

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

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/1023.html>

From: devis (*devis_at_easynix.net*)

Date: 11/21/04

Date: Sun, 21 Nov 2004 07:32:56 +0100

Paul Schmehl wrote:

> --On Friday, November 19, 2004 01:12:31 PM -0500 "Crotty, Edward"

> <Edward.Crotty@dowjones.com> wrote:

>

>> I'm not a Win based guy (troll?) - Un*x here - and even I was

>> offended by

>> #1.

>>

>> There is such a thing as "runas" for Windows.

>>

> That's not all.

>

>> -----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

>>

>> 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.

>

>

> Apparently you don't have very broad experience with OSes. ON *every*

> OS I'm familiar with, the first user is the administrator (or root)

> account.

>

Are You an idiot ? When i start MS and look at my emty desktop, under what ID that graphic interface runs ?

If i configure my outlook and go to fetch nice infected mails, who i am then launching outlook ? Administrator

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

On unix, launching a graphic interface under root would have printed a big warning panel or for more descent OSES not allowed me AT ALL.

I am NOT argueing that the first user is and admin, i am argueing that the DEFAULT user is an admin. The default user on UNIX is not root.

Try to re reading before making a fool of yourself.

```
>> 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 ).
>
>
> When's the last time you installed an OS from scratch? Gentoo,
> FreeBSD, OpenBSD, RedHat, Fedora, Slackware, Mac OS X, Debian,
> Solaris, *all* create the first user as uid0 during the install
> process. (I can't speak for the others because I haven't done those,
> but I'd be willing to bet that NetBSD, AIX, HP-UX, SCO et. al. work
> exactly the same way.)
>
```

See up there. You need to learn to read and make sense of it. Once again, I AM NOT ARGUEING THAT THE FIRST ACCOUNT CREATED HAS AN UID0. Please open ur eyes and try to pinpoint the difference between first user and default user. Even MS is confused on that subject it seems.

```
> Unix does not grant users root access by default, and it does a much
> better job of separating privileges by requiring you to join the wheel
> group *and* either use sudo or su to do work as root, but Windows
> doesn't make users the admin by default *either*, unless you setup
> Fast User Switching *during* the install.
>
```

IT does makes the first installer of the box the default user. And that first default user HAS administrator priviledges. What what part of this is not clear ? With or without Fast User Switching. Ever installed XP ?

many unixes don't use a wheel group.

----- snip -----

```
% grep wheel /etc/group
%
Debian linux
```

Playing on words ? Sure Linux isn't Unix, but then write Unix like so: Unix(tm) and i will know.

```
>> 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,
>
```

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

>
> *That's simply false. Windows has several groups. By default users*
> *are in the "USERS" group, *not* the ADMINISTRATORS group.*
>
> *It might make sense if you actually had knowledge of an OS before you*
> *criticize it.*

>
Please prove ur point and run IIS from an unprivileged account.

>> *Please install a proper unix, create 2 accounts and try to*
>> *read the home directory of the second user from the first.*
>>
> *Please do the same in Windows. Here's a hint. You'll get the same*
> *results.*
>
>> *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 ?*

>
>
> *Probably. Otherwise they wouldn't have those stupid warnings popup*
> *every time you try to delete something. Are you SURE you want to do*
> *this???? Yes, damn it!!*

>
>>
> *[snipped the rant]*
>
>>
>> *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.*

>>
> *Oh baloney. Learn a little more about the OS before you make*
> *assumptions that make you look ignorant.*
>
> *Aside from the default permissions, you can also granularly apply*
> *privileges in many ways. For example, by default USERS have Read &*
> *Execute, List Folder Contents and Read access to the Windows folder,*
> *its contents and all it's subfolders. In addition, there are fourteen*
> *(14) separate rights that can be explicitly granted or denied to them*
> *at that level only or to all subfolders as well, to files only, to*
> *subfolders only, to subfolders *and* files only, etc., etc.*

>
I ahve admined nt4 boxes, and before being insulting, u should maybe
look up again and re read. I do know nt ways, and it is just a pale
implementation of permissions. They perfected it in 2003 but still has
much to be desired. Took them long enuf to get user roles / id werking.

> *I'm not Windows fan, but the least you can do is learn the subject*
> *before you claim expert status and presume to preach to others.*

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

- >
- > *While we're lecturing the unwashed, would you mind trimming your*
- > *replies? Who needs six levels of FD disclaimers?*

Its un moderated, live with it.

- >
- > *Paul Schmehl (pauls@utdallas.edu)*
- > *Adjunct Information Security Officer*
- > *The University of Texas at Dallas*
- > *AVIEN Founding Member*
- > <http://www.utdallas.edu>
- >
- > _____
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*
- >
- >

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>