

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-05/msg00036.html>

- *From:* Sat Jagat Singh <flyingedervish@xxxxxxxxxx>
 - *Date:* Mon, 5 May 2008 10:42:45 -0700 (PDT)
-

I'll count myself as corrected on the issue of privilege escalation through MS Office. I actually did find one. MS06-009 pertains to a vulnerability in the Korean Input Method Editor of multi-language versions of Office 2003 that Microsoft says can be exploited to escalate privileges. So, that's pretty obscure and unlikely to be found in most environments. But it demonstrates that such a thing is conceptually possible.

Concerning access control and other "unauthorized" access, in some environments simply being able to use ping or browse the network is a violation of policy, though it may not violate the configured access rights. One needs to distinguish between what is authorized in the sense of managerial policy versus permissions that are actually configured. These types of unintended access are often the gateway to finding poorly secured assets that are actually sensitive. That is why such desktop restrictions are implemented as one way of enforcing access control. You are certainly correct that in and of themselves these measures are not access control.

--- On Fri, 5/2/08, Thor (Hammer of God) <thor@xxxxxxxxxxxxxxxxxx> wrote:

From: Thor (Hammer of God) <thor@xxxxxxxxxxxxxxxxxx>
Subject: RE: Fwd: Terminal services and remote programs.
To: "PenTest" <pen-test@xxxxxxxxxxxxxxxxxx>
Date: Friday, May 2, 2008, 3:50 PM
Inline:

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

From: listbounce@xxxxxxxxxxxxxxxxxx
[<mailto:listbounce@xxxxxxxxxxxxxxxxxx>] On Behalf Of Sat

Jagat Singh

Sent: Wednesday, April 30, 2008 7:48 AM
To: PenTest
Subject: Re: Fwd: Terminal services and remote

programs.

Our team regularly breaks into Terminal Servers

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

through social

engineering and phishing techniques. So, measure #1

to protect these:

require either ipsec vpn to be able to connect to the

box or two

factor

authentication such as RSA or Vasco to get on it.

Always excellent advise, and not just for terminal services. Multiple authentication methods are always recommended.

When I have credentials, I have never yet seen a

Terminal Server or

Citrix Metaframe server on which I wasn't able to

gain unauthorized

access to programs and escalate that to where I could

get to most

anything, no matter how tightly somebody thought it

was locked down.

There are dozens of ways to break out of an

application jail in

Windows.

Well, you might choose to call it "unauthorized" access, but it is clearly "authenticated" access, and access to files that you have *permission* to access. More next...

1) In the programs you mention, just go to the file

RE: Fwd: Terminal services and remote programs.

open dialog box.

Now you basically have a Windows Explorer interface.

You can use this

to create shortcuts on your desktop to executables

that may be

otherwise inaccessible, browse the network, delete

files and more.

2) The help system for the application is basically an

Internet

Explorer interface. This has been widely exploited by

many people to

carry out all kinds of mischief.

So, yes — there are many, many ways to "exit" out of published applications or otherwise "desktop access limitation" methods like found in the resource kit. Help–menu access is a well known method of opening other windows while in a "limited desktop" environment, as is "alternateshell" or "launch on connect" options. However, limited desktop measures are *not* security solutions – they are simply methods by which to streamline deployments and to keep users from "hurting themselves" by accident.

But don't confuse "using help to access an Internet Explorer interface" with something like "bypassing permissions" or "un–authenticated access" or "privileged escalation." I know *you* are not confusing the two, but others on this list may think you are saying that accessing IE via Help is the same thing as bypassing an access control, which you

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

are not.

Escalating from a normal user to admin on a properly secured box (or just a regular, say, Win2k3 box for that matter) is not as easy as you make it sound. You'll have to either find an unpatched vulnerability to exploit, or some other terribly misconfigured service to leverage.

In this example, the OP was concerned with a full desktop of all Office and Adobe applications — the issue is NOT about "getting IE" or "explorer" windows – it is about taking simple measures of auditing system permissions so that users cannot trivially (or even non-trivially) escalate privilege. All applications via RDP will be run in the context of the logged on user (to answer the original question) and no manner of "unauthorized access" to IE or Explorer changes that. This is the crux of the past post about a "RDP vulnerability" that dude didn't understand.

