

RE: privilege escalation techniques

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0154.html>

From: Roy Stapleton (*roy_at_stapleton.biz*)

Date: 01/21/05

Date: Fri, 21 Jan 2005 00:46:54 -0000

To: <pen-test@securityfocus.com>

I have tried the sethc.exe one, the 'at' command scheduler technique and the 'c:\program' technique.

The OS I used was windows XP pro sp2. I logged in as a domain user with no added rights, i.e. only local user access to the machine.

There is no write access in the c:\ or c:\windows\system32 folder, so the sethc.exe technique fell at this hurdle, default rights on these folders are users: read & execute and list (this folder, subfolders and files), create folders (this folder and subfolders), create files (subfolders only).

For the same reasons, the c:\program exploit failed as well.

The domain user does not have the privilege to create schedules with the at command, so this failed as well.

The problem seen below does exist on XP. It may be (pardon the fuzziness here) to do with caching load images of executable files and prefetch stores. If you look in the C:\WINDOWS\Prefetch directory you will see all the recently loaded executable files stored in a prefetch format.

This may be why the original loaded when BSK tried the sethc.exe technique in BSK's email.

For the below, I checked these on a machine I had local admin access on.

XP also watches files in the system32 directory. If you browse there and rename the sethc.exe to something else and then refresh the screen, you will see XP restore the sethc.exe file after a few seconds.

If you open a dos prompt and (make a backup of the sethc.exe file warning here) copy cmd.exe to sethc.exe, answering that yes, you do want to overwrite the original, you will see the new sethc.exe in an explorer window with a cmd.exe icon. Now, if you delete that, windows will restore sethc.exe but with a cmd.exe icon (note the file sizes). When

SecurityFocus Penetration: RE: priviledge escalation techniques

done this way, pressing shift 5 times will indeed open a cmd prompt.

This subject does interest me greatly, if you know of any techniques that will escalate privileges on an XP machine I would like to know them.

Thanks

Roy

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

From: BSK [mailto:bishan4u@yahoo.co.uk]

Sent: 20 January 2005 11:13

To: miguel.dilaj@pharma.novartis.com; pen-test@securityfocus.com

Subject: Re: priviledge escalation techniques

- > *That's really strange. It works in WinXP.*
- > *Perhaps there was a change in functionality (for bad!) from Win2K to XP?*
- > *The only possibility I can imagine is either:*
- > *a) something blocks launching interactive programs before logon in 2K, but not in XP*
- > *b) 2K is checking that sethc.exe is valid before launching it, and XP is not doing that check (I don't really think that this is the case, but...)*
- >
- > *Do you have any XP box to test?? I'll try to get hold of a 2K as well.*

I couldn't try on a XP box, but tried on a windows 2000 server. It behaves very differently here, after the replacement of sethc.exe with cmd.exe:

1. before logging in, pressing 'shift' 5 times, invokes sethc.exe but the original one, which in fact doesn't exist in system32 directory, atleast with same name. I think windows regenerated that file but with some other name.
2. if I press 'shift' 5 times after logging in, nothing appears, neither original sethc.exe nor the replaced sethc.exe

Any clues?

ALL-NEW Yahoo! Messenger – all new features – even more fun!
<http://uk.messenger.yahoo.com>

RE: priviledge escalation techniques