HACKING YOUR GF'S X BOYFRIEND

(Protocol Analysis & Comp. Forensics)

Written By :

Nipun Jaswal (Ap3x Pr3Dat0r)

AFCEH , CISE , C|EH

Star Cast:

- The Script kid
- The Ub3r ☺
- The Victim

Catch That Looser who's recording every activity.

Dedicated To My Mom / My Best Friend:

Mrs. Sushma Jaswal

About The Author

Nipun Jaswal is an IT-Security researcher presently working in the field of penetration testing and vulnerability assessments, he is currently holding the position of **Chief Technical Officer** in **Secugenius Security Solutions**, **India.**
He is also working as Marketing & Conference Head at **DEFCON PUNJAB (DC141001)**, He is certified with 3 prestigious certifications – **Ankit Fadia's Certified Ethical Hacker, Certified Information Security Expert, Certified Ethical Hacker By EC-COUNCIL US.** He is also the **FOUNDER / Sr. Administrator** at www.starthack.com , also he has worked as the **R&D Security Analyst** At Cyber Cure Solutions New Delhi and he is also the Ambassador of **EC-COUNCIL** for security courses in **Lovely Professional University.**

His field Of Interest and expertise is – **Metasploit Exploitation Framework and exploit development, Wireless Security, Protocol Analysis and Cyber forensics**

He has tested and patched over 30k websites and currently helped **Schools India** enterprise to successfully patch over **900** hacked websites by Pakistani hackers.

His Recent research on Metasploit Framework was previously published in a research paper called " Blind date with your girlfriend" which got over 25k hits all over the world .

He is presently working on **IEEE 802.11 protocol and Mail Tracking System.** He is currently pursuing his final year in bachelors of technology from Lovely professional university

Introduction

Elizabeth wakes up Monday morning and starts her regular social media, suddenly she founds that none of her email, social media , and bank account password are working she is unable to realize that what exactly just got happened . Later she finds out that her system has been hacked and each of her activity had been monitored and stolen. Later in the evening she finds that a private video chat of her is leaked on a professional porn site. She gets depressed and calls out her boyfriend who's the cyber crime investigator in the nearby crime branch. Kevin finds that her system has been trojanised and there is no trace of the file which is sending all the information. Elizabeth suspiciously thinks of her X boy friend who was interested in doing such activities in his college life. Now Kevin starts investigating and monitors her network for suspicious activities and tries to trace the victim out. Kevin is good at monitoring network and has deep knowledge of forensics and protocols working.

After some time he founds that some packets from SMTP are regularly sent by the system to an unknown server and he collects its credentials from there. From the email id he is now able to trace the attacker and quickly goes in and arrests the culprit. Now rephrasing the whole scene we will be looking at how the attacker was able to create a malicious file? , how the attacker collected data from the target system? How Kevin was able to trace the victim?

So let's start up things from the very beginning how everything actually happened?

In Order To Know The Importance of writing this research paper . I have included the screenshots and scenarios from both the attacker's side and the victim side .

So First Of All The Tools We Will Require In this Research :

1. **Any Good Keylogger**
2. **A Binder / Crypter**
3. **Wireshark**

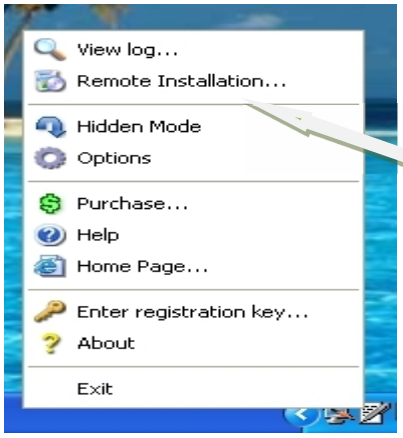
In This Case we will be using **Ardamax Keylogger** Preety Basic one . but the technique works for all.

So First Lets Move on to the Attacker Machine .

I Assume You Can install a Basic Keylogger Software on your systems .

After Successful installation of the keylogger (Ardamax)

We have our system tray like this :

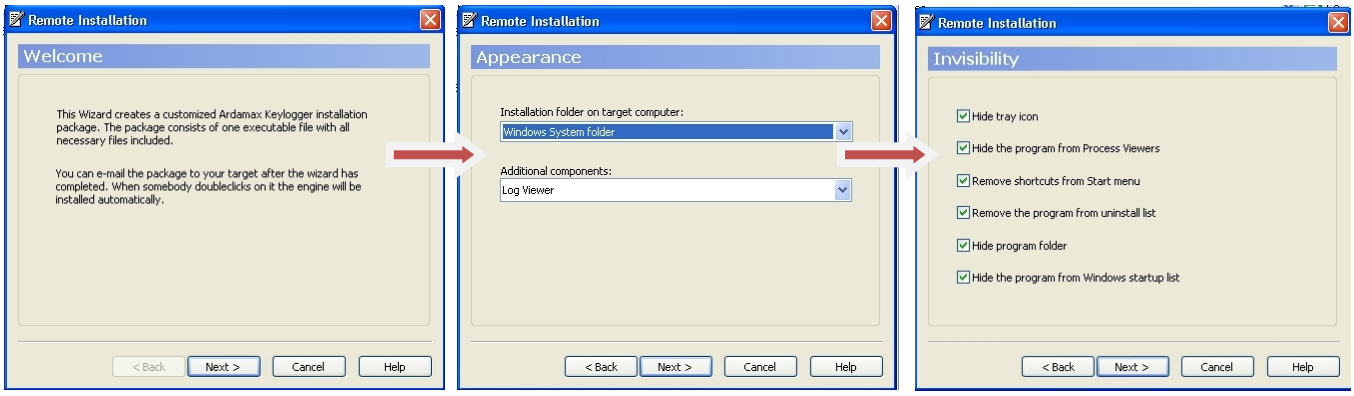


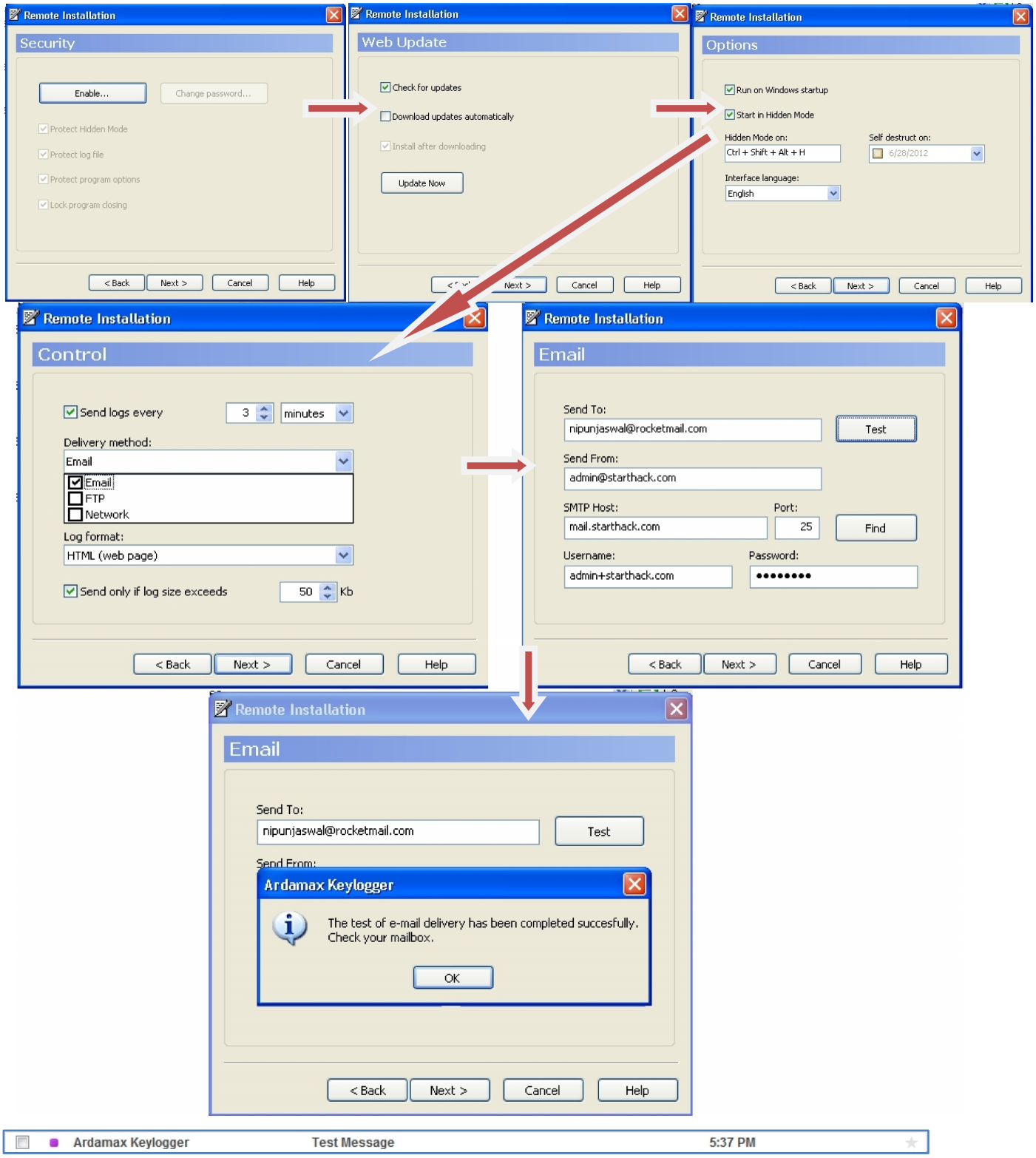
You can Clearly see the pen-paper icon of ardamax in the bar . now to create a remote file which we can spread across a network we need to choose

