28-Domain Trusts Primer

Scenario

Many large organizations will acquire new companies over time and bring them into the fold. One way this is done for ease of use is to establish a trust relationship with the new domain. In doing so, you can avoid migrating all the established objects, making integration much quicker. This trust can also introduce weaknesses into the customer's environment if they are not careful. A subdomain with an exploitable flaw or vulnerability can provide us with a quick route into the target domain. Companies may also establish trusts with other companies (such as an MSP), a customer, or other business units of the same company (such as a division of the company in another geographical region). Let's explore domain trusts more and how we can abuse built-in functionality during our assessments.

يعني إيه Trust؟

الـ **Trust** في **Active Directory** هو ببساطة وسيلة بتخلي **دومينين أو فورستين** يقدروا يتواصلوا مع بعض ويعملوا **مزامنة مصادقة** (Authentication).
يعني المستخدمين في دومين معين يقدروا يدخلوا على موارد (Resources) موجودة في دومين تاني، سواء علشان يستخدموا حاجات معينة أو حتى علشان يعملوا مهام إدارية (Administrative Tasks).

الـ **Trusts** دي ممكن تكون:

- **اتجاه واحد (One-way)**: دومين واحد يسمح للمستخدمين بتوعه يوصلوا للدومين التاني لكن مش العكس.
- **اتجاهين (Two-way)**: الاتنين يقدروا يدخلوا على موارد بعض.

أنواع الـ Trusts الموجودة:

1. **Parent-Child Trust**
   - ده بيكون بين دومين رئيسي (Parent) ودومين فرعي (Child) جوه نفس الـ **Forest**.
   - بيكون **Two-way Transitive Trust** يعني الاتنين بيقدروا يثقوا في بعض تلقائيًا.
   - مثال:
     لو عندك دومين اسمه **inlanefreight.local**، والدومين الفرعي بتاعه اسمه **corp.inlanefreight.local**، المستخدمين في الدومين الفرعي يقدروا يوصلوا لحاجات في الدومين الرئيسي والعكس صحيح.

---

2. **Cross-link Trust**
   - ده Trust بيتعمل بين **Child Domains** علشان يسرّع عملية **المصادقة (Authentication)**.
   - مفيد لو في دومين فرعي عايز يتواصل بسرعة مع دومين فرعي تاني من غير ما يمر بالدومين الرئيسي.

---

3. **External Trust**

- ده بيكون بين **دومينين منفصلين في Forests مختلفة**.
- النوع ده بيكون **Non-Transitive**، يعني مش بيعدي الثقة بشكل تلقائي للدومينات التانية.
- بيستخدم حاجة اسمها **SID Filtering** علشان يمنع أي طلبات مصادقة من دومينات مش موثوقة.

---

4. **Tree-root Trust**
   - بيتعمل لما تضيف **Tree Root Domain** جديد جوه **Forest** موجودة.
   - بيكون **Two-way Transitive Trust**، يعني الدومين الجديد بيقدر يثق في الـ **Root Domain** بتاع الفورست والعكس.

---

5. **Forest Trust**
   - ده بيكون بين **Root Domains** لفورستين مختلفين.
   - النوع ده Transitive، يعني الدومينز جوه كل فورست يقدروا يتواصلوا مع الدومينز جوه الفورست التانية لو في صلاحيات.

