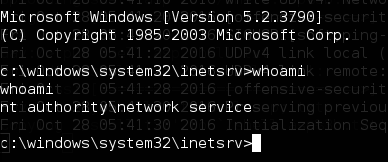
**Windows Privelege Escalation via Token Kidnapping**

If you have access to a box as nt authority\\network service (for example you’ve managed to upload [ASP.NET](http://ASP.NET/) shell) you can easily elevate your privileges on the box.

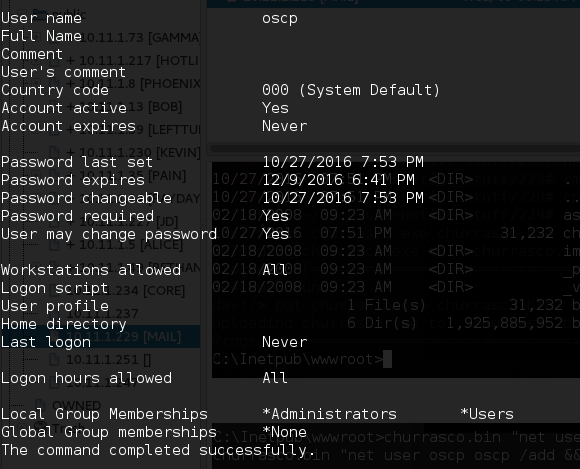


I’m against uploading binaries to the boxes (but still, it’s my favorite part), but as I know there’s no metasploit module for that so we have no choice. You can download the exploit [here](https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/6705.zip) and compile by yourself or you can use the one from sqlninja which is located at /usr/share/sqlninja/apps/churrasco.exe. It’s used by sqlninja in cases when we bruteforced sa password.

After uploading you can easily elevate your privileges (I tested it on Windows Server 2003). By entering:

`churrasco.bin "net user oscp oscp /add && net localgroup Administrators oscp /add"`

You can create admin account successfully.



You can read about this vulnerability on Microsoft [website](https://technet.microsoft.com/library/security/ms09-012):

This security update is rated Important for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.