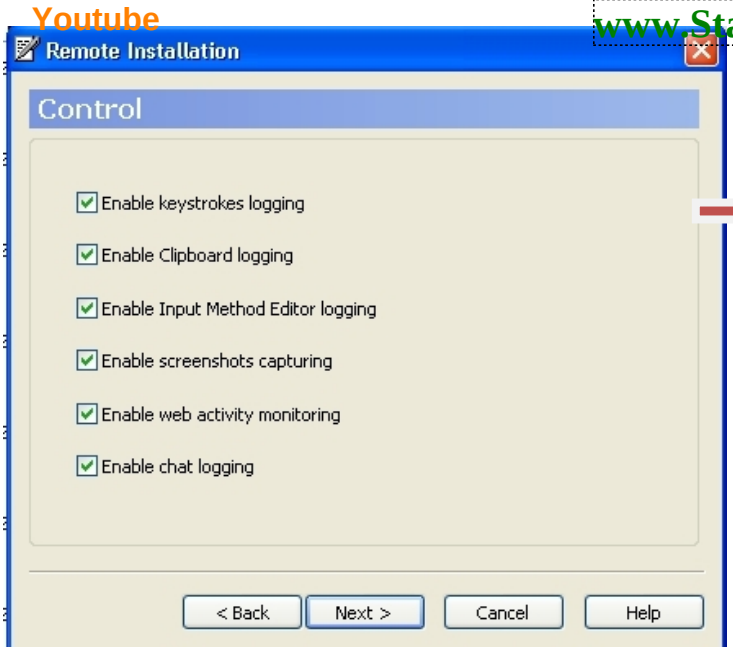
Remote Installation

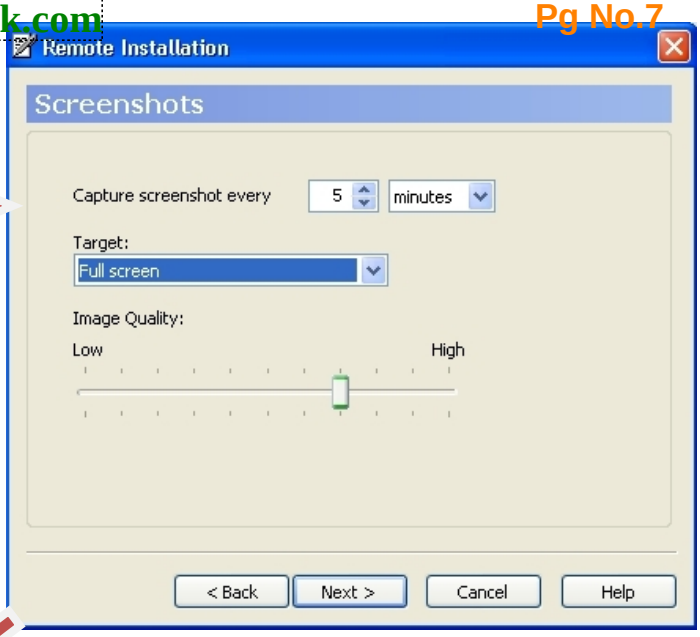
After That , a series of steps and we are ready with our malicious file .

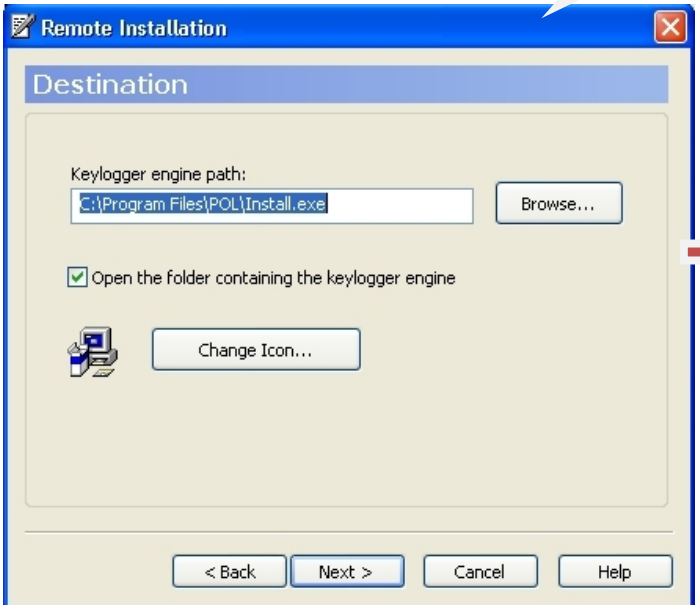
Steps:-

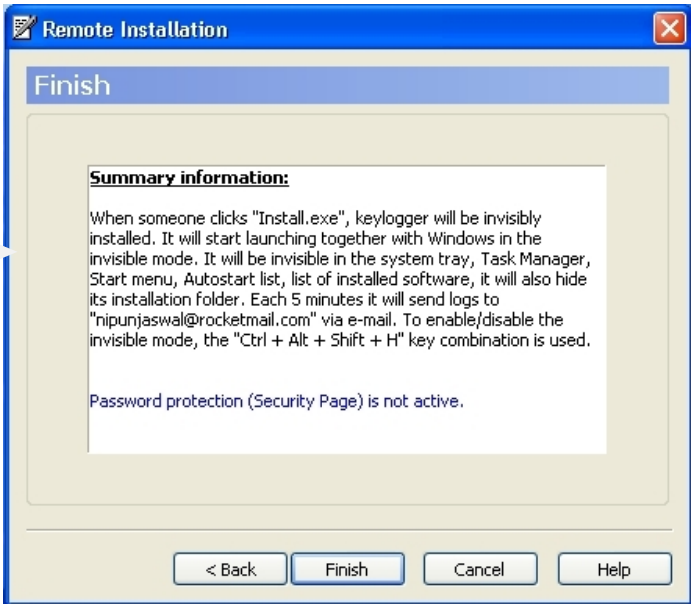


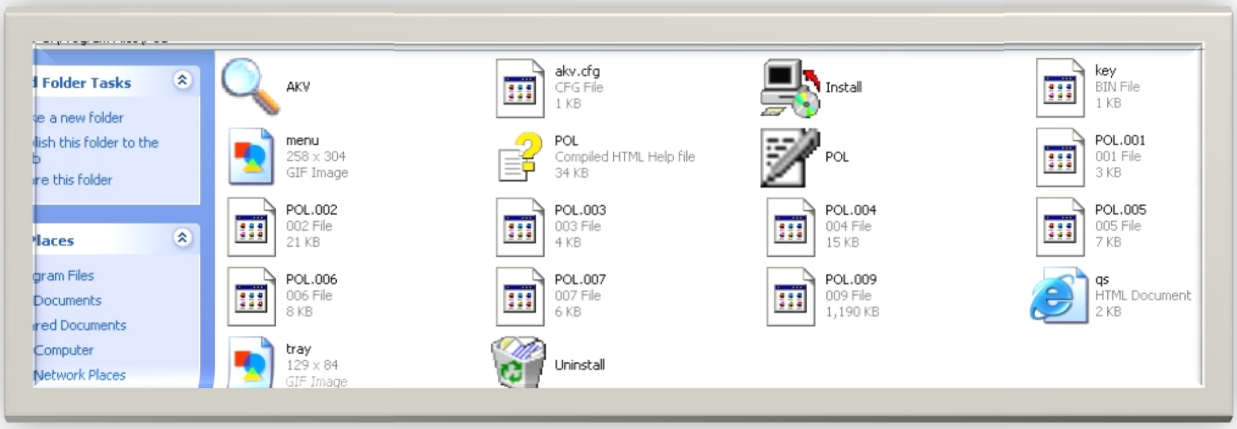

Remote Installation
Security
Enable...
Change password...
Protect Hidden Mode
Protect log file
Protect program options
Lock program closing
< Back
Next >
Cancel
Help
Remote Installation
Web Update
Check for updates
Download updates automatically
Install after downloading
Update Now
Remote Installation
Options
Run on Windows startup
Start in Hidden Mode
Hidden Mode on:
Ctrl + Shift + Alt + H
Self destruct on:
6/28/2012
Interface language:
English
Remote Installation
Control
Send logs every
3
minutes
Delivery method:
Email
Email
FTP
Network
Log format:
HTML (web page)
Send only if log size exceeds
50
Kb
Remote Installation
Email
Send To:
nipunjaswal@rocketmail.com
Test
Send From:
admin@starthack.com
SMTP Host:
mail.starthack.com
Port:
25
Find
Username:
admin+starthack.com
Password:
Remote Installation
Email
Send To:
nipunjaswal@rocketmail.com
Test
Send From:
Ardamax Keylogger
The test of e-mail delivery has been completed succesfully.
Check your mailbox.
OK
Ardamax Keylogger
Test Message
5:37 PM


Remote Installation
Control
Enable keystrokes logging
Enable Clipboard logging
Enable Input Method Editor logging
Enable screenshots capturing
Enable web activity monitoring
Enable chat logging
< Back
Next >
Cancel
Help


Remote Installation
Screenshots
Capture screenshot every
5
minutes
Target:
Full screen
Image Quality:
Low
High
< Back
Next >
Cancel
Help


Remote Installation
Destination
Keylogger engine path:
C:\Program Files\POL\Install.exe
Browse...
Open the folder containing the keylogger engine
Change Icon...
< Back
Next >
Cancel
Help


Remote Installation
Finish
Summary information:
When someone clicks "Install.exe", keylogger will be invisibly installed. It will start launching together with Windows in the invisible mode. It will be invisible in the system tray, Task Manager, Start menu, Autostart list, list of installed software, it will also hide its installation folder. Each 5 minutes it will send logs to "nipunjaswal@rocketmail.com" via e-mail. To enable/disable the invisible mode, the "Ctrl + Alt + Shift + H" key combination is used.
Password protection (Security Page) is not active.
< Back
Finish
Cancel
Help


Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Program Files
My Documents
Shared Documents
My Computer
My Network Places
AKV
akv.cfg
CFG File
1 KB
Install
key
BIN File
1 KB
menu
258 x 304
GIF Image
POL
Compiled HTML Help file
34 KB
POL
POL.001
001 File
3 KB
POL.002
002 File
21 KB
POL.003
003 File
4 KB
POL.004
004 File
15 KB
POL.005
005 File
7 KB
POL.006
006 File
8 KB
POL.007
007 File
6 KB
POL.009
009 File
1,190 KB
qs
HTML Document
2 KB
tray
129 x 84
GIF Image
Uninstall

As You guys can see how easy is to create a malicious file, but guys the difficult part is to bind and crypt the file . So it evades antivirus detection

I would like to recommend you to two crypters which generate 100% FUD files

- ✓ **Heaven Crypter**
- ✓ **Chrome Crypter**

Now I **leave binding and Crypting up to you** as it's easy to perform if you have the right tools.

