Kerberos Altyapısı NASIL

Yazan:
V. Alex Brennen
<vab (at) cryptnet.net>

Düzenleyen:
Michael Murray
Teknik gözden geçirme

Düzenleyen:
Emma Jane Hogbin
Biçimsel gözden geçirme

Çeviren:
Necdet Yücel
<nyucel (at) comu.edu.tr>

2005–10–29

Özet

Bu belge GNU/Linux ile kimlik denetiminde kullanılan Kerberos altyapısının tasarımını ve yapılandırılmasını tanımlar. Sunucuların kurulması, Kerberos yazılımı, mevcut sistemin dönüştürülmesi aşamalarını ayrıntılandırır ve sıkça sorulan sorulara yanıt verir.

Konu Başlıkları

1. Belge Hakkında 4
- *1.1. Genel Bilgi* 4
- *1.2. Çeviriler* 4
- *1.3. Yazarlar ve Katkıda Bulunanlar* 4
- *1.4. Geri bildirim* 4

2. Kerberos Altyapısının Tanıtımı 4
- *2.1. Kerberos'a Giriş* 4
- *2.2. Kerberos'un Yararları* 4
- *2.3. Kerberos Nasıl Çalışır* 5
- *2.4. Kerberos Altyapısının Ele Geçirilmesi* 6

3. Kurulum ve Yapılandırma 6
- *3.1. Yapılandırmaya Genel Bir Bakış* 6
- *3.2. Donanım* 6
- *3.3. GNU/Linux Kurulumu* 7
- *3.4. Bir Bölge Seçmek* 7
- *3.5. Kerberos Yazılımı Yapılandırması* 8
- *3.6. Yetkili Kullanıcı Yaratma* 9

4. Eşzamanlama 9
- *4.1. Eşzamanlamanın Önemi* 9
- *4.2. NTP'ye Giriş* 9
- *4.3. NTP Kurulumu ve Yapılandırması* 10

5. Kerberos Sunucusunun Birebir Kopyalanması 10
- *5.1. Birebir Kopyalamanın Tanımı* 10
- *5.2. Gerçekleme* 10
- *5.3. Bakım* 11

6. İstemci Yapılandırması 11

6.1. Genel GNU/Linux İstemci Yapılandırması . . . 11
6.2. PAM . . . 12
6.3. Apache Web Sunucusu . . . 12
6.4. Microsoft Windows . . . 13
7. Kerberos ile Yazılım Geliştirme . . . 13
7.1. Kerberos API . . . 13
A. Daha Fazla Bilgi İçin Kaynaklar . . . 14
B. Terimler Sözlüğü . . . 15

Bu çevirinin sürüm bilgileri:

1.0	Kasım 2005	NY
İlk çeviri		

Özgün belgenin sürüm bilgileri:

2.0.0	2004-05-28	VAB
DocBook XML biçemine dönüştürüldü. İçerik genel olarak güncellendi.		
1.0.3	2003-04-01	VAB
Küçük güncellemeler, düzeltmeler, yeni bağlar.		
1.0.2	2002-09-13	VAB
Küçük güncellemeler, düzeltmeler, 8.6 eklendi, yeni bağlar eklendi.		
1.0.1	2002-07-15	VAB
Küçük güncellemeler, düzeltmeler.		
1.0.0	2002-06-13	VAB
İlk sürüm.		

Feragatname

1. Belge Hakkında

1.1. Genel Bilgi

Bu belge kamu malıdır.

Belgenin güncel sürümü http://cryptnet.net/fdp/admin/kerby-«infra/en/kerby-«infra.html adresinde bulunabilir.

1.2. Çeviriler

Belge sadece aşağıdaki dillerde bulunmaktadır:

- [en[B4]] İngilizce
- [tr[B5]] Türkçe

Eğer bu belgenin başka bir dile çevirildiğini biliyorsanız ya da kendiniz çevirmek istiyorsanız lütfen bana <vab (at) cryptnet.net> haber verin. Böylece ben de çevirilmiş sürüme bağ verebilirim.

1.3. Yazarlar ve Katkıda Bulunanlar

- V. Alex Brennen[B6] (VAB[B7]) <vab (at) cryptnet.net> (Yazar)
- Nickolai Zeldovich[B8] <kolya (at) zepa.net> (Teknik öneriler ve düzeltmeler)

1.4. Geri bildirim

Lütfen katkı, yorum, düzeltme ve değerlendirmelerinizi <vab (at) cryptnet.net> adresine gönderin.

2. Kerberos Altyapısının Tanıtımı

2.1. Kerberos'a Giriş

Kerberos; Athena Projesinin bir parçası olarak MIT'de geliştirilen bir kimlik denetim sistemidir. Kerberos açık bir ağda güvenli kimlik denetimini sağlamak için şifreleme teknolojisini ve hakem olarak güvenilen bir üçüncü tarafı kullanır. Parolaların ağda düz metin olarak aktarılması kriptografik biletler kullanılarak önlenir. Kerberos Needham–Schroeder protokolünü temel alır.

Kerberos'un halen kullanımda olan iki sürümü vardır; sürüm 4 ve sürüm 5. Kerberos'un sürüm 1'den sürüm 3'e kadar olan sürümleri iç geliştirme sürümleridir ve hiç yayınlanmamışlardır. Kerberos sürüm 4'ün bilinen bir çok zayıflığı bulunduğundan kullanılmamalıdır. Bu belgede sadece Kerberos 5'e değinilmektedir. Kerberos 5 RFC1510[B9]'da tanımlanmıştır.

Kerberos Altyapısı terimi ile bir yöneticinin Kerberos protokolünü kullanarak ağda kimlik denetimi yapmasına izin veren yazılım, sunucu ve istemci yapılandırmaları kastedilir. Kerberos Altyapısı, Kerberos yazılımının kendisini, güvenli kimlik doğrulama sunucularını ve Kerberos protokolü üzerinden kimlik denetimi yapmak için yapılandırılmış sistemleri kapsar. Bu belge sizi böyle bir altyapının kurulum, yapılandırma ve yerleşim aşamalarından geçirecektir.

2.2. Kerberos'un Yararları

Kerberos protokolüne aşina olmayanlar için onu ağda kullanmanın yararları açık olmayabilir. Bununla birlikte, tüm sistem yöneticileri Kerberos'un hafifletmek için tasarlandığı sorunlara aşinadır. Parola dinlenilmesi, parola veya dosya/veritabanı çalınması ve büyük miktarda hesabın bulunduğu veri tabanlarının korunması bu sorunlardan bazılarıdır.

Uygun bir şekilde yapılandırılmış bir Kerberos Altyapısı bu sorunları adreslemenize yardımcı olarak işletmenizi daha güvenli hale getirir. Kerberos kullanımı parolaların ağda düz metin olarak iletilmesini önler. Kerberos sistemi, kullanıcı adı ve parola bilgilerinizi merkezileştirerek korunmasını ve yönetilmesini de kolaylaştırır. Son olarak, Kerberos parola bilgilerinizi yerel bir iş istasyonunda veya sunucuda tutma zorunluluğunuzu ortadan kaldırır. Böylece bir makinanın karşılaşacağı tehlikenin diğerlerini etkileme ihtimali azaltılmış olur.

