

## Re: privilege escalation techniques

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0133.html>

---

*miguel.dilaj\_at\_pharma.novartis.com*

**Date:** 01/17/05

To: pen-test@securityfocus.com  
Date: Mon, 17 Jan 2005 16:20:12 +0000

Hi Dan,

Let's suppose a Windows environment. I don't know if this is your case.

The first, obvious step, is to check what kind of physical access the insiders have to their workstations.

If they can boot to alternate media (floppy, CDROM, USB) there are several possibilities, for example:

1) boot to NTFSDOS Pro, that allows NTFS write access, and change some exe that usually runs as system (the antivirus is a good candidate) by a copy of cmd.exe, then when the program is executed, a nice CLI starts with SYSTEM privileges... then you can install software (for example a sniffer, more at the bottom of the email).

2) boot to Knoppix or any other live-linux-on-CD distribution, there you've all the tools you need, and you can install additional ones (to RAM) from the Internet

3) the one I've chosen, similar to (1) above. I've XP with the Accessibility Tools installed by default. They monitor some keys, and if for example you press SHIFT 5 times a popup appears where you can activate and configure the accessibility tools. The program responsible for that is sethc.exe, and the guys at Micro\$oft comit the cardinal mistake of not making IT check if SHIFT was pressed 5 times, but to include that in some other part of the OS (kernel? ;-)

So if you press SHIFT 5 times, sethc.exe is executed, but doesn't matter WHAT IS sethc.exe

You guess that, I replaced sethc.exe by a copy of cmd.exe

If I press that BEFORE login, a CLI as SYSTEM is started, I can launch compmgmt.msc and add myself to the local administrators group (please note that if you start it AFTER login, a CLI is started as your user).

Now let's suppose that you manage to use your own tools, by any of the methods above.

You can launch a sniffer, gather login credentials, and crack them using the password cracking program you like more.

## SecurityFocus Penetration: Re: priviledge escalation techniques

If the network is switched, perhaps you need an ARP poisoning tool. It's very unlikely that your switch is configured to avoid that (I still have to see one in a real environment!).

You can also launch a program to intercept SMB logins (like SMBproxy and similar tools) and act as the user who's logging in without even the need to crack his/her password.

Is the above useful? It'll depend... if the administrators have the bad idea of logging in into the servers over the network, perhaps you can gather their credentials or abuse their own login. Otherwise you'll get access as different users...

If the network is composed of Linux/UNIX machines, you can still sniff passwords for unencrypted services (telnet, pop3, ftp, etc.) in the hope you can find something useful.

And of course there's still the possibility of using a local xexploit for an unpatched vulnerability to raise your privileges to admin/system/root/whatever...

IT Security is nice ;–)

Solutions:

- 1) don't use any services that send information in cleartext
- 2) remove all physical access that allows booting to alternate media
- 3) configure your switches (if you can, it's not possible for all switches) in such a way that you can fool an ARP poisoning attempt. Be sure that you are not vulnerable to a DoS!
- 4) investigate packet signing in Windows networks, to fool SMBproxy and similar man-in-the-middle tools
- 5) investigate tools to detect sniffers (i.e. NIC in promiscuous mode)
- 6) have a lot of luck. It's almost impossible to deter a skilled insider in most company's setup

Cheers,

Miguel Dilaj (Nekromancer)  
Vice-President of IT Security Research, OISSG

Dan Rogers <pentestguy@gmail.com>  
16/01/2005 15:58  
Please respond to Dan Rogers

To: pen-test@securityfocus.com  
cc: (bcc: Miguel Dilaj/PH/Novartis)  
Subject: priviledge escalation techniques

Hi List,

I have been asked to test the network security of my organisation from an internal perspective. My boss has not been particularly specific in

Re: priviledge escalation techniques

## SecurityFocus Penetration: Re: privilege escalation techniques

his requirements (other than asking that I don't break any operational infrastructure) so I can approach the problem from whichever way I deem most appropriate.

I suspect the first thing I will attempt is privilege escalation techniques from a workstation with a domain user account to see if I can install my own software/toolset. Can anyone suggest any good whitepapers or tools that I can use to get a head start?

I intend to follow this up by scanning/targeting critical parts of our infrastructure – domain controllers, mail servers, routers etc. However, I am interested to know what other people would do when given free reign to identify internal weaknesses – so how should I approach this? This is not an 'audit' exercise, as I will not be given access to server/infrastructure configurations.

Any advise on this appreciated.

Dan