Security Benchmarks™

A DIVISION OF CENTER FOR INTERNET SECURITY

CIS MIT Kerberos 1.10 Benchmark

v1.0.0

12-28-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, CIS MIT Kerberos 1.10 Benchmark v1.0.0, provides prescriptive guidance for establishing a secure configuration posture for MIT Kerberos 1.10-based Key Distribution Centers (KDC)s. This guide was tested against MIT Kerberos 1.10.3 running on Red Hat Enterprise Linux 6 x64. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, identity managers, security specialists, and auditors who plan to develop, deploy, assess, or secure solutions that incorporate MIT Kerberos 1.10.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored
Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored
Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **KDC with DB2 Database**

  Items in this profile apply to MIT Kerberos KDC 1.10 installations that leverage a DB2 file for the Kerberos database. Additionally, items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **KDC with LDAP Database**

  Items in this profile apply to MIT Kerberos KDC 1.10 installations that leverage LDAP for the Kerberos database. Additionally, items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor
JR Aquino
Richard Basch
Jeff Blaine
Blake Frantz, *Center for Internet Security*
Roger Kennedy
Tao Zhou

Recommendations

1 Kerberos Runtime

Recommendations in this section apply to libraries and executable that are installed as part of the MIT Kerberos 1.10 software.

1.1 Secure the KDC daemon (krb5kdc) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The KDC daemon is implemented as an executable service, `krb5kdc`. Ensure access to the KDC daemon executable reflects least privilege.

Rationale:

Ensuring that access to the KDC daemon executable reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/krb5kdc` is `root:root`.
2. Ensure the permission on `/usr/sbin/krb5kdc` prevent `writes` by `group` and `other`.

```
# stat -L --format "%U:%G %A" /usr/sbin/krb5kdc
root:root -rwxr-xr-x
```

Remediation:

1. Set the ownership on `/usr/sbin/krb5kdc` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/sbin/krb5kdc`.

```
chmod og-w /usr/sbin/krb5kdc
chown root:root /usr/sbin/krb5kdc
```

1.2 Secure the Kerberos administration server daemon (kadmind) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos administration server is implemented as an executable service, `kadmind`. Ensure access to the Kerberos administration server reflects least privilege.

Rationale:

Ensuring that access to the Kerberos administration server executable reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kadmind is root:root.`
2. Ensure the permission on `/usr/sbin/kadmind` prevent writes by `group` and `other.`

```
stat -L --format "%U:%G %A" /usr/sbin/kadmind
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/sbin/kadmind to root:root.`
2. Revoke write permission from `group` and `other` on `/usr/sbin/kadmind.`

```
chmod og-w /usr/sbin/kadmind
chown root:root /usr/sbin/kadmind
```

1.3 Secure the Kerberos database administration utility (kadmin.local) (Scored)

Profile Applicability:

- KDC with DB2 Database

- KDC with LDAP Database

Description:

The Kerberos database administration utility is implemented as an executable command line tool, `kadmin.local`. Ensure access to the Kerberos administration server reflects least privilege.

Rationale:

Ensuring that access to the Kerberos database administration utility reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kadmin.local is root:root.`
2. Ensure the permission on `/usr/sbin/kadmin.local` prevent writes by `group` and `other.`

```
stat -L --format "%U:%G %A" /usr/sbin/kadmin.local
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/sbin/kadmin.local` to `root:root.`
2. Revoke write permission from `group` and `other` on `/usr/sbin/kadmin.local.`

```
chmod og-w /usr/sbin/kadmin.local
chown root:root /usr/sbin/kadmin.local
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kadmin_local.html

1.4 Secure the Kerberos LDAP configuration utility (kdb5_ldap_util) (Scored)

Profile Applicability:

- KDC with DB2 Database

- KDC with LDAP Database

Description:

The Kerberos LDAP configuration utility is implemented as an executable command line tool, `kdb5_ldap_util`. Ensure access to the Kerberos LDAP configuration utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos LDAP configuration utility executable reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kdb5_util` is `root:root`.
2. Ensure the permission on `/usr/sbin/kdb5_ldap_util` prevent `writes` by `group` and other.

```
stat -L --format "%U:%G %A" /usr/sbin/kdb5_ldap_util
```

3. Ensure the output from the above command reflects the following:
   - The output starts with `root:root`
   - The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/sbin/kdb5_ldap_util` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/sbin/kdb5_ldap_util`.

```
chmod og-w /usr/sbin/kdb5_ldap_util
chown root:root /usr/sbin/kdb5_ldap_util
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kdb5_ldap_util.html

1.5 Secure the Kerberos configuration utility (kdb5_util) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos configuration utility is implemented as an executable command line tool, `kdb5_util`. Ensure access to the Kerberos configuration utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos configuration utility executable reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kdb5_util` is `root:root`.
2. Ensure the permission on `/usr/sbin/kdb5_util` prevent `writes` by `group` and other.

```
stat -L --format "%U:%G %A" /usr/sbin/kdb5_util
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/sbin/kdb5_util` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/sbin/kdb5_util`.

```
chmod og-w /usr/sbin/kdb5_util
chown root:root /usr/sbin/kdb5_util
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kdb5_util.html

1.6 Secure the Kerberos propagation utility (kprop) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos database propagation utility is implemented as an executable command line tool, `kprop`. Ensure access to the Kerberos database propagation utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos database propagation utility executable reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kprop` is `root:root`.
2. Ensure the permission on `/usr/sbin/kprop` prevent `writes` by `group` and other.

```
stat -L --format "%U:%G %A" /usr/sbin/kprop
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/sbin/kprop` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/sbin/kprop`.

```
chmod og-w /usr/sbin/kprop
chown root:root /usr/sbin/kprop
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kprop.html

1.7 Secure the Kerberos slave KDC update daemon (kpropd) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos slave KDC update daemon is implemented as an executable service, `kpropd`. Ensure access to the Kerberos slave KDC update daemon reflects least privilege.

Rationale:

Ensuring that access to the Kerberos slave KDC update daemon reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kpropd` is `root:root`.
2. Ensure the permission on `/usr/sbin/kpropd` prevent `writes` by `group` and other.

```
stat -L --format "%U:%G %A" /usr/sbin/kpropd
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/sbin/kpropd` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/sbin/kpropd`.

