

# RE: Windows Independant GUI

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-09/msg00041.html>

---

- *From:* "Isaac Van Name" <[ivannname@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:ivannname@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 7 Sep 2006 10:41:58 -0500
- 

Yes, you can change the Terminal Services dll to an older version from a beta version of XP SP2. However, this dll is inherently less secure and this "fix" doesn't work on a Windows XP box that is on a domain (as far as I know... please correct me if you've found otherwise).

As for which dll, Santosh, this website was posted earlier, but I will show it again:

<http://sig9.com/articles/concurrent-remote-desktop>

If you don't like the method detailed there, there are a million other websites showing the same thing that Joshua pointed out (do a Google search for "concurrent remote desktop XP")...Been there and did that while I was looking for a concurrent desktop solution for our domain users' computers. Hence, the mention of the inoperability on a domain computer.

I can't say I dislike VNC... it hasn't crashed on me yet, and it seems like a good solution. I'm sure it just depends on which version you use. One thing I do like about VNC is that you can use the same program (VNC Viewer) to remote into Windows and Linux boxes.

Of course, as always, I'm constantly looking for a better solution for such tools. If anyone has any suggestions that are low-cost or "reasonable" cost, I'd be glad to hear them. Thanks.

Isaac Van Name

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

From: joshua barker [<mailto:joshua.barker@xxxxxxxx>]  
Sent: Wednesday, September 06, 2006 1:48 PM  
To: pen-test@xxxxxxxxxxxxxxxxxxxxx  
Subject: Re: Windows Independant GUI

You can change a dll in Windows XP with an older version plus a registry setting to allow as many concurrent terminal service sessions as you need. Also, remote desktop is inherently more reliable than vnc as I have had it crash on me several inopportune times.

On 9/6/06, Marios A. Spinthiras <[mario@xxxxxxxxxxxxxxxx](mailto:mario@xxxxxxxxxxxxxxxx)> wrote:

RE: Windows Independant GUI

Goodmorning,

You are right upon the terminal services but with regards to the user being "kicked off" this is meer configuration. There are actual RDP lisences that you can purchase from windows. Many people in a corporate environment do so. In a single "poor man's" setup with RDP the event you referred to will occur. Yet again a "poor man's" setup is VNC in most cases :P Personally I dont use windows that much and definately not RDP! VNC has done fine for the passing years and I dont see why it wouldnt for the upcoming years.

Many Thanks,  
Mario A. Spinthiras

Beauford, Jason wrote:

Isaac Van Name wrote:

For the record, Remote Desktop Connection only spawns another "virtual desktop" on a system running Terminal Services (Server 2003 and, I believe, Server 2000). Windows XP runs Terminal Services Lite and, as such, Remote Desktop Connection used on a Windows XP box will kick off the user currently logged in. WinConnect XP Server is an option to get multiple RDP sessions, and I'm sure others know of better ways (or, at least, I hope so), as WinConnect is not cheap.

Isaac Van Name

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

From: Marios A. Spinthiras [<mailto:mario@xxxxxxxxxxxxxx>]  
Sent: Tuesday, September 05, 2006 5:02 AM  
To: pen-test@xxxxxxxxxxxxxxxxxxxxxx  
Subject: Re: Windows Independant GUI

Remote Desktop Connection spawns another "virutal desktop" under the account credentials you specify. This is unlike VNC which simply connects to the active display of the user currently logged on. If VNC is running as a system service it still means that you

RE: Windows Independant GUI

will be connecting to the Administrator account. If the station is locked (ALT CTRL DEL) then you will be looking at the same screen that the user looks at when he looks at the monitor of the workstation. Disregarding that simply for aesthetic purposes , what you need is a RDP like connection.

Regards,  
Mario A. Spinthiras

One2@xxxxxxxxxx wrote:

Hey All,

After compromising Windows workstations  
I am able to gain a remote  
GUI via

either Terminal Services, VNC, GetScreen, etc.

However, this remote access gives me access  
to the user's GUI, which

limits me to using the GUI when they seem to have left for  
lunch. ;o)

Does anyone know of any way that I can  
gain an independant GUI so  
that I

can use and install GUI software to continue the attack,  
without  
having to worry about whether the user is using their GUI?

All ideas are welcome.

My opinion is that the more programs you install, the more likely you  
are to be detected. CLI equivalents should be used instead of trying to

RE: Windows Independant GUI

use GUI interfaces.

That aside, this hack may help you. I've never tried myself so I cannot report on it. Just putting it out there for you to try.

<http://sig9.com/articles/concurrent-remote-desktop>

Kind Regards,

JMB

---

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

[http://www.cenzic.com/products\\_services/download\\_hailstorm.php](http://www.cenzic.com/products_services/download_hailstorm.php)

---

---

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

[http://www.cenzic.com/products\\_services/download\\_hailstorm.php](http://www.cenzic.com/products_services/download_hailstorm.php)

---

---

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

[http://www.cenzic.com/products\\_services/download\\_hailstorm.php](http://www.cenzic.com/products_services/download_hailstorm.php)

---