HACKING YOUR GF'S X BOYFRIEND

(Protocol Analysis & Comp. Forensics)

Written By :

Nípun Jaswal (Ap3x Pr3Dator)

AFCEH , CISE , C|EH



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 "<u>Blind date with your</u> <u>girlfriend</u>" 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 :





	Kemote Installation	🔜 🗹 Re	mote Installation	
Security	Web Update	Ор	tions	
Enable Change password	Check for updates		Run on Windows startup	
✓ Protect Hidden Mode	Download updates automatically		Start in Hidden Mode	
✓ Protect log file	✓ Install after downloading		Ctrl + Shift + Alt + H 6/28/2012	~
Protect program options	Update Now		Interface language:	
Cock program closing			Linglish 💌	
< Back Next > Cancel	Help < ' '' Next >	Cancel Help	< Back Next > Cancel	He
🛿 Remote Installation		Remote Installation		
Control		Email		
Control		Lindi		
		Send To:		
	minutes	nipunjaswal@rocketmail.com	Test	
Email		Send From:		
Email		admin@starthack.com		
		SMTP Host:	Port:	
Log format:		mail.starthack.com	25 Find	
HTML (web page)	✓	Username:	Password:	
Send only if log size exceeds	50 🗘 КЬ	admin+scartnack.com		
< Back Next >	Cancel Help	< Back	Next > Cancel Help	
Rema	te Installation			
Ema	il			
Ema	il			
Ema	il nd To:			
Ema Sei ni	il nd To: 'punjaswal@rocketmail.com	Test		
Ema Sei Sei	il nd To: ipunjaswal@rocketmail.com ad From:	Test		
Ema Sei A	il nd To: ipunjaswal@rocketmail.com od From: <mark>r damax Keylogger</mark>	Test		
Ema Se N	il nd To: ipunjaswal@rocketmail.com nd From: r damax Keylogger The test of e-mail delivery has been com	Test		
Ema Se A	il nd To: ipunjaswal@rocketmail.com od From: r damax Keylogger The test of e-mail delivery has been com Check your mailbox.	Test		
Ema Sei A	il nd To: ipunjaswal@rocketmail.com od Erom: rdamax Keylogger The test of e-mail delivery has been con Check your mailbox.	Test		
Ema Se A	il nd To: ipunjaswal@rocketmail.com nd Erom: r damax Keylogger i The test of e-mail delivery has been corr Check your mailbox. OK	Test		
Ema Se A	il nd To: ipunjaswal@rocketmail.com ord From: ordamax Keylogger OK OK	Test		
Ema Se P	il nd To: ipunjaswal@rocketmail.com od Erom: r damax Keylogger the test of e-mail delivery has been com Check your mailbox. OK	Test		
Ema Se A	il nd To: ipunjaswal@rocketmail.com od Erom: xr damax Keylogger iv damax Keylogger The test of e-mail delivery has been com Check your mailbox. OK	Test		
Ema in Se	il nd To: ipunjaswal@rocketmail.com od From: vr damax Keylogger	Test		
Se Ardamay Keylogoor	il nd To: ipunjaswal@rocketmail.com od From: vrdamax Keylogger	Test	77 DM	



www.StartHack.com	Pa No.7
Kemote Installation	X
Screenshots	
Capture screenshot every Target: Image Quality: Low Image Quality: Image Quality: <th>High</th>	High
Remote Installation	X
se Se Se Se Se Se Finish Summary information: When someone clicks "Install.exe", keyloge installed. It will be invisible in the syst Start menu, Autostart list, list of installed its installation folder. Each 5 minutes it will "nipunjaswal@rocketmail.com" via e-mail. 1 invisible mode, the "Ctrl + Alt + Shift + H" Password protection (Security Page) is not	ger will be invisibly th Windows in the tem tray, Task Manager, software, it will also hide send logs to ro enable/disable the key combination is used.
	StartHack com Screenshots Capture screenshot every 5 in in Target: Image Quality: Low Setting Comments Setting Comm





Written by : Nipun Jaswal

FB Connect

08E

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



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



Written by : Nipun Jaswal

FB Connect

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 2^{nd} 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,

	admin@starthack.com	Logs from "Administrator"	6:02 PM	0 🛨
	Jabong.com	Get upto 40% off over 200+ brands	4:00 PM	*
	LinkedIn Updates	LinkedIn Network Updates, 6/28/2012	11:06 AM	*
	Iforex Online Trading	Become Professional Trader.	10:07 AM	*
	Make My Trip	Get up to 50% off on Holidays, Airfares & Hotels	5:08 AM	*
	sneakpeeq.com	3 Mind-Altering Options For Inspiring Inner Creativity	3:25 AM	0 *
	Dale Gardner	Log Correlation Engine 4.0 Now Available	1:25 AM	*
Log	s from "Administrator" 🖉 2			Hide Details
FROM	admin@starthack.com +		Thursda	v. June 28, 2012 6:02 PM
тс	nipuniaswal@rocketmail.com			*
	Jun_28_2 Keys_Jun			
	View Slideshow Download All			

Reply to admin@starthack.com	Send

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.

