

RE: Windows Remote Desktop

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0271.html>

From: Shawn Jackson (sjackson_at_horizonusa.com)

Date: 01/20/04

Date: Tue, 20 Jan 2004 10:39:33 -0800

To: "erisk" <erisk@iinet.net.au>, "Depp, Dennis M." <deppdm@ornl.gov>, <jamesworld@intelligencia.com>

If Internal:

ACL access to your TS servers network interface.

Use windows IPSEC TCP Security to create secure communications between the server and client in addition to RDP encryption.

Use VLANs to segment the allowed users of the server from the rest of the network.

If External:

Use the TS Advanced Client web interface and create a secured webserver (on the TS Server). Block inbound TS connections, except from 127.0.0.1. SSL the webserver only give the matching cert to the allowed clients.

Use IPSEC VPN/SSL VPN to create a tunnel into the network then use the above Internal security idea.

Use a direct SSH tunnel from the server to the clients, then port-forward the TS traffic through the SSH tunnel.

Shawn Jackson
Systems Administrator
Horizon USA
1190 Trademark Dr #107
Reno NV 89521

www.horizonusa.com
Email: sjackson@horizonusa.com
Phone: (775) 858-2338
(800) 325-1199 x338

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

SecurityFocus BASICS: RE: Windows Remote Desktop

From: erisk [mailto:erisk@inet.net.au]
Sent: Tuesday, January 20, 2004 1:14 AM
To: Shawn Jackson; Depp, Dennis M.; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: Re: Windows Remote Desktop

Hi all,

On the topic of securing RDP i was wondering if anyone can help....

So far I have done the following on one of soon to be released Terminal servers where we want only small amount of users to acces it from their homes or other remote locations:

- (1) Hardend box, virus, patches, strong password controls etc
- (2) Changed the default port to something way up there..
- (3) Enforced 128 bit encryption on the sessions

Now everything works fine but Im still security concious and would like to know anymore tweeks to improve the overall security of Terminal Services.. I thought about two factor but we cant afford SecureID... Has anyone else got any other ideas or what they have done to their boxes? Something that is free or cheap and token based perhaps?

Regards,
Nick

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

From: "Shawn Jackson" <sjackson@horizonusa.com>
To: "Depp, Dennis M." <deppdm@ornl.gov>; <jamesworld@intelligencia.com>
Cc: "Michael Gale" <michael@bluesuperman.com>;
<security-basics@securityfocus.com>
Sent: Saturday, January 17, 2004 9:26 AM
Subject: RE: Windows Remote Desktop

That's beyond the scope of the discussion, but a good majority of exploits and hacks our there revolve around gaining root access to a system. A certificate is not an end-all to prevent a MiM attack that was the point.

Shawn Jackson
Systems Administrator
Horizon USA
1190 Trademark Dr #107
Reno NV 89521

www.horizonusa.com
Email: sjackson@horizonusa.com

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

Phone: (775) 858-2338
(800) 325-1199 x338

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

From: Depp, Dennis M. [mailto:deppdm@ornl.gov]
Sent: Friday, January 16, 2004 5:07 PM
To: Shawn Jackson; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Is it possible to gain access to a certificate without having admin privs on the box?

Denny

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

From: Shawn Jackson [mailto:sjackson@horizonusa.com]
Sent: Thursday, January 15, 2004 7:05 PM
To: Depp, Dennis M.; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

If you get a hold of the certificate the server presents to the clients and match your server configuration to match the target server the certificate can remain valid and it won't be flagged by the client. I've done this with some servers on a few 'crunch time' occasions.

Shawn Jackson
Systems Administrator
Horizon USA
1190 Trademark Dr #107
Reno NV 89521

www.horizonusa.com
Email: sjackson@horizonusa.com
Phone: (775) 858-2338
(800) 325-1199 x338

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

From: Depp, Dennis M. [mailto:deppdm@ornl.gov]
Sent: Thursday, January 15, 2004 3:06 PM
To: Shawn Jackson; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Https would not be subject to a MiM attack using the method I described. This is because a third party is willing to vouch for the identity of the server. This is done through the ssl certificate. If my browser/client trusts the third party, then they can also trust the server. If I attempt a MiM attack, the client should notify me there is a problem with the server. This prevents the MiM attack.

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

Denny

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

From: Shawn Jackson [mailto:sjackson@horizonusa.com]
Sent: Thursday, January 15, 2004 4:51 PM
To: Depp, Dennis M.; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Well if you use that example everything is subject to a MiM attack. You could do that with websites, application servers, network programs, etc. With Citrix you can setup a HTTP gateway, protect it with SSL/HTTPS then use the Citrix ICA encryption on top of that, only give the Cert to client you wish to have access to the gateway. That is how Citrix can be more secure then RDP. If you are not using a separate system for your http gateway you mitigate the risk of a MiM attack. Additionally you can create ICA Client packages that have all the required information hard coded, this makes it hard for the user to change the server information and harder for it to connect to a 'wrong' server. The TSAC (Terminal Services Advanced Client) has a web TS interface; you can protect that the same way using SSL and certificates and only allow known people to access it. I've personally never used TSAC in this way, but I believe it's possible.

