Global Information Assurance Certification Paper

Windows NT Remote Access Service (RAS) Secure Configuration

Remote Access Service (RAS) provides a means for remote Windows NT systems to connect to a LAN across a dial-up connection. RAS is simply a remote extension of a Windows NT Network. It is a remote client connection. The local corresponding system acts as a router for the remote RAS client. All traffic to and from the remote system passes through the local system. The application processing is done on the local system as well.

RAS consists of a server and a client portion. The server authenticates the client and manages the connection. RAS provides mechanisms to protect a potentially insecure connection between server and client. To take full advantage of the RAS security functions, a RAS server must be used in conjunction with a RAS client. These mechanisms include authentication, encryption and dial-back functions.

RAS provides three authentication protocols. Each protocol uses a different handshaking technique and may offer the use of various encryption algorithms. They are CHAP, SPAP, and PAP.

- CHAP (Challenge Handshake Authentication Protocol) is the most secure of the three RAS authentication protocols. One of two encryption algorithms can be chosen when using CHAP: DES or MD5. DES is the default option used by CHAP. MD5 is the recommended encryption algorithm.

- SPAP (Siva Password Authentication Protocol) is a proprietary secure authentication.

- PAP (Password Authentication Protocol) should not be used. There is no encryption of the authentication process under PAP. It is usually used when a client is not able to use one of the other methods.

RAS Encryption

- Windows NT provides protection against data capture through link-based encryption. Link-based encryption will encrypt all network packets that are bound for a RAS connection and decrypt all packets that have been received from RAS connections. The algorithm used for providing link-based encryption in Windows NT is RSA Data Security's RC4.

RAS Dial-Back

- Windows NT provides a built in alternative to dial-back modems. RAS permits administrators to enable dial-back functions to heighten security. The modem requires no dial back functionality. The NT RAS server authenticates the user, terminates the connection, and calls back the user at a prearranged number.

Secure Configuration of RAS

- Before installing and configuring Windows NT RAS, considerations should be made as to which servers require the use of RAS. RAS should only be installed on servers that require dial-up support.

- Each Windows NT server can support 256 active RAS sessions. This centralized access eases the administrative/security overhead.

- Installing the RAS server on a Windows NT server will not automatically permit all users to use RAS. The right to use RAS access must be specifically assigned by the administrator.

NOTE: After installing RAS on an existing NT 4.0 server you must reapply Service Pack 4 and any additional patches.

RAS Step by Step Server Configuration:

- Select Start, Settings, Control Panel
- Click Network Icon
- Select Services
- Highlight Remote Access Service
- Click Properties
- Highlight the port to configure
- Click the Configure button
- RAS server: Select Dial out and Receive calls in the Port Usage button
- For RAS client: Select Dial out only in the Port Usage button
- Click OK
- Click Network

For a RAS Server ensure:

- Ensure only the TCP/IP checkbox is checked in the dial out protocols section
- Ensure only the TCP/IP checkbox is checked in the Server Settings
- Select Require Microsoft encrypted authentication radio button

NOTE: ensure your clients use the CHAP authentication. Additionally, the use of link-based encryption is highly recommended. Link based encryption significantly increases security.

NOTE: Only allow remote access to the local RAS server not to the entire network.

- Configure TCP/IP: DHCP or Static
- Click OK to close the RAS server TCP/IP window
- For a RAS client ensure only the TCP/IP checkbox is checked in the Dial out Protocols section
- Click OK for Network Configuration Menu
- Click continue to close the RAS setup window
- Click close to close the Network window

RAS Permissions

By default, users are not permitted access to the RAS server remotely without explicit authorization from the system administrator. To allow user access to a RAS server:

- Select Start, Programs, Administrative Tools, User Manager
- Select the user account to be granted RAS dialin permissions
- Click the Dialin button
- Check Grant dialin permissions to user box
- Configure the Call Back settings appropriately.

Point to Point Tunneling Protocol

NT includes functionality to generate encrypted tunnels using Point to point tunneling Protocol (PPTP). PPP is an extension of the Point to Point Protocol (PPP). PPTP creates a secure tunnel by encapsulating normal data in to encrypted packets.

To enable PPTP:

- Right click the Network Neighborhood icon
- Select Properties
- Select Protocols
- Select the TCP/IP Protocol
- Click Properties
- Click Advanced
- Check the Enable PPTP Filtering box
- Click OK to close the Advanced IP Addressing window
- Click OK to close the Microsoft TCP/IP Properties window
- Click OK to close the Network window

RAS Auditing:

RAS can be enabled to generate records in the audit logs that indicate a number of activities, including normal connections, successful disconnection, successful callbacks, disconnects due to idle lines, timed-out authentication, and line errors. Excessive failed connections may indicate that someone is trying to break into an account. Administrators should make use of the logging and auditing facilities available.

Setting Registry parameters for RAS auditing:

- Select: Start, Run

- Type Regedt32.exe in the Open dialog box
- Select the Hkey_Local_Machine on the Local Machine window
- Navigate to \System\CurrentControlSet\Services\RemotAccess\Parameters
- Click the enable Audit key
- Ensure the value in the DATA filed is 1
- Click OK to close the DWORD Editor
- Exit the Registry Editor

Ross Coppage, (Ross3000@home.com)

References:

- Daily, Sean, "Whats New With NT 4.0 RAS " http://www.win2000mag.com/Articles/Index.cfm?ArticleID=586
- 281 Communications Web Support Board "Helpdesk Windows NT 4.0" http://www.281.com/281/config/winnt/nt40ras.html
- IOP's Technical Support Library, "Windows NT 4.0 RAS Setup" http://www.iop.com/support/winnt4/ntsetup.html
- Microsoft Administering NT 4.0 Official Curriculam, Pg 36 RAS
- Milione, Ron "RAS", "MCSE Core Exam Prep", Chapter 4, Section 4.2

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor