того, что Microsoft рекомендует для текущих доменов использовать для шифрования authentication request AES-256. А mimikatz, когда отправляет данные authentication request, шифрует их с помощью устаревшего RC4.

В трафике наблюдается еще одно отличие из-за особенностей mimikatz. Оно основано на разнице набора шифров в легитимном домене и том, что отправляет mimikatz.

Golden Ticket

Что атакующий может сделать, если у него есть хеш пароля специальной учетной записи, которая называется krbtgt? Ранее мы рассматривали случай, когда пользователь мог быть непривилегированным. Сейчас мы рассматриваем пользователя, хешем пароля которого подписываются абсолютно все билеты на получение других билетов (TGT). Соответственно, злоумышленник больше не обращается к Key Distribution Center, он сам у себя генерирует этот билет, поскольку Golden Ticket, по сути, и есть TGT. Затем он уже может отправлять запросы на аутентификацию на любом сервисе внутри AD, причем на неограниченное время. В итоге он беспрепятственно обращается к этому ресурсу — Golden Ticket неспроста называется золотым.

Как детектить по событиям. Существует событие 4768, говорящее о том, что был выдан TGT, и событие 4769, говорящее о том, что был выдан сервисный билет, который необходим для аутентификации на каком-то сервисе внутри AD.

Здесь мы можем играть на разнице: так как при атаке Golden Ticket не запрашивает TGT у контроллера домена (он генерирует его самостоятельно), а TGS ему запрашивать необходимо, то, если мы обнаруживаем разницу в полученных TGT и TGS, можем предположить, что происходит атака Golden Ticket.

INFO

В MaxPatrol SIEM с использованием табличных списков, в которых мы логируем все выданные TGT и TGS, нам удалось реализовать такой детект.

Как атакующий может обойти групповые политики, запрещающие создание локального админа?

- Отключит комп от ЛВС, загрузится с флешки и создаст локального админа
- Загрузит Windows в безопасном режиме и внесет необходимые изменения
- Никак, GP имеют высший приоритет

Стадия 3. Эксплуатация

После того как задача аутентификации и авторизации на желаемых хостах решена, атакующий может приступить к выполнению задач удаленно.

WMI Remote Execution

WMI — встроенный механизм для удаленного исполнения, он отлично подходит для задач злоумышленника. Последние несколько лет в тренде понятие living off the land («жить с земли»), что означает пользоваться встроенными в Windows механизмами. В первую очередь потому, что позволяет маскироваться под легитимную активность.

На скриншоте — использование встроенной утилиты wmic. Ей указывается адрес хоста, к которому нужно подключиться, учетные данные, оператор process call create и команда, которую необходимо выполнить на удаленном хосте.

Как детектить. По связке событий удаленного логона 4624 (обрати внимание на Logon ID) и событию 4688, говорящему о запуске процесса с command line. 4688 — можно увидеть, что родитель запускаемого процесса — WmiPrvSE.exe, специальный сервисный процесс WMI, который используется для удаленного администрирования. Видна команда, которую мы отправляли net user /add, и Logon ID совпадает с событием 4624. Соответственно, мы можем совершенно точно сказать, с какого хоста запущена данная команда.

Детект по трафику. Здесь мы явно видим характерные слова Win32 process create, а также command line, которая отправляется на запуск. На скриншоте — недавно встреченная нами малварь, которая распространялась в виртуальных сетях по принципу, схожему с WannaCry, только вместо шифрования файлов она устанавливала майнер. Малварь несла с собой mimikatz и EthernalBlue, она дампила учетки, с их помощью логинилась на все те хосты, до которых могла дотянуться по сети. С помощью WMI она запускала на них PowerShell, скачивала PowerShell payload, который опять же содержал в себе mimikatz, EthernalBlue и майнер. Таким образом получалась цепная реакция.