```
chmod og-w /usr/sbin/kpropd
chown root:root /usr/sbin/kpropd
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kpropd.html

1.8 Secure the Kerberos propagation log utility (kproplog) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos propagation log utility is implemented as an executable command line tool, `kproplog`, and is used to display the contents of the Kerberos principal update log. Ensure access to the Kerberos propagation log utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos propagation log utility reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/kproplog` is `root:root.`
2. Ensure the permission on `/usr/sbin/kproplog` prevent `writes` by `group` and other.

```
stat -L --format "%U:%G %A" /usr/sbin/kproplog
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/sbin/kproplog` to `root:root.`
2. Revoke write permission from `group` and `other` on `/usr/sbin/kproplog.`

```
chmod og-w /usr/sbin/kproplog
chown root:root /usr/sbin/kproplog
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kproplog.html

1.9 Secure the Kerberos problem report utility (krb5-send-pr) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos problem report utility is implemented as an executable command line tool, `krb5-send-pr`, and is used to submit problem reports to a central support site. Ensure access to the Kerberos problem report utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos problem report utility binary reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/sbin/krb5-send-pr` is `root:root`.
2. Ensure the permissions on `/usr/sbin/krb5-send-pr` prevent `writes` by `group` and `other`.

```
stat -L --format "%U:%G %A" /usr/sbin/krb5-send-pr
```

3. Ensure the output from the above command reflects the following:
   - The output starts with `root:root`
   - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/sbin/krb5-send-pr` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/sbin/krb5-send-pr`.

```
chmod og-w /usr/sbin/krb5-send-pr
chown root:root /usr/sbin/krb5-send-pr
```

1.10 Secure the Kerberos host key table manipulation utility (k5srvutil) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos host key table manipulation utility is implemented as an executable command line tool, `krb5-send-pr`, and is used to list, change, or remove keys in a given keytab. Ensure access to the Kerberos host key table manipulation utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos host key table manipulation utility binary reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/bin/k5srvutil` is `root:root`.
2. Ensure the permissions on `/usr/bin/k5srvutil` prevent `writes` by `group` and `other`.

```
stat -L --format "%U:%G %A" /usr/bin/k5srvutil
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/bin/k5srvutil` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/bin/k5srvutil`.

```
chmod og-w /usr/bin/k5srvutil
chown root:root /usr/bin/k5srvutil
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/k5srvutil.html

1.11 Secure the Kerberos database administration utility (kadmin) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos database administration utility is implemented as an executable command line tool, `kadmin`. Ensure access to the Kerberos database administration utility reflects least privilege.

Rationale:

Ensuring that access to the Kerberos database administration utility executable reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/usr/bin/kadmin is root:root.`
2. Ensure the permission on `/usr/bin/kadmin` prevent `writes` by `group` and `other.`

```
stat -L --format "%U:%G %A" /usr/bin/kadmin
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/bin/kadmin` to `root:root.`
2. Revoke write permission from `group` and `other` on `/usr/bin/kadmin.`

```
chmod og-w /usr/bin/kadmin
chown root:root /usr/bin/kadmin
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/kadmin_local.html

1.12 Secure the kdestroy utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `kdestroy` utility is used to destroy a given user's active Kerberos authorization tickets as they exist in the credential cache. Ensure access to the `kdestroy` utility reflects least privilege.

Rationale:

Ensuring that access to the `kdestroy` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/kdestroy` is `root:root.`

2. Ensure the permission on `/usr/bin/kdestroy` prevent `writes` by `group` and `other`.

```
stat -L --format "%U:%G %A" /usr/bin/kdestroy
```

3. Ensure the output from the above command reflects the following:
   - The output starts with `root:root`
   - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/bin/kdestroy` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/bin/kdestroy`.

```
chmod og-w /usr/bin/kdestroy
chown root:root /usr/bin/kdestroy
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/user/user_commands/kdestroy.html

1.13 Secure the kinit utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `kinit` utility is used to create and cache Kerberos ticket-granting tickets. Ensure access to the `kinit` utility reflects least privilege.

Rationale:

Ensuring that access to the `kinit` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/kinit` is `root:root`.
2. Ensure the permission on `/usr/bin/kinit` prevent `writes` by `group` and `other`.

```
stat -L --format "%U:%G %A" /usr/bin/kinit
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/bin/kinit` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/bin/kinit`.

```
chmod og-w /usr/bin/kinit
chown root:root /usr/bin/kinit
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/user/user_commands/kinit.html

1.14 Secure the klist utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `klist` utility is used to list cached Kerberos tickets. Ensure access to the `klist` utility reflects least privilege.

Rationale:

Ensuring that access to the `klist` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/klist` is `root:root`.
2. Ensure the permission on `/usr/bin/klist` prevent `writes` by `group` and `other`.

```
stat -L --format "%U:%G %A" /usr/bin/klist
```

3. Ensure the output from the above command reflects the following:

- The output starts with `root:root`
- The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/bin/klist` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/bin/klist`.

```
chmod og-w /usr/bin/klist
chown root:root /usr/bin/klist
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/user/user_commands/klist.html

1.15 Secure the kpasswd utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `kpasswd` utility is used to change a given user's Kerberos password. Ensure access to the `kpasswd` utility reflects least privilege.

Rationale:

Ensuring that access to the `kpasswd` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/kpasswd` is `root:root`.
2. Ensure the permission on `/usr/bin/kpasswd` prevent `writes` by `group` and other.

```
stat -L --format "%U:%G %A" /usr/bin/kpasswd
```

3. Ensure the output from the above command reflects the following:
   - The output starts with `root:root`
   - The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/bin/kpasswd` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/bin/kpasswd`.

```
chmod og-w /usr/bin/kpasswd
chown root:root /usr/bin/kpasswd
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/user/user_commands/kpasswd.html

1.16 Secure the krb5-config utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `krb5-config` utility is used for linking against MIT Kerberos libraries. Ensure access to the `krb5-config` utility reflects least privilege.

Rationale:

Ensuring that access to the `krb5-config` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/krb5-config` is `root:root`.
2. Ensure the permission on `/usr/bin/krb5-config` prevent `writes` by `group` and `other`.

```
stat -L --format "%U:%G %A" /usr/bin/krb5-config
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "-".

Remediation:

1. Set the ownership on `/usr/bin/krb5-config` to `root:root`.
2. Revoke write permission from `group` and `other` on `/usr/bin/krb5-config`.

```
chmod og-w /usr/bin/krb5-config
chown root:root /usr/bin/krb5-config
```

1.17 Secure the ksu utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `ksu` utility is a kerberized implementation of the su command and can be used to switch user IDs. Ensure access to the `ksu` utility reflects least privilege.

Rationale:

Ensuring that access to the `ksu` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/ksu` is `root:root.`
2. Ensure the permission on `/usr/bin/ksu` prevent `writes` by `group` and `other.`

```
stat -L --format "%U:%G %A" /usr/bin/ksu
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/bin/ksu` to `root:root.`
2. Revoke write permission from `group` and `other` on `/usr/bin/ksu.`

```
chmod og-w /usr/bin/ksu
chown root:root /usr/bin/ksu
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/user/user_commands/ksu.html

1.18 Secure the kswitch utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `kswitch` utility is used to set the given credential cache to the primary credential cache. Ensure access to the `kswitch` utility reflects least privilege.