The older NT 4 Terminal Service edition used Citrix ICA protocols. RDP5 is a Microsoft only protocol and was created mostly from scratch. A good comparison of the protocols is at <http://www.purenetworking.net/RDPvsICA.htm>.

Everything is possible in the world of security; you can't protect yourself 100% no matter how hard you try. The only thing we as security professionals can do is try and decrease/mitigate the risk as much as possible. I agree that use of RDP/ICA can open up a hole into your network. But you can mitigate the risk of a RDP/ICA connection with planning, thoroughness and foresight.

Shawn Jackson
Systems Administrator
Horizon USA
1190 Trademark Dr #107
Reno NV 89521

www.horizonusa.com
Email: sjackson@horizonusa.com
Phone: (775) 858-2338
(800) 325-1199 x338

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

From: Depp, Dennis M. [mailto:deppdm@ornl.gov]
Sent: Thursday, January 15, 2004 1:14 PM
To: Shawn Jackson; jamesworld@intelligencia.com

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Shawn,

I still fail to see the difference between Citrix and RDP as far as security goes. RDP like Citrix can be configured on the server side. As for the MiM attack. Theoretically I can setup an machine and have it masquerade as your Citrix server. When you logon to my machine you enter your Username and Password. I pass this information on to your Citrix server and I have compromised your data. This is possible because no authentication is done at the client to ensure your machine is authentic. This is true for both the HTTP interface/gateway and the ICA client. The same also holds true for the RDP protocol. (Which I believe has a lot of Citrix components in it.)

I still don't want end users accessing their home workstation via RDP, Citrix, PCAnywhere, VNC or any other protocol. This creates another portal into my network for virii and worms.

Denny

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

From: Shawn Jackson [mailto:sjackson@horizonusa.com]
Sent: Thursday, January 15, 2004 3:52 PM
To: Depp, Dennis M.; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Citrix ICA defaults to the setting on the server side, so if you configured your server with *some* security then a 'basic default' is not the case. Personally I separate raw data (Files, Databases, etc) and interactive 'streaming' data. Raw data is a file/component in transit on the wire that can be sniffed and recompiled, while streaming data can't be recompiled into anything but can be sifted through for information.

Capturing interface information from even an unencrypted RDP connection is difficult. Setup three workstations on a hub then setup VNC server on 1 and the viewer on the 2nd. From the 3rd workstation use SNORT and sniff the traffic between the two. Have another person play with the viewer to give you something too look at.

To my understanding Citrix is only at risk of a MiM attack when using the HTTP interface/gateway and not the ICA client. If I'm incorrect please supply a link to information about this attack. Also I don't believe you can use SSL with XP RDP and that's Terminal Services.

Personally I can justify the need of using RDP to my workstation at home, but then again I know that system and its security. I setup and maintain that network and servers so I can be reasonably sure that my connection is clean and my systems are not at risk. Would I personally

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

let my users have RDP access to their workstations at home, nope. My reasoning for this is that they could be violating the company policy (browsing bad sites, playing games, listening to their MP3 collection, etc) and we can't see it. Would I let our IT/IS guys, yep. I'm not worried about people taking data offsite because everyone has USB drives already. I'm also not *too* worried about virii or hackers; it's that it just walks too fine a line with our security policy. But then again, if them have a business need...

My 2,000,000 cents! :-)

Shawn Jackson
Systems Administrator
Horizon USA
1190 Trademark Dr #107
Reno NV 89521

www.horizonusa.com
Email: sjackson@horizonusa.com
Phone: (775) 858-2338
(800) 325-1199 x338

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

From: Depp, Dennis M. [mailto:deppdm@ornl.gov]
Sent: Thursday, January 15, 2004 10:29 AM
To: Shawn Jackson; jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Two statements I don't agree with:

1) "Additionally no actual 'data' is transferred through the RDP connection, it's just interface information (mouse movement, button clicks, typing) and screen refreshes. Now if you were using the resource mapping then data would traverse the RDP connection and would be subject to its encryption."

Data is sent over the wire concerning keystrokes, mouse movements and screen refresh data. Obviously this information, particularly keystrokes can provide data to a hacker. However all information set via RDP is encrypted the default is 56-bit with the capacity to use 128-bit RC4. Even when using local resources, the data is still encrypted with 128-bit security.

2) "All in all I think that PCAnywhere and Citrix have more secure RDP/VNC like interfaces"

The default security setting in Citrix is basic (no encryption) PCAnywhere maybe better, I'm not sure. Both Citrix and RDP are vulnerable to MiM attacks. Citrix does have the capability to use SSL but this is comprable to Microsoft's VPN solution.

Denny

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

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

From: Shawn Jackson [mailto:sjackson@horizonusa.com]
Sent: Wednesday, January 14, 2004 6:36 PM
To: jamesworld@intelligencia.com
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Well transferring data outside a company is easier then pie these days. With everything from encrypted email to USB drives it's hard to use that as a sole point 'ban' RDP to offsite resources. Unless you're running at high level security i.e. Military, Extremely Sensitive Work, National Security the movement of data offsite would be a secondary concern.