Özetle, büyük bir işletmede Kerberos'un yararları; kullanıcı hesabı ve parolalaların daha kolay yönetilebilmesi sayesinde azaltılmış yönetim maliyeti ve güçlendirilmiş güvenlik olur. Daha küçük işletmelerde ise, ölçeklendirilebilir kimlik denetimi alt yapısı ve güçlendirilmiş ağ güvenliği gibi faydaları vardır.

2.3. Kerberos Nasıl Çalışır

Kerberos istemcilerin kimlik kanıtlamaları için, paylaşılan bir sırrı ve güvenilen üçüncü taraf bir hakemi kullanan bir kimlik denetim protokolüdür. Kerberos'da istemci kullanıcılar, sunucular veya yazılımlar olabilir. Güvenilen üçüncü taraf hakem ise Anahtar Dağıtım Merkezi (KDC) olarak bilinen Kerberos artalan sürecinin çalıştığı bir sunucudur. Paylaşılan sır kullanıcının kriptografik anahtara dönüştürülmüş parolasıdır. Sunucular ve yazılım sistemleri için rasgele anahtarlar üretilir.

Kerberos'da kullanıcılar yetkililerdir. KDC kullanıcılardan ve onların kimlik kanıtlamasında kullandıkları parolalarından oluşan bir veritabına sahiptir. Kerberos'da gizli anahtar bilgisinin kimlik kanıtlamada yeterli olduğu kabul edildiğinden Kerberos sunucusu bir istemcinin diğer bir istemciye kimliğini kanıtlamasında güvenilir taraf olarak kabul edilebilir. Kerberos'da kimlik kanıtlaması ağda hiç düz metin iletilmeden gerçekleştirilir. Aşağıda Kerberos protokolünün GNU/Linux'da Kerberos yazılımıyla nasıl gerçekleştirildiğini açıklayacağım.

KDC iki önemli Kerberos artalan süreci çalıştırır. Bunlar **kadmind** ve **krb5kdc**'dir. GNU/Linux artalan süreci adlandırmasında "k" ile başlayan süreçlerin Çekirdekle ilgili veya Çekirdek bölgesi süreçleri olması önerilmesine rağmen **krb5kdc** ve **kadmind** böyle süreçler değildirler. Bu iki artalan süreci root haklarıyla kullanıcı alanında çalışırlar.

kadmind Kerberos sunucusunun yönetimle ilgili sürecidir. **kadmind** yetkili kullanıcıların ve kural yapılandırma veritabanının muhafaza edilmesi için **kadmin** isimli program tarafından kullanılır. Eğer Kerberos donanımınıza **ssh** ile uzak bağlantı yapılmamasını seçmişseniz **kadmin** sunucunuzun bileşenlerini uzaktan yönetme imkanı sunar.

krb5kdc Kerberos sunucusunun yükünü taşıyan süreçtir. Kerberos kimlik denetiminde güvenilen üçüncü taraf hakem rolünü yerine getirmekle yükümlüdür. Bir kullanıcı kimliğini bir sistem veya bir servise kanıtlamak isterse KDC'den bir bilet talebinde bulunur. Bilet; istemcinin kimliği, oturum anahtarı, zaman bilgisi ve bazı diğer bilgilerden oluşan bir datagramdır. Datagram sunucunun gizli anahtarıyla şifrelenir.

Bu süreç ayrıntılı olarak şöyle çalışır; ilk olarak kimlik denetim talebi **krb5kdc** artalan sürecine gönderilir. Artalan süreci bu isteği aldığında istemciyi esas veritabanından kimlik denetimi yaparak kontrol eder. İstemcinin gizli anahtarını bu veritabanından okur ve ona geri göndermek için Bilet Veren Bilet (TGT) adında özel bilet olarak şifreler. İstemci oturum anahtarını içeren bu şifrelenmiş TGT'yi alır. Eğer istemci parolayı bilir (gizli anahtar esas veritabanında tutulur) ve başarıyla TGT'nin şifresini çözebilirse bileti oturum anahtarını da ekleyip şifreleyerek Bilet Verme Servisine (TGS) sunabilir. TGS daha sonra istemcinin özel bir sistem veya servisi kullanmasını sağlayacak yeni bir bilet yayınlar.

Sadece gizli anahtarı bilen istemcilerin şifresini çözebileceği şifrelenmiş biletlerin kullanımı sayesinde güvenli kimlik denetimi gerçekleştirilmiş olur. Tekrarlama ataklarından korunabilmek için bilete zaman bilgisi de dahil

edilir. Tekrarlama atağı; yetkisiz erişim hakkı kazanmak için daha önceden kullanılmış bir biletin sahte gösterimidir.

2.4. Kerberos Altyapısının Ele Geçirilmesi

Bir Kerberos altyapısını ele geçirmek isteyen bir saldırganın öncelikle yapacağı şey Kerberos sunucularına saldırmak olacaktır. Eğer saldırgan KDC'ye root hakkıyla erişebilirse şifrelenmiş parolaların bulunduğu veritabanına da erişebilir. Böylece saldırgan Kerberos yazılımına ve yapılandırma dosyalarına da erişebilecek ve sistemi uygunsuz erişimlere izin verecek hale getirebilecektir.

Kerberos Altyapısına saldırmanın diğer yolları tekrarlama atakları ve parola tahmin ataklarıdır. Tekrarlama atağı bir Kerberos biletinin durdurulması veya ele geçirilmesi ve ardından sahtekarlıkla yetkisiz erişim kazanmaya çalışmak için kullanılması demektir. Parola tahmini ise bir Kerberos sisteminde ağdaki bütün Kerberos biletlerinin yakalanarak onları deşiflemek için mümkün tüm parolaların denenmesidir.

Bir saldırgan altyapıya saldırmak için eskimiş bir yazılımın açıklarından faydalanabilir. Örneğin Kerberos 4'ün bilinen pek çok sorunu vardır. En önemlisi, Kerberos 4'ün şifrelemede kullandığı protokolün temel zayıflıkları vardır. Kerberos 4'ün tasarımında standart kipte DES kullanılmıştır, bu sayede bir saldırgan Kerberos biletlerinin şifrelenmiş hallerini durdurup değiştirebilmekte ve tespit edilememektedir. Bu ataklardan korunmak için Kerberos 5, üçlü DES'i CBC kipinde kullanacak şekilde değiştirilmiştir.

Kerberos 4'ün dayanıklılığını tartışırken birçok Kerberos 4 uygulamasının hafıza taşması (buffer overflow) açığına sahip olduğu unutulmamalıdır. Sürüm 4'ün hafıza taşması zayıflığını kapatacak sürüm 5 geliştirilirken Kerberos dağıtımları genellikle Kerberos 4 uygulamaları için geriye dönük uyumluluk sağlayacak şekilde dağıtıldı. Kerberos 5'deki geriye uyumluluk kodlarının hala hafıza taşması ataklarına açık olduğuna inanılmaktadır.