Rationale:

Ensuring that access to the `kswitch` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/kswitch` is `root:root.`
2. Ensure the permission on `/usr/bin/kswitch` prevent `writes` by `group` and `other.`

```
stat -L --format "%U:%G %A" /usr/bin/kswitch
```

3. Ensure the output from the above command reflects the following:
    - The output starts with `root:root`
    - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/bin/kswitch` to `root:root.`
2. Revoke write permission from `group` and `other` on `/usr/bin/kswitch.`

```
chmod og-w /usr/bin/kswitch
chown root:root /usr/bin/kswitch
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/user/user_commands/kswitch.html

1.19 Secure the ktutil utility (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `ktutil` utility is used perform maintenance tasks on a given keytab. Ensure access to the `ktutil` utility reflects least privilege.

Rationale:

Ensuring that access to the `ktutil` utility reflects least privilege will ensure that the integrity of the utility is not compromised.

Audit:

1. Ensure the owner of `/usr/bin/ktutil is root:root.`
2. Ensure the permission on `/usr/bin/ktutil` prevent `writes` by `group and other.`

```
stat -L --format "%U:%G %A" /usr/bin/ktutil
```

3. Ensure the output from the above command reflects the following:
   - The output starts with `root:root`
   - The 2nd and 5th characters from the right are "–".

Remediation:

1. Set the ownership on `/usr/bin/ktutil` to `root:root.`
2. Revoke write permission from `group` and `other` on `/usr/bin/ktutil.`

```
chmod og-w /usr/bin/ktutil
chown root:root /usr/bin/ktutil
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/admin_commands/ktutil.html

2 KDC Configuration (kdc.conf)

2.1 [kdcdefaults]

The kdcdefaults section specifies default values for realm variables to be used if the realms subsection does not contain the configuration directive.

2.1.1 Ensure restrict_anonymous_to_tgt is set to true (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

This option allows anonymous PKINIT to be enabled for use as FAST armor tickets without allowing anonymous authentication to services. If set to true, the KDC will reject ticket requests from anonymous principals to service principals other than the realm's ticket-granting service.

Rationale:

For auditing and accounting, access to a service should be tied to a specific identity principle, not an anonymous principle.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[kdcdefaults]` section
3. Locate the `restrict_anonymous_to_tgt` directive
4. Ensure the `restrict_anonymous_to_tgt` directive is set to `true`.

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[kdcdefaults]` section
3. Locate the `restrict_anonymous_to_tgt` directive
4. Set the `restrict_anonymous_to_tgt` directive to `true`.

Default Value:

`restrict_anonymous_to_tgt` is set to `false`.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/krb_admins/conf_files/kdc_conf.html#kdcdefaults
2. http://k5wiki.kerberos.org/wiki/Anonymous_kerberos

2.2 [realms]

The realms section creates and configures the realm(s) that the KDC provides.

2.2.1 Secure the Kerberos database access control file (acl_file) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `acl_file` directive specifies the location of the ACL file that `kadmin` uses to determine a given principal's permissions on the Kerberos database. Ensure that the `acl_file` is owned by `root:root` and is not accessible by any principal other than `root`.

Rationale:

Ensuring that access to the KDC Access Control List file reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `acl_file` directive
4. Locate the file referenced by the `acl_file` directive. If the acl_file directive is not present, it is implicitly set to *<LOCALSTATEDIR>*`/krb5kdc/kadmn5.acl`, such as `/var/kerberos/krb5kdc/kadm5.acl`.
5. Run the following command:

```
stat -L --format "%U:%G %a" <path_to_acl_file>
```

6. Ensure the output of the above command is as follows:

```
root:root 600
```

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `acl_file` directive
4. Locate the file referenced by the `acl_file` directive. If the acl_file directive is not present, it is implicitly set to *<LOCALSTATEDIR>*/krb5kdc/kadmn5.acl, such as /var/kerberos/krb5kdc/kadm5.acl.
5. Run the following command:

```
chmod 600 <path_to_acl_file>
chown root:root <path_to_acl_file>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.2 Secure the kadmin keytab (admin_keytab) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `admin_keytab` directive specifies the location of the keytab file that `kadmin` uses to authenticate to the database. Ensure that the `admin_keytab` is owned by `root:root` and is not accessible by any principal other than `root`.

Rationale:

Ensuring that access to the KDC admin keytab file reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `admin_keytab` directive
4. Locate the file referenced by the `admin_keytab` directive. If the directive is not present, the implicit path is `/usr/local/var/krb5kdc/kadm5.keytab`.
5. Run the following command:

```
stat -L --format "%U:%G %a" <admin_keytab>
```

6. Ensure the output of the above command is as follows:

```
root:root 600
```

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `admin_keytab` directive
4. Locate the file referenced by the `admin_keytab` directive. If the directive is not present, the implicit path is `/usr/local/var/krb5kdc/kadm5.keytab`.
5. Run the following command:

```
chmod 600 <admin_keytab>
chown root:root <admin_keytab>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.3 Secure the KDC database file (database_name) (Scored)

Profile Applicability:

- KDC with DB2 Database

Description:

The `database_name` directive specifies the location of the Berkeley DB file that the KDC uses as a database backend. Ensure that the `database_name` is owned by `root:root` and is not accessible by any principal other than `root`.

Rationale:

Ensuring that access to the KDC Database file reflects least privilege will in-turn help ensure the integrity and availability of KDC operations.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. Locate the `database_name` directive
4. Locate the file referenced by the `database_name` directive. If the `database_name` directive is not present, it is implicitly set to

<*LOCALSTATEDIR*>/krb5kdc/principal, such as /var/kerberos/krb5kdc/principal.

5. Run the following command:

```
stat -L --format "%U:%G %a" <database_name>
```

6. Ensure the output of the above command starts with "root:root" and ends with "00".

Remediation:

1. Open /var/kerberos/krb5kdc/kdc.conf
2. Locate the [realms] section
3. Locate the database_name directive
4. Locate the file referenced by the database_name directive. If the database_name directive is not present, it is implicitly set to <*LOCALSTATEDIR*>/krb5kdc/principal, such as /var/kerberos/krb5kdc/principal.
5. Run the following command:

```
chmod og-rwx <database_name>
chown root:root <database_name>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#kdc-realms

2.2.4 Ensure that pwservice is not in the default_principal_flags (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The pwservice flag a principal as a password change service, which grants it permission to change passwords without going through normal password authentication.

Rationale:

Access to a principle with the pwservice flag can result in passwords being changed, denying service to legitimate users and elevating the access of an attacker.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `default_principal_flags` directive
4. Ensure that `default_principal_flags` contains `-pwservice`

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `default_principal_flags` directive
4. Adjust the list so that that `default_principal_flags` contains `-pwservice`

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.5 Secure the dictionary file (dict_file) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `dict_file` directive specifies the location of the file that contains values that are not allowed as passwords. Ensure that the `dict_file` is owned by `root:root` and is writable by any principal other than `root`.

Rationale:

Ensuring that access to the `dict_file` reflects least privilege will help ensure that the integrity of the `dict_file` is not compromised. If the integrity of the `dict_file` is compromised, the efficacy of the password blacklist controls may be reduced.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `dict_file` directive
4. Locate the file referenced by the `dict_file` directive.

5. Run the following command:

```
stat -L --format "%U:%G %a" <dict_file>
```

6. Ensure the output of the above command exhibits the following:
   - Start with `root:root`
   - The 2nd and 5th characters from the right are set to "–".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `dict_file` directive
4. Locate the file referenced by the `dict_file` directive.
5. Run the following command:

```
chmod og-w <path_to_dict_file>
chown root:root <path_to_dict_file>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.6 Secure KDC key stash file (key_stash_file) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `key_stash_file` directive specifies the file containing the master key as stored with `kdb5_stash`. Ensure access to the file referenced by the `key_stash_file` directive reflects least privilege.

