

RE: locked out of XP, need file access

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0030.html>

From: Miner, Alan G (alan.miner_at_nwa.com)

Date: 01/02/04

Date: Fri, 2 Jan 2004 10:28:56 -0600
To: <security-basics@securityfocus.com>

To paraphrase Isaac Asimov, I can see far because I stand on the shoulders of giants.

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

From: Muhammad Naseer [<mailto:naseer@digitallinx.com>]

Sent: Wednesday, December 31, 2003 1:41 PM

To: JGrimshaw@ASAP.com; security-basics@securityfocus.com

Subject: RE: locked out of XP, need file access

Quietly agree with your post. I was just about to hit the submit button with a solution and your email came in and my view changed. This is correct that most of the ppl around just want "Click here to Continue" or something like ready-to-fly stuff (hehehe, I am a flyer and this is a typical term) but one thing I am not able to understand by your point of view, if an individual is not ready to read all those 100s of pages on the very topic and want a quick answer, isn't this he wants to save time? It smells like you learned most of the things the *hard way* but that can't be true for all others. Some people just want a short answer other dig all the way till the end themselves.

Regards,

Muhammad Naseer
+92-300-8449347

Digital Linx – We eDrive your Business
info@digitallinx.com
+92-42-5166617

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

From: JGrimshaw@ASAP.com [<mailto:JGrimshaw@ASAP.com>]

Sent: Tuesday, December 30, 2003 11:42 PM

To: security-basics@securityfocus.com

Subject: Re: locked out of XP, need file access

SecurityFocus BASICS: RE: locked out of XP, need file access

Security through obscurity is not the solution I was soliciting from the group.

The individual in question openly stated that he did not want to read 1000s of a pages for an answer, and requested a quick answer. A simple search engine query, as many people suggested, would have yielded a less-than-1000-page result. You offered to help him in exchange for a personal email—is that security through obscurity, so that no one else would know? And your email address is a hotmail address—is that not a personal address? It is certainly not business related. And your presented name of "..."? Is this not obscured? I am not pointing this out as an attack; I am demonstrating that you are exercising evasion when you told us that the information is out there anyway.

We all know data is out there. A number of list members replied to me and said that lock-picking data was out there—the thief would get it anyway. And I am sure there are plans to make a number of appropriate, inappropriate, and questionable alternatives, along with any matter of information out on the Internet. But he did not want to read 1000 pages of hits. The example of the car thief was taken out of proportion by some—Yes the data is out there. However, unless he has wireless internet access and the means to use the information he found, provided he took the time to read it while standing outside, it is unlikely that he could search the internet efficiently while targeting the car of choice. The crime of opportunity has passed from the lack of opportunity. Conversely, he could also use a blunt object and just smash the window to get in. This wouldn't require any extensive searching, other than for a rock. But would you give our theoretical intrepid footpad the idea to do this? Or hand him a rock? Probably not.

My intent was to alert people, if not exactly to alarm them. People are helpful; that is not a bad thing. (This can easily break down into a philosophical discussion that escapes the bounds of this forum; I do not wish to lead us down that path.) My point is that just because there is something out there, does not mean we have to present it to whomever asks because they will find it anyway. Just because the man doesn't have his keys does not mean we should smash the window for him, or point out the rocks he can use. You are correct—the information is out there. He might come back later with a rock. He might come back with a skilled friend, or skilled himself; he might even come back with a locksmith because, hey, it really IS his car.

I am not asking everyone to deny information, either, or hold back because they are overly suspicious. That would be pointless and is out of focus for this mailing list. But a "Hi, I do not know please tell me how" post... couldn't they search first? Couldn't they say what they have tried? What failed so far? Maybe some background on what caused it? (this is not entirely in relation to the post I originally referenced—I am sure that one can come up with a few posts that are lacking in detail) Many people here do post great questions—and provides for great archive material for scenarios and solutions. Questions akin to "How do I Own my b0x" does

RE: locked out of XP, need file access

SecurityFocus BASICS: RE: locked out of XP, need file access

not seem to apply in the professional business sense, however, and I believe that a professional business sense is the objective that this list is trying to achieve.