Sürüm 4'ün protokol zayıtlıkları ve olası hafıza taşması atakları yüzünden en iyisi Kerberos 4'ü kullanmamak ve desteklememektir.

Özetle, Kerberos altyapısının nasıl ele geçirilebileceğinin bu tanımından Kerberos sunucuların güvenliklerine birincil derecede önemin verilmesi gerektiği, güncel Kerberos yazılımı kullanılması gerektiği ve tedbirli olup iyi parolalar seçilerek iyi bir parola politikası uygulanması gerektiği sonuçları çıkarılmalıdır.

3. Kurulum ve Yapılandırma

3.1. Yapılandırmaya Genel Bir Bakış

Bu bölümde KDC olarak işlev yapacak bilgisayarların ve yazılımları yapılandırmaları anlatılacaktır. Önerilen yapılandırmalarda küçük ayarlamalar yapmak isteyebilirsiniz ama KDC'nizi yapılandırırken burada gösterilen bazı anahtar noktaları hatırlamanız çok önemli olacaktır. Bu yüzden, eğer alternatif bir yapılandırma stratejisi izlemeye karar verirseniz buradakileri anladığınızdan emin olun.

Bilgisayarlar Kerberos artalan sürecini çalıştıracak ve parolaları saklayacak olduklarından, sunucuların güvenli kalabilmeleri için bulundukları ağın güvenliği son derece önemlidir. Bu sunucuların ele geçirilmesini önlemek için mümkün olan bütün önlemleri almamız gerekir. Bu bölümdeki tüm güvenlik uyarıları dikkatle uygulanmalıdır.

Güvenlik tavsiyelerinin anahtar noktası Kerberos KDC servisi verecek sunucunun adanmış sunucu olmasıdır. Bu sunucunun fiziksel güvenliğini sağlamalı ve üzerinde çalışacak GNU/Linux'u mümkün olduğunca güçlendirmelisiniz. Eğer KDC ele geçirilirse tüm Kerberos alt yapınız ele geçirilmiş olur.

3.2. Donanım

Kerberos servisi donanıma fazlaca bağlı olmadığından ve Kerberos servisleri yedekli çalışabildiğinden sunucunun donanımı minimum olabilir. İşlettiğim Kerberos sunucularım bir PIII işlemcisi ve iki RAID 1 diski olan sunucu-lardı. Bu bilgisayarlar günde elli ila yüz bin arası kimlik denetimi yapması gereken sunuculardı. Sunucular yedekli NIC kartları ile çalıştırılırken her iki kartın birden etkin olmamasına dikkat edilmesi gerekir. Kerberos'da biletler KDC'nin IP'sini de içerdiğinden eğer bir istemci kimlik denetimi sırasında KDC'nin birden fazla arabirimi ile iletişim kurarsa kimlik denetiminde zorluklarla karşılaşabilir.

Kerberos servisinin adanmış bir sunucu üzerinde çalışmasına dikkat edilmelidir. Adanmış bir sunucu ile kas-dedilen sadece Kerberos yöneticisinin oturum açmasının gerekeceği bir sunucudur. Bu aynı zamanda, belki SSH hariç, başka hiç bir servisin çalışmaması anlamına da gelmelidir. Tüm kullanıcılarınızın parolaları Kerberos sunucuları üzerinde tutulacağından bu donanımlara erişimi mümkün olduğunca kısıtlamak iyi olacaktır. Kerberos için adanan sunucuları fiziki güvenliklerini de mümkün olduğunca sağlamak gereklidir. Kerberos sunucuları için bu güvenlik sunucuların bir kabin içerisine kilitlenmesi ve adanmış bir terminalin kullanılmasını da kapsar.

Kerberos'un yedekli çalışma özelliğinden faydalanabilmek için en az iki bilgisayar KDC olarak çalışmalıdır. Ker-beros bir ana (master) sunucu ve bir veya daha fazla yardımcı (slave) sunucu ile çalışabilecek şekilde tasar-lanmıştır. İstediğiniz kadar ikincil sunucunuz olabilir.

3.3. GNU/Linux Kurulumu

GNU/Linux kuracağımız sunucular sadece Kerberos servislerinde kullanılacağından güvenliklerini sağlamak için birkaç ilave işlem yapabiliriz.

İlk olarak, sadece Kerberos servisleri için gerekli yazılımları kuracağız. Bu tanım temel işletim sistemini ve Ker-beros yazılımını kapsar. X'i veya herhangi bir GUI uygulamasını kurmayacağız. SSH kurulumu isteğe bağlıdır. Eğer sunucuları uzaktan yönetmek isterseniz SSH kurabilirsiniz. Ama sunuculara sadece onlara bağlı termi-nalden erişmek sunucuları önemli derecede daha fazla güvenli kılar.

Fedora Core GNU/Linux'da Kerberos servisi vermek için gerekli paketler şunlardır:

```
krb5-server
krb5-libs
```

Bilgisayarları KDC servisleri haricinde bir iş için kullanmak istemediğimizden belgeler veya geliştirme kütüphaneleri kurulmayacaktır.

Sıradaki adım gerekli olmayan bütün portların kapatılması ve gerekli tüm yamaların yapılmasıdır. Hangi yönetim yazılımı kurulmuşsa onun güvenlik yamaları yapılmalıdır. Bilgisayarın hangi portları dinlediği **netstat** komutu kullanılarak öğrenilebilir. Örneğin sadece ssh çalıştıran bir bilgisayarda aşağıdaki sonucu görmelisiniz:

```
bash$ netstat -an | grep -i listen | less
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
```

Son olarak, sunucuyu sadece kimlik denetimi için gerekli sunucularla konuşacak şekilde kısıtlandırarak yapılandıracağız. Bu işlem `iptables` ile yapılabileceği gibi `/etc/hosts.allow` ve `/etc/hosts.deny` dosyalarını düzenleyerek de yapılabilir.

3.4. Bir Bölge Seçmek

Bölge adları büyük–küçük harfe duyarlıdır ve ağınızda benzersiz olmalıdır. İkinci seviye alan adınızı tümü büyük harflerle bölge adınız olarak kullanmak bir uygulama standardı olmuştur. Kerberos'u tüm ağınıza değil de bir alt ağa kuracaksanız bu alt ağın alan adını kullanmalısınız.

Bölge topolojinizi belirlerken, örgütlenmenizin tüm yapısını göz önüne almalısınız. Eğer örgütünüzün bir ya da daha fazla uzak ofisi veya bağımsız alt grubu varsa, onları ayrı bölgelere dahil etmek daha iyi olacaktır. Kerberos bölge topolojisi fiziksel ağ topolojisine değil sistem yönetim topolojisine benzemelidir.

Son olarak, miras sistemleri de örneğin Kerberos mirası veya korumak istediğiniz mevcut ağ topoloji gruplamaları (Windows NT alanı gibi) hesaba katmalısınız.

