Vertrauen ist gut, Pentests sind besser

Sicherheitsprobleme in Active Directory Forests (Star Wars Edition)
Trust in the force you must.
The Republic will be reorganised into the first Galactic Empire!
Merger: Sharing Resources

new name

republic.org → empire.gov

Enterprise Galactic Empire Imperial Government

Subsidiary Regional Governors e.g. Genosis

Death Star
Domains are container objects. Domains are a collection of administratively defined objects that share a common directory database.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)
(Forest) Root Domain

empire.gov

Child Domains

army.empire.gov  alderan.empire.gov

Enterprise Administrator

Schema Admins

Protect those!
### Permission Entry for sbatraining

<table>
<thead>
<tr>
<th>Principal:</th>
<th>Everyone</th>
<th>Select a principal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Allow</td>
<td></td>
</tr>
<tr>
<td>Applies to:</td>
<td>This object only</td>
<td></td>
</tr>
</tbody>
</table>

**Permissions:**

- [ ] Full control
- [ ] List contents
- [x] Read all properties
- [ ] Write all properties
- [ ] Delete
- [ ] Delete subtree
- [ ] Read permissions
- [ ] Modify permissions
- [ ] Modify owner
- [ ] All validated writes
- [ ] All extended rights
- [ ] Delete msImaging-PSP objects
- [ ] Create MSMQ Queue Alias objects
- [ ] Delete MSMQ Queue Alias objects
- [ ] Create msPKI-Key-Recovery-Agent objects
- [ ] Delete msPKI-Key-Recovery-Agent objects
- [ ] Create msSFU30MailAliases objects
- [ ] Delete msSFU30MailAliases objects
- [ ] Create msSFU30NetId objects
- [ ] Delete msSFU30NetId objects
- [ ] Create msSFU30NetworkUser objects
- [ ] Delete msSFU30NetworkUser objects
Threat model: Subdomain Compromized, is the Root Domain in Danger?
“Each time you create a new domain container in a forest, a two-way, transitive trust relationship is automatically created between the new domain and its parent domain.”
Kerberos Ticket

Active Directory Migration: SidHistory

Objects are migrated into the new domain. Not yet migrated users have access using the old SIDs.

→ You can add arbitrary groups (SIDs) to the TGT.
... the **forest is a security boundary** for the information that is contained in that instance of Active Directory.
- MSDN
Enterprise Administrators

Principal: Enterprise Admins (SBATRAINING\Enterprise Admins)
Type: Allow
Applies to: This object and all descendant objects

Permissions:
- Full control
- List contents
- Read all properties
- Write all properties
- Delete

- Delete mslmaging-PSPs objects
- Create MSMQ Queue Alias objects
- Delete MSMQ Queue Alias objects
- Create msPKI-Key-Recovery-Agent objects
- Delete msPKI-Key-Recovery-Agent objects
It's an older code, sir but it checks out
Demo: ExtraSIDs and dcsync
**dcsync** the other krbtgt password hashes from the other domains

- empire.gov
- alderan.empire.gov
- army.empire.gov
- (Forest) Root Domain

Protect those

- Enterprise Administrator
- Schema Admins

Enterprise Admin
Findings

• Automatic two-way trust between root and child
• Migration feature SidHistory is enabled by default
• The AD-Forest is the security boundary, not the domain

Counter Measures

• Sid History Filtering
• Untrusted domains in a separate forest (?)
Threat model: Separate Forests
Is the trusting Forest in Danger?
Separate Forests

Domain quarantine (SID filtering) is **enabled** by default. No foreign ExtraSIDs

Ressource is secured by ACL

Other ressources may be accessible

User is authenticated here

Forest Trust (two-way)

dearthstar.mil
Impersonation through Delegation

- Access service as user vader@
- e.g. WebDav service runs under a service user
- e.g. CIFS Server Impersonation as user vader@

Service Ticket:
- vader
- http/websrv
- cifs/file

Domain Controller (Kerberos AS/KDC)
Implications of Unconstrained Delegation

Service Ticket
Granting Ticket

Administrator

Service Ticket
Granting Ticket

kenobi

Lsass.exe
Granting Ticket
Granting Ticket
Separate Forests

empire.gov

deathstar.mil

Service Ticket
Granting Ticket

Service Ticket
Granting Ticket

Lsass.exe

Granting Ticket
Granting Ticket
Microsoft Printer Bug

Image from: https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/
https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1
Attack Path of Unconstrained Delegation + Printer Bug

Request to EMPIRE-DC: Notify WEBDAV

Kerberos Service Ticket

Granting Ticket (TGT)
empire-dc$

Service Ticket
ldap/empire-dc$

webdav$

empire-dc$

dcsync

TGT empire-dc$
Demo: Printer Bug and Delegation abuse
Merger: Sharing Ressources
Counter Measures

• Patch (July 2019, KB unknown)
• netdom trust [...] /enabletgtdelegation:no
  o Each Domain Controller in each Forest ;-)  
• Put Admins in Protected Users Security Group  
• Account flag „Account is sensitive and cannot be delegated“ of Administrators (not Computers)  
• Disable Spooler on Domain Controllers
Windows Hacking Training (3 Day course)

@ SBA Research

https://www.sba-research.org/professional-services/advanced-training/windows-hacking/
Trust in the force you must.

Pentest you should
Questions
