Dark Art Defenses

Dear Linux Magazine Reader,

About half past five one morning I was heading for a train when I moved a mouse attached to one of my home machines.

The screen blank program stopped and to my shock revealed the cursor moving on its own, opening up various file managers. I was suffering a hack. I hit the reset button.

Although time was ticking and I was in danger of missing the train, I waited for the system to reboot. When it did the cursor was back with a life of its own. With no time to explore I removed the network lead and power down.

Once I caught my breath on the train I started to think about the potential damage. A home system is not too important. Personal files can usually be regenerated. My worries eventually rested on possible credit card loss and all my passwords. A few phone calls later and all my credit cards were cancelled. While drinking British Rail tea I was left with the loss of my passwords.

All my work passwords are memorized and never written down, but for some reason I could not remember if I had ever jotted down my home machine's details. In truth it did not matter as I could not trust the system and when reinstalling I always change the settings. The train eventually arrived and I spent a busy weekend playing with more computers.

Once home I was left with a hacked machine to rebuild. On the upside I got to install a new distribution and a new larger hard drive. The downside is still the feeling of being violated.

A week later I have a new firewall and I can start exploring the hacked drive. A simple VNC error enabled access for someone. There, in the vulnerability notes is a mention and a fix.

Why had I not previously patched the system? The usual answer is one I am sure I am not alone in suffering from – laziness, too many machines, too little time. It is fine on a work server where you get paid to be proactive, but quickly becomes such a time sump if it is on your own machines. Still once bitten, twice shy.

I do not blame someone for hacking me. It has been an interesting learning curve for me and they had the chance to play and learn on one of my systems. It would have been nice to watch from start to finish so as to learn and develop counter measures, but that is for another time maybe.

In need of a solution to my laziness I have started to use the commercial update facilities that so many of the distributions come with. That is not to say I do not now keep a more watchful eye on the vulnerabilities, it does however mean I sleep a little sounder knowing that out there someone practicing the dark arts might just be cursing more than usual.

Safe hacking,

John Southern
Editor

Preview Newsletter

As a service to our readers, and in response to many requests that we have received, we have recently launched the monthly Linux Magazine Newsletter. This opt-in email newsletter will give you a preview of Linux Magazine's next issue, including links to new articles posted on our website.

The Linux Magazine Newsletter will also inform you about others website additions as well as international Linux events and other Linux-related activities.

The Linux Magazine Newsletter is available to everyone, you can subscribe and unsubscribe here:
http://www.linux-magazine.com/Newsletter

LINUX MAGAZINE

We pride ourselves on the origins of our publication, which come from the early days of the Linux revolution.

Our sister publication in Germany, founded in 1994, was the first Linux magazine in Europe. Since then, our network and expertise has grown and expanded with the Linux community around the world.

As a reader of Linux Magazine, you are joining an information network that is dedicated to distributing knowledge and technical expertise. We're not simply reporting on the Linux and Open Source movement, we're part of it.