

RE: Remote Desktop vs VPN on Windows 2003

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-01/0244.html>

From: Roger A. Grimes (roger_at_banneretcs.com)

Date: 01/19/05

Date: Tue, 18 Jan 2005 21:12:29 -0500

To: <rgrant@nextsequence.com>, <security-basics@securityfocus.com>

Rhett wins my latest book, Honeypots for Windows book (<http://www.amazon.com/exec/obidos/tg/detail/-/1590593359>).

Rhett, send me your name and address back if you are interested.

I had RDP on 33000. 33001, 33002, and 33003 are honeypots.

Ports 25 and 110 are my Exchange server. The rest of the ports are false-positives. There are no services running there.

Let's see. I had over 1200 unique IP address and 71,203 scan packets (and climbing) hit my home computers. I had 37 people send me guesses. Only Rhett was even close. How much combined effort did it take to find the port? And if I changed the header information, it could have been even more difficult.

So, if a RDP buffer overflow worm came out, it would probably attack TCP port 3389. One packet per IP address breaks in on most networks running RDP. On my network, it took 70,000 scan packets and a distributed scan.

Now tell me again how changing the default port doesn't add ANY security value? Security through obscurity is another tool in our defense plans.

If the world used more random ports, all worms would have to randomly scan all ports to find the service they were hoping to take advantage of. They would become significantly slower, and many would not work because alternative defense-in-depth devices would block the scanning.

Thanks to everyone who participated. I've got logs and statistics for my next talk at SANS.

Roger

*Roger A. Grimes, Banneret Computer Security, Computer Security Consultant

*CPA, CISSP, MCSE: Security (NT/2000/2003/MVP), CNE (3/4), CEH, CHFI

*email: roger@banneretcs.com

*cell: 757-615-3355

*Author of Malicious Mobile Code: Virus Protection for Windows by O'Reilly

*<http://www.oreilly.com/catalog/malmobcode>

*Author of Honeypots for Windows (Apress)

SecurityFocus BASICS: RE: Remote Desktop vs VPN on Windows 2003

[*http://www.apress.com/book/bookDisplay.html?bID=281](http://www.apress.com/book/bookDisplay.html?bID=281)

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

From: Rhett Grant [mailto:rgrant@nextsequence.com]

Sent: Tuesday, January 18, 2005 6:22 PM

To: 'Paris E. Stone'; Roger A. Grimes; 'Jeff Randall'; security-basics@securityfocus.com

Subject: RE: Remote Desktop vs VPN on Windows 2003

Hi Roger,

68.106.158.136:33000 WinXP Pro

68.106.158.136:33001 Win2003 Enterprise

Here is what the rest of my scan picked up

PORT STATE SERVICE

25/tcp open smtp

110/tcp open pop-3

111/tcp filtered rpcbind

136/tcp filtered profile

137/tcp filtered netbios-ns

138/tcp filtered netbios-dgm

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

27374/tcp filtered subseven

33000/tcp open unknown

33001/tcp open unknown

33002/tcp filtered unknown

33003/tcp filtered unknown

If someone was looking to hack your network your security through obscurity would not work (yes you can get around the simple virus's with are only looked for certain ports). All it means is someone have to spend 5 more mins discovering what these open ports are. And there are so many auditing tools out there that can automate telling me what these open ports are. I just chose a simple port scan. Will this kind of security work??? For a novice or script kiddies, maybe...., but not someone that has an interest in your network, no way. Just my 2¢

I would take Paris advice and put some real security up.

By the way, what book is it? ;)

Rhett

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

From: Paris E. Stone [mailto:pstone@alhurra.com]

Sent: Tuesday, January 18, 2005 2:20 PM

To: Roger A. Grimes; Jeff Randall; security-basics@securityfocus.com

Subject: RE: Remote Desktop vs VPN on Windows 2003

And that domain (host or domain) is not protected by a firewall?

No IDS?

RE: Remote Desktop vs VPN on Windows 2003

SecurityFocus BASICS: RE: Remote Desktop vs VPN on Windows 2003

No IPS?
No honeypots?

My error in my original post was not in being clear, so, restated.

Security through Obscurity, by it's self is not security at all.

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

From: Roger A. Grimes [mailto:roger@banneretcs.com]
Sent: Tuesday, January 18, 2005 1:53 PM
To: Paris E. Stone; Jeff Randall; security-basics@securityfocus.com
Subject: RE: Remote Desktop vs VPN on Windows 2003

Security through obscurity is a type of security, and it works...just not in a vacuum...and not alone.

