

Re: Attacked by UNIX Rootkit

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-08/2512.html>

From: karl [x y] (jamescagney90210@excite.com)

Date: 08/03/02

From: "karl [x y]" <jamescagney90210@excite.com>

Date: Fri, 2 Aug 2002 19:31:49 -0400

"Scott" <scott_chan@ahm.honda.com> wrote in message news:021a01c23a4b\$68832aa0\$9ae62ecf@tkmsftngxa02...
> *I have Win 2000 Adv Server using IIS to host multiple web
> sites and a FTP server. I suspect that the server has
> been attacked by Rootkit recently (Please see attached
> image). Under the ftproot folder, there is a
> folder "~tmp" and under that there is a folder with no
> name. I can't delete those folder. May I know how to
> clean Rootkit attack in Win 2000 machine? The ip address
> is 208.179*

That's not all you'll want to do. If you haven't already, you want to identify how they accessed your system, so you can close that and other vulnerabilities. If you left an FTP folder so that anonymous user could both read and write to any one folder, then that is probably not such a big intrusion.

However, if you failed to apply all the latest IIS and Windows patches [at least up through March 2002] then a hacker could have used IIS or another means to install back doors to compromise your system. Once this happens, the only way to be sure you've removed all the back doors allowing access to your system is to format, reinstall windows and everything else and secure it correctly before making it internet-visible.

You can try to detect certain types of installed hacker software by running fport from foundstone.com and looking for unusual ports and/or programs. You can also try looking at your IIS web server logs for log entries mentioning .EXE or % and that also have a code 200 or 502 in that line in the log.

Securing a Windows computer involves installing all security patches from Microsoft and following the checklists all at www.microsoft.com/security [and you can also find some additional recommendations and varying checklists by searching www.google.com for "harden OR hardening windows-2000" [or whatever your version of Windows is]. You also want to

microsoft.public.inetsrvr.iis.security: Re: Attacked by UNIX Rootkit

consider both software and hardware firewalls, starting at the low end with
Sygate software firewall [free for n