The Ultimate Guide to Hacking Windows Part III

By:SLIPStream

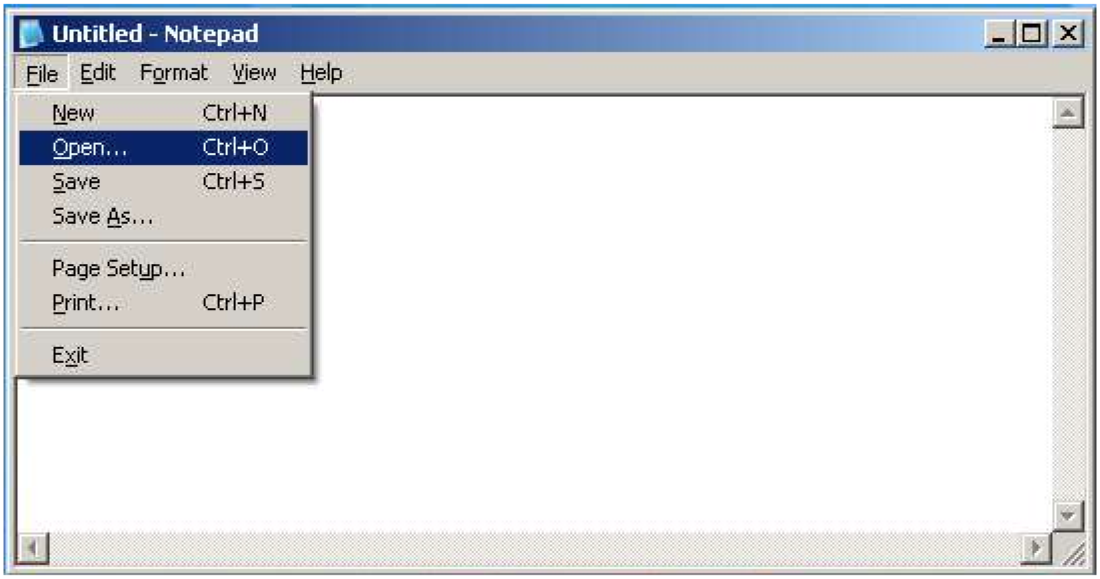
Liked the previous two parts and decided to stop by for a taste of the newest version eh? Well, your in for a treat.

But enough small talk. Its time to get your hands dirty with more hacking tips, tricks, and exploits.