The Wireshark Network Analyzer [Wireshark 1.6.8 (SVN Rev 42761)	from /trunk-1.6)]	
Ele Edit Yew Go Capture Analyze Statistics Telephony Tools Internals	Heb	
服果我我我! ID 因 X 动助 <i>d</i> + + + + 2 T 	E E Q Q Q E # M 58 % 12	
Filter:	gression Clear Apply	
 Per V V V V V V V V V V V V V V V V V V V	rk Protocol Analyzer rk Protocol Analyzer row Files Open Open spexicly opened file ComRent: W Ande assessed of sample topologies Ande assessed of sample topologies	Chiline Website Vata ha poperly website Vata ha poperly website Vata ha poperly website The tark of additional for additite for additional for additite for additional for additite
Ready to load or casture No Packets		Profile: Default
Start To Wrechesk Mehro		
		C B Ster control





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.

🗖 Capturing from VMware Accelerated AMD F	Net Adapter (Microsoft's Packet Scheduler) [Wireshark 1.6.8 (SVN Rev 42761 from /trunk-1.6)]	. @ 🗙
Eile Edit View Go Capture Analyze Statistics	Telephony Iools Internals Help	
Filter:	Expression Clear Apply	
No. Time Source	Destination Protocol Length Info	~
410 63.665268 199.167.145.26	192.168.112.130 TCP 60 [TCP window Update] smtp > servergraph [ACK] Seq=474 Ack=174801 win=47821 Len=0	
411 63.865476 199.167.145.26	192.168.112.130 TCP 60 [TCP Window Update] smtp > servergraph [ACK] Seq=4/4 Ack=1/4801 Win=50/41 Len=0	
412 64.203266 199.167.145.26	192.168.112.130 TCP 60 [TCP window update] smtp > servergraph [ACK] seq=4/4 Ack=1/4801 win=35001 Len=0	
413 04.747348 199.107.143.20	192.106.112.100 TCP 60 [TCP window update] smtp > servergraph [ACK] seq474 ACK=174001 win=30301 Len=0	
415 65 004643 199 167 145 26	192,106,112,130 TCP 60 [CP window Update] smtp > server graph [Ack] Seq.474 Ack-17461 win-56061 Len=0	
416 65 005549 199 167 145 26	$122.106.112$ 130 TCP 60 [TCP window Undate] smtp λ server practice [act] $3cq-474$ act-17461 window $1cd-201$	
417 70 226150 199 167 145 26		
418 70 227002 192 168 112 130		
419 70.227384 199.167.145.26	192.168.112.130 TCP 60 smtp > servergraph [ACK] seg=502 Ack=174807 Win=64240 Len=0	
420 70.865206 199.167.145.26	192.168.112.130 SMTP 102 S: 221 velocity, indervers.com closing connection	
421 70.868521 192.168.112.130	199.167.145.26 TCP 54 servergraph > smtp [FIN. ACK] Seg=174807 Ack=550 win=63691 Len=0	
422 70.869153 199.167.145.26	192.168.112.130 TCP 60 smtp > servergraph [ACK] Seg=550 Ack=174808 Win=64239 Len=0	
423 70.905255 199.167.145.26	192.168.112.130 TCP 60 smtp > servergraph [FIN, PSH, ACK] Seg=550 Ack=174808 Win=64239 Len=0	
424 70.906485 192.168.112.130	199.167.145.26 TCP 54 servergraph > smtp [ACK] Seg=174808 Ack=551 win=63691 Len=0	~
<		>
Ename 1: 175 butter on wine (1400	ite) 175 bytes conturned (1400 bits)	
E Fibernet II. Snc: Wavere c0:00:09	(0):50:50:00:00 Det : TB/dmcset 7f:ff:fs (0):00:50:7f:ff:fs)	
E Internet Protocol Version 4 Src:	(00.100.00.000.000, 000.000, 000.0000, 000.000	
E liser Datagram Protocol Src Port:	196:100:111 (196:100:111), 096: 299:299:299 (299:299:299)	
Hypertext Transfer Protocol	(1)52 (4)52), 55 (1010, 550) (1905)	
a type text in anoter in otocor		
0000 01 00 5e 7f ff fa 00 50 56 c	00 08 08 00 45 00	~
0010 00 a1 19 33 00 00 01 11 77 7		
0030 43 48 20 2a 20 48 54 54 50 2	40 20 35 43 41 32	
0040 6f 73 74 3a 32 33 39 2e 32 3	35 2e 32 35 35 2e ost:239, 255,255.	~
0050 27 25 20 25 21 20 20 20 04 0	52 54 25 75 75 66 250:1000 strupp	
In the second se	Lecs: 424 usplayeu: 424 markeu: 0 Pronie: Default	
Start Capturing from VMwa		6:02 PM



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'

