# Firewall Guru
# BOB ZEIGLER

**When we're looking at security it would be remiss not to mention Bob Zeigler and the impact he's had on the field of Linux firewalls. Richard Ibbotson caught up with him in the US**

Bob is one of those rare individuals whose personality, humanity and depth of character are hidden to the casual observer. To get the best out of him you have to get to know him reasonably well or at the very least you have to talk to him for a few days. His understanding of the human condition is probably quite unique. Without him the world would have been a much sadder place. I talked to him at his home in Cambridge, Massachusetts and at Ryles jazz club at Hampshire street, a place that was once inhabited by the world's most amazing academics. The club and the musicians are still there but the people are very different.

We live in times when the sharing of knowledge is officially frowned upon. Bob was originally from the state of Wisconsin, which is known for its beautiful scenery and laidback attitude to most things. He lived at Madison with his parents before going to college at the University of Wisconsin-Madison to take an undergraduate degree in psychology in the 1970s. He says that there is a very large cross over in psychology and computing at the college that he went to. After that he went back for a degree in counselling. His interest in computers began to take shape when he got his first machine from Radio Shack (in more recent times known as Tandy). He says that he didn't know what assembly language was, so he began to take an interest in it and also in BASIC. He taught himself a lot about it and really liked it. His hobby really began to get a grip on him.

Bob's line of study made him think that he was going to be a corrections professional for the rest of his life – possibly a person who looks after serious criminals. He said he liked the prisoners and didn't like the guards. He found himself working for the State of Wisconsin and most of the time he performed a role as a statistician. Testing of prisoners was computerised – something that needed a large budget. His colleagues at that time told him that he "had to do a Masters degree in computing science". He objected and said that he couldn't do the maths but they finally got him there. He found himself working with highly academic people and discovered COBOL whilst still studying. If it hadn't been for this strange mix of circumstances Bob would never have become involved in Unix and his interest in GNU/Linux and network security would not have become what they are today.

Copyright
Bob Keene 1999

## The lure of Unix

Bob has worked as a Unix operating systems developer since his days of academia. He was working with a team of people on a mini supercomputer where he had to write just about every line of code. He developed a multi-processor version of BSD 4.3 as a spin-off from the original uniprocessor project. Since then he has worked as a Unix system kernel developer in the Boston area. Then later on things began to fall off and he wasn't doing very much. Eight companies have died under him in ten years whilst he was an employee.

Whilst he was working for Hewlett-Packard he began to take an interest at home in firewalls and network security. The people he was working with told him that he should develop this further as his


## Author

Richard Ibbotson is the Chairman and organiser for Sheffield Linux User's Group. You can view its Web site at *http://www.sheflug.co.uk*.

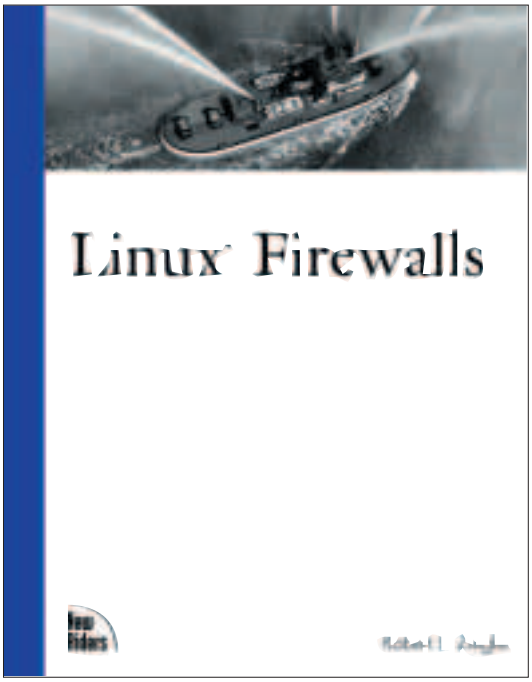
proper line of work. He began to develop his Linux firewalls site. He was also working on Tiger and Tripwire at the same time. It all came to a head when a publisher approached him and asked him to write a book about ipchains. The first edition of book about Linux Firewalls was first published back in November 1999. In between the first and and second editions he worked for Nokia as their principal engineer, designing and developing firewall products for Nokia's Ipsilon family. At that time it was explained to him that he should write his second book whilst at his place of work.

His claim is that he thinks that his first book, which gave a more than adequate description of ipchains, was probably lacking in something somewhere. When iptables came along he thought that it was about time that he corrected any mistakes that he might have made with his first book. He thought that some help from someone else would probably be a good thing. He asked Carl Constantine to be his contributing author. Carl has worked in the IT business for many years. He was been a technical writer, a programmer and a consultant. He works at the Department of Computer Science at the University of Victoria at British Columbia in Canada. The technical reviewers are Joshua Jensen, who was the first Red Hat instructor and examiner, and John Millican, who has been providing information consulting services since 1978. John is currently certified by SANS GIAC for intrusion detection in depth and firewalls VPNs and perimeter protection and related security issues. He is the chairman of the SANS Unix security certification board. With this impressive line of highly qualified and experienced people Bob set to and wrote his second book.

## A second coming

Linux Firewalls second edition was published in November 2001. It's all about iptables and is extremely comprehensive owing to the nature of the people who helped to write it. It was pressure from this book and some of the people mentioned above that brought an update in the iptables application with a view to fixing a few bugs. It covers, in 13 chapters and four appendices, the kind of things that most small SOHO LANs might need. What it doesn't cover the security policies and procedures that large businesses need. However, if you are someone who is involved in administering a large business or Government network then you might just find that this is a good book to read for some introductory ideas.

There is also a Web site that Bob has put together for reference and for creating firewall rules for your network. You might want to have a look at that. The reader is given some basic concepts about network security such as packet-filtering firewalls and then he or she is carefully taken through some simple and




more advanced concepts.

Bob describes his local area in Massachusetts as "greed central". To the casual observer it is a beautiful part of America to go to. Boston, which is on the other side of the river, has some great attractions. Cambridge itself is home to both the Massachusetts Institute of Technology and Harvard. On the day that I was there the Patriots parade took place and the New England Patriots soccer team won for the first time in years. MIT was its usual busy self, bustling with activity and expectation of the new semester. It was good to be the most popular Englishman in America for just a few hours.

To finish off I might mention the dedication which never got published in the second edition but it was published in the errata... "In constant memory of Jake". Jake used to be Bob's pet cat. He loved Jake as much as he loved his wife. Jonas is now his friend and life companion. Long live Jonas.

We hope you will be with us next month when Bob Zeigler starts his Linux firewalls tutorial series.

## Info

Buy a Linux Firewalls book: *http://www.newriders.com/books/title.cfm?isbn=0735710996*
Bob's site: *http://www.linux-firewall-tools.com*
University of Wisconsin-Madison: *http://www.wisc.edu*
Errata: *http://www.linux-firewall-tools.com/linux/book/errata.html#top*
Design your own GNU/Linux firewall: *http://www.linux-firewall-tools.com/linux/firewall/index.html*
Jazz: *http://www.rylesjazz.com/index.shtml*

**which gave a more than adequate description of ipchains**