

# Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

POST CATEGORY : [Windows Hacking Tricks](#)

Search

## How to Enable and Monitor Firewall Log in Windows PC

posted in [PENETRATION TESTING](#) , [WINDOWS HACKING TRICKS](#) on [MARCH 26, 2017](#)  
by [RAJ CHANDEL](#) with [0 COMMENT](#)

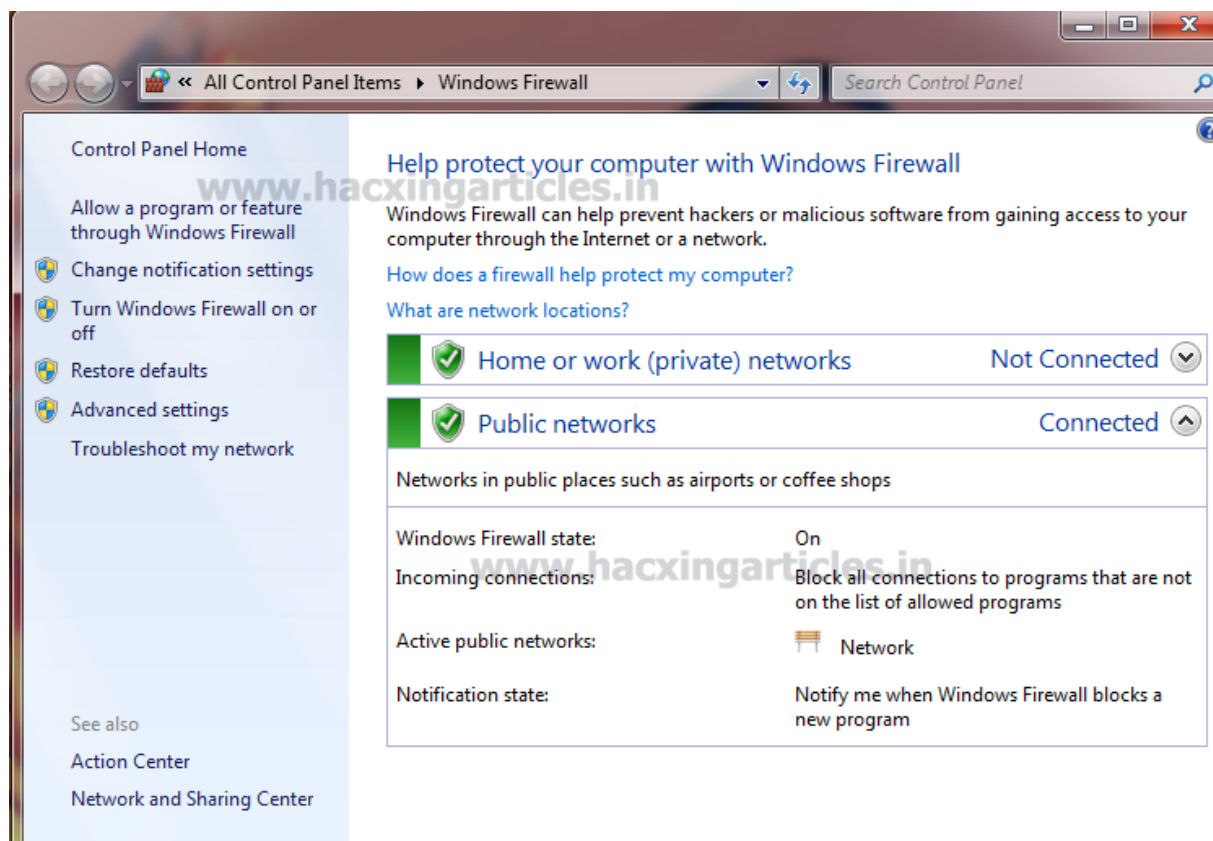
For any network administration it is very important that he should know how to check firewall logs in his network in order to maintain security of system. In this article you will learn more about firewall utility where we have try to describe how can any person check firewall log in his private network.

**LETS START!!!**

Subscribe to Blog via Email

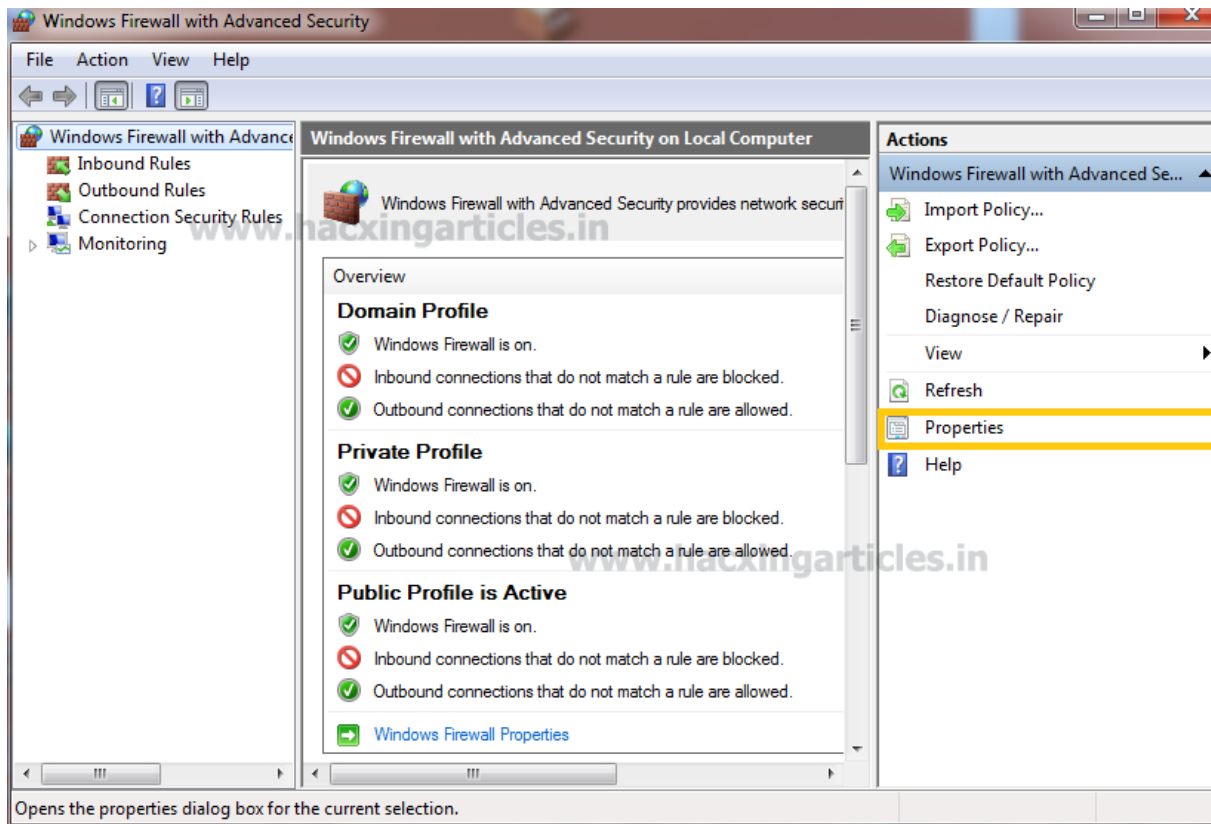
**SUBSCRIBE**

Let have a look where you will learn more about firewall security. Open windows firewall then select **advance setting** on the left side under control panel home.



Here we are at windows firewall advance setting; explore its **property tab** present on the right side of window's frame.

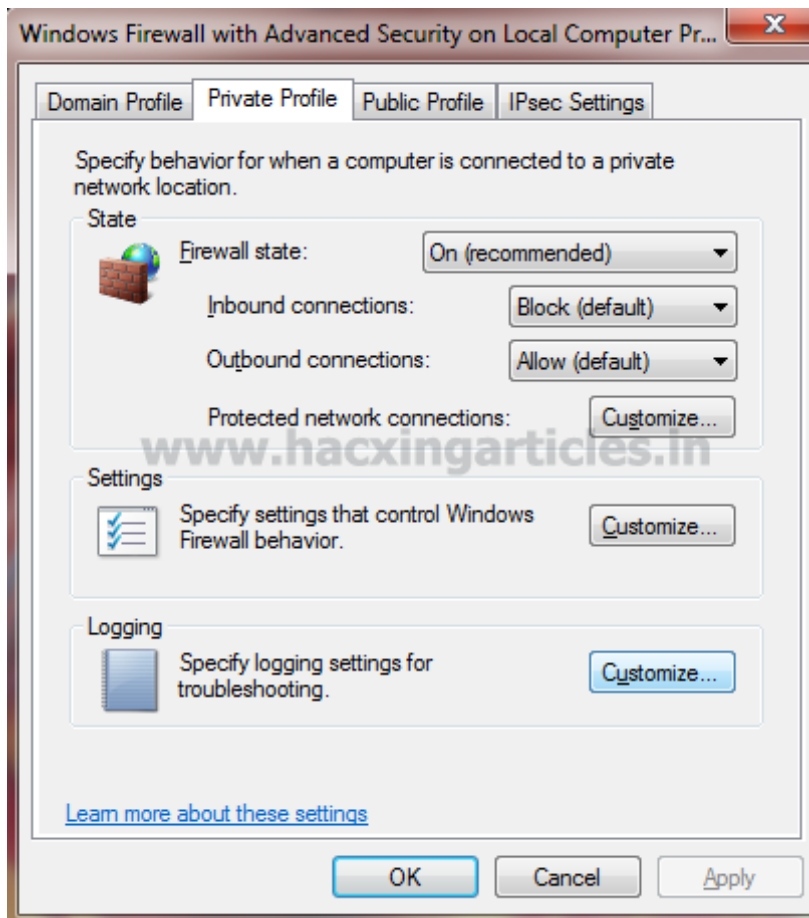




Now you can see the local computer property dialog box has been opened, here select the **private profile** option.

## Categories

- 🔖 BackTrack 5 Tutorials
- 🔖 Best of Hacking
- 🔖 Browser Hacking
- 🔖 Cryptography & Steganography
- 🔖 CTF Challenges
- 🔖 Cyber Forensics
- 🔖 Database Hacking
- 🔖 Domain Hacking
- 🔖 Email Hacking
- 🔖 Footprinting
- 🔖 Hacking Tools
- 🔖 Kali Linux
- 🔖 Nmap
- 🔖 Others
- 🔖 Penetration Testing
- 🔖 Social Engineering Toolkit
- 🔖 Trojans & Backdoors
- 🔖 Website Hacking
- 🔖 Window Password Hacking
- 🔖 Windows Hacking Tricks
- 🔖 Wireless Hacking
- 🔖 Youtube Hacking



Here another dialog box will get appear in front of you to configure **private profile** for firewall.

