GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Kerberos Network Authentication Security Protocol Recent Security Vulnerabilities

© SANS Institute 2000 - 2002 Author retains full rights.

GIAC Level One Security Essentials
Practical Assignment for Certification
Version 1.1

Jay Holcomb

February 16, 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Kerberos Network Authentication Security Protocol – Recent Security Vulnerabilities

What is Kerberos?

Kerberos is an authentication process that attempts to secure communication between clients and servers throughout a network. In this process, the Key Distribution Center (KDC) issues "tickets" and the client must use these "tickets" to communicate (authenticate) with each server they are trying to access on the network. Kerberos uses DCS encryption for secure communication between client and server.

Please refer to my Kickstart paper "*Kerberos Network Authentication Security Protocol,*" dated January 30, 2001, for a more detailed explanation of the Kerberos Network Authentication Security Protocol.

Recent Security Vulnerabilities with Kerberos:

Recent Kerberos security advisories have included:

1. Kerberos 4 and Kerberos 4 compatible code within Kerberos 5 -- Buffer Overrun – Possibly gain root access (May 2000)
2. Kerberos 4 and Kerberos 5 (krb5-1.1x KDC implementations) -- Denial of Service – May issue "bogus" tickets or "unknown" errors (June 2000)
3. Login Security (June 2000)
4. FTPD Security (June 2000)

Specifics of the Vulnerabilities:

Buffer Overrun – Possibly gain root access (May 2000):

This security issue is with the MIT version of the Kerberos 4 protocol (other versions of the Kerberos 4 protocol are not known to be affected). With Kerberos 4 authentication (distributed from MIT), and Kerberos 4 authentication compatible code in MIT Kerberos 5, there is a buffer overrun vulnerability with the "Kerberized Berkley remote shell daemon (krshd) for at least the i386-Linux platform, and possible others."[6] (Although the known vulnerability is with the i386-Linux version, this does not mean other platforms and operating systems are immune -- patches and updates should be implemented on all platforms. The true venerability is with the krb_rd_req() function that the krshd uses.

The danger with this security vulnerability is that the attacker could compromise the krshd (remote shell daemon) which is normally run with root access. Once the attacker has accessed the krshd he/she will have root access. This issue becomes even more crucial when you consider that since you are using Kerberos 4 authentication the krshd and the associated krb_rd_req() function will be active on the realm's Key Distribution Center (KDC) server. Once an attacker breeches the KDC within a realm the entire Kerberos "secure" network has been

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

comprised, as the attacker now controls the server that issues all of the tickets and maintains the "security keys."

Denial of Service – May issue "bogus" tickets or "unknown" errors (June 2000):
This security issue is again associated with the MIT Kerberos 4 protocol and in the Kerberos 4 compatibly code within Kerberos 5 (krb5-1.1.x KDC implementations and krb5-1.2-beta1).

At least 5 buffer overflow vulnerabilities exist in these versions of the MIT Kerberos protocol. By sending the correct parameter(s) to the Key Distribution Center (KDC) server, an attacker can cause the KDC to issue "bogus tickets or to return an error of the form 'principal unknown' for all principals."[5] Once the KDC server is compromised with one of the buffer overflow conditions either the KDC will crash, or in the case of issuing bogus tickets, the KDC server will have to be restarted in order to reset the KDC and all memory buffers.

The obvious danger with this security vulnerability is that the realm's KDC can be corrupted which will prevent valid users from accessing the Kerberos security realm. The corruption varies in degree from issuing "bogus" tickets, to not allowing "authorized" users into the Kerberos realm, to causing the KDC to crash.

Login Security (June 2000):
This security issue was actually identified by attempted fixes to the "Denial Service – Buffer Overruns" listed above.

According to MIT advisors, when users upgraded to the corrected version of Kerberos 5 (without the Buffer Overflow problems), krb5-1-1.1 and used the "—without –krb4 option" there is a significant flaw in the code that allows a "dangling else statement" to open up a significant logon security breech.[8]

FTPD Security. (June 2000):
This security issue only applies to users who are running an FTP server (this particular advisory is directed towards the GSSFTP Daemon) on your Kerberos Server.
The attacker could "execute certain FTP commands without authorization."[7]
Depending on the commands, the attacker could simulate a Denial of Service attack against server, or the attacker may issue the correct commands, through a local account, and gain root access to the Kerberos server.
However, in either case, the Kerberos Server has to have the FTP service active. This security issue could easily be prevented -- simply remove/disable FTP services on your Kerberos Servers!

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Corrective Actions:

Buffer Overrun (May 2000):
Update your Kerberos Version to Kerberos 5 release krb5-1.2.1, which includes the patches for this security issue (see the MIT link below!).
If this is not possible, or practical, and you are running a version of Kerberos 5, you can disable the Kerberos 4 Authentication (backwards compatibility) -- however this has the possibility of leaving vulnerabilities with the Remote Shell Daemon. It is also recommended that the Remote Shell Daemon be disabled -- or at least install the Patch for the Remote Shell Daemon.
Patches for this security issues include:

- Krb4 buffer overruns in Kerberos 5 Release 1.0.x: krb4buf10x
- Krb4 buffer overruns in Kerberos 5 Release 1.1.1 (includes patch for Login Security discussed below!): krb4buf111

However, when installing patches and upgrades to correct his vulnerability, be careful not to create another vulnerability. For example, note the "Login Security" issue identified below – which is related to updating patches for know security vulnerabilities – Buffer Overruns! Again, the best choice is to update your Kerberos Authentication Protocol to the latest release – Kerberos 5 release krb5-1.2.1.