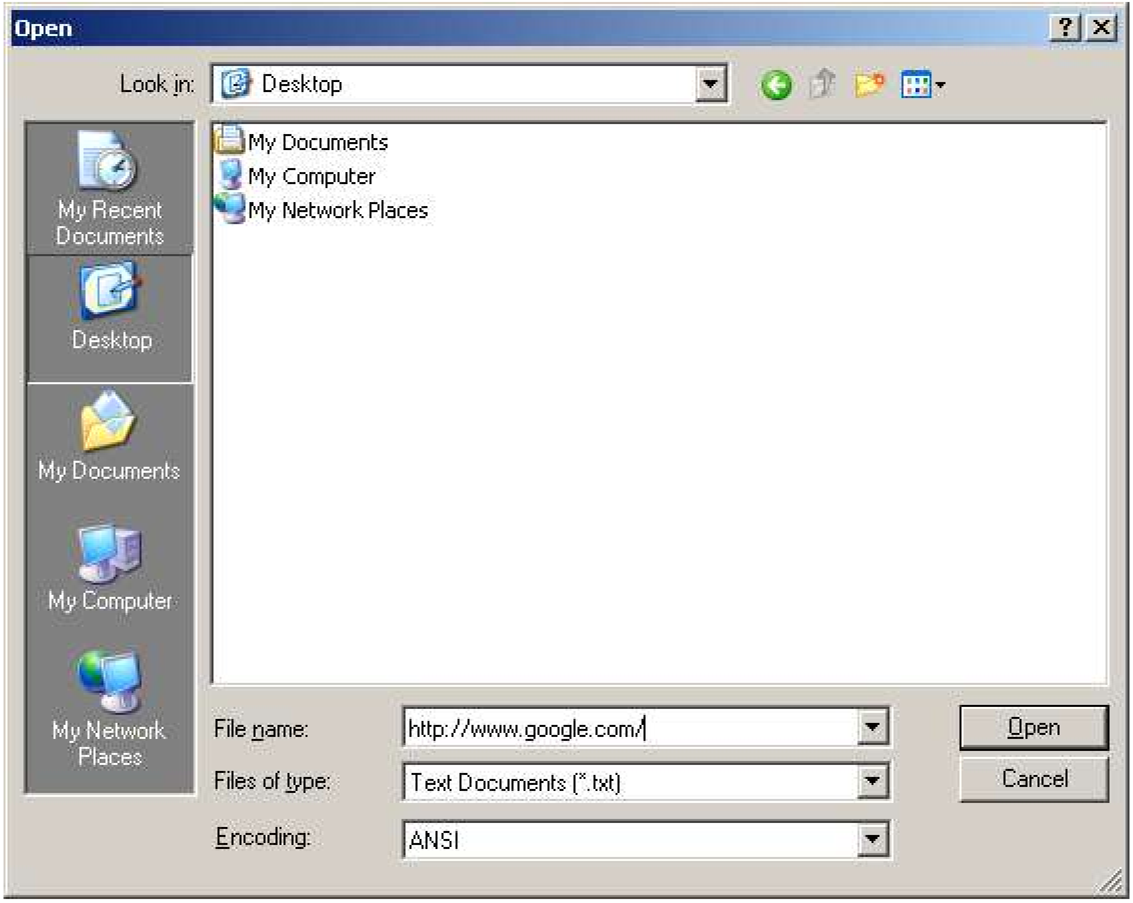
Chapter 1: Web Hacking with Notepad

You probably would have never guessed that notepad is a great hacking tool provided by microsoft. How? What? Let me explain. Notepad comes with the ability to access files on remote computers. This applies to any file storage protocols [ex: http, ftp]. This is done by using the following procedures:

Open up notepad:



Then when the open window comes up, type something like this:



Look in: Desktop

File name: http://www.google.com/

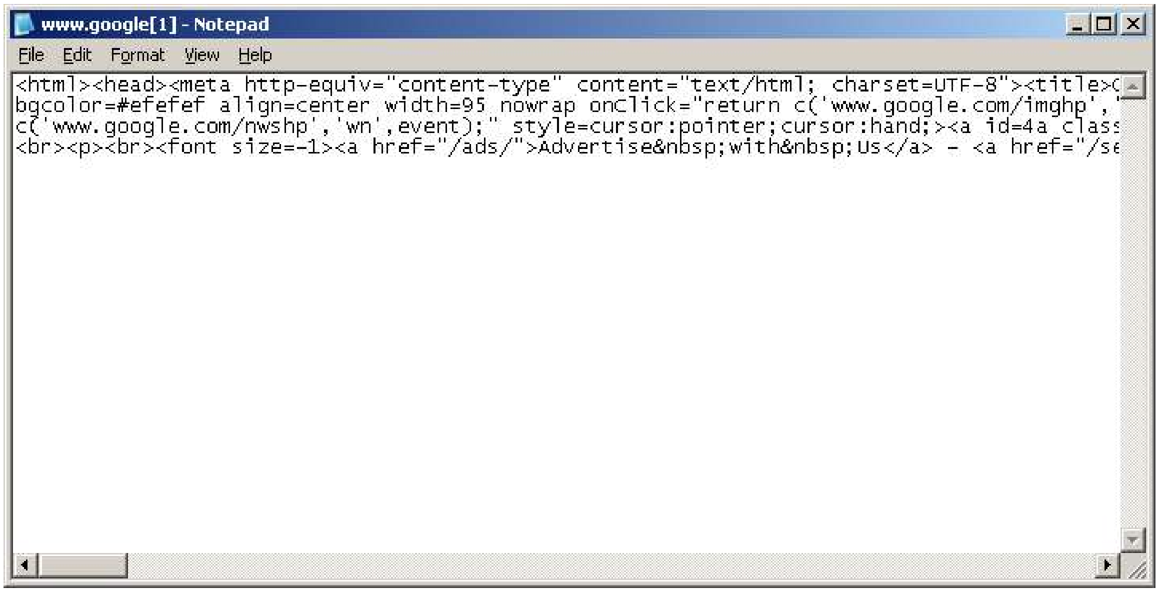
Files of type: Text Documents (*.txt)

Encoding: ANSI

[Note the File Name]

If you did it right you should get something like

this:



```
<html><head><meta http-equiv="content-type" content="text/html; charset=UTF-8"><title>
bgcolor=#efefef align=center width=95 nowrap onClick="return c('www.google.com/imghp','
c('www.google.com/nwshp','wn',event);" style=cursor:pointer;cursor:hand;><a id=4a clas
<br><p><br><font size=-1><a href="/ads/">Advertise&nbsp;with&nbsp;Us</a> - <a href="/se
```

Bang! The source code to google.com's homepage. Not much of an achievement, but it still showes what you can do with notepad. Now applie this same procedure to a cgi script or php script and u can gain access to anything. Heres an example of a portion of a cgi script:

```
if [ [$password eq “smj8xls9”] &&
     [$username eq “root”     ] ]
{
     print “<b>Welcome Root.”;
     fileshow[];
}
```

Wow, youve just gotten access to some pretty important stuff.