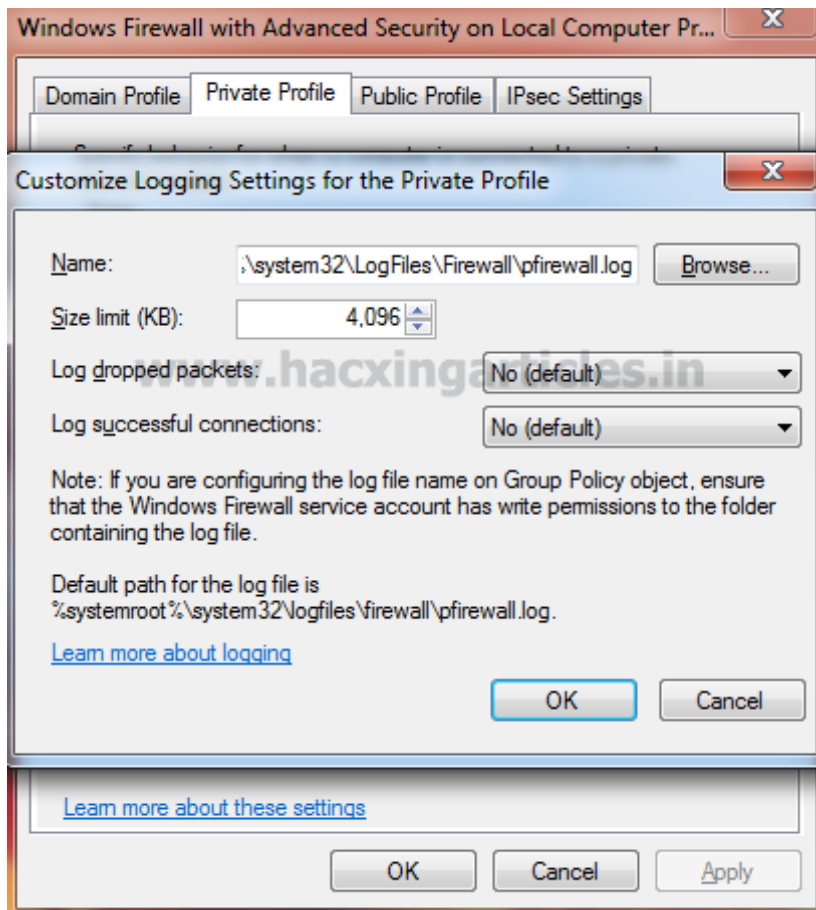
## Articles

Select Month

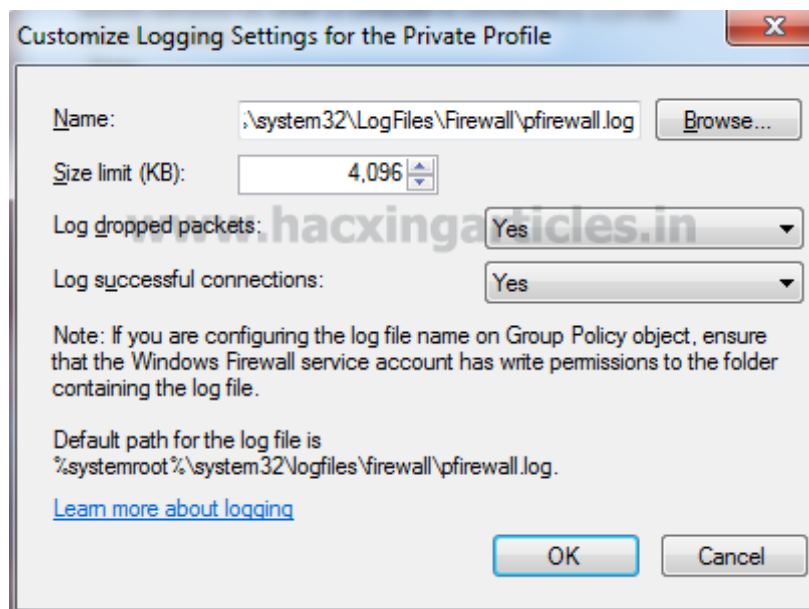


## Facebook Page

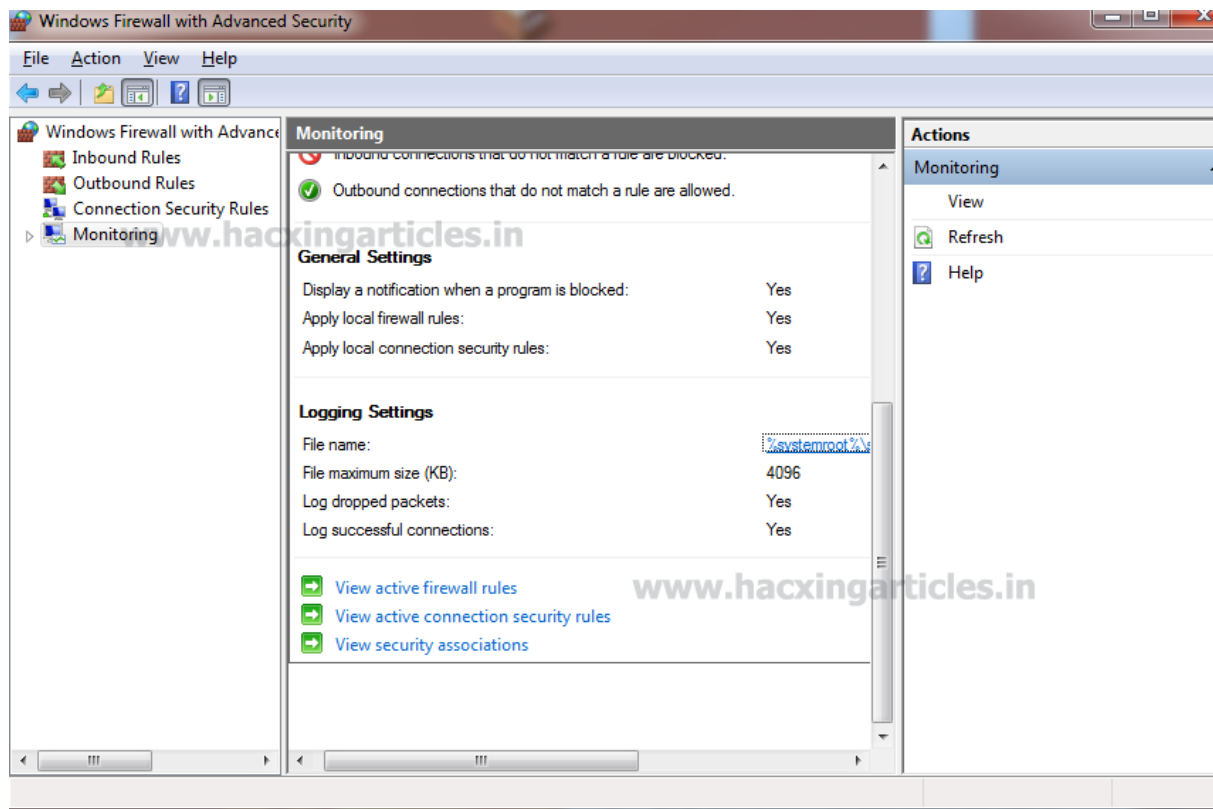




Only we need to manipulate two things in this profile without disturbing other settings. Change “**NO (default)**” into “**YES**” for log dropped packets and log successful connection as shown in given screenshot. At last click on **OK**.



Now again we are at advance security setting of firewall here bring your cursor down toward **monitoring** option. From screenshot you can see window frame for firewall monitoring where it contains **general** and **logging setting**. As we want to read firewall logs therefore now click on the **blue link** given as file name under logging setting.



**GREAT!!!** Finally we can read firewall log and can investigate firewall traffic in our network.



pfirewall - Notepad

File Edit Format View Help

```
2017-03-25 12:50:14 ALLOW UDP 127.0.0.1 239.255.255.250 57380 1900 0 ----- SEND
2017-03-25 12:50:14 ALLOW UDP 127.0.0.1 239.255.255.250 57380 1900 0 ----- RECEIVE
2017-03-25 12:50:14 ALLOW UDP fe80::d48a:9497:9d8a:473 ff02::1:3 56976 5355 0 ----- SEND
2017-03-25 12:50:14 ALLOW UDP 192.168.52.1 224.0.0.252 56976 5355 0 ----- SEND
2017-03-25 12:50:14 ALLOW UDP fe80::3438:ddba:37f8:cb2c ff02::1:3 56976 5355 0 ----- SEND
2017-03-25 12:50:14 ALLOW UDP 192.168.232.1 224.0.0.252 56976 5355 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP 192.168.232.1 192.168.232.254 68 67 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP fe80::65cc:174d:d2d9:b5c9 ff02::1:3 55163 5355 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP 192.168.1.101 224.0.0.252 55163 5355 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP fe80::d48a:9497:9d8a:473 ff02::1:3 52261 5355 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP 192.168.52.1 224.0.0.252 52261 5355 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP fe80::3438:ddba:37f8:cb2c ff02::1:3 52261 5355 0 ----- SEND
2017-03-25 12:50:15 ALLOW UDP 192.168.232.1 224.0.0.252 52261 5355 0 ----- SEND
2017-03-25 12:50:27 ALLOW UDP 192.168.1.101 192.168.1.1 55531 53 0 ----- SEND
2017-03-25 12:50:27 ALLOW ICMP 192.168.1.101 216.58.199.164 -- 0 ---- 8 0 - SEND
2017-03-25 12:50:29 ALLOW UDP 192.168.1.101 192.168.1.1 63577 53 0 ----- SEND
2017-03-25 12:50:32 ALLOW ICMP 192.168.1.101 216.58.199.164 -- 0 ---- 8 0 - SEND
2017-03-25 12:50:33 ALLOW ICMP 192.168.1.101 216.58.199.164 -- 0 ---- 8 0 - SEND
2017-03-25 12:50:34 ALLOW ICMP 192.168.1.101 216.58.199.164 -- 0 ---- 8 0 - SEND
2017-03-25 12:50:34 ALLOW UDP fe80::d48a:9497:9d8a:473 ff02::1:2 546 547 0 ----- SEND
2017-03-25 12:50:34 ALLOW UDP fe80::3438:ddba:37f8:cb2c ff02::1:2 546 547 0 ----- SEND
2017-03-25 12:50:43 ALLOW UDP 192.168.1.101 192.168.1.1 57060 53 0 ----- SEND
2017-03-25 12:50:43 ALLOW TCP 192.168.1.101 111.221.29.13 55086 80 0 - 0 0 0 --- SEND
2017-03-25 12:50:43 ALLOW UDP 192.168.1.101 192.168.1.1 61570 53 0 ----- SEND
2017-03-25 12:50:43 ALLOW TCP 192.168.1.101 23.205.218.128 55087 443 0 - 0 0 0 --- SEND
2017-03-25 12:50:53 ALLOW UDP 192.168.1.101 192.168.1.1 63527 53 0 ----- SEND
2017-03-25 12:50:53 ALLOW UDP 192.168.1.101 216.58.220.206 63528 443 0 ----- SEND
2017-03-25 12:50:53 ALLOW UDP 192.168.1.101 216.58.220.206 63529 443 0 ----- SEND
2017-03-25 12:51:00 ALLOW 2 192.168.1.101 224.0.0.252 -- 0 ----- SEND
2017-03-25 12:51:15 ALLOW UDP 192.168.1.1 239.255.255.250 1900 1900 0 ----- RECEIVE
2017-03-25 12:51:16 ALLOW TCP 192.168.1.101 204.79.197.200 55088 443 0 - 0 0 0 --- SEND
2017-03-25 12:51:16 ALLOW UDP 192.168.1.101 239.255.255.250 57379 1900 0 ----- SEND
2017-03-25 12:51:16 ALLOW UDP 127.0.0.1 239.255.255.250 57380 1900 0 ----- SEND
2017-03-25 12:51:18 ALLOW TCP 192.168.1.101 204.79.197.200 55092 443 0 - 0 0 0 --- SEND
2017-03-25 12:51:18 ALLOW UDP 192.168.1.101 192.168.1.1 54715 53 0 ----- SEND
2017-03-25 12:51:23 ALLOW TCP 192.168.1.101 204.79.197.200 55093 443 0 - 0 0 0 --- SEND
2017-03-25 12:51:23 ALLOW TCP 192.168.1.101 204.79.197.200 55094 443 0 - 0 0 0 --- SEND
2017-03-25 12:51:25 ALLOW UDP 192.168.1.101 192.168.1.1 61238 53 0 ----- SEND
2017-03-25 12:51:28 ALLOW UDP 192.168.1.101 192.168.1.1 61221 53 0 ----- SEND
```

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

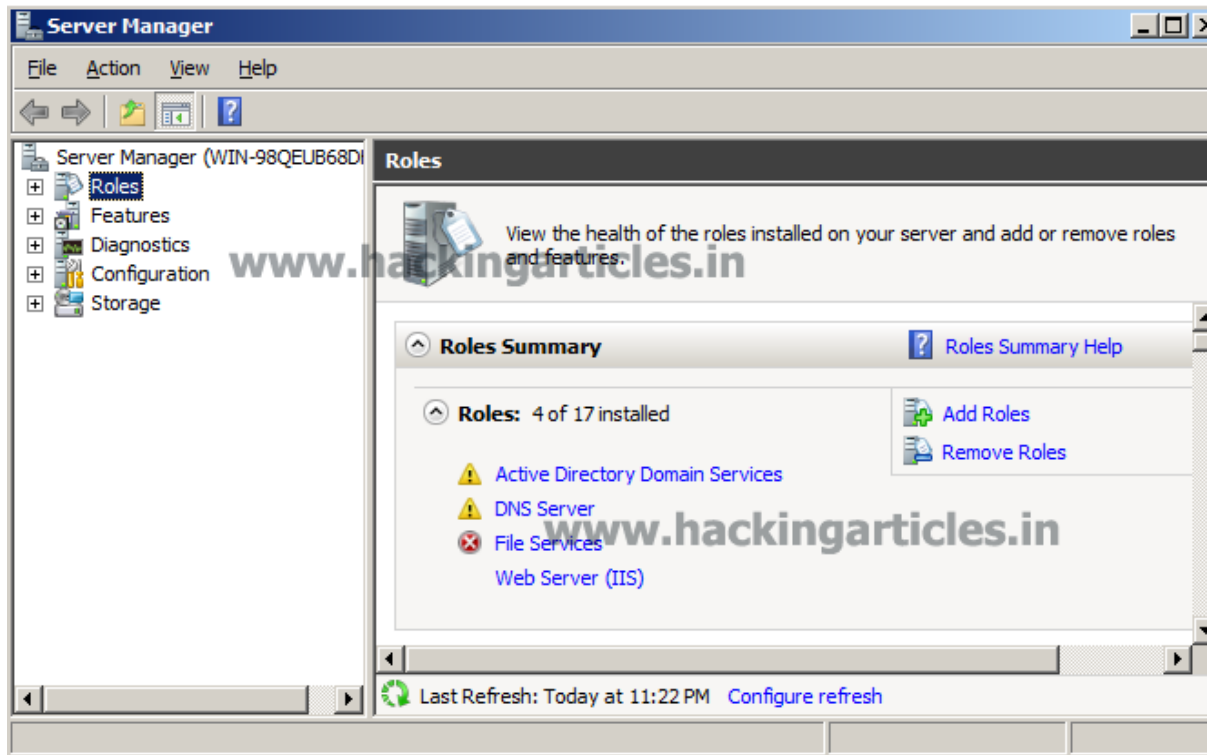


# Setup VPN Penetration Testing Lab in Server 2008

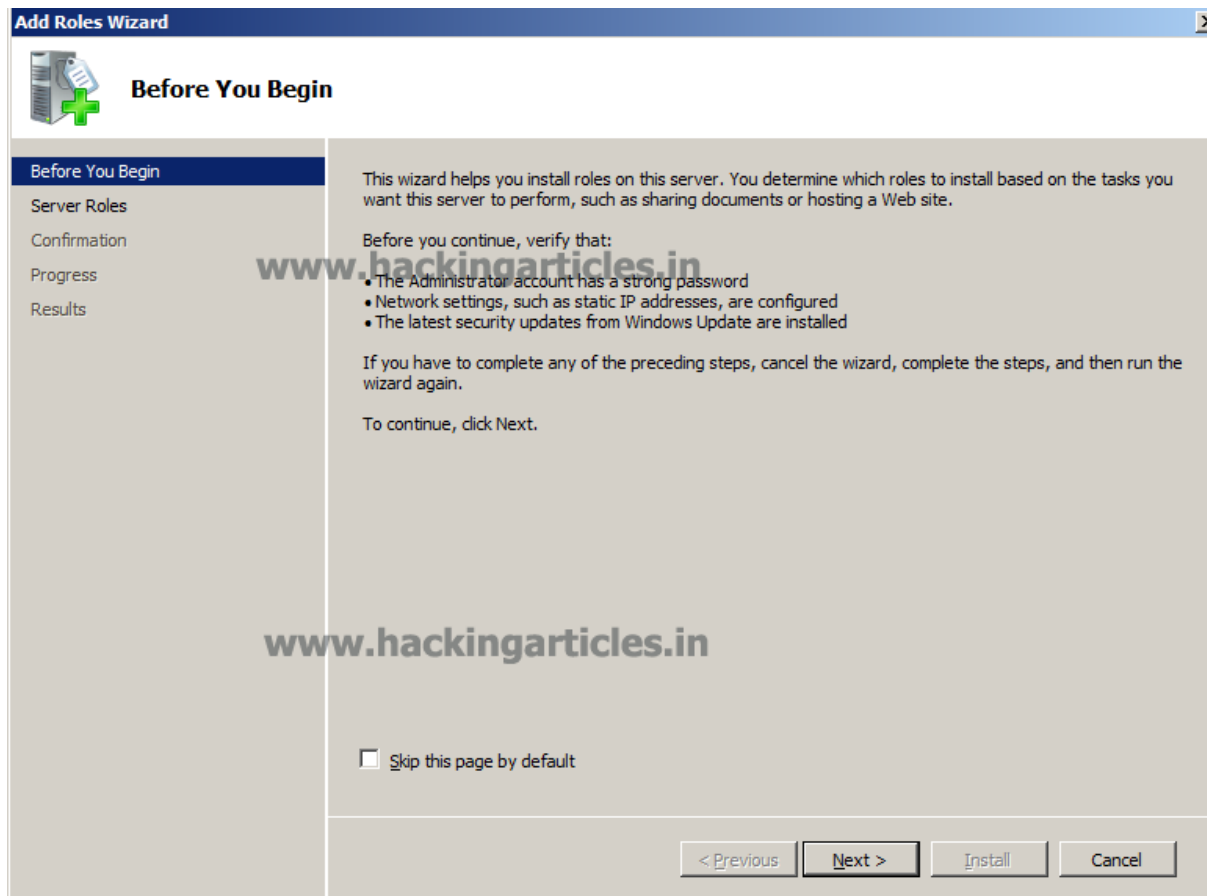
posted in [PENETRATION TESTING](#) , [WINDOWS HACKING TRICKS](#) on [AUGUST 23, 2016](#)  
by [RAJ CHANDEL](#) with [0 COMMENT](#)

You just need to follow the basic steps for configuring a remote access virtual private network (VPN) server using Server Manager, the Add Roles Wizard, and the Routing and Remote Access Server Setup Wizard. After you finish configuring a basic remote access VPN server, you can perform additional configuration tasks on client depending on the way you want to use the remote access VPN server.

***Start -> Administrative Tools -> Server Manager. Click Add Roles***




This wizard helps you install roll on your server, click on **next** to continue



Check the status of “**Network Policy Server**” under Role Services and click on **next**.

