

Re: [SLE] connecting to an XP box.

Re: [SLE] connecting to an XP box.

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2006-01/msg01294.html>

- *From:* Carl Hartung <suselinux@xxxxxxxxxxxxxx>
 - *Date:* Thu, 12 Jan 2006 13:34:28 -0500
-

On Thursday 12 January 2006 08:31, Al Active wrote:

> On Thu, 2006-01-12 at 07:00 -0600, Stan Glasoe wrote:
>> Please post it here also. Most of us need this information.
> I second that suggestion ... most of us **have to** support Win Boxes in
> Networks ...

OK, All, I can't believe I'm doing this on my beloved SUSE list, but I'm getting (and responding to) direct requests, too.

– Carl

Here's the info:

Sign up and download the .pdf "Securing Windows XP":
<http://www.abxzone.com/forums/showthread.php?t=83570>
Read it completely before implementing any suggestions.

More valuable info is available at these resources:
<http://www.markusjansson.net/exp.html>
http://www.tweakhound.com/xp/security/page_1.htm
http://csrc.nist.gov/itsec/guidance_WinXP.html
<http://www.dwheeler.com/essays/securing-windows.html>

If the system has already been connected to the internet, you should wipe it clean and reinstall XP while the system is **not** connected to the Internet. The procedure is described in the document you downloaded, above.

Additional Software:

Spybot Search & Destroy (Google "download Spybot Search & Destroy")
Install, configure and run Spybot Search & Destroy. Don't be rushed... take your time and use **all** the tools. It's like a Swiss Army Knife full of useful/important stuff that stays hidden until it's noticed and pulled up. If you invest the hours to explore and learn it, the effort will pay off in spades. Specifically:

- 'deselect' any "ignore products" under "Tools"
- install the Spybot S&D hosts file
- enable all of the IE 'tweaks'
- change all IE start/search pages to Google or another safe site

Re: [SLE] connecting to an XP box.

Re: [SLE] connecting to an XP box.

- Use the "Immunize" function
- view and check unknown processes in the process explorer
- view, export and delete (careful!) unwanted items in the startup viewer
- remove unwanted/suspect Active-X controls (Browser Helper Objects)
- Verify only authorized/desired network connections are configured (no phantoms; keep the 'green checkmark' items)

Ad-Aware Personal (Google "download Ad Aware Personal")
Install and run this scan, too.

Spywareblaster (Google "download Spywareblaster")
Install and enable all protections.

Trojan Hunter (Google "download Trojan Hunter")
Download, install and run the free 30 day trial. If you do a lot of surfing (don't!) and you also do e-mail (don't!) on XP, the paid subscription is definitely worth it.

Grisoft's AVG Free (This is a PITA to find; keep digging, it's there.)
This is a great anti-virus program. In the years I've used it (since day one) I've only had one or two config 'hiccups' to iron out after virus definition /and/ program updates. They've done a great job of making it as painless as possible.

Zone Alarm Free (Google "download ZoneAlarm Free")
You turn OFF the built-in XP firewall and ICS (Internet Connection Sharing) <shiver!> install Zone Alarm and then... critical... learn how to use it.
This kills two birds with one stone: ICS is highly insecure and ZA gains you program level control, meaning you can manage all *outgoing connections.*

www.sysinternals.com has TWO critical programs:
– tcpview (see *all* network connections, resolved locally and remotely)
– process explorer (like a task manager on steroids)

Now, it might seem like there's a lot of redundancy in all of these packages and one vendor's suite might be less hassle, but you've got to realize that not every developer can detect and defeat every exploit in real time. This overlap overcomes that situation by sticking to packages that are proven "best of breed" and, in some cases, highly specialized to target specific types of vulnerabilities.

One final note: The minimum ongoing update/scan schedule that I've found to be effective is twice a week... keep a simple text file log and build the process into a habit. (I put shortcuts to each program except AVG and ZA into one 'Security' folder with the log. It is much easier that way: open the folder, open the log, run each program to update and scan, update the log accordingly, close all, done.)

--

Check the headers for your unsubscribe address
For additional commands send e-mail to suse-linux-e-help@xxxxxxxxx

Re: [SLE] connecting to an XP box.

Re: [SLE] connecting to an XP box.

Also check the archives at <http://lists.suse.com>

Please read the FAQs: suse-linux-e-faq@xxxxxxxx

- **References:**

- ◆ **[SLE] connecting to an XP box.**
◇ From: John Meyer
- ◆ **Re: [SLE] connecting to an XP box.**
◇ From: Stan Glasoe
- ◆ **Re: [SLE] connecting to an XP box.**
◇ From: Al Active

- Prev by Date: **Re: [SLE] Verizon DSL**
- Next by Date: **Re: [SLE] suse on proliant DL320 G3**
- Previous by thread: **Re: [SLE] connecting to an XP box.**
- Next by thread: **Re: [SLE] connecting to an XP box.**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**