Eğer halen tüm ağında veya bir alt ağında Kerberos çalışan bir ağa Kerberos kuruyorsanız bölge isimlerinin çakışmasından kaçınmalısınız. Çalışan bir Kerberos sistemi mevcutken yeni bir Kerberos kurulmasına en çok ağların IBM SP kümelemesi içerdiği durumlarda karşılaşılır. Böyle durumlarda en iyi çözüm SP kümelemesi için üçüncü ya da daha üst seviyeden alan adında özel bir bölge yaratarak birincil Kerberos bölgeniz için ikinci seviye alan adını kullanmanız olacaktır.

Bu belgede altyapının tasarımı ve yapılandırmasının tasvirine yardımcı olmak için bir örnek kullanacağız. Örneğimiz için hayali Gnu Üniversitesini (Dublin, İrlanda) kullanacağız. Dublin Gnu Üniversitesi, öğrencilerinin ve fakültelerinin kimlik denetimi için iki Kerberos sunucusu kullanacak. Üniversitenin adresi gnud.ie olduğundan, Kerberos alanı için GNUD.IE adını kullanacağız.

3.5. Kerberos Yazılımı Yapılandırması

Şimdi Kerberos'u yapılandırmalı, bir yönetici yaratmalı, kurallarınızı belirlemeli ve Kerberos'un esas (principal) veritabanını ilklendirmelisiniz.

İlk adım `/etc/krb5.conf` yapılandırma dosyasını düzenlemektir. Bu dosyada bölge belirlenir, Kerberos sunucuları belirtilerek bölge tanımlaması genişletilir ve son olarak alan bölgesi ayarlanır. Bizim örneğimizde bu aşağıdaki gibi yapılır:

```
default_realm = GNUD.IE

[realms]
 GNUD.IE = {
  kdc = kerberos1.gnud.ie:88
  kdc = kerberos2.gnud.ie:88
  admin_server = kerberos1.gnud.ie:749
  default_domain = gnud.ie
 }

[domain_realm]
 .gnud.ie = GNUD.IE
 gnud.ie = GNUD.IE
```

Kerberos veritabanını yaratmak ve ilklendirmek için aşağıdaki komutu çalıştırmalısınız:

```
{Kerberos1}bash# /usr/Kerberos/sbin/kdb5_util create -s
```

`-s` seçeneği ile KDC'ye kendisinin kimlik denetimi için bir gizli dosya yaratması söylenir. Bir bölge belirlemek için `-r` seçeneğini kullanabilirsiniz. Yeni veritabanı için bir bölge belirlemek ancak `krb5.conf` dosyasında birden çok bölge tanımlıysa gerekli olur.

Ardından Kerberos sizden veritabanı için bir yönetici parolası ister. Bu parolayı unutmamanız çok önemlidir. Eğer bu parolayı unutursanız Kerberos'u yönetemezsiniz.

KDC'ye yönetici olarak erişebilmek için acl dosyasını düzenlemelisiniz. Bu dosya öntanımlı olarak `/var/Kerberos/krb5kdc/kadm5.acl` konumundadır. Gerekirse acl dosyasının yerini `kdc.conf` dosyanızda belirtin. `kdc.conf` dosyanızın yeri `/etc/krb5.conf` dosyasında yazar, öntanımlı olarak `/var/Kerberos/krb5kdc/kdc.conf` konumundadır. Örneğimizdeki Dublin GNU Üniversitesi için acl dosyamızı aşağıdakileri içerecek şekilde düzenleyeceğiz:

```
*/admin@GNUD.IE      *
```

Bu acl'ler *GNUD.IE* bölgesinde `/admin` ile biten bir hesabın tam erişim yetkisine sahip olduğu anlamına gelir.

Şimdi yönetici kullanıcılarımızın erişimini ayarlamalıyız; önce yönetici kullanıcıları yaratalım. Bunu KDC'de root kabuğunda **kadmin.local** komutunu **addprinc** komutu ile birlikte çalıştırarak yapabilirsiniz. Yöneticinin kullanıcı adı standart olarak *admin*'dir. Dublin GNU Üniversitesi Kerberos Yöneticisi için aşağıdaki komut yeterli olacaktır:

```
{Kerberos1}bash# /usr/Kerberos/sbin/kadmin.local -q "addprinc admin/admin"
```

Sunucuda çalışması gereken artalan süreçleri **krb5kdc** ve **kadmin**'dir. Eğer gerekirse **krb524** çalıştırılarak Kerberos 4 istemcileri için geriye dönük uyumluluk sağlanabilir. **krb524** uygulamasını çalıştırmadan önce Kerberos 4 ile ilgili güvenlik uyarılarımızı hatırlayın ve ancak mutlaka bu işlevin gerekli olduğundan emin olduğunuzda çalıştırın. **krb5kdc** ve **kadmin**'nin KDC'de otomatik başlayacak şekilde yapılandırılması için **chkconfig** komutu kullanılabilir.

```
{Kerberos1}bash# /sbin/chkconfig krb5kdc on
{Kerberos1}bash# /sbin/chkconfig kadmin on
```

Son olarak, aşağıdaki komutları kullanarak elle başlatalım:

```
{Kerberos1}bash# /etc/rc.d/init.d/krb5kdc start
{Kerberos1}bash# /etc/rc.d/init.d/kadmin start
```

ve artık çalışan bir KDC'miz var.

3.6. Yetkili Kullanıcı Yaratma

Aşağıdaki komutla Kerberos'da ilk yetkili kullanıcınızı yaratabilirsiniz:

```
{Kerberos1}bash# kadmin.local
{Kerberos1}kadmin.local: addprinc kullanıcıismi
```

Kerberos ile destekleyeceğiniz çok sayıda kullanıcınız varsa hesapların açılması için bir betik yazılabilir.

4. Eşzamanlama

4.1. Eşzamanlamanın Önemi

Kerberos kimlik denetimi kısmen biletlerin zaman bilgisine dayandığı için, Kerberos sunucuların saatlerinin dakik olarak ayarlanması kritik öneme sahiptir. Kerberos'a giriş bölümünde bahsettiğimiz gibi saldırganların tüm parolaları denedikleri veya tekrarlama atağı yaptıkları durumlarda başarısız olmaları için biletlerin yaşam süreleri çok kısa tutulur.

Sunucularınızın saatlerinin birbirinden farklı olmasına izin verirseniz, ağınız bu tür ataklara karşı savunmasız olur. Eşzamanlama Kerberos protokolünün güvenliğinde bu derece önemli olduğundan, saatler kabul edilebilir bir aralık içinde eşzamanlanmamışsa Kerberos kaçınılmaz hatalar raporlayacak ve çalışmayacaktır. Saati hatalı bir bilgisayardan kimlik doğrulaması yapmaya çalışan istemcilerin saatleri KDC'den farklı olacağından KDC tarafından reddedileceklerdir.

4.2. NTP'ye Giriş

Ağ Zaman Protokolü (NTP) sunucuların saatlerini eşzamanlamak için kullanılır. Eşzamanlama için genel kullanıma açık NTP sunucuları bulunmaktadır. NTP istemcilerin saatlerini LAN üzerinden milisaniyede, WAN üzerinden ise onlarca milisaniyede eşzamanlayabilir. NTP sunucuları katmanlara ayrılırlar. Birincil NTP sunucuları 1. katman olarak sınıflanır. Bu genel kullanıma açık sunucuların sayıları göreceli olarak az olduğundan

istemcilerin saatlerini eşzamanlamak için kullanılmamalıdır. 2. katman genel kullanıma açık sunucular istemcileri eşzamanlamak için kullanılırlar ve kendi saatlerini 1. katman sunuculardan eşzamanlayabilirler. Kerberos sunucularımız için NTP'yi ikinci katmandan üç sunucudan sorgulama yapacak şekilde yapılandıracağız. Genel kullanıma açık ikinci katman sunucuların güncel bir listesi burada [B10] bulunabilir.

4.3. NTP Kurulumu ve Yapılandırması

GNU/Linux üzerinde NTP'yi etkinleştirmek için NTP paketini kurmalı ve yapılandırma dosyasının adını değiştirmelisiniz. Öntanımlı olarak NTP yapılandırma dosyasının adı `/etc/ntp.conf`'dur. Yapılandırmanın öntanımlı değerleri, kabul edilebilir değerlerdir. Bütün ihtiyacımız olan saatlerimizi eşzamanlamakta kullanacağımız sunucuları eklemektir. Kimlik denetimi gerekli değildir ama yapılması güvenliği arttırır. Eğer kendi ağınızdaki NTP sunucularını kullanıyorsanız kimlik denetimini kullanabilirsiniz. Örnek bir `ntp.conf` [B11] dosyasını inceleyebilirsiniz.

Son olarak gerçek eşzamanlamayı gerçekleştirmek için cron'a bir görev ekliyoruz:

```
30 * * * * /usr/sbin/ntpdate -s
```

Eğer sistemleriniz bir güvenlik duvarının arkasındaysa `-s` yerine `-su` kullanmanız gerekebilir. `-u` seçeneği ile **`ntpdate`** ikinci katman sunuculara bağlantısını imtiyazlı olmayan bir portu kullanarak gerçekleştirir.

5. Kerberos Sunucusunun Birebir Kopyalanması

5.1. Birebir Kopyalamanın Tanımı

Kerberos ana/yardımcı birebir kopyalama kümelemesine izin verecek şekilde tasarlanmıştır. Bir kerberos kümelemesinde istenilen sayıda düğüm olabilmesine rağmen en az iki adet olması önerilmektedir. Birincil sunucu olarak bir ana sunucu ve onu yedeklemek için en az bir yardımcı sunucu bulunmalıdır. Ana ve yardımcı sunucular birincil ve ikincil sunucular olarak düşünülebilirler.

Kerberos hesaplar ve kurallar ile ilgili tüm verilerini bir uygulama veritabanında tutar. Kerberos yazılımı bu verileri diğer sunuculara yedekleyecek veya kopyalayacak yazılımları da içerir.

Kerberos istemci uygulamaları eğer birincil sunucuya ulaşılamaz ise ikincil sunucudan kimlik denetimi yapmayı deneyecek şekilde tasarlanmıştır. Bu yüzden bir sistem arızası durumunda Kerberos kimlik denetimi servisinin yedekleme sunucusundan yapılması için ilave bir çaba harcamanıza gerek yoktur. Kerberos'un yönetimsel özellikleri otomatik hata telafisini içermez.

Birincil sunucunuzun erişilemez olması durumunda **`kadmind`** erişilemez olacaktır. Bu nedenle sunucu tamir edilene veya değiştirilene kadar yönetimsel işlevler çalışmayacaktır. Özellikle yetkili kullanıcı yönetimi, anahtar üretimi ve anahtar değişimi birincil sunucu çalışmadığı sürece yapılamayacaktır.

5.2. Gerçekleme

Sunucunun birebir kopyalaması **`kprop`** komutu ile yapılır. **`kprop`** komutu birincil ana KDC üzerinde çalıştırılmalıdır. Zamanlandırılmış bir görev olarak çalıştırılmalı ve esas veritabanının tüm sunucularda eşzamanlı olması sağlanmalıdır.

Sunucuyu birebir kopyalamanın ilk adımı, **`kpropd`** için ACL'ler hazırlamaktır. **`kpropd`** acl dosya adları öntanımlı olarak `/var/Kerberos/krb5kdc/kpropd.acl` dosyasında bulunur. Bizim örneğimizde içerik aşağıdaki gibi olacaktır:

```
host/kerberos1.gnud.ie@GNUD.IE
```

```
host/kerberos2.gnud.ie@GNUD.IE
```

`kpropd.acl` dosyası sadece yardımcı Kerberos sunucularında bulunmalıdır. Fedora GNU/Linux'da, `/var/Kerberos/krb5kdc/kpropd.acl` dosyasının bulunduğu bir Kerberos sunucusunda **kadmin** çalışmayacaktır.

Sıradaki adımda ana ve yardımcı Kerberos sunucularınız için konak anahtarlarını yaratmanız gerekir:

```
{Kerberos1}bash# kadmin.local
{Kerberos1}kadmin.local:  addprinc -randkey host/kerberos1.gnud.ie
{Kerberos1}kadmin.local:  addprinc -randkey host/kerberos2.gnud.ie
```

Şimdi bu anahtarların `keytab` dosyasından çıkartılması gereklidir. `keytab` dosyası kriptografik anahtarları içerir ve KDC ile kimlik kanıtlaması yapmak için kritik önem taşır. Anahtarların çıkartılması **ktadd** alt komutu ile yapılır:

```
{Kerberos1}kadmin.local:  ktadd host/kerberos1.gnud.ie
{Kerberos1}kadmin.local:  ktadd host/kerberos2.gnud.ie
```

Son olarak, kimlik kanıtlamasında kullanabilmeleri için `keytab` dosyasını yardımcı sunuculara kopyalamanız gereklidir.

```
{Kerberos2}bash# scp root@kerberos1.gnud.ie:/etc/krb5.keytab /etc
```

Aşağıda her onbeş dakikada bir Kerberos sunucusunda çalışacak ve esas veritabanını eşleyecek crontab girdisi bulunmaktadır:

```
15 * * * * /usr/local/bin/krb5prop.sh
```

`krb5prop.sh` betiğinin içeriği şöyledir:

```
#!/bin/sh

/usr/Kerberos/sbin/kdb5_util dump /var/Kerberos/krb5kdc/slave_datatrans

/usr/Kerberos/sbin/kprop -f /var/Kerberos/krb5kdc/slave_datatrans kerberos2.gnud.ie > /
```

Bu komutu ilk olarak elle çalıştırdığınızda aşağıdakine benzer bir çıktı almalısınız:

```
{Kerberos1}bash# /usr/Kerberos/sbin/kdb5_util dump /var/Kerberos/krb5kdc/slave_datatran
{Kerberos1}bash# /usr/Kerberos/sbin/kprop -d -f /var/Kerberos/krb5kdc/slave_datatrans k
3234 bytes sent.
Database propagation to kerberos2.gnud.ie: SUCCEEDED
{Kerberos1}bash#
```

Yardımcı sunucu artık esas veritabanını ana sunucudan eşleyecektir.

