Global Information Assurance Certification Paper

Securely Operating Windows Terminal Services/Remote Desktop in a Multiplatform Environment

by Keith Lawson

February 23, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment: Version 1.4b (Option 1)

Table of Contents

Trademarks

The following terms are trademarks of other companies:

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

LINUX is a registered trademark of Linux Torvalds

VMware, the VMware "boxes" logo, Multiple Worlds, GSX Server, and ESX Server are trademarks of VMware, Inc.

Other company, product, and service names may be trademarks or service marks of others.

ABSTRACT
This paper will discuss Microsoft Windows Terminal Services (TS) and Remote Desktop (RD) servers. An overview of the technology will be reviewed and compared to other similar products that either complement or compete against TS/RD. A discussion of overall Information Technology (IT) security will be assessed regarding how it relates to TS. Specific security relating to the configuration of the servers and services will be examined as well as security around underlying protocol Remote Desktop Protocol (RDP) used to transmit data through the network. A review of details in the configuration of the management tools needed to run the TS and RD servers will follow. Also the paper will outline security recommendations for each of the operating systems on servers and workstations relating to TS and the Terminal Services Client (TSC) or Remote Desktop Client (RDC). The focus of the TS/RD clients in this paper are the most common multiplatform computing environments and specifically the following Operating Systems (OS): UNIX/Linux, Mac OS X, and Windows. Next the paper will look briefly at the benefits and weaknesses of the software and protocol used by Microsoft in this technology. By taking the steps necessary to secure the computing environment, TS/RD can provide benefits in reduced costs, user and administrator convenience, and reuse of computing resources.

INTRODUCTION
As technology evolves companies, such as Microsoft and many other large software providers, continue to offer creative ways for users and administrators to access systems. By using TS and RD services in today's computing environment executives are looking for ways to reduce cost and improve productivity. Technology similar to Microsoft's Terminal Services is trying to provide the ability to give companies and organizations increased productivity and cost benefit. Although this paper's primary focus is on Microsoft's thin client server and Remote Desktop solution, other companies exist and provide similar functionality to organizations today. VMware[i], Citrix[ii], NeTraverse[iii], Microsoft's Virtual PC (Formerly Connectrix)[iv] and other software vendors either have similar solutions to TS or provide add on features. As technology has evolved over the years Microsoft has been trying to produce products that will take the place of the other 3rd party solutions that run on their operating systems and have organizations use to their products instead. Citrix provides a solution that offers the functionality of Microsoft's terminal services to an array of different system OS platforms with additional security and productivity features. Since the release of the latest development of RDP 5.X Microsoft is catching up with the functionality that Citrix and other vendors provide.

As with most technology, Microsoft's Terminal Services will operate on a network

[i] URL:http://www.vmware.com/
[ii] URL:http://www.citrix.com/
[iii] URL: http://www.netraverse.com
[iv] URL: http://www.microsoft.com/windowsxp/virtualpc/

infrastructure that must be secure. The security starts with the engineers who design the networks from the core routers, switches, firewalls, servers, etc., to the policy documents, and foundations or business case for use of the network. These topics will be left for another discussion, but some understandings of security essentials are important to using technology securely and Microsoft's Terminal Service is no different.

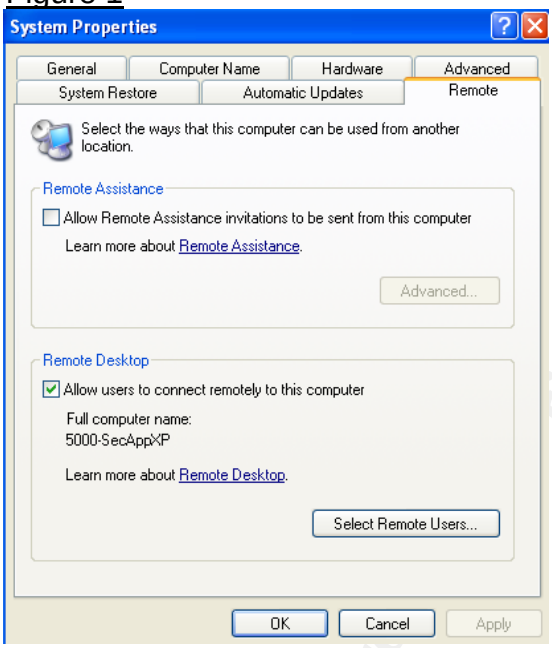
When starting to look at security around a specific technology, it is important to review some documents that will give you an overall understanding of fundamentals of network security. Some of these resources can be found at the following locations: the National Institute of Standards (NIST) Computer Resource Center[v], SANS Reading Room[vi], Microsoft Security Guidance Center[vii] and other computer security resources such as TruSecure[viii] and Security Focus[ix].

