

Re: Need help closing security holes in my Windows XP home system!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-02/1297.html>

From: Leythos (*void_at_nowhere.lan*)

Date: 02/25/05

Date: Fri, 25 Feb 2005 14:20:43 GMT

On Fri, 25 Feb 2005 04:46:31 -0800, Joe wrote:

> *Leythos wrote:*

>> *On Fri, 25 Feb 2005 03:02:18 -0800, Bob Ladbury wrote:*

>>

>>

>>> *I have a two-computer home network system. I only recently learned how to setup a network system, and now I'm concerned about having opened up new portals of access to internet hackers, because of all the configuring I had to do to get this system to work. Here's a list of some of those possible security holes:*

>>>

>>> *1. My router came with a default MAC address printed on the bottom. Should I change this, if so, to what? (Can you tell I don't know what the heck a MAC address is?)*

>>

>>

>> *No, leave it alone – the MAC address is a physical code that relates to your unique hardware as in your segment of the network – no other device in your segment should have the same MAC.*

>>

>>

>>> *2. I had to enable the GUEST ACCOUNT in XP Pro in order to get the printer sharing to work. Can hackers off the net use this now enabled account to access the computer? What about the ADMINISTRATOR account?*

>>

>>

>> *This is a big screw-up, you never enable GUEST, NEVER! What you needed to do was setup the same users/passwords on both machines – so that if you have user s,d,f,g on machine one you have user s,d,f,g with the EXACT SAME PASSWORDs on machine 2,3,4,5,6....*

>>

>>

>>> *3. The remote computer in my 2-comp network is "supposed" to have its IP masked because the router is a NAT router (with SPI), that supposedly shields all remote computers in the network because it uses what it*

comp.security.firewalls: Re: Need help closing security holes in my Windows XP home system!

>>>calls a built in "DHCP" server to assign its own internal IP addresses
>>>to the remote computers. If this is so, why then can I go on the net
>>>with the remote computer, and any header analysis site will show me my
>>>real IP address?!

>>
>>
>> NAT only blocks unsolicited INBOUND access, it does not stop your browser
>> from running a script that can report back to a web site that you visited
>> what your real, internal, IP address is. What you need to do is visit one
>> of the network scanner sites that will scan all 65535 ports on your public
>> IP to see if you have any holes.

>>
>> Using IE to browse the Internet in a default config, with GUEST enable, or
>> even using an Administrator level account, is asking for your machine to
>> be compromised. Visit the Windows site and seek out the info on how to
>> secure IE, high-security mode. You could also start using Fire Fox as your
>> browser, it's not anywhere near as exploited as IE is.

>>
>>
>>
>>>4. When programs on my system call out to the net, they are initially
>>>blocked by my software firewall (which is an SPI firewall). After a few
>>>adjustments to the personal firewall, they have no problem communicating
>>>with the net. The router also has an SPI firewall. Why doesn't it block
>>>the programs as well? Given that it has never impeded access to or from
>>>anything on my system, it acts like it doesn't even exist!

>>
>>
>> The router is just a router, it's basic function is to ROUTE TRAFFIC ONLY.
>> If you choose to make a outbound connection the ROUTER will let ANY
>> traffic out to where it wants to go, that's how routing works. As for
>> inbound traffic, since the router doesn't see an internal machine
>> requesting the communication, it blocks those unsolicited inbound
>> sessions, there is no path back for them.

>>
>> As for outbound, since a router is not a firewall, there is no real
>> outbound blocking.

>>
>>
>>>5. I set the RPC (Remote Procedure Call) service to avoid rebooting in
>>>all 3 circumstances, to prevent hackers from rebooting my machine from
>>>the net. Will this really prevent reboots, and if so, is there any other
>>>way these cyberscum can automatically reboot my computer?

>>
>>
>> Your computer has a lot of ways it can be compromised, RPC is
>> insignificant once you're not live on the internet.

>>
>>
>>>If you have any other important tips on closing security holes to
>>>prevent hacker access, don't be shy!

Re: Need help closing security holes in my Windows XP home system!

comp.security.firewalls: Re: Need help closing security holes in my Windows XP home system!