---

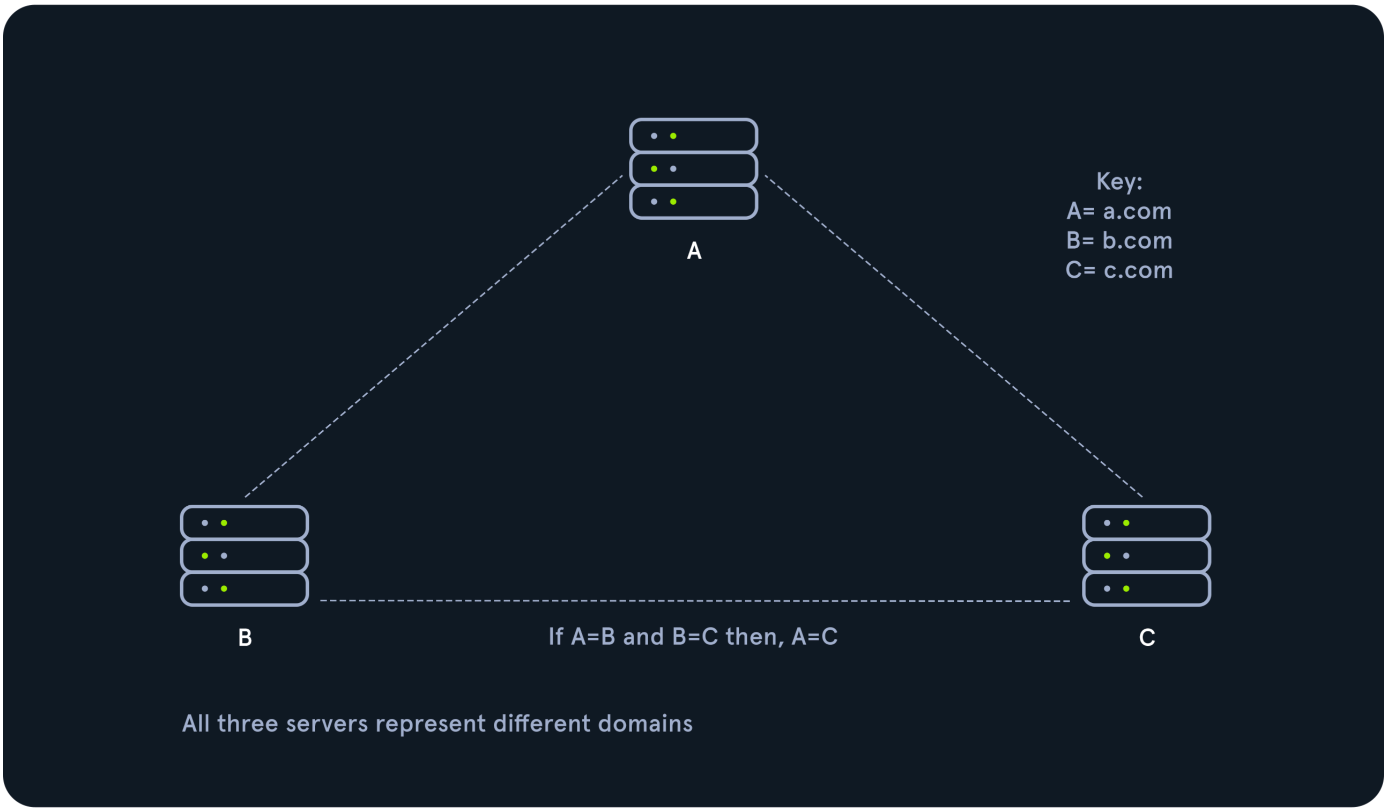
6. **ESAE (Enhanced Security Administrative Environment)**
   - ده حاجة اسمها **Bastion Forest**، ودي بتكون فورست معزولة وآمنة بتُستخدم لإدارة الـ **Active Directory** علشان تحمي الأدمِنز والـ Privileged Accounts.

الخلاصة:الـ Trust ده زي "تأشيرة عبور" بتخلي المستخدمين من دومين معين يقدروا يروحوا للدومين التاني. في أنواع كتير من الـ Trusts على حسب علاقة الدومينات ببعض، سواء كانوا في نفس الفورست أو في فورست مختلفة. النوع بيتحدد حسب احتياجك للأداء والأمان.

- A `transitive` trust means that trust is extended to objects that the child domain trusts. For example, let's say we have three domains. In a transitive relationship, if `Domain A` has a trust with `Domain B`, and `Domain B` has a `transitive` trust with `Domain C`, then `Domain A` will automatically trust `Domain C`.
- In a `non-transitive trust`, the child domain itself is the only one trusted.

transitive : if A trust B and B trust C : A will trust C

non-transitive : if A trust B and B trust C : A will not trust C



Trust Table Side By Side

Transitive	Non-Transitive
Shared, 1 to many	Direct trust
The trust is shared with anyone in the forest	Not extended to next level child domains
Forest, tree-root, parent-child, and cross-link trusts are transitive	Typical for external or custom trust setups

An easy comparison to make can be package delivery to your house. For a `transitive` trust, you have extended the permission to anyone in your household (forest) to accept a package on your behalf. For a `non-transitive` trust, you have given strict orders with the package that no one other than the delivery service and you can handle the package, and only you can sign for it.

Trusts can be set up in two directions: one-way or two-way (bidirectional).

- **`One-way trust`: Users in a `trusted` domain can access resources in a trusting domain, not vice-versa.**
- **`Bidirectional trust`: Users from both trusting domains can access resources in the other domain. For example, in a bidirectional trust between `INLANEFREIGHT.LOCAL` and `FREIGHTLOGISTICS.LOCAL`, users in `INLANEFREIGHT.LOCAL` would be able to access resources in `FREIGHTLOGISTICS.LOCAL`, and vice-versa.**

الكلام ده بيلفت الانتباه لنقطة في غاية الأهمية: **Domain Trusts** ممكن تتحول لنقطة ضعف كبيرة جدًا في بيئة Active Directory لو اتعملت بشكل غير مدروس أو بدون مراجعة للأمان.

إيه المشكلة مع الـ **Domain Trusts**؟

1. **الإعداد الخاطئ:**
   - أحيانًا بتتعمل الـ **Trusts** بسرعة أو بدون اعتبار أمني.
   - وتفترض إن كل حاجة آمنة، خاصة بعد عمليات **الاستحواذ أو الدمج** (**M&A -**) بين شركتين **Bidirectional Trust** ممكن تعمل لكن الحقيقة إن الشركة المستحوذ عليها ممكن تكون **نقطة ضعف**.
2. **نقطة الدخول غير المباشرة:**
   - لو حد (مهاجم مثلًا) عايز يوصل لشركتك، ممكن يروح للشركة اللي أنت اشتريتها أو دمجتها لأنها **هدف أسهل** (Softer Target).
   - بمجرد ما يدخلوا للدومين التاني، الثقة بين الدومينات بتسمح لهم إنهم يوصلوا **للموارد أو الحسابات** في الشركة الرئيسية.

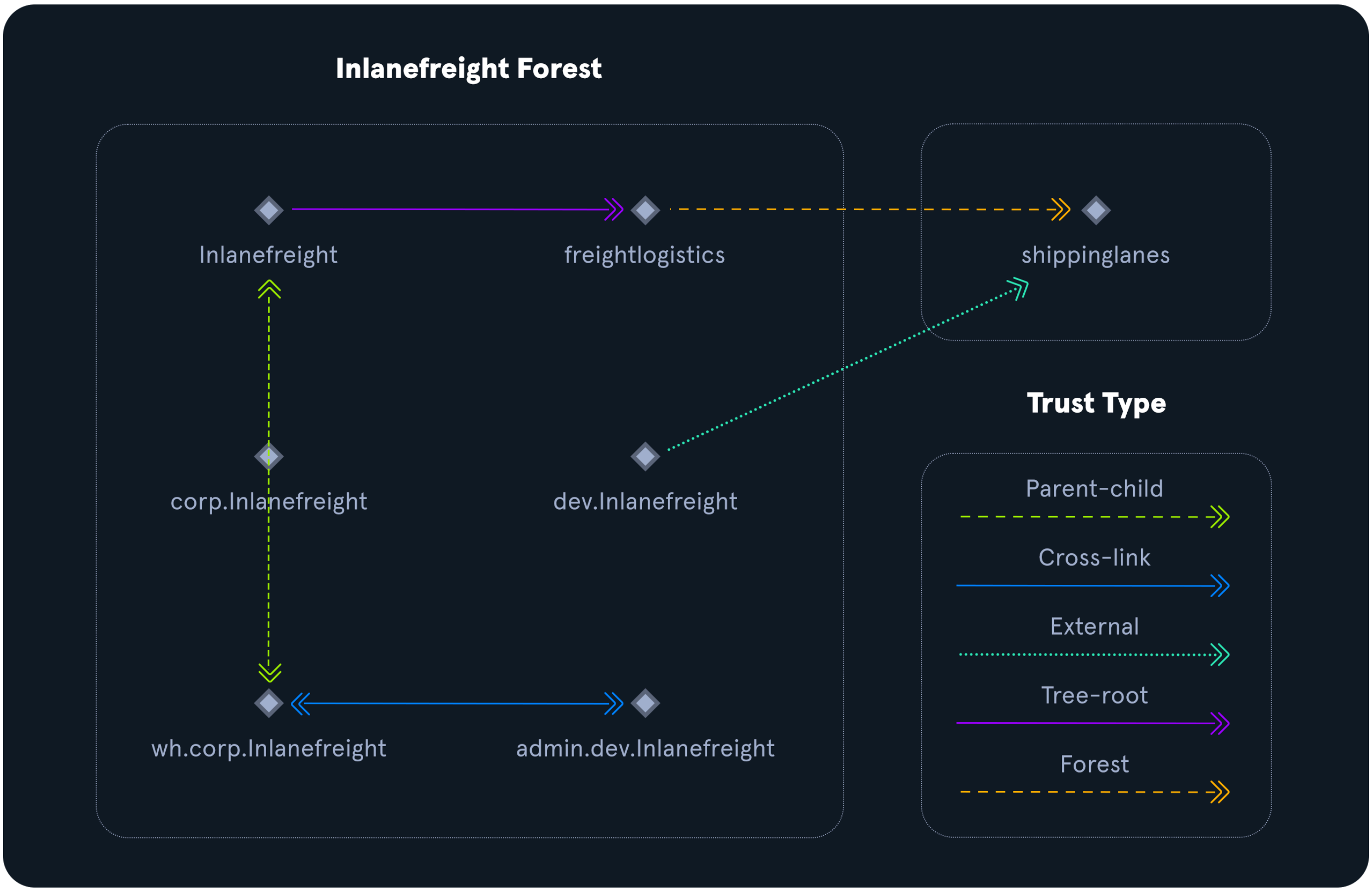
هجمات شائعة مع الـ **Domain Trusts**

1. Kerberoasting Attack

- ده هجوم بيستهدف الـ **Service Accounts** في بيئة الدومين.
- لو فيه Trust مع دومين تاني، المهاجم ممكن يستغل ده وينفذ **Kerberoasting** ضد الدومين التاني علشان يحصل على **Hash** خاص بـ Service Account.
- في بعض الحالات، الـ **Service Account** ده ممكن يكون له **صلاحيات إدارية** (**Admin**) في الدومين الرئيسي، وبالتالي المهاجم يدخل من باب خلفي.

مثال عملي

- كنت بتعمل **Penetration Test** على دومين رئيسي، لكن كان مؤمّن بشكل قوي.
- اكتشفت دومين تاني مرتبط معاه بـ **Bidirectional Trust**، وأمانه ضعيف.
- استغليت نقطة ضعف في الدومين التاني، وقدرت توصل لحسابات إدارية في الدومين الرئيسي.



Enumerating Trust Relationships

We can use the Get-ADTrust cmdlet to enumerate domain trust relationships. This is especially helpful if we are limited to just using built-in tools.

Using Get-ADTrust

```
PS C:\htb> Import-Module activedirectory
PS C:\htb> Get-ADTrust -Filter *


Direction                   : BiDirectional
DisallowTransivity          : False
DistinguishedName           :
CN=LOGISTICS.INLANEFREIGHT.LOCAL,CN=System,DC=INLANEFREIGHT,DC=LOCAL
ForestTransitive            : False
IntraForest                 : True
IsTreeParent                : False
IsTreeRoot                  : False
Name                        : LOGISTICS.INLANEFREIGHT.LOCAL
ObjectClass                 : trustedDomain
ObjectGUID                  : f48a1169-2e58-42c1-ba32-a6ccb10057ec
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
```

```
Source                     : DC=INLANEFREIGHT,DC=LOCAL
Target                     : LOGISTICS.INLANEFREIGHT.LOCAL
TGTDelegation              : False
TrustAttributes            : 32
TrustedPolicy              :
TrustingPolicy             :
TrustType                  : Uplevel
UplevelOnly                : False
UsesAESKeys                : False
UsesRC4Encryption          : False

Direction                  : BiDirectional
DisallowTransivity         : False
DistinguishedName          :
CN=FREIGHTLOGISTICS.LOCAL,CN=System,DC=INLANEFREIGHT,DC=LOCAL
ForestTransitive           : True
IntraForest                : False
IsTreeParent               : False
IsTreeRoot                 : False
Name                       : FREIGHTLOGISTICS.LOCAL
ObjectClass                : trustedDomain
ObjectGUID                 : 1597717f-89b7-49b8-9cd9-0801d52475ca
SelectiveAuthentication    : False
SIDFilteringForestAware    : False
SIDFilteringQuarantined    : False
Source                     : DC=INLANEFREIGHT,DC=LOCAL
Target                     : FREIGHTLOGISTICS.LOCAL
TGTDelegation              : False
TrustAttributes            : 8
TrustedPolicy              :
TrustingPolicy             :
TrustType                  : Uplevel
UplevelOnly                : False
UsesAESKeys                : False
UsesRC4Encryption          : False
```

The above output shows that our current domain `INLANEFREIGHT.LOCAL` has two domain trusts. The first is with `LOGISTICS.INLANEFREIGHT.LOCAL`, and the `IntraForest` property shows that this is a **child domain**, and we are currently positioned in the root domain of the forest. The second trust is with the domain `FREIGHTLOGISTICS.LOCAL,` and the **`ForestTransitive`** property is set to `True`, which means that this is a **forest trust or external trust**. We can see that both trusts are set up to be bidirectional, meaning that users can authenticate back and forth across both trusts. This is important to note down during an assessment. If we cannot authenticate across a trust, we cannot perform any enumeration or attacks across the trust.

Aside from using built-in AD tools such as the Active Directory PowerShell module, both PowerView and BloodHound can be utilized to enumerate trust relationships, the type of trusts established, and the authentication flow. After importing PowerView, we can use the Get-DomainTrust function to enumerate what trusts exist, if any.

Checking for Existing Trusts using Get-DomainTrust

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

SourceName      : INLANEFREIGHT.LOCAL
TargetName      : LOGISTICS.INLANEFREIGHT.LOCAL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 11/1/2021 6:20:22 PM
WhenChanged     : 2/26/2022 11:55:55 PM

SourceName      : INLANEFREIGHT.LOCAL
TargetName      : FREIGHTLOGISTICS.LOCAL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 11/1/2021 8:07:09 PM
WhenChanged     : 2/27/2022 12:02:39 AM
```

PowerView can be used to perform a domain trust mapping and provide information such as the type of trust (parent/child, external, forest) and the direction of the trust (one-way or bidirectional). This information is beneficial once a foothold is obtained, and we plan to compromise the environment further.

Using Get-DomainTrustMapping

```
PS C:\htb> Get-DomainTrustMapping

SourceName      : INLANEFREIGHT.LOCAL
TargetName      : LOGISTICS.INLANEFREIGHT.LOCAL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 11/1/2021 6:20:22 PM
WhenChanged     : 2/26/2022 11:55:55 PM
```

```
SourceName      : INLANEFREIGHT.LOCAL
TargetName      : FREIGHTLOGISTICS.LOCAL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 11/1/2021 8:07:09 PM
WhenChanged     : 2/27/2022 12:02:39 AM

SourceName      : FREIGHTLOGISTICS.LOCAL
TargetName      : INLANEFREIGHT.LOCAL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 11/1/2021 8:07:08 PM
WhenChanged     : 2/27/2022 12:02:41 AM

SourceName      : LOGISTICS.INLANEFREIGHT.LOCAL
TargetName      : INLANEFREIGHT.LOCAL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 11/1/2021 6:20:22 PM
WhenChanged     : 2/26/2022 11:55:55 PM
```

From here, we could begin performing enumeration across the trusts. For example, we could look at all users in the child domain:

Checking Users in the Child Domain using Get-DomainUser

```
PS C:\htb> Get-DomainUser -Domain LOGISTICS.INLANEFREIGHT.LOCAL | select
SamAccountName

samaccountname
--------------
htb-student_adm
Administrator
Guest
lab_adm
krbtgt
```

Another tool we can use to get Domain Trust is `netdom`. The `netdom query` sub-command of the `netdom` command-line tool in Windows can retrieve information about the domain, including a list of workstations, servers, and domain trusts.

Using netdom to query domain trust

```
C:\htb> netdom query /domain:inlanefreight.local trust
Direction Trusted\Trusting domain                         Trust type
========= =======================                         ==========

<->       LOGISTICS.INLANEFREIGHT.LOCAL
Direct
 Not found

<->       FREIGHTLOGISTICS.LOCAL
Direct
 Not found

The command completed successfully.
```

Using netdom to query domain controllers

```
C:\htb> netdom query /domain:inlanefreight.local dc
List of domain controllers with accounts in the domain:

