Global Information Assurance Certification Paper

Remote Access Security; A Layered Approach

Lane Melton
November 14, 2000

Overview

This paper will examine remote access security from a layered perspective utilizing the Remote Access Dial-In User Service (RADIUS) Protocol and CiscoSecure Software V2.4. It will briefly review the authentication, authorization, accounting process and its relationship to a Microsoft Windows NT user database, as well as access control lists (ACLs) residing on a router. It will not attempt to portray and explain a complete and all encompassing RADIUS compliant information system.

Introduction

In today's technological environment much attention is given to network security; particularly Internet or Web-based security. Protection of the associated information and systems is vital. Security policy should not only examine network protection from Internet or Web-based access, but also against unauthorized dial-in access. RADIUS is a protocol developed by Livingston Enterprises, Inc. to support authorization and accounting for dial-in users[1]. CiscoSecure ACS is the server software developed by Cisco Systems to utilize the RADIUS protocol.[2] Implementing the RADIUS protocol and combining it with CiscoSecure software and ACLs provides a good, layered defense against unauthorized remote dial-in access to a corporate network.

With the need for increased employee mobility in support of the brick and mortar workplace, remote dial-in access security has become an issue of great concern. The proper implementation and configuration of the RADIUS protocol and associated hardware and software will help harden remote dial-in access. The process of granting remote access should determine that a dial-in user is indeed who they say they are, provide limited, predetermined access to network and Internet resources and document or log the entire event. These requirements are known as the authentication, authorization and accounting (AAA) process supported by the RADIUS protocol and CiscoSecure software.

Remote Access Process

The single point of entry for a dial-in user is a modem bank (in this scenario) housed in a Cisco 3640 router running Cisco Systems IOS software. The router becomes one of two servers within this immediate system. By association between the two, the router becomes a Network Access Server (NAS). Its responsibility is to receive incoming calls, house configuration files and ACLs and send user information to the CiscoSecure AAA server. The CiscoSecure AAA server is run by CiscoSecure ACS software and can maintain a user database, set system configuration options and query external network systems and databases for information. Configuration files within the NAS will require the AAA process to take place every time a call is placed to the modem bank. An example portion of the NAS configuration file that prompts the AAA process to start is

shown below. This entry will require that the dial-in user provide a user id and password to be authenticated against a user database either within the AAA server or an external server such as a MS-Windows NT user database.

aaa authentication ppp default group radius *[Requires user to authenticate to a AAA server.]*
aaa authorization network default group radius *[Assigns group privileges to dial-in users.]*
aaa accounting network default start-stop group radius[3] *[Turns on accounting.]*

The user id and password will be compared to user information located within a configured CiscoSecure AAA server. If no information for that user is found, the AAA server will query (in an MS-Windows NT based network) the Primary Domain Controller (PDC) user database for the appropriate user id and password. If the user id is not found, the user will be denied access and the connection terminated. If the user id is found and the password matches the user will be authenticated.

After authentication, the user is granted authorization to predetermined resources. These resources can be governed by several things. Features such as time of day access, group assignment, AAA user id and password assignment, call back ability, IP Address assignment and modem port access can all be determined within the CiscoSecure ACS software. Authorization can also be granted by implementing an ACL within the NAS (the router). This list could determine if the dial-in user has the ability to sign-on to the corporate network or only have the ability to visit one or two locations on the web. The ACL below shows an example of a user that has the ability to be authenticated using their MS-Windows NT user id and password, log-on to the corporate network, visit two web locations and telnet to a specific location based on IP Address. The user however, will not have access to anything else except features specified by the ACL. The example below is also part of the NAS configuration file.

access-list 150 permit tcp any host (**IP Address for LAN Login**) eq 135 *[Allows LAN Logon]*
access-list 150 permit tcp any host (**IP Address for LAN Login**) eq 139 *[Allows LAN Logon]*
access-list 150 permit udp any host (**IP Address of WINS Server**) eq netbios-ns *[Allows LAN Logon]*
access-list 150 permit udp any host (**IP Address of for sending datagrams**) eq netbios-dgm *[Allows usage of datagram packets]*
access-list 150 permit tcp any host (**IP Address of telnet location**) eq telnet *[Allows telnet]*
access-list 150 permit tcp any host (**IP Address of web location**) eq www *[Allows link to WWW address]*
access-list 150 permit tcp any host (**IP Address of web location**) eq www*[Allows link to WWW address]*
access-list 150 permit udp any host (**IP Address of DNS Server**) eq domain *[Identifies DNS Server for authentication]*
access-list 150 deny ip any any *[Deny any IP Addresses, protocols or ports other than those listed above, last line of Access Control List]*[4]