🕅 VMware Accelerated AMD PCNet Adapter (A	Wicrosoft's Packet Schedul	er) [Wireshark 1.6	.8 (SVN Rev 42761 from /trunk-1.6)]	
Eile Edit View Go Capture Analyze Statistics	Telephony <u>T</u> ools <u>I</u> nternals	Help		
	< < ⇒ <> < < < < 4 < < < 4 < < < 3 < 4 <		@, 🖭 👪 🔟 🎨 🞉 💢	
Filter: smtp	~	Expression Clear Ap	ply	
No. Time Source	Destination	Protocol Length Inf	0	
21 49.484885 199.167.145.26	192.168.112.130	SMTP 235 S	: 220-velocity.indservers.com ESMTP Exim 4.77 #2 Thu, 28 Jun	2012 18:02:20 +0530 220
22 49.489906 192.168.112.130	199.167.145.26	SMTP 76 C	: EHLO NIPUN-63C3A0681	(1 (2] 250 STTE 52420000
24 30.203139 199.107.143.20	192.108.112.130	SMTP 202.5	: 250-Verucity. Indservers.com Herro NIPON-63C3A0681 [115.240.	61.63] 230-SIZE 32428800
27 50 805201 199 167 145 26	199.107.143.20	SMTP 72 S	: 334 V/VI]cm5bbw06	
28 50 806967 192 168 112 130	199 167 145 26	SMTP 92.5	: VWPtawArc3PbcnPoVWNrLmNybO==	
30 51, 365240 199, 167, 145, 26	192.168.112.130	SMTP 72 S	: 334 LIGEZC3dvcm06	
31 51.365805 192.168.112.130	199.167.145.26	SMTP 68 C	: MTaxMDE50Da=	
33 51.925202 199.167.145.26	192.168.112.130	SMTP 84 S	: 235 Authentication succeeded	
34 51.925678 192.168.112.130	199.167.145.26	SMTP 88 C	: MAIL FROM: <admin@starthack.com></admin@starthack.com>	
36 52.465243 199.167.145.26	192.168.112.130	SMTP 62 S	: 250 OK	
37 52.467755 192.168.112.130	199.167.145.26	SMTP 93 C	: RCPT TO: <nipunjaswal@rocketmail.com></nipunjaswal@rocketmail.com>	
39 53.185235 199.167.145.26	192.168.112.130	SMTP 68 S	: 250 Accepted	
40 53.186349 192.168.112.130	199.167.145.26	SMTP 60 C	DATA	
42 54.145332 199.167.145.26	192.168.112.130	SMTP 110 S	: 354 Enter message, ending with "." on a line by itself	~
<				>
NOTICE, NOU 3				<u>^</u>
0 = Congestion w	/indow Reduced (CWR):	Not set		
0 = ECN-ECNO: NO	ot set			
	set			
Acknowledgem	ient: Set			
I = Push: Set	+			
0 = Reset: Not sot	.eu			
= Syn: Not set				
window size value: 64240				
[Calculated window size: 64240]				
[window size scaling factor: -2	(no window scaling	used)]		
E Checksum: 0xd2b9 [validation di	sabled	abca/]		
[Good Checksum: False]				
[Bad Checksum: False]				
Simple Mail Transfer Protocol				
Response: 220-velocity.indserve	ers.com ESMTP Exim 4.	77 #2 Thu, 28 Ju	ın 2012 18:02:20 +0530 \r\n	×
0000 00 0c 29 39 e0 5a 00 50 56 e	c 75 54 08 00 45 00		. F.	
0010 00 dd bf ec 00 00 80 06 f0 4:	1 c7 a7 91 1a c0 a8			
0020 70 82 00 19 04 e3 7f 43 11 e	d 7e e1 cc c9 50 18	pc~.;	·P:	
	0 /0 03 00 0T 03 09 6 65 72 73 2e 63 6f	ty indse rvers		
0050 ed 20 45 52 4d 54 50 20 45 7	0 60 64 00 24 00 27	m remth rvim	A 7	<u> </u>
Hile: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem P	ackets: 475 Displayed: 188 Marke	ed: U Dropped: 0		Prohie: Default .:
Start Mware Accelerated				🔇 🖉 💁 🚾 6:06 PM

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 .