**Add Roles Wizard**

 **Select Server Roles**

**Before You Begin**

**Server Roles**

Network Policy and Access Services

Role Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☒ File Services (Installed)
- ☐ Hyper-V
- ☒ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☒ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

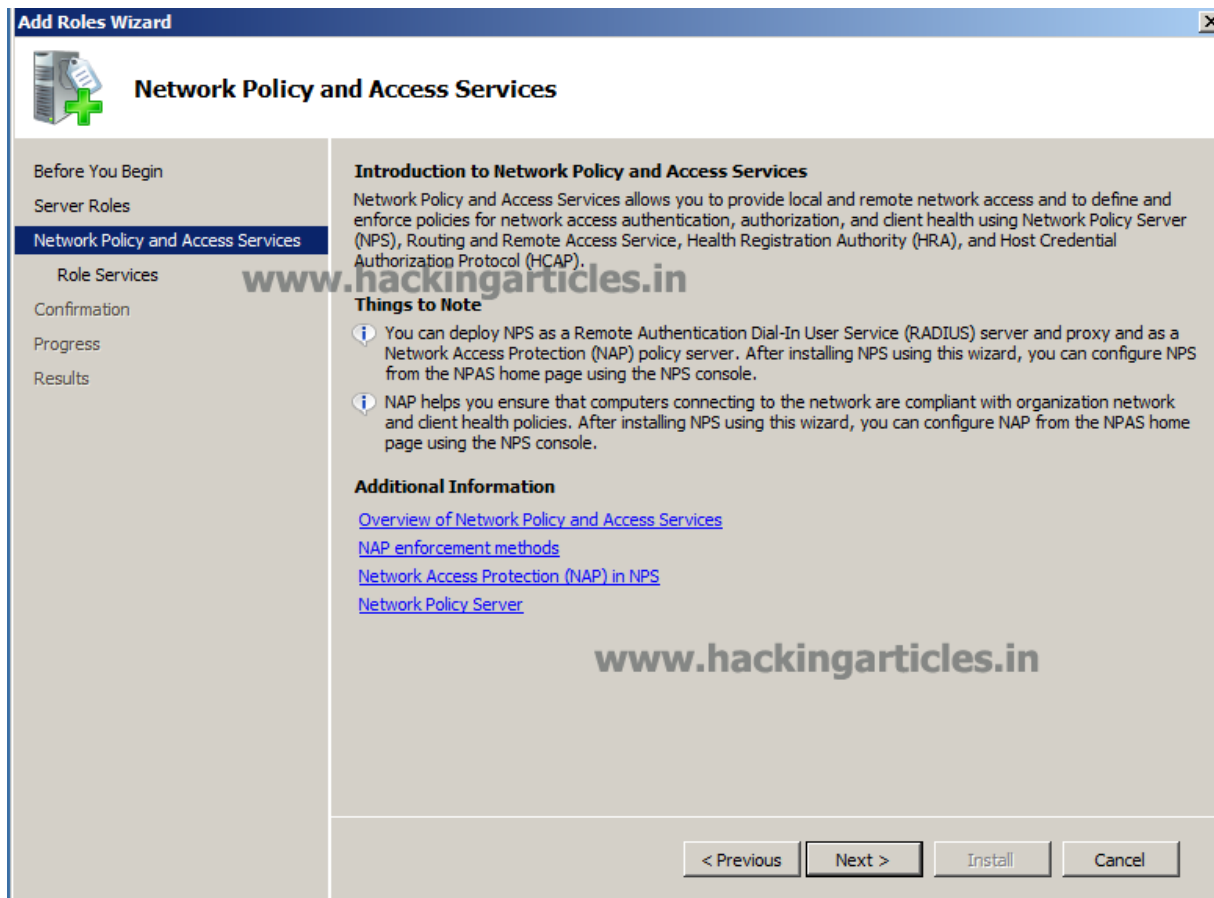
Description:

[Network Policy and Access Services](#) provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

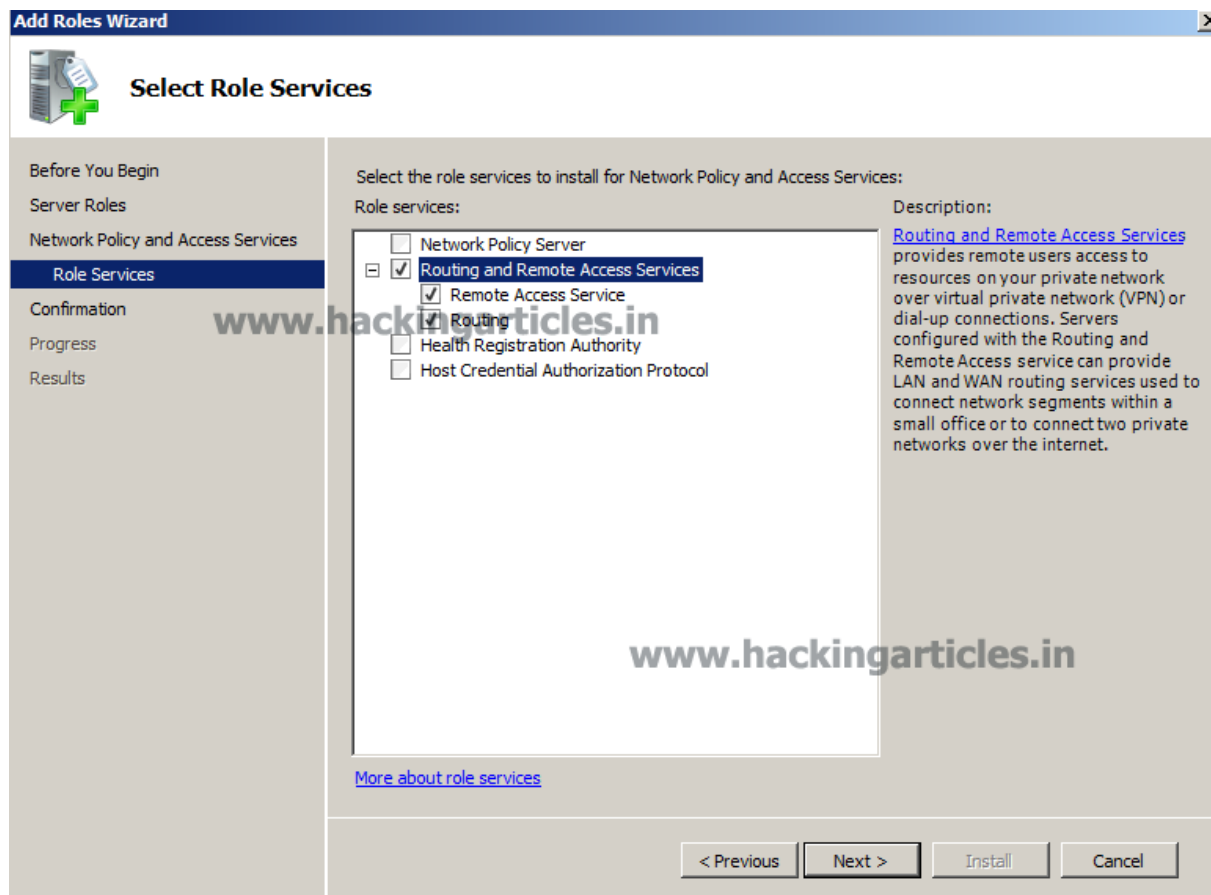
[More about server roles](#)

< Previous   Next >   Install   Cancel

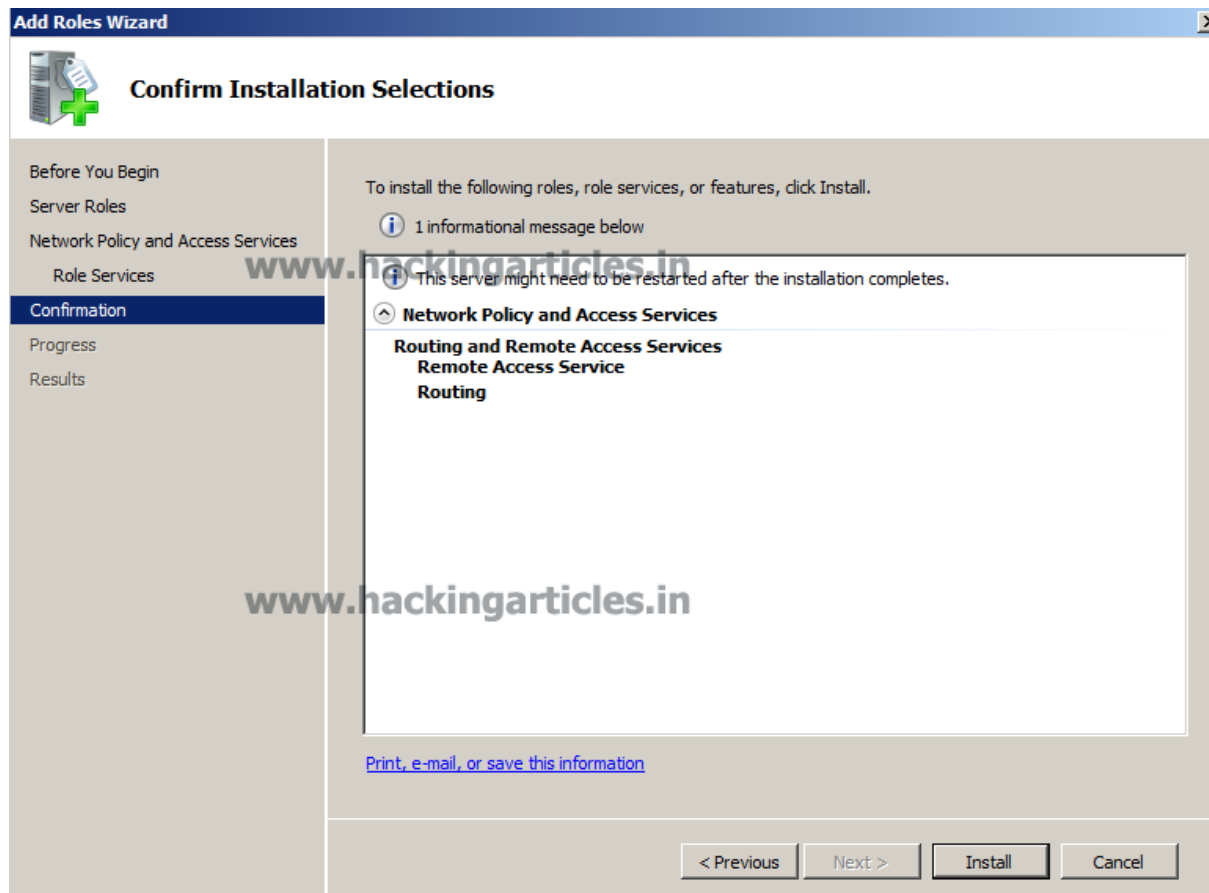
Read the requirements and click “**Next**” to continue.



On the following screen “Select Role Services” for Network Policy and Access Service, place a check mark on **Routing and Remote Access Services** and make sure “**Remote Access Service**” and “**Routing**” are selected as well. Click **next** to continue.



To install following role services for Network Policy and Access Service click on **Install**.

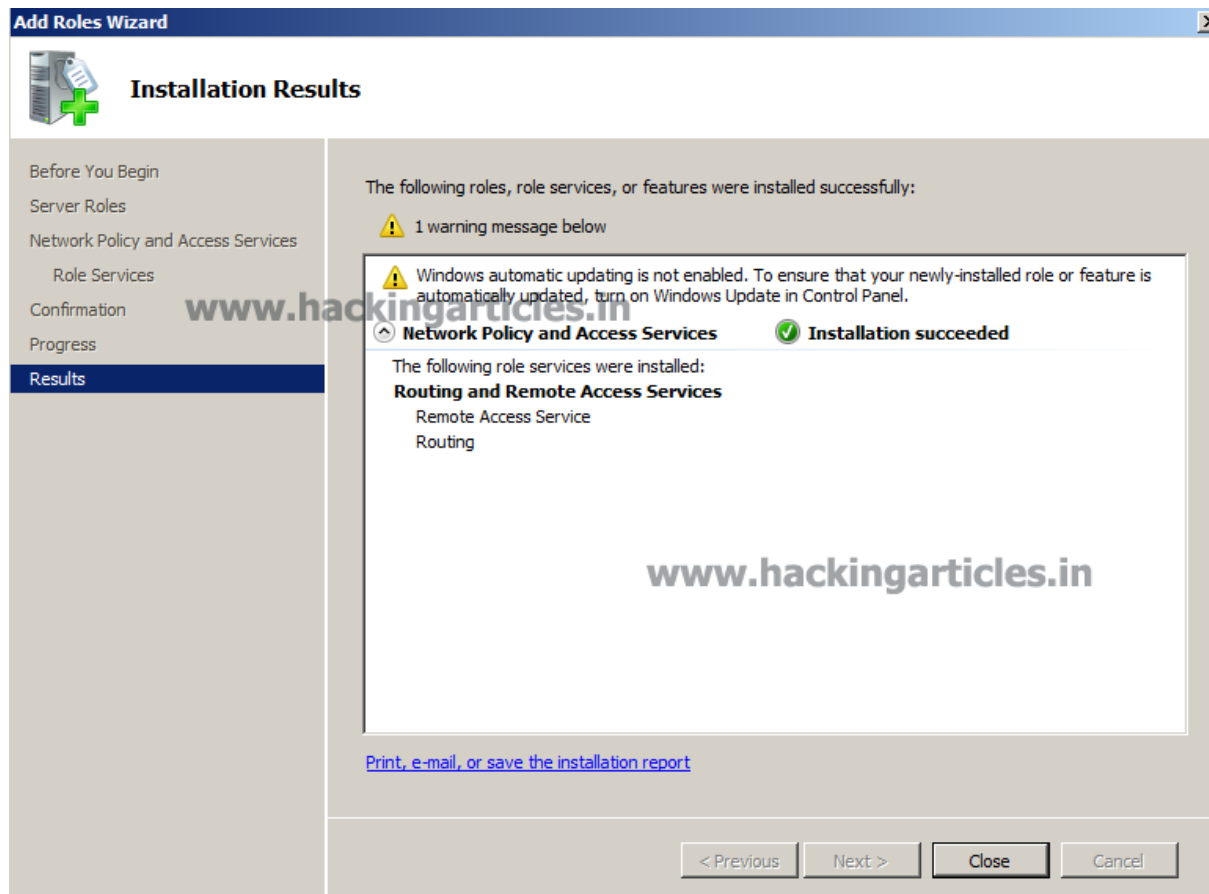


This shows the summary of Remote Access services and Routing were installed successfully.

Once the installation finishes, click **close** to end the wizard.