ACADEMY-EA-DC01
The command completed successfully.
```

Using netdom to query workstations and servers

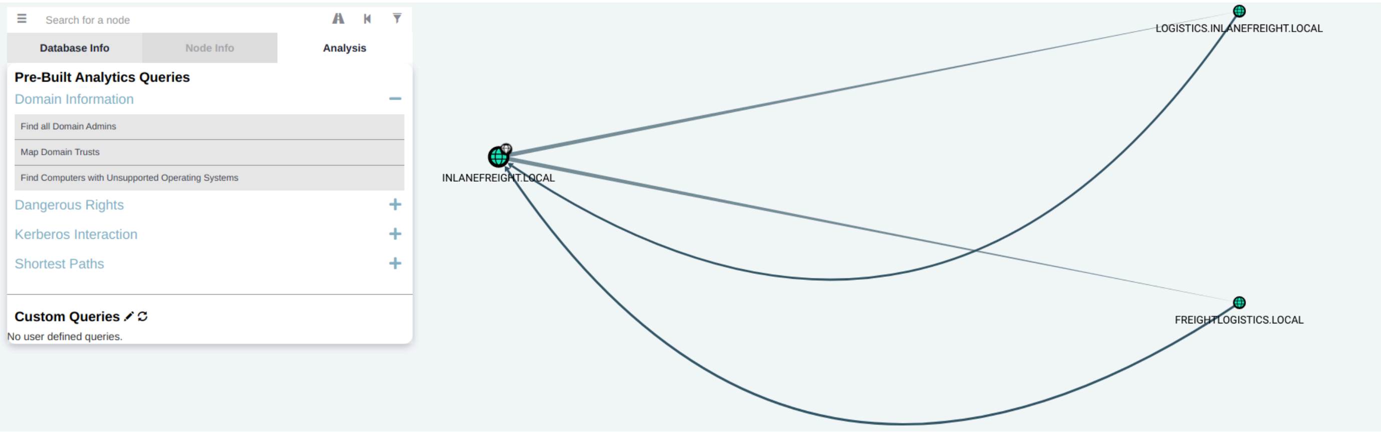
```
C:\htb> netdom query /domain:inlanefreight.local workstation
List of workstations with accounts in the domain:

ACADEMY-EA-MS01
ACADEMY-EA-MX01      ( Workstation or Server )

SQL01      ( Workstation or Server )
ILF-XRG      ( Workstation or Server )
MAINLON      ( Workstation or Server )
CISERVER      ( Workstation or Server )
INDEX-DEV-LON      ( Workstation or Server )
...SNIP...
```

We can also use BloodHound to visualize these trust relationships by using the `Map Domain Trusts` pre-built query. Here we can easily see that two bidirectional trusts exist.

Visualizing Trust Relationships in BloodHound



Enumeration the trust from linux but should be have username and passwrod

1. Using `rpcclient`

The `rpcclient` tool, part of the Samba suite, can query information about trusts on a DC.

```
rpcclient -U 'username%password' DC_IP
```

Once logged in, run the following commands:

- **List trusted domains**:

  `enumtrustdom`

  This will display trusted domains and their relationships.

- **Get detailed information**:

  `querydominfo TRUSTED_DOMAIN_NAME`

---

2. Using Impacket's `lookupsid.py`

Impacket includes several scripts for enumerating information from a DC. The `lookupsid.py` script can help identify domains and trust relationships.

```
python3 lookupsid.py DOMAIN/username:password@DC_IP
```

Look for any references to external or trusted domains in the output.

---

3. Using Impacket's `GetADTrusts.py`

For direct enumeration of trust relationships, `GetADTrusts.py` is ideal.

```
python3 GetADTrusts.py -dc-ip DC_IP DOMAIN/username:password
```

This will list all the trust relationships for the specified domain.

---

4. Using LDAP Queries

If LDAP is accessible, you can query for trust relationships using `ldapsearch` or Impacket's `ldapdomaindump`.

- **Using `ldapsearch`:**

  ```
  ldapsearch -x -H ldap://DC_IP -D "DOMAIN\username" -w password -b "CN=Configuration,DC=DOMAIN,DC=com" "(objectClass=trustedDomain)"
  ```

- **Using `ldapdomaindump`:**

  ```
  python3 ldapdomaindump.py DOMAIN/username:password@DC_IP
  ```

Check the generated files for trust-related objects (`trustedDomain`).

---

5. Using `enum4linux`

`enum4linux` can also enumerate trust information from a DC.

```
enum4linux -T DC_IP
```

This will display any trust relationships discovered.