geb get g	🚾 VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) [Wireshark 1.6.8] (SVN R	v 42761 from /trunk-1.6)]
Image Source Destination Clear Apply No. Time Source Destination Clear Apply 22 494.489805 199.167.145.26 SMTP 76 C: EHLO NI MeX Packet (toggle) State Apply 22 494.489805 199.167.145.26 SMTP 76 C: EHLO NI Packet (toggle) State Apply 22 494.489805 199.167.145.26 SMTP 76 C: EHLO NI State Apply 22 50.25519 199.167.145.26 SMTP 76 C: EHLO NI State Apply	Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help	
Piter: Surge Proceed Length Info 22.443.458353 1009.165.132.130 100.139.165.132.130 10		🖬 🕅 🎆 💥 🔯
Filter: Clar Source Destination Other Acply 22 49.4848685 109.167.145.26 112.110.30 SMTP 76.5 E EHLO NI 224 50.265148 129.166.112.130 SMTP 76.5 E EHLO NI 224 50.265148 129.166.112.130 SMTP 76.5 E EHLO NI 224 50.265148 129.166.112.130 SMTP 76.5 E EHLO NI 225 50.25648 129.166.112.130 SMTP 76.5 E EHLO NI 225 50.25648 129.166.112.130 SMTP 72.5 S 334 UGF Mark Padet (toggle) Ignere Padet (toggle) NIPUN-63C3A0681 [115.240.61.63] 250-5IZE 52428800 30 51.36526 199.167.145.26 192.166.112.130 SMTP 72.5 S 334 UGF Prophy as Filter		
No. Thme Source Desthation Protocol Length Info 21 149.448365 149.166.112.130 199.167.145.26 SMTP 225 S1220-vel Mark Packet (toggle) porce Packet (toggle) porce Packet (toggle) porce Packet (toggle) porce Packet (toggle) St.1.45.26 SMTP 225 S1.220-vel St.1.67.145.26 SMTP 225 S1.2250-vel St.1.8617.145.26 SMTP 66 C: Auruk Mark Packet (toggle) St.1.8657(1.19.1.67.145.26 SMTP 62 S1: 334 VXR Marualy Resolve Address 30 S1.365240 199.167.145.26 SMTP 68 C: MTP 88 C: 331 S1.365805 192.168.112.130 SMTP 68 C: Marualy Resolve Address 31 S1.365805 192.168.112.130 SMTP 68 C: MTP 68 C: Marual Packet Address Prepare a Filer Correstation Filer <t< td=""><td>Filter: smtp Expression Clear Apply</td><td></td></t<>	Filter: smtp Expression Clear Apply	
22 49.4830900 192010612012030 199.167.145.26 199.167.145.26 192.168.112.130 SMTP 70 C: EHLO NI grow Packet (toggle) 24 50.26548 192.168.112.130 199.167.145.26 192.168.112.130 SMTP 70 C: EHLO NI grow Packet (toggle) 27 50.805201 199.167.145.26 192.168.112.130 SMTP 72 S: 334 VXH 82 50.806067 192.168.112.130 199.167.145.26 192.168.112.130 SMTP 72 S: 334 VXH 83 51.355240 199.167.145.26 192.168.112.130 SMTP 72 S: 334 VXH Mark Packet (toggle) 83 51.952502 199.167.145.26 192.168.112.130 SMTP 72 S: 334 VXH Mark Packet (toggle) 83 51.9252678 192.168.112.130 199.167.145.26 192.168.112.130 SMTP 63 C: MTTgwho 63 C: MTGwho 34 51.925678 192.168.112.130 199.167.145.26 192.168.112.130 SMTP 63 C: MTGwho 5CP 5CP 35 53.185235 199.167.145.26 192.168.112.130 SMTP 63 C: MTAL RR 63 C: MAIL RR Cohro Conversion 5CP 5C	No. Time Source Destination Protocol Length Info	۸ ۵ - ۱۹۰۰ ۵۰ - ۵۰ - ۵۹ - ۵۹ - ۵۹ - ۹۰ - ۲۹ - ۲۹ - ۲۹ - ۲۹ - ۵۹ - ۵۹ - ۵۹ - ۵۹
24 \$0.265159 199.167.145.26 192.168.112.130 smtp 205 5: 250-vel Impore Packet (toggle) 25 \$0.265648 192.168.112.130 199.167.145.26 smtp 66 C: AUTH LO 25 \$0.265648 192.168.112.130 199.167.145.26 smtp 66 C: AUTH LO 25 \$0.265648 192.168.112.130 199.167.145.26 smtp 75 C: AUTH LO 35 \$1.365240 199.167.145.26 192.168.112.130 smtp 75 C: AUTH CO 35 \$1.365240 199.167.145.26 199.167.145.26 smtp 86 C: MURTAME 36 \$12.2651 199.167.145.26 192.168.112.130 smtp 84 S: 1255 C: Conversation Filer 36 \$22.467755 192.168.112.130 199.167.145.26 smtp 93 C: RCPT TO 39 \$3.185235 199.167.145.26 Smtp 93 C: RCPT TO Folow UCP Stream 760w USP Stream Folow US Stream Folow US Stream Folow US Stream 0.1	22 49.484883 199.107.143.20 192.108.112.130 SMTP 233 S. 220-VE	Mark Packet (toggle) P EX III 4.77 #2 110, 28 Juli 2012 18.02.20 +0350 220
25 50.265648 192.168.112.130 199.167.145.26 SMTP 6 C: ANTH LO 27 50.805201 199.167.145.26 192.168.112.130 199.167.145.26 SMTP 72 S: 334 VXN 30 51.365240 199.167.145.26 SMTP 72 S: 334 VXN Apply as Filter Prepare a Filter 33 51.365260 192.168.112.130 199.167.145.26 SMTP 68 C: MTgMDE Prepare a Filter 33 51.925202 199.167.145.26 SMTP 68 C: MTgMDE Colvies Conversation Filter Colvies Conversation Filter 36 52.465243 199.167.145.26 SMTP 68 C: MTGMDE Colvies Conversation Filter Colvies Conversation Filter 37 52.467755 192.168.112.130 199.167.145.26 SMTP 68 C: 250 OK SCTP Colvies Conversation Filter <	24 50.265159 199.167.145.26 192.168.112.130 SMTP 202 5: 250-ve	Ignore Packet (toggle) NIPUN-63C3A0681 [115.240.61.63] 250-SIZE 52428800