Im sure you can use this same method with many other text editors, but notepad is the fastest when it comes to accessing remote files. However, if you have a firewall up it might

take a while and the firewall will ask you if you want to allow the program 'notepad.exe' to access the internet. Just answer yes and it will continue as normal.

FTP Hacking 101

When hacking internet sites and such, hacking ftp services can be VERY useful since the password file is sometimes kept there [normaly under /etc/passwd unless the file is shadowed].

Sometimes, you can use the username 'anonymous' to access an ftp server, and enter an email adress as the password. Then use the 'get' command to download the /etc/passwd file off the server. Of couse, this method can also usualy be used in a web browser, by entering the adress in this format:
ftp://ipadress
Into the adress bar. It will most likely ask you for a password and you can try and break the password manualy. Also, some programs and/or security scanners will automaticly break ftp passwords. There are two that i know of. I believe that Cain and Abel Password Cracker contains a utility for breaking ftp passwords, and if i am not mistaken, Xscan comes equiped with a utility to break ftp passwords.

You can probably run an internet search and find plenty of sites with security utilities what will break ftp passwords for you, however, this process may take some time to perform, especialy on a dialup connection or if the computer is located in a foreign country. But it still beats trying to guess the password manualy.

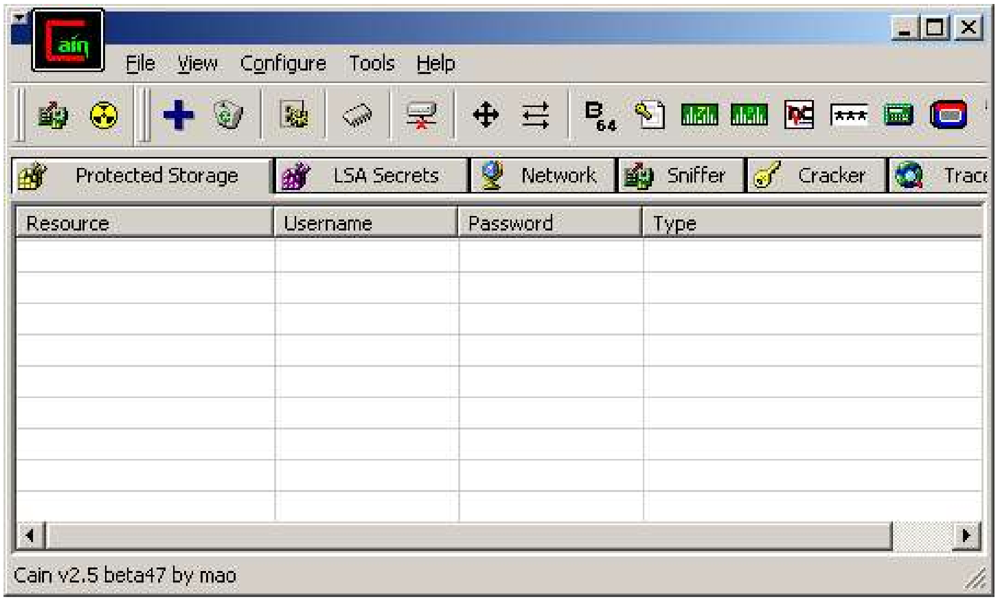
<u>WARNING:</u> Some computer administrators protect their computers by logging the bad attempts to guess passwords so make sure you know what your doing before you use any remote password crackers.

While were on the topic, lets talk about breaking windows passwords.

Hacking Windows Passwords

For this section pretty much all you need is a tool called Cain and Abel password recovery tool. It is available at http://www.oxid.it/cain.html

