

[VulnWatch] Re: Hacking Citrix Faq (+DEF CON presentation)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-09/0034.html>

From: Ossian Vitek (ian.Vitek@ixsecurity.com)

Date: 09/28/02

To: wirepair@roquemail.net, bugtraq@securityfocus.com

From: "Ossian Vitek" <ian.Vitek@ixsecurity.com>

Date: Sat, 28 Sep 2002 02:49:00 +0200

Hi!

The URL to my Citrix tools is:

<http://www.cqure.net/itools01.html>

My DEF CON presentation is also there now!

sh0dan (wirepair@roquemail.net) wrote (Citrix quotation):

- > 1. Disable MetaFrame XP server broadcast response. CMC |
- > Right-click on farm | MetaFrame Settings tab | Uncheck the
- > two boxes in the "Broadcast Response" section. This will
- > prevent that perl scanner from working.

Maybe... But if it doesn't stop the Citrix client (with the use of citrix-pa-proxy.pl) to enumerate applications I could write a new PA scanner that enumerates the applications.

I will check that next week.

Some simple "breaking out from given environment":

Very easy: Start the task manager, choose run... explorer.exe (both the task manager and run.. can be disabled).

Easy: If not started; start the given application. Choose File->Open and on a directory; right click and choose explore.

(If there is no open..., search for open..., save as..., attach... or similar.)

Lots of clicking: Press F1 and search for open... (another help file). Or try to find a link to web based support (starts IE) or email (starts IE).

(You can sometimes find links that starts commands in new help files).

Even more clicking: Choose print... and try to right click/explore everywhere. The printer could have it's own help file.

So, conclusion:

=====

Start with:

task manager (Default CTRL+F1 [Citrix client])

F1 (Help)

VulnWatch: [VulnWatch] Re: Hacking Citrix Faq (+DEF CON presentation)

Try the following everywhere:

Right click and explore.

F1 if it seems that a new application has started (like printer or help).

Click on everything that looks like an URL or an email. (Tip: Look in the Help->About or icons on the application)

If you cant find and an URL or email address; try to write one somewhere.

This is for the desktop. Remember; A hacker doesn't need a desktop. Command prompt is better for a hacker.

CMD.EXE, COMMAND.COM (Yes, it is still there, and has bugs), FTP.EXE and shell escape with "!" or "! command.com /c regedit.exe".

Prevention?

Applications written for Terminal Services/Citrix/Tarantella is usually very hard to break out from.

Fire up regedt32 and disable most of windows. Remove execute and read from almost every file.

Securewave has a nice product:

http://www.securewave.com/products/secureexe/secure_exe.html

Check out their nice live DEMO. I have succeeded to halt their DEMO server once (cmd /k cmd /k cmd /k cmd /k cmd /k cmd /k you get the point). You can now only spawn a few processes.

If you know about other similar applications, please mail me.

//Ian Vitek, iXsecurity

- **Previous message:** [FVS: "\[VulnWatch\] FVS318 Config stores usernames/passwd's in plain text"](#)
- **Next in thread:** [ET LoWNOISE: "\[VulnWatch\] \[LoWNOISE\] "Get Knowledge" SunONE Starter Kit - Sun Microsystems/Astaware"](#)
- **Reply:** [ET LoWNOISE: "\[VulnWatch\] \[LoWNOISE\] "Get Knowledge" SunONE Starter Kit - Sun Microsystems/Astaware"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)