

AntiOnlinez

Maximum Security for a Connected World

Newsletter #9

INSIGHT

Table of Contents

Editorial
by MsMittensp. 3

Mitigating the Effects of Cyber Crime
by Gunit0072003.....p. 4

Style Sheet How To
by DeadAddict.....p. 8

Me Culpa or Tu Culpa?
by Tony Bradley.....p. 12

Slipsteaming Windows 2000
by Noodle.....p. 16

A little Wine and some Crossing Over
by MsMittens.....p. 21

What are YOUR Insights into Next Year?
by MsMittens.....p.26

MsMittens' Editorial

Well, it has been an interesting summer. Right when we thought it was safe to use our Windows machines a new virus and worm pop up. It's interesting to see that these two items caused so much havoc on the Internet. Did we not go through these exact same kind of issues – especially with the likes of Sobig (which was a variant of an already existing virus) – not too long ago with "I Love You", Melissa and others? Evidentially, the lessons are lost.

While this was happening I got – albeit a bit late – the CSI's Spring 2003 Computer Security Journal. This included the results of the 2003 FBI/CSI Computer Crime and Security Survey. (You can download an electronic version of the survey results at: <http://www.gocsi.com/forms/fbi/pdf.jhtml> . You'll have to fill out a form to get the PDF). The results were certainly interesting:

- Costs of attacks dropped about 50% compared to last year, from \$400M to \$200. This year, however, the highest costs were attributed to theft of proprietary information (\$70M) and DOS attacks (\$65M). While the theft has remained first for many years, this is the first in a long time that DOSes appeared. In addition, the amount represents an increase of 250% over last years DOS costs. Financial fraud, which was 2nd last year at \$116M, dropped significantly to \$10.
- The attack split is still largely from external sources (internet: 78%) while the remaining came from internal sources (30%). Note that some companies evidentially had both internal and external attacks. Most of the attacks came from either "Independent Hackers" (82%) or disgruntled employees (77%).
- Of the 530 companies that responded 99% said they were using anti-virus software and 98% said firewalls (other technologies:IDS – 73%; Physical Security – 91%; Encrypted login – 58%; Encrypted Files – 69%; Access Control – 92%; Biometrics – 11%; honeypots seem to be an unknown tool). Interesting to this is that the #1 attack: virus(82%) and 2nd is insider abuse of net access (80%) .

So where are these firewalls and AV software that are apparently setup? Well, one could look at it and blame an admin since they are supposed to be responsible for this but I wonder if it's more a side issue. Rather that the admins are being so overworked and stretched that they cannot maintain the networks adequately to ensure that the more common method of attacks are dealt with.

cont'd on Page 7

MITIGATING THE EFFECTS OF CYBER CRIME

by Gunit0072003

SYNOPSIS:

There is a lack of involvement within the international community, and among nations as well, that addresses and deals with Internet Security. More and more within each day, our financial, government and civic infrastructures are relying on the power of the Internet making the world community vulnerable to a major disaster waiting to happen.

With the rampant existence of viruses and malicious code infecting tens and hundreds of thousands of users each year, it is only a matter of time before an incident renders a devastating effect on our daily lives. Major institutions, that we rely on from day to day, can easily become disrupted resulting in the loss of millions if not billions of dollars in revenue; and possibly in the loss of lives as well.

Major financial computer systems, hospital databases, fire and EMS dispatch services, and computers managing electrical and water treatment plants are all in one way or another vulnerable to experiencing a systems compromise or a systems halt. With today's information age, these scenarios are easily foreseeable and unfortunately due to lack of awareness and education, we've become complacent and only react to disasters as they occur.

This is why it is important for the international community to come together and establish a governing body that will work to curtail and mitigate the rampant abuses of the Internet.

BACKGROUND:

The Internet as we know it today is vastly growing and has provided us with enormous benefits from digitally tying in our banking and financial systems to our major civic and educational institutions. In addition it has created new businesses benefiting the world economy with E-commerce.

However, the Internet was not designed with the intent that it would one day become available to the public sector, growing at an astonishing rate as it has today and play a major role in our daily lives. If the founders and creators of the Internet could have ever imagined the profound impact the Internet would have on our daily lives, they would have remedied the

security flaws that exist today and would have campaigned for the legislation of new laws on protecting the Internet.

We as nations govern and set forth laws and guidelines to protect our air space, bodies of water and highway systems, but the laws are limited when it comes to protecting one of our most technological advancements and vital communications system, the Internet.

Most developed nations around the world regulate and govern the use of their major roads and highway systems. The laws strictly enforce guidelines and policies with severe penalties. Here in the US, in order to operate a vehicle one must possess a driver license and follow the rules and regulations set forth by the various states. If one abuses that privilege, the individual's driver's license is revoked with additional fines and penalties imposed. In addition, here in the US the FCC (Federal Communications Commission) governs the use of the air space for communications. Laws that govern this sector are far stringer and carry heavier fines and sentences if violated.

However, when it comes to the Internet, "the information superhighway" as we know it, the laws and technology that exists today to detect, prevent or prosecute cyber crime are crude, outdated and are lacking the attention and resources deserved. Anyone, due to lack of legislation that promotes education, awareness and control, can gain access to the Internet without knowing the security implications that are posed to him, herself or to someone else. Anyone with limited knowledge or skill, as we have seen occur around the world, can bring a major system down to a halt and avoid being captured. In addition, to perpetuate the problem even further, when a culprit is identified, little can be done in most cases to prosecute that individual. Many nations do not view cyber crime as a real crime and with some of the nations that do, view it only as a minor offense.

PROPOSAL:

The international community needs to create a security council or body dedicated to maintaining the integrity and security of the Internet.

1. They need to govern the ways Internet Service Providers (ISPs) manage their traffic.
2. They need to define strict mandatory security guidelines ISP customers must adhere to when accessing the Internet.

3. They need to set international laws for extraditing and fairly prosecuting perpetrators accused and or convicted of committing cyber crime.