Now send your files to the victim.

Also, most importantly the above installation snapshot no. 7 & 8

Plays an important role

Here the Logs are sent to: nipunjaswal@rocketmail.com Call it A

By remotely logging into: admin@starthack.com Call it B

So technically the mail id which is sending a mail to **A is B**.

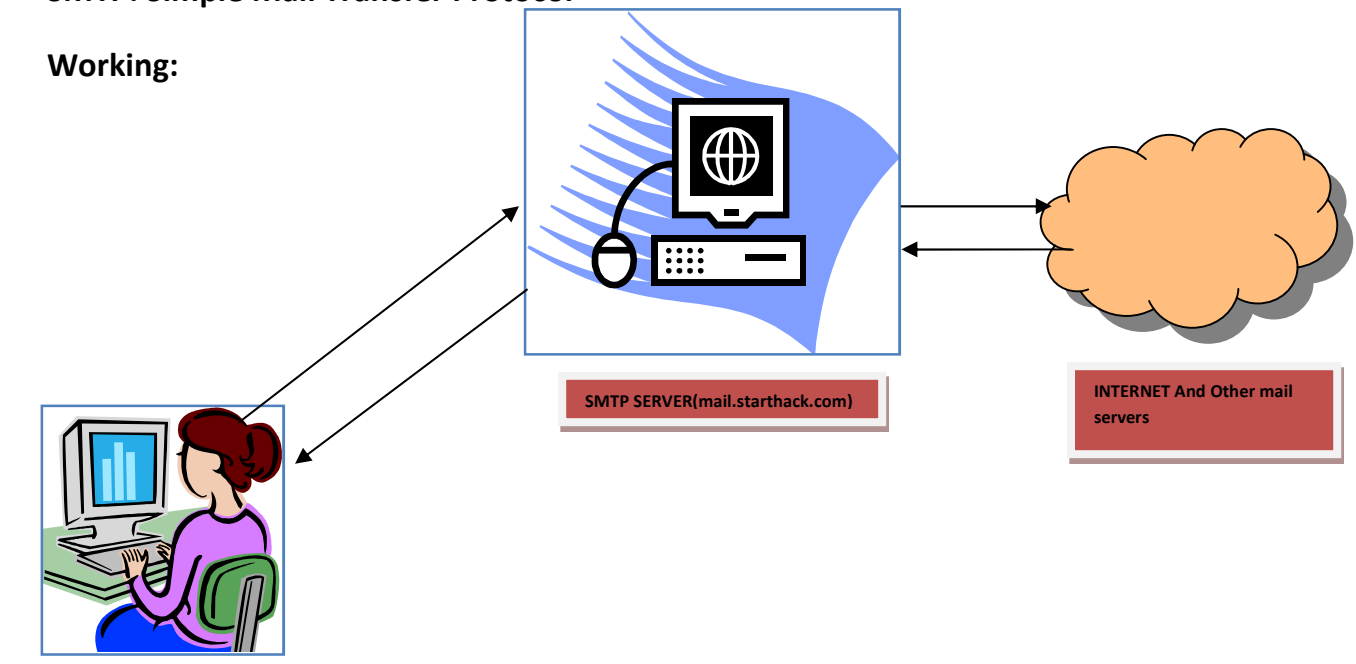
Every time a remote key logger is used it requires you to supply username and the password of the mail id which is used to send the logs created by the Key logger to the attacker which is **A**

Now also these logs can be sent via **FTP.** Which can also be traced using same technique.

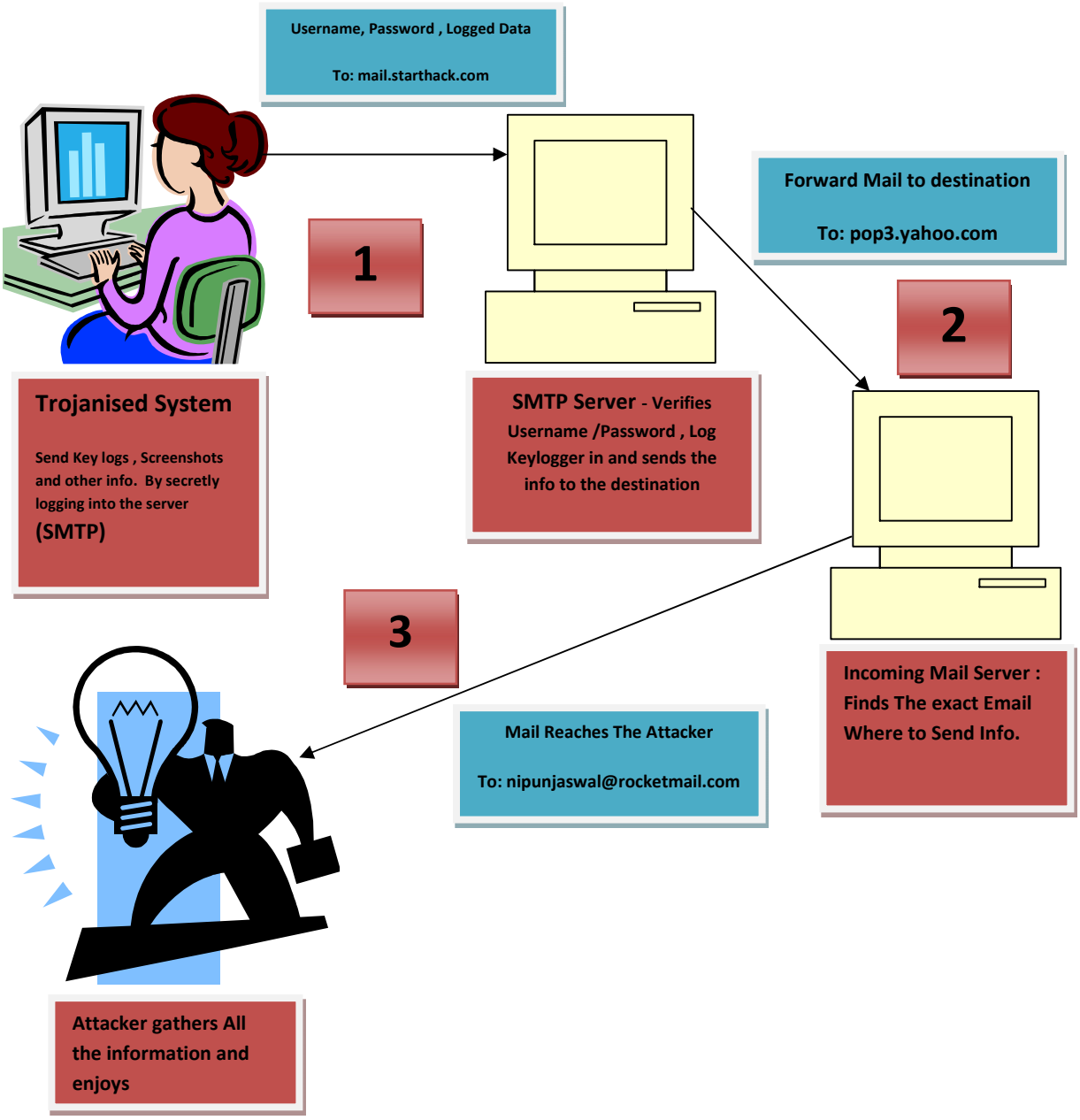
Terminologies used here:

SMTP: Simple Mail Transfer Protocol

Working:



Attack Scenario



So Now The Question That Arises Is We Know That The Communication is happening between the key logger and the attacker . but **we can't see it** because key loggers come with options such as hide

from process view , hidden files that we can't find where exactly they are or how exactly they work ? or where the actual file that sends the information back and forth to the attacker is ? where do it resides ?

We take typical two scenarios 1 – where we know the file capturing and transmitting information and 2nd where we dnt knw the location of the file

Typically if we know where the file is , what we can do? We can simply try to delete that ..

But will it repent the lost information? ..the answer is **NO ..** or do we know where exactly It has travelled and to whom?

Again the Anwer is **NO.**

What in case 1 one actually do ?

A Good Known REVERSE ENGINEER can break the shackles of the malicious file and can try finding out where the information has exactly gone .

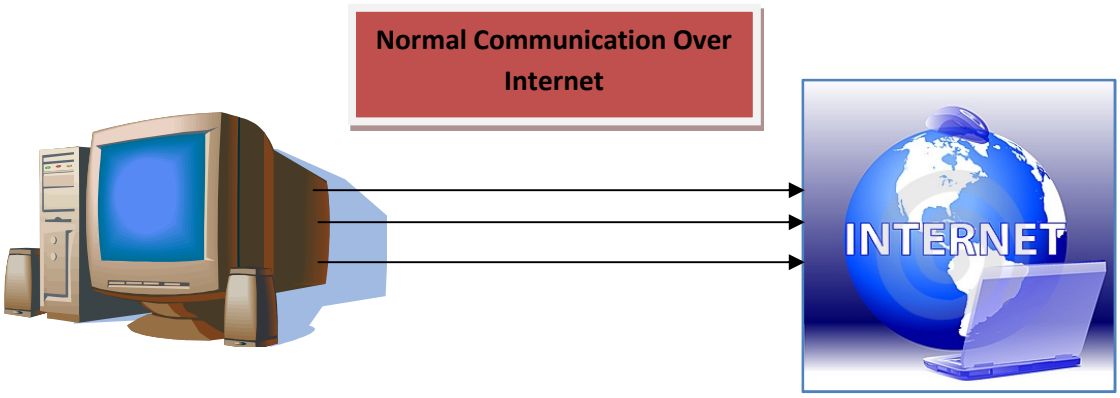
But We must keep in mind every person out there in the real world may not be an expert REVERSE ENGINEER.. or have no relation to it ..