27 50.805201 199.167.145.26 192.168.112.130 SMTP 72 53.334 VXH 28 50.806967 192.168.112.130 SMTP 72 53.334 VXH Manually Resolve Address 30 51.365200 199.167.145.26 192.168.112.130 SMTP 72 53.334 UXH Apply as Filer 33 51.92502 199.167.145.26 192.168.112.130 SMTP 84 52.35 Aut Proprese as Filer Conversation Filer 34 51.92502 199.167.145.26 192.168.112.130 SMTP 84 52.35 Aut Conversation Filer Conversation Filer 35 52.465743 192.168.112.130 SMTP 62 52.250 OL Colorie Conversation SCTP	25 50.265648 192.168.112.130 199.167.145.26 SMTP 66 C: AUTH LC	Set Time Reference (toggle)
28 50.806967 192.168.112.130 199.167.145.26 SMTP 84 C: YWRTAWA 30 51.365240 199.167.145.26 192.168.112.130 SMTP 72 S: 334 UMC 33 51.92502 199.167.145.26 SMTP 84 S: 235 Aut Conversation Filter 33 51.92507 192.168.112.130 199.167.145.26 SMTP 88 C: MAIL FR Conversation Filter 34 51.925678 192.168.112.130 199.167.145.26 SMTP 88 C: MAIL FR Conversation Filter 35 52.465243 199.167.145.26 SMTP 93 C: RCPT 70 Conversation Filter Conversation Filter 36 52.465243 192.168.112.130 SMTP 62 S: 230 OK SCTP Foldow UCP Stream 37 52.46775 192.168.112.130 SMTP 60 C: DATA Foldow UCP Stream Foldow UCP Stream 40 53.185235 199.167.145.26 192.168.112.130 SMTP 100 S: 354 Ent Foldow UCP Stream Foldow UCP Stream	27 50.805201 199.167.145.26 192.168.112.130 SMTP 72 5: 334 VXI	Manually Resolve Address
33 51,35740 199.167,143.26 192.168.112.130 SMTP 72 51 S34 0d4 33 51,052502 199.167,145.26 192.168.112.130 SMTP 84 S2 235 Aut Conversation filter 34 51,925768 192.168.112.130 199.167.145.26 SMTP 88 C: MALL Colver conversation filter 35 52.467755 192.168.112.130 199.167.145.26 SMTP 92 C: RCPT Follow ICP.Stream 39 53.185235 199.167.145.26 192.168.112.130 SMTP 68 S: 250 ACC Follow ICP.Stream 40 53.186349 199.167.145.26 192.168.112.130 SMTP 68 S: 250 ACC Follow ICP.Stream Follow ICP.Stream 40 53.186349 192.168.112.130 SMTP 68 S: 250 ACC Follow ICP.Stream Follow ICP.Stream 0 ECOnsection window Reduced (CwR): Not set Follow S12.Stream Conv 0 ECOnsection window Reduced (CwR): Not set Phile Show Padet in New Window 0 Experiment: Set Phile Show Padet in New Window Show Padet in New Window 0 Fillow S12 Goad chacksum: Sate Phile	28 50.806967 192.168.112.130 199.167.145.26 SMTP 84 C: YWRtaW4	Δpply ac Filter
33 51.92500 109.167.145.26 192.168.112.130 SMTP 84 5: 235 Aut Conversation Filter 34 51.92500 109.167.145.26 192.168.112.130 SMTP 84 5: 235 Aut Conversation Filter Conversation 35 52.46775 192.168.112.130 199.167.145.26 SMTP 86 C: NAIL FR Conversation Filter Conversation 37 52.46775 192.168.112.130 199.167.145.26 SMTP 93 C: RCPT TO Follow ICP Stream Conversation 39 53.186349 192.168.112.130 SMTP 93 C: RCPT TO Follow ICP Stream Follow ICP Stream 40 53.186349 192.168.112.130 SMTP 10 S: 354 Ent Follow ICP Stream Follow Strest Conv expected for Window Reduced (CwR): Not set Follow ICP Stream Conv	30 51.365240 199.167.145.26 192.168.112.130 5MTP /2 5: 334 UGF 31 51 365805 192 168 112 130 199 167 145 26 SMTP 68 C MTGYMDG	Prenare a Filter
34 \$1,925678 192.168.112.130 199.167.145.26 SMTP 88 C: MAIL FR 36 \$2,465243 199.167.145.26 SMTP 62 \$2 \$20 oK SCIP Colorec Conversation Colorec Conversation Colorec Conversation SCIP Colorec Conversation Coloreconversation Colorec Conversation	33 51.925202 199.167.145.26 192.168.112.130 SMTP 84 5: 235 Aut	Conversation Filter
36 52.465243 199.167.145.26 192.168.112.130 SMTP 62 52 250 oK SCTP > 37 52.467755 192.168.112.130 199.167.145.26 SMTP 93 C: RCPT To Folow ICP.Stream com> 40 53.185235 199.167.145.26 199.167.145.26 SMTP 60 C: RCPT To Folow ICP.Stream com> 40 53.185235 199.167.145.26 199.167.145.26 SMTP 60 C: DATA Folow ICP.Stream Com> Folow ICP.Stream Folow ICP.Stream Folow ICP.Stream Folow ICP.Stream Folow ICP.Stream Folow ICP.Stream Com> Folow ICP.Stream Folow ICP.	34 51.925678 192.168.112.130 199.167.145.26 SMTP 88 C: MAIL FF	Colorize Conversation
37 52.467755 192.168.112.130 199.167.145.26 SMTP 93 C5: 250 AC7 Folow ICP Stream 39 53.186349 192.168.112.130 SMTP 66 S: 250 AC7 Folow ICP Stream Folow ICP Stream 42 54.145332 199.167.145.26 SMTP 60 C: DATA Folow ICP Stream Folow ICP Stream Folow ICP Stream 42 54.145332 199.167.145.26 SMTP 110 S: 354 Ent Folow ICP Stream Folow ICP	36 52.465243 199.167.145.26 192.168.112.130 SMTP 62 5: 250 OK	SCTP +
39 53.185235 199.167.145.26 192.168.112.130 SMTP 68 5: 250 Acc Folow UDP Stream 42 54.145332 199.167.145.26 192.168.112.130 SMTP 110 s: 354 ent Folow UDP Stream 42 54.145332 199.167.145.26 192.168.112.130 SMTP 110 s: 354 ent Folow UDP Stream Copy * * * * * * * 0 = Copy * <t< td=""><td>37 52.467755 192.168.112.130 199.167.145.26 SMTP 93 C: RCPT TO</td><td>Follow TCP Stream COM></td></t<>	37 52.467755 192.168.112.130 199.167.145.26 SMTP 93 C: RCPT TO	Follow TCP Stream COM>