At a minimum, all Internet edge routers need to be designed to route packets based on the destination and the source address combined. As it currently exists, all packets are routed based on the destination address only. This makes it difficult next to impossible to trace the source of origin to some of the major attacks that occur today. This new proposed routing technology, which is not too difficult to implement, can mitigate certain types of cyber crime that use a popular method to conceal one's identity. This method also referred to as "spoofing a packet" is the ability to masquerade one's source address making it one of the major problems ISPs and government agencies encounter when attempting to trace the source of an attack. Since currently a router will route a packet regardless of the identity of the source, little can be done to prevent and identify certain types of attacks.

However, by monitoring the source address before routing a packet, routers can make more intelligent decisions about the identity of packets and discard and log spoofed packets as they appear. Although, this method may not always identify the exact source of an attack, it can at least identify the region from where an attack was initiated from.

Another important law that needs to be mandated is for every household or organization that desires to access the Internet to go through a basic training and or pre-certification process, which can easily be provided online. In addition, each user should be required to install a protective application that includes but is not limited to an antivirus and a firewall program. Many current users today are unprotected and know little about network security serving as zombies or hosts to potential hackers. By increasing the level of awareness to the average individual and organizations alike, we can significantly reduce the number of compromised hosts.

The last proposal that needs to be enforced is the establishment of international laws to extradite and fairly prosecute individuals who commit cyber crime. Without any means of accountability to someone's ill actions, it will be very difficult to reduce the number of cyber crime that occurs today. We also need to adopt a no tolerance policy where if a nation does not adhere to any of the laws, they simply lose their privileges to reaping the benefits of the Internet.

CONCLUSION:

Unfortunately, we can never prevent every single individual from attempting to compromise a computer system or unleash a malicious virus onto the Internet. There will always be those who will attempt to do so and unfortunately some who even succeed. However, we can tremendously reduce the amount of cyber crime that occurs today by taking preventative measures through advances in technology, education, awareness programs and in the legislation of new laws. This article is by far a complete solution to all the problems we face today with Internet security. Its objective was to merely highlight key points to help us advance in the right direction.

MsMittens Editorial (cont'd)

Perhaps the lesson that should have been learned from the first wave of massive worm/virus attacks (Melissa et al) should have been the need for adequate number of administrators and technical support rather than strictly technical responses to those threats. Technology will only go so far with those kinds of attacks and until appropriate AI is in place that matches that of a normal, functioning, weird human, companies will need more humans to look over logs, IDS, honeypots and such to find the villains. Perhaps companies will realize that security shouldn't be the bandage at the end of the budget but rather an important component of it. Canadian companies, if they are any indication, only spend about 10% of their IT budget on security.

Maybe we shouldn't be so surprised at the attacks and blackouts. This issue is the first under the new name of Insight as suggested by KorpDeath. I enjoyed all the ideas and suggestions for a name for the newsletter but Insight seemed to fit the most. AntiOnline is a unique site, that has a variety of people who bring their own "insight" into security and other computer (and sometimes non-computer or non-technical) to the community at large.

Even this issue which covers things from Cyber Crime to Style Sheets to Windows 2000 to Wine to Who's At Fault for all these Worms. Different insights to different issues. I hope these help you with your insights into the computer and specifically, security, worlds.

Articles for AntiOnline Insight #10 are due: **November 21st, 2003** by midnight EST. Email me at **msmittens@msmittens.com** or pm me with your article.

Enjoy! :)

Style Sheets How To

by DeadAddict

Style sheets allow you to make changes to your web page quickly and easily because it is located in one location As an example you can change all of the H1 headings at one time without having to change every tag that has H1 in it

The important tags that are used when creating a style sheet are
<style>the style tag goes between the <head> and </head> tag.
The left and right curly brace are used to start and stop the characteristics for the tag { } it is just like the / in </bold> it ends the tag

Creating a class will give you more control over the formatting of the content on your web page as a example you can create a class of important paragraphs **P.important** this will display a little bit different than the regular paragraphs <p> the P.important paragraphs will show the formatting you define for the regular paragraphs as well as the formatting you do for the P.important paragraphs

As an example you can make the text and headers appear in a specific font and color

Example H1{color:blue;text-align: center}

To start using a style sheet start out by using the basic html tags

Single web page

```
<html>
<meta name =keywords content="blah blah"></meta>
<head>
<title>What your web page is called</title>
<style>
H1 {text -align: center; font-style: italic}
P{color: red} or the hex number #ff0000
</style>
</head>
<body>
```

Multiple web pages

Setting up a style sheet for multiple web pages allows you to give your web pages a consistent appearance when you make a change to the style sheet all of the pages that use the style sheet will show the changes to make it work for each the pages you have to have the following tag

<link rel=stylesheet type="text/css" Href=?> on each web page that you want to use the style sheet on (change the ? to the location of the style sheet on your computer)

To create a Css document follow these steps

1. Create a new in word processor or a text editor
2. Type a tag you want to define the characteristics for Example
H1{color:blue;text-align: center}
3. Type { to begin the characteristics for the tag
4. Type } to end the tag
5. repeat steps 2- 4 for each tag you want to use in your web page
6. Save the document in text only format use the .css extension to name the document
7. To save the file in word pad click on the floppy disk that is below the words edit and view a dialog box will come up and at the bottom the word Document will be highlighted you can give this file any name you want. once you have picked a name for it add .CSS to the name example mystyle.css and in the "Save as type" box select text document and click on yes when it asks you "You are about to save the document in a text only format witch will remove all formatting. Are you sure you want to do this?" click on yes Before closing the save dialog box look at the top of the dialog box to see where you are saving the file to so you won't have to create another one or do a time consuming search for it.

View your page before putting it on the web

To view your page before putting it on the web for your friends and family to see open up the .css file you created and add the file extension .html to it and click on save. then browse to the files location and double click on it and presto you are viewing your web page now if you want to make any changes just reopen the .css file and make your changes and then save them then refresh the html page if you have not closed it and you will see the changes you have made. Now when you want to upload the page you created make sure you upload the file that has the .html extension or your page will not be displayed correctly.

