August 2003 Volume 19 Number 8

PPCUG NEWS

A PUBLICATION OF THE PRINCETON PC USERS GROUP

Monday, August 11, 2003

How Websites Work

Jeff Gould,
Princeton Online

A lot happens when you say you want to go to the Princeton Online website. How the request is translated into information on your screen is complex, and putting all the pieces together to make the request work involves several settings on several computers around the world. We will talk about: Domain names, Network Solutions, IP addresses, Webservers, DNS servers, E-mail, Web pages. The discussion will inevitably lead to talk about search engines and directories.

At:
Lawrence Library
Meeting Rooms 1 & 2
US Alternate Route 1 South & Darrah Lane, Lawrenceville, NJ

Meetings of an organization at any of the facilities of the Mercer County Library System in no way imply endorsement of its programs.

In this issue

About PPCUG 2
President's Message 2
To Linux or Not.....2
Security Testing Online 4
Did Microsoft send it?.....5
Coming Events.....6

PPCUG Web Site News:

Look for the email address directory online instead of here in the newsletter.

When made available by the presenter, a file with links mentioned in a program will be added online. Check for a link to "Links" in the meeting schedule.

The PPCUG bylaws are available - see the About Us page.

Suggestions to improve our site are welcome.

About PPCUG

General Meetings

Second Monday of the month at the Lawrenceville Library, Alternate Route 1 and Darrah Lane.
7:00 PM: Social Time / Tech Corner
7:45 PM: Meeting Comes to Order
8:00 PM: Featured Presentation

For information about upcoming meetings or joining PPCUG, see our web site:

http://www.ppcug-nj.org

Board Meetings

For meeting location and time, call 609-883-5262. Board meetings are open to all members.

Board Members

President:	
Clarke Walker	609-883-5262
Vice-President:	
Tom Carman	732-828-6055
Secretary:	
Don Arrowsmith	609-883-9874
Treasurer:	
Paul Kurivchack	908-218-0778
Members-At-Large:	
Al Axelrod	609-737-2827
Vic Laurie	609-924-1220
Kim Goldenberg	609-631-9140
Sol Libes	609-520-9024

Chairpersons

Hospitality:	
Bill Hawryluk	609-655-0923
Member Records:	
Paul Kurivchack	908-218-0778
Newsletter Editor:	
Don Arrowsmith	609-883-9874
Program Coordinator:	
Sol Libes	609-520-9024
Web Master:	
Don Arrowsmith	609-883-9874

Annual Dues

Dues are $30 per calendar year. New members pay $2.50 per month times the number of months remaining in the current year.

President's Message
Clarke Walker

Since I missed last month's deadline for the newsletter, let me do some catching up.

At the June meeting, Vic Laurie did a great job introducing us to batch and script files. Thanks again Vic!

For the July meeting Don Slepian showed us a DVD that he created using his computer. Don then stepped us though the process of creating a video for DVD playback and offer us valuable tips.

Sadly Jim Russ who spoke to us about Lindrows at the May meeting passed away on July 4th. We were all impressed by Jim's technical knowledge and more so by his warmth. You can read about Jim at www.hunterdoncomputerclub.org/JimRuss-Obit.htm

During June I have been struggling to restore my computer's system disk. My computer reported a "no partition table" when I booted it one rainy night. I started by looking at software that would recover damaged disks using the catalog on http://downloads-zdnet.com.com. (Yes there are two ".com" in the address.) The three products I have been trying are:

Recover My Files (www.recovermyfiles.com)
Stellar Phoenix FAT (www.stellarinfo.com)
VirtualLab Data Recovery (www.binarybiz.com)

I settled on using Stellar Phoenix FAT but would like to hear other member experiences recovering damaged disks. I plan to provide more details of this adventure in a forthcoming article.

At our August 11th meeting we will have Jeff Gould of Princeton Online speak to us about what goes on inside the web. Sure to be an interesting topic.

Enjoy the mid-summer!

To Linux or not to Linux...

Nancy J. Cristolear
The Dayton Microcomputer Association, Inc.
njc@dmapub.dma.org

On July 13 the Linux SIG of The Dayton Microcomputer Assn. Inc. will be having another installfest. I've participated in quite a few and have seen many people leave either happy or disappointed. I thought by writing this article I could help you make your experience a positive one.

Should you or shouldn't you take the plunge? Well that depends on several things. We'll take a few minutes to go over some of the things you should consider.

First, what are your expectations? Are you a person who has been working with a Windows or a Macintosh and expect Linux to be the same thing? I can guarantee you will be disappointed.