Rationale:

Ensuring that access to the file referenced by the `key_stash_file` directive reflects least privilege will help ensure the integrity of authentication services provided by Kerberos and the confidentiality of credentials used by participating principals and servers.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. Locate the `key_stash_file` directive
4. Locate the file referenced by the `key_stash_file` directive. If the `key_stash_file` directive is not present, it is implicitly set to *<LOCALSTATEDIR>*`/krb5kdc/.k5.`<REALM>, such as `/var/kerberos/krb5kdc/.k5.example.com`.
5. Ensure the owner of the referenced file is `root:root` and permissions prevent access by `group` or `other`.

```
stat -L --format "%U:%G %a" <key_stash_file>
```

6. Ensure the output of the above command starts with "`root:root`" and ends with "`00`".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf.`
2. Locate the `[realms]` section.
3. Locate the file referenced by the `key_stash_file` directive. If the key_stash_file directive is not present, it is implicitly set to *<LOCALSTATEDIR>*/krb5kdc/.k5.<REALM>, such as /var/kerberos/krb5kdc/.k5.example.com.
4. Set the owner of the referenced file to `root:root`.

```
chown root:root <key_stash_file>
```

5. Set the permissions on the referenced file to prevent access by `group` or `other`.

```
chmod og-rwx <key_stash_file>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.7 Ensure the master_key_name is set to K/M (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

This string specifies the name of the principal associated with the master key. The default value is K/M.

Rationale:

While there is no direct security impact for renaming the master key, the master key principle has special access controls that require auditing. Changing the master key name may cause ACL audits to improperly fail.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `master_key_name` directive
4. Ensure that the `master_key_name` is set to `K/M`

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `master_key_name` directive
4. Set the `master_key_name` to `K/M`

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.8 Ensure master_key_type is using a strong encryption algorithm (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

This directive controls the master key's key type. It is recommended to only use an algorithm from the following list:

- aes256-cts-hmac-sha1-96
- aes128-cts-hmac-sha1-96

- des3-cbc-sha1
- arcfour-hmac-md5

Rationale:

Strong encryption algorithms should be used to prevent various cryptographic attacks as well as to comply with various industry standards and government regulations.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `master_key_type` directive
4. Ensure the value is set to one of the following: `aes256-cts-hmac-sha1-96`, `aes128-cts-hmac-sha1-96`, `des3-cbc-sha1`, `arcfour-hmac-md5`

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `master_key_type` directive
4. Set the value to one of the following: `aes256-cts-hmac-sha1-96`, `aes128-cts-hmac-sha1-96`, `des3-cbc-sha1`, `arcfour-hmac-md5`

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.9 Ensure max_life is 24 hours or less (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

This directive uses a timedelta to specify the maximum time period that a ticket may be valid for in this realm.

Rationale:

Kerberos tickets should expire regularly to ensure that compromised tickets cannot be used indefinitely.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `max_life` directive
4. Ensure that the time is set to `24h 0m 0s` or lower

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `max_life` directive
4. Change the time to `24h 0m 0s` or lower

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.10 Ensure max_renewable_life is less than 14 days (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

This directive controls the maximum time period that a ticket may be renewed.

Rationale:

A compromised Kerberos ticket may be renewed indefinitely. This directive should be used to limit the impact of such a credential compromise.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `max_renewable_life` directive
4. Ensure `max_renewable_life` is set to less than `14d`

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`

2. Locate the `[realms]` section
3. For each defined realm, locate the `max_renewable_life` directive
4. Set `max_renewable_life` to less than `14d`

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.2.11 Ensure only strong encryption types are supported (supported_enctypes) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `supported_enctypes` directive specifies the default key/salt combinations for this realm. Any principals created through `kadmin` will have keys of these types. Ensure the `supported_enctypes` directive includes only strong key/salt combinations.

Rationale:

Strong encryption algorithms should be used to prevent various cryptographic attacks as well as to comply with various industry standards and government regulations.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `supported_enctypes` directive
4. Ensure the `supported_enctypes` directive is set to the following value:

```
aes256-cts-hmac-sha1-96:normal aes128-cts-hmac-sha1-96:normal \
des3-cbc-sha1:normalarcfour-hmac-md5:normal
```

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `supported_enctypes` directive.

4. Set the `supported_enctypes` directive to the following value:

```
aes256-cts-hmac-sha1-96:normal aes128-cts-hmac-sha1-96:normal \
des3-cbc-sha1:normal arcfour-hmac-md5:normal
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/krb_admins/conf_files/kdc_conf.html#realms

2.2.12 Ensure reject_bad_transit is set to true (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

This boolean specifies whether or not the list of transited realms for cross-realm tickets should be checked against the transit path computed from the realm names and the `[capaths]` section of its `krb5.conf`. If this value is set to false, such tickets will be issued anyways, and it will be left up to the application server to validate the realm transit path.

Rationale:

Realm transit path should be enforced by the KDC, not left to the application. Some applications may not check the transit path, which could result in unauthorized resource access.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `reject_bad_transit` directive
4. Ensure that `reject_bad_transit` is set to `true`

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[realms]` section
3. For each defined realm, locate the `reject_bad_transit` directive
4. Set `reject_bad_transit` is to `true`

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#realms

2.3 [dbdefaults]

2.3.1 Secure the Kerberos database file (database_name) (Scored)

Profile Applicability:

- KDC with DB2 Database

Description:

The `database_name` directive specifies the location of the Kerberos database on the file system. This directive is significant only when a Berkeley DB database type is configured. Ensure that access to the Kerberos database reflects least privilege.

Rationale:

Ensuring that access to the Kerberos database reflects least privilege will help ensure the integrity and confidentiality of database contents.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[dbdefaults]` section
3. Locate the `database_name` directive
4. Locate the file referenced by the `database_name` directive.
5. Run the following command:

```
stat -L --format "%U:%G %a" <database_name>
```

6. Ensure the output of the above command starts with "root:root" and ends with "00".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[dbdefaults]` section
3. Locate the `database_name` directive
4. Locate the file referenced by the `database_name` directive.