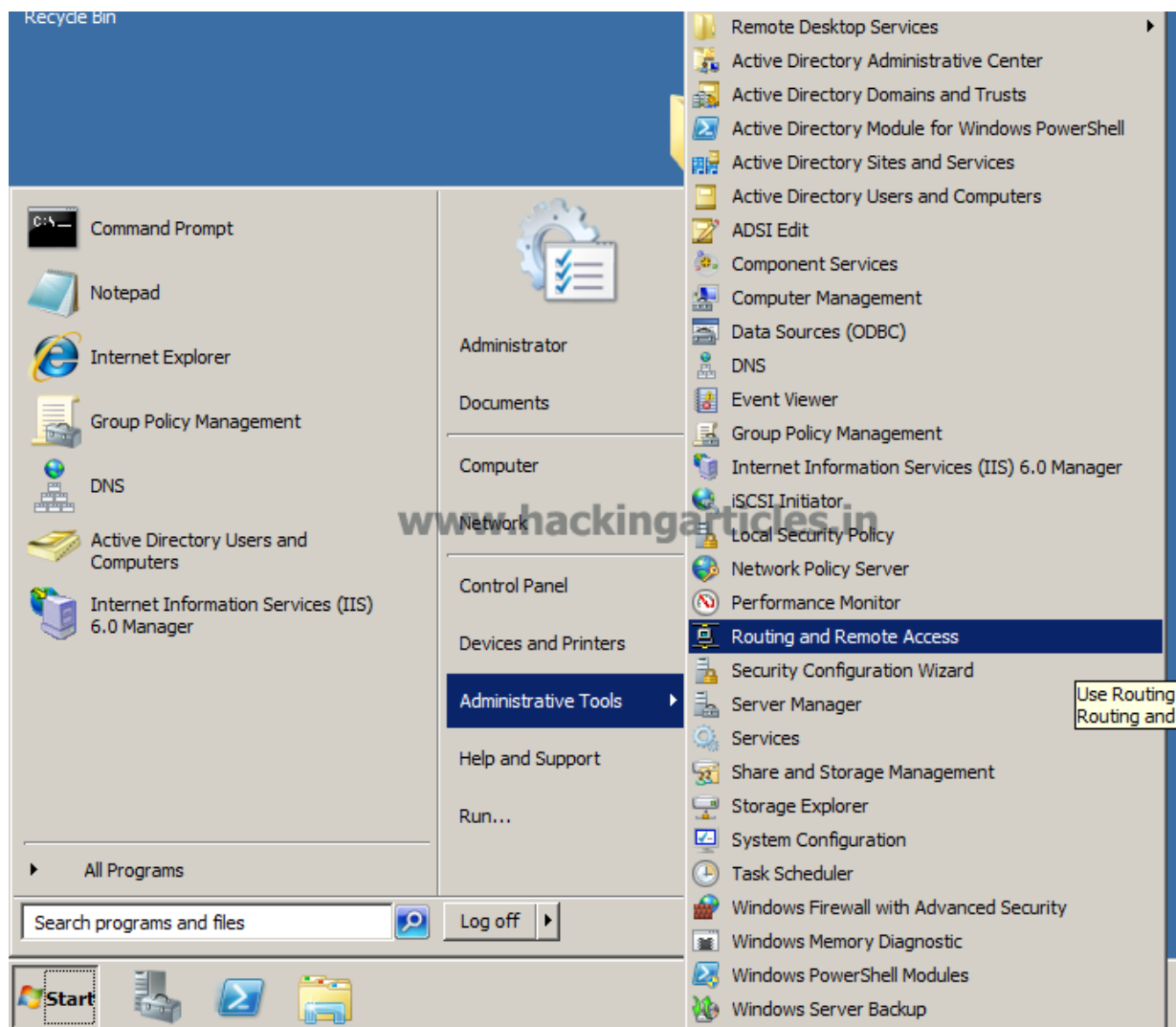
Till here I have completed installation of VPN in server.



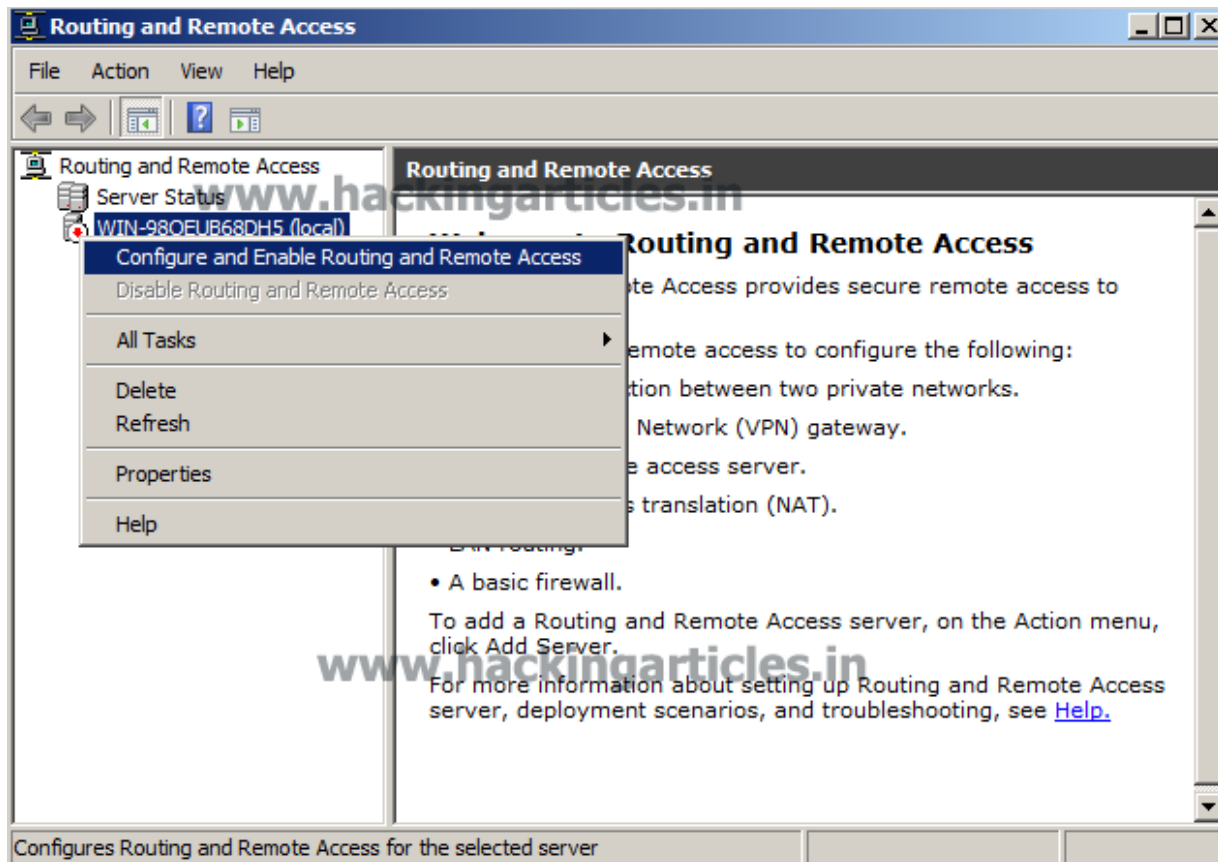


To complete configuration in Routing and Remote Access follow these step.

***Start -> Administrative Tools -> Routing and Remote Access***



In the console that opens, right click your server name and right click on “**Configure and Enable Routing and Remote Access**” this configures Routing and Remote Access on the selected server.



In the Wizard you can enable any of following combinations of services. I will choose **Custom Configuration** for my server and click on **Next**.

**Routing and Remote Access Server Setup Wizard**

**Configuration**  
You can enable any of the following combinations of services, or you can customize this server.

☐ Remote access (dial-up or VPN)  
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

☐ Network address translation (NAT)  
Allow internal clients to connect to the Internet using one public IP address.

☐ Virtual private network (VPN) access and NAT  
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

☐ Secure connection between two private networks  
Connect this network to a remote network, such as a branch office.

☒ Custom configuration  
Select any combination of the features available in Routing and Remote Access.

[For more information.](#)

< Back   Next >   Cancel

Next is Routing and Remote Access server setup wizard in which I am going to decide which type of access should be allows to client to access server network.

You can configure the selected services in the Routing and Remote Access console. I am selecting the Check Box **VPN access** service on this server and click on **next** to continue

**Routing and Remote Access Server Setup Wizard**

**Custom Configuration**  
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

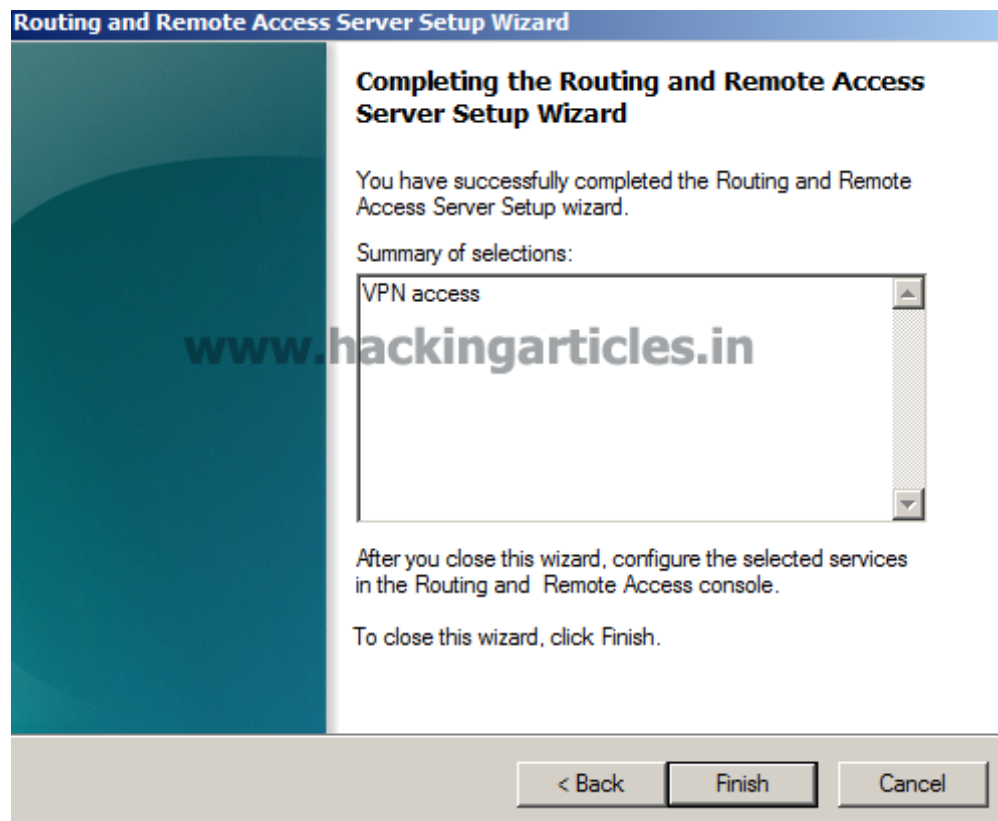
- ☒ VPN access
- ☐ Dial-up access
- ☐ Demand-dial connections ( used for branch office routing )
- ☐ NAT
- ☐ LAN routing

[www.hackingarticles.in](http://www.hackingarticles.in)

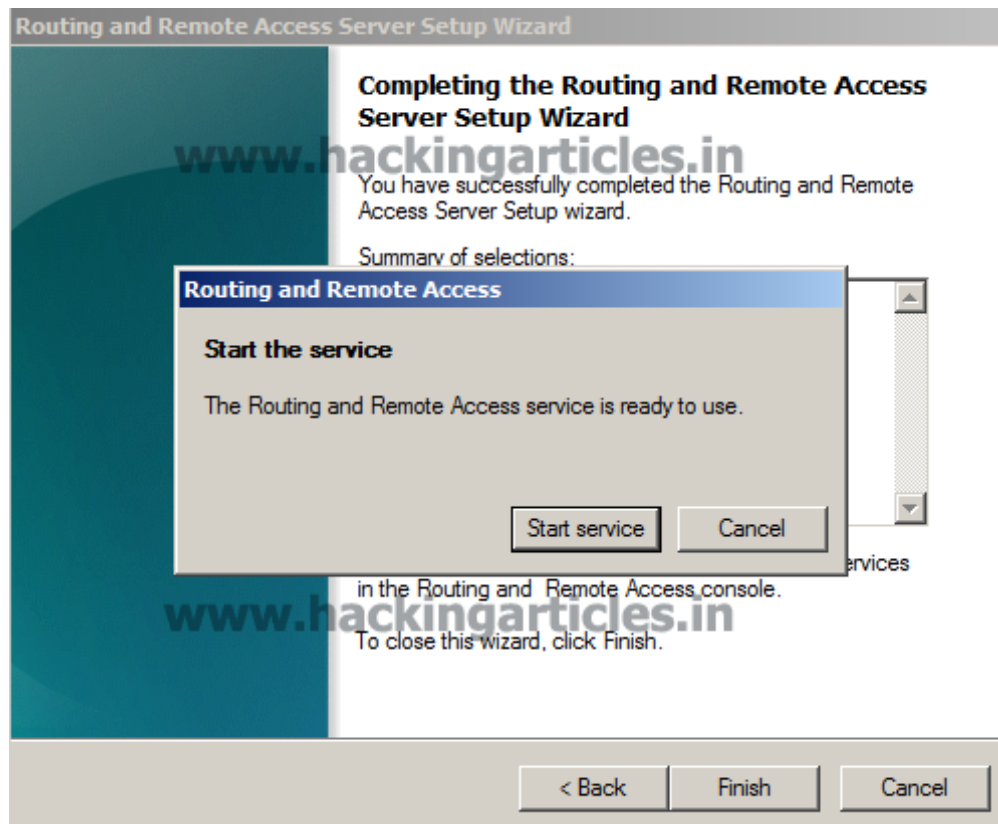
[For more information](#)

< Back   Next >   Cancel

Now you have successfully completed the task of VPN access service in your server, to close this wizard click on **finish**.

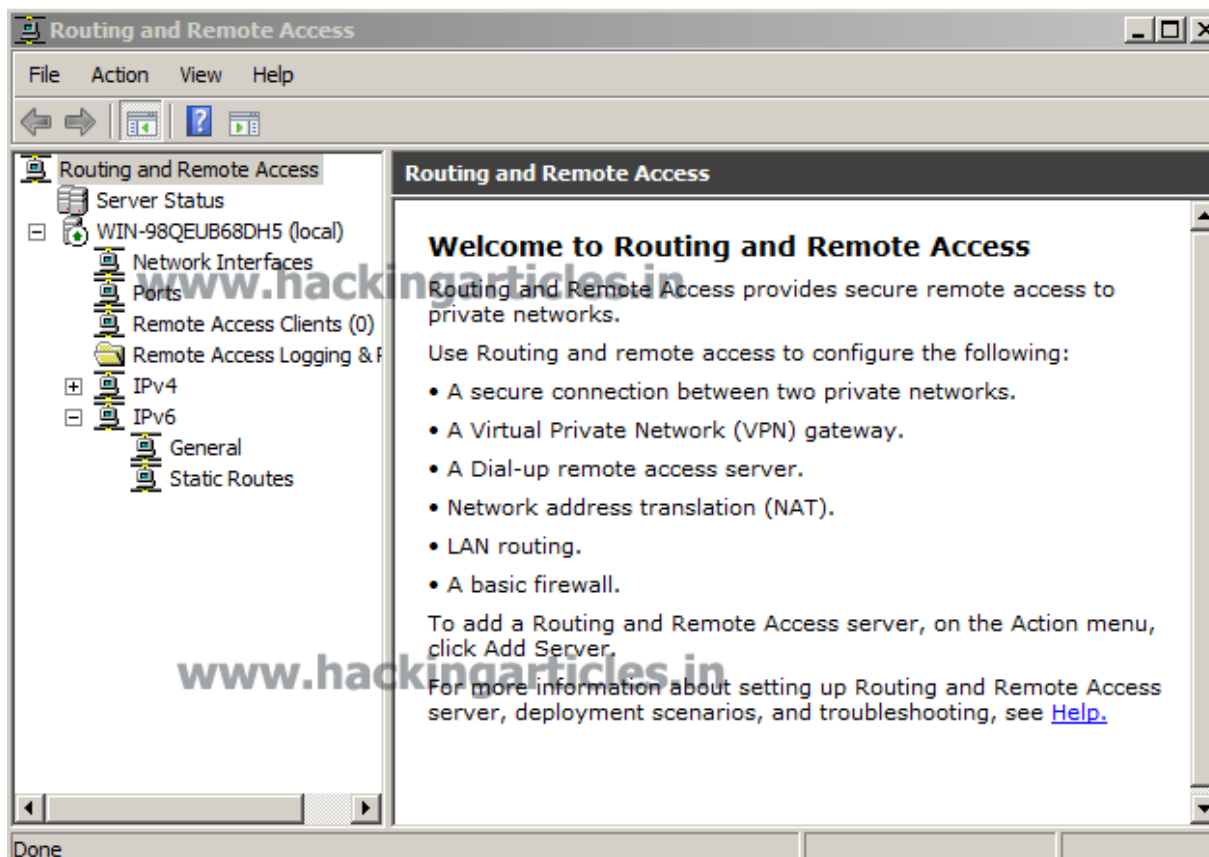


Now you will get the dialog box which shows message that Routing and Remote Access service is ready to use. So click on **Start Service**.