5.3. Bakım

Bu cron betikleri ile esas yayılımın yeterince otomatikleşmiş olması ve ilave bakıma ihtiyaç duymaması gerekir. Birincil KDC'nin çalışmaması durumunda arıza uzun sürmedikçe insan müdahalesine gerek olmaz.

6. İstemci Yapılandırması

6.1. Genel GNU/Linux İstemci Yapılandırması

Kerberos'un GNU/Linux dağıtımları KDC ile Kerberos kimlik denetiminde istemcilerin ihtiyaç duyacakları bütün yazılımları ve yapılandırma dosyalarını içerirler. Fedora GNU/Linux'da bu paket *krb5–workstation* paketidir. Sisteminizin ve uygulamalarınızın Kerberos kimlik denetimi yapabilmesi için sisteminizde Kerberos'u yapılandırmanız gerekir.

Yapılandırma için `/etc/krb5.conf` dosyası düzenlenmelidir. Bu dosyada bölge, KDC'ler, yönetim sunucusu, öntanımlı etki alanı ve KDC bilgisi belirtilmelidir. `krb5.conf` dosyasında yeri belirtilen `kdc.conf` dosyası da düzenlenmelidir. Bu dosya öntanımlı olarak `/var/Kerberos/krb5kdc/kdc.conf` adresindedir. `kdc.conf` dosyasında bölgenin şifreleme algortima politikası bilgisi bulunur.

Kerberos kimlik denetimini gerçekleştirmek istediğiniz sistemin yapılandırma bilgisi, KDC'deki `/etc/krb5.conf` dosyasındaki bilginin aynısıdır. İstemci için örnek `krb5.conf`[B12] ve `kdc.conf`[B13] dosyalarını inceleyebilirsiniz.

Artık Kerberos kimlik denetimini **`kinit`** komutunu kullanarak deneyebilirsiniz:

```
bash$ kinit kullanıcıismi
```

Eğer kimlik denetimi başarısız olursa, nedenini öğrenmek için bakılacak en iyi yerler; istemcinin sistem kayıt dosyaları ve KDC kayıt dosyasıdır. Kimlik denetimi sorunlarının analizinde KDC'de bir terminal penceresi açıp kayıt dosyaları için *tail –f* komutunu çalıştırmanız oldukça yararlı olacaktır. Örnek `krb5.conf` dosyamızda KDC kayıt dosyası `/var/log/Kerberos/krb5kdc.log`'dur.

6.2. PAM

Birçok GNU/Linux dağıtımı ile birlikte gelen PAM (Pluggable Authentication Module) teknolojisi **`pam_krb5`** modülü ile Kerberos'la bütünleştirilebilir. Kerberos kimlik denetimini PAM ile kullanmak için **`pam_krb5`** modülünü yüklemeli ve PAM yapılandırma dosyalarını düzenlemelisiniz.

`pam_krb5` modülü ile birlikte `/usr/share/doc/pam_krb5-1.55/pam.d` dizininde örnek yapılandırma dosyaları da gelir. Bu yapılandırma dosyalarında yapılacak temel değişiklik, PAM'ın kontrol ettiği servislerin Kerberos'tan kimlik denetimi yapmalarını aşağıdaki gibi sağlamaktır:

```
auth       required     /lib/security/pam_krb5.so use_first_pass
```

6.3. Apache Web Sunucusu

Kerberos Apache Web Sunucusu için bir kimlik denetimi mekanizması olarak kullanılabilir. Bu görevi bir apache modülü olan **`mod_auth_kerb`** yerine getirir. Bu modülü kullanarak, Kerberos'u `httpd.conf` dosyasında bir erişim denetimi türü olarak ayarlamak mümkündür. Kerberos kullanıldığı sürece, bunun kimlik denetiminde ideal mekanizma olmadığı unutulmamalıdır. Çünkü biletler istemcide değil web sunucuda tutulmaktadır. Bununla birlikte, eğer hedefiniz bir oturum açma çözümü üretmek veya hesapları bir yerde toplamaksa işinizi görecektir. **`mod_auth_kerb`** Kerberos 4'ü destekleyebiliyor olmasına rağmen Kerberos 4'ün bilinen zayıflıkları yüzünden bu özellikten bu belgede bahsedilmeyecektir.

`mod_auth_kerb` uygulamasının web adresi `http://modauthkerb.sourceforge.net/`'tir. **`mod_auth_kerb`** kullanan bir siteye erişilmek istendiğinde HTTPS protokolü kullanmak önemlidir çünkü **`mod_auth_kerb`** temel kimlik denetimi mekanizmasını kullanır. Temel kimlik denetimi kolaylıkla çözülebilecek 64 bit şifreleme kullandığı için kimlik denetimindeki kullanıcı adı ve parola değişiminin SSL ile şifrelenerek yapılması web sunucuya güvenli gönderilmelerini sağlamak için önemlidir.

Apache'yi **`mod_auth_krb`** modülü ile birlikte derlemek için aşağıdaki adımları takip etmelisiniz:

```
bash$ export 'LIBS=-L/usr/Kerberos/lib -lkrb5 -lcrypto -lcom_err'
bash$ export 'CFLAGS=-DKRB5 -DKRB_DEF_REALM=\\"GNUD.IE\\"'
```

```
bash$ export 'INCLUDES=-I/usr/Kerberos/include'
bash$ mkdir apache_x.x.x/src/modules/kerberos
bash$ cp mod_auth_kerb-x.x.x.c apache_x.x.x/src/modules/kerberos
bash$ ./configure --prefix=/home/httpd --add-module=src/modules/Kerberos/mod_auth_kerb.
bash$ make
bash$ make install
```

Çalıştığından emin olmak için apache'yi denemelisiniz. Apache'nin SSL ile çalıştığını gördükten sonra `httpd.conf` dosyasını düzenleyerek belli bir dizin için Kerberos kimlik denetimini sağlayabilirsiniz:

Aşağıda belli bir dizin için Kerberos 5 kimlik denetimini etkin hale getiren bir `mod_auth_kerb` apache modül örneği bulacaksınız:

```
<Directory "/home/httpd/htdocs/content">
   AllowOverride None
   AuthType KerberosV5
   AuthName "Kerberos Login"
   KrbAuthRealm GNUD.IE
   require valid-user
</Directory>
```

6.4. Microsoft Windows

Kerberos standardının Microsoft tarafından kusurlu uygulanması sonucu, standart MIT Kerberos ile Microsoft'un Kerberos'u arasında kısıtlı bir uyumluluk vardır. Microsoft kendi kırık Kerberos sürümünün standart Kerberos ile birlikte çalışabilmesinin kısıtlı yöntemlerini açıklayan bir belge yayınlamıştır. Belgeye buradan[B15] ulaşılabilir.