Also , if you dnt knw exactly which file is suspicious what can u do?

Now I will demonstrate you guys a little bit about packet capturing .

in a normal case a typical communication happens when you send out something or receive something from the internet

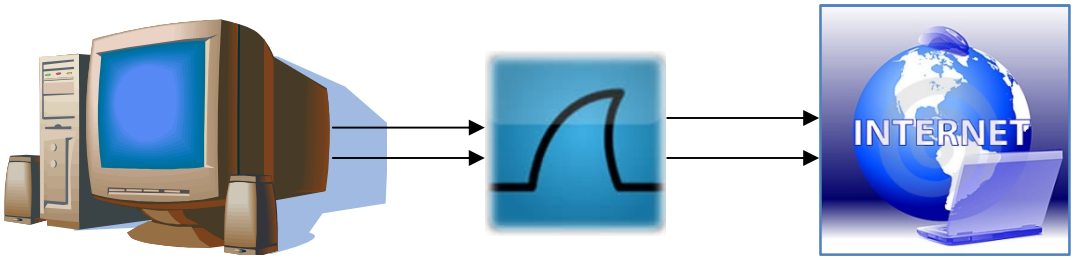
this happens like –



Now What exactly is a packet capturer , It Monitors All the packets travelling to and from the system to the internet or the external network.

So every data sent from a Trojanised computer must pass through the packet capturer.

In this kind of communication the above medium is changed to:



Now the Most Important part :

We Need to filter out data which is most important to us .

In This Case If we don't know what method is used to send the logs to the attacker we will be eyeing for two types of packets

1. S.M.T.P(Simple Mail Transfer Protocol)
2. F.T.P (File Transfer Protocol)

By studying these packets we will be able to trace the attacker as well as the main email account used to carry logs to the attacker .

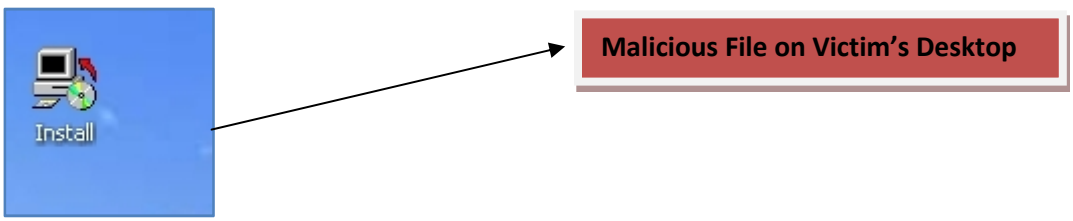
So Now , First Things To do to handle Trojanised system :

1. Connect with the system locally by joining your system into the network
2. Or Install Wireshark on the Trojanised system and wait for packet accumulation.

So Now as we have reached in the practical part to the making and Crypting of the malicious file .

I assume that you can send the file to the victim.

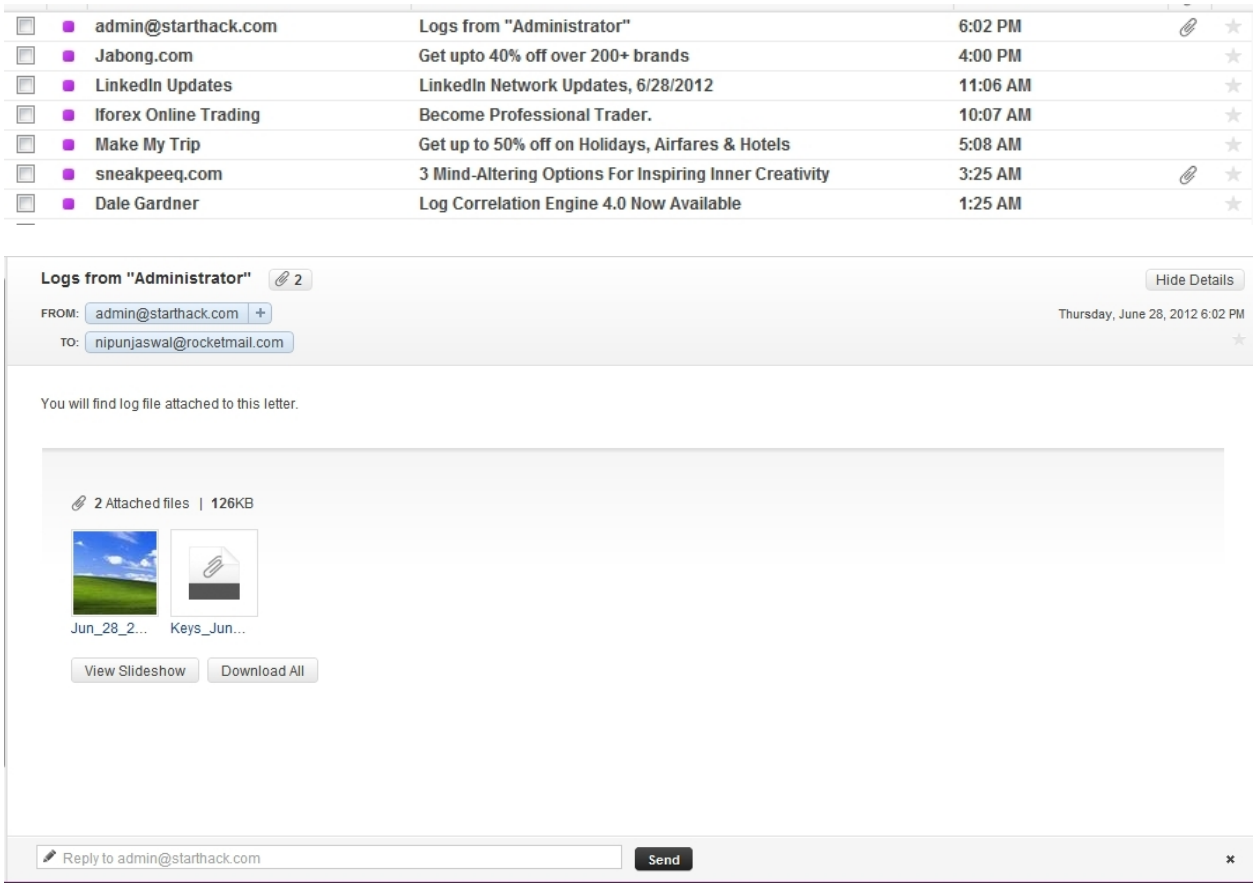
Now lets study further scenario:



Suppose The File is Clicked by the victim at any instance .

And logs to attacker has started coming ..

Like these,



Now this mailicous file gets destroyed as soon as it gets executed (MELT Feature in Some Keyloggers)

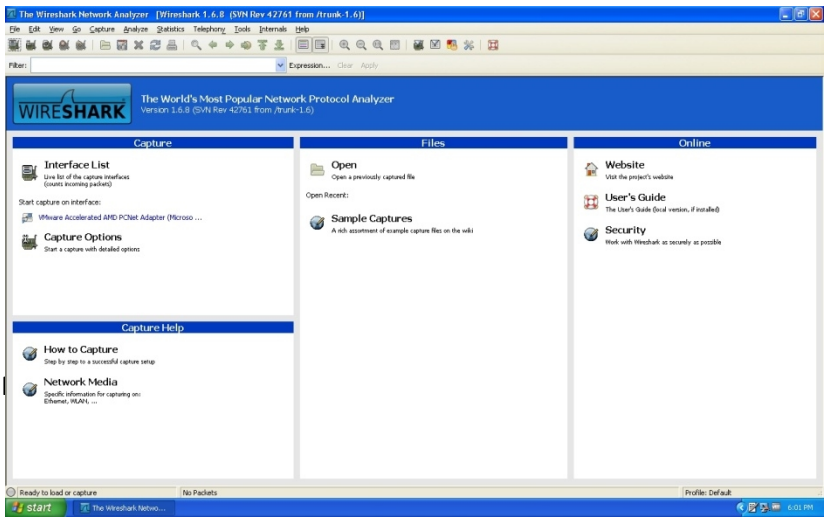
Now How To Find The Culprit ??

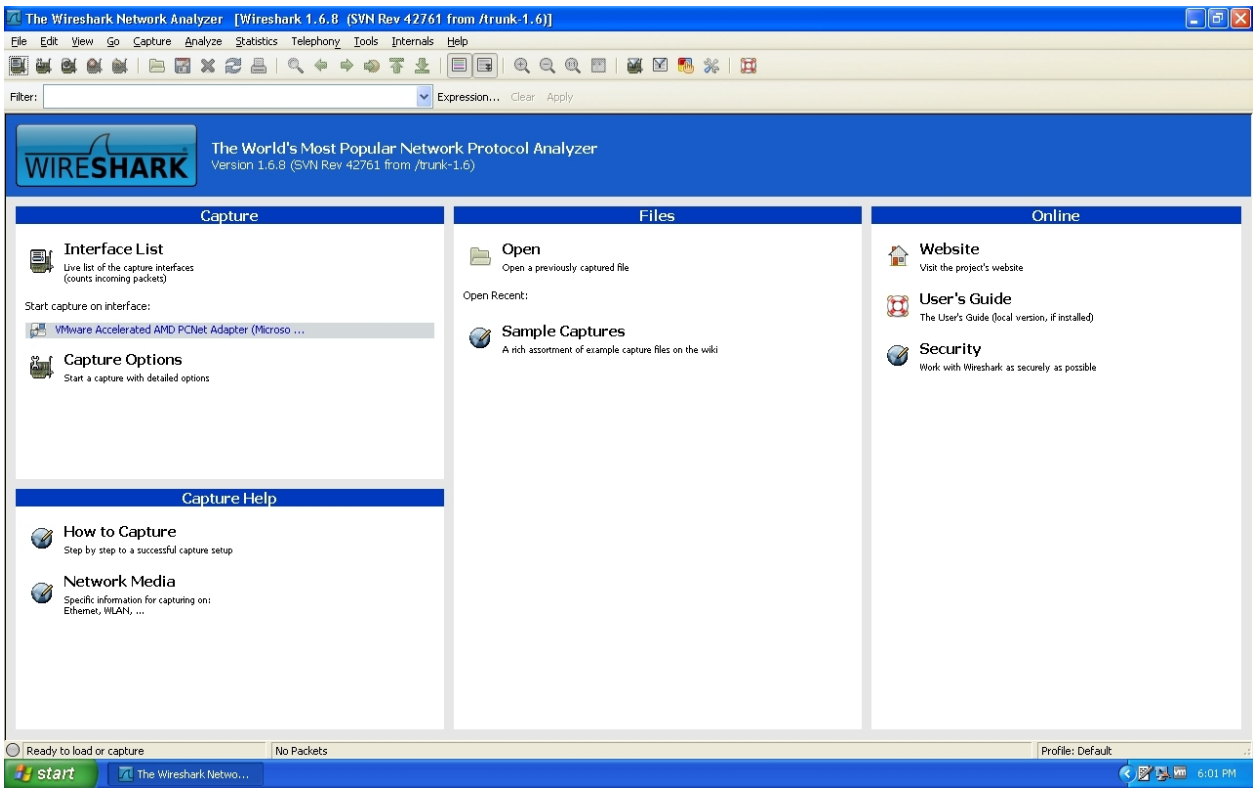
Now to trace back the hacker as I told you before we need to capture the communication that the file is making with the outside world .