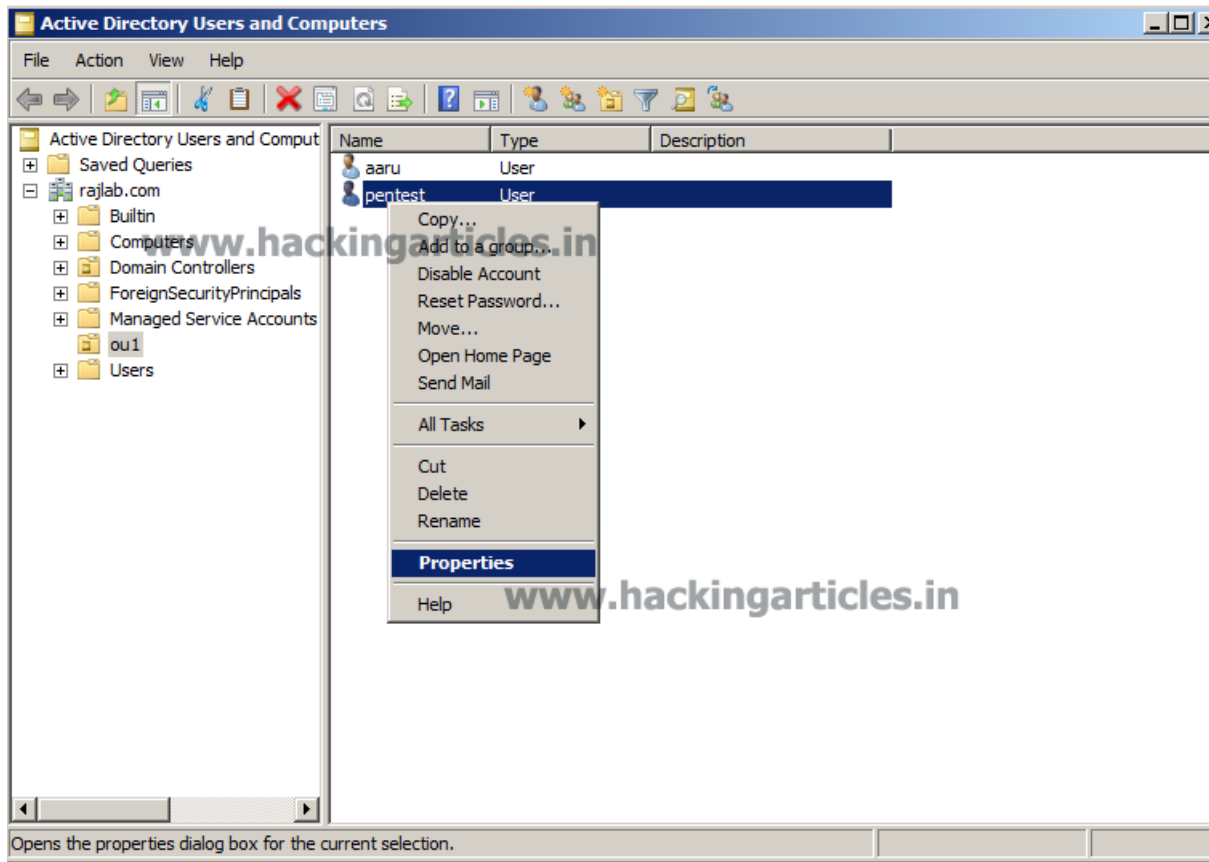
Once the process is finished, and you are back on the main Server Manager window, routing and remote access should now be up and running.





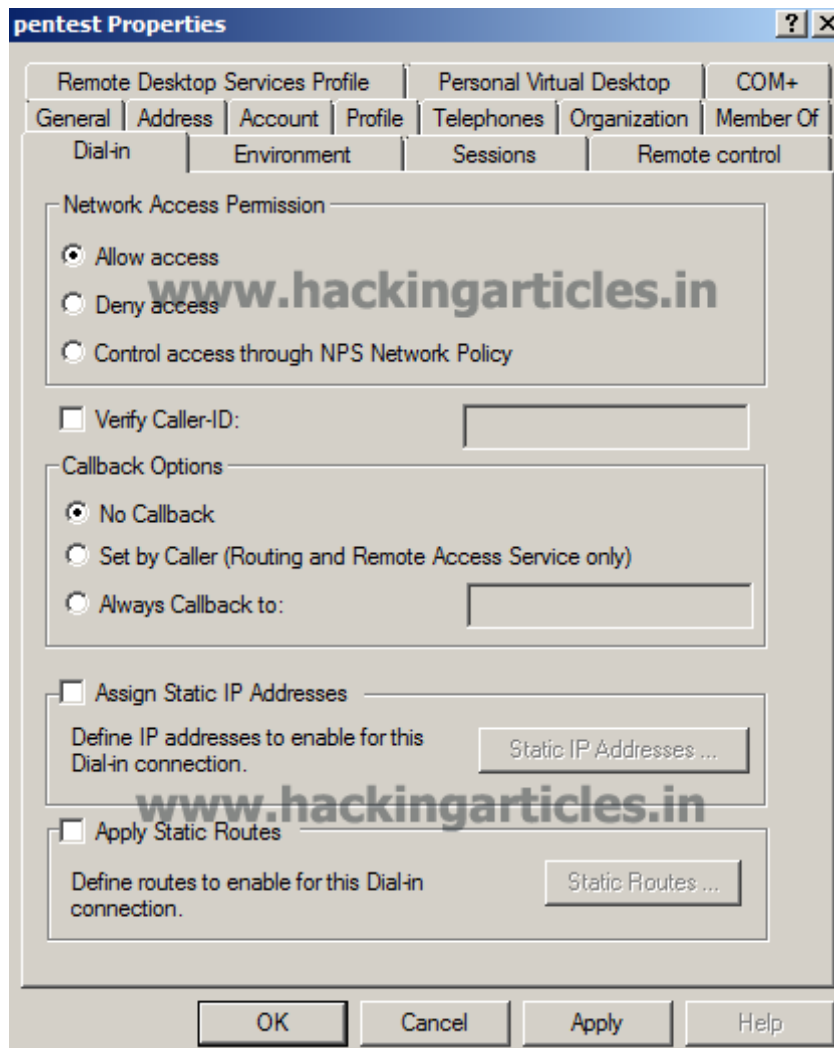
Once you have successfully configuration of Routing and Remote, the administrator will select the desire user and give privilege to access the server through VPN connection for connecting client from different location.

***Start -> Administrative Tools -> Active Directory Users and Computers -> Right Click the properties of an user***



Click on the **Dial-In** tab and under “Network Access Permission” select **Allow Access**. Click on **Apply** and **Ok** to finish. Only selected client will be able to connect with server network through VPN using different network.

This was first phase of VPN configuration on server-side performs by administrator.



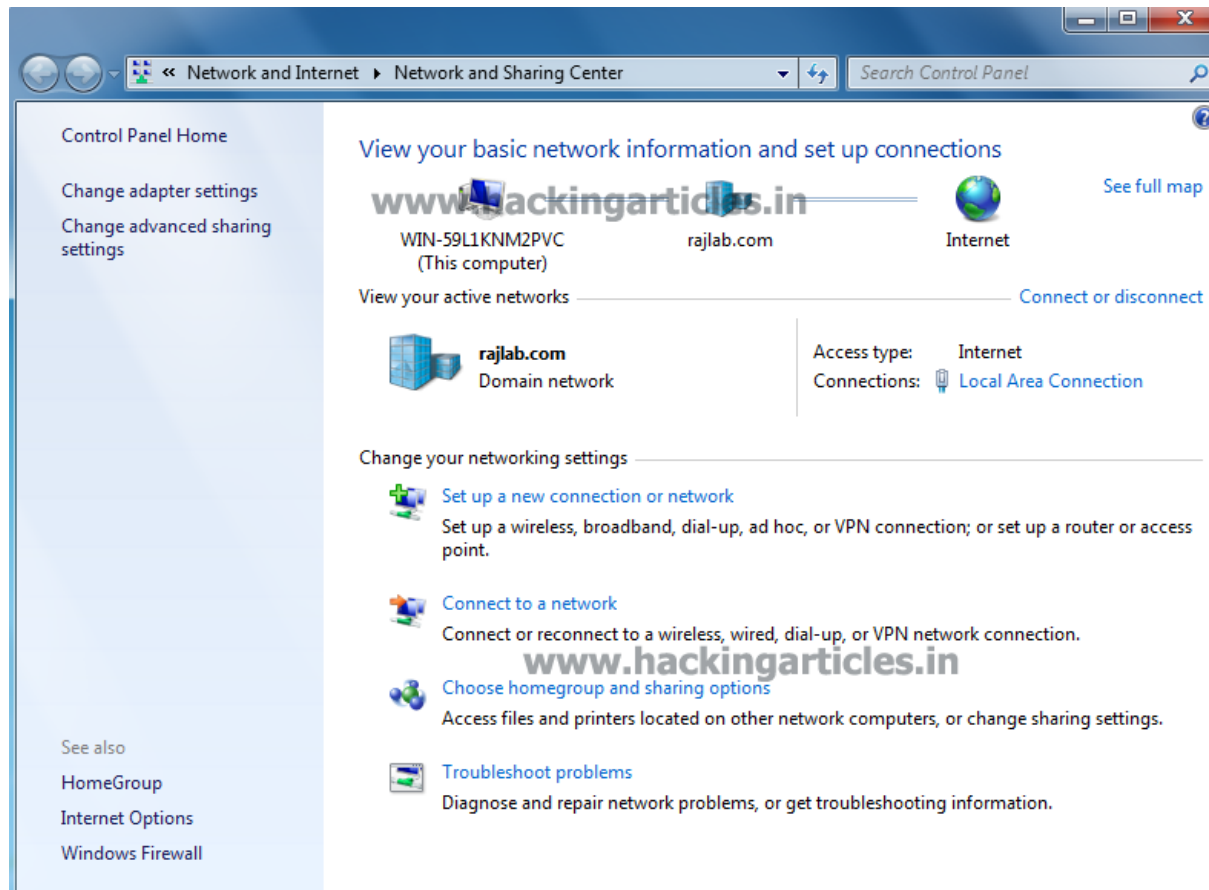
## SETUP VPN CONNECTION FOR CLIENT ON WINDOWS 7

Setting up a client connection to a VPN network is very similar to setting up an old-fashioned Dial-Up connection through a phone line. You need to enter a server address (hostname or IP), user and password. Once connected, this system will receive an IP

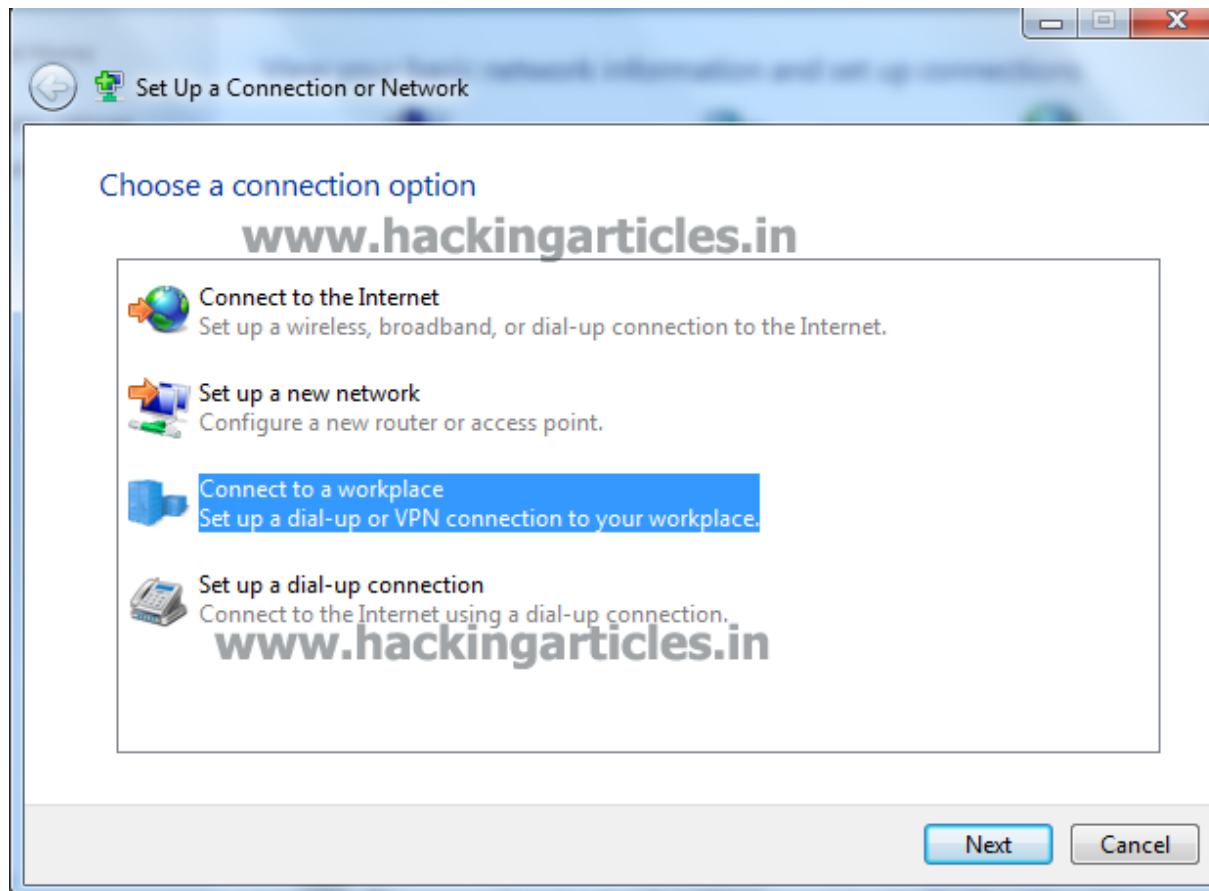
address within the VPN network, so you'll be able to access it from any other machines also connected to the same VPN network.

Click on the **Start -> Control Panel -> Network and Internet -> Network and Sharing Center**

Change your network settings click on setup a new connection or network option, this contains different types of network connection options like broadband, dial-up, VPN or set up a router or access point.



Here you can many other options as I told, I will choose **connect to a workplace** to set a dial-up or VPN connections to your workplace. This option will set the connection to a workplace or say to our server for the client.