5. Run the following command:

```
chmod og-rwx <database_name>
chown root:root <database_name>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbdefaults
2. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

2.3.2 Ensure "Last successful authentication" field is updated (disable_last_success) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `disable_last_success` directive determines if the KDC will suppress updates to the "Last successful authentication" field of principal entries requiring preauthentication. Ensure that "Last success authentication" events are not suppressed.

Rationale:

Ensuring that "Last success authentication" updates occur may provide useful information when investigating an operational or security event.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[dbdefaults]` section
3. Ensure the `disable_last_success` directive is absent OR is present and set to `false`.

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[dbdefaults]` section
3. Locate the `disable_last_success` directive.
4. Set the `disable_last_success` directive to `false`.

Impact:

Setting this directive to `false` results in network traffic for each login, which can result in a denial of service under heavy usage. If you opt to set this directive to `true`, account lockouts are not possible as there is no success/failure logging. This will conflict with Recommendation 2.3.3.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbdefaults
2. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

2.3.3 Ensure account lockouts are not disabled (disable_lockout) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `disable_lockout` directive determines if the KDC will suppress updates to the "Last failed authentication" and "Failed password attempts" field of principal entries requiring preauthentication. Ensure that these events are not suppressed.

Rationale:

Ensuring that "Last failed authentication" and "Failed password attempts" updates occur may provide useful information when investigating an operational or security event. Additionally, allowing these updates enables accounts to be locked out due to too many successive authentication failures.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[dbdefaults]` section
3. Ensure the `disable_lockout` directive is absent OR is present and set to `false`.

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`

2. Locate the `[dbdefaults]` section
3. Locate the `disable_lockout` directive.
4. Set the `disable_lockout` directive to `false`.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbdefaults
2. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

2.3.4 Secure the LDAP server password file (ldap_service_password_file) (Scored)

Profile Applicability:

- KDC with LDAP Database

Description:

The `ldap_service_password_file` directive specifies the file containing the stashed passwords for the `ldap_kadmind_dn` and `ldap_kdc_dn` objects. This directive is only significant if the LDAP database type is configured. Ensure access to the file referenced by the `ldap_service_password_file` directive reflects least privilege.

Rationale:

Ensuring that access to the file referenced by the `ldap_service_password_file` directive reflects least privilege will help ensure the integrity of authentication services provided by Kerberos and the confidentiality of credentials used by participating principals and servers.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[dbdefaults]` section
3. Locate the `ldap_service_password_file` directive
4. Locate the file referenced by the `ldap_service_password_file` directive.
5. Ensure the owner of the referenced file is `root:root` and permissions prevent access by `group` or `other`.

```
stat -L --format "%U:%G %a" <ldap_service_password_file>
```

6. Ensure the output of the above command starts with "`root:root`" and ends with "`00`".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`.
2. Locate the `[dbdefaults]` section.
3. Locate the `ldap_service_password_file` directive.
4. Locate the file referenced by the `ldap_service_password_file` directive.
5. Set the owner of the referenced file to `root:root`.

```
chown root:root <ldap_service_password_file>
```

6. Set the permissions on the referenced file to prevent access by `group` or `other`.

```
chmod og-rwx <ldap_service_password_file>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbdefaults
2. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

2.3.5 Ensure kadmin and KDC run as different LDAP users (Scored)

Profile Applicability:

- KDC with LDAP Database

Description:

When using LDAP as a Kerberos backend, the two server components, kadmind and kdc, each have an LDAP user DN configured with `ldap_kadmind_dn` and `ldap_kdc_dn`.

Rationale:

Different users should be created and configured for the two server components to ensure separation of privilege.

Audit:

1. Open kdc.conf
2. Find the lines `ldap_kadmind_dn` and `ldap_kdc_dn`
3. Ensure that two different LDAP DNs are configured

Remediation:

1. Open kdc.conf Find the lines
2. `ldap_kadmind_dn` and `ldap_kdc_dn`
3. Set each directive to a unique LDAP DN

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

2.4 [logging]

2.4.1 Secure the default location (default) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `default` logging entry determines where logs are sent in the absence of an explicit entry for a given role, such as `kdc` and `admin_server`. The `default` logging entry may be prefixed by `FILE=`, `FILE:`, `STDERR`, `CONSOLE`, `DEVICE`, or `SYSLOG`. For all `default` entries prefixed with `FILE=` or `FILE:`, ensure access to the specified location reflects least privilege.

Note: One or more `default` directives may exist.

Rationale:

Ensuring that access to the default log location reflects least privilege will help ensure the integrity and confidentiality of Kerberos logs.

Audit:

1. Open */var/kerberos/krb5kdc/kdc.conf*
2. Locate the `[logging]` section
3. Locate all `default` directives
4. For each `default` directive prefixed with `FILE:` or `FILE=`, locate the referenced file on the file system.
5. Ensure the owner of the referenced file is `root:root` and permission prevent access by `group` or `other`.

```
stat -L --format "%U:%G %a" <location_referenced_by_default_directive>
```

6. Ensure the output of the above command starts with "`root:root`" and ends with "`00`".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Locate all `default` directives
4. For each `default` directive prefixed with `FILE:` or `FILE=`, locate the referenced file on the file system.
5. Set the owner of the referenced file to root:root.

```
chown root:root <location_referenced_by_default_directive>
```

6. Set the permissions on the referenced file to prevent access by `group` or `other`.

```
chmod og-rwx <location_referenced_by_default_directive>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#logging

2.4.2 Secure the kdc log location (kdc) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `kdc` logging entry determines where the KDC logs are sent. The `kdc` logging entry may be prefixed by `FILE=`, `FILE:`, `STDERR`, `CONSOLE`, `DEVICE`, or `SYSLOG`. For all `kdc` entries prefixed with `FILE=` or `FILE:`, ensure access to the specified location reflects least privilege.

Note: One or more `kdc` directive may exist.

Rationale:

Ensuring that access to the KDC log location reflects least privilege will help ensure the integrity and confidentiality of Kerberos logs.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Locate all `kdc` directives
4. For each `kdc` directive prefixed with `FILE:` or `FILE=`, locate the referenced file on the file system.
5. Ensure the owner of the referenced file is `root:root` and permission prevent access by `group` or `other`.

```
stat -L --format "%U:%G %a" <location_referenced_by_kdc_directive>
```

6. Ensure the output of the above command starts with "`root:root`" and ends with "`00`".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Locate all `kdc` directives
4. For each `kdc` directive prefixed with `FILE:` or `FILE=`, locate the referenced file on the file system.
5. Set the owner of the referenced file to root:root.

```
chown root:root <location_referenced_by_kdc_directive>
```

6. Set the permissions on the referenced file to prevent access by `group` or `other`.

```
chmod og-rwx <location_referenced_by_kdc_directive>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#logging

2.4.3 Secure the administrative server log location (admin_server) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `admin_server` logging entry determines where the administrative server logs are sent. The `admin_server` logging entry may be prefixed by `FILE=`, `FILE:`, `STDERR`, `CONSOLE`, `DEVICE`, or `SYSLOG`. For all `admin_server` entries prefixed with `FILE=` or `FILE:`, ensure access to the specified location reflects least privilege.

Note: One or more `admin_server` directive may exist.

Rationale:

Ensuring that access to the administrative server log location reflects least privilege will help ensure the integrity and confidentiality of the logs.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Locate all `admin_server` directives
4. For each `admin_server` directive prefixed with `FILE:` or `FILE=`, locate the referenced file on the file system.
5. Ensure the owner of the referenced file is `root:root` and permission prevent access by `group` or `other`.

```
stat -L --format "%U:%G %a" <location_referenced_by_admin_server_directive>
```

6. Ensure the output of the above command starts with "`root:root`" and ends with "`00`".

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Locate all `admin_server` directives

4. For each `admin_server` directive prefixed with `FILE:` or `FILE=`, locate the referenced file on the file system.
5. Set the owner of the referenced file to root:root.

```
chown root:root <location_referenced_by_admin_server_directive>
```

6. Set the permissions on the referenced file to prevent access by `group` or `other`.

```
chmod og-rwx <location_referenced_by_admin_server_directive>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#logging

2.4.4 Ensure a persistent log sink is configured for default log location (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `default` logging entry determines where logs are sent in the absence of an explicit entry for a given role, such as `kdc` and `admin_server`. The `default` logging entry may be prefixed by `FILE=`, `FILE:`, `STDERR`, `CONSOLE`, `DEVICE`, or `SYSLOG`. Ensure at least one `default` entry is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG`.

Rationale:

Ensuring that at least one `default` entry is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG` will ensure that logs sent to the default sink are persisted to disk. Information sent to `STDERR` or `CONSOLE` are unlikely to be persisted to disk. Persisting logs to disk will increase the probability that logs are available in support of resolving operational or security events.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section

3. Locate all `default` directives
4. Ensure at least one `default` directive is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG`.

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Add a `default` entry that leverages the `FILE:`, `FILE=`, `SYSLOG`, or `DEVICE` prefix.