Unlike Windows or Macintosh, the Linux distributions are not as refined. What do I mean? Well, if you are familiar with Windows, then you are also probably familiar with applications like WordPad, NotePad, Calculator, Paint to name a few. Many of the Linux applications have names like GIMP, an acronym that stands for Graphics Image Manipulation Program. It would not jump out at you that this is a Photoshop clone would it? So, you will have to invest time into exploring the applications to see

what they do. The good news is there will be LOTS of them. Ultimately, you may have to tweak the menu system so that you can find what you want.

OK, the next thing we will consider is your skill level. If you are the kind of user that expects to be able to buy something off the shelf and have it work, then Linux is not for you. Linux often requires a number of tweaks to make it work properly. However, if you are the kind of user that would throw the manual away, click a link to see what it would do, or take your box apart to see what is in there, then Linux might just be for you.

It will help if you are comfortable working with a DOS prompt. Most of the things Linux can do are more easily done from a prompt. In fact, most of the people I know have XWindows installed just to get a terminal window. [Editor: XWindow is a windowing system developed at MIT, which runs under UNIX and all major operating systems. It lets users run applications on other computers in the network and view the output on their own screen. XWindow generates a rudimentary window that can be enhanced with GUIs-Graphical User Interfaces.]

Then there are the Unix commands. They are the kind of commands that only a geek would love. Consider some of the names: grep, ls, mv, cp, ps, vi.

Lastly, what is your goal for your Linux system? Do you want to replace your Windows system? Or perhaps you just want to play around a bit. This last is where we lose the folks who are more Windows oriented. If you do not have a commitment to Linux, you won't be inclined to wade through the setup and will just forget about it.

Are you ready to take the plunge? OK then, there are still a few things to consider. Do you buy one of the packaged distributions or do you take advantage of the free software available at the installfest. What kind of machine will you be using and what do you want it to do? How old is that machine? Do you have enough hardware? Memory? Processor?

Linux is famous for being "free", however, you may want to invest in one of the packaged distributions. They run around $75. What is the difference? Well, often the commercial distributions will include tools and software that is not available for free. For instance, you might get StarOffice with all its templates and art as opposed to OpenOffice. It may come with special tools that will help with the installation and upgrade. Most important, the boxed distributions come with HELP! This help is in the form of a manual and on call technical support. This may be worth the money right here.
That doesn't mean you can't make things work with the available distributions at the installfest. They often come with a large amount of Open Source software. If you are willing to regularly attend SIG meetings, you can learn all you may need to know (or at least where to find it). In the long run though, you would probably be more motivated to work with something that you have money invested in. Either way, bring your software or not, it can all be installed at the installfest.

Next we will consider some of the choices you may want to make about what to install Linux on. Linux was originally written to run on a 386 machine with 4 Meg of memory and you can still run it on that kind of machine, in theory. However, just like Windows, as ability has been added, so has the level of machine that Linux runs best on. Most of the package distributions require at least a Pentium level machine with 64 Meg of memory. If you want to be able to install and run with a minimum of tweaking, you should have standard hardware, known components, and as much memory as you can afford (Linux is a memory hog). You can get by with about 6Gig of disk space for everything that comes with your distribution.

Next, will you run Linux on a standalone machine or will it share a system with Windows. The ideal system will run Linux and only Linux. However, many cannot afford a whole system for Linux so they share the machine with Windows. OK, do you use removable hard disks and swap them (ideal), or must you have both Windows and Linux on the same hard disk? Windows just does not do well with other operating systems on the same machine. That doesn't mean you can't do it, it just means you may have to work harder. If your skill level is lower, you will probably do better at installing Linux on a standalone or swappable disk. If you must install everything on one disk, do your Windows install first, then install Linux. Linux comes with a couple of tools to manage and partition drives or you may want to invest in programs like System Commander or Partition Magic. People at the installfest can help you to get your system set up with either. OH, if this is your regular production machine, BACK UP YOUR EXISTING DATA! Some people have tried to install Linux and ended up wiping out the entire disk. BACK UP EVERYTHING!!!!!!!!

What? You thought you could just use your 386 with a 40 Meg hard drive and 4 Megs of RAM that's sitting in the bottom of your closet? Well, don't throw it away. You can install a bare bones Linux OS with no bells and whistles. What you can't do is install XWindows and pretty graphics. You can still do a lot with it. Consider using it as a print server, mail server, or a firewall. (A 486 might be a better choice though.)

You just bought the latest and greatest thing? Well, it may be a good idea to wait a couple of months. Linux developers have to wait for hardware to be released for drivers to be written for it. So you may find that Linux is a little behind the state of the art.

Want to make sure you can install Linux on your machine? Or maybe you are just not sure you want to take the plunge completely yet. Consider getting a KNOPPIX CD. KNOPPIX is a single CD distribution that runs on the CD drive

and doesn't touch your hard drive. If your hardware is all detected by KNOPPIX, then you can be confident that the Linux installs will find your hardware. You will also know if you have the patience to deal with some of Linux's idiosyncrasies. You can download KNOPPIX at http://www.knopper.net/knoppix/index-en.html. Choose the Order/Download link. Download sites are at the bottom of the page.