CONFIGURE HOST MACHINES

Microsoft Terminal Services and Remote Desktop technology is offered as in two primary installation or licensing packages: Remote Control/administration and the traditional thin-client Terminal Services. From Server NT 4 through Server 2003 Microsoft has been offering both functionalities to its users. The server platform of TS has matured over the years and provides benefits of more mature software. Also as Microsoft matures its software they are always looking at ways to mature their revenues and expand the features into different areas of their business. One way that this expansion is taking place today is with the new Remote Desktop and Remote Assistance features built into the latest Microsoft desktop Operating System Windows XP. Remote Assistance is a means of allowing others such as help desk, technical friends, or support representatives to view issues on a computer. Remote Desktop is similar to the mature TS connection that is offered by the Server Family of Microsoft OSs.[1] To enable Remote Assistance or Remote Desktop on your XP Professional system (Note: XP Home Edition does not include RD) one must access the "System Properties" control panel by either accessing it through the XP control panel and opening "System" or by right clicking on "My Computer" or choosing "Properties". Once you have this control panel on your screen click on "Remote" and you can configure your XP machine for RD.

[v] URL: http://csrc.nist.gov/
[vi] URL: http://www.sans.org/rr/
[vii] URL: http://www.microsoft.com/security/guidance/default.mspx
[viii] URL: http://www.trusecure.com/
[ix] URL: http://www.securityfocus.com/

Figure 1



Remote Desktop on the Windows XP system also uses RDP for transmitting across the network at layer four, transport (TCP) layer, in the Open System Interconnect (OSI) model.[2 (p. 63)]

Microsoft TS was initially developed to provide thin client connections for Windows 9X and NT clients. Early deployments of Windows NT Server 4.0, Terminal Server Edition (TS 4.0) were primarily focused on the performance of the protocol. Microsoft's RDP is the core behind the technology. "When TS 4.0 was release, RDP was a new protocol based on an existing ITU T.120 family of protocols."[3 (p. 4)] Later RDP 5.0 was developed and is used today which provided greater performance, scalability and additional features. The basis for the security of the protocol is encryption. Without encryption, one could "sniff"[x] the network and potentially compromise the server and network by gathering information such as passwords. "Every version of RDP uses RSA Security's RC4 cipher, a stream cipher designed to efficiently encrypt small amounts of varying size data. RC4 is designed for secure communications over networks, and is also used in protocols such as SSL, which encrypts traffic to and from secure web sites."[3 (p. 4)] Typically SSL is a generally acceptable form of data encryption and therefore one could deduce that RDP is acceptable. RC4 cipher (128-bit) is a generally acceptable encryption for most environments. With the release of Microsoft's latest server operating system, Windows Server 2003 released around first quarter 2003, RDP encryption has taken yet another step in

[x] sniff v.,n. 1. To watch IP packets traversing a local network. Most often in the phrase `packet sniffer', a program for doing it. [5] or 2. sniffing: A synonym for "passive wiretapping" [2]

the right direction. RDP, new version 5.2, has now incorporated Federal Information Processing Standard (FIPS) 140-1 compliant encryption algorithms as an option for encrypting RDP traffic across a network. This new version's features help those who wish to use RDP in a government/federal agency, which is required to protect unclassified information within computer systems to the mandate of FIPS 140 standards[xi].

TS encryption on Windows 2000 server can be set to one of three security settings: 'low' encryption only encrypts data from client to server and is a 56-bit key (this protects sensitive information such as passwords), 'medium' encryption with is the default and is bi-directional 56-bit key encryption, or 'high' encryption is bi-directional and uses 128-bit key which can be enabled after installing Windows 2000 High Encryption Pack.[3 (p. 6)] To offer the best security of TS, the 'high' encryption setting on your server software should be used. On Windows Server 2003 Microsoft has made some minor changes to the encryption settings. Now four options exist:

