

# Re: Linux client in Windows Domain (Security Advice)

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-08/msg01232.html>

---

- *From:* Joe <joe@xxxxxxxxxxxxxxxx>
  - *Date:* Thu, 09 Aug 2007 14:15:09 +0100
- 

Jason wrote:

Hi all, just want to pick your brains.

I have a windows environment and all clients are XP controled with strict security measures controled via group policy etc. I have Trend Micro Client Server Messaging Security for SMB looking after our network.

The problem is, one of the other IT guys has a liux client that sits out side most of these systems. I am about to go through his set up and have to be satisfied that it can work within our network without breaching security etc.

My question is, is there anything obvious I should determine? What kind of stuff could he do that he wouldnt/shouldnt be able to do if using a XP machine.

Any info you have would be great. (You've probably worked out I'm a windows man with very basic Linux experience.

The important bit is to present him with your written security policy and request him to sign his compliance with it, if you haven't done that already. You can't really stop someone with physical access to an XP workstation from doing naughty things, and someone in your position certainly couldn't stop a malicious Linux user.

Having said that, most security policy is not designed to stop a malicious workstation user, but to keep a clueless one from accidentally damaging the machine/network. There is less scope for that with Linux (there's no such thing as Linux AV software, clamav and other virus checkers are designed to block Windows viruses) but there are a few basic security precautions.

Being an IT person, and certainly the local admin of his machine by default, he will need access to the root (built-in admin) account. Your position sounds like some kind of IT admin, so you should also have the root password, as you would for the XP local admin accounts. He should run as an unprivileged user (as I'm sure you normally do) as it is

## Re: Linux client in Windows Domain (Security Advice)

perfectly possible for all admin work to use the equivalent of RunAs, confined to a text terminal. The graphical desktop should not be run as root. No sane Linux user runs as root, as there's too much scope for self-inflicted damage. Everyone makes mistakes. Most graphical desktops are configured by default not to accept root logins, you need to drop to a text terminal to do that, on the very rare occasions it may be necessary.

The only serious external risk to Linux at the moment is by dictionary attack on the SSH server, the Secure Shell. Presumably he will expect SSH access to this machine from outside. The safe way to do it is by public/private key pairs, like SSL (which it uses). A further precaution is to disallow remote root access (he can become root after connection, using a second password) which is something I'd like to see Microsoft do. I don't give Domain Admins either VPN or RWW rights. Something else which is useful, but doesn't add security, is to use a high port for SSH instead of the default 22. The attacks are carried out by bots, and it really isn't practical to do a dictionary attack on the whole range of ports, so they stick to 22. That's not to say that it's safe to use passwords when a different port is used, but it does mean less cluttered logs.

A feature of SSH you may not be aware of is that it can tunnel an arbitrary number of TCP/IP protocols, like a VPN. What this means is that a remote SSH user can talk to any LAN machine on any port. I use this for most RDP access, as I do most of my remote Windows admin work from Linux, and my main client runs an SSH server. It is possible to tunnel the SMB protocol this way, giving remote access to shares (with appropriate credentials, of course). There is a good free Windows SSH client, called puTTY, and you may want to ask for an account on this machine, and for him to show you how to connect to it. Even if this doesn't help you much now, you will probably pick up some Linux knowledge over time.

The standard security precaution, for Windows or \*nix, of only running services which are actually required is valid here. There is a built-in firewall, of ISA grade, which will help in protecting the Linux machine itself from local hostiles. OK, it's extremely unlikely that someone who's just compromised a Windows machine in a LAN will then try to go for a Linux one, but every little helps.

There should be no way that a Linux machine can get 'more' access to a Microsoft server than XP, so it isn't worth worrying about what is installed on the machine. SBS should already be designed to limit access to shares and other sensitive regions to people with appropriate permissions, so they can get the same access from XP. A Linux installation is likely by default to contain many tools which can be used maliciously, but all those tools are also available for Windows.

.