

## RE: Windows Remote Desktop

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0236.html>

---

**From:** Depp, Dennis M. (*deppdm\_at\_ornl.gov*)

**Date:** 01/16/04

Date: Fri, 16 Jan 2004 08:45:07 -0500

To: jamie@nucdc.org, security-basics@securityfocus.com

The RDP protocol must setup the RD4 encryption. The first packet must be sent in plain text because the two machines have not yet agreed on how to encrypt the data. You will notice the mstshash= before administrator. This is what RDP is using to setup the encryption. I assume mstshash stands for MicroSoft Terminal Server HASH.

Denny

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

From: Jamie Pratt [mailto:jamie@nucdc.org]

Sent: Thursday, January 15, 2004 4:31 PM

To: security-basics@securityfocus.com

Subject: Re: Windows Remote Desktop

hmm... the 'main' traffic does appear encrypted, but this third packet sent on the initial RDP connection prior to login is somewhat odd: (the RDP session has 'Administrator' as the default account on the TS login screen, and I am running as Administrator myself – what's up with the username showing in the data section of the packet if it's all encrypted then?) – Well..at least I can't see the password going over the wire!

---

Frame 20 (94 bytes on wire, 94 bytes captured)

Ethernet II, Src: 00:07:f4:ed:e4:af, Dst: 00:0f:43:71:2c:6e

Internet Protocol, Src Addr: 192.168.X.X (192.168.X.X), Dst Addr: X.X.X.X (X.X.X.X)

Transmission Control Protocol, Src Port: 1054 (1054), Dst Port: 3389 (3389), Seq: 1, Ack: 1, Len: 40

Source port: 1054 (1054)

Destination port: 3389 (3389)

Sequence number: 1

Next sequence number: 41

Acknowledgement number: 1

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

Window size: 16560

Checksum: 0x25c9 (correct)

SecurityFocus BASICS: RE: Windows Remote Desktop

Data (40 bytes)

0000 03 00 00 28 23 e0 00 00 00 00 00 43 6f 6f 6b 69 ...(#.....Cooki  
0010 65 3a 20 6d 73 74 73 68 61 73 68 3d 41 64 6d 69 e: mstshash=Admi  
0020 6e 69 73 74 72 61 0d 0a nistra..

---

regards,  
jamie

Depp, Dennis M. wrote:

> *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  
>  
> -----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  
>  
<snip>*

---

---

RE: Windows Remote Desktop

## SecurityFocus BASICS: RE: Windows Remote Desktop

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!

-----