Denial of Service (June 2000):
Update your Kerberos Version to Kerberos 5 release krb5-1.2.1, which includes the patches for this security issue (see the MIT link below!).
Again, if it is not possible to upgrade to Kerberos 5's latest release (1.2.1), the administrator should at a minimum apply the following patches depending on the release of Kerberos that the organization is currently using:

- Patch for Kerberos 5 Release 1.0.x KDCs: Krb4kdc_10x
- Patch for Kerberos 5 Release 1.0.1 KDCs: Krb4kdc_111
- Patch for CNS KDC: Krb4kdc_cns
- "Untested" Patch for Kerberos 4 Patch 10: Krb4kdc_krb4p10

Login Security (June 2000):
Update your Kerberos Version to Kerberos 5 release krb5-1.2.1, which includes the patches for this security issue (see the MIT link below!).
This security issue is actually created when administrators try to correct the security issue, found with the Buffer Overflow/Denial of Service attack identified in the previous discussion. When users try to add the corrective patch (krb5-1.1.1) and use the option "–without –krb4," a bug in the code actually causes a major login security problem (so while the administrator fixes the Buffer Overflow security issue they also create another major security issue).
With this security issue it is extremely important that the administrator apply the correct security patch to correct this issue, in addition to still correcting the Denial of Service issues (patch app1/bsd/login.c).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As usual, the best choice is to update you Kerberos Authentication Protocol to the latest release – Kerberos 5 release krb5-1.2.1.

FTPD Security. (June 2000):
Update your Kerberos Version to Kerberos 5 release krb5-1.2.1, which includes the patches for this security issue (see the MIT link below!).
This security issue is one of the easiest to correct and prevent! Remove, or disable, any FTP service you may have on your Kerberos Servers. Especially if you are using the GSSFTP Daemon!
If FTP is critical to your organization's Kerberos Authentication realm, then update your Kerberos Protocol to Version 5 – krb5-1.2.1

How to (try to) stay ahead

This is probably the hardest part of any administrator's job -- staying ahead of the bad guys. Or at least quickly correcting known security vulnerability once it has been identified! Besides staying in touch (networking) with other system administrators who are also using Kerberos Network Security -- monitoring Kerberos specific web sites and newsgroups can be very worthwhile. In addition, it is critical that you add yourself to the security mailing lists of organizations that research, track, and issue advisories of the latest security breaches. While we all strive to "lock down" our servers and networks as much as possible, realistically we all must accept that bad guys will find a way through the best of our defenses. Where there is a challenge -- you can be sure someone is out there who will accept the challenge and eventually defeat the security one way or another.

Our job is to be vigilant, implement all known corrective patches and service packs while being prepared to quickly correct any new security vulnerabilities once they are identified!

Below are some Kerberos specific web sites, security specific web sites, and some recommended mailing lists to join to help administrators keep current and move forward with the administration of their Kerberos enabled networks.

Monitor the following Web Sites:	**Address**:
Massachusetts Institute of Technology (MIT) Kerberos Web Site	http://web.mit.edu/kerberos/www/
Global Operating Systems Technology Group, located at the Information Sciences Institute of the University of Southern California Web Site	http://www.kerberos.isi.edu

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CERT Coordination Center Web Site	http://www.cert.org
System Administration, Networking, and Security (SANS) Institute Web Site	http://www.sans.org

Add yourself to the following Mailing Lists:	**Address**:
MIT Kerberos mailing list	http://web.mit.edu/kerberos/www/mail-lists.html
CERT Advisory Mailing List	http://www.cert.org/contect_cert/certmaillist.html

Monitor the following Newsgroups:	**Address**:
Kerberos Newsgroup	comp.protocols.Kerberos

References:

1. Massachusetts Institute of Technology (MIT) Kerberos Web Site, "Security Advisories", http://web.mit.edu/kerberos/www/advisories/index.html , June 9, 2000

2. CERT Coordination Center, "CERT Advisory CA-2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services", http://www.cert.org/advisories/CA-2000-06.html , Original Release May 17, 2000. Last Updated June 27, 2000

3. CERT Coordination Center, "CERT Advisory CA-2000-11 MIT Kerberos Vulnerable to Denial-of-Service Attacks", http://www.cert.org/advisories/CA-2000-11.html , June 9, 2000

4. Massachusetts Institute of Technology (MIT) Kerberos Web Site, "Kerberos Release 1.2", http://web.mit.edu/kerberos/www/krb5-1.2/index.html , June 30, 2000

5. Massachusetts Institute of Technology (MIT) Kerberos Web Site, "Multiple Denial of Service Vulnerabilities in KRB4 KDC", http://web.mit.edu/kerberos/www/advisories/krb4kdc.txt , June 9, 2000

6. Massachusetts Institute of Technology (MIT) Kerberos Web Site, "Buffer Overrun Vulnerabilities in Kerberos", http://web.mit.edu/kerberos/www/advisories/krb4buf.txt , June 9, 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7. Massachusetts Institute of Technology (MIT) Kerberos Web Site, “Remote Root Vulnerabilities in GSSFTP Daemon”, http://web.mit.edu/kerberos/www/advisories/ftp.txt , June 14, 2000

8. Massachusetts Institute of Technology (MIT) Kerberos Web Site, “login.c”, Jeff Schiller and Tom Yu, http://web.mit.edu/kerberos/www/advisories/withoutkrb4.txt , June 10, 2000

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS