

RE: Remote Desktop vs VPN on Windows 2003

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-01/0251.html>

From: Paris E. Stone (*pstone_at_alhurra.com*)

Date: 01/19/05

Date: Wed, 19 Jan 2005 11:11:03 -0500

To: "Roger A. Grimes" <roger@banneretcs.com>, "Joe Dumass" <joe_dumass@hotmail.com>, <security-ba

If you are getting that volume of traffic, I am sure your ISP is not pleased with all the extra traffic they are having to route.

And to issue such an open "come and get me" is careless if not reckless. You have, for all intents and purposes, eliminated any legal recourse you could have, and any protections for yourself by issuing such a statement.

"Well your honor, they did compromise my server, and yes, they did use it to launch a DoS against ebay.com, but I don't think that a judgement of 2 million dollars is appropriate simply because they were offline for 3 days."

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

From: Roger A. Grimes [mailto:roger@banneretcs.com]

Sent: Tuesday, January 18, 2005 5:35 PM

To: Joe Dumass; security-basics@securityfocus.com

Subject: RE: Remote Desktop vs VPN on Windows 2003

If I was supposed to do it, the RFC would say NEVER do it. But the protocol actually has the flexibility built in.

As long as the Internet is an unsafe place, I will move my ports around unless I need the standardization part.

BTW, so far 20,000 scans against my system, only 5 guesses, no one close...nothing creative. I'm sure I'll start to see the slow port scans come in soon.

Roger

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

From: Joe Dumass [mailto:joe_dumass@hotmail.com]

Sent: Tuesday, January 18, 2005 4:21 PM

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

Subject: RE: Remote Desktop vs VPN on Windows 2003

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

I think that the problem with arbitrarily assigning services to non-standard ports is that it disrupts the flow of communication. Is it somewhat more secure against worms, etc? Maybe... but the protocol definition exists to define how to standardize communication for a reason. If our partners go out and redefine https to non-standard ports, we would have to open new rules in our firewalls to allow communication to them, resulting in a less secure environment than simply allowing out-bound 443, and more of an administrative burden of trying to remember what outbound 8888, 4422, 1192, 65213, etc are.

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

From: Roger A. Grimes [mailto:roger@banneretcs.com]
Sent: Tuesday, January 18, 2005 12:53 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

RE: Remote Desktop vs VPN on Windows 2003

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

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.

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

SecurityFocus BASICS: RE: 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.
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