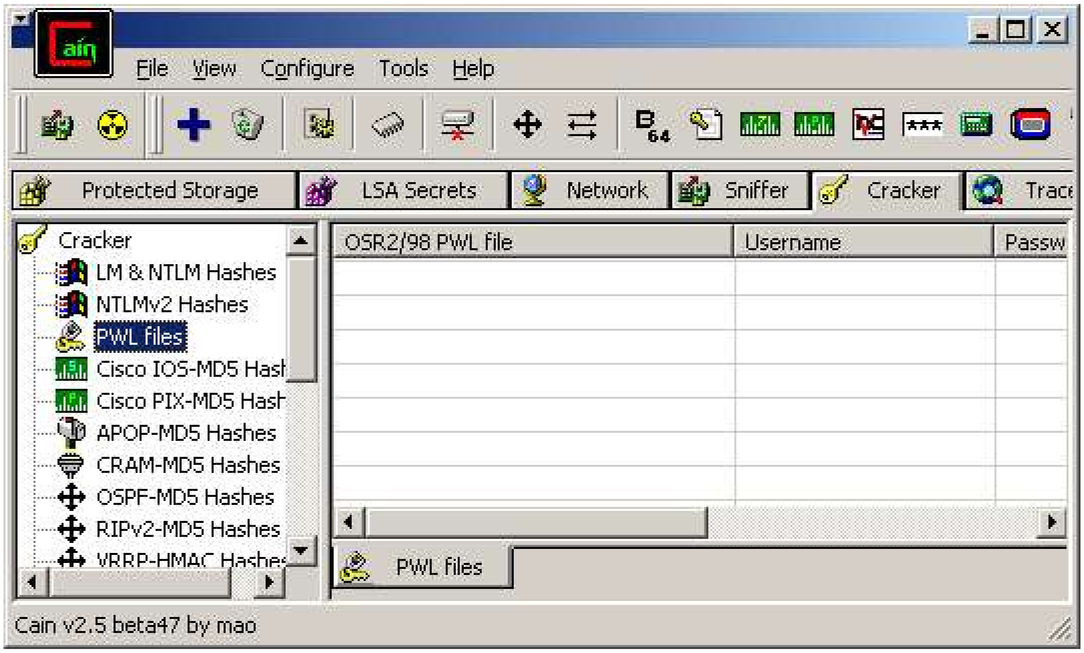
I would definitely recommend this tool. Heres a screenshot:



Resource	Username	Password	Type

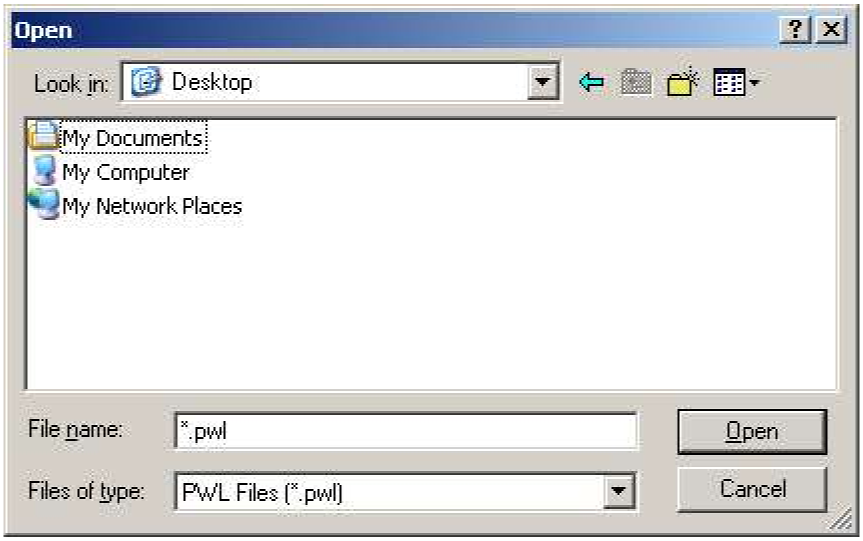
Cain v2.5 beta47 by mao

Ok, in my first text file i included the method to collect .pwl files from a windows 9x computer. This is the tool used to crack it. Open up cain after downloading it and click on the tab labeled 'cracker'.



Cain v2.5 beta47 by mao

And select 'PWL files' as shown above.



Look in: Desktop

File name: *.pwl

Files of type: PWL Files (*.pwl)

Then open up a pwl file you got from a computer.

Then just crack the files! It might take a while depending on your processor speed. On my piece of crap laptop it takes about 45 minutes to crack a password file [it has has an intel pentium I processor and like 64 megs of ram [that does say sixty four, not eighty four] :P] So on a computer with 128 its probably gonna take around 15-20 minutes. My computer's got 360 megs and an amd type processor and it only takes like 10 minutes to crack depending.

TIP: There is a program called FreeRAM. It free's up ram not being used by other programs and speeds up your computer a lot. Also, if your using windows xp, change the style of the desktop to classic windows. The windows xp look takes TONS of ram up.

CRACKING THE SAM FILE!

Unfortunately, Cain and Abel doesnt come with the ability to crack SAM files.
BUT, there is a password recovery tool used to crack them. Its called lopht. No, that isnt 1opht, its an L. I dont have much experience with it, but the times ive used it, it has worked great.

Well, thats all for now.