```
4. default = SYSLOG:INFO:DAEMON
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#logging

2.4.5 Ensure a persistent log sink is configured for kdc logging (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The kdc logging entry determines where the KDC logs are sent. The `kdc` directive's value may be prefixed by `FILE=`, `FILE:`, `STDERR`, `CONSOLE`, `DEVICE`, or `SYSLOG`. Ensure at least one `kdc` directive has a value that is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG`.

Rationale:

Ensuring that at least one `kdc` entry is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG` will ensure that logs sent to the `kdc` sink are persisted to disk. Information sent to `STDERR` or `CONSOLE` are unlikely to be persisted to disk. Persisting logs to disk will increase the probability that logs are available in support of resolving operational or security events.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[logging]` section
3. Locate all `kdc` directives

4. Ensure at least one `kdc` directive's value is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG`.

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[logging]` section
3. Add a `kdc` entry that leverages the `FILE:`, `FILE=`, `SYSLOG`, or `DEVICE` prefix.

```
4. kdc = SYSLOG:INFO:DAEMON
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#logging

2.4.6 Ensure a persistent log sink is configured for administrative server logging (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The admin_server logging entry determines where the administrative server logs are sent. The `admin_server` logging entry may be prefixed by `FILE=`, `FILE:`, `STDERR`, `CONSOLE`, `DEVICE`, or `SYSLOG`. Ensure at least one `kdc` entry is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG`.

Rationale:

Ensuring that at least one `admin_server` entry is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG` will ensure that logs sent to the `kdc` sink are persisted to disk. Information sent to `STDERR` or `CONSOLE` are unlikely to be persisted to disk. Persisting logs to disk will increase the probability that logs are available in support of resolving operational or security events.

Audit:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Locate all `admin_server` directives

4. Ensure at least one `admin_server` directive is prefixed by `FILE=`, `FILE:`, `DEVICE`, or `SYSLOG`.

Remediation:

1. Open `/var/kerberos/krb5kdc/kdc.conf`
2. Locate the `[logging]` section
3. Add a `admin_server` entry that leverages the `FILE:`, `FILE=`, `SYSLOG`, or `DEVICE` prefix.

```
4. admin_server = FILE:/var/log/kadmin.log
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#logging

2.5 Secure the KDC configuration file (kdc.conf) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The KDC configuration file contains directives that dictate how the Kerberos Authentication Service and Key Distribution Center (AS/KDC) operate. Ensure access to the KDC configuration file reflects least privilege.

Rationale:

Ensuring that access to the KDC configuration file reflects least privilege will help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/var/kerberos/krb5kdc/kdc.conf` is `root:root`.
2. Ensure the permission on `/var/kerberos/krb5kdc/kdc.conf` prevent `read`, `write`, and `execute` by `group` and `other`.

```
stat -L --format "%U:%G %a" /var/kerberos/krb5kdc/kdc.conf
```

3. Ensure the output of the above command is as follows:

```
root:root 600
```

Remediation:

1. Set the ownership on `/var/kerberos/krb5kdc/kdc.conf` to `root:root`.
2. Revoke read, write, and execute permission from `group` and `other` on `/var/kerberos/krb5kdc/kdc.conf`.

```
chmod og-rwx /var/kerberos/krb5kdc/kdc.conf
chown root:root /var/kerberos/krb5kdc/kdc.conf
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html

3 Kerberos Configuration (krb5.conf)

3.1 [libdefaults]

3.1.1 Secure the default keytab (default_keytab_name) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

A keytab is a file that contains Kerberos principles and encrypted keys. The default keytab is typically used to identify the local kerberos service to the KDC.

Rationale:

The keytab file can be used to authenticate without a password. Read access to the keytab may allow an attacker to elevate privilege or impersonate other users.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_keytab_name` directive
4. Locate the file referenced by the `default_keytab_name` directive. If the directive is not present, the implicit path is `/etc/krb5.keytab`.

5. Run the following command:

```
stat -L --format "%U:%G %a" <default_keytab_name>
```

6. Ensure the output of the above command is as follows:

```
root:root 600
```

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_keytab_name` directive
4. Locate the file referenced by the `default_keytab_name` directive. If the directive is not present, the implicit path is /etc/krb5.keytab.
5. Run the following command:

```
chmod 600 <default_keytab_name>
chown root:root <default_keytab_nane>
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.2 Ensure AES256 is the preferred encryption type for TGS (default_tgs_enctypes) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `default_tgs_enctypes` directive specifies the list of session key encryption types supported by the Kerberos library. Ensure this directive is configured to prefer AES256.

Rationale:

Setting AES256 as the preferred encryption type reduces the probability of sensitive information becoming compromised. AES256 may also be required to comply with industry and government standards.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tgs_enctypes` directive
4. Ensure the list pointed to by the `default_tgs_enctypes` directive begins with `aes-256-cts`.

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tgs_enctypes` directive
4. Insert the following value at the beginning of the list pointed to by the `default_tgs_enctypes` directive:

```
aes-256-cts
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.3 Ensure single DES-based encryption types are disallowed for TGS (default_tgs_enctypes) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `default_tgs_enctypes` directive specifies the list of session key encryption types supported by the Kerberos library. Ensure this directive disallows Single DES-based encryption types.

Rationale:

Ensuring that single DES encryption types are disallowed reduces the probability of sensitive information becoming compromised. Single DES encryption is considered "weak". Using modern hardware and cloud computing, cracking single DES is considered both affordable and fast. Some government compliance my also disallow the use of single DES.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tgs_enctypes` directive
4. Ensure the list pointed to by the `default_tgs_enctypes` directive contains no entries that start with "`des-`"

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tgs_enctypes` directive
4. Remove all entries from the list pointed to by the `default_tgs_enctypes` directive that start with "`des-`"

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.4 Ensure AES256 is the preferred encryption type for TKT (default_tkt_enctypes) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `default_tkt_enctypes` directive specifies the list of session key encryption types requested by the client. Ensure this directive is configured to prefer AES256.

Rationale:

Setting AES256 as the preferred encryption type reduces the probability of sensitive information becoming compromised. AES256 may also be required to comply with industry and government standards.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tkt_enctypes` directive

4. Ensure the list pointed to by the `default_tkt_enctypes` directive begins with `aes-256-cts`.

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tkt_enctypes` directive
4. Insert the following value at the beginning of the list pointed to by the `default_tkt_enctypes` directive:

