MUUGLines

The Manitoba UNIX User Group Newsletter

September 2008 Volume 21 No. 01

Next Meeting: September 9th, 2008

Advanced Usage of *Open*SSH

Presented by Sean Cody.

This month, Sean Cody will speak on SSH (Secure Shell). SSH provides a secure communication path to a remote machine, and is a replacement for protocols such as telnet and rlogin which send passwords in plain text over a network.

In many ways SSH has become the ubiquitous tool for using remote shells. It is that, and a *lot* more. Over the years SSH (specifically *Open*SSH) has blossomed into a networking and security Swiss army knife. When used properly, SSH is a powerful tool which can solve some surprisingly difficult problems in very simple and elegant ways. You can also use it to get some peace of mind when working in hostile, administratively constrained or seemingly closed networks.

This presentation will show you a few tips, tricks and secure practices of some lesser known *Open*SSH features, and will introduce you to defenses against a few of the more clever uses of *Open*SSH.

Where to find the Meeting

Meetings are held at 7:30pm at the IBM offices, at 400 Ellice Ave. (between Edmonton and Kennedy).

For more information, please check the MUUG web site (**www.muug.mb.ca/meetings/**).

Upcoming Meetings:

October 14th, 2008: What's new in OpenSUSE 11

John Lange will demo the recently released **OpenSUSE 11** running the **Gnome** desktop, highlighting the major changes from the OpenSUSE 10.X series and focusing on its rich desktop features, especially things that go "whizz-bang!" such as the 3D Desktop Effects.

MUUG Board Elections - Call for Nominations

Every October the Manitoba Unix User Group holds its Annual Meeting, the main goals of which are to elect a new Board of Directors and to pass any special resolutions. (Aside from that, it is a regular meeting)

Any MUUG member in good standing can be nominated to run for a position on the Board.

As of this writing, the following members of the current Board have let their names stand for re-election:

Gilbert Detillieux
Systems Analyst - University of Manitoba

Michael Doob
Professor - University of Manitoba

Kevin McGregor
Network Analyst - City of Winnipeg

Montana Quiring
Systems Administrator - University of Manitoba

Doug Shewfelt
Systems Specialist - City of Winnipeg

Adam Thompson
Consultant - athompso.net

Of course, this list is just a starting point. Any member in good standing of the group can be nominated simply by getting the support of one other member. If you feel you would like to contribute to the group by running for a board position, please don't hesitate to do so. (In fact, we'd like to see the number of board members increase.)

If you want to be nominated, or to nominate someone else, send a letter to the group's postal box or deliver it in person to a current board member. The letter must contain the name, title, and employer of the nominee, along with a short (100 word or so) biography, and must contain the signatures of the nominee and one other member. The letter must be received no later than September 30, 2008, which is 14 days prior to the October 14 meeting.

Although the by-laws require that the nominations be done in writing, with signatures, you can speed up the process by sending e-mail to **election@muug.mb.ca**, with the above information, and sending the signed paper copy later. In this case, please include the e-mail address of both the nominee and the supporter on the CC: list of the message, so that all parties concerned have a record of the communication.

Nominees should familiarize themselves with the MUUG bylaws, found here:

http://www.muug.mb.ca/pub/bylaws/

If you have any questions about the election or the nomination process, please contact Gilbert Detillieux, either by phone (474-8161) during business hours, or by e-mail to **election@muug.mb.ca** anytime.

Gilbert Detillieux
Election Committee Chair

Summer News Roundup

Fixing DNS

Earlier this year, Dan Kaminsky found a vulnerability in the Domain Name System, which could enable an attacker to insert incorrect information into a server's DNS cache. This means that traffic that should be sent to one web site would be sent to a different site that could impersonate the real site.

Kaminsky quietly worked with several vendors to develop patches for DNS software. On July 8th, he held a press conference where he announced that a problem exists, but that patches to DNS were available for immediate installation. In order to give administrators time to install these patches, he asked that people respect a 30-day period of silence where people wouldn't disclose the details of the bug, or speculate on the details of the bug. Unfortunately, people did start speculating, so administrators only had about two weeks before the details were publicly known, instead of the month that Kaminsky had requested.

When a computer wants to contact a particular server, it asks a name server for the address associated with that server's hostname. If the name server doesn't know the answer, it passes the question up to another name server (which in turn might query another name server). When the original name server gets an answer giving the hostname's address, it will add that information to its cache, and use the cached information for some time.

A name server may have several outstanding requests, so it assigns a query ID number to each request. When it receives a DNS response, it matches the query ID to its list of outstanding queries. If there is no corresponding outstanding request, it ignores the response. This means that when a server sends out a DNS query, an attacker may be able to slip in a false

response before the authentic reply arrives. In this case, the original name server will accept the false information, and ignore the true information.

To poison a name server's cache, the attacker would first request a host's address from a name server, which could trigger the victim name server to query another name server. The attacker would then flood the victim name server with false responses, hoping to get the victim name server to accept one of these responses.