- *Low: This level encrypts data sent from the client to the server using 56-bit encryption, helps secure the user logon information and data that is sent to the server, but does not encrypt the data that is sent from the server to the client. Microsoft recommends that you use this encryption level in an intranet environment.*
- *Client Compatible: This level encrypts data sent between the client and the server at the maximum key strength that the client supports. Use this level when the terminal server runs in an environment that contains mixed or earlier-version clients.*
- *FIPS Compliant: This level encrypts and decrypts data sent from a client to the server and from the server to a client with the Federal Information Processing Standard (FIPS) encryption algorithms by using the Microsoft cryptographic modules.*
- *High: By default, Windows Server 2003 uses this level of encryption. High encryption encrypts the data transmission in both directions by using a 128-bit key. Microsoft recommends that you use this encryption level if the network is not secure and is located in North America. Use this level when the terminal server runs in an environment that contains 128-bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption cannot connect.*[4]

As stated above, the recommended security setting for Server 2003 is the same as it was with Server 2000 but now Microsoft has offered the "Client Compatible" option for ease of use (not recommended) and "FIPS Compliant" option for federal agencies or organizations that have adopted FIPS policy requirements.

Some suggested standard RDP Best Practices include the following administrative functions[2 (p. 1348)]:

[xi] URL: http://csrc.nist.gov/publications/fips/fips140-1/fips1401.htm

- Apply latest Service Pack and hot fixes.
- Block unwanted TCP/3389 traffic at firewall.
- Get latest version of thin client software from Microsoft.
- Require 128-bit (High) RDP encryption at server.
- Use IPSec or a VPN instead of RDP encryption when data is sensitive.
- Disable Remote Desktop and Remote Assistance on XP workstations if not needed.
- Require password and a short TTL for Remote Assistance initiations.

Other RDP security suggestions include the following session settings: end a disconnected session at 30 minutes, set active session limit to "Never" (Default), set idle session limit to "10 minutes", and when session limit is reached or connection is broken "End session."[5] Another source of TS best practices is to configure user properties. Microsoft recommends to the following user properties specifically in Server 2003[6]:

- *Use Terminal Services-specific groups*
  Create User Groups that are specifically for Terminal Services users.

- *Use Terminal Services-specific profiles*
  Assign a separate profile for logging onto Terminal Services.

- *Use mandatory profiles*
  Use a mandatory Terminal Services profile that is created to suit the needs of all of the different types of clients and that provides the best server performance.

- *Set time limits*
  Setting limits on the duration of client connections can improve server performance.

- *Use Starting program*
  If you have users who need access to only one application on the terminal server, use the Starting program option.

- *Create preconfigured connection files for users or groups of users*
  To make connecting to Terminal Services easier, you can supply users with preconfigured connection files.

Configuring the encryption level to high 128-bit RC4 encryption level in (Windows Server 2000 Family) or FIPS Compliant Encryption (Windows Server 2003 Family) for TS and RD can be configured on the server in the Terminal Services Configuration (tscc) Microsoft Management Console (MMC) software. To enable 'high' encryption on Server 2000 or 'FIPS Compliant' encryption on Server 2003 refers to the figures below. Because there are only minor differences (primarily the FIPS Compliant option) between Terminal Server 2000 and 2003 our figures includes screen prints from TS 2003 to show both.

Changing encryption level within Terminal Services Configuration utility

1. Open TS Configuration Utility:
   - Start->Program Files->Administrative Tools->Terminal Services Configuration utility

   OR
   - Start->Settings->Control Panel->Administrative Tools->Terminal Services Configuration utility

Figure 2 (Server 2000):