7. Kerberos ile Yazılım Geliştirme

7.1. Kerberos API

Kerberos geliştirme kitaplıkları Kerberos'u etkinleştirmenize ya da herhangi bir uygulamayı kerberoslaştırmanıza izin verir. İki temel kitaplık mevcuttur. Biri genel kullanım Kerberos kitaplığıdır ve temel kulanıcı doğrulaması için kullanılır. Diğeri ise yönetim kitaplığıdır, kurallar üzerinde işlemler gibi yönetim işlevleri için kullanılır. Fedora GNU/Linux'da yeralan `krb5-devel` rpm dosyası geliştirme kitaplıklarını ve belgelendirmeyi içerir. Bu kitaplıkların API ayrıntıları çoğu Kerberos dağıtımına dahil edilen belgelerde bulunabilir. Bu dizin Fedora GNU/Linux'da `/usr/share/doc/krb5-devel-1.2.2/api` dizinidir.

Belgeler LaTeX biçeminde olduğundan görüntülemek için dvi dosyalarını üretmeniz gerekir. Bu dosyaları **xdiv** ile görüntüleyebilirsiniz. Bütün bunlar aşağıdaki komutlarla yapılabilir:

```
bash$ cd /usr/share/doc/krb5-devel-x.x.x/api/
bash$ su
bash# make
bash# (^d)
bash$ xdvi library.dvi
```

A. Daha Fazla Bilgi İçin Kaynaklar

İlgili Belgeler

- Kerberos V5 Kurulum Rehberi[B16]
- Kerberos V5 UNIX Kullanıcı Rehberi[B17]
- Kerberos V5 Sistem Yöneticisi Rehberi[B18]
- Kerberos V4'den Kerberos V5'e Geçiş[B19]
- Kerberos SSS[B20]
- Bir Kimlik Denetimi Tasarımı: Dört Perdelik Diyalog[B21]
- Sitenizi Nasıl Kerberoslaştırabilirsiniz[B22]
- Moron'lar İçin Kerberos Rehberi[B23]
- AFS SSS[B24]
- Kerberos 5 API[B25]
- Kerberos 5 Yönetici API[B26]

İlgili Adresler

- MIT Kerberos Web sitesi[B27]
- NTP Ana Sayfası[B28]
- 2. kademe halka açık NTP Sunucuları listesi[B29]
- OpenAFS Web sitesi[B30]
- Heimdal Kerberos Web sitesi[B31]
- The Crypto Publishing Project[B32] (Kerberos kaynak kodu için sınırlamasız kaynak)
- SESAME[B33] (Secure European System for Applications in a Multi–vendor Environment)

İlgili RFC'ler

- RFC2744: Generic Security Service API Version 2: C–bindings[B34]
- RFC2743: Generic Security Service Application Program Interface, Version 2 Update 1[B35]
- RFC2712: Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)[B36]
- RFC2078: Generic Security Service Application Program Interface, Version 2[B37]
- RFC1964: The Kerberos Version 5 GSS–API Mechanism[B38]
- RFC1510: The Kerberos Network Authentication Service (V5)[B39]
- RFC1509: Generic Security Service API : C–bindings[B40]

- RFC1508: Generic Security Service Application Program Interface[B41]
- RFC1411: Telnet Authentication: Kerberos Version 4[B42]
- RFC1305: Network Time Protocol (Version 3) Specification, Implementation and Analysis[B43]
- RFC1119: Network Time Protocol (Version 2) Specification and Implementation[B44]
- RFC1059: Network Time Protocol (Version 1) Specification and Implementation[B45]
- RFC958: Network Time Protocol (NTP)[B46]

Diğer Kaynaklar

- [Uygulamalı Kriptografi] İkinci Baskı, Bruce Schneier [ISBN: 0–471–11709–9[B47]]

İlave Kaynaklar

- Kerberos Kullanıcı Denetim Sistemi E–posta Listesi[B48]
- Kerberos Kullanıcı Denetim Sistemi E–posta Listesi Arşivi[B49]
- comp.protocols.kerberos[B50] UseNet Haber grubu

Uzman Kerberos Danışmanlık Hizmeti Veren Firmalar

- Cybersafe, Ltd.[B51]
- e–TechServices.com, Inc.[B52] IBM Business Partner

B. Terimler Sözlüğü

Ağ Zaman Protokolü [NTP]
: Konakların ve yönlendiricilerin saatlerini Internetten eşzamanlamaları için kullanılan protokol.

Anahtar Dağıtım Merkezi [KDC]
: Kerberos protokolünde güvenilen hakem rolünü oynayan yazılım ve bilgisayar.

ASN.1
: Abstract Syntax Notation One. ASN.1 mesaj tanımlamak için kullanılan bir notasyondur. Mesajları ardışık bileşenler olarak tanımlar. ASN.1 Kerberos datagramlarını tanımlamada kullanılır. Eğer yazılım geliştiricisi değilseniz ASN.1 bilgisine ihtiyacınız yoktur.

Bilet
: Sunucunun gizli anahtarı ile şifrelenmiş, istemcinin kimliği, oturum anahtarı, zaman bilgisi ve diğer bilgilerden oluşan veri iletisidir. Kimlik kanıtlamasında kullanılır.

Bilet Veren Bilet [TGT]
: İstemci ile KDC'nin iletişiminde kullanılan oturum anahtarını içeren bilet.

Bilet Verme Servisi [TGS]
: İstemcilere Bilet Veren Bilet'i (TGT) almalarından sonra bilet vermeye yetkili servis.

Bölge

Kerberos'un kapsama alanıdır. KDC'nin yetkili kullanıcılar için kimlik denetiminde güvenilir olacağı işletme alanıdır.

Çapraz Bölge Kimlik Denetimi
: Eğer iki farklı bölgenin sırları KDC'ler tarafından paylaşılırsa, bir bölgenin yetkili kullanıcısı diğer bir bölgenin KDC'sinde kimlik kanıtlaması yapabilir. Bu bölgeler arası kimlik denetimine çapraz bölgeli kimlik denetimi denir.

Geçerli olacak bilet
: Kerberos 5'de başlangıçta geçersiz olmasına rağmen gelecekte geçerli hale gelen bilet. Normal Kerberos biletleri yaratıldıkları zamandan izin verilen sürenin sonuna kadar geçerlidirler.

Geçişli Çapraz Bölgeli Kimlik Denetimi
: Kerberos 5'de, bölgeler arasında bir güven yolu etkisi yaratarak, eğer X ve Z bölgeleri Y bölgesi ile bir sırrı paylaşmışlar ise Z bölgesindeki bir kullanıcı ile kimlik kanıtlaması yapmak isteyen X bölgesindeki bir kullanıcının X bölgesindeki KDC'nin Z bölgesi ile bir sır paylaşmadan kimlik kanıtlaması yapabilmesidir.Y bölgesi güven yolunda "sıçramak" için kullanılabilir.