40 53.186349 192.168.112.130 199.167.143.26 SMTP 60 0 C: DATA 42 54.145332 199.167.145.26 192.168.112.130 SMTP 110 S: 354 Ent Cov Interpretation window Reduced (CWR): Not set Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Interpretation window Reduced (CWR): Not set Interpretation window Interpretation window Interpretation window size: Set Interpretation window Interpretation window Interpretation window size: 64240 Interpretation window size: 64240 Interpretation window Interpretation window size: 64240 Interpretation window Interpretation window Intere	39 53.185235 199.167.145.26 192.168.112.130 SMTP 68 5: 250 Acc	Follow UDP Stream
42 54.145522 199.167.145.20 192.166.112.150 SmP 110 5: 554 Ent Copy Image: Copy in the content of the copy in	40 53.186349 192.168.112.130 199.167.145.26 SMTP 60 C: DATA	Follow SSL Stream
Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set Image: Constraint of the set	42 34.143332 199.107.143.20 192.108.112.130 SMIP 110 5: 334 EIN	Copy On a time by itself
<pre>into into a congestion window Reduced (CwR): Not set into into a congestion window Reduced (CwR): Not set into into a congestion window Reduced (CwR): Not set into into a congestion window Reduced (CwR): Not set into into a congestion window Reduced (CwR): Not set into into a congestion window reduced (CwR): Not set into into a congestion window size: Set into into a congestion window scaling used)] Calculated window size: Set222 Congestion window scaling used)] Congestion window scaling used) Congestion window scaling used)] Congestion window scaling used) Congestion window scaling</pre>		
<pre>0 = ECN-Echo: Not set</pre>	0 = Congestion Window Reduced (CWR): Not set	Gli Decode As
<pre>0 = Urgent: Not set Show Packet in New Window1 = Acknowledgement: Set1 = Push: Set0. = Reset: Not set0. = Syn: Not set0. = Fin: Not set window size (64240) [Calculated window size: 64240] [Calculated window size: 64240] [Window size scaling factor: -2 (no window scaling used)] @ checksum: 0xd2be [validation disabled] [Good checksum: False]</pre>	0 = ECN-Echo: Not set	E Print
<pre>1 = Acknowledgement: Set </pre>	0 = Urgent: Not set	Show Packet in New Window
<pre></pre>	1 = Acknowledgement: Set	
<pre></pre>	1 = Push: Set	
<pre></pre>		
<pre>window size value: 64240 [Calculated window size: 64240] [window size scaling factor: -2 (no window scaling used)] [window size scaling factor: -2 (no window scaling used)] [cood checksum: Calse] [Cood checksum: False] [Cood checksum: False]</pre>		
[Calculated window size: 64240] [Window size scaling factor: -2 (no window scaling used)] □ Checksum: 0xd2b9 [validation disabled] [Good Checksum: False]	Window size value: 64240	
[Window size scaling factor: -2 (no window scaling used)] ⊠ checksum: 0xd2be [validation disabled] [Good checksum: False]	[Calculated window size: 64240]	
Clocksum: Oxd2b9 [validation disabled] [Good Checksum: False] [Food Checksum: False] [Food Checksum: False]	[window size scaling factor: -2 (no window scaling used)]	
[Good Checksum: False]	Checksum: 0xd2b9 [validation disabled]	
	[Good Checksum: False]	
	Ead Checksum: Faisej	
a Simple Mail Transfer Protocol	Simple Mail Transfer Protocol	
🖻 Response: 220-velocity.indservers.com ESMTP Exim 4.77 #2 Thu, 28 Jun 2012 18:02:20 +0530 \r\n	□ Response: 220-velocity.indservers.com ESMTP Exim 4.77 #2 Thu, 28 Jun 2012 1	3:02:20 +0530 \r\n
0000 00 c2 9 39 e0 5a 00 50 56 ec 75 54 08 00 45 00)9.Z.P V.UTE.	0000 00 0c 29 39 e0 5a 00 50 56 ec 75 54 08 00 45 00)9.7.P V.UTF.	
0010 00 dd bf ec 00 00 80 06 f0 41 c7 47 91 14 c0 48	0010 00 dd bf ec 00 00 80 06 f0 41 c7 a7 91 1a c0 a8	
10020 70 82 00 19 04 e3 7f 43 11 ed 7e e1 cc c9 50 18 pP.	0020 70 82 00 19 04 e3 7t 43 11 ed 7e e1 cc c9 50 18 pC~P.	
0040 74 79 2e 69 6e 64 73 65 72 76 65 72 73 2e 63 6f ty.indse rvers.co	0040 74 79 2e 69 6e 64 73 65 72 76 65 72 73 2e 63 6f ty.indse rvers.co	
0050 64 00 45 52 44 54 50 20 45 72 60 64 20 24 22 27 m restruct an restruct and restruction an	0050 6d 20 45 52 4d 54 50 20 45 79 60 6d 20 24 26 27 ministration resting 4 7	Profile: Default
γ start 🔰 🕅 Whate Accelerated	Start Received a system stratege start and stratege stratege start and stratege stratege stratege start and stratege stratege s	