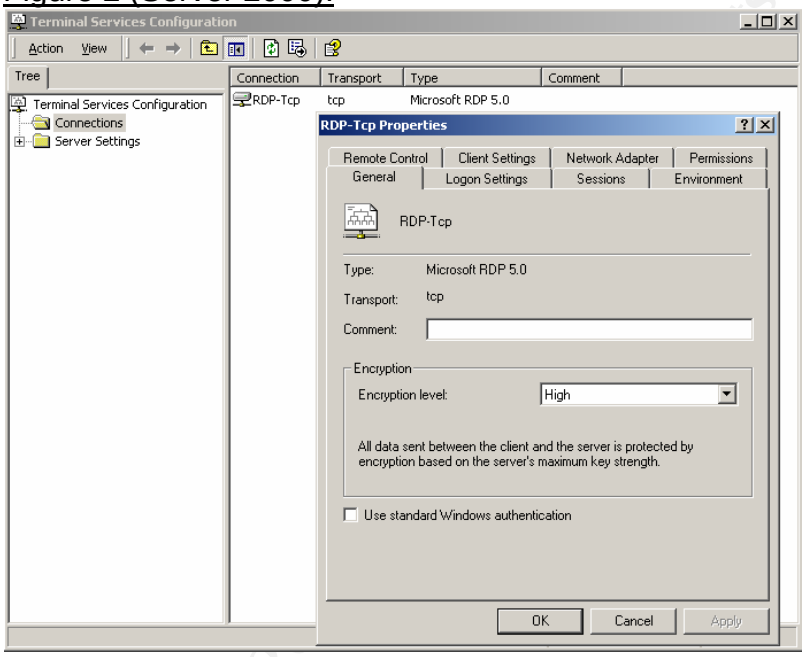
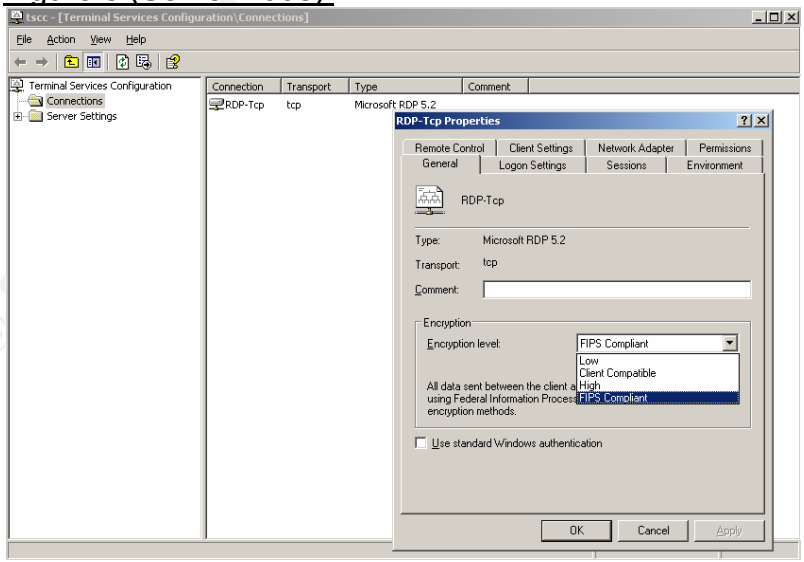


Figure 3 (Server 2003):



The details of security and configuration of the TS/RD product outlined above provide for a good understanding of some options that security administrators

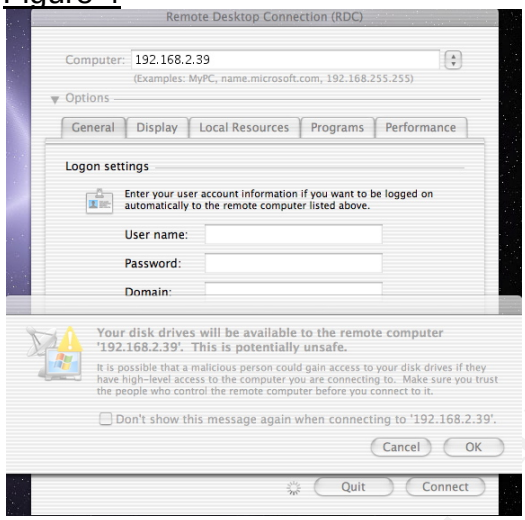
have when securing this product. It is recommended to configure and architect your TS/RD Servers by using the standard security methodology of Defense-in-Depth. Configure your networks with multiple layers to require an attacker to have to penetrate and overcome the challenges of each security layer that you place in your environment.[2 (p. 292)] Some suggested Windows Security and Terminal Services guides can be accessed by the following URLs:

- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/w2ktsscl.asp
- http://www.microsoft.com/downloads/details.aspx?FamilyId=9964CF42-E236-4D73-AEF4-7B4FDC0A25F6&displaylang=en
- http://csrc.nist.gov/pcig/CHECKLISTS/01-20-2004-DOT-SBCS-Win2K.doc
- http://csrc.nist.gov/pcig/CHECKLISTS/win2k-checklist012304.zip
- http://www.nsa.gov/snac/index.html
- http://www.cisecurity.org/bench_win2000.html
- http://www.hp.com/sbso/productivity/howto/it_windowsxp/security.html

