Global Information Assurance Certification Paper

GIAC Security Essentials Practical Internet Research Project

Submitted By Geoffrey Wright

Remote Access Security and RADIUS

Introduction

There is an ever-increasing demand for mobile computing. As businesses increase their investment and utilization of remote access products and capabilities, they must also increase their investment in remote access security. This demand is, in part, fuelled by such things as new developments in high-speed data communications, advances in wireless computing, advances in portable computing devices, and an increased demand for instant access to information.

"According to US-based researcher Forrester, there are more than 25 million professional staff working away from their offices in the US, and a sizable proportion of these workers access corporate networks via modems".[1]

Remote Access Security a Challenge

Remote access provides some unique security challenges that network administrators might not normally encounter in a typical LAN environment. Firewalls and passwords generally protect local area networks. Security guards, surveillance systems, locked doors, and passwords protect the equipment that comprises the LAN. The same cannot necessarily be said for remote computing devices. Remote computing creates a threat to network security, which must be addressed by network administrators. Because no physical security (such as keys, ID badges, or security guards) are in place to ensure the user who is dialing in is who they claim to be, accurate authentication is *vitally* important!

Network administrators must always remember that when they hand out a remote-computing device or enable an account for remote access, they are essentially handing out keys to the building. Security breeches such as a stolen or lost machine, 'sniffing' on the phone lines, or easily guessed passwords compromise network security.

RADIUS

Radius (*Remote Access Dial In User Service*) is an Internet security protocol originally developed by Livingston Enterprises. It is defined in RFC 2138 and RFC 2139 (RFC 2138 deals with the authentication aspect of RADIUS and RFC 2139 deals with the accounting component of RADIUS). Some key aspects of RADIUS which have led to its success are as follows:

- open protocol
- based on client/server model
- supports many authentication mechanisms
- encrypted transactions between client and server

- centralized authentication
- interoperability with other protocols

RADIUS is an open protocol, which means that the source code is freely available. This allows RADIUS to be tailored to suit the particular needs of a particular environment. Shiva Access Manager (Intel/Shiva's RADIUS implementation), for example, has many customized features which give it a richer feature set when interacting with other Intel/Shiva devices as opposed to other network access servers.

RADIUS is based on a client/server model. The remote machine acts as the client with the RADIUS server at the other end handling authentication.

RADIUS also supports many authentication methods. This is tied to (in part) the fact that RADIUS is an open protocol. A RADIUS server can authenticate a user based on its own internal username/password list or it can act as a client to authenticate the user based on various other authentication systems (such as UNIX, NT, NetWare, DCE, et cetera). RADIUS servers can also act as clients to other RADIUS servers. This is particularly useful in situations where a company wishes to outsource its remote access capability but still wants control over security. An ISP's RADIUS server can act as a client to the particular company's RADIUS server. This way, the company still has control over the security while the ISP handles the management of the remote access services.

Transactions between the client and the RADIUS server can be encrypted which further adds to the integrity of the system. Various authentication methods are used depending on the particular vendor (again, the flexibility of the open protocol is evident). PAP (password authentication protocol) can be used but protocols such as CHAP (challenge handshake authentication protocol) or proprietary encryption methods such as Intel/Shiva's SPAP are more secure as the password is encrypted as it travels from the client to the RADIUS server. This thwarts anyone who is watching packets flow over the line.

Radius is also able to interact with other authentication protocols such as TACACS, TACACS+, and Cisco Systems' XTACACS.

How RADIUS Works

RADIUS is based on the UDP (user datagram protocol). The two *well-known* port numbers that are involved in RADIUS are UDP 1645 (for authentication) and UDP 1646 (for accounting). The RADIUS server itself generally runs on either a UNIX or an NT machine.

A user will make a connection to some sort of remote access server (RAS – also sometimes referred to as a network access server or NAS). This connection is often a dial-up connection but may also be an 'always-on' connection via a cable-modem or DSL line. The RAS may also be some sort of VPN device. The user sends the username and password to the RAS, which in turn passes this information to the RADIUS server for authentication. The RADIUS server will return either a PASS or a FAIL to the user via the RAS.

The RADIUS server can authenticate the user based on an internal username/password list or it may elect to act as a client (via a proxy) to another type of authentication such as NT, NetWare, UNIX, et cetera. The RADIUS protocol is very rich in features and the success or failure of a user's login attempt may also depend on such things as which NAS the request comes from, time of day, day of week, the number that the user is calling from.

If the RADIUS user allows the user to login, then it also may place restrictions on the type of transactions that the user is able to perform.

Two-Factor Authentication

Two-factor authentication further strengthens remote access security. Two-factor authentication is based on something you possess and something that you know. An example of this would be your bank account. You can make a withdrawal at the branch if they know who you are. If you are making a withdrawal remotely (from a bank machine) then the bank needs to accurately obtain your identity. They do this by providing you with a bank card to access your account (something that you have) and also with a number or a PIN (something that you know). Only with these two factors together can you access your account. This is essentially how two-factor authentication works. It combines the use of a token and a password. Traditionally, this token has been a hardware device, but now some vendors are using software-based tokens.

With two-factor authentication, the user is required to send some sort of time-dependant password. Sometimes this is a response based on a challenge from a server (the server sends out a challenge and the client generates a response (via the token) based on a hashing. Sometimes the user will possess a token with a code which changes regularly – this code is in sync with a code on the server. Security Dynamics is a big player in this field with their ACE Server.

A Final Word

Tools such as RADIUS and two-factor authentication methods do improve remote computing security, but they are not totally bulletproof. As a network administrator, the first step to protecting your company against a breech through your remote access system is to have control on which employees have remote access capability. Good security begins with policy.

References

1 – http://www.funk.com/new_one/ResourceLibrary/secwp.htm

2 - Rigney, C., Rubens, A., Willens, S. RFC 2138. April 1997. URL: http://www.theinternetbook.net/RFC/rfc2138.html.

3 - Full, B., Roderick, M., Clark, M., Vian, J. URL: http://www.squashduck.com/~roundman/radius/.

4 – URL: http://www.shiva.com/remote/samwhitepaperz.html.

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event