

## RE: Running more than one service on one box

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2001-09/0428.html>

---

**From:** Gary McKinney ([gmckinney@megabits.net](mailto:gmckinney@megabits.net))

**Date:** 09/19/01

From: "Gary McKinney" <[gmckinney@megabits.net](mailto:gmckinney@megabits.net)>  
To: "Dustin Puryear" <[dpuryear@usa.net](mailto:dpuryear@usa.net)>  
Subject: RE: Running more than one service on one box  
Date: Tue, 18 Sep 2001 19:46:51 -0400  
Message-ID: <NEBBLDFCALKLLLEEGDFBPIEFMDIAA.gmckinney@megabits.net>

Hi Dustin,

I can only answer from my own experience but I have found most M\* products to be, shall we say, lacking in the testing department (which leads to all sorts of added and unwanted "features")...

While it is very (and sometimes painfully) true there is \*NO\* bulletproof operating system in use today you have the option of going into the source code in Linux to correct or negate the added "features" whereas you must rely on others (read: Microsoft) to fix and patch their problems.

Now – a little note: Microsoft does allow some VERY LIMITED access to some of their source code (if you have really deep pockets and wear a blindfold) but for the most part open source code (such as Linux) is much easier to fix than proprietary code. The statement that Linux is "more secure" is in the fact it does not have all of the complexities of Microsoft Operating systems (which is one of the reasons it runs so much faster on the same hardware) and it's source code is freely available for all to see and patch as required.

One other "interesting" facts I have noted since I got involved with microprocessors in general (and I own the Intel 8008 ceramic chip serial number 5 if that gives you any idea of how long I have been playing with micros <grin>). \*MOST\* of the vulnerabilities being exploited are unchecked buffer overflows! Most of the libraries used in most compilers contain code with this condition – and could be "hardened" better if the developers of those packages would take the time to do it (or had the resources available to do it). I have seen (and have) source code which deals with the unchecked stack buffer overflow conditions but it increases subroutine processing time anywhere from two to two-thousand times longer to execute (depending on the operations involved). The code can be implemented in the GNU compiler to negate the effects of unchecked buffer overflows but at a penalty to program execution speed – I suppose when we see 10-GHz CPU speeds it may become a viable solution but for the current state of hardware it is not a very good solution to the problems being currently encountered.

RE: Running more than one service on one box

## SecurityFocus BASICS: RE: Running more than one service on one

It's rather interesting that most of the Windows-2000 vulnerabilities are for the most part a rehash of NT-4.0 vulnerabilities (caused by aforesaid problems in the compiler libs). Before anyone starts flaming me I realize the problems are not exact duplicates but most are one form or another of an uncheck stack buffer overflow condition – which are the majority of NT-40 problems as well... Heck, even the president of Microsoft was miffed about the fact they had to release 4 security patches within several weeks time of Win2K's release because of unchecked buffer overflows (and he made the statement to the effect that they should have caught the problems before Win2K went out the door!)

As to your statement that an "out of the box" installation of Windows NT vs. Linux is more secure – it would depend on your definition of "out of the box".... are you referring to installation will all patches applied or just the base installation?? <grin>... My point here is both products have "deficiencies" straight out of the box and must be "tuned" for the applications in which they are going to be used. This applies not only to removal of unwanted services but also any security hardening required for the intended purpose. My experience has found that the Linux systems are easier for the most part to tune over the Microsoft OS systems.

(ever wonder why most software vendors setup the installation to be mostly an open configuration – can you say "less tech support calls"!). It is up to the installer of the software to make sure the software is installed and configured properly for the intended purpose – and I have found Linux to be easier to harden than Microsoft's OS...

I too have not seen any studies to the effect of comparison of Microsoft vs. Linux in terms of security but I would refer you to all of the CERT and BugTrac advisories if you wish to determine this yourself... I am sure there are others here who would be interested in the outcome of such a study...

I hope I have answered why most make the statements you are questioning but again I reiterate this is just my opinions and do not represent in any way the opinions of anyone else on this forum...

Just my two cents....

Gary N. McKinney  
GMSCI LLC  
WGCP (WatchGuard Certified Professional)  
[gotta love all the letters <grin>]

RFC-882 put the "." in dot com – not Sun Microsystems....