CONFIGURE REMOTE MACHINES

As the TS/RD technology has progressed over the years it has become more popular with system administrators and central application users. As the popularity grows with Linux and Mac OS X, remote Windows computing have become more popular for secondary Windows users and administrators. Users and administrators can have UNIX and Mac based desktop workstations and is able to access their Windows servers at the same time without physically having the Windows servers close by or having a Windows client on their desktop. Since the encryption of RDP is implemented on the server as previously discussed, the client system can be configured with the client alone. Some common best practices when using Remote Desktop Client software is to only connect when you specifically need to use the system. Disconnect when you are finished or are not going to be using the system. Do not share resources such as: drives, printers, or ports. Also, if you do share these resources, disconnect the devices after you have completed your resource sharing even if you must continue use of the remote computer. In the Microsoft clients, for Mac and Windows, a warning about local resource sharing will alert you if you establish this type of connection. Below you will see the warning given by a Macintosh RD client when attempting to connect with local drive resources shared.

Figure 4



TS/RD offers benefits to the traditional UNIX administrator and users who are required to manage or use some Windows machines. Most UNIX administrators are already familiar with exporting X-Windows from different UNIX systems for remote connectivity. With the development of rdesktop, an open source terminal services client, UNIX administrators can configure their UNIX desktop to manage their Windows TS/RD systems as well without purchasing additional software such as Citrix. In the computing world today, administrators are working on multiple platforms across entire enterprise LANS, so having the ability to remotely control systems is a huge benefit.

Configuring the rdesktop software is relatively simple for most UNIX users and administrators. The software can be downloaded in source form from SourceForge[xii] or the developer's Remote Desktop Site[xiii]. Using the software on most Linux and UNIX distributions simply require compiling the source code and installing the compiled code. Specifically on a typical GNU-style system the build procedure is as follows:

```
% ./configure [options]
% make
% make install
```

Once you have installed the software you can run the software in X-Windows by running the command "rdesktop" from a command line. The latest version of this open source software was written utilizing RDP 5 by default and will allow this protocol to be reduced by a flag when starting the program. This program has limited performance and features compared to the latest clients for Microsoft Windows and Mac OS X but the client still supports 'high' encryption when

[xii] URL:http://sourceforge.net/project/showfiles.php?group_id=24366&package_id=1660&release_id=211668
[xiii] URL: http://www.rdesktop.org

configured on the server. One core aspect of security and Defense-in-Depth is securing all systems that connect to the network. Securing this remote UNIX user can be accomplished by hardening or security the workstation. Review the links[xiv,xv] below for some references to securing a UNIX workstation.

RD for the Macintosh is limited to the latest OS versions 10.2 (Jaguar) and 10.3 (Panther) but supports RDP 5.1 and has all of the performance and functionality issues of RDP 5 that was previously discussed. The software for the Macintosh is very easy to install and only requires downloading the .bin or .hqx file from Microsoft's Mactopia[xvi] web site and copying the installation folder to your system. After the copy has been completed the software can be run and connection to the TS Server can be established. As with the UNIX systems it is recommended that some Macintosh client security configurations are setup. To secure your Macintosh system, review the following document[xvii] and web site[xviii] for additional assistance.

The client software for Microsoft Windows RDC systems will run on Windows 3.11 (Workgroups), 9x/Me, NT, 2000, XP, Server 2003, and CE devices. A few of these operating systems are very outdated or unrealistic platforms for most TS users; therefore, the security of Windows 9X, NT, 2000, XP and Server 2003 clients will be this paper's focus. All of the Windows clients can be used to access terminal services securely using built in encryption with the clients and their operating systems. Windows systems have many potential vulnerabilities and security issues that can be controlled to some extent.

When configuring a RDC on 9x/Me systems, which inherently do not have security built-in, it is recommended that these systems only be used as "thin clients" to the TS servers. Administrators should implement the few controls that can be placed on these systems and inform users to store all data on the TS Servers. The controls that SANS[2 (p. 1139)] recommends to place on these 9x/Me systems are: installing the Active Directory Client Extensions (ADCE), upgrading to enable NTLMv2 support, and mapping drive letters to a remote server for all document storage, etc. Other controls can be placed on these systems that will not allow users to configure or install additional software. One such software product that can be used is OnGuard[xix] secure desktop control software. With these controls and proper policy documents in place the use of these older

---

[xiv] URL: http://www.nsa.gov/selinux/index.html
[xv] "Secure OS Environments for Linux." 2003. URL: http://www.sans.org/rr/papers/index.php?id=1083. (April, 2003)
[xvi] URL:http://www.microsoft.com/mac/downloads.aspx?pid=download&location=/mac/DOWNLOAD/MISC/RDC.xml&secid=80&ssid=9&flgnosysreq=True
[xvii] "MacOS X: User Friendlier Security for UNIX." 2003. URL: http://www.sans.org/rr/papers/index.php?id=1282
[xviii] URL: http://www.apple.com/macosx/features/security/
[xix] URL: http://www.poweronsoftware.com/products/onguard/

systems can be relatively secure and can reduce cost of upgrading to newer systems. The concept discussed here is similar to that of configuring a bastion host[xx].