Even if you're just curious, consider coming out to the installfest. It will be at the Russ Engineering Center at Wright State University, July 13, 2003 from 12-6. There will be plenty to do. Presentations will be given and members will have their systems set up. You will definitely get something out of it.

There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author. This article is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member.

Security Testing Online - Fraud or Not?

Greg West
Editor of SCUG REPORT
Sarnia Computer User's Group (SCUG), Sarnia, Ontario, Canada
gjwest@sympatico.ca

Recently, while researching material I came across an article which discussed "Spring Cleanup" and computer maintenance. The first suggestion was to run your computer through an online test to see whether your system is secure or insecure. The current warnings of updating patches, Spam attacks, and overall computer safety, prompted me to say, "why not" as I clicked into "NanoProbe Technology Internet Security Testing for Windows Users" that uses a program called: Shields UP!! (http://grc.com). Suspecting a scam of some sort I figured I would attempt to trick this program. I would run the test twice, once with my firewall turned off and another test with it operating.

My curiosity peaked immediately after my first click when I received a message that I "was about to view pages over a secure connection", a more than familiar message indeed. So I continued on, yet still mostly skeptical that there was some sort of come-on to reach out and take my money. No sooner than I clicked the "ok" button, did I receive this strange message:

" Greetings Gregory! Without your knowledge or explicit permission, the Windows networking technology which connects your computer to the Internet may be offering some or all of your computer's data to the entire world at this very moment!
(For example . . . that's how I know your name!)"

Next I was given a choice of testing my "Shields" or "Ports"…I clicked on "Shields" became even more skeptical when I received this message:

"Preliminary Internet connection established! Your computer has accepted an anonymous connection from another machine it knows nothing about! (That's not good.) This ShieldsUP! web server has been permitted to connect to your computer's highly insecure NetBIOS File and Printer Sharing port (139). Subsequent tests conducted on this page, and elsewhere on this website, will probe more deeply to determine the extent of this system's vulnerability. But regardless of what more is determined, the presence and availability of some form of Internet Server HAS BEEN CONFIRMED within this machine . . . and it is accepting anonymous connections!"

The message continued to give the full details of its findings, or non-findings:

"The rest of this website explains the implications and dangers of your present configuration and provides complete and thorough instruction for increasing the security of this system. At the moment, any passing high speed Internet scanner will quickly spot this computer as a target for attack. The phrase you must remember is: "My port 139 is wide OPEN!" Unable to connect with NetBIOS to your computer. The attempt to connect to your computer with NetBIOS protocol over the Internet (NetBIOS over TCP/IP) FAILED. But, as you can see below, significant personal information is still leaking out of your system and is readily available to curious intruders. Since you do not appear to be sharing files or printers over the TCP/IP protocol, this system is relatively secure. It is exposing its NetBIOS names (see below) over the Internet, but it is refusing to allow connections, so it is unlikely that anyone could gain casual entry into your system due to its connection to the Internet. Several of your private names are being served up to the Internet by the Windows networking system. (see below) While it's unlikely that this information can be exploited, you should know what anyone can learn about you and your system."

But the kicker was that my User Name, my Computer's Name, and my Workgroup was identified on screen…I knew I had to go to the next level and test my Ports. Here are the results of the Port testing:

It declared that my Port 80 (http) was open and that "having port 80 "open" as it is here causes intruders to wonder how much information you might be willing to give away."

The test program also found my Port 139 (Net BIOS) was open and I received this warning:

"As you probably know by now, the NetBIOS File Sharing port is the single largest security hole for networked Windows machines. The payoff from finding open Windows shares is so big that many scanners have been written just to find open ports like this one. Closing it should be a priority

for you!"

Well, I must admit I was becoming a tad worried, but still I was skeptical towards the reality of these results. Next I wanted to run these test using my Zone Alarm Firewall operating. Here are the results of testing both my shields and ports:

On the Shield's test I got the same first "GREETINGS" message, only this time it did not contain my name. The results were amazingly secure. The Shield's UP test could not find my Port 139, nor was it able to connect with my NetBIOS to my computer. Here are the results of the Shield's test:

"Your Internet port 139 does not appear to exist! One or more ports on this system are operating in FULL STEALTH MODE! Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND (that's very cool!) which represents advanced computer and port stealthing capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attack and intrusion. Unable to connect with NetBIOS to your computer. All attempts to get any information from your computer have FAILED. (This is very uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be VERY SECURE since it is NOT exposing ANY of its internal NetBIOS networking protocol over the Internet."