```
aes-256-cts
```

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.5 Ensure single DES-based encryption types are disallowed for TKT (default_tkt_enctypes) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `default_tkt_enctypes` directive specifies the list of session key encryption types supported by the Kerberos library. Ensure this directive disallows single DES-based encryption types.

Rationale:

Ensuring that single DES encryption types are disallowed reduces the probability of sensitive information becoming compromised. Single DES encryption is considered "weak". Using modern hardware and cloud computing, cracking single DES is considered both affordable and fast. Some government compliance my also disallow the use of single DES.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tgs_enctypes` directive

4. Ensure the list pointed to by the `default_tgs_enctypes` directive contains no entries that start with "`des-`"

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `default_tkt_enctypes` directive
4. Remove all entries from the list pointed to by the `default_tkt_enctypes` directive that start with "`des-`"

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.6 Ensure single DES-based encryption types are not permitted (permitted_enctypes) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `permitted_enctypes` directive specifies the list of permitted encryption types. Ensure this directive disallows Single DES-based encryption types.

Rationale:

Ensuring that single DES encryption types are disallowed reduces the probability of sensitive information becoming compromised. Single DES encryption is considered "weak". Using modern hardware and cloud computing, cracking single DES is considered both affordable and fast. Some government compliance my also disallow the use of single DES.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `permitted_enctypes` directive
4. Ensure the list pointed to by the `permitted_enctypes` directive contains no entries that start with "`des-`"

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `permitted_enctypes` directive
4. Remove all entries from the list pointed to by the `permitted_enctypes` directive that start with "`des-`"

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.7 Disallow weak encryption types (allow_weak_crypto) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `allow_weak_crypto` directive determines if weak encryption types are permitted. Ensure this directive is configured to disallow weak encryption types.

Rationale:

Ensuring that weak encryption types are disallowed reduces the probability of sensitive information becoming compromised. These encryption types are considered "weak" because there are cryptographic attacks that significantly reduce the search space or the search space is small relative to modern computing power. These algorithms are typical very old and use small key sizes.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Ensure the `allow_weak_crypto` is present and set to `false`.

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `allow_weak_crypto` directive and set it to `false`.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.8 Ensure clockskew tolerance is minimized (clockskew) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `clockskew` directive determines the maximum allowable amount of clockskew in seconds that the library will tolerate before assuming that a Kerberos message is invalid. Ensure this directive is set to less than or equal to five minutes.

Rationale:

In order to prevent intruders from resetting their system clocks in order to continue to use expired tickets, Kerberos is set up to reject ticket requests from any host whose clock is not within the specified maximum clock skew of the KDC. Similarly, hosts are configured to reject responses from any KDC whose clock is not within the specified maximum clock skew of the host.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Ensure the `clockskew` directive is present and set to less than or equal to `300`.

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `clockskew` directive and set it to less than or equal to `300`.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.1.9 Ensure ignore_acceptor_hostname is not set to true (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

When accepting GSSAPI or krb5 security contexts for host-based service principals, ignore any hostname passed by the calling application and allow any service principal present in the keytab that matches the service name and realm name (if given). This option can improve the administrative flexibility of server applications on multi-homed hosts, but can compromise the security of virtual hosting environments.

Rationale:

An attacker may attempt to use alternate hostnames to bypass restrictions that the administrator has placed on the service.

Audit:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Ensure the `ignore_acceptor_hostname` directive is absent OR is present and set to `false`.

Remediation:

1. Open `/etc/krb5.conf`
2. Locate the `[libdefaults]` section
3. Locate the `ignore_acceptor_hostname` directive and set it to `false`.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html#libdefaults

3.2 [plugins]

3.2.1 Prevent blank password creation (pwqual:empty) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The password quality interface (`pwqual`) has a built-in module, named `empty`, that will reject attempts to set a blank password. Ensure the `empty` module is enabled.

Rationale:

Ensuring that blank passwords are rejected will increase the efficacy of authentication and authorization controls. If blank passwords are allowed, confidence in the identify of the actor authenticating with a given credential can not be assured.

Audit:

1. Open `/etc/krb5.conf`.
2. Locate the `[plugins]` section.
3. Locate the `pwqual interface` subsection.
4. Locate the `disable` directive.
5. Ensure `empty` is not present on the `disable` directive line.
6. If the `enable_only` directive is present, ensure `empty` is present on the `enable_only` directive line.

Remediation:

1. Open `/etc/krb5.conf`.
2. Locate the `[plugins]` section.
3. Locate the `pwqual interface` subsection.
4. Locate the `disable` directive.
5. Remove `empty` from the `disable` directive line.
6. If the `enable_only` directive is present, add `empty` to the `enable_only` directive line.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/krb_admins/conf_files/krb5_conf.html#pwqual-interface

3.2.2 Prevent dictionary word password creation (pwqual:dict) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The password quality interface (`pwqual`) has a built-in module, named `dict`, which will reject attempts to set a password that is present in the realm's dictionary file. Ensure the `dict` module is enabled.

Rationale:

Ensuring that password based on dictionary words are rejected will increase the efficacy of authentication and authorization controls. If passwords based on dictionary words are allowed, confidence in the identiyy of the actor authenticating with a given credential cannot be assured.

Audit:

1. Open `/etc/krb5.conf`.
2. Locate the `[plugins]` section.
3. Locate the `pwqual interface` subsection.
4. Locate the `disable` directive.
5. Ensure `dict` is not present on the `disable` directive line.
6. If the `enable_only` directive is present, ensure `dict` is present on the `enable_only` directive line.

Remediation:

1. Open `/etc/krb5.conf`.
2. Locate the `[plugins]` section.
3. Locate the `pwqual interface` subsection.
4. Locate the `disable` directive.
5. Remove `dict` from the `disable` directive line.
6. If the `enable_only` directive is present, add `dict` to the `enable_only` directive line.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/krb_admins/conf_files/krb5_conf.html#pwqual-interface

3.2.3 Prevent creation of passwords derived from the principal's name (pwqual:princ) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The password quality interface (`pwqual`) has a built-in module, named `princ`, which will reject attempts to set a password that is derived from the principal's name. Ensure the `princ` module is enabled.

Rationale:

Ensuring that passwords derived from the principal's name are rejected will increase the efficacy of authentication and authorization controls. If passwords derived from the principal's name are allowed, confidence in the identity of the actor authenticating with a given credential cannot be assured.

Audit:

1. Open `/etc/krb5.conf`.
2. Locate the `[plugins]` section.
3. Locate the `pwqual interface` subsection.
4. Locate the `disable` directive.
5. Ensure `princ` is not present on the `disable` directive line.
6. If the `enable_only` directive is present, ensure `princ` is present on the `enable_only` directive line.

Remediation:

1. Open `/etc/krb5.conf`.
2. Locate the `[plugins]` section.
3. Locate the `pwqual interface` subsection.
4. Locate the `disable` directive.
5. Remove `princ` from the `disable` directive line.
6. If the `enable_only` directive is present, add `princ` to the `enable_only` directive line.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/krb_admins/conf_files/krb5_conf.html#pwqual-interface

3.3 Secure the Kerberos configuration file (krb5.conf) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos configuration file contains information needed by the Kerberos library, including descriptions of realms and the location of the KDC for those realms. Ensure access to the Kerberos configuration file reflects least privilege.

Rationale:

Ensuring that access to the Kerberos configuration file reflects least privilege will help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/etc/krb5.conf is root:root.`
2. Ensure the permission on `/etc/krb5.conf prevent write by group and other.`