3) Application vulnerabilities that permit code execution.

Indeed. RDP hosts must be properly patched just like desktops. The one good benefit of an RDP host over a desktop is that the user doesn't have direct physical access by which they can easily get admin. However, they still must be audited, patched, and have logs reviewed.

Critical measures to prevent these include:
– install the system on an isolated network if

possible, or restricted

DMZ otherwise;
– such servers should be either standalone or a member

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

of a Windows

domain that is used only for administering the

Terminal Servers;

– ensure that all of the application patches are

installed promptly

Great advise, of course.

Other security controls are also relevant, including,

personnel

controls such as background checks, user account

management that

include promptly deleting obsolete accounts.

I'm really glad you mentioned this. Policy counts here. Just like on desktops, users caught trying to bypass authentication methods or practicing unsafe computing should be shot immediately. Corporate due diligence in hiring, old account maintenance, and general good housekeeping is a must, and an excellent inclusion.

To answer your other question, if there is a

patch-based vulnerability

in the application that someone can exploit to execute

code, it would

typically give them the security context of their own

user account.

But I think their have been at least a few MS Office

vulnerabilities

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

that were exploitable to escalate privileges.

Like which? Can you name one? I'm not aware of an office vuln that allowed for escalation.

It would depend on the nature of the vulnerability. Typically, MS has gotten

better over time

at limiting the opportunities to carry out exploits

and the impact of

the exploit when it does succeed. So, it would be

worth considering

Windows 2008 to deploy such a solution. While it is

largely untested

in the wild, it should benefit from Microsoft's

improved development

and testing processes under the "security

development lifecycle" and

"trustworthy computing" regime.

Again, great advise. 2008 offers many new methods by which to secure TerminalServices and RemoteApp deployments, including certificate connectoids, TLS/SSL connections, digitally signed RDP files and MSI-based remote app deployments, and in combination with ISA, even client-certificate based TSWeb connection options.

t

Check out Tim Mullen's "Microsoft Ninjitsu"

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

training at Blackhat Vegas
2008.

There are also some other great NGS classes lead by
world-class
researchers and trainers available.

<http://www.blackhat.com/html/bh-usa-08/train-bh-usa-08-tm-ms-bbe.html>

--- On Fri, 4/25/08, Paul Halliday

<paul.halliday@xxxxxxxx> wrote:

From: Paul Halliday

<paul.halliday@xxxxxxxx>

Subject: Fwd: Terminal services and remote
programs.

To: pen-test@xxxxxxxxxxxxxxxxxxxx

Date: Friday, April 25, 2008, 4:03 PM

I am just curious if any of you have performed an
audit on a

setup
like this:

In a nutshell, tech services is looking to offer
the

entire
Microsoft Office suite and Adobe Creative suite

through

Terminal
services.

My immediate concern is, If there is a

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

vulnerability in

the remote
apps, what will the context be for the attacker?

Is there anything else I should be looking more

closely

at?

Thanks.

This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real"

vulnerabilities fast.

Click to try it, buy it or download a solution

FREE today!

<http://www.cenzic.com/downloads>

Be a better friend, newshound, and
know-it-all with Yahoo! Mobile. Try it now.

http://mobile.yahoo.com/;_ylt=Ahu06i62sR8HDtDypao8Wcj9tAcJ

RE: Fwd: Terminal services and remote programs.

–
This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities

fast.

Click to try it, buy it or download a solution FREE

today!

<http://www.cenzic.com/downloads>

–
This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities fast.
Click to try it, buy it or download a solution FREE today!

<http://www.cenzic.com/downloads>

Be a better friend, newshound, and
know-it-all with Yahoo! Mobile. Try it now.
http://mobile.yahoo.com/?_ylt=Ahu06i62sR8HDtDypao8Wcj9tAcJ

This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities fast.
Click to try it, buy it or download a solution FREE today!

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

<http://www.cenzic.com/downloads>
