

RE: Internet security on "hotspots"

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2006-04/msg00089.html>

- *From:* "David LeBlanc" <dleblanc@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 20 Apr 2006 20:41:39 -0700
-

There's actually a few more twists to it than that.

On XP, there's a setting in the security policy under Network Access where you can toggle whether or not everyone includes anonymous. IIRC, default is disabled (anonymous isn't part of everyone), but I'm not positive what I may have tweaked on my own system.

Now if we're talking shares, anonymous never did have access in most cases, everyone or not. That's the topic of a couple of settings further down – "Shares that can be accessed anonymously", and there's another for named pipes. If you have some legitimate need to make a share that anonymous can access, you have to add it there. The need for anonymous share access is largely gone – it was mostly needed because prior to Win2k, the machine account wasn't a user that could be recognized remotely.

You're right that Guest isn't normally an authenticated user, but it's also normally disabled by default, so it typically isn't even a factor. This whole deal over everyone vs. auth users dates back to the "red button" episode about 1997, which was largely a tempest in a teapot.

Like most of the checklists, this could cause more trouble than it is worth. For example, they recommend disabling simple file sharing. Excepting the actual files in the shares that would be accessible, this is bad advice for a home user. Forcing all the network access to log on as guest means that the ability to admin the system over the default mechanisms has just vanished. If you want to check it out, set one up that way with a default blank user password and then try and hack it from the network. You won't get far. Their advice to hide the shares is dubious at best. Anyone capable of coding a wrapper over NetShareEnum can see "hidden" shares, and there's lots of tools that have been able to do this for about 10+ years. IIRC shares, even on home, can still be removed as shares, even if you can't disable simple file sharing (though I'm not 100% sure this is actually true).

Their advice to use non-blank passwords is really bad for home users, unless you have multiple users. A blank password can't be used across the network, and is a lot safer overall, except obviously against console access.

Disabling the guest account – it's been disabled by default since NT 3.5, maybe 3.51. I don't remember the last time I had a system that had an

RE: Internet security on "hotspots"

enabled guest account by default. It was at least 10 years ago. If they're that out of date, how much should you trust this info?

One bit of advice that's actually good is to rename the admin account. Basically, you can get a lot of attempted logons against your administrator account just from someone logged on as admin pulling up explorer and browsing the network. This is noise. But if you see failed logons as the renamed admin, then someone is seriously trying to get into your system. It's useful to be able to tell the difference between benign logons and real hacking.

I'm really cautious about these checklists. They often don't help, cause weird problems and side-effects and otherwise cause trouble. The security guidance from Microsoft is what you ought to deal with because it's supported information.

I once reviewed a book on hardening to find that step 3 said to disable something, then step 5 needed that functionality. To actually do any of that would have been a disaster.

Even the experts make mistakes. When we did OpenHack 4, Jesper Johansson did the config for the SQL server configuration. It was secure, but we couldn't administer it at all any more. When we got it on site, the first thing we had to do was change the IP addresses, so guess what – we had to undo some of the changes, reconfigure, then reapply. Jesper contributed to most of the security guidance, so if he and I can foul things up, anyone can.

I haven't personally done a lot of security tweaking since NT 4.0 days. I generally set an admin password that's not guessable (assuming a domain joined system), enable logging and let it go. The systems I put into OpenHack 2 were set up exactly like this, except we enabled IPsec. Those were the only systems in the contest not hacked, other than the firewall itself. The defaults on XP SP2 and better are really good enough for nearly all uses. The thing I always use as a rule is that if you don't know why a given setting is going to mitigate a threat that's really going to get you, don't set it. If you want to play with it at home and see what happens, fine. I have all sorts of things changed on my home network. But if you're dealing with a corporate network, be careful. For example, getting rid of the LM hashes is a good thing in my book, but you do that on a big network and then you find out some weird old system running some critical app doesn't work any more.

It's almost never lack of tweaks that is going to keep you from getting hacked. It's missing patches, dumb user tricks like bad passwords, passwords sitting in batch files on shares, web applications accessing the SQL server as sa with an embedded password AND the web site source on an everyone:R share (oops). Those are the things that will get you. I've seen people worried about the permissions on the SAM file when they didn't have vulnerability assessment, IDS, a response plan, etc.

Funny how this stuff just keeps on going. If you can find archives of the

RE: Internet security on "hotspots"

RE: Internet security on "hotspots"

old ntsecurity@xxxxxxx list, you'll find me saying the same things as this 10 years ago, just a few updates for some new features and tweaks.

Hope this helps.

This is my personal opinion, and should absolutely not be construed as an official statement on behalf of Microsoft. The information provided is intended to help, but you may or may not find it useful.

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

From: Laura A. Robinson [<mailto:larobins@xxxxxxxxxxxxxxxxxxx>]

Sent: Thursday, April 20, 2006 7:26 AM

To: larobins@xxxxxxxxxxxxxxxxxxx; 'Trevor'; focus-ms@xxxxxxxxxxxxxxxxxxx

Subject: RE: Internet security on "hotspots"

Whoops, one amendment- "Guest" (the built-in account, and only that one guest account) is part of "Users", IIRC, but not "Authenticated Users".

Sorry about that. I haven't had my coffee today. :-) In any case, the URL I gave might still be useful.

Laura

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

From: Laura A. Robinson [<mailto:larobins@xxxxxxxxxxxxxxxxxxx>]

Sent: Thursday, April 20, 2006 10:08 AM

To: 'Trevor'; 'focus-ms@xxxxxxxxxxxxxxxxxxx'

Subject: RE: Internet security on "hotspots"

Authenticated Users and Everyone are not the same, and the difference

between them has nothing to do with the Guest account or

Guests/Domain

Guests groups. In Windows 2000 and earlier, Everyone includes Anonymous Logon. In Win2K3, the Anonymous Logon account was removed

from the Everyone group.

Mixed-mode domains (Win2K) and Windows 2000 mixed functional level domains (Win2K3) have nothing whatsoever to do with the

membership of

the Everyone group. Mixed mode/FL relating to groups is

about whether

RE: Internet security on "hotspots"

or not you can create universal security groups and fully utilize domain local groups. Last, the built-in Guest account is

part of both

Authenticated Users *and* Everyone.

An old post I wrote so I don't have to type the details up again:

<http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-01/0046.html>

Laura

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

From: Trevor [<mailto:trevor@xxxxxxxxxxx>]

Sent: Wednesday, April 19, 2006 7:41 PM

To: focus-ms@xxxxxxxxxxxxxxxxxxx

Subject: RE: Internet security on "hotspots"

How about looking into using IPSec with a Pre-shared key

(since the

home user likely does not have a Cert Authority or AD)?

That link does have a few misnomers. Using "Authenticated

Users" on

shares over Everyone is only necessary in a mix-mode domain.

Otherwise, AU and Everyone are the same (as 2000 removed

Guest from

the Everyone group).

-Trevor

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

From: ilaiy [<mailto:ilaiy.e@xxxxxxxxxxx>]

Sent: Wednesday, April 19, 2006 9:03 AM

To: nimda@xxxxxxxxxxxxxxxx

Cc: Agent Zr0; focus-ms@xxxxxxxxxxxxxxxxxxx

Subject: Re: Internet security on "hotspots"

Came across this checklist for home users which is pretty good ..

RE: Internet security on "hotspots"

[url]

<http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm>

[/url]

./thanks

ilaiy