>>
>>
>> *Stop running Internet Explorer*
>> *Stop using Outlook Express / Outlook*
>> *Stop browsing questionable sites*
>> *Stop sharing files with anything outside your internal network*
>> *Stop file sharing programs*
>> *Stop loading browser helper tools – not even google/yahoo bars*
>> *Stop using the Administrator level account unless making system changes*
>> *Stop using GUEST*
>> *Apply ALL Windows Updates*
>> *Apply ALL MS Office Updates (if you have OE/MS Office)*
>> *Apply ALL Antivirus updates, run the update daily*
>> *Use a quality Antivirus program*
>> *Install AdAwareSE and SpyBot Search & Destroy and run them*
>> *Use FireFox and ThunderBird for Browsing and Email*
>> *Stop/Don't forward ports through the router to your internal network*
>> *Don't let others use your computer*
>> *Check for router firmware updates once a month*
>>
>>
>>
>
> *I run OE with no problems ever, IE, no problems ever. I don't like it*
> *that people always tell you to do that when at least for me I've never*
> *had a problem.*

Well, I didn't TELL him what to do, he ASKED for options to make his entire experience more secure.

> *I do not use OE right now, but have and never had an*
> *issue, I also like firefox much better and use it way more then IE. To*
> *tell someone to stop using the admin account in windows i say bull*
> *shit!! it really ticks me off when people say that cus they are fine. to*
> *tell a user like Bob, someone who doesn't seem to know anything really,*
> *stop using the win xp user account with admin, that makes it even harder*
> *for him and 99.9% of the time he won't ever have a problem running with*
> *admin rights. dang, i just freaken hate it when people say don't use*
> *windows as the admin, there's nothing wrong with it. again, i never have*
> *issues and won't ever run as a limited user, that's just bull crap.*

If you really think that using the Admin level account don't expose the user to a higher level of risk all the time, and that it's fine to run as a Admin level account, then you really don't understand security for the masses of ignorant users. It's a simple fact that running as an Administrator level account user is the easiest way to compromise your computer while browsing or reading email. You can "freaken hate it", but the fact is that few people have problems running as a Limited User account type as there are only a couple commercial apps that don't comply with basic security.

Re: Need help closing security holes in my Windows XP home system!

comp.security.firewalls: Re: Need help closing security holes in my Windows XP home system!

To make a blanket statement that there is nothing wrong with running as an Admin is to be completely ignorant of the different threats, to ignore what MS suggests, and to ignore what all the security people around the world suggest, and to put users that listen to you into a vulnerable situation.

Now, as an example, I run as a local admin on all of my Windows computers, but I also have a real firewall appliance, filter HTTP sessions to remove malicious content, use Outlook with Exchange, but also remove all malicious scripts and attachments from email before it reaches the mail server, and I also have quality AV software on my machine. I'm also a security expert, so I know what to look for, don't run crap/P2P apps, don't visit questionable web sites, don't open/review questionable email, don't really do anything to put myself in harms way – the same can not be said for the general public.

> *checking for router firmware, lol, if it aint broke dont fix it. most companies, I'll bet none do that often of an update. maybe once every few months is ok and only when having issues. otherwise it's fine.*

If you don't check how do you know if it's broke or not – They don't produce firmware to change the colors of the interface, they produce new firmware to fix issues in the old version. While a router with 5 year old firmware may appear to be working fine, there may be an exploit or some other vulnerability that you are unaware of in your blissfully ignorant state.

> *don't let others use the pc is like telling you lock yerself in yer home and don't go out and dont let people in.*

No it's not, a limited use account that's been locked down is fine, but more times than not, a guest (not guest account) using a computer will compromise your machine since they don't have as much concern about it as the owner would.

> *adaware and stuff i guess is ok, but again, i never have to and never have problems. and i have tried them before and guess what. no problems,. it only finds cookies and they are harmless.*

Again, we're talking about the masses, and those products are very good at determining if you are clean and in helping one stay clean. Not all cookies are harmless.

> *the only thing i really agree with you on Leythos is apply all updates to all programs.*
>
> *anyway im not going to reply again to this thread since you now will reply to me in a rage or fight me, so i don't want conflict, i just got annoyed at you for a lot of stuff you said and i wanted to reply. im sorry, :(*

Re: Need help closing security holes in my Windows XP home system!

comp.security.firewalls: Re: Need help closing security holes in my Windows XP home system!

If you don't care to learn from your mistake then you don't have to reply, but it's obvious that either you don't understand threats in the real world or that your trying to help people compromise their machines.

Don't forget, the OP asked for advise, it was not posted without being asked. While you may not care about security of systems many others do, and there is nothing wrong with what I posted. Even MS, for several month, recommended that users stop using IE 6.

I don't post to fight, just to state facts, you might try learning about security.

--

spam999free@rrohio.com
remove 999 in order to email me