So in this case we install WIRESHARK , a powerful packet sniffer /capturer on the victim system

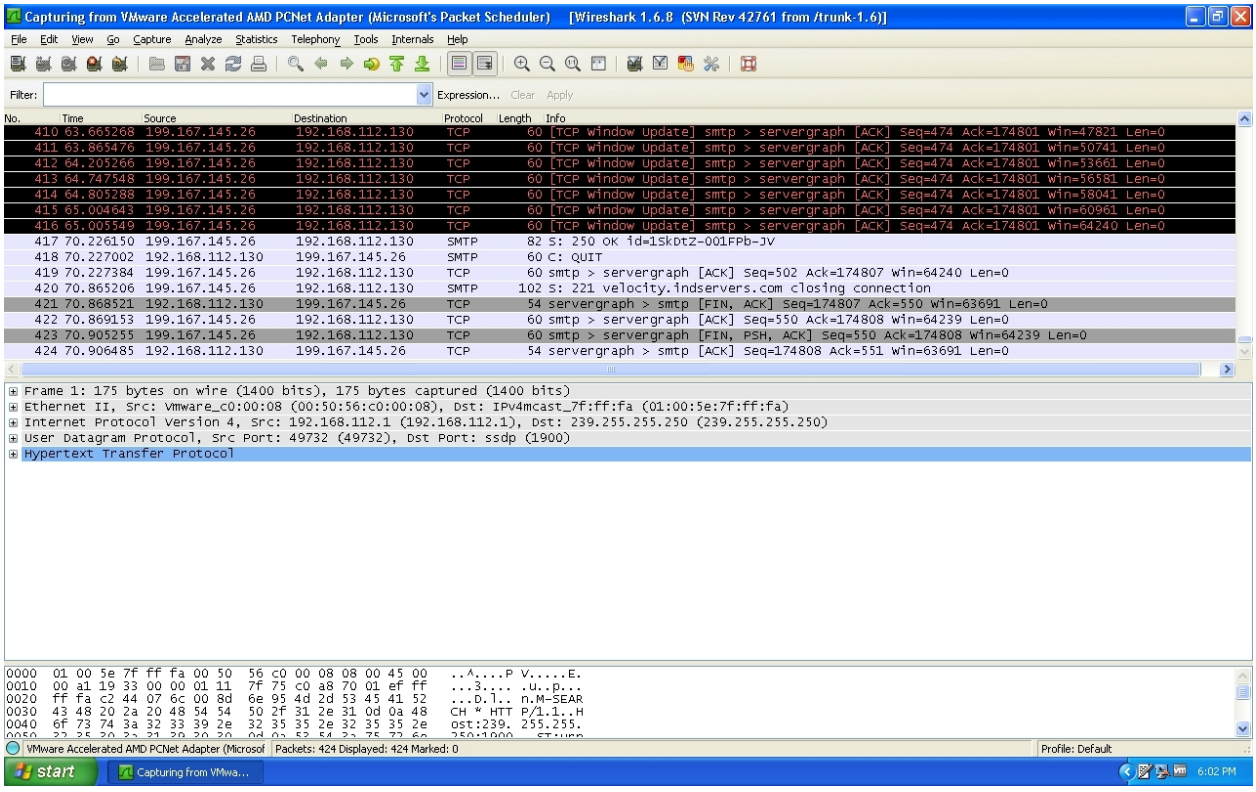
And Set it to capture the current usable “network Interface “ , We analyze each and every packet Until some suspicious activity is found .

Now Wireshark Opens up.





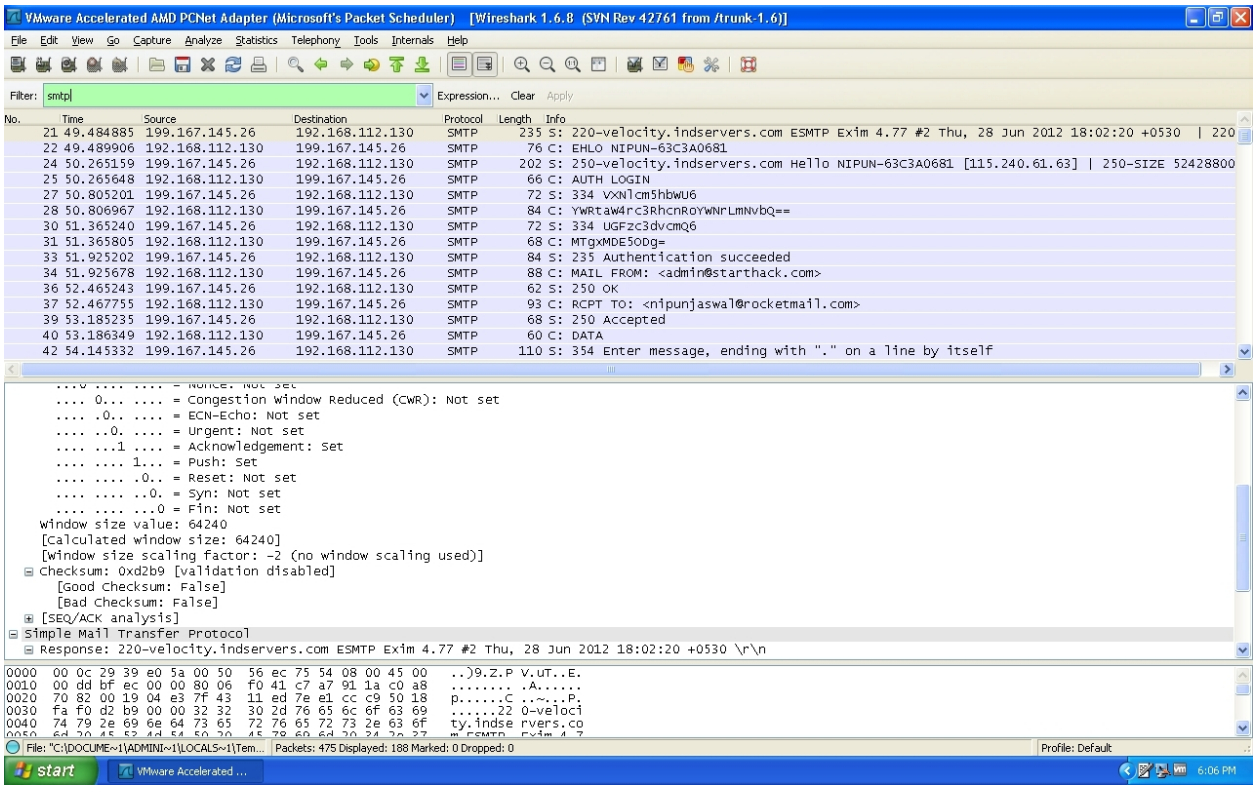
Remember we made the keylogger in above steps with an options of sending logs every 2 minutes so it is clear that we will see activity every two minutes for sure.



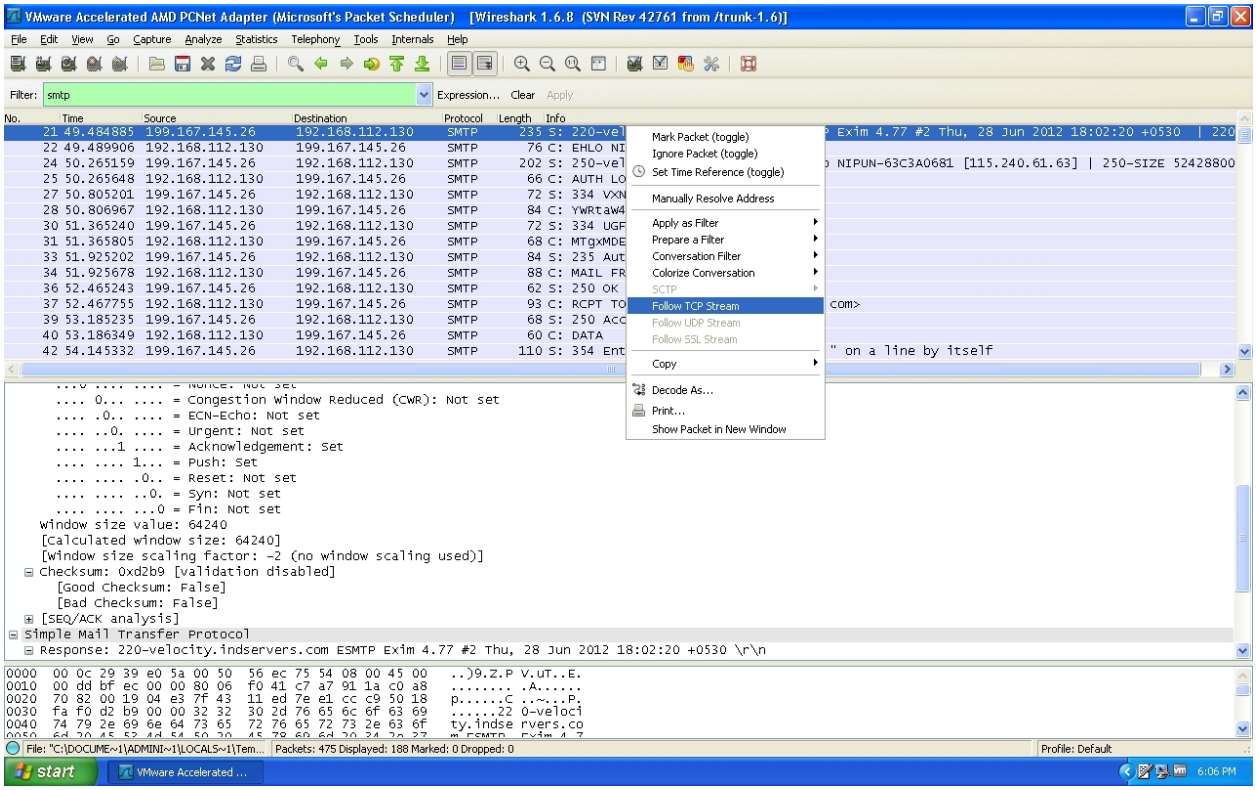
As we can see there is too much traffic of packets on the interface we need only the interested ones , we can do one thing we can filter the packets out to our intrest so that we can easily see the interested packets only .