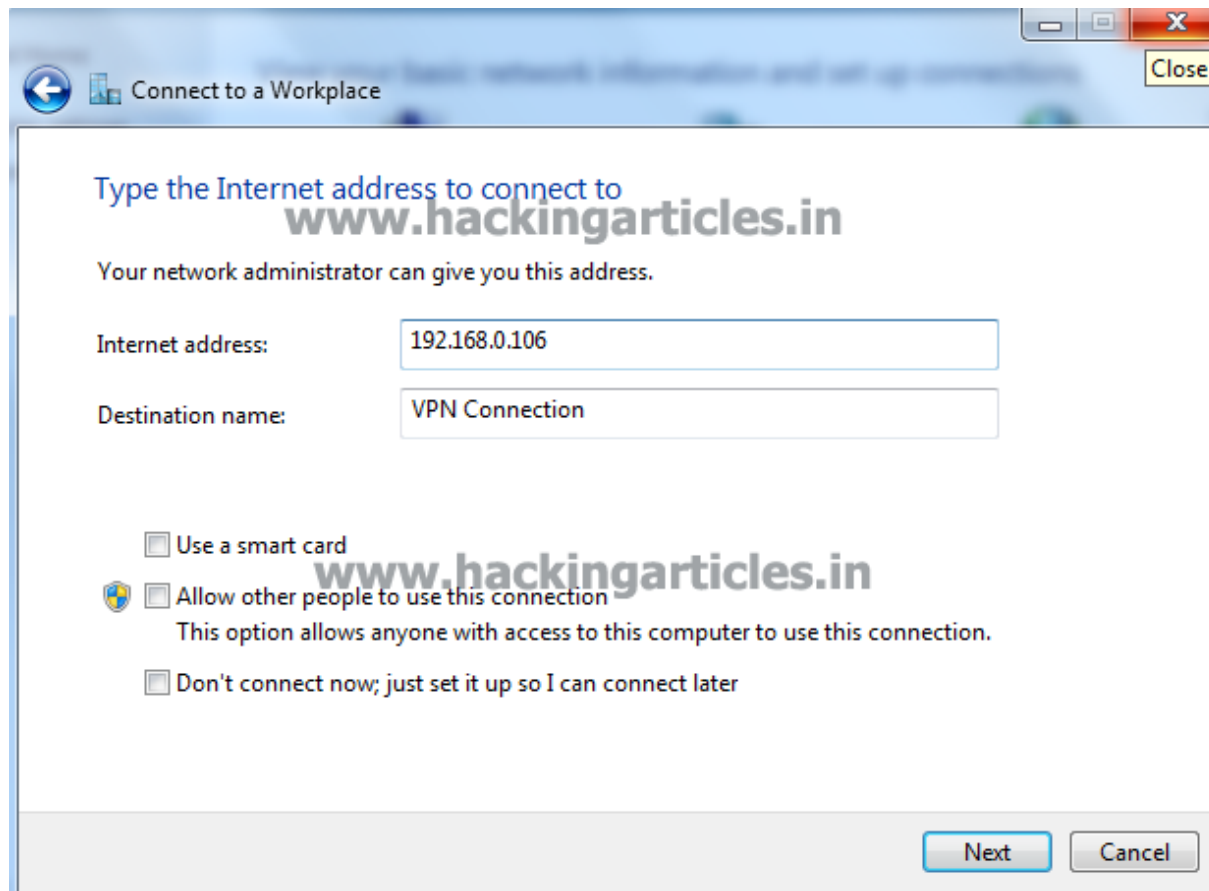


Now you will see next wizard for connect to workplace, which will ask for type of connection through which you will connect to your workplace or server.

My option will be **use my internet connection (VPN)** and the will be established using internet.



Now connecting network you must aware of IP address of workplace or say server. **192.168.0.106** it is the IP of my windows server 2008 r2 having VPN setup and configuration ,so I have mention this IP in **Internet Address** for connection



Now I had set privilege for user **pentest** to Allow Access for VPN connection. When you will try to connect it will ask for your credentials for authentication. Client will enter his **username** and **password** for establishing connection and click on **connect**.



Connect to a Workplace

Type your user name and password

User name: pentest

Password: ...

☐ Show characters

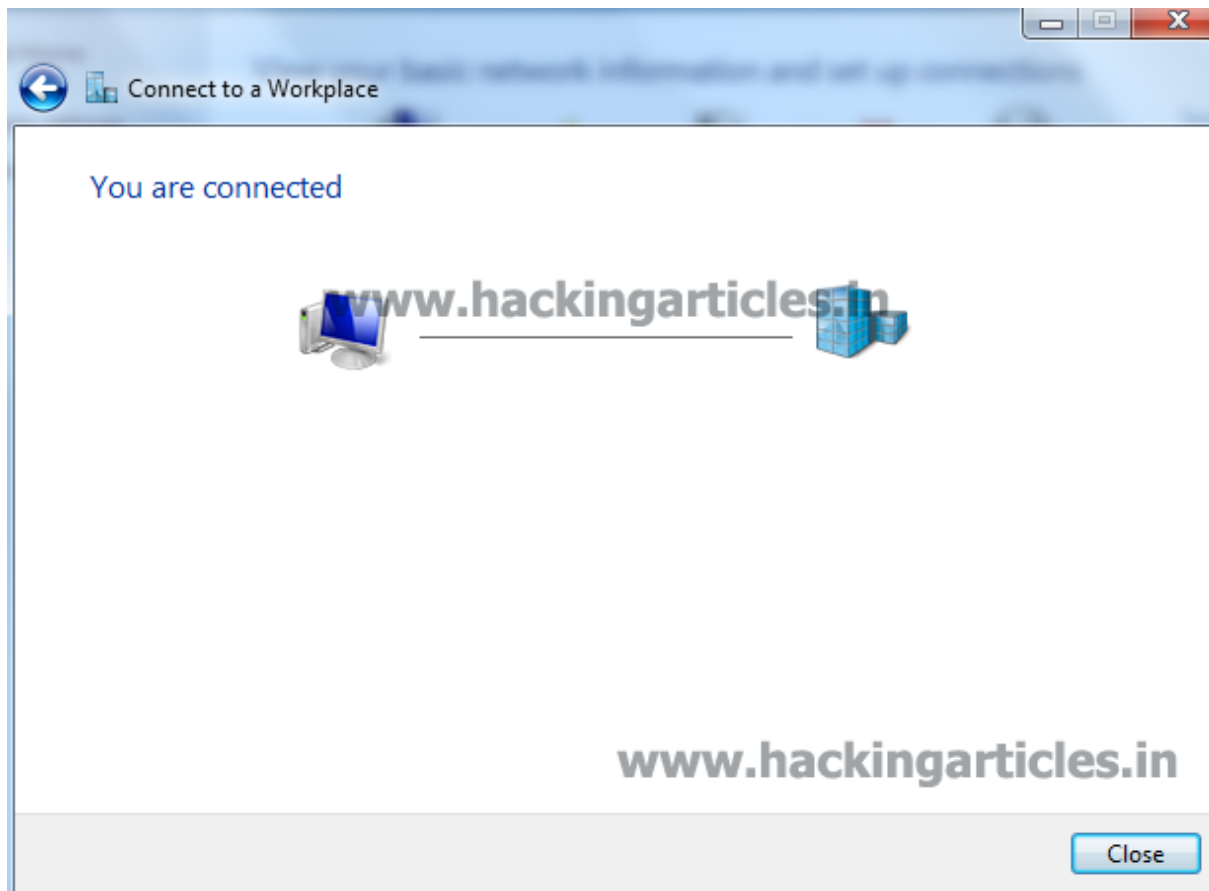
☐ Remember this password

Domain (optional):

Connect Cancel

When given credential will be found authorized, it will allow client to connect with workplace and provide VPN connection.

This is unshared and secure connection over internet between client and server for sharing data in a transparent medium.



To ensure that you have successful VPN connection open your **command prompt** and type **ipconfig** this show another IP over LAN.

My IP is **192.168.0.104** under PPP adapter VPN connection, which will be used for login in server to access network and share data, as I am also having my LAN IP **192.168.0.105**. This shows my VPN connection is established successfully.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\pentest>ipconfig

Windows IP Configuration

PPP adapter VPN Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.0.104
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 0.0.0.0

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.0.105
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{9368D504-B6C0-4258-BD54-54DD5944A242}:

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

Tunnel adapter isatap.{BB8B7A9B-DAC5-4E44-A590-94BF9F98586B}:

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

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets.

## Remote Windows PC Enumeration using PSTools

posted in **PENETRATION TESTING** , **WINDOWS HACKING TRICKS** on **AUGUST 18, 2016**  
by **RAJ CHANDEL** with **0 COMMENT**

PS Tools Kit is a collection of 13 tools developed by Mark Russinovich. These tools are command-line tool that lets you execute processes on remote systems and redirect console

applications' output to the local system so that these applications appear to be running locally. All of these are special tools that are compatible with the NT windows version or later. Being a console application, these tools can work on both local computer and remote host. These tools require no manual installation of software on the remote system, and they let you specify alternative credentials to access the remote system. The "Ps" prefix in PsList relates to the fact that the standard UNIX process listing command-line tool is named "ps", so this prefix has been adopted for all the tools in order to tie them together into a suite of tools named PsTools.

You can download PsTool Kit from -> <https://technet.microsoft.com/en-us/sysinternals/pstools.aspx>

Listed below are all tools in the said tool kit:

- **PsExec** – execute processes remotely
- **PsFile** – shows files opened remotely
- **PsGetSid** – display the SID of a computer or a user
- **PsInfo** – list information about a system
- **PsPing** – measure network performance
- **PsKill** – kill processes by name or process ID
- **PsList** – list detailed information about processes
- **PsLoggedOn** – see who's logged on locally and via resource sharing (full source is included)
- **PsLogList** – dump event log records
- **PsPasswd** – changes account passwords
- **PsService** – view and control services
- **PsShutdown** – shuts down and optionally reboots a computer
- **PsSuspend** – suspends processes

Let us now learn how we will use these through command prompt one by one

Firstly, let us open PSTool Kit and to do so open your command prompt and open PSTool kit using cd command as shown below :

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>cd pstools
C:\Users\Administrator\Desktop\PSTools>dir
Volume in drive C has no label.
Volume Serial Number is 660B-ADA4

Directory of C:\Users\Administrator\Desktop\PSTools

17-08-2016  14:30    <DIR>          .
17-08-2016  14:30    <DIR>          ..
03-03-2016  21:44             7,490 Eula.txt
28-06-2016  11:44      339,096 PsExec.exe
28-06-2016  11:41      374,944 PsExec64.exe
28-06-2016  11:35      149,664 psfile.exe
28-06-2016  11:32      168,608 psfile64.exe
05-07-2016  17:45      287,392 PsGetsid.exe
05-07-2016  17:40      326,824 PsGetsid64.exe
05-07-2016  17:32      313,496 PsInfo.exe
05-07-2016  17:27      351,904 PsInfo64.exe
28-06-2016  10:57      284,320 pskill.exe
28-06-2016  10:52      318,624 pskill64.exe
28-06-2016  10:44      178,848 pslist.exe
28-06-2016  10:42      202,400 pslist64.exe
18-06-2016  00:51      151,728 PsLogcat.exe
```

## Get SID

Once you have open PSTool kit, run **dir** command so that you can see the list of al tools.

Now, we run a command that will help us use PSGetsid tool in the Tool Kit. The command is:

**PSGetsidc64.exe \\192.168.1.104 -u administrator -p Ignite@123**

Here,

192.168.1.104 -> our victim's IP

-u -> denotes username

Administrator -> username

-p -> denotes password

Ignite@123 -> password

```
C:\Users\Administrator\Desktop\PSTools>PsGetsid64.exe \\192.168.1.104 -u administrator -p Ignite@123
www.hackingarticles.in
PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\192.168.1.104:
S-1-5-21-3168362048-22907649-2562303471
www.hackingarticles.in
C:\Users\Administrator\Desktop\PSTools>
```

## System Information

Executing these commands for system information of remote PC.

Next, we will learn about psinfo.exe tool which gives us all the necessary information of the remote PC. To make this tool work type:

**psinfo.exe \\192.168.1.104 -u administrator -p Ignite@123**

```
C:\Users\Administrator\Desktop\PSTools>psinfo.exe \\192.168.1.104 -u administrator -p Ignite@123

PsInfo v1.78 - Local and remote system information viewer
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\192.168.1.104:
Uptime:                0 days 0 hours 45 minutes 8 seconds
Kernel version:        Windows Server 2008 R2 Standard, Multiprocessor Free
Product type:          Server (Domain Controller)
Product version:       6.1
Service pack:          0
Kernel build number:    7601
Registered organization: Microsoft
Registered owner:       Microsoft
TE version:            8.0000
System root:           C:\Windows
Processors:            4
Processor speed:        3.3 GHz
Processor type:         Intel(R) Core(TM) i3-4130 CPU @
Physical memory:        3182 MB
Video driver:           Intel(R) HD Graphics 4400

C:\Users\Administrator\Desktop\PSTools>
```

## Share Folder

After this command has been run, it will give you the information as you can see above.

Moving forward, we will now make psfile tool work by typing the following command:

```
psfile64.exe \\192.168.1.104 -u administrator -p Ignite@123
```



```
C:\Users\Administrator\Desktop\PSTools>psfile64.exe \\192.168.1.104 -u administrator -p Ignite@123

PsFile v1.03 - Lists files and directories opened remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals
www.hackingarticles.in

Files opened remotely on 192.168.1.104:

[23] D:\Share\
      User:   pc6
      Locks:  0
      Access:
[24] E:\user Share\
      User:   pc6
      Locks:  0
      Access: www.hackingarticles.in
[438] E:\user Share\
      User:   Administrator
      Locks:  0
      Access:
[439] E:\CEH V9 Tools\
      User:   Administrator
      Locks:  0
      Access:
[495] D:\Share\
      User:   Administrator
      Locks:  0
      Access: Read
www.hackingarticles.in
```

## Process Information

Execution of this command will help us to see every file and directories that are remotely open on the PC of victim.

Our next tool is pslist and to make it work type:

```
pslist64.exe \\192.168.1.104 -u administrator -p Ignite@123
```

```

C:\Users\Administrator\Desktop\PSTools>pslist64.exe \\192.168.1.104 -u administrator -p Ignite@123

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for 192.168.1.104:

Name                Pid Pri Thd  Hnd  Priv      CPU Time  Elapsed Time
idle                 0  0  4   0   0      3:14:19.655  0:00:00.000
system               4  8 140  847  112     0:00:10.966  0:49:25.549
smss                 340 11  2  32  520     0:00:00.062  0:49:25.502
csrss                476 13  9  734 2468     0:00:00.842  0:49:21.290
csrss                544 13 13  339 12944    0:00:02.074  0:49:20.651
wininit              552 13  3   85 1712     0:00:00.031  0:49:20.651
winlogon             588 13  3  114 2296     0:00:00.078  0:49:20.495
services             648  9  7  272 5080     0:00:00.343  0:49:20.120
lsass                656  9 32 1468 32404    0:00:02.355  0:49:19.949
lsmd                 668  8  9  151 2464     0:00:00.000  0:49:19.886
svchost              832  8  9  362 4124     0:00:00.452  0:49:15.206
svchost              924  8  7  287 3936     0:00:00.124  0:49:14.769
svchost             1008  8 14  344 11812    0:00:00.639  0:49:14.629
svchost              376  8 28  953 20012    0:00:02.074  0:49:14.426
svchost              500  8 12  307 6104     0:00:00.171  0:49:14.145
mgfxCUIService      532  8  6  135 2600     0:00:00.015  0:49:13.927
svchost              776  8  7  248 5004     0:00:00.296  0:49:13.849
svchost              536  8 18  456 13216    0:00:00.452  0:49:13.568
svchost             1144  8 16  302 11428    0:00:00.374  0:49:13.024

```

## Services

This command lets us see the list of all the files on our remote PC as seen above.

Our next command is PsService.exe which lets us know about all the services running on our victims' PC. The command is:

**PsService64.exe \\192.168.1.104 -u administrator -p Ignite@123**

```

C:\Users\Administrator\Desktop\PSTools>PsService64.exe \\192.168.1.104 -u administrator -p Ignite@123

PsService v2.25 - Service information and configuration utility
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AdobeARMService
DISPLAY_NAME: Adobe Acrobat Update Service
Adobe Acrobat Updater keeps your Adobe software up to date.
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0 ms

SERVICE_NAME: ADWS
DISPLAY_NAME: Active Directory Web Services
This service provides a Web Service interface to instances of the directory service (AD DS and AD LDS) that a
is service is stopped or disabled, client applications, such as Active Directory PowerShell, will not be able
ce instances that are running locally on this server.
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0 ms

```

## Log List

You can result in the above pic.

One of these tools helps us to see the logs of victim PC. That tool is psloglist.exe and the command to run this tool is:

```
psloglist.exe \\192.168.1.104 -u administrator -p Ignite@123
```

```
C:\Users\Administrator\Desktop\PSTools>psloglist.exe \\192.168.1.104 -u administrator -p Ignite@123

Psloglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
www.hackingarticles.in
System log on \\192.168.1.104:
[5898] Service Control Manager
  Type: INFORMATION
  Computer: WIN-NR5JQEBKNIE.rajlab.com
  Time: 17-08-2016 14:53:05 ID: 7036
The Windows Modules Installer service entered the running state.

