

RE: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/0981.html>

From: joe (*mvp_at_joeware.net*)

Date: 11/20/04

To: "'devis'" <devis@easynix.net>

Date: Sat, 20 Nov 2004 09:21:02 -0500

Devis:

I guess you probably mean me. I don't take offense to it though as you aren't really technically correct but I understand where you are trying to come from (I think) and trust that you believe what you say versus just being a zealot and thinking anything but Windows.

1. The first account created on Windows is Administrator, it is the administrator account, just like *NIX's first account is root. Outside of that then the next account is the account of the person building the box. I haven't built one through the default processes in several months but I think the last time I did I was offered the choice of making the account limited or admin. I personally didn't like the term limited because who is going to give themselves a limited account if an unlimited account is available as an option. Everyone wants the bigger/better whatever when the two choices sit next to each other even if they don't know what is supposed to be better about it. It is why people buy the newer electronics every couple of years and the single guy buys the Excursion over the Expedition over the Explorer over the escort. He has one person to carry around but the SUVs are bigger and better even though he may never carry a single thing or another living soul the whole time he has it.

Anyway, the base cause is a simple one, Windows is consumer based and *nix wasn't and really still isn't. Look at the market penetrations. *nix tends to have people already knowledgeable with its workings or people who WANT to learn the details using it, windows primary users have no experience and want none. A *nix user with no computer experience will get extremely frustrated very quickly, every time they go to do something they feel they should, they get slapped down (I, in my security thoughtful opinion do not think this is a bad idea). Windows initially was a standalone OS, recall it was Microsoft initially thinking there was nothing to the internet and spinning the opposite direction. UNIX was designed from scratch to be networked, and even it had poor initial security when it was really tested. Couple that with the idea that MS doesn't like to leave people behind and it is all logical progression as to where we have gotten where we are (contrast

Full-Disclosure: RE: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

with Apple – can you run an Apple II app on OSX? I have DOS apps written in 86/87 still running fine today, doesn't require admin either). However, that being said, they are offering more and more tools to make it possible to run securely. You will be seeing a rather cool app in the fairly near time frame to help the whole running as admin issue.

Outside of new stuff that is coming, there are a ton of features that have been around for some time to help with this stuff. I personally have run corporate Windows NT Machines as non-admin for some time, had a whole bank division department running as Power User at best in 1996, it was possible if you knew what you were doing as an admin. You had SU and net user /user: in NT4 and the API was fully open but sorry if you can't write something based on docs and instead need the source of the API instead. The big issue from my standpoint was that it wasn't pushed as the way to do things, this stuff wasn't mentioned in the MCSE courses[1]. In the end however, you could blame the OS or you could blame the people using the machines. You have blinkers on a car, it is the drivers choice to actually use them.

2. I completely disagree here. Your experience is most likely with tech people. Most users don't know and don't want to know the differences between accounts and have to work out the idea that you have to log on in special ways to install the latest game or image editing software for their digital camera they just got for xmas. They are there to use the machine, not understand it. Something MS could have done a long time ago and didn't probably because it was outside of the normal mindset is to reduce permissions when running certain apps. Say someone is running as admin, if they fire up IE, that process gets run as guest or anything that is only available to the administrator group is unavailable because that admin group SID is removed from the token. This is done with the most recent version of netmon which was surprising and quite annoying the first time I used it and tried to save a CAP to c:\temp.

- > *Lets not hide from ourselves whats needed from MS to reach*
- > *modern world security: a complete rewrite, and a ditch of*
- > *old Dos base and the 20 years old legacy code.*

Imagine, if you will, if they did this. Think of the fall out of SP2 alone on this list which is supposed to have competent security professionals primarily... Bill might as well just say, you know, I have made enough money for myself and those I care about, let me just close the company down. Doing this would most likely break just about everything if not everything. People who already don't want to move from Win9x to WinXP because some odd piece of crap software doesn't work the same way won't ever consider moving to the new platform Q or whatever they choose to call it. This is such a non-realistic viewpoint it is actually quite laughable. And again, if you go back to a previous conversation from this list, it isn't all of Windows, especially Windows kernel/core level stuff that has an issue. It is some key pieces of the shell. Possibly in your understanding of Windows though, the Shell is all of what you believe Windows is comprised of.

joe

RE: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

Full-Disclosure: RE: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

[1] Don't get me started on MCSEs. As a whole I think they hurt Windows far more than any other thing. A bunch of people who feel they are experts in Windows because they took a couple of tests that 10 year olds could memorize and pass and yet still not be able to run anything. The best I can say about MCSEs is that I will *try* not to look down upon them for being MCSEs and let them prove themselves to be worthless before I assume it in person.

--

Pro-Choice

Let me choose if I even want a browser loaded thanks!

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

From: full-disclosure-admin@lists.netsys.com

[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of devis

Sent: Friday, November 19, 2004 11:10 AM

Cc: full-disclosure@lists.netsys.com

Subject: Re: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

This message is primarily destined to all MS trolls, no matter their levels, and i can see so many in this list that i am happy to target a large audience.

Please run some unix or at least read about the unix permission system, and lets pray god this sheds some light in your mono cultured brains.

Here are the relevant points:

1) Despite recent ameliorations of MS (multi user finally, permissions ...) and some effort at making the system more secure, something very important is still left out: The first default user of the MS computer is made an administrator. This comes down to giving uid0 to ur first unix user. Unix does NOT do that. It requieres you to use su and become root (administrator) after proper credentials submission (password).

The first user is NOT and administrator, and any recent Unix documentation will insist on the danger of running as root(admin). Unix keeps the admin account well separated from the user account, which MS DOESN'T, despite all wrong arguments i read on this list. VERY BAD practice generally. So its user friendly, as the user has admin rights and can therefore install and remove software and change major configuration. Majority of users don't and will never know there is an 'administrator' user that hides from their eyes. This little detail that apparently Ms people can't 'understand' is a huge step. Please install a proper unix, create 2 accounts and try to read the home directory of the second user from the first.

2) "After all, they don;t need to know" . " You're on a need to know basis job"

Do MS really think the users are stupid ? Do understanding different IDs/ roles / accounts on a computer that much of a tough message to pass to the end user ? Isn't security important and supposedly the goal of recent MS developpements ? If they really did target security, their efforts will have been into making the user understand that he should be admin to install programs, and a non privileged user to surf the web.

IS that that hard to understand ? And that much hidden into high IT security professionnall unreachable knowledge ? I don;t think so. Doesn't a company such as MS has enough ressources to make that a priority and educate the users ? Off course it has. Just not very 'commercially' friendly as if user then understand roles, it might requires less Anti virus, personnal firewall and other bullshit FUD's scareware (Yes its scareware, and it is the best selling software category OF ALL times of software history).

This is why, Firefox being independant from this OS that carries 60 of its code base as being legacy code for older system hardware and backward compatibility, is likely more secure than the in house integrated application. Now if u are running Firefox as an administratordon't be surprised if something happens. Don;t blame the software, but your poor security practices.

Lets not hide from ourselves whats needed from MS to reach modern world

RE: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

Full-Disclosure: RE: [in] Re: [Full-Disclosure] IE is just as safe as FireFox

security:

a complete rewrite, and a ditch of old Dos base and the 20 years old legacy code.

Hopes that clears things.

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>