So we create a filter in WIRESHARK.

'Smtp'

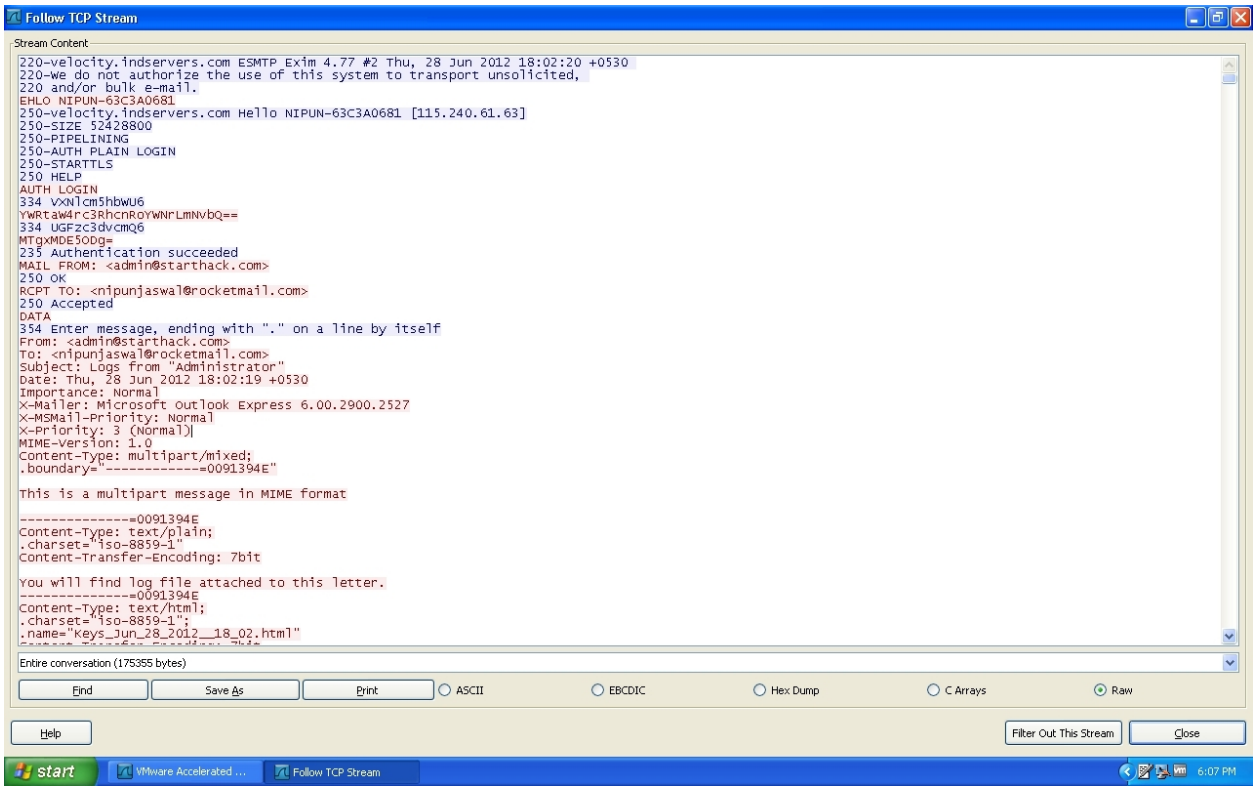


So as you can see each and every packet of SMTP listed here by order . so as we remember the first step that a user or a malicious file before sending must make contact with the SMTP server so we find the first step or the first packet useful .



In order to see what exactly is in that packet we right click it and set it to follow the TCP stream.

Wireshark presents us with the following result



VOILA ! we got the information that keylogger is sending something to mail id " nipunjaswal@rocketmail.com" from the mail id admin@starthack.com

Now what information is contained in it and how we can login to same mail id and find the culprit ?

We need username and the password , where is it ? can't see any .

As the above scenario strikes one thing in mind .. what?

The 11th line from the above screenshot . "AUTH LOGIN" followed by 334

Here 334 is the default message which a server send when asking credentials from the user.

Means is what is followed by 334 the text VXN…… is some sort encrypted.

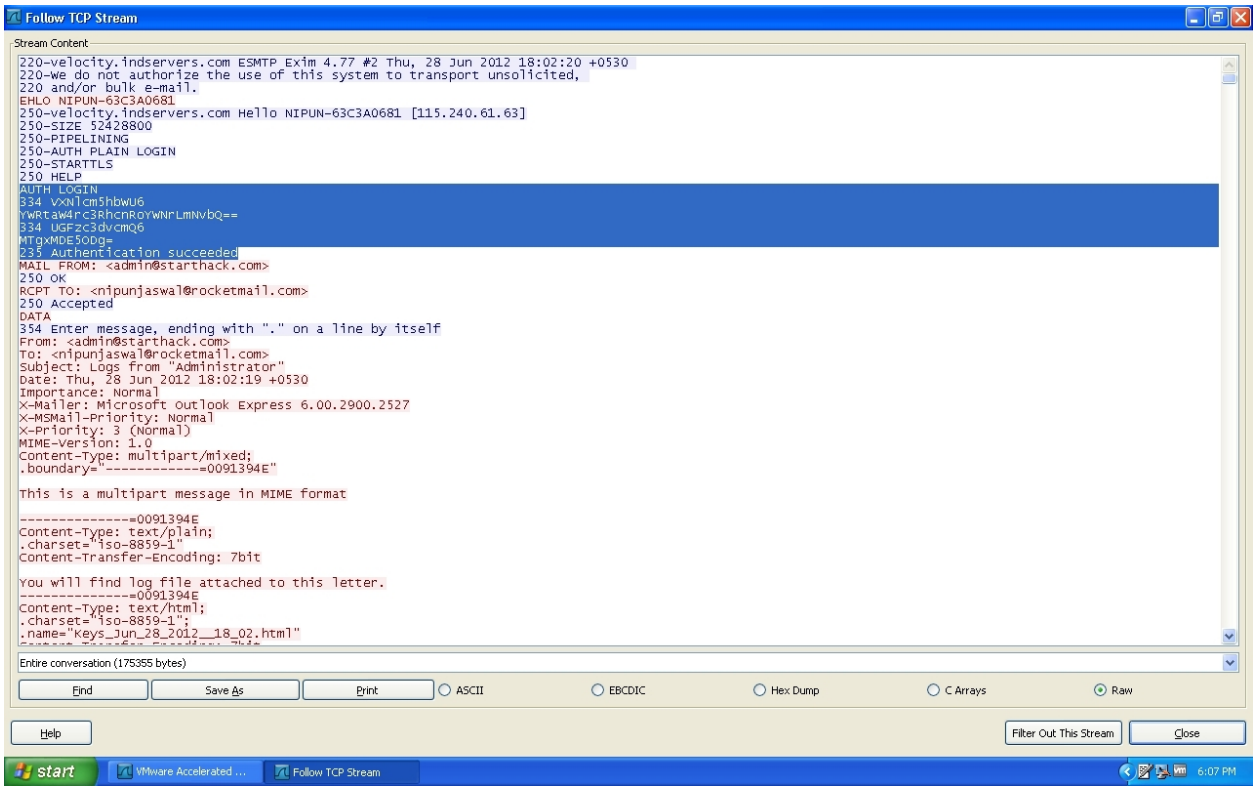
How to decrypt that? As by looking at the hashes of the encrypted text and by seeing the trailing '==' symbols instincts tells me that this is BASE 64 Encoded scheme

