Center for Internet Security Benchmark for FreeRADIUS v1.0

Aug 2, 2007

Editor: Ralf Durkee

http://cisecurity.org

cis-feedback@cisecurity.org

Table of Contents

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff

resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."

Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

Terms of Use Agreement Version 2.1 – 02/20/04

Introduction

This benchmark is intended to assist administrators in securing FreeRadius, the most popular open source RADIUS server used to provide network access control, including authentication, authorization and accounting. RADIUS stands for Remote Authentication Dial In User Service, published as RFC 2865 and RFC 2866. Although RADIUS was originally used for dial-up network access control, it's also commonly used for other network access controls, such as DSL, 802.1X, wireless 802.11, and VoIP. Of course RADIUS servers are just one part of a typical network infrastructure, and their security depends in part on the security of the rest of the infrastructure. However, this benchmark will focus primarily on the secure configuration of the FreeRadius server.

Applicability

While the majority of the recommendations and steps outlined in this document apply to most Unix systems, it should be noted that specific paths and some syntax may vary for some Unix platforms so the reader is encouraged to be familiar with the differences specific to their individual platforms. The provided configurations have been tested using FreeRadius 1.1.3 on Red Hat Fedora Core 6. The audience for the document is at the level of an experienced system administrator, with some specific experience in administering the FreeRadius server. The configuration and security controls provided have been developed through a consensus effort of best practices recommended by a majority of participating security experts.

1 Operating System Level Configuration

The following specifies the recommended operating system level installation, configuration and permissions for FreeRADIUS

1.1 OS Hardening

Security of the RADIUS service absolutely depends on having a secured operating system as a foundation.

Harden the operating system using appropriate CIS benchmark from http://www.cisecurity.org/

1.2 Non-privileged Radius Account

There must be no other usage of the user account except for running the radiusd server.

Discussion:

Configure radiusd to execute under a dedicated non-privileged user and group account, by ensuring that user and group are configured in the radiusd.conf file.

Example:

```
user = radiusd
group = radiusd
```

1.3 Logging Partition

In the event that attacks or even normal events causing excessive logs to fill up the file system other critical system partitions which contain system executables and configuration files should not be affected.

Discussion:

Do not use the root file system partition for the radiusd log file. Instead use a separate file system dedicated to logging and other run time data storage. The /var file system is typically used for logging, and should be it's own partition.

1.4 Ownership of raddb

The radius client.conf file typically contains clear text shared secrets to authenticate client systems and devices and therefore must have minimal ownership and access.

Discussion:

The /etc/raddb directory or the equivalent directory containing the freeradius configuration files must be owned by root, as well as all files contained therein.

1.5 Permissions for raddb

Allowing write access to Radius DB directory would allow deletion and replacement of the configuration files to undermine the entire security of the server configuration.

Discussion:

The /etc/raddb directory and the configuration files in the directory must be read-only for the radiusd group with no-access for other.

Example:

```
drwxr-x--- 3 root radiusd /etc/raddb/
```

1.6 Client Configuration File Ownership

The system default RADIUS client configuration file must be protected from modification to prevent configuration attacks on local clients.

Discussion:

The radius clients configuration file, must be owned by root with a group of radiusd.

1.7 Client Configuration File Permissions

The system default RADIUS client configuration file must be protected from modication to prevent configuration attacks on local clients.

Discussion:

The radiusd clients.conf file must not be readable only by the raidusd server and by root.

Example:

```
 -rw-r----- 1 root radiusd clients.conf
```

1.8 Dedicated System

FreeRadius should be installed on a system dedicated to the directory and authentication services, to reduce the risk of potential vulnerabilities in other services jeopardizing the server.

Discussion:

System must be dedicated to running the RADIUS service, only administrative services like SSH and other closely related authentication services, should be running on the same system.

1.9 Restricted Network Access

Restricting network access with IP filtering to those just those systems or networks that require access, reduces the risk of the most common attacks.

Discussion:

Restrict network access using host based IP filtering to the minimal networks or systems requiring access. This may be accomplished with tcpwrappers, iptables, bpf or ipf depending on the platform

2 The radiusd.conf Configuration File

The following configuration directives are made to the radius.conf configutation file typically found in /etc/raddb/

2.1 Enable Logging

The log files must also be frequently monitored to be an effective security control.

Discussion:

The log directory and log file must be configured to a suitable directory where the FreeRadius logs will be rotated and monitored. Typically the directory is /var/log/radius/.

Example:

```
logdir = ${localstatedir}/log/radius log_file =
${logdir}/radius.log
```

2.2 Log All Authentications

The log files needs to be monitored as a large number of authentication failures maybe indicate a password guessing attack, or at least constitutes an event warranting some investigation.

Discussion:

All authentications must be logged, while the password itself should not be logged whether the password was valid or invalid password.

Example:

```
log_auth = yes log_auth_badpass = no log_auth_goodpass = no
```

2.3 Disable Core Dumps

Core dumps are disabled, since sensitive information such as passwords would be available in the core dump file.

Discussion:

For productions server the creation of core dumps must be disabled.

