Microsoft Exchange – Mailbox Post Compromise

Microsoft Exchange – Privilege Escalation

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 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.

Search the Lab

Search...

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

Enter your email address

Follow

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 pentest
2  Add-ADGroupMember -Identity "Exchange Trusted Subsystem" -Mem
```

```
[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

Recent Posts

- Microsoft Exchange – Privilege Escalation
- Microsoft Exchange – ACL
- Microsoft Exchange – Mailbox Post Compromise
- Microsoft Exchange – Code Execution
- Microsoft Exchange – NTLM Relay

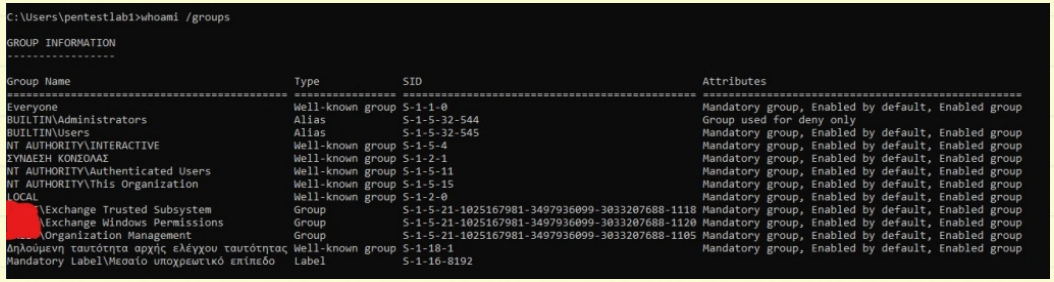
Categories

- 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.

```
whoami /groups
```



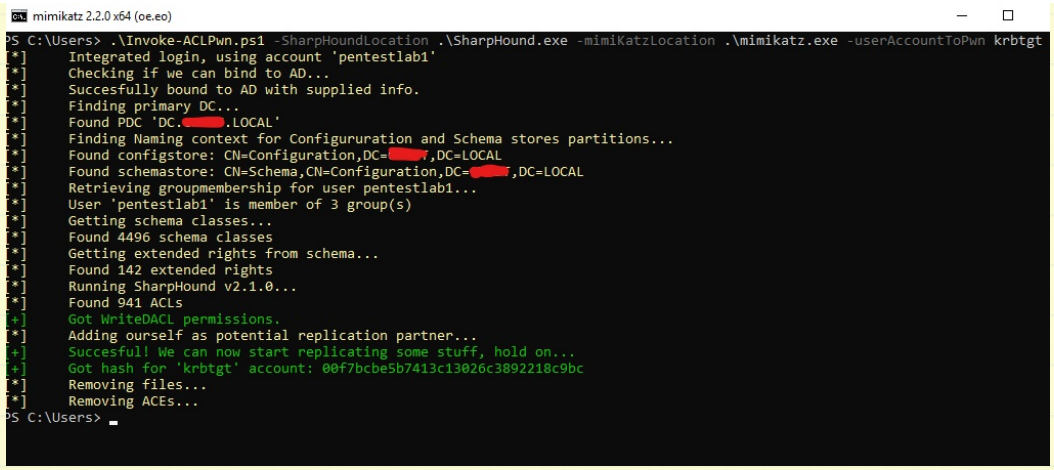
Verification that User was Added to Exchange Security Groups

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

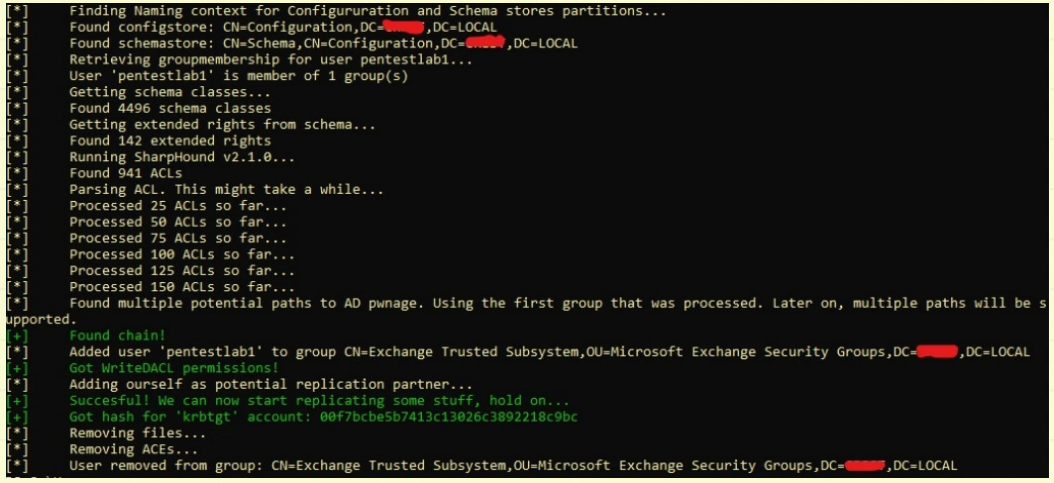
The script requires SharpHound for retrieving Access Control Entries (ACE's) and enumeration of domain objects and Mimikatz for DCSync operations (dumping the password hash of Kerberos account). The following command can be executed to retrieve the hash of the Kerberos account (krbtgt).

```
.\Invoke-ACLPwn.ps1 -SharpHoundLocation .\SharpHound.exe -mim
```



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.



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).

Rate this:

Rate This

Share this:

Twitter Facebook LinkedIn Pinterest Reddit Tumblr

Like

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

Enter your comment here...

Microsoft Exchange – Mailbox Post Compromise

Microsoft Exchange – Privilege Escalation