The attacker would have to guess the query ID to success. Kaminsky showed that it would be relatively easy for the attacker to do this. The query ID is only 16 bits long; as well the pseudo-random number generator used by some versions of the DNS software produces predictable sequences.

Most of the DNS software used the same source port for outbound queries. These were patched to use a wider range of randomly assigned source ports. This meant that the attacker would have to guess both the port number and the query ID, which is much more difficult. Also, a name server could be modified to accept DNS responses only from trusted machines, and allow only trusted machines to request hostname addresses.

For more details, you can read "An Illustrated Guide to the Kaminsky DNS Vulnerability" at **http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html**.

Kaminsky has a small application that will test if your name server is patched. Go to his web site at **http://www.doxpara.com/**, and click on the "Check My DNS" button. This web site also has an embedded video of a world map showing the spread of the patch over time.

You can view his Powerpoint presentation at **http://www.doxpara.com/DMK_BO2K8.ppt**, which talks about the DNS vulnerability, and then goes on to discuss more general security issues, including problems with how people use SSL.

Fixing Old Bugs

An OpenBSD developer Otto Moerbeek has produced a new version of malloc, a memory allocation function. One of his testers reported that when the tester compiled a large C++ program, the compiler would fail with an "Internal Compiler Error" message when the tester used Moerbeeks new malloc. However, the compiler would work properly when it used the standard malloc function.

Moerbeek traced the problem to a buffer overflow bug in yacc. The bug apparently has been in BSD distributions since the earliest versions of the software. In fact, Moerbeek was able to find a variant of this bug in AT&T's Sixth Edition UNIX, which was released in 1975.

Fixing Old Systems

California's fiscal year starts in July, but by August the state still hadn't passed its budget. To help conserve the state's cash reserves, Governor Arnold Schwarzenegger signed an executive order recommending that the state reduce the salaries of all 200,000 state employees to minimum wage until the state passes the budget.

The problem is that California runs an aging COBOL-based payroll system and has to manage a large number of job classifications and bargaining units. Schwarzenegger wants the pay cut to be implemented within the next month; the state controller estimates that it will take six months to implement the change, and nine or ten months to process back pay for the employees when the budget is finally passed.

California is having trouble finding programmers who know COBOL and who can maintain these old systems. The state often ends up hiring retired programmers on a part-time basis. However, the same executive order that called for the pay cut also terminated 10,000 temporary and part-time employees. The semi-retired returnees were one of the groups targeted for layoffs.

Fixin' to Challenge Google

At the end of July, Cuil lauched as a new search engine. Some of the core people at the new company were search engine specialists at Google.

Cuil claims that its biggest advantage is that it can index web pages faster and cheaper than Google can. Cuil index pages based primarily on the content of the pages; in contrast, Google ranks web pages by the popularity of a web page. One result of this approach is that, compared to Google, Cuil presents more obscure web sites. Several testers noted that, for example, Google often has a Wikipedia entry at the top of its search results, while Cuil rarely displays Wikipedia entries.

Also, Cuil currently doesn't keep an archive of the search history of users, which is important to users concerned about their online privacy.

Cuil has displayed many of the growing pains of a new company. When it was launched, it lagged under a large user load. Also, the results of searches tended to change dramatically from day to day, as the company worked on improving the search engine.

Cuil is found at **http://www.cuil.com/**

Virtual Machines

Sun has released version 1.6.4 of VirtualBox., a virtual machine systems that run on a host operating system. Sun provides the source under the GNU General Public License.

One design feature of Virtual Box is that Sun has separated the graphical user interface from the virtual machines. Each virtual machine runs as a background service and is only loosely connected to the user interface. This can help you manage a large collection of virtual machines from a single user interface.

Sun provides free downloads from their web site. Pre-compiled binaries are available for Solaris, Windows, MacOS, and various distributions of Linux.

Also, VMWare has offered free downloads of their ESXi Hypervisor. You are required to register to obtain a free license. Their ESXi product doesn't run on a host operating system; instead, it runs on the bare hardware, and guest operating systems connect to the hypervisor. This tends to provide better performance than a virtual machine supervisor that runs on a host operating system.

Red Hat Servers Compromised

Red Hat detected an intruder on its servers in mid August. They feel that the problem was contained, but noted that the intruder was able to sign a small number of *Open*SSH packages for some distributions of Red Hat Enterprise Linux.

Django Update

At our last meeting, Bill Reid spoke on Django, a Python web framework. The developers distributed Django Version 1.0 Release Candidate 1 in late August, and are planning on rolling out the Version 1.0 final release at the beginning of September.

Microsoft Sponsors Apache

Microsoft has become a platinum sponsor of the Apache Software Foundation, promising to contribute $100,000 per year to the project. Pundits are debating whether Microsoft is trying to support open source projects, or subvert them.

Just What I Always Wanted

TimmyMe is a new free application for the Apple iPhone 3G, which determines your location and then lists the closest Tim Horton outlets.

Share Your Thoughts

E-mail us with your comments on the newsletter, and continue to send in articles or ideas for the same. Specifically, what sort of material you would rather see: Announcements, technical articles, new products, or…? Send it to **editor@muug.mb.ca**.