[5897] Service Control Manager
  Type: INFORMATION
  Computer: WIN-NR5JQEBKNIE.rajlab.com
  Time: 17-08-2016 14:48:01 ID: 7036
The Application Experience service entered the stopped state.

[5896] Service Control Manager
  Type: INFORMATION
  Computer: WIN-NR5JQEBKNIE.rajlab.com
  Time: 17-08-2016 14:41:35 ID: 7036
The Google Update Service (gupdate) service entered the stopped state.
```

## Change Password

So, like this our command is successful as we have our desired result.

Now, pspasswd64.exe is the most important tool as it lets us to change the password of a PC. And the command to achieve this is:

```
pspasswd64.exe \\192.168.1.104 -u administrator -p ignite@123 administrator forever
```

Here,

**192.168.1.104** -> our victim's IP

**-u** -> denotes username

**Administrator** -> username

**-p** -> denotes password

**Ignite@123 --> password**

**Administrator** --> username (which we have to give again to specify that which user's password we want to change)

```
C:\Users\Administrator\Desktop\PSTools>pspasswd64.exe \\192.168.1.104 -u administrator -p Ignite@123 administrator forever
PsPasswd v1.24 - Local and Remote password changer
Copyright (C) 2003-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password successfully changed.
C:\Users\Administrator\Desktop\PSTools>
```

This can successfully change the password as shown in above image.

## Remote Connect Shell

Another important tool is PsExec64.exe which takes us directly in the shell of victim's PC. Its command is:

**PsExec64.exe \\192.168.1.104 -u administrator -p forever cmd**

```
C:\Users\Administrator\Desktop\PSTools> PsExec64.exe \\192.168.1.104 -u administrator -p forever cmd
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

## Shutdown

Lastly our next tool helps us to shutdown remote PC. And for that just type:

**pssshutdown.exe \\192.168.1.104 -u administrator -p forever**

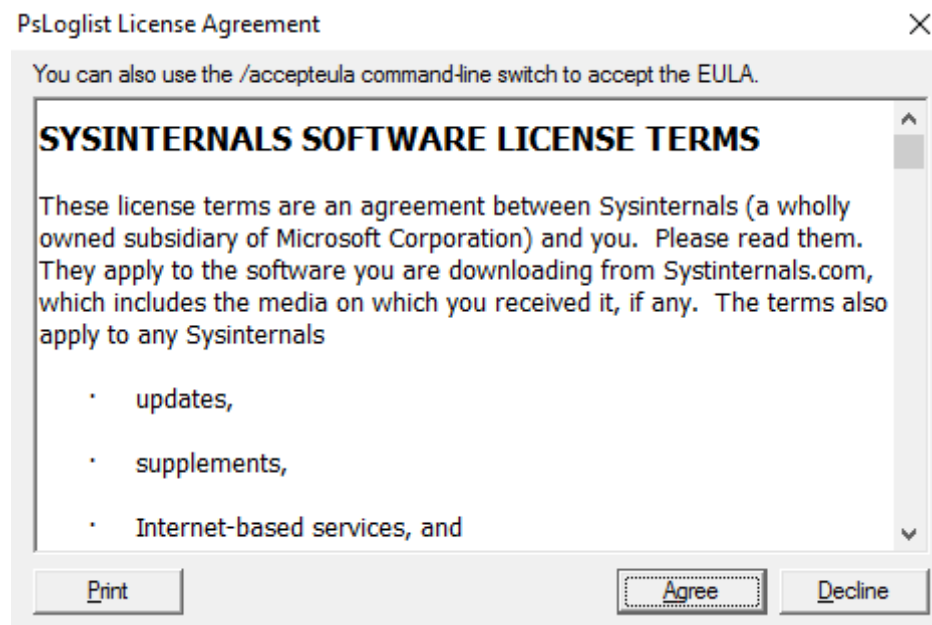
```
C:\Users\Administrator\Desktop\PSTools>psshutdown.exe \\192.168.1.104 -u administrator -p forever
www.hackingarticles.in
PsShutdown v2.52 - Shutdown, logoff and power manage local and remote systems
Copyright (C) 1999-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

192.168.1.104 is scheduled to power off in 00:00:20.
www.hackingarticles.in
C:\Users\Administrator\Desktop\PSTools>
```

And as shown in the image above the remote PC will shutdown in 20 seconds.

So, these were tools in the PSTool kit and the commands to run them. These tools make our work a lot easy and come in handy.

PS -> If you come across such dialogue box then always click on **AGREE** or else the above commands will not work. The image of dialogue box is shown below



**Author: Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles.  
She is a hacking enthusiast. contact [here](#)

## Pentest Lab Setup for Windows Server 2008 R2

posted in **PENETRATION TESTING** , **WINDOWS HACKING TRICKS** on **APRIL 23, 2016**  
by **RAJ CHANDEL** with **0 COMMENT**

To install Windows server 2008 R2 click this [link](#)

To install active directory in the windows server, assign static IP address.

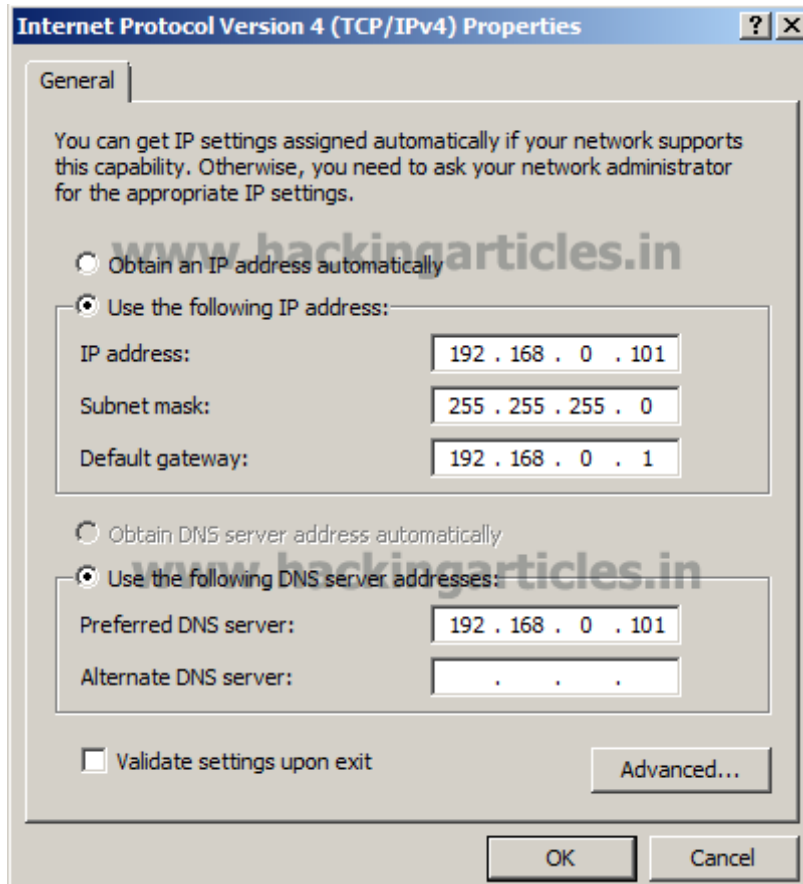
Such as IP Address : 192.168.0.101

Subnet mask : 255.255.255.0

Default Gateway : 192.168.0.101

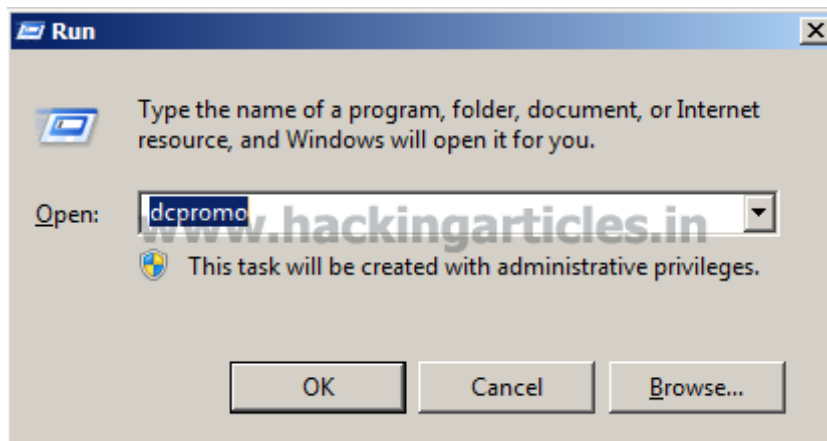
Preferred DNS Server : 192.168.0.101

Click OK

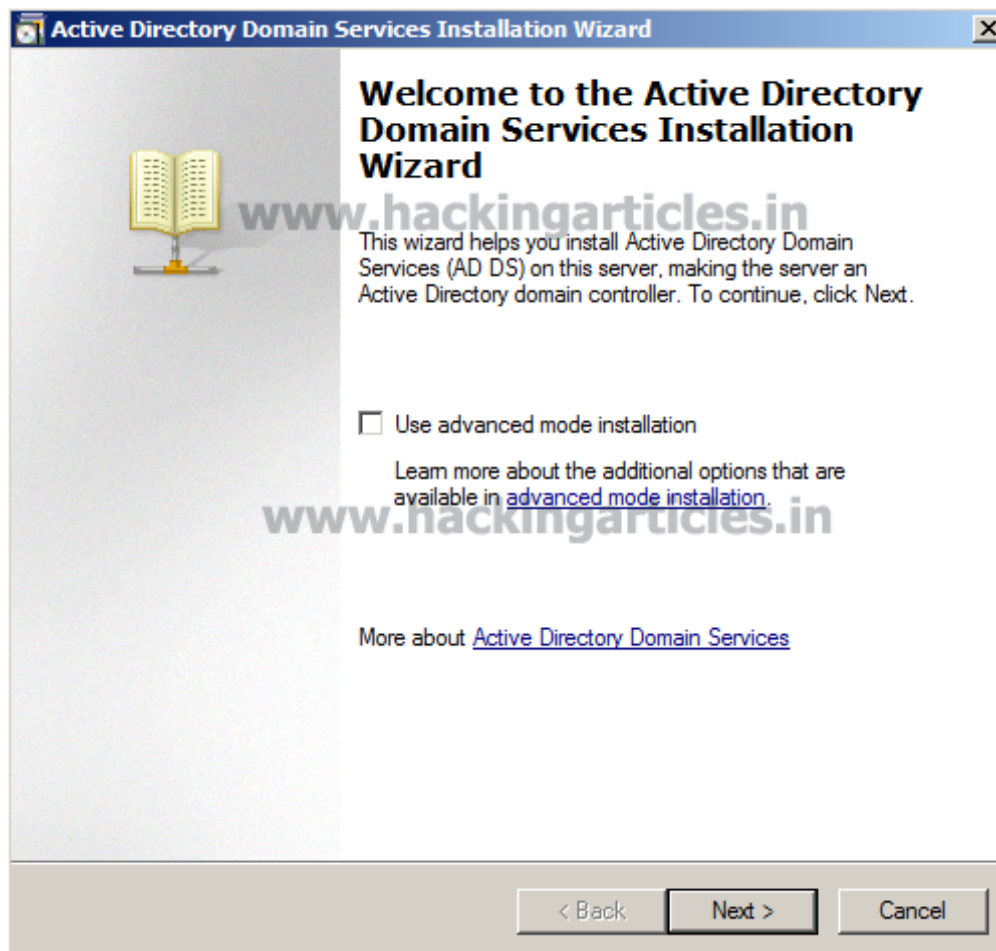


To install Active Directory, Type **DCPROMO** (Domain Controller Promotion) in Run Command With Run as Administrator. Click OK.