Example:

```
allow_core_dumps = no
```

2.4 Allow Password Spaces

Eliminating spaces from passwords would decrease the password complexity and increase the risk of password guessing.

Discussion:

Spaces must be allowed in passwords by ensuring that the nospace_pass is set to the value of no.

Example:

```
nospace_pass = no
```

2.5 Max Attributes

The intent is to mitigate a denial of service attack using an excessive number of attributes.

Discussion:

In the security section of the radiusd.conf file the maximum number of attributes allow should be set a number greater than zero, which is high enough to allow all legitimate requests. A limit of 200 should be plenty for most cases.

Example:

```
max_attributes = 200
```

2.6 Reject Delay

The purpose of delaying reject packets is to significantly slow down password guessing and DoS attacks. Setting a value to high may introduce confusion with timeout issues for clients.

Discussion

In the Security section the reject_delay item configures the number of seconds to delay before sending a reject packet. The setting should be set to a value of 1 or slightly higher, 2 is recommended.

Example:

```
reject_delay = 2
```

2.7 No Server Status

Server Status request and keep-alive techniques are considered useless and possibly harmful. See: http://www.freeradius.org/ rfc/rfc2865.html#Keep-Alives

Discussion:

The server status configuration should be set to 'no' to disable status responses which includes the server uptime.

Example:

```
status_server = no
```

2.8 Proxy Request

Also remember to comment out any include of the proxy configuration.

Discussion:

Unless the Radius Server is acting as proxy to other radius servers, the proxy_request directive must be disabled.

Example:

```
proxy_requests = no ## $INCLUDE ${confdir}/proxy.conf
```

2.9 Client IP Address

Usage of a host name is not recommended as it leaves the service subject to DNS attacks.

Discussion:

Each Radius Client Network Access System (NAS) must be configured with its individual IP Address rather than a network ID.

Example:

```
client 10.2.3.4 { . . . }
```

2.10 Unique Client Secret

Do NOT use the example secret. Having each client configured with a unique secret is worth the extra work to ensure that compromise of one doesn't necessarily compromise the whole.

Discussion:

Each client Network Access System must be configured with a unique shared secret.

Example:

```
client 10.2.3.4 { secret = foz4c0wce-ufBojto=nvoxxxc9owgOoghit~p
```

2.11 Strong Shared Secrets

The security of RADIUS depends heavily on the strength of the shared secret. Usage of a password generator is helpful. Old NAS clients limited the length to 16 and should be upgraded.

Discussion:

The shared secret string for each client must be at least 22 characters, but not more than 31 characters. The secret must not use dictionary words, or guessable patterns or variations of words. It should include a variety of special, numeric and alphabetic characters.

2.12 Users File Passwords

Clear text user password storage in the user file increases the risk of a user password disclosure.

Discussion:

Passwords must NOT be stored in the Radius users text file in clear text using the User-Password attribute.

2.13 User Password Storage

Storage of user passwords in clear text or with reversible encryption increases the risk of password disclosure via directly attacking the password storage.

Discussion:

User passwords must be stored using a secure one-way hash regardless of whether the storage is a flat file, database or directory service.

2.14 User Network Authentication

TLS configurations must be configured to require strong ciphers. Such as the example LDAP TLS configuration:

TLSCipherSuite HIGH:MEDIUM:!ADH:-SSLv2 `TLSCipherSuite HIGH:MEDIUM:!ADH:-SSLv2`

Discussion:

If a directory service is used to authenticate users, a secure protocol with at least 128 bit or stronger encryption must be used. Compliant protocols include PEAP, EAP-MCCHAPv2, EAP-TLS, EAP-TTLS and LDAP with TLS. See the table below for details.

Authentication Protocol	**Recommended**	**Comments**
PAP	NO	Clear text passwords over the net protected only by weak usage of MD5 hash
CHAP	NO	Weak, requires clear text password storage
MSCHAP	NO	Requires Clean Text Storage of Passwords
EAP-MD5	NO	Vulnerable to password dictionary and guessing attack
EAP-LEAP	NO	Vulnerable to password dictionary and guessing attack.
EAP-TLS	YES	Uses client TLS certificates, very strong protection with proper certificate management.
EAP-TTLS	YES	Uses client passwords or other authentication tunneled in TLS
PEAPv0 aka EAP-MSCHAPV2	YES	Compatible with MS implementation, not with Cisco's Implementation
PEAPv1 aka EAP-GTC	YES	Not supported natively on Windows.
LDAP with TLS	YES	

Revision History

Original Version 0.9 Feb-Apr 2007 -- Editor Ralph Durkee
Consensus updates 1.0 Aug 2007 -- Editor Ralph Durkee

Additional Resources

FreeRadius Wiki documentation - http://wiki.freeradius.org
How-to on FreeRadius with OpenLDAP - http://www.ibm.com/developerworks/linux/library/l-radius/ Linux Magazine Article on RADIUS and 802.1X - https://www.linux-magazine.com/issue/52/Freeradius_802.1X.pdf
RFC 2865 RADIUS - http://www.ietf.org/rfc/rfc2865.txt RFC 2866 - RADIUS Accounting - http://www.faqs.org/rfcs/rfc2866.html