WordPress Security: Checking for backdoors

This website and 8 other websites on the server were going off line from time to time. Upon investigation I found all the PHP files of the WordPress installation were deleted! At first I thought a hacker deleted the files. I re-installed the WordPress installation, the theme and all the plugins (a whole day's work for 9 websites!) but a few weeks later the sites went down again. All the PHP files were again deleted.

I wrote the server company (Avahost) and told them of the problem. They informed me that its was *their* anti-virus software that deleted the files because all PHP files were infected with malicious code!

I didn't believe ALL the files could have been infected and so I bought new hosting with Bluehost and transferred 4 of the websites to it. Lo and behold after a week or so the websites on Bluehost (including this one) started to have trouble. The security plugin Wordfence reported the WordPress installation, theme and plugins were all infected with malicious code! But in this case, there was no antivirus software on the server to delete them. Avahost was telling me the truth!

I did a Google search to learn more about WordPress security. At last I found the culprit! A hacker installed a backdoor in the database. In the list of users I found a user with no name or email but with administrator privileges!! See the image below:

What you see just above the red line should *NOT BE* in ANY WordPress list of Users! A valid user has a name, a username and an email address, but this one does not. If you are a WordPress administrator, my suggestion is for you to check out your list of users and see if anything like the above is in that list. If it is, just delete it. I chose delete the user with all content.

How the NSA has hacked YOUR PC

In spite of the fact there are a lot of tips on the Internet about how to protect your PC privacy and security, after you watch this terrific presentation from tech researcher and journalist Jacob Appelbaum, you might want to change your policy to either not care who knows anything about what you do, or not touching a PC, cell phone, or *ANY kind of electronic means of communication* again! Don't even use the postal system. Just stick to passing paper and ink messages only to trusted friends and family.

At December's Chaos Computer Congress in Hamburg, Mr. Appelbaum presented the latest documented revelations about how deep the NSA spying rabbit hole really goes. How do you know that the NSA has not hacked the BIOS of your motherboard? Or hacked the firmware of your hard-disk? You don't. There is no way you can even find out.

How to secure Grub 2 in Fedora Linux

This is an technical article that only Linux users would understand and appreciate.

I like to secure the Grub boot loader to make it harder for anybody but me to get root access to my PC by either a cold startup, or rebooting the system. Grub version 1 had a password option. It was easily implemented by editing the grub.conf configuration file and adding the password option data. But in Fedora 16, Grub version 2 has replaced Grub 1, and Grub 2 doesn't seem to have a password option. At least I haven't figured it out yet. Moreover, Grub 2 makes it even more apparent how to get root access because it gives a system recovery option for each kernel version!

I learned by chance that changing the default Grub time out to 0 in Grub 2 prevents the Grub startup screen from showing even when purposely trying to show it by hitting the ESC key! Grub 1 did show the Grub options screen when hitting ESC just before booting the kernel even though its time out was set to 0, but Grub 2 does not show the Grub options when its time out is set to 0 no matter how many times I hit the ESC key, and even after repeated attempts!

> Disclaimer: Do this at your own risk! Fedora does not recommend it because you have no option to use the previous kernel if a kernel update fails! However you can still use the recovery option from the installation DVD – if you know what you're doing.

To change the default time out in Grub 2, from Terminal log in as a super user with the su command, and with your favorite editor load the /etc/default/grub file. I used Leafpad:

```
# leafpad /etc/default/grub
```

The first line has: GRUB_TIMEOUT=10
I changed the 10 to zero: GRUB_TIMEOUT=0

Next save the file, exit the editor and run the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Next time you boot your PC, you should not see the Grub screen again. Though you don't have recovery options from the startup screen anymore, you can still use your Fedora installation disk for system recovery if you need to.

PC security issues

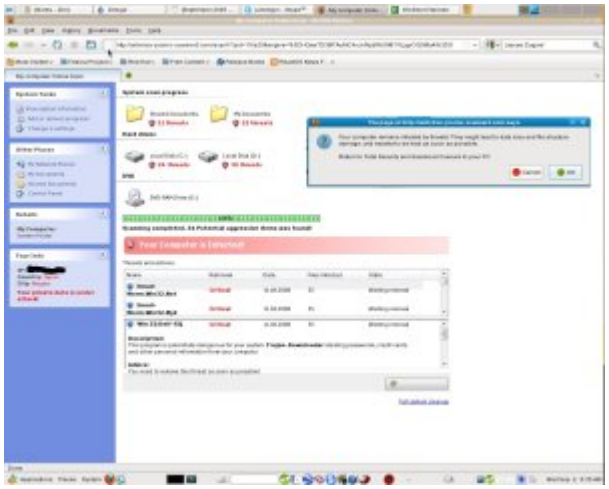
I noticed the performance of a certain Windows XP PC was down again, even though I cleaned it from malware only a few months ago. I installed and ran Super Anti Spyware and it found over **1500 security issues**!! The browser was hijacked and a **fake anti-virus** program called Antivirus 2008 was installed. SuperAntiSpyware cleaned it up and its running fine again.

The particular user of that machine is a young adult who uses a peer to peer file sharing application known as Bearshare. I'm sure she affected her PC again as a result of poor Internet browsing habits. I certainly do not recommend file sharing networks and software such as Bearshare but recommend Bittorrent instead for downloading large files. My favorite Bittorrent client is Deluge. It's better security, and especially so in Linux, Mac, or a Windows PC when the user is logged in with limited privileges, and not as the Administrator.

Did you know that the German government has warned web users to find an alternative browser to Internet Explorer to protect security? I highly recommend Firefox. It's much better security, open source, and heavily supported by software developers from around the world, and not just by a single cooperation like Microsoft whose bottom line is always money. I believe they have often put the priority on user convenience, and to do that, they sacrificed the user's security. Not requiring the user to always log in

with limited access (as in Mac / Unix / Linux) is one example of this.

Beware of False Virus Popup Reports from Internet Pages



I clicked on a link to access a certain article when all of a sudden a window popped up saying that my hard disk was undergoing an online scan for viruses and trojans. It reported that my private data is under attack and my PC is infected with security threats. I was advised to download and install “Total Security” to remove the threats.

Notice the interface of the PC screen in the image is that of Microsoft Windows? I’m *not* running Windows on my PC! I’m running Fedora **Linux** with the Gnome desktop environment.

The scan reported C drive and D drive infected, but Linux has *no concept of drive letters* as in Windows. My Linux system *doesn’t have* a C drive or D drive. Neither do I have any folders named “My Documents” and “Shared Documents.” This proves without a doubt that such unsolicited online PC scans that report problems are really **scams** to try to rip us off!

The best way to safeguard your PC from bugs and viruses

The best thing any Windows user can do to protect their PC from the getting infected from the Internet is to create a second user account with administrator privileges and to change the working user account to one with only limited user access. I promise you if you do so, your chances of picking up some web-bug, or virus are probably 99% less no matter how good your anti-virus program is. This is because a virus or malware cannot modify your Windows registry, nor can it copy itself into your Windows system folders if you work as a user with *limited* privileges. A simple reboot will kill any virus that may invade into the PCs memory.

The purpose of the Administrator account should be only to install software or to do certain tasks like changing the time or date, or to de-fragment the hard disk. It should never be used to browse the Internet! Probably more than 90% of all Windows users (especially Windows XP users) browse the Internet with Administrator privileges. It’s no wonder their PCs get infected, perform slower and slooooower, and sometimes come to a grinding halt!