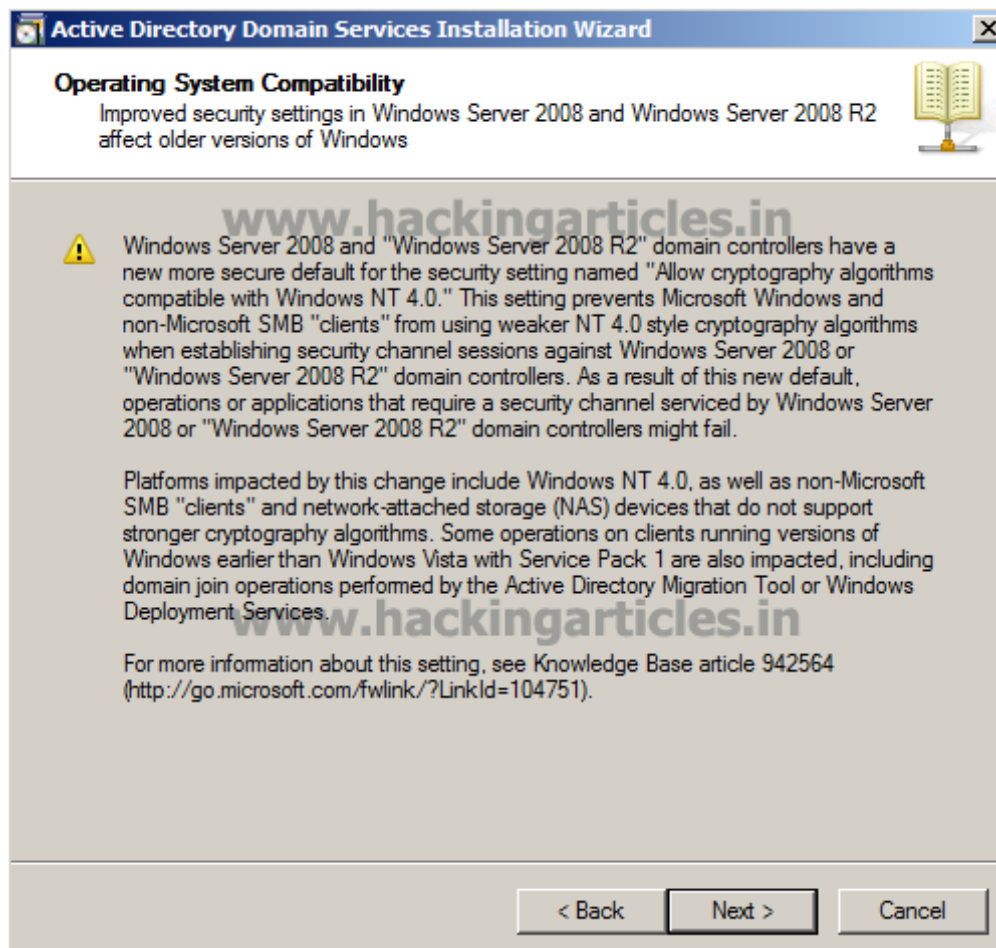




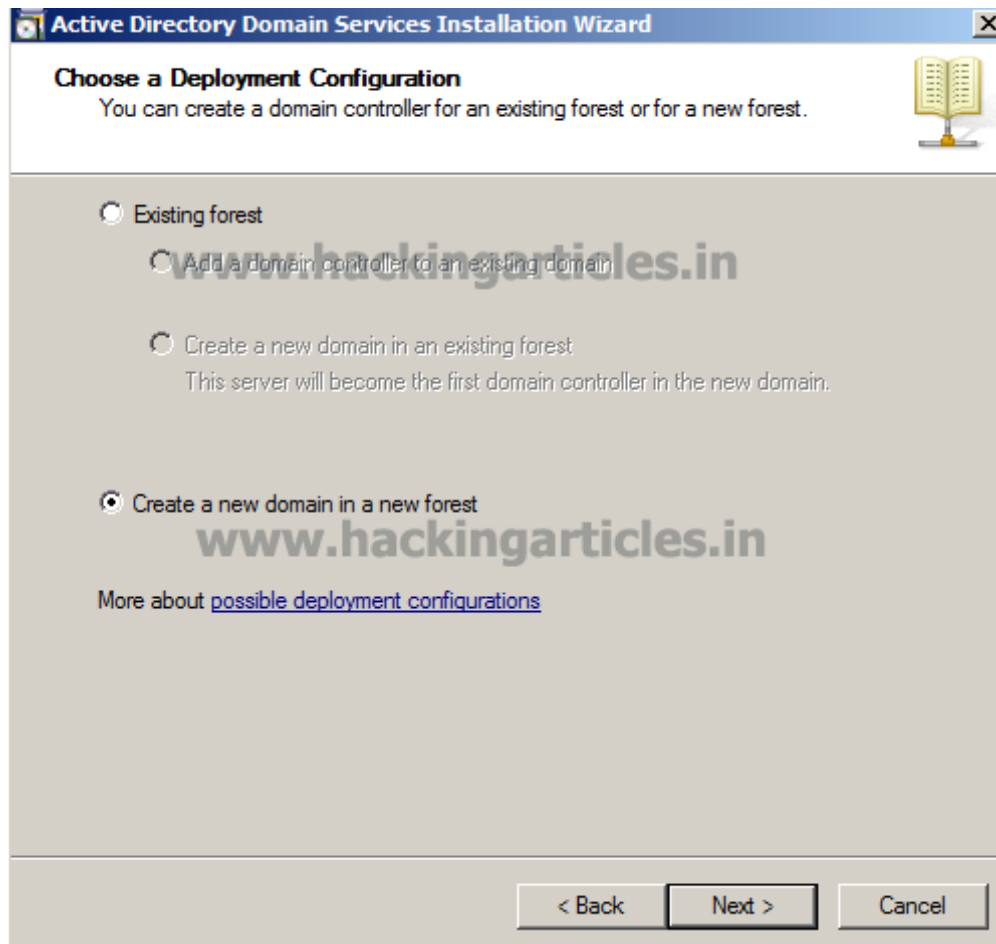
To start the installation click on “**Next**”



Click next to move on



We going to install new domain Controller in new forest please select the option “**Create a new domain in new forest**” option and click on “**Next**”



Now we have to provide the name for new domain. It must be FQDN. In our case I used **hackingarticles.in** as the domain. Please click “**Next**” after it.

**Active Directory Domain Services Installation Wizard**

**Name the Forest Root Domain**  
The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

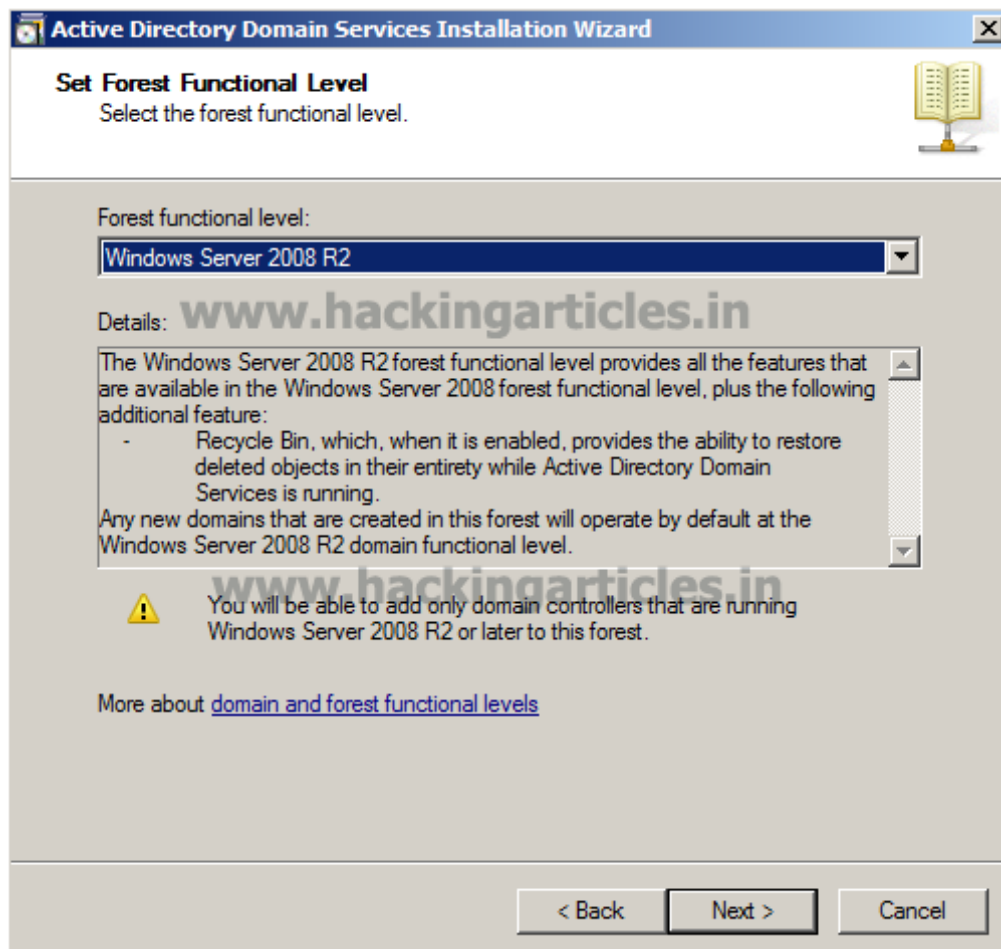
FQDN of the forest root domain:

Example: corp.contoso.com

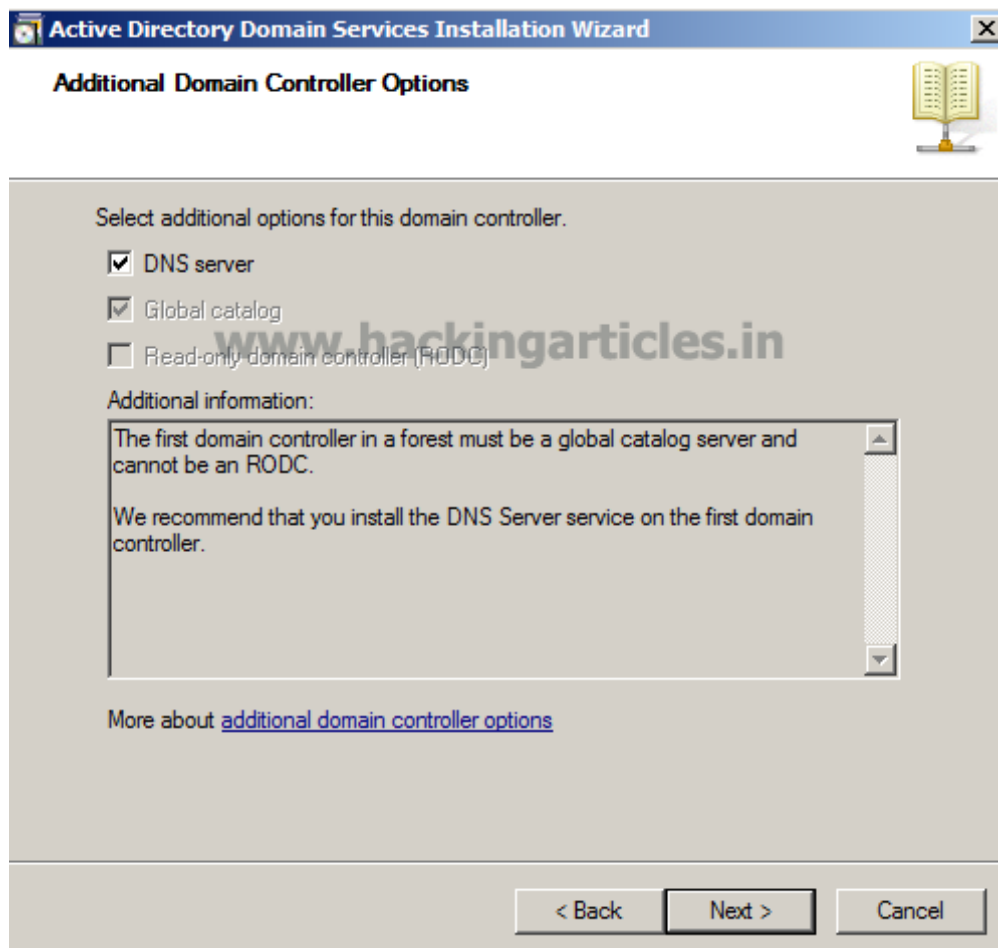
[www.hackingarticles.in](http://www.hackingarticles.in)

< Back   Next >   Cancel

Select forest functional level to Server 2008 R2 to add domain controller of Windows server 2008 R2 or later.



In next window since it's the first DC we should make it as **DNS server** too. Leave the default selection and click on "Next"



If the wizard cannot create a delegation for the **DNS server**, it displays a message to indicate that you can create the delegation manually. To continue, click “Yes”



In next window it will show up the database location. If you want to change it physical location Click browse and do the changes or click on “Next” to proceed.



**Active Directory Domain Services Installation Wizard**

**Location for Database, Log Files, and SYSVOL**  
Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

Database folder:

Log files folder:

SYSVOL folder:

[More about placing Active Directory Domain Services files](#)

Choose a Strong Active Directory Restore Mode Password and click next twice to kick off the configuration.

**Active Directory Domain Services Installation Wizard**

**Directory Services Restore Mode Administrator Password**

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

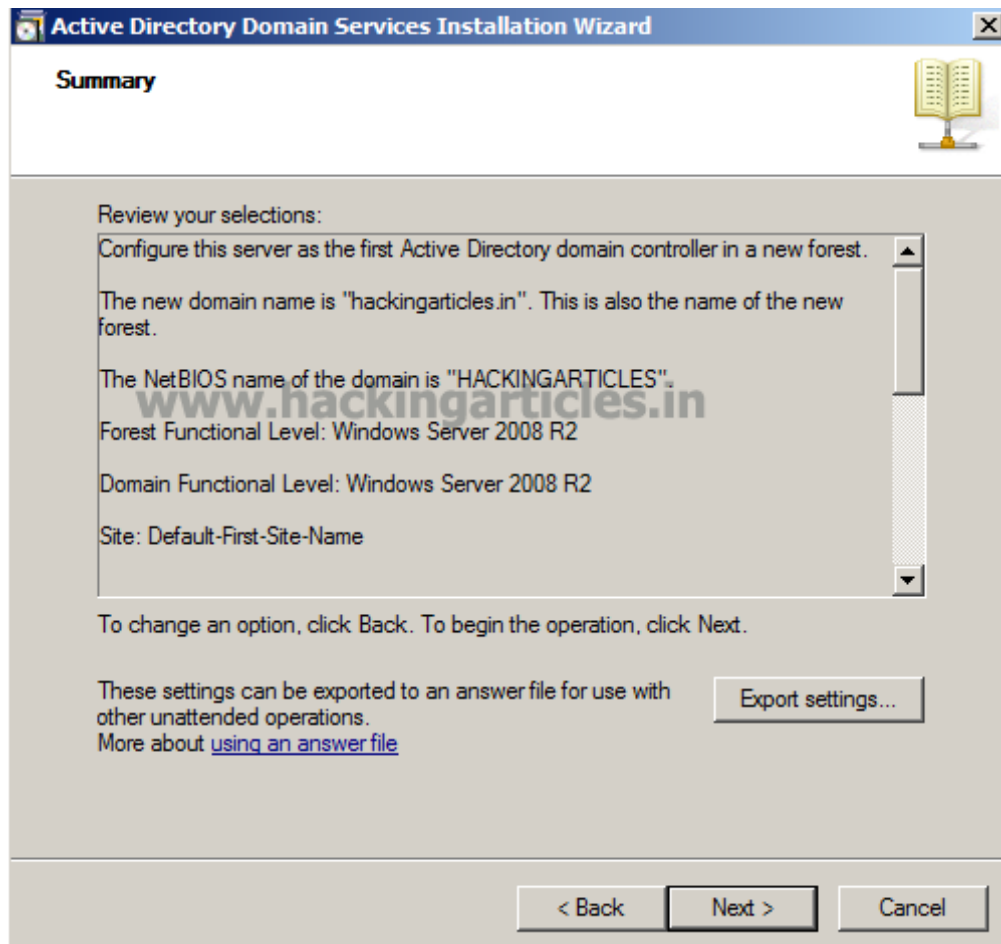
Password:

Confirm password:

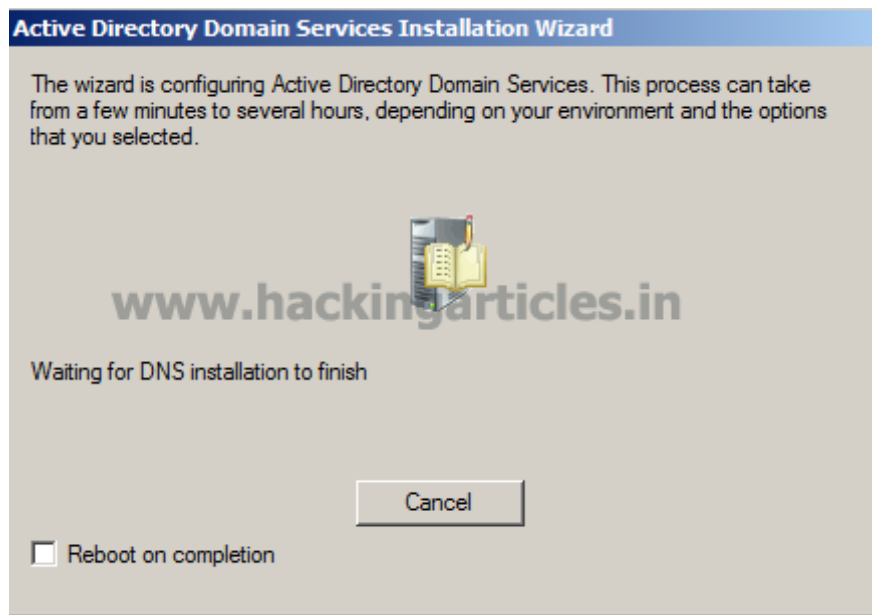
More about [Directory Services Restore Mode password](#)

< Back   Next >   Cancel

Next window is giving you a brief of the installation. Click on “**Next**”



Then it will start the installation of the AD. It will take some time to complete.



When its done you will be notified and required to reboot your PC.

← OLDER POSTS