My firewall came through with shining colors and with full security. Next was the Port test with the firewall operating. This test reported my Port 80 was open (http), however this is my connection to the net and my firewall blocks the incoming attacks as they are produced…giving me the choice whether to accept or reject, but nothing comes through without my acceptance. So this warning is ok. The next warning I received was again concerning Port 139, this time I got the same message that it could not get through to this port and furthermore, "There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!"

Not a fraud, only success! My confidence in firewalls stands firm, sound and free of worry.

There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author. This article is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member.

Did Microsoft send it?

Siles Bazerman
siles.bazerman@gte.net
APCUG Representative
Orange County IBM PC Users' Group, CA
orcopug.org

Return-Path:
<1.spar.metzger@wanadoo.fr>Received: from mel-rto6.wanadoo.fr ([193.25.19.25]) by orval.sprint.ca (InterMail vM.5.01.02.00 201-253-122-103-101-20001108) with ESMTPid
<200300225200401.DVU126901.orval.sprint.ca@mel-rt06.wanadoo.fr>for<xxxxxxxxxx@sprint.ca>; Tue, 25 Feb 2003 15:04:01 -0500Received: from mel-rta10.wanadoo.fr (193.252.19.193) bymel-rto6.wanadoo.fr (6.7.015)id 3E0C343F02651838; Tue, 25 Feb 2003 20:59:47 +0100Received: from JJE1GO (81.50.38.12) by mel-rta10.wanadoo.fr (6.7.015)id 3E26DAA6016CCA66; Tue, 25 Feb 2003 20:59:46 +0100Date: Tue, 25 Feb 2003 20:59:46 +0100 (added by **postmaster@wanadoo.fr>** Message-ID: **<3E26DAA6016CAA66@mel-rta10.wanadoo.fr>** (Added by **postmaster@wanadoo.fr**) FROM: "Microsoft Corporation Internet Security Division" **<zgyegdwd201593@AvVyZc.com>** TO: "MS Customer <SUBJECT: Newest Internet Security Update> Mime-Version: 1.0 Content-Type: multipart/mixed; boundary="cGwarduOGAAVvQYBK"

From: Microsoft Corporation Internet Security Division
To: MS Customer
Sent: Tuesday, February 25, 2003 2:59 PM
Subject: Newest Internet Security Update

MS Customer this is the latest version of security update, the "February 2003 Cumulative Patch" update which eliminates all known security vulnerability affecting Internet Explorer, Outlook and Outlook Express as well as five newly discovered vulnerabilities. Install now to protect your computer from these vulnerabilities, the most serious of which could allow an attacker to run executable on your system. This update includes the functionality of all previously released patches. System requirements Win 9x/Me/2000/NT/XP. This update applies to Microsoft Internet Explorer, version 4.01 and later.

Recommendation: Customers should install the patch at the earliest opportunity.How to install Run attached file. Click Yes on displayed dialog box.

How to use: You don't' need to do anything after installing this item. Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact us. Please do not reply to this message. It was sent from an unmonitored email address and we are unable to respond to any replies. Thank you for using Microsoft products. Best wishes from Microsoft Corporation Internet Security Division

_____

herein may be the trademarks of their respective owners.

Is this a legitimate message or a hoax or worse? I am sure some of you have received the above message and attached file. It has been circulating the internet for over a month.

The message is a hoax, and the attachment is a worm/virus that is particularly virulent. It not only replicates itself but starts deleting files on your hard drive. Let us look at the message and see how we can tell it is a hoax.

1. Microsoft NEVER-NEVER-NEVER sends out messages with patches or attachments, especially unsolicited ones. At the most, Microsoft will refer you to a secure site where the patch can be downloaded. (Did I say NEVER?)

2. This is a rather good copy of the format used by Microsoft, but look at the first line. There is no capital letter to start the sentence. Also there are a number of grammatical errors as well as format errors.

3. The message is not sent through a Microsoft site, but from a *melrto6.wanadoo.fr* (a French site with no Microsoft connection).

4. Microsoft does not have the named division, although it does have units that deal with security, internet or otherwise.

If you receive this or any other similar message, do not immediately install or run the executable file. Check it out. There are numerous sites devoted to security as well as many usenet groups which report on these matters. Your first line of defense is to contact your User Group officers and ask them. They will know or will have access to resources to verify or debunk the claims. Remember to practice "Safe Hex."

Coming Events:

September 8, 2003 - Genealogy - Blanche Sneath

October 20, 2003 - Pocket PC (Third Monday!)

November 10, 2003 - Recycling Inkjet Cartridges

December 8, 2003 - Annual Meeting and Party

Princeton PC Users Group
PO Box 291
Rocky Hill, NJ 08553