Genel Güvenlik Servisleri Uygulama Programlama Arayüzü [GSS–API]
: Kullanıcılarına güvenlik servisleri sağlayan C dili atamaları (bindings) kümesi. Bu API bir çok kriptografik sistemde gerçeklenebilir. Kerberos böyle sistemlere bir örnektir.

Gizli Dosya
: Gizli anahtarları içeren dosya.

İletilebilir Bilet
: Kullanıcının farklı IP adreslerinden ilave biletler talep etmesine izin veren KDC tarafından verilen bilet. Aslında, kimlik doğrulaması yapmış bir yetkili kullanıcının diğer bilgisayarlarda geçerli biletler talep etmesine izin veren bir TGT.

Kanıt
: Sunucu için bir bilet ve yetkili kullanıcının kimliğini kanıtlaması için kullanılan oturum anahtarı.

Kanıtlayıcı
: Sadece istemci ve sunucunun bildiği oturum anahtarını kullanarak yakın zamanda yaratıldığını gösterebilecek bilgiyi içeren kayıt. (Tanım RFC1510[B53]'den alınmıştır.)

Kerberos
: İstemcilerin kimlik denetiminin TCP/IP ağında güvenilen bir üçüncü taraf hakem kullanılarak yapıldığı bir kimlik denetim protokolü. Bu protokol ağda geleneksel düz metin parolaları iletmek yerine şifrelenmiş biletleri kullanacak şekilde tasarlandığı için güvenli kimlik denetimine imkan sağlar.

Kerberoslaştırmak
: (f.) Bir sistemi, servisi veya yazılım parçasını Kerberos protokolünü kullanarak kimlik denetimi yapabilecek şekilde değiştirmek.

  (sıfat), kerberoslaşmış: Kerberos üzerinden kimlik denetimini destekleyen sistem, servis veya yazılım parçası.

Ön Kimlik denetimi
: KDC'nin bir yetkili kullanıcıya TGT vermeden önce devreye giren ilave kimlik denetimi. Böyle bir kimlik denetimine bir örnek biyometrik sistemler verilebilir.

Tuz (Salt)

Verilen bir düz metinden oluşturulacak şifreli metinlerin sayısını arttırmak için, düz metin parolasını şifrelemede kullanılan başlangıç değeri. Bu başlangıç değerini kullanmak şifrelenmiş parolaları sözlük ataklarına karşı daha dirençli hale getirmek için kullanılır.

Üçlü DES
: DES'in verinin iki farklı anahtar kullanılarak standart DES ile üç kez şifrelendiği bir türevi.

Vekil Bilet
: Kerberos 5'de farklı bir IP adresi için bir TGT talep etmenize izin veren bilet.

Veri Şifreleme Standardı [DES]
: Birleşik Devletlerin şifrelemede kullanılmış resmi algoritmasıdır. NSA'nın desteğiyle IBM tarafından geliştirilmiştir. Algoritma 64 bit bloklar ve 56 bit anahtarlar kullanarak 16 tur blok şifreleme yapar.

Yenilenebilir Bilet
: Kerberos 5'de yetkili kullanıcının standart bilet yaşam süresine ek olarak maksimum yenilenebilir yaşam süresi eklenmiş bilet. Yenilenebilir biletler geçerli oldukları sürece KDC'den ilave biletler istemek için kullanılabilirler. Yenilenmiş biletler özgün yenilenebilir biletin azami yenilenebilir yaşam süresince talep edilebilirler.

Yetkili
: KDC veritabanında gizli anahtarı bulunan kullanıcı veya sunucu.

Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(*B1*) http://cryptnet.net/people/vab/

(*B2*) http://cryptnet.net/people/vab/

(*B4*) http://cryptnet.net/fdp/admin/kerby-«infra/en/kerby-«infra.html

(*B5*) http://www.belgeler.org/howto/kerberos-«howto-«howto.html

(*B6*) http://cryptnet.net/people/vab/

(*B7*) http://cryptnet.net/people/vab/

(*B8*) http://kolya.net/

(*B9*) http://cryptnet.net/mirrors/rfcs/rfc1510.txt

(*B10*) http://www.eecis.udel.edu/~mills/ntp/clock2b.html

(*B11*) http://cryptnet.net/fdp/admin/kerby-«infra/en/ntp.conf

(*B12*) http://cryptnet.net/fdp/admin/kerby-«infra/en/krb5.conf

(*B13*) http://cryptnet.net/fdp/admin/kerby-«infra/en/kdc.conf

(*B15*) http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp

(B16) http://web.mit.edu/kerberos/www/krb5-«1.2/krb5-«1.2.6/doc/install_toc.html

(B17) http://web.mit.edu/kerberos/www/krb5-«1.2/krb5-«1.2.6/doc/user-«guide_toc.html

(B18) http://web.mit.edu/kerberos/www/krb5-«1.2/krb5-«1.2.6/doc/admin_toc.html

(B19) http://web.mit.edu/kerberos/www/krb5-«1.2/krb5-«1.2.6/doc/krb425_toc.html

(B20) http://www.nrl.navy.mil/CCS/people/kenh/kerberos-«faq.html

(B21) http://web.mit.edu/kerberos/www/dialogue.html

(B22) http://www.ornl.gov/~jar/HowToKerb.html

(B23) http://www.isi.edu/gost/brian/security/kerberos.html

(B24) http://www.angelfire.com/hi/plutonic/afs-«faq.html

(B25) http://cryptnet.net/mirrors/docs/krb5api.html

(B26) http://cryptnet.net/mirrors/docs/krb5adm_api.html

(B27) http://web.mit.edu/kerberos/www/

(B28) http://www.ntp.org/

(B29) http://www.eecis.udel.edu/~mills/ntp/clock2b.html

(B30) http://www.openafs.org/

(B31) http://www.pdc.kth.se/heimdal/

(B32) http://www.crypto-«publish.org/

(B33) http://www.cosic.esat.kuleuven.ac.be/sesame/

(B34) http://cryptnet.net/mirrors/rfcs/rfc2744.txt

(B35) http://cryptnet.net/mirrors/rfcs/rfc2743.txt

(B36) http://cryptnet.net/mirrors/rfcs/rfc2712.txt

(B37) http://cryptnet.net/mirrors/rfcs/rfc2078.txt

(B38) http://cryptnet.net/mirrors/rfcs/rfc1964.txt

(B39) http://cryptnet.net/mirrors/rfcs/rfc1510.txt

(B40) http://cryptnet.net/mirrors/rfcs/rfc1509.txt

(B41) http://cryptnet.net/mirrors/rfcs/rfc1508.txt

(B42) http://cryptnet.net/mirrors/rfcs/rfc1411.txt

(B43) http://cryptnet.net/mirrors/rfcs/rfc1305.txt

(B44) http://cryptnet.net/mirrