

SecurityFocus Microsoft: RE: What server hardening are you doing these days?

RE: What server hardening are you doing these days?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-11/0063.html>

From: Kurt Dillard (Kurt.Dillard_at_microsoft.com)

Date: 11/14/05

Date: Mon, 14 Nov 2005 06:18:36 -0800

To: "James Eaton-Lee" <james.mailing@gmail.com>

James;

I interpreted your original note in the manner you clarify below.

Leaving aside MAC, DAC, and RBAC since you seem to understand them and they aren't relevant to your comments about the Microsoft platform, I think that there are excellent tools for viewing and managing ACLs in Windows. There are both graphical and command shell utilities that are robust and reliable. Microsoft encourages customers to lock down permissions on their data, and Microsoft encourages ISVs to minimize access to their applications. The problems that arise from changing ACLs on OS components is the unforeseen consequences that arise, as illustrated by the problems from a recent patch already mentioned in this thread. I couldn't agree more with your assertion that "there's nothing stopping you learning about the platform you've chosen to deploy and doing some testing!" Unfortunately, only a small minority of the folks who use our guides, or 3rd party guidance, appear to do significant testing. Even fewer understand the kind of extra testing they'll need to undertake before deploying patches.

I've been able to discuss ACLs and other security issues in Windows with many of the architects, developers, testers, and program managers. Over the last few versions of Windows ACLs have become more and more restrictive, but they have been looking for fundamental changes to the OS as well as new tools that provide a significant improvement in security. Hence the removal of anonymous from the Everyone group, the addition of the Security Configuration Wizard, and the system services lockdown using Network Service and Local Service.

Regards,

Kurt

-----Original Message-----

From: James Eaton-Lee [<mailto:james.mailing@gmail.com>]

Sent: Friday, November 11, 2005 2:11 PM

RE: What server hardening are you doing these days?

SecurityFocus Microsoft: RE: What server hardening are you doing these days?

To: matthew patton
Cc: focus-ms@securityfocus.com
Subject: RE: What server hardening are you doing these days?

On Thu, 2005-11-10 at 23:03 -0800, matthew patton wrote:
> *hehe, good one. my point was never about MAC. Heck, I haven't done*
> *anything with roles yet and that would be very good to have worked*
out.

I'm not sure if you're inferring that this is what I'm doing, but just to clarify, as I pointed out in my e-mail, the point of my post wasn't to score points or contradict the person I was replying to – I was genuinely interested in a friendly discussion because I wasn't sure as to what, precisely, Kurt Dillard meant, and I was interested!

I also (politely) don't agree with you with regard to filing systems, either in theory or in practice, and this is why:

Possibly the strongest pointer for me towards an increase in permission hardening in windows is that consulting within the financial sector as I am at the moment, I can see first hand the breakage which ensues thanks to the filing system and registry (arguably more important) permission changes resultant in Windows Server 2003 – colleagues of mine have had to devote significant amounts of time actually reducing the security of permissions on servers in a granular fashion in order to get their applications to work without (overly) compromising the security of their systems.

In an altogether different environment, permissions on many unix and linux platforms are only better documented and understood due to the common, open architecture such systems share and the (traditionally) greater number of command line tools for enumerating, debugging, and setting permissions on these platforms. (note: I'm not trying to start a flamewar here, and I work with linux/unix too, so this isn't just a windows guy opining!)

More recently, however, the number of such tools has increased (and the options available for windows admins at the command line have always been better-than-advertised thanks to the number of resource kits out there and also freeware offerings such as those from sysinternals). Unfortunately, the commercial nature of windows and the adherence which it lacks to a specific family of OS means that it lacks the open/ubiquitous factor which unix/linux have.

But don't get this the wrong way round – I think this difference (locking permissions in unix is easier) owes a lot to this ubiquitous nature of the unix architecture and applications (such as apache) which commonly run on unix and linux/unix-derived operating systems. This isn't the same thing as the architecture being impossible to secure in this manner or a lack of support for doing it, neither of which (I think) are the case. Coupled with the commercial (and therefore

RE: What server hardening are you doing these days?

SecurityFocus Microsoft: RE: What server hardening are you doing these days?

proprietary) nature of the OS, this creates an environment in which it's easy to fall into the trap of assuming you have no options.

My experience has been that, more recently, given contact with Microsoft (which is a gotcha, but with the complexity of modern operating systems is a gotcha which even open platforms like linux share if you're a large business), the options for locking down windows are increased and they're not as dire as you seem to assume. Besides this, there's nothing stopping you learning about the platform you've chosen to deploy and doing some testing!

With some of my clients in the financial sector, I see (as above with a server build which owes much of its security both to the base OS and the organisation in question's default build security policy) permissions just as (if not more) locked down than unix over and above the base level.

Further to what I've just said, in response to what you say here:

> *IMO before one gets wrapped up in roles or MAC, the stupid filesystem*
> *has got to be done right.*

Arguably, you've got this the wrong way round, although contemporary philosophy seems to view this the other way round – if you read up on trusted computing (for instance, the NCSC orange book, which is over 20 years old –

<http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>), you'll find quite a different philosophy – that Discretionary Access Control or DAC (which is what you're referring to by the "stupid filesystem") is viewed as a companion to (and even further step than, when implemented properly), MAC.

(Of course, if your DAC was never implemented properly in the first place, you need to establish a baseline from somewhere, but this is one of the reasons why DAC is such a mess and "locking down permissions" can feel, at times, really quite a sisyphan task!)

See the following quote from the orange book:

"...Discretionary controls are not a replacement for mandatory controls. In an environment in which information is classified (as in the DoD) discretionary security provides for a finer granularity of control within the overall constraints of the mandatory policy..."

And, further to that:

"...Access to classified information requires effective implementation of both types of controls as precondition to granting that access. In general, no person may have access to classified information unless: (a) that person has been determined to be trustworthy, i.e., granted a personnel security clearance — MANDATORY, and (b) access is necessary

RE: What server hardening are you doing these days?

SecurityFocus Microsoft: RE: What server hardening are you doing these days?

for the performance of official duties, i.e., determined to have a need-to-know -- DISCRETIONARY. In other words, discretionary controls give individuals discretion to decide on which of the permissible accesses will actually be allowed to which users, consistent with overriding mandatory policy restrictions..."

ie. once you've implemented your MAC, you'll be re-implementing DAC over the top of it to restrict your information based on Need To Know over and above your existing security level.

But just my 2c! Sorry, this got quite long quite fast. :)

- James.