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





www.StartHack.com

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

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 11^{th} 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.

7 Follow TCP Stream	
r Stream Content	
220-velocity indservers.com ESMTP Exim 4.77 #2 Thu, 28 Jun 2012 18:02:20 +0530 220-we do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. EHLO NTPUN-63C3A00681 250-velocity indservers.com Hello NIPUN-63C3A0681 [115.240.61.63] 250-size 52428800 250-PIPELINING 250-PIPELINING 250-STARTILS	
AUTH LOGIN 334 vxNlcm5hbwU6 YwRtaw4rc3BhcnRoYwNrLmNvbQ== 334 uGF23dvcmQ6 MTGwMDE50Dg= 725 uMEDFiction cucconded	
AALL FROM: <adminustrathack.com> 250 oK RCPT TO: <nipunjaswal@rocketmail.com></nipunjaswal@rocketmail.com></adminustrathack.com>	
250 Accepted Data 334 Enter message, ending with "." on a line by itself From: sadmin@starthack.com> To: <nipunjaswal@rocketmail.com> Subject: Logs from "administrator" Date: Thu, 28 Jun 2012 18:02:19 +0530 Importance: Normal X-mBmail-Priority: Normal X-mBmail-Priority: Normal X-mPiority: 3 (Normal) XIME-Version: 1.0 Content-Type: multipart/mixed: .boundary=0091394E" This is a multipart message in MIME format </nipunjaswal@rocketmail.com>	
.charset="iso=8859-1" Content-Transfer-Encoding: 7bit	
Content-Type: text/html; .charset="iso-8859-1"; .name="keys_jun_28_2012_ls_02.html"	M
Entire conversation (175355 bytes)	~
Eind Save As Print ASCII EBCDIC Hex Dump O C Array:	s 💿 Raw
Цер	Filter Out This Stream
start VMware Accelerated I Follow TCP Stream	🔦 🖉 🕵 🚾 6:07 PM