The access list above specifically dictates based on IP Address the resources that a dial-in user can access. Resource location access is also based on traffic type such as udp or tcp. Using the deny statement will deny all traffic except that type that is specifically allowed by the criteria statements within the list itself.[5]

Based on remote access policy, the dial-in user may log into the corporate network. This

will be allowed only if the ACL, CiscoSecure ACS software and the network operating system are configured to permit this. While on the local area network, the dial-in user will usually have the same permissions as on site access; so this feature must be implemented with caution.

Once the user has been authorized, the session events are recorded in an event log. This log will record who logs in, the start and end time, idle time, IP Address, modem port entry, failed attempts and reasons for failed attempts. It can also notify an administrator of suspicious activity during the login process.

Advantages/Disadvantages

There are several advantages and disadvantages to using the RADIUS protocol and CiscoSecure system. The AAA process is a distinct advantage to the remote dial-in access community. There is a single point of entry into the system. This entry point is easily monitored and manageable. Users are authenticated by one of two ways. First, the user can be authenticated by the AAA server database and never has to rely on the corporate network for other resource access. Second users can be authenticated via the network operating system user database. This method eliminates any administrative duplication efforts and ties the two systems together. Authorization is based on either user or group imposed permissions set by the AAA server or the network server if so desired. Also an ACL residing on the NAS (the router) can dictate the resources available to each user and group. Accounting or logging features record session events as well as provide notification to administrators for suspicious activity.

There are also several disadvantages to this system. Recently it was discovered that CiscoSecure V2.1 - 2.4.3 was vulnerable to a DoS attack. The problem was corrected with a software upgrade.[6] Also the configuration file which contains the AAA information as well as the ACL is difficult to configure requiring the administrator to have fairly extensive experience with router configuration. The NAS (router) is also susceptible to standard router attacks. This aspect requires implementing additional security precautions for it.

Summary

The RADIUS protocol, combined with the CiscoSecure AAA system is a good, layered approach to security in the dial-in arena. It provides authentication, authorization and accounting features that protect the corporate network from undesired entry. The RADIUS protocol is not limited to only the PC or network server world. This versatile protocol can also be implemented in an AS/400 environment as well.[7] By incorporating the layered approach of authentication, authorization and accounting to remote dial-in security, corporate networks have an additional tier of security.

---

[1] Rigney, C., et. al "RFC#2058." "Remote Authentication Dial In User Service (RADIUS)" Jan. 1997 http://www.cis.ohio-state.edu/htbin/rfc/rfc2058.html

[2]Whitepaper. "Cisco IOS Technologies: RADIUS Support in Cisco IOS Software" June 30, 2000 http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iolk/tech/rdius_wp.htm

[3]Melton, Lane, et. al. "DHIAP RADIUS Supplemental Installation and Maintenance Guide" Page 10 April

2000 http://ips.aticorp.org/TR/index.html

[4]Melton, Lane, et. al. "DHIAP RADIUS Supplemental Installation and Maintenance Guide" Page 12 and 13 April 2000 http://ips.aticorp.org/TR/index.html

[5] Cisco Technical Team. "Cisco IOS 12.0 Network Security." Page 301. Documentation from the Cisco IOS Reference Library. Copyright 1999 Cisco Systems, Inc. Cisco Press.

[6] Advisory. " Cisco Security Advisory: Multiple Vulnerabilities in CiscoSecure ACS for Windows NT Server, Revision 1.3". Sept. 21, 2000 http://www.cisco.com/warp/public/707/csecureacsnt-pub.shtml

[7]Avi, Oron. "AS/400: The Ideal RADIUS Server -- Sentinel/400" February 1998 http://www.bosweb.com/sen400ar.html

Last Updated: July 25th, 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event