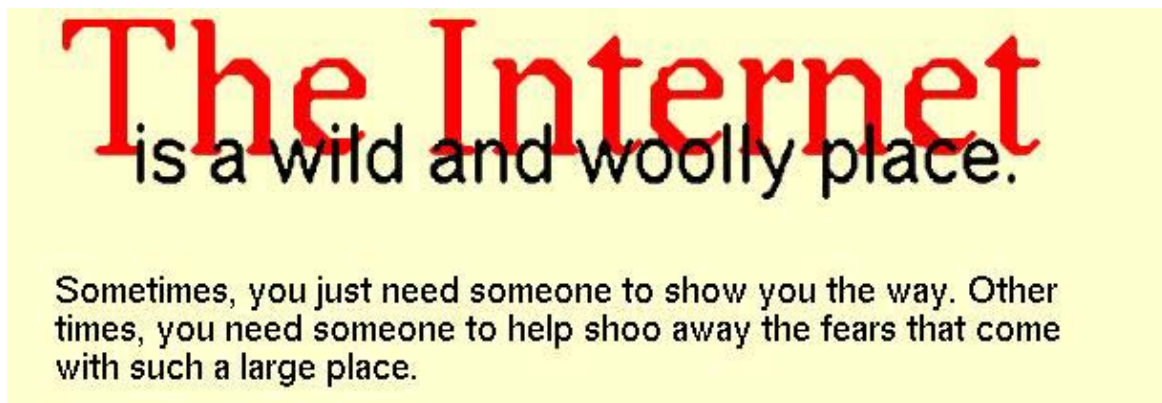
This next section is how to hide your style sheet from older browsers Reason for this is if someone is looking at your web page and they are using a older browser that can't understand Style sheets the browser will just ignore the style sheet

To do this you add this below the <style> tag <! - - and this goes above the </style> tag — >

Example

```
<html>
<head>
<meta name =keywords"content=Yak Yak"></meta>
<title>Blah Blah Blah</title>
<style>
< !- -
H1{ text-align: Center; font-style: Italic}
P{color: Red or the hex number}
— >
</style>
</head>
<body>
<h1> Header blah blah</h1>
```

This is an example of a single page Style sheet that you will see when you are done creating it. MsMittens provided a screenshot of her page for sample use. :D



Special characters

Seeing how I couldn't edit my first html tutorial I will add a small list of special Characters such as ®

To see the full list of them in windows click on start then programs – accessories-system tools then click on character map. And when you find one you like just highlight it and at the bottom right of the character map screen you will see the keystroke number To make them in any document you hold down the alt key and then press the number 0174 and you will get ® These key codes are used in your Html code they are the same numbers in the character map but with out the 0(zero)

Symbol	Keycode	Symbol	Keycode
"	"	<<	«
&	&	>>	»
<	<	1	¹
>	>	2	²
¡	¡	3	³
¢	¢	¼	¼
£	£	½	½
£	¤	¾	¾
¥	¥	æ	æ
§	§	Æ	Æ
!	¦	÷	÷
©	©	é	é

A milestone is coming!! AO Insight #10!!!

We want articles on security tools, “hacking” tools, ideas, rants, raves, reviews, etc.

Send a note to msmittens@msmittens.com with AONewsletter in the subject line or send a private message to my AO account, MsMittens.

Next deadline: November 21, 2003

Mea Culpa or Tu Culpa?

by TonyBradley

Mea culpa is Latin for "my fault". The more contemporary slang translation might be "my bad". The bottom line is that in saying these words you accept personal responsibility for your part in the problem.

What problem you ask? For the purposes of this article the problem is that of not patching known vulnerabilities, propagating worms that could have easily been stopped and otherwise not taking the basic, simple steps necessary to do your part in protecting the Internet community you are sharing with the rest of the world.

The real question though is whose "culpa" is it? The vendor for not creating more secure software in the first place? The ISP's for not blocking and locking down useless ports that can be used to propagate malicious code? Or each individual user for not applying the necessary patches? There certainly seem to be more parties at fault than fingers to point at them with.

In a perfect world operating system and software application developers would write bulletproof code without exploitable vulnerabilities. There would be no need for vulnerability mailing lists like Bugtraq or vulnerability scanners like Eeye Retina. Users and administrators would not have to be constantly watching for the next vulnerability announcement and continuously applying patches just to try and stay half a step ahead of the malicious code writers of the world.

In an almost perfect world vulnerabilities might exist, but would be discovered by whitehat security researchers or the original software developers themselves and patches would be made available that users and administrators could apply at their leisure rather than racing the clock to patch their systems before the malicious code writers can release a worm to exploit the vulnerability.

Unfortunately, this is not a perfect world. The operating systems and software applications are not perfect, vulnerabilities are discovered daily and often the blackhats know about it before the general public. By the time the vendor creates a patch and publicly announces the vulnerability it is a race to get your systems patched before the blackhats can exploit the vulnerability.

On July 24, 2002 Microsoft released Microsoft Security Bulletin MS02-039. It related to three security vulnerabilities in Microsoft SQL Server 2000 – the most serious of which could lead to an attacker gaining complete control of the SQL Server machine. On January 25, 2003- almost exactly 6 months later- the SQL Slammer worm spread around the world in under an hour and crippled the Internet by infecting and propagating to unpatched SQL Server systems. With six

whole months to apply the patch there were still tens of thousands of vulnerable machines ripe for the worm to infect.

On July 16, 2003 Microsoft released Microsoft Security Bulletin MS03-026 which related to a buffer overrun flaw affecting **ALL** versions of Microsoft Windows which could allow an attacker to execute anything they would like on the vulnerable system. Less than a month later- on August 11, 2003- the MSBlast worm hit the Internet and bogged things down as it spread throughout the world infecting unpatched systems.

Infecting an unpatched system was taking on average approximately 30 seconds once the machine was connected to the Internet. On a 56k dial-up connection it would probably take about 5 minutes to download the necessary patch to protect the system. However, applying the patch required certain minimum service pack levels. For instance, the patch for Windows 2000 could only be applied on Windows 2000 Service Pack 2 or higher. Many home users may not have ever applied Service Pack 2 because it is a 100Mb file. Downloading SP2 on a dial-up connection could take more than 4 hours.

Therein lies the problem with expecting the home user market to take responsibility. First, most home users have little to no clue about vulnerabilities or security risks. Many use their computers like they do their toaster or their VCR or any other appliance in their house. But, because the majority of the home user market is still on 56k dial-up connections it is unreasonable to think they can keep current with patching even if they wanted to when some service packs and security updates are as large or larger than the application they are patching.

Generally, corporations are more able to download and apply patches in a timely manner because they have high-speed connections. That same Windows 2000 SP2 that takes almost four and a half hours to download on a 56k dial-up connection takes less than 10 minutes on a T1 line. Combine that with the fact that most corporations have some control over their routers and the knowledge to implement steps to mitigate the risks by blocking the ports used by the worms and it seems that most corporations should be able to protect themselves.

Knowing that their customer base is generally not security savvy and that even if they were their connection to the Internet would be insufficient to allow them to patch their systems, maybe the ISP's should take a more active role in protecting the Internet? Even if only for the self-serving reason of providing service to their paying customers who have taken the necessary precautions to protect themselves, it seems like there are basic steps they could take.

At a corporation you would generally have a firewall protecting the perimeter of your network and block **ALL** unnecessary traffic from entering. This means

locking down all ports and only opening traffic on ports that you must in order to conduct business. Even then it is generally possible to limit the computers that are allowed to talk on that port rather than letting all incoming traffic through.

All of these precautions slow things down though. It takes time for a hardware device or software application to analyze each packet of information to determine the source and destination machines as well as the port being used and compare it against the rules established by you to determine if the packet should be blocked or allowed through. An ISP is trying to provide the maximum bandwidth possible to as many customers as possible. While it may make the network more secure to monitor and filter packets, it would be counter-productive to the ultimate goal of giving people the speed they desire.

Yet, there should be a middle ground. If the argument is that blocking ports or filtering traffic will slow things down and that seems unacceptable, then is it not **more** unacceptable to allow a handful of your customers to propagate malicious code that bogs the network down to the point that it is unusable at all? Perhaps the customers would be willing to exchange a decrease in overall speed if it means not losing the network altogether.

My home ISP- Wide Open West- recently ran into such issues as a result of the MSBlast worm and the MSBlast "anti-worm" (aka "Nachi"). I had taken the time to download and apply all necessary patches and to run updated antivirus software to protect my computers, but that didn't do me much good when the entire Wide Open West network was essentially ground to a halt from the MSBlast traffic.

In fairness to Wide Open West, I wrote to the regional Vice President of Technical Operations on August 18, 2003 and expressed my concerns. I asked them what, if any steps they had proactively taken to protect the network. I let him know that I would be writing this article and gave them a chance to respond. As of yet I have not received any reply.

In my opinion the ISP should start by communicating proactively with the customers. They have all of our email addresses so it shouldn't be that hard to distribute a communication. When a vulnerability of the magnitude exploited by MSBlast is discovered they should issue some sort of bulletin to the entire customer-base explaining the issue. They should outline what steps they are taking and what steps they expect the home users to take. They should include links to the patch or other useful resources and describe other protective measures that users can implement such as blocking ports or updating antivirus software.

In the case of a worm such as SQL Slammer or MSBlast that uses specific ports to propagate, I think that the ISP should be prepared to block those ports if necessary. Perhaps blocking them proactively is a little extreme, but once the

worm hits and it is impacting the network already the loss of performance from filtering the ports would be preferable to the loss of the entire network from the overwhelming amount of traffic.

Lastly, I don't see why ISP's can't implement some sort of honeypot or IDS (Intrusion Detection System) on their network to monitor and log infected systems. Rather than trying to monitor every packet that flows through the network and slow the whole thing down they can strategically place systems throughout the network and let the infected traffic come to them. Once they log the IP addresses of the systems that are propagating the malicious code on their networks they can take steps to disconnect those customers and contact them to let them know they are infected. If they wanted to really provide customer service they could also walk the user through the steps necessary to clean and patch the system so they can safely get back online.

It is truly difficult to point a finger at one entity and determine whose "culpa" the problem really is. The answer seems to be "all of the above". The vendors need to do more to write more secure, less vulnerable products to begin with. The users need to do more to patch and protect their systems to keep from becoming a victim and propagating malicious code on to others. The ISP's need to accept more responsibility for protecting their networks and their customers from the few who do become infected. Maybe if all parties would do just a little more to protect their piece of the problem the whole Internet would benefit and be safer from threats such as SQL Slammer and MSBlast.

So, you wanna be famous?!

Valhallen is creating a who's who of AO and posting it up for downloading. If you want your name featured in it or think someone should be featured in it, send valhallen the following information:

- A picture of yourself
- Short passage (200 words or less) this can be anything you want . You can include description, hobbies, intrests, random rant - anything
- Links to what you think are some of your best posts on Antionline
- Any other sites you visit regularly
- Also if you can a short video of you (no porn pls) avi preferred and it can have full audio if you like.

Zip all this and uploaded to valhallen via PM. Please note that all text should be done in plain text. Picture can be in any format you wish.

If you prefer to tar or rar file feel free just rename extension to .zip so you can upload and remember to state the correct file type in your post. And if you want you can include a .ico design for the final piece - which ever Valhallen likes from those submitted will be used and full credit given in finished file.

Also, if you have any ideas for this project or would like to lend a hand in its development please PM Valhallen.

Slipstreaming Windows 2000 by Noodle

Windows 2000 is a nice operating system developed and released by the Microsoft Corporation. As other Microsoft releases this operating system has service packs to be applied. At the time of writing this document the fourth Service Pack has been released a couple of weeks.

I will try to explain to you how to intergrate the service packs into an installation/bootable cd.

Every once in a while you need or want to reinstall your operating system to start clean again. Reinstalling is a proces where not much fun is to be found. That is why we want to do it with the least amount of administrative efforts.

To intergrate the service pack into the installation you will need the following:

Free hard disk space (take a gig for this).

The original installation CD.

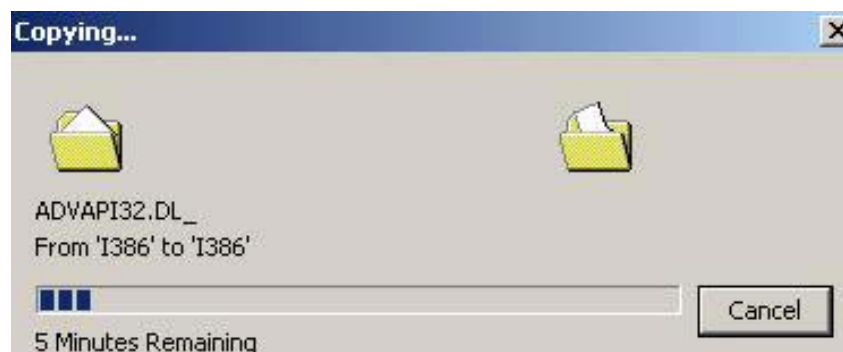
Windows 2000 Service Pack 4 Network Install (about 100 MB).

Third party software called isobuster.

Burning software.

Note that I will be using NERO version 5.0.1.2 and some options may be somewhat different in different versions/products.

The first thing you will need to do is copy the contents of the CD to a folder on your harddisk. For this example I will use k:\W2K\



Whenever you copy files from a cd to the harddrive they will all have the read-only flag set. This needs to be removed. (does it really :: btw ?)

Open a command prompt and change to k:\W2K\. Perform the following command: **'attrib -r /s *.*'** from this directory to remove the read-only flag on all files.

Next I have the service pack in the following directory: **k:\SP4**. Change into this directory and use W2KSP2.exe -x. This is the only switch the SP understands. From Microsoft:

Extract W2ksp2.exe without starting Update.exe You are prompted to provide the directory path to which you want to extract W2ksp2.exe.



I chose to extract the files into the directory k:\SP4\EXTRACT

Wait a while until you are prompted by a box telling you the integration was successful.

Now change into the specified directory and then to the i386\update folder.

In this folder you will find the executable update.exe.

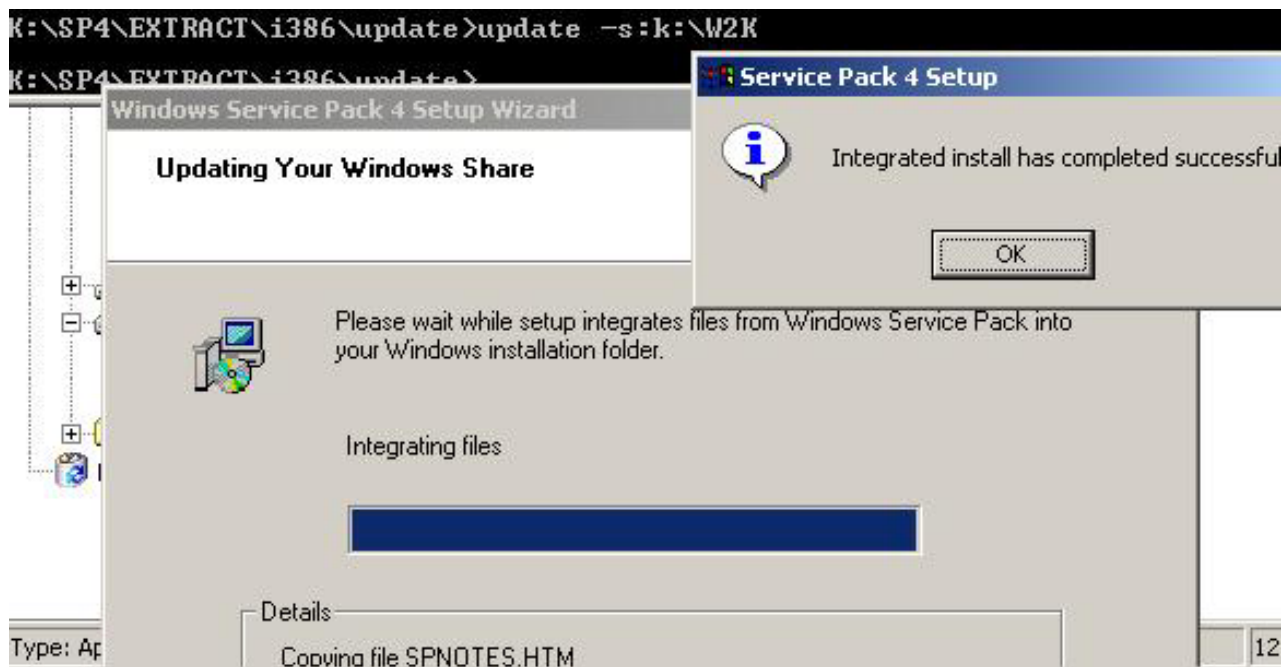
This file can take several parameters but we will only use the -s one.

For a full overview of the options choose 'update /?'

You will have to specify where the installation files are at so for this example the full command would look like:

update -s:k:\W2K

Wait until you see the message that the intergration has completed succesfull.



If you get an error message here my best bet would be that your SP is corrupt.

Redownload. If you are sure the SP is correct and you still get error messages use some googleism.

Where half way there. If you burn the working directory to a cd you will have a installation cd with SP4 intergrated. We want to have a bootable installation cd though so we will need to do some more work.

Install isobuster if you have not done it yet and launch the program with the original cd in the tray. Under 'Bootable CD' you will find a file called 'Microsoft Corporation.img'. Extract this file to the working directory (d:\W2K\).

Now thew tricky part.
Creating the bootrom.

I will use NERO Burning software 5.0.1.2 but you can do it with others.

If the 'create cd' wizzard pops up close that.

Select 'Create CD (boot).

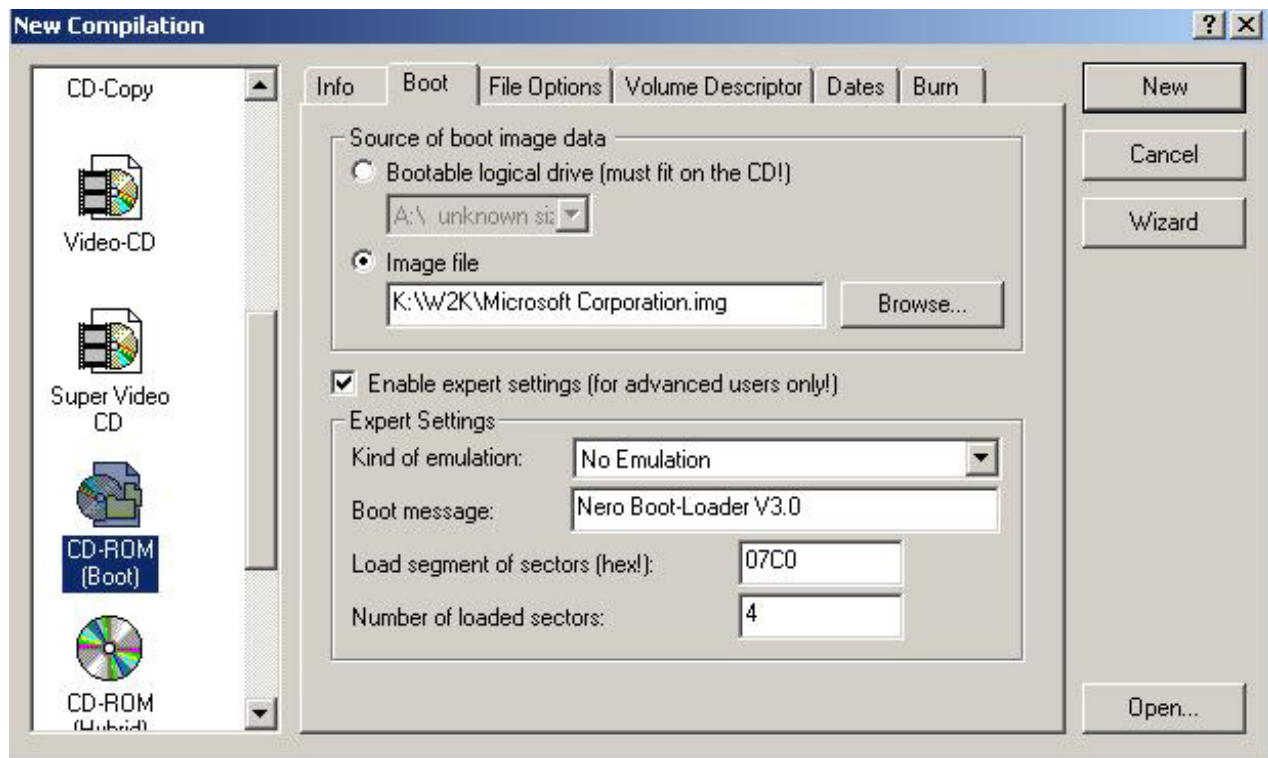
You will get popped into the second tab called 'boot'.

Here select the 'Microsoft Corporation.img' image file.

Set the emulation type to 'No Emulation'.

Make sure the 'Load segment of sectors' is set to '07C0' (hex).

Set the 'Number of loaded sectors' to '4' (default is 1).



In the next tab (ISO for some versions File Options in others) make sure that the following are set:

ISO Level 1(Max of 11=8+3 chars)

Format = Mode 1

Character set is ISO 9660

Joliet check box is selected.

The ISO relaxation checkboxes are checked.(If there are only two checkboxes here you probably have an older version of NERO (like my version).

In this case you will have to edit a registry entry. Go to

HKEY_CURRENT_USER\Software\ahead\Nero - Burning Rom\General and set the 'AddISOFileVersion' to 0 (A REBOOT WILL BE REQUIRED)

On the next tab set the following:

ISO9660

Volume Label: W2KVOL_EN

System Identifier: W2KVOL_EN

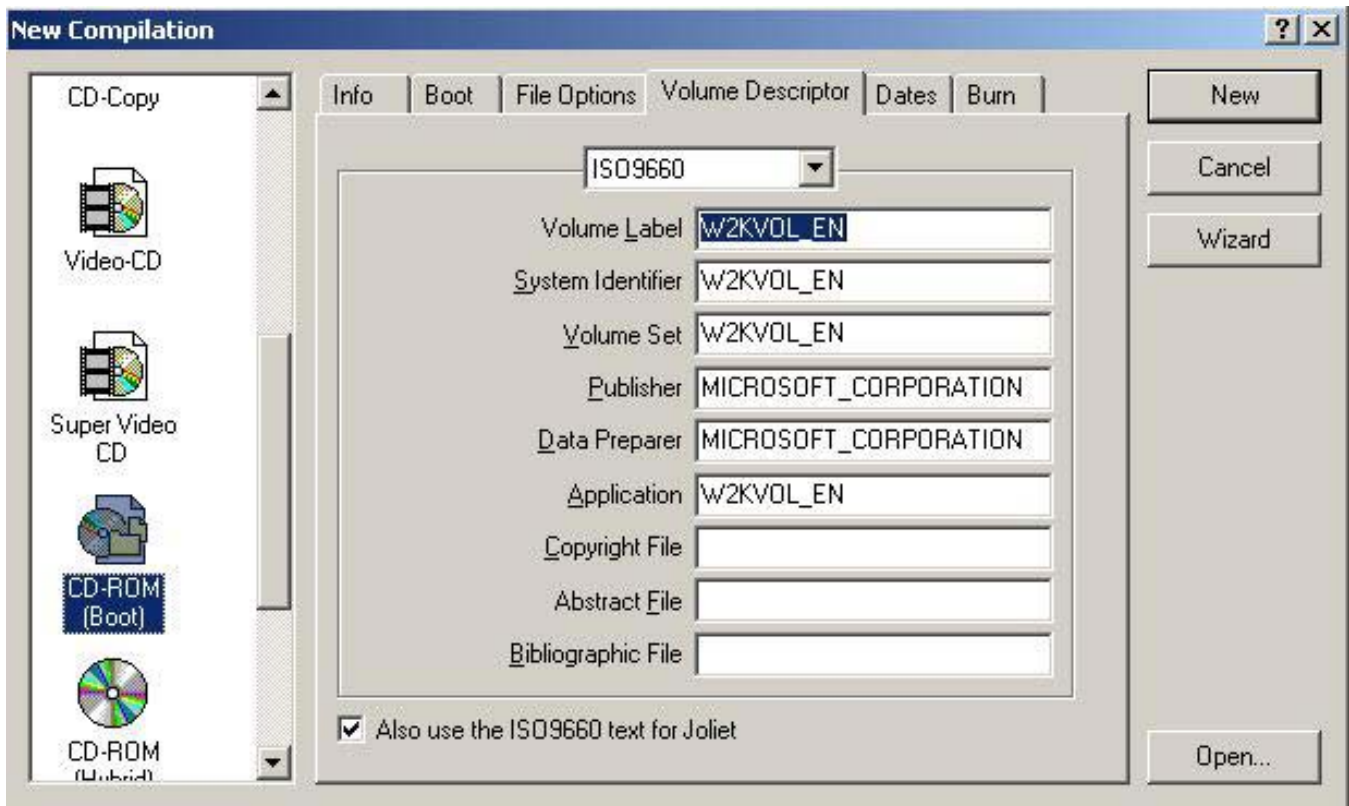
Volume Set: W2KVOL_EN

Publisher: MICROSOFT_CORPORATION

Data Preparer: MICROSOFT_CORPORATION

Application: W2KVOL_EN

Also use the ISO9660 text for Joliet



Set the date to 'use date from original file' (this is the default setting).
We are almost there.