Windows NT was the beginning of a more secure Microsoft OS. The security built into this OS includes many features, which were a huge improvement from previous Windows OSs. In today's computing world, Microsoft has officially declared NT an abandoned product line considers it dead. Due to the facts that the vendor does not support NT and that its successors 2000, XP, and 2003 (.NET) have many security and overall system benefits companies and organizations should upgrade if finances permit. For those who cannot upgrade specific NT Workstations and Servers that will be accessing data via TS, it would be recommended to follow some steps to making these systems bastion hosts. As of October 2003, Microsoft is issuing some security patches for NT and even 2000, which support was previously halted. But it could be expected that in the next few years or sooner support of NT would be discontinued. For references on making your older systems into secure bastion hosts refer to the following resources.[5]

The most recent Microsoft workstation OS is XP Home and Professional Edition. Prior to XP, Microsoft released Windows 2000 Professional. These OSs along with the server versions of 2000 and 2003 have also made security enhancements. Because of the security enhancements as well as performance improvements the latest Microsoft OSs make good clients to their TS/RD technology. Furthermore, with the latest development and security of RDP 5.2 (Default on Server 2003) the clients offered by Microsoft for their workstation OS will allow users to take advantage of the security benefits. Configuring the Microsoft RDC only requires downloading the latest client from the Microsoft download site[xxi] and running the installation package on the client system. The latest version 5.2.X will run on the following list of Microsoft[7]:

> **Supported Operating Systems:** Windows 2000, Windows 2000 Service Pack 2, Windows 2000 Service Pack 3, Windows 95, Windows 98, Windows 98 Second Edition, Windows ME, Windows NT, Windows Server 2003, Windows XP, Windows XP Media Center Edition

Again, the concept of Defense-in-Depth applies to these systems as well and it is recommended to address as many security concerns as possible when deploying the Microsoft Client workstations as well as the other platforms.

[xx] bastion host[2 (p. 1293)] n. 1. A machine which has been hardened specifically in anticipation of vulnerabilities that have not been discovered yet.

[xxi] URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=a8255ffc-4b4a-40e7-a706-cde7e9b57e79&displaylang=en

BENEFITS

TS/RD offers multiple benefits to those who implement a secure solution. Many times a secure solution is not an inexpensive solution but with the TS and proper Server Systems administration this solution can be less costly than implementing and maintaining the LAN environment that already exists in most organizations. Also, due to the lack of software needed on the "thin client" machine users and administrators do not have the issues of as many viruses and vulnerable systems as in a typical LAN environment. As briefly discussed previously many of these "thin client" systems are being configured as bastion hosts by hardening and removing services not needed or by installing software that controls access control on these systems. One of the primary benefits for a TS/RD enterprise solution is Data Security. By limiting the access to data directly through all workstations and servers the TS Server solution puts more emphasis on the servers that typically are controlled closer in most organizations.

> *"Data Security - Most security failures do not happen because of technology failures, but because the technology was not configured and managed properly. By eliminating the storing of corporate information on local PC and remote office server hard drives, the tasks of managing backups, monitoring access, and providing database synchronization are dramatically transformed and reduced."*[8]

Other typical benefits include, but are not limited to, bandwidth reduction, remote administration capabilities, reduced travel costs, and increased productivity for regular users and personnel who do not work from one office.[9] The remote connectivity is ultimately only as secure as the server and the architecture security within the organization. To implement everything correctly supporting documentation on baselines, auditing, and policy must coincide with the technical implementation of the server and clients.