Рекомендации к стадиям 1–3

1. Сложные и длинные (>25 символов) пароли для сервисных учетных записей. Это не оставит злоумышленнику шанса провести атаку Kerberoasting, так как брутить придется очень долго.
2. Логирование PowerShell. Поможет обнаружить использование многих современных инструментов для атак на AD.
3. Переезд на Windows 10, Windows Server 2016. Microsoft создала Credential Guard: больше не удастся сдампить из памяти NTLM-хеши и билеты Kerberos.
4. Строгое разграничение ролей. Опасно сочетать в одной роли администратора AD, DC, всех серверов и рабочих машин.
5. Двойная смена пароля krbtgt (это та самая учетная запись, которой подписываются TGT-билеты). Каждый год. И после ухода администратора AD:
   1. менять нужно дважды, так как хранится текущий и предыдущий пароль;
   2. менять каждый год, а также после ухода доменного администратора. Даже если сеть уже скомпрометирована и злоумышленники выпустили Golden Ticket, изменение пароля делает этот Ticket бесполезным. И им снова нужно начинать все сначала.
6. Средства защиты с непрерывно обновляющейся экспертной базой знаний. Необходимо для обнаружения реальных актуальных атак.

Как обойти SRP (Software Restriction Policies)?

- Никак. SRP проверяет как имена запускаемых файлов, так и их хеши, подмена невозможна
- При помощи Group Policy Bypassing Tool
- Инжектом gpdisable.dll в WordPad через COM-сервер AnalogCable Class

Стадия 4. Захват домена

DCShadow

24 января 2018 года на конференции Microsoft BlueHat в Израиле Бенджамен Делпи и Венсан ле Ту (Vincent Le Toux) представили новый модуль mimikatz, который реализует атаку DCShadow. Суть атаки в том, что создается поддельный контроллер домена, чтобы изменять и создавать новые объекты в AD через репликацию. Исследователям удалось выделить минимальный набор Kerberos SPN, необходимых для прохождения процесса репликации, — их требуется всего лишь два. Кроме того, они представили специальную функцию, которой можно запускать репликацию контроллеров принудительно. Авторы атаки позиционируют ее как атаку, которая сделает твой SIEM слепым. Так как поддельный контроллер домена не отправляет события в SIEM, это значит, что злоумышленники могут творить темные дела с AD и SIEM об этом не узнает.

Схема атаки: на той системе, с которой производится атака, необходимо добавить два SPN, которые нужны, чтобы другие домен-контроллеры могли аутентифицироваться по Kerberos для репликации. Поскольку согласно спецификации контроллер домена представлен в базе AD объектом класса nTDSDSA, необходимо такой объект создать. И в завершение вызвать репликацию с помощью функции DRSReplicaAdd.

Как детектить. Каким образом DCShadow выглядит в трафике. По трафику мы отчетливо видим добавление нового объекта в схему конфигурации типа домен-контроллер, а затем принудительный запуск репликации.

Хотя авторы атаки и говорят, что SIEM обнаружить ее не поможет, мы нашли способ, как можно дать понять службе ИБ, что в сети подозрительная активность.

Благодаря тому что наша корреляция знает список легитимных домен-контроллеров, она будет срабатывать, когда произойдет репликация с домен-контроллера, не входящего в этот белый список. Соответственно, подразделение ИБ может провести расследование и уже понять, это легитимный домен-контроллер, который добавила ИТ-служба, или атака DCShadow.

Как в домене бесплатно выполнять аудит сетевого взаимодействия?

- Смотреть журналы вручную, или писать парсеры лог-файлов самому
- Утилитой Sysmon с конфигом Threat Intelligence Configuration
- Никак, только платными SIEM

Заключение

Пример DCShadow показывает, что появляются новые векторы атак на предприятия. В этом океане ИБ-событий очень важно оставаться на гребне волны: смотреть дальше и двигаться быстро. Мы в PT Expert Security Center исследуем новые угрозы и разрабатываем для них способы и инструменты обнаружения. И готовы делиться этой информацией и дальше.