Press the NEW button to get into the file selection screen.

Here check all the files you copied to the harddrive.

(In this example this would be all the files in the k:\W2K folder , you can exclude the 'Microsoft Corporation.img' file).

Press write and wait for your boot cd to be created.

The next step to perform is to create a setup disk that will perform an unattended installation for us (I know this eliminates the need to boot from the CD) but that would be another tutorial, perhaps next time.

Note that there is also space on the CD. This could be usefull for for example the dotnet framework WMP 9 and IE 6.0 or other software.

References:

<http://support.microsoft.com/?kbid=271791>

http://www.winsupersite.com/showcase/sp1_slipstream.asp

<http://www.duspinnst.com/bootcd.htm>

<http://www.ahead.com/>

<http://www.isobuster.com/>

Thanks

A Little Wine and some Crossing Over...

by MsMittens

I've always been one to try things. I'm, in fact, the worst for RTFMing. Give me a program or game (games especially) I'll install it and go and play. I completely ignore the instructions until I have to read something to understand why someone wanted to use Alt+C for copying rather than Ctrl+C. This was how I ended up with Slackware 9. It was my latest project and I had always heard this was the distro of choice of hackers (in the true sense of the word). It is definitely that (although not as much as Slackintosh where you have to install your own X-Windows environment - that will be the next big challenge for my PowerPC box).

The advantage (although some might view it as a disadvantage) is that the box has minimal, stable installs of items. To configure and/or customize you're going to have to do research and understand better how your box works. This was particularly true of my experiments with Wine.

First to explain. One of the things that I hate is the lack of some games in Linux. I'm very impatient at waiting for ports and I want to play CivIII. I thought, why not install wine? In a sense it's a poor man's VMWare by allowing you to run windows programs in your fav linux distro. So off I go to WineHQ to download the latest version to install on my spiffy slack box.

As I begin my install, wine complains that it needs access to my existing windows install if I have one. I figure why not use the existing install as many of the dlls will be in place for wine to grab. I go to mount my windows partition. Hmmm. Right. Regular users cannot mount partitions, only the "big guy" can. So as root I load up the partition.

```
root@MsMittens:~# mount /dev/hda2 /windows
```

I go back to wine and try to install. Wine says that it's not supposed to be installed by root (although later it needs the root password for access to certain areas). Ok. I switch to my regular user and begin the install. And get an error that it cannot access the /windows partition. Weird. I go check the permissions and see:

```
root@MsMittens:~# ls -ld /windows
drwxr-r-  31 root    root          4096 Dec 31  1969 /
windows/
```

Well. That'd explain it. I try as root to open up the perms since my box is just for me but to no avail. This resulted in me doing some research on fstab and the mount command. I had been spoiled by Red Hat, which previously had set the fstab (File System TABLE) to allow for regular user control of windows partitions.

I tried using sudo as an option to have the regular user mount the necessary partition but that still lead me to the same spot: root having control over the partition. So I paid a visit to my favourite search engine: Google. As I read through a variety of "close but no cigar" articles and forum postings around the 'Net, I did realize that the mount command had the ability to designate which user had authority over the partition. Ah-ha!

Exactly what I was looking for. Doing a man mount led me to the correct usage and I ended up with the following command:

```
root@MsMittens:~# mount -t vfat -o
uid=1001,gid=100,umask=000 /dev/hda2 /windows
```

Basically, the command becomes: mount a vfat type of filesystem with the options for a user id of 1001, a group id of 100 and let the default umask permissions fall through. And then use the 2nd partition of the first hard drive and give it a mount point of /windows. I think I might just make an alias of this to remember for future usage.

Well, with that done, I could now continue with the full install of wine. Once installed I opened the default practise app: notepad. Worked like a charm. I tried other apps like solitaire (perfect), Adobe Acrobat (ok), mIRC (unable to connect although the app opened), WinZip (perfect for zip and exes) and ICQ (opened but unable to connect; network issues apparently are still being worked on). I did get Trillian to work but don't try moving the window (you can minimize it however). If you attempt to move it, the app will freeze everything. WineHQ provides a database of applications and their success or failures along with comments by users (<http://appdb.codeweavers.com/>)

Wine overall, I thought, was quite nifty. For some apps, like ICQ and MSN Messenger, to even to get them to run (nevermind network connectivity) you would have to point to necessary dlls. For example:

```
wine -dll shell,shell32,comdlg32,comctl32=n Icq.exe
wine -dll shell,shell32,comdlg32,comctl32=n msnmsgr.exe
```

Basically, I am telling wine which dlls are required and whether to run the

ddl(s) in native or builtin mode. The last place is the location of the file. Sometimes you can try:

```
wine -dll shell,shell32,comdlg32 "C:\Program  
Files\ICQ\ICQ.exe"
```

As you can see, it gives the "location" of the file in the "false" windows environment.

One of my biggest challenges in Windows 98 (my default trashy windows install) was the instability of Pagemaker, the app I use to create the newsletter. Without fail, every newsletter would require about 5-8 reboots of 98 and continually drove me up the wall. I tried it with wine but it crashed a couple of times. Ah well, I thought... or did I need to give up? Back to trusty ol' Google.