The RDP encryption is 'in transit' protection and won't protect the resources. I personally never use the clipboard sharing, drive/printer mapping, etc. Access to those resources should be dictated by the company security policy and doesn't follow the 'security' of the protocol/connection. Seaming the connection is one-way (From Workstation or RDP Host) it hard to open a hole/exploit through an infected RDP host and use the RDP interface to your advantage.

Additionally no actual 'data' is transferred through the RDP connection, it's just interface information (mouse movement, button clicks, typing) and screen refreshes. Now if you were using the resource mapping then data would traverse the RDP connection and would be subject to its encryption. All in all I think that PCAnywhere and Citrix have more secure RDP/VNC like interfaces but RDP is pretty secure by itself. Just as James stated, watch the local resource mapping.

Shawn Jackson
Systems Administrator
Horizon USA
1190 Trademark Dr #107
Reno NV 89521

www.horizonusa.com
Email: sjackson@horizonusa.com
Phone: (775) 858-2338
(800) 325-1199 x338

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

From: jamesworld@intelligencia.com [mailto:jamesworld@intelligencia.com]
Sent: Wednesday, January 14, 2004 3:03 PM
To: Shawn Jackson
Cc: Michael Gale; security-basics@securityfocus.com
Subject: RE: Windows Remote Desktop

Ahh,,

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

but what about the option to connect local resources.....

Drives
Printers
Serial Ports
Smart Cards

....

Talk about the ability to transfer company data out... What is protecting the actual data, MS RDP encryption which defaults to "medium" security by default.

Again it comes back to.....What is the company policy? If it doesn't cover it, the policy needs to be updated.

-James

At 12:14 01/14/2004, Shawn Jackson wrote:

> *Eh' for 'Testing' I use a remote SSH server off my backbone. I*
> *do 'periodically' login to my remote XP workstation and do some work.*
> *Because only screen information is transmitted even if that system was*
> *hacked or infected with a virus it won't affect my network at work. My*
> *XP system doesn't sit directly on the Internet through; it goes through*
> *a Debian box running iptables.*
>
> *Shawn Jackson*
> *Systems Administrator*
> *Horizon USA*
> *1190 Trademark Dr #107*
> *Reno NV 89521*
> *www.horizonusa.com*
>
> *Email: sjackson@horizonusa.com*
> *Phone: (775) 858-2338*
> *(800) 325-1199 x338*
>
> -----Original Message-----
> *From: Michael Gale [mailto:michael@bluesuperman.com]*
> *Sent: Tuesday, January 13, 2004 8:35 PM*
> *To: security-basics@securityfocus.com*
> *Subject: Windows Remote Desktop*
>
> *Hello,*
>
> *I have a question, I have locked down a company network*
> *allowing*
> *only*

RE: Windows Remote Desktop

SecurityFocus BASICS: RE: Windows Remote Desktop

>web browsing, SSH and FTP. Nothing else is need and soon SSH and FTP
>will be gone hopefully once the VPN is final.
>
>Right now a internal user is complaining about the fact their remote
>desktop connection to their home PC is no longer working.
>
>The justification is that a remote PC out side the network is needed
for
>testing. At which point I gladly offered to setup a out side box for
>testing. :)
>
>Any ways the question I have is, do you feel that Remote Desktop (into
>WinXP) is a secure enough connection to allow it. I mind you that this
>is supposed to be a outbound connection only but you never know with
>windows.
>
>
>--
>Hand over the Slackware CD's and back AWAY from the computer, your geek
>rights have been revoked !!!
>
>Michael Gale
>Slackware user :)
>Bluesuperman.com
>
>-----
-
>----
>Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off
>any
>course! All of our class sizes are guaranteed to be 10 students or
less.
>
>We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion
>Prevention,
>and many other technical hands on courses.
>Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720
>off
>any course!
>-----
-
>-----
>
>
>-----

>Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off
any
>course! All of our class sizes are guaranteed to be 10 students or
less.
>We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion

SecurityFocus BASICS: RE: Windows Remote Desktop

Prevention,
>and many other technical hands on courses.
>Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720
off
>any course!

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off
any
course! All of our class sizes are guaranteed to be 10 students or less.
We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion
Prevention,
and many other technical hands on courses.
Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720
off
any course!

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off
any
course! All of our class sizes are guaranteed to be 10 students or less.
We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion
Prevention,
and many other technical hands on courses.
Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720
off
any course!

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off
any
course! All of our class sizes are guaranteed to be 10 students or less.
We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion
Prevention,
and many other technical hands on courses.
Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720
off
any course!

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off
any
course! All of our class sizes are guaranteed to be 10 students or less.
We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion
Prevention,
and many other technical hands on courses.
Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720
off
any course!

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off any
course! All of our class sizes are guaranteed to be 10 students or less.

SecurityFocus BASICS: RE: Windows Remote Desktop

We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion Prevention, and many other technical hands on courses.

Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720 off any course!