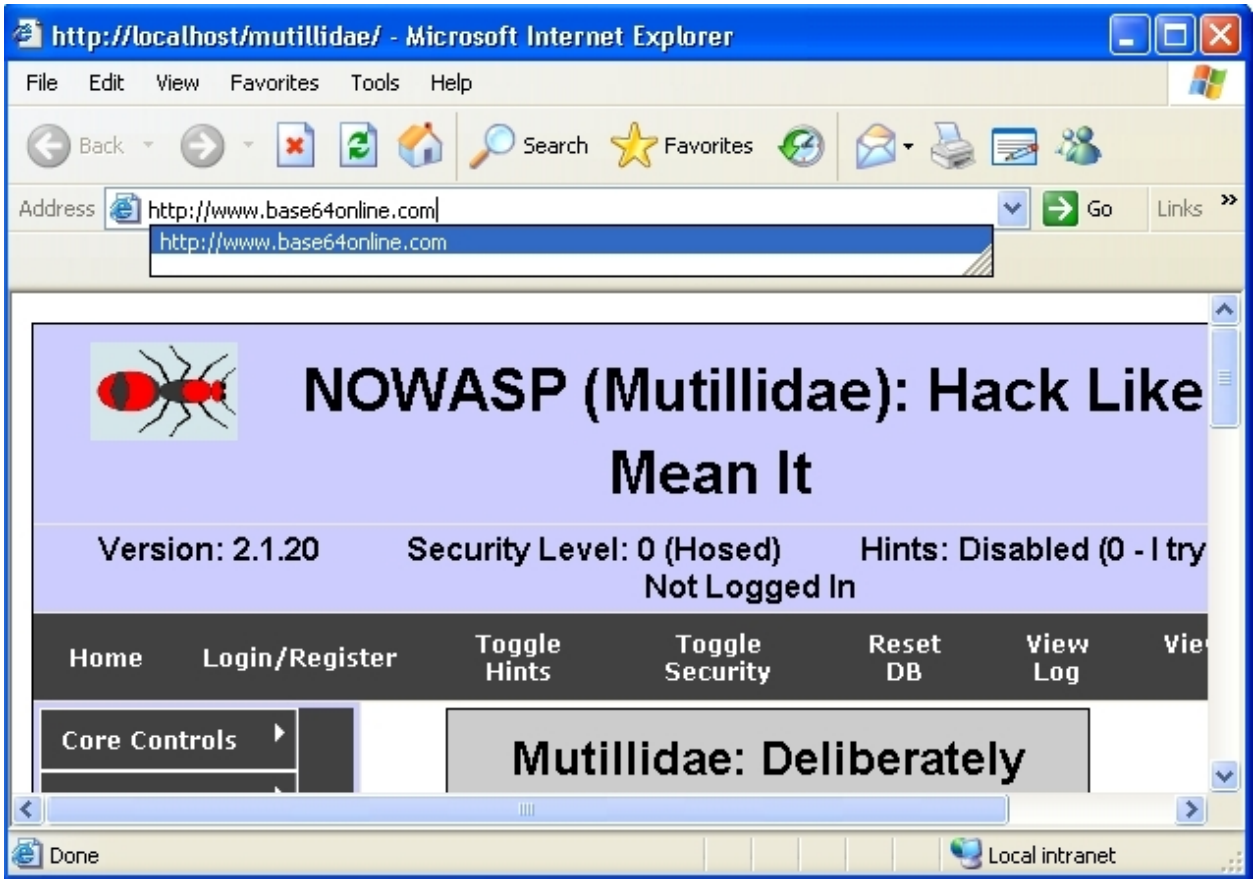
So now what ?

Lets copy the content of 12th and 13th line and go to

http://www.base64online.com /

paste the text you have copied and hit decode wait for the results.



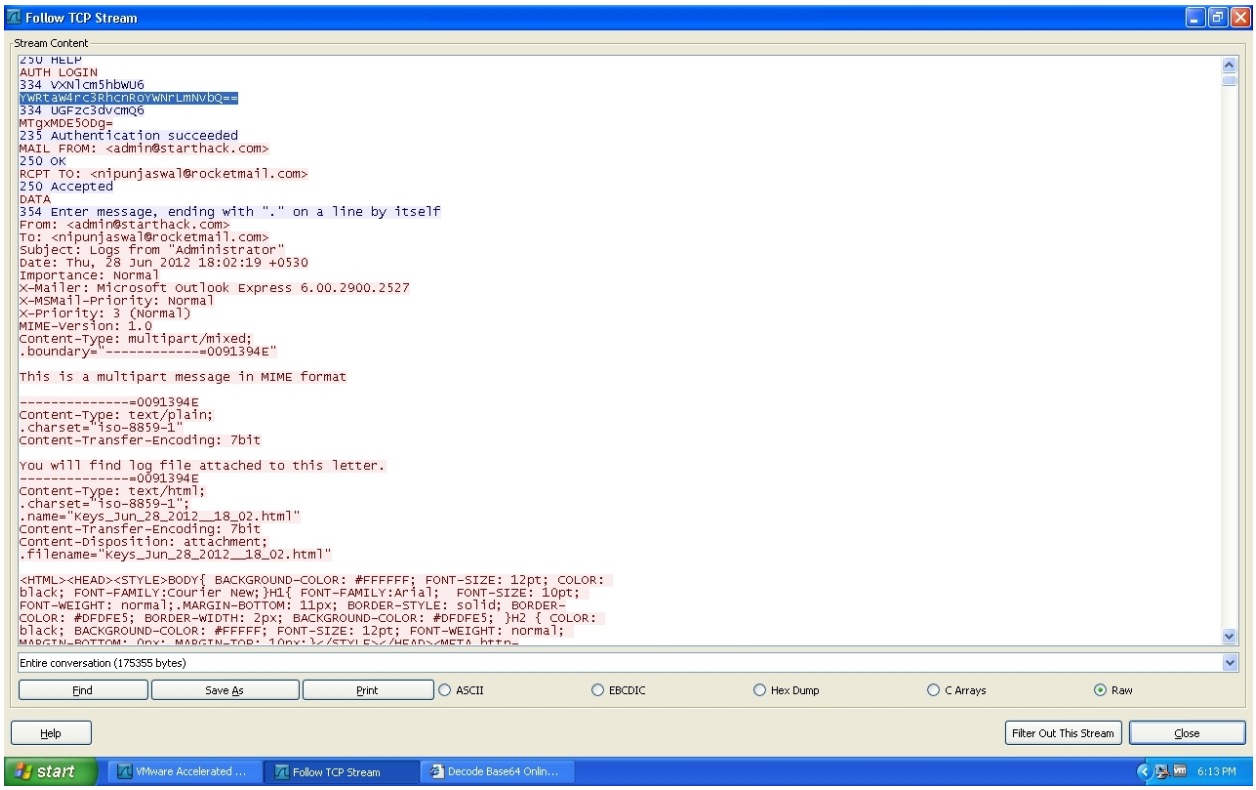

http://localhost/mutillidae/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.base64online.com
http://www.base64online.com
Go Links
NOWASP (Mutillidae): Hack Like Mean It
Version: 2.1.20 Security Level: 0 (Hosed) Hints: Disabled (0 - I try
Not Logged In
Home Login/Register Toggle Hints Toggle Security Reset DB View Log
Core Controls
Mutillidae: Deliberately
Done
Local intranet


Decode Base64 Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.base64online.com/
Go Links
Go Translate Free PC scan Babylon Mobile Games SikhNet Radio
Sri Ganesh Hosting
Start your business with Sri Ganesh
Click Here
Best for Start Up
Only ₹99/Per Month
Base64 decode | encode
Username
Ads by Google Encoder Image Converter Image Convert Convert Image
Base64 Encode Base64 Decode
How base64 encoding works?
Done
Internet
start
6:13 PM

Above Was the result of the 12th line code after 334

Now Lets Decrypt 13th

Same procedure copy and paste it in the above website

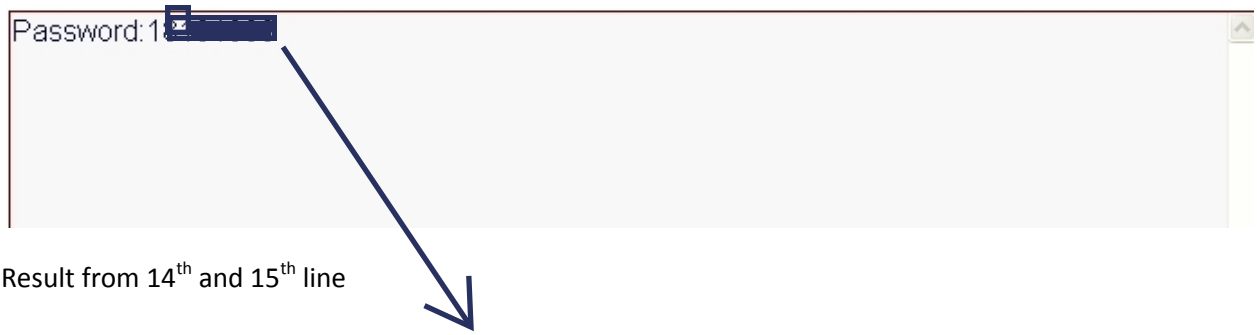


Awesome We got the **username** some of you might be thinking why there is a + sign in the username field . as we have discussed so far this email id used is created from a website and not from gmail or yahoo servers so remember by default every mail id made from the CPanel has the username " mail id " like everywhere but @ changes to +

If we have used gmail or yahoo there would have been @ symbol remember .

Okk so now lets find the password :

Base64 decode | encode



Result from 14th and 15th line

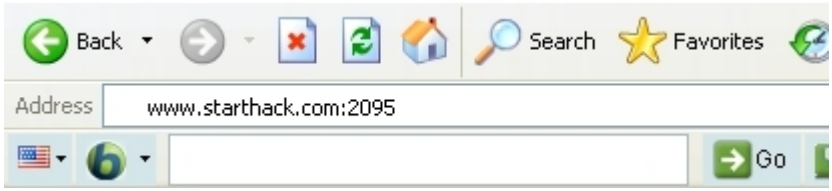
Now we have the username and the password.