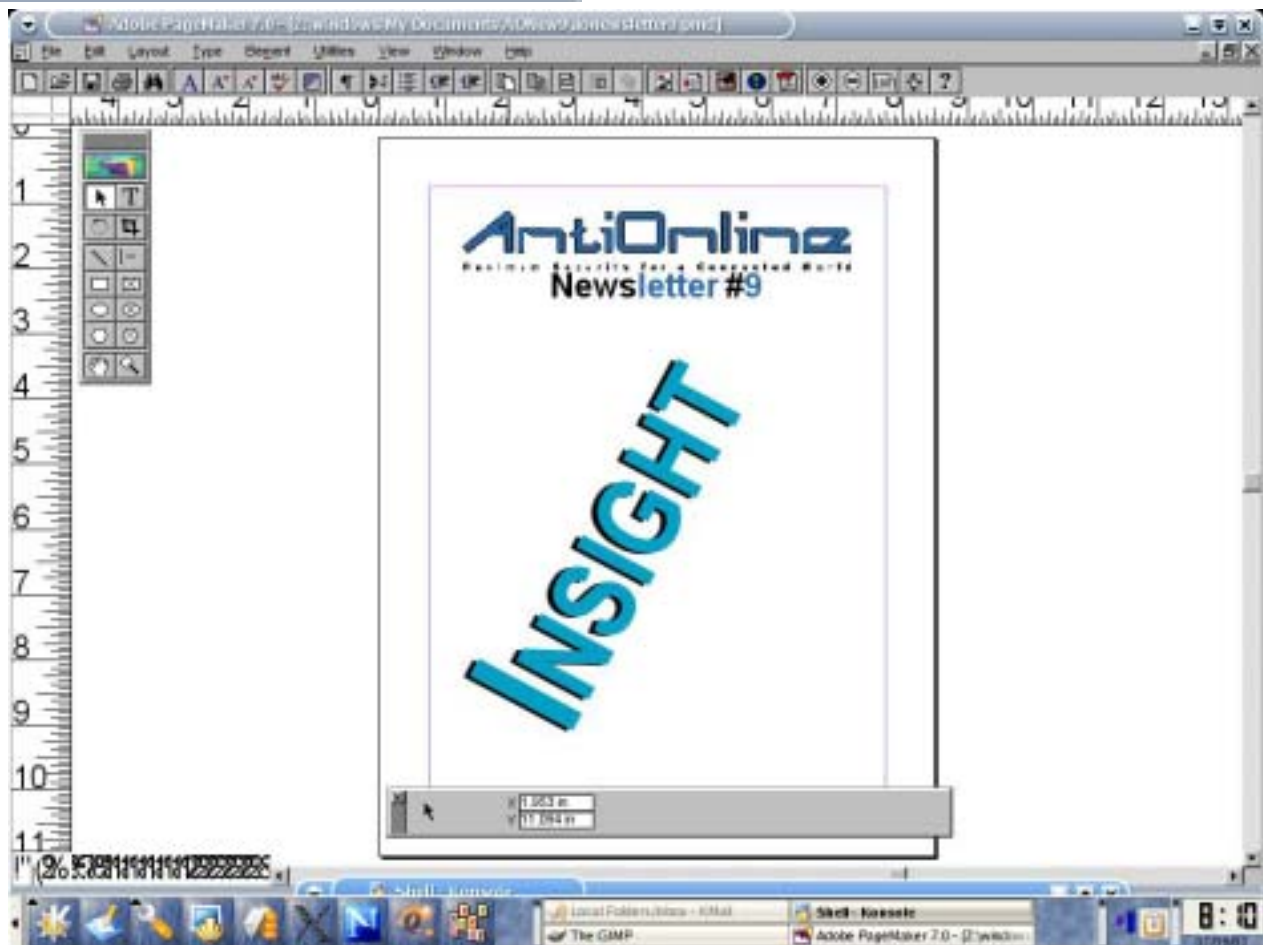
As I was looking for help on getting certain apps running, I came across something called Cross Over Office by CodeWeavers. This was an add-on (or ontop of) kind of app over Wine. Originally designed for Microsoft Office, it claims (quite successfully) at being able to run apps without crashing and with ease. Ease, they weren't kidding!

While not free (\$70USD), it's not that expensive and certainly is far cheaper than VMWare. It is also far more stable than wine by itself and installing software is easy enough. In fact, when you do install, it's much like being in the Windows environment and yet more stabler.

In addition to the main Cross Over Office app, you can also install/buy the eplugin option. I found this useful to download QuickTime and Windows Media Player. I'm still trying to figure out how to use them adequately but I did get to view some QuickTime trailers (Texas Chainsaw Massacre) so I consider it a success (albeit I had to copy the link to the trailer from the source of the trailer page at Apple's site).

The program is not perfect however. Attempts to install full Adobe Acrobat Reader (which includes the Distiller Program) and Eeye's Retina did fail, so there still is room for improvement. But what I've been able to run thus far, I consider it a success. The less I need to use Windows, the happier I am. Below you will find screenshots of the program and of Pagemaker "running" on Slack.

Well worth the investment IMHO.



References:

- RTFM: <http://www.altgeek.org/methuselah/rtfm/>
- Slackware: <http://www.slackware.com/>
- Slackintosh: <http://slackintosh.exploits.org/>
- Wine: <http://www.winehq.com/>
- Cross Over Office: <http://www.codeweavers.com/products/office>

What's your Insight into Next Year? by MsMittens

In a few days, America will remember September 11th. The security "pundits" have been saying that there are plans of an attack by Al-Quaeda using planes coming from Canada. They have also espoused that there will probably be an online attack. How true these potentials are is unknown but I have this for everyone:

What do you think next year will hold for security? The CSI/FBI survey certainly did a big change and seems to reflect more of a response to "script kiddie" activity rather than against the kind of "hackers" that were seen in the late 70s/80s/early 90s. Will admins get slacker in their security because they think they are only against "script kiddies"? Will we see more repeats of worm/virus combinations propogating around as a result of old holes that have patches? New methods of dealing with patches?

The next issue will be the 10th issue and will be a milestone for AntiOnline. I invite all members to send me a brief (but somewhat realistic response — "Macs will die!"/"Unix/Linux will die!"/"Microsoft will die!" have been happening for years and is not * THAT* interesting.) paragraph on what you think the future of security holds for all of us in 2004. Where will the attacks come from; where will security turn to for the next latest greatest thing; what will continue to work; what will continue to fail.

I look forward to seeing your "insights" into 2004! :)

You can either pm me or email me at msmittens@msmittens.com