http://localhost/	mutillidae/ - Mi	crosoft Internet	Explorer			
File Edit View Fa	avorites Tools I	Help				-
G Back * O	💌 🖻 🎸) 🔎 Search 🚽	Favorites) 🔗 - 🌺	2 🔏	
Address 🕘 http://www	w.base64online.com				💌 🔁 Go	Links »
http://ww	vw.base64online.co	m				
						~
	NON	IASP (N	lutillid	ae): Ha	ack Li	ke
		Ν	lean It			
Version: 2	.1.20 S	ecurity Level:	0 (Hosed) Not Logged	Hints: Di I In	sabled (0	- I try
Home Log	in/Register	Toggle Hints	Toggle Security	Reset DB	View Log	Vie
Core Controls	• •	Mutill	idae: De	liberate	ly	~
<u>s</u>		1111				>
E Done				3	Local Intranet	.::
Decode Base64 Online - Microsoft Into File Edit View Eavorites Tools Help	ernet Explorer					
🕝 Back 🝷 💿 🖌 🗾 🛃 🏠 🔎	Search 👷 Favorites 🚱 👔	3- 칋 🖂 🦓				
Address 🕘 http://www.base64online.com/	→ Go 🕞 Tra	anslate • 🕼 Free PC scan () Bat	ylon Mobile	(a) Games	🕜 SikhNet Radio 🕤	✓ → Go Links ³ (+-) → → → → → → → → → → → → → → → → → → →
	🔊 Sri Gai	nesh Hosting	Click Here	Only FOO/Per		
	Start your busine	ss with Sri Ganesh 🖌	Best for Start Up	(99/ Month		
	Start your busine	ess with Sri Ganesh र्म्ज Base64 decodo	Best før Start Up e encode	99/Month		





Above Was the result of the ${\bf 12}^{\rm th}$ line code after 334

Now Lets Decrypt 13^{th}

Same procedure copy and paste it in the above website

🗖 Follow TCP Stream							
Stream Content							
250 HELP AUTH LOGIN 334 VXN1cm5hbwu6 YwstawdrcBhonbwu6 WmgtawdrosBhonbwu6 MigxMbSSOdg 235 Authenticatio Mall FROM: <admin 250 oK RCPT TO: <nipunja 250 oK RCPT TO: <nipunja 250 Accepted 354 Cnter message From: <admin@star To: <nipunjaswa10 Subject: Logs fro Date: Thu, 28 Jun Importance: Norma X-Mailar: Microso X-MSMail-Priority X-Priority; 3 (No MIME-Version: 1.0 Chonter-Type: mul</nipunjaswa10 </admin@star </nipunja </nipunja </admin 	WNFLMNVbQ== n succeeded @starthack.com> swal@rocketmail , ending with " thack.com> "thack.com "Administrato , 2012 18:02:19 1 ft outlook Expr : Normal rmal) tipart/mixed:	.com> ." on a line by its r" +0530 ess 6.00.2900.2527 "	elf				
This is a multina	rt message in M	TME format					
Content-Type: tex .charset="iso-885 Content-Transfer- You will find log Content-Type: tex .charset="iso-885 .name="keys_Jun_2" Content-Transfer- Content-Transfer- Content-Dispositi .filename="keys_J <html><head><styl black: FONT-FARL FONT-WEIGHT: norm COLOR: #APCFPES: B black: BACKGROUND MascIL BACKGROUND</styl </head></html>	91394E t/plain; 9-1" Encoding: 7bit file attached 91394 t/ntm; attached; 91394 s_2012_18_02,h Encoding: 7bit un_28_2012_18_02,h Encoding: 7bit un_28_2012_18_02,h ExBODY{ BACKGRO Y:Courier New; 1a]; MARGIN-BOTTH: 2p -COLOR: #FFFFF; . MARGIN-TOP:	to this letter. tml" 02.html" UND-COLOR: #FFFFF; 14. FONT-FMILYIAN OM: 11px; BORDER-ST 7: BACKSROUND-COLOR FONT-SIZE: 12pt; F 10px: J/2TX, ISX/LEX	FONT-SIZE: 12pt; CC al; FONT-SIZE: 10pt YLE: solid; BOADER- : #OFDFES; JH2 { CO ONT-WEIGHT: normal; DX-MEIG HITA-	DLOR: ;; _OR:			×
Entire conversation (175355	i bytes)						V
Eind	Save <u>A</u> s	Print	O ASCII	EBCDIC	O Hex Dump	🔘 C Arrays	Raw
Help							Filter Out This Stream
🛃 start 🔰 🔽 🗤	ware Accelerated	Tollow TCP Stream	Decode Base64 Onlin				🤦 📜 🚾 6:13 PM

baseb4 decode | encode

admin+starthack.com		

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



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 <u>www.starthack.com:2095</u>

Voila ! success! Login found





🔷 Webmail Login	× 🖾 (1145 unread) - nipunjaswal × New Tab × 🗖	
$\leftarrow \Rightarrow \times \bigcirc$ www.st	arthack.com:2095	☆ 🔝 🔧
	Left-click and drag to define a rectangular area you want to be shot.	
	Email Address	
	an a	
	Password	
	En Enter your email pussioora.	
	Log in	
	📕 👌 🔕 😣 💷	€:17 PM 6/28/2012

Now lets login with the credentials found !

🖉 Webmail Login 🛛 🗙 🖾 (1145 unrea	id) - nipunjaswal × 🔪 New Tab 🛛 × 🔽	
\leftrightarrow \Rightarrow X (S) www.starthack.com:2095		公 🗟 🔧
	Cogin successiti. Redirecting	
	œ	
Waiting for www.starthack.com		
	3 🖳 🧏 📴	▲ 🖬 🖓 📢 6:17 PM 6/28/2012

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 <u>IIT Guwahati</u> 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