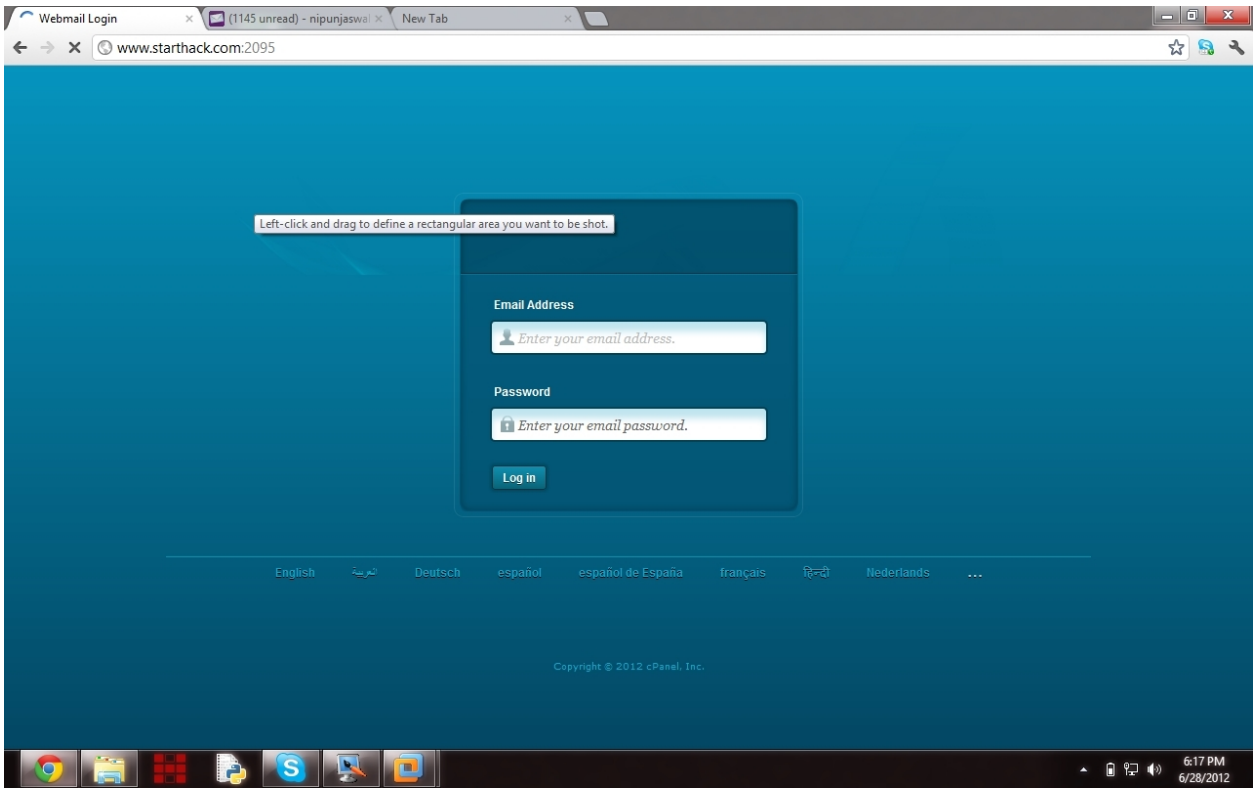
And we know what mail servers are used like cpanels generally have mail.[site name].com so where do we login?

Here in this case site's name is starthack.com so to login we know that webmail is supported at port number 2095

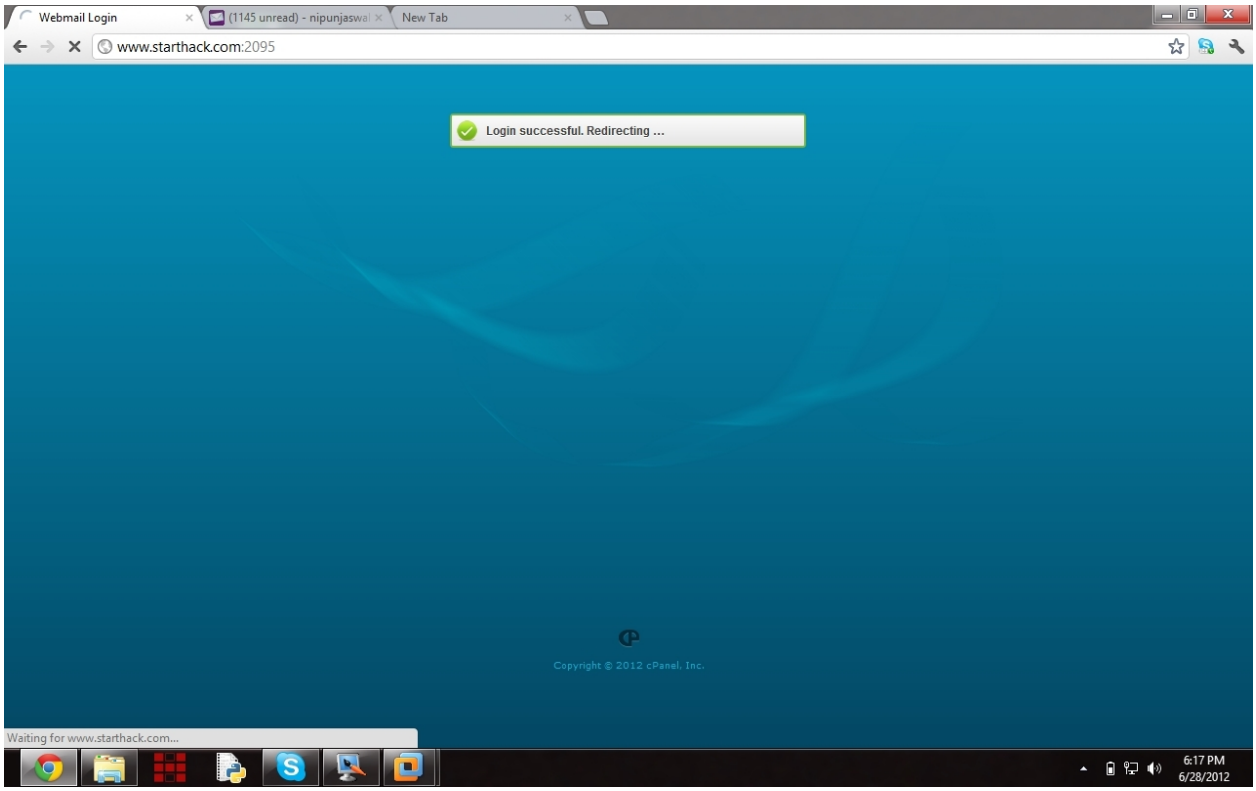
So we hit www.starthack.com:2095

Voila ! success! Login found

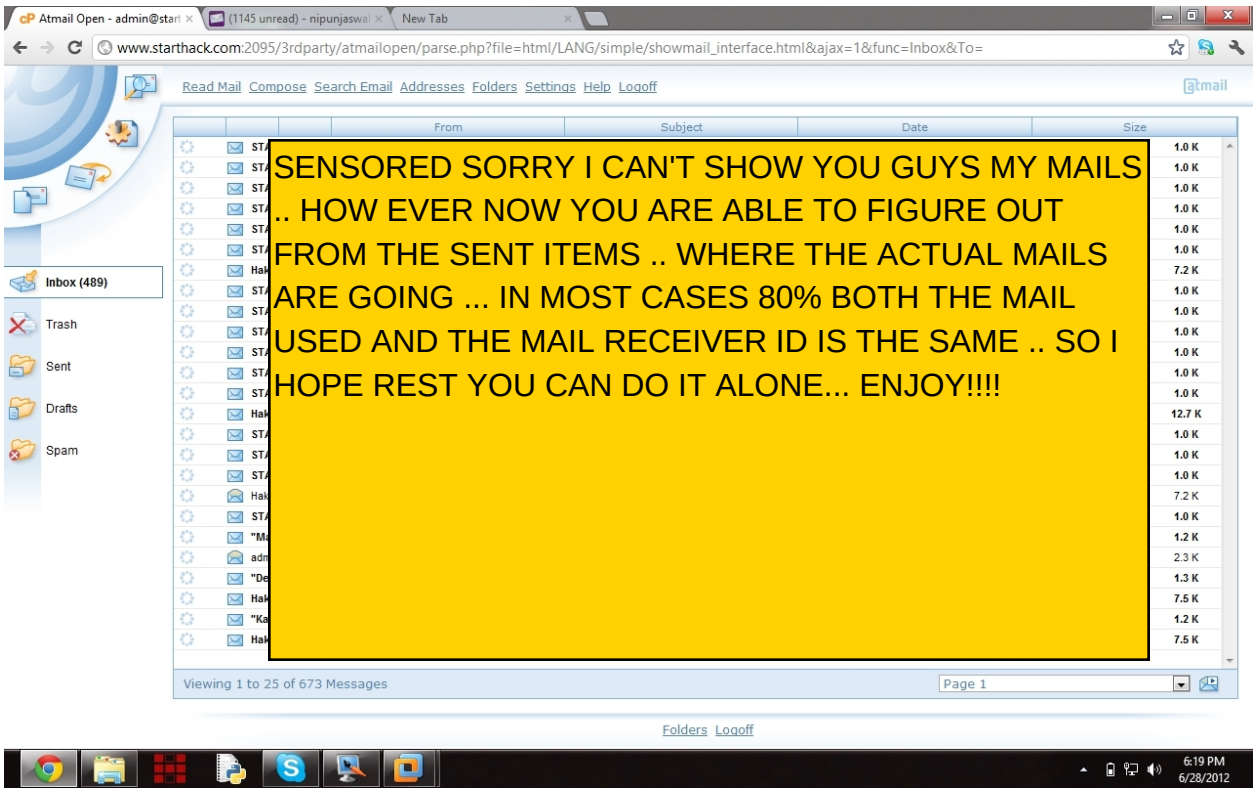




Now lets login with the credentials found !



So we logged in successfully !



Finally we are in the mail inbox. Now we can figure out whose mail is this , where the mails are travelling ? who exactly is using these mails etc.

Special Thanks To:

Laura Chappell

Protocol Analysis Institute was created by Laura Chappell, foremost network analyst and one of the top industry speakers at events such as Microsoft TechEd, HP Tech Forum, HTCIA International Conference and more.

Protocol Analysis Insitute is the parent company of Chappell University and Wireshark University.

Mr. Nickson

Mr TCGNickson is the admin at totalcomputergeek.com and promotes hackingtalks.com website . a great place to learn technology faster.

Mr. Vivek ramachandran

Vivek Ramachandran is a world renowned security researcher and evangelist. His expertise includes computer and network security, exploit research, wireless security, computer forensics, embedded systems security, compliance and e-Governance. He is the author of the books - "Wireless Penetration Testing using Backtrack" and "The Metasploit Megaprimer", both up for worldwide release in mid 2011. Vivek is a B.Tech from IIT Guwahati and an advisor to the computer science department's Security Lab.

Chetan Soni

My best friend and a pro hacker currently working as Sr. Security Specialist at SECUGENIUS SECURITY SOLUTIONS