Step 1

Restart Windows 2003 in Directory Service Restore Mode.

Note: At startup, press F8 and choose Directory Service Restore Mode. It disables Active Directory.

When the login screen appears, log on as Local Administrator. You now have full access to the computer resources, but you cannot make any changes to Active Directory.

Step 2

You are now going to install SRVANY. This utility can virtually run any programs as a service. The interesting point is that the program will have SYSTEM privileges (LSA) (as it inherits the SRVANY security descriptor), i.e. it will have full access on the system. That is more than enough to reset a Domain Admin password. You will configure SRVANY to start the command prompt (which will run the 'net user' command).

Copy SRVANY and INSTSRV to a temporary folder, mine is called D:\temp. Copy cmd.exe to this folder too (cmd.exe is the command prompt, usually located at %WINDIR%\System32).

Start a command prompt, point to d:\temp (or whatever you call it), and type:

```
instsrv PassRecovery "d:\temp\srvany.exe"
```

(change the path to suit your own).

It is now time to configure SRVANY.

Start Regedit, and navigate to

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
```

Create a new subkey called Parameters and add two new values:

```
name: Application
type: REG_SZ (string)
value: d:\temp\cmd.exe

name: AppParameters
type: REG_SZ (string)
value: /k net user administrator 123456 /domain
```

Replace 123456 with the password you want. Keep in my mind that the default domain policy require complex passwords (including digits, respecting a minimal length etc) so unless you've changed the default domain policy use a complex password such as P@ssw0rd

Now open the Services applet (Control Panel\Administrative Tools\Services) and open the PassRecovery property tab. Check the starting mode is set to Automatic.

Go to the Log On tab and enable the option Allow service to interact with the desktop.

Restart Windows normally, SRVANY will run the NET USER command and reset the domain admin password.

Step 3

Log on with the Administrator's account and the password you've set in step #2.

Use this command prompt to uninstall SRVANY (do not forget to do it!) by typing:

```
net stop PassRecovery

sc delete PassRecovery
```

Now delete d:\temp and change the admin password if you fancy.

Done!

Supplement

Robert Strom has written a cool script that will completely automate this process. He wrote:

"My script is really just an automation of his process which performs all the post cleanup of itself. Launch one script and it's all done. No manual registry entries, the service is created, the service settings are all imported into the registry, etc."

Download it from HERE (186kb).

Note that you still need physical access to the DC and the ability to log on locally as the local administrator. If you do not have the local administrator's password use the following tip: Forgot the Administrator's Password?.

Thanks Robert!