Almost all major Internet worms would have be rendered defenseless by simply changing the port number one port up. 99.9% of hacks are automated using worms, viruses, and malicious scripts. Almost of of them (9999.99%) only look on the default port. Fastest worm ever..SQL Slammer...only worked on the default SQL port. Code Red...only port 80.

Spambots look for ports 25 and 80. FTP exploits ONLY look for port 21. I could go on and on.

Security by obscurity works, and works well. Come find my RDP port on my domain at banneretcs.com. Prize (free book) to the first person who finds it. Go.

Roger

*Roger A. Grimes, Banneret Computer Security, Computer Security Consultant *CPA, CISSP, MCSE:
Security (NT/2000/2003/MVP), CNE (3/4), CEH, CHFI
*email: roger@banneretcs.com
*cell: 757-615-3355
*Author of Malicious Mobile Code: Virus Protection for Windows by O'Reilly
*<http://www.oreilly.com/catalog/malmobcode>
*Author of Honeypots for Windows (Apress)
*<http://www.apress.com/book/bookDisplay.html?bID=281>

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

From: Paris E. Stone [mailto:pstone@alhurra.com]
Sent: Tuesday, January 18, 2005 10:40 AM
To: Roger A. Grimes; Jeff Randall; security-basics@securityfocus.com
Subject: RE: Remote Desktop vs VPN on Windows 2003

"Security through Obscurity" i.e. put it on a different port, is not security at all.

Rdesktop on the internet, is generally a bad idea, no matter what port it runs on.

SecurityFocus BASICS: RE: Remote Desktop vs VPN on Windows 2003

Put a firewall in front of it if possible, if not, run a software firewall and then add openvpn.

www.openvpn.net is free, and will allow IPSEC connectivity that you can use to access the machine, then you get MSTSC(remote desktop) access over the tunnel.

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

From: Roger A. Grimes [mailto:roger@banneretcs.com]
Sent: Friday, January 14, 2005 5:16 PM
To: Jeff Randall; security-basics@securityfocus.com
Subject: RE: Remote Desktop vs VPN on Windows 2003

I can think of NO reason not to use Remote Desktop. Remote Desktop is fast and secure. Everything is encrypted past the logon name. To get additional security assurance, change the default TCP port from 3389 to something randomly high...like 58645 (which you can do with a regedit on the server...just google it). Then add the new port number to your server address...like www.example.com:58645.

Roger

*Roger A. Grimes, Banneret Computer Security, Computer Security Consultant *CPA, CISSP, MCSE: Security (NT/2000/2003/MVP), CNE (3/4), CEH, CHFI
*email: roger@banneretcs.com
*cell: 757-615-3355
*Author of Malicious Mobile Code: Virus Protection for Windows by O'Reilly *<http://www.oreilly.com/catalog/malmobcode>
*Author of Honeypots for Windows (Apress)
*<http://www.apress.com/book/bookDisplay.html?bID=281>

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

From: Jeff Randall [mailto:Jeff.Randall@ksg-llc.net]
Sent: Thursday, January 13, 2005 3:23 PM
To: security-basics@securityfocus.com
Subject: Remote Desktop vs VPN on Windows 2003

I have setup a web server running win2k3 and was curious about remotely accessing it with an XP box. Only one requirement, it has to be FREE.
=20

Here is what I have setup and as of now working but I would like in the end to only run one.

1. RRAS using PPTP. It's not a DC so I use local accounts.
2. VNC. TiteVNC to be specific.

RE: Remote Desktop vs VPN on Windows 2003

SecurityFocus BASICS: RE: Remote Desktop vs VPN on Windows 2003

3. Remote Desktop – went into the admin tools and set the encryption level to high.

Please no crazy setups like upgrade to DC and run IAS for Radius or running IPSEC tunnels, just would like peoples thoughts on the security level of each of these programs and what they feel are the most secure. If you can get specific about encryption, keys, key lengths, that would be great. Thanks

--

No virus found in this incoming message.
Checked by AVG Anti-Virus.
Version: 7.0.300 / Virus Database: 265.7.0 - Release Date: 1/17/2005

--

No virus found in this outgoing message.
Checked by AVG Anti-Virus.
Version: 7.0.300 / Virus Database: 265.7.0 - Release Date: 1/17/2005