WEAKNESSES/VULNERABILITIES

Like most software, Terminal Services and RDP are vulnerable to attack. Enumerating TS can be accomplished by using search engines, port scanning RDP default port 3389, or using tools like TSProbe.exe or TSEnum.exe to check for vulnerabilities. Tools for attacking the TS vulnerabilities also exist and security administrators should be aware of such attacks to defend against them. Some of the attacks are as follows:

- Password Grinding Attack
- User Privilege Elevation Attacks
- IME Remote Root Compromise
- Malformed RDP Denial of Service[10 (p. 309)]

See the reference[11] below for more detail on these vulnerabilities and attacks and procedures to defend against them.

An excellent resource for finding TS Vulnerabilities by categories is the Security Focus Vulnerability archive[xxii] and specifically by selecting “Microsoft” as “Vendor” with “RDP” and ”TSAC AcitiveX Control” as “Title”. Other databases exist for security administrators who would like to search for specific vulnerabilities. One of the more respected organizations that offer alerts is Carnegie Mellon University’s CERT® Coordination Center (CERT/CC) [xxiii].

CONCLUSION

Security of Microsoft’s Terminal Services and Remote Desktop technology is a challenge yet the tools do provide benefits to organizations in security and business challenges. Security best practices and Defense-in-Depth, which are standard concepts for securing Information Technology, are very relevant with TS/RD deployments. Specifically securing servers that run the TS and RD services is a must to acquire a secure environment. Additional third party software exists can improve the security and should be considered if funds allow. Overall good IT security comes down to practicing common sense, doing your research, and assuring that measures are in place to protect your resources. Security of TS/RD finally comes down to following guidelines outlined in security essentials[2] and building a layer of defense around the IT environment that will house the Windows Terminal Services or Remote Desktop systems.

[xxii] URL: http://www.securityfocus.com/bid/vendor/
[xxiii] URL: http://www.cert.org/nav/index_red.html

DOCUMENT REFERENCES

[1] "Solutions - IT guides; Windows XP and desktop management." 2004. URL:http://www.hp.com/sbso/productivity/howto/it_windowsxp/important_benefits.html. © 2004 Hewlett-Packard Development Company, L.P.

[2] Cole, E. AND Fossen, J. AND Northcutt, S. AND Pomerantz, H. SANS Security essentials with CISSP CBK, Volume 2, Version 2.1: The SANS Institute. 2003.

[3] "Remote Desktop Protocol (RDP) Features and Performance." 2000. URL:http://www.microsoft.com/Windows2000/techinfo/howitworks/terminal/rdpfandp.asp (June, 2000)

[4] "HOW TO: Secure Communication Between a Client and Server with Terminal Services." 2003. URL:http://support.microsoft.com/default.aspx?kbid=816594. (Dec, 2003)

[5] Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. O'Reilly & Associates, Inc. 2001.

[6] "Terminal Services User Properties." 2003. URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/ts_usr_bestpractices.asp. (2003)

[7] "Remote Desktop Connection for Windows Server 2003 [5.2.3790]." 2004. URL:http://www.microsoft.com/downloads/details.aspx?FamilyID=a8255ffc-4b4a-40e7-a706-cde7e9b57e79&DisplayLang=en. (March 2003)

[8] "Using Access Infrastructure to Architect Improved Security." 2004. URL:http://www.thinplanet.com/opinion/security.asp. (Jan. 2004)

[9] "J.D. Edwards Improves Manageability and Expands Sales Capabilities Using Windows 2000 Terminal Services." 2001. URL:http://www.microsoft.com/windows2000/server/evaluation/casestudies/jdedwards.asp. (May 2001)

[10] Scambray, Joel AND McClure, Stuart. Hacking Exposed Windows 2000: Network Security Secrets & Solutions. Osborne/McGraw-Hill. 2001.

Last Updated: June 25th, 2018

Upcoming Training

SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Annapolis Junction SEC401	Annapolis Junction, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Riyadh July 2018	Riyadh, Kingdom Of Saudi Arabia	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Mentor Session - SEC401	Ankara, Turkey	Aug 08, 2018 - Oct 03, 2018	Mentor
Northern Virginia- Alexandria 2018 - SEC401: Security Essentials Bootcamp Style	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Mentor Session AW - SEC401	Raleigh, NC	Aug 22, 2018 - Aug 29, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201809,	Sep 11, 2018 - Oct 18, 2018	vLive
SANS Munich September 2018	Munich, Germany	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
Mentor Session - SEC401	Columbia, SC	Oct 02, 2018 - Nov 13, 2018	Mentor
SANS London October 2018	London, United Kingdom	Oct 15, 2018 - Oct 20, 2018	Live Event