". ." <miklohnews@hotmail.com>
12/29/2003 05:08 PM

To
security-basics@securityfocus.com
cc

Subject
Re: locked out of XP, need file access

I agree, all valid points. However

– i went overseas for a few months and came back only to find myself having forgotten the admin password to both my w2k machines at home. I thought i remembered it, and was surprised when my machines didnt wanna accept what i typed in at all! hmmm... must've changed them right before i left. ;) – as u can see by the replies to this question, the information is defenitely out there anyway, whether u find it urself (google) or ask like

this in a formum, so no point in trying to hide it.
– to hide information like this may lead to a false sense of security. someone not knowing how easy it is to crack a system may feel that they're

all secure since they have a password setup. security by obscurity is the term i think.

i think it's more up to the local administrators to try to keep a close eye on people in his/her area. on a forum like this, hey, what can i do anyway

if someone on the other side of the world wants to break into some system (maybe mine!! oops...)? i look after my things and hope that someone wont be able to break into my machines. hopefully, if this guy doesnt have legitimate reasons to reset the password, his local admin doesn't allow him physical access to this machine. but on the other hand, as u or someone else said, he may have physical access if it's the neighbour machine in his office. ah well. my point is that the info is out there, u can always find

out, so no real point in trying to hide things.

>From: JGrimshaw@ASAP.com
>CC: security-basics@securityfocus.com
>Subject: Re: locked out of XP, need file access
>Date: Mon, 29 Dec 2003 11:05:32 -0600
>
>To preface, I apologize if I am wrong. I also expect to be bashed for

RE: locked out of XP, need file access

SecurityFocus BASICS: RE: locked out of XP, need file access

>being harsh, but sometimes reality stings.
>
>A question that I have, is that if the box is his, and those files are his
>(and are important), how did he suddenly just "forget" the admin password?
> What has he been using to log in on a daily basis? Why isn't the
>password for this box the same as the other local admin passwords on
>the network? Why is he administrating an XP box and then throwing up
>comparisons to Windows 98 PWL files? Why not connect to the network
>and log on with domain administrator rights? If he does not have the
>access, why not call their helpdesk and have one of the administrators do this?
>
>While I agree that sharing of wisdom is vital to the growth of this
>mailing list, the temperance of such wisdom should be considered. I
>shared this email with my co-workers, and we all thought a laptop fell out
>of the back of a truck into the requestor's lap.
>
>Perhaps it is because I do not trust email's originating from a hotmail
>address asking for a hack. Anyone can get a hotmail address with any
>information provided. Nigerian officials offering me vast rewards have
>emailed me from Hotmail. If this was a legitimate request, why not post
>it from his place of business? It looks like to me that someone saw
>something he wanted on someone else's computer, and from looking over
>the shoulder, caught a few characters of the password. The person has
>physical access to the box, and now wants the data but doesn't know how to
>get it without a script being handed to him. Perhaps this is paranoid,
>but this is SECURITY we are talking about.
>
>Responding in the positive to his request akin to offering a burglar a set
>of lockpicks and detailed picking instructions because he "lost" his
>keys to his car. I am under the impression that giving a wink, a nod,
>and looking the other way... is not the appropriate approach to this
>sort of request. You tell the person to find a locksmith to get into
>their car, or offer to call the police for him. You aren't supposed to
>provide locksmithing instructions when you don't even know the car is his.
>
>This is nothing more then social engineering. How would any of you
>react if you received a call from a user in your business asking how to
>crack the admin password on their machine? Would you tell that user?
>You just did.
>
>
>
>
>
>
>

RE: locked out of XP, need file access

SecurityFocus BASICS: RE: locked out of XP, need file access

> > *my files asap.*

> >

> > *What would be some of the necessary simple steps to take at this time?*

> > *Thanks in advance...*

> >

> >

> > *Expand your wine savvy ? and get some great new recipes ? at MSN Wine.*

> > <http://wine.msn.com>

> >

> >

> >

> -----

> ----

> -

> >

> -----

> ----

> --

> >

> >

>

>

> -----

> ----

> -----

> -----

>

>

>

Hot chart ringtones and polyphonics. Go to
<http://ninemsn.com.au/mobilemania/default.asp>