> -----Original Message-----  
> From: Dustin Puryear [mailto:[dpuryear@usa.net](mailto:dpuryear@usa.net)]  
> Sent: Monday, September 17, 2001 12:12 PM  
> To: Joe Lyman  
> Cc: [michael@kjarling.com](mailto:michael@kjarling.com); [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)  
> Subject: Re: Running more than one service on one box

RE: Running more than one service on one box

SecurityFocus BASICS: RE: Running more than one service on one

>  
>  
> *I have yet to see any studies that prove that Linux is any more secure  
> that Windows NT. In fact, most Linux distributions take the dangerous  
> tactic of running most services out of the box. Excluding IIS (hell,  
> what can you do?) a default install of NT is arguably more secure than a  
> default install of popular Linux distributions.*  
>  
> *Don't get me wrong, I run \*a lot\* more Linux servers than NT servers  
> over here, but I think it's misleading when someone states simply that  
> Linux "is more secure" or "has better security." What does that mean?*  
>  
> *Regards, Dustin*  
>  
>  
>  
> *On Fri, 2001-09-14 at 13:05, Joe Lyman wrote:*  
>> *Michael,*  
>>  
>> *If you are a small company you should definitely consider using lower  
> cost/higher security software, e.g. Linux. A 486 Makes a decent DNS  
> server, IDS or Firewall. Anyway you look at it your overall costs are  
> going to be much lower with Linux, and you're going to learn some great  
> stuff in the process. If you're concerned about the difficulty of the  
> task, just think of all the help you could get here...*  
>>  
>>  
>>  
>>  
>> *Joseph Lyman*  
>> *Graphic Products, Inc.*  
>> *503-644-5572 ex 5662*  
>> *800-788-5572 Toll Free*  
>> *[jlyman@graphicproducts.com](mailto:jlyman@graphicproducts.com)*  
>>  
>>>> *Michael Kjorling <[michael@kjorling.com](mailto:michael@kjorling.com)> 09/13/01 09:26AM >>>*  
>> -----BEGIN PGP SIGNED MESSAGE-----  
>> *Hash: SHA1*  
>>  
>> *Please apologize me if this has been asked before, but I haven't seen  
>> it lately at least.*  
>>  
>> *Right now several of my servers are serving more than one thing - one  
>> does web, mail (both SMTP and POP), and DNS. Another does the same and  
>> adds the usual risks with being a workstation as well.*  
>>  
>> *I have been lobbying to split this up on more machines, and using one  
>> per service. That is, let one machine handle the email (possibly  
>> forwarding it to internal systems), let one handle the web, two for  
>> DNS (master and slave) and so on. But we are talking about a pretty  
>> small company so I am having a problem of getting the hardware this  
>> would require. It took an actual break-in to one of the systems before*

SecurityFocus BASICS: RE: Running more than one service on one

> > *I was allowed to buy a dedicated hardware firewall, and I would prefer  
> > not having to go through the same mess again.*  
> >  
> > *Could someone please give me some hints as to what the actual security  
> > implications would be of a setup like this? As it is, the company in  
> > question is rather dependant on their Internet connectivity (web site,  
> > email and so on), and I don't want to get into trouble if someone  
> > breaks in through a DNS implementation problem and then escalates  
> > their access and starts messing with the web site, for example.*  
> >  
> > *Any help is greatly appreciated!*  
> >  
> >  
> > *Michael Kjörling*  
> >  
> > ---  
> > *Michael Kjörling – [michael@kjoerling.com](mailto:michael@kjoerling.com) – PGP: 8A70E33E  
> > Manager Wolf.COM -- Programmer -- Network Administrator  
> > "We must be the change we wish to see" (Mahatma Gandhi)  
> >  
> > ^..^ Support the wolves in Norway -- go to ^..^  
> > [http://home.no.net/ulvelist/protest\\_int.htm](http://home.no.net/ulvelist/protest_int.htm) ✓  
> >  
> > \*\*\*\*\* Please only send me emails which concern me \*\*\*\*\*  
> >  
> > -----BEGIN PGP SIGNATURE-----  
> > Version: GnuPG v1.0.6 (GNU/Linux)  
> > Comment: For my PGP key: <http://michael.kjoerling.com/contact/pgp.html>  
> >  
> > iD8DBQE7oN5TKqN7/Ypw4z4RAkUwAJ43lou3pPNOtuDYx4Rp2DP64Tj1KQCeIOtn  
> > EDoYeS++weIT3TWxp3PnkWA=  
> > =4/7X  
> > -----END PGP SIGNATURE-----  
>  
> --  
> *Dustin Puryear <[dpuryear@usa.net](mailto:dpuryear@usa.net)>  
> <http://members.telocity.com/~dpuryear>  
> In the beginning the Universe was created.  
> This has been widely regarded as a bad move. – Douglas Adams*  
>  
>*

- 
- **Previous message:** [Michael Bell: "RE: Windows 2000 Questions"](#)
  - **In reply to:** [Dustin Puryear: "Re: Running more than one service on one box"](#)
  - **Next in thread:** [Devdas Bhagat: "Re: Running more than one service on one box"](#)
  - **Next in thread:** [Michael Kjörling: "Re: Running more than one service on one box"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)