

## Re: hacked.e-microsoft.net attacks!!!

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2005-09/0162.html>

---

**From:** Moe Trin ([ibuprofin\\_at\\_painkiller.example.tld](mailto:ibuprofin_at_painkiller.example.tld))

**Date:** 09/13/05

Date: Tue, 13 Sep 2005 14:57:59 -0500

In the Usenet newsgroup comp.os.linux.security, in article <Xns96CFED8C99CF82124@216.196.97.142>, darkog wrote:

>in the event of something like this happening, and other than the above  
>method -- are there any other more efficient options you have tried and  
>used effectively?

The 'remove from net, wipe, and reinstall' mantra (which should also include updating to current and fixing the hole used after the reinstall, but before returning the system to the net) is about the only real "sure" method – and this has been true for decades. One standard reference is "CERT Summary CS-98.06" (<http://www.cert.org/summaries/>) which says:

### 3. Root Compromises

We continue to receive daily reports of sites that have suffered a root compromise. Many of these compromises can be traced to systems that are unpatched or misconfigured, which the intruders exploit using well-known vulnerabilities for which CERT advisories have been published.

(Can you hear the author of that advisory banging his head against the wall – same problem, time after time, and he's tired of repeating this.)

It then refers to several other documents (URLs included) pertaining to "Intruder Detection Checklist", "Steps for Recovering from a UNIX Root Compromise", "UNIX Configuration Guideline", and as "List of Security Tools". Note that second item, which is a web page at [http://www.cert.org/tech\\_tips/root\\_compromise.html](http://www.cert.org/tech_tips/root_compromise.html).

The advisory should also be at '[ftp://ftp.cert.org/pub/cert\\_summaries/](ftp://ftp.cert.org/pub/cert_summaries/)'

There is one, and only one solution, which is a wipe and reinstall. Why? Because you don't know with absolute certainty what has been done to your system. Someone else owns it now, and it may well be lying to you – hidden files, kernel modules, and so on. The windoze concept of "remove the virus, and all will be well" is ludicrous. Some \*nix admins want to use a windoze wannabe tool like "rkhunter" (<http://www.rootkit.nl/>)

Re: hacked.e-microsoft.net attacks!!!

or "chkrootkit" (<http://www.chkrootkit.org/>) to look for signs of a compromise. I suppose they are better than nothing, but if they DON'T find a problem, that could mean nothing is wrong, or that the r00t kit author changed a file name, or default directory, and your "tool" isn't aware that this might have happened. Both tools are available as source, and both use extensive scripts – read them, and make up your own mind.

*>can we implement some sort of OS snap shot system and revert back to a  
>safer point in time before the security breach? perhaps something like M\$  
>system restore (no flames pls) but for a \*nix based OS?*

True of all operating systems, not just \*nix – if you have good backups taken BEFORE your box was compromised, you can use those to bring things back to the way they were – in other words, uncompromised, but vulnerable. That last item (true if you wipe and reinstall and fail to grab the updates or correct the configuration hole), you are still at risk – perhaps more so, because whoever r00ted your box knows how to do it again. But then you also have to answer the question – when did "they" get in, so you can go back far enough to be sure that they haven't left a back door wide open waiting for another try. Oh, and how many people have known good backups of ANYTHING? When was the last time you tested your backups?

*>can we use or follow some sort of tried and true method of exporting our  
>config files to be able to quickly bring a duplicate system up and running  
>in much fast time frame?*

So that you can be r00ted that much quicker? Yes, bringing the system back up quickly is important, but you ALSO need to see that the hole that was used to break in has been fixed. That could be an update to some application, but (at least in my experience) it is more often a problem with the configuration that let the bad guys in. Your restoring to a previous snapshot (or the out-of-box setup) is not fixing either problem.

Old guy