```
stat -L --format "%U:%G %A" /etc/krb5.conf
```

Remediation:

1. Set the ownership on `/etc/krb5.conf to root:root.`
2. Revoke write permission from `group` and `other` on `/etc/krb5.conf.`

```
chown root:root /etc/krb5.conf
chmod og-w /etc/krb5.conf
```

4 Kerberos Database Access Control List (kadm5.acl)

The Kerberos `kadmind` daemon uses an Access Control List (ACL) file to manage access rights to the Kerberos database.

4.1 Ensure kiprop principles are only allowed propagation permission (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

Principles named `kiprop/*` are used for Kerberos propagation.

Note: The ordering of permissions is important: permissions are determined by the first matching entry/glob. Please review the documentation for kadm5.acl for more details.

Rationale:

Principles used for Kerberos propagation should have restricted access to ensure principle of least-privilege.

Audit:

1. Open the `kadm5.acl` file
2. Search for lines beginning with `kiprop`
3. Ensure the second column contains only the character `p`

Remediation:

1. Open the `kadm5.acl` file
2. Search for lines beginning with `kiprop`
3. Set the second column to the character `p`

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kadm5_acl.html

4.2 Ensure kadmin/changepw principle does not have multiple key versions (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `kadmin/changepw` principle is a special principle used by the KDC to change user passwords.

Rationale:

Multiple key versions could allow an attacker to initiate replay attacks or perform offline cracking attempts against expired Kerberos credentials.

Audit:

Log into the KDC and run the following command:

```
kadmin.local -q "get_principal kadmin/changepw" | grep "^Key:" | awk {'print $3'}
```

Ensure the all the lines contain the same number.

Remediation:

Log into the KDC and run the following command:

```
kadmin.local -q "purgekeys kadmin/changepw"
```

4.3 Ensure krbtgt/<REALM> principle does not allow duplicate session keys (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `krbtgt/<REALM>` principle is the Ticket-Granting Ticket and is essential to Kerberos protocol operations.

Rationale:

Duplicate session keys could allow an attacker to spoof identities.

Audit:

Log into the KDC and run the following command:

```
kadmin.local -q "get_principal kadmin/<REALM>" | grep "^Attributes:"
```

Ensure the output contains `DISALLOW_DUP_SKEY`

Remediation:

Log into the KDC and run the following command:

```
kadmin.local -q "modify_principal -allow_dup_skey krbtgt/<REALM>"
```

4.4 Ensure krbtgt/<REALM> principle does not have multiple key versions (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The `krbtgt/<REALM>` principle is the Ticket-Granting Ticket and is essential to Kerberos protocol operations.

Rationale:

Multiple key versions could allow an attacker to initiate replay attacks or perform offline cracking attempts against expired Kerberos credentials.

Audit:

Log into the KDC and run the following command:

```
kadmin.local -q "get_principal krbtgt/<REALM>" | grep "^Key:" | awk {'print $3'}
```

Ensure the all the lines contain the same number.

Note: During a key rotation, you may choose to keep the old TGT for a short interval to prevent invalidating existing tickets. This window should be no longer than the length of the ticket expiration/renewal window.

Remediation:

Log into the KDC and run the following command:

```
kadmin.local -q "purgekeys krbtgt/<REALM>"
```

4.5 Secure the Kerberos Access Control List (kadm5.acl) (Scored)

Profile Applicability:

- KDC with DB2 Database
- KDC with LDAP Database

Description:

The Kerberos `kadmind` daemon uses `kadm5.acl` to manage access rights to the Kerberos database. Ensure access to `kadm5.acl` reflects least privilege.

Rationale:

Ensuring that access to `kadm5.acl` reflects least privilege will help ensure the integrity and availability of KDC operations.

Audit:

1. Ensure the owner of `/var/kerberos/krb5kdc/kadm5.acl` is `root:root.`
2. Ensure the permission on `/var/kerberos/krb5kdc/kadm5.acl` prevent `write` by `group` and `other.`

```
stat -L --format "%U:%G %A" /var/kerberos/krb5kdc/kadm5.acl
```

Remediation:

1. Set the ownership on `/var/kerberos/krb5kdc/kadm5.acl` to `root:root.`
2. Revoke write permission from `group` and `other` on `/var/kerberos/krb5kdc/kadm5.acl.`

```
chown root:root /var/kerberos/krb5kdc/kadm5.acl
chmod og-w /var/kerberos/krb5kdc/kadm5.acl
```

5 LDAP Object Security

This section contains considerations for securing Kerberos related objects that persist in LDAP. Items in this section are only applicable to Kerberos deployments that leverage LDAP to store the KDC database.

5.1 Restrict KDC write access to all attributes other than counters and timers (Not Scored)

Profile Applicability:

- KDC with LDAP Database

Description:

The `ldap_kdc_dn` is the LDAP object used by the KDC daemon to access the LDAP database.

Rationale:

To prevent escalation of privilege, the Kerberos server should not be allowed to access arbitrary LDAP data.

Audit:

Connect to your LDAP server and determine if the `ldap_kdc_dn` user is granted unnecessary write access. The specific steps to do so will differ by LDAP server and organizational policy.

Remediation:

Grant the `ldap_kdc_dn` write permissions on the following LDAP attributes:

- "Last successful authentication" principal field
- "Last failed authentication" principal field
- "Failed password attempts"

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

5.2 Ensure only KDC and kadmin can read attributes (Not Scored)

Profile Applicability:

- KDC with LDAP Database

Description:

The LDAP users configured in `ldap_kadmind_dn` and `ldap_kdc_dn` are used by the Keberos server to read and write Kerberos attributes in the LDAP database.

Rationale:

To prevent escalation of privilege, the Kerberos server should not be allowed to access arbitrary LDAP data.

Audit:

Connect to your LDAP server and determine if the `ldap_kadmind_dn` and `ldap_kdc_dn` users are granted unnecessary read access. The specific steps to do so will differ by LDAP server and organizational policy.

Remediation:

Configure the access controls so that the `ldap_kadmind_dn` and `ldap_kdc_dn` users have only the necessary read access.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

5.3 Ensure only kadmind (ldap_kadmind_dn) can write to all attributes (Not Scored)

Profile Applicability:

- KDC with LDAP Database

Description:

The LDAP user configured in `ldap_kadmind_dn` is used by the `kadmind` server to read and write Kerberos attributes in the LDAP database.

Rationale:

To prevent escalation of privilege, the Kerberos server should not be allowed to modify arbitrary LDAP data.

Audit:

Connect to your LDAP server and determine if the `ldap_kadmind_dn` user has the appropriate write access. The specific steps to do so will differ by LDAP server and organizational policy.

Remediation:

Configure the access controls so that the `ldap_kadmind_dn` user only has the necessary write access. The `ldap_kadmind_dn` should only have write access to the Kerberos attributes and objects in the LDAP database.

References:

1. http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/kdc_conf.html#dbmodules

Appendix: Change History

Date	Version	Changes for this version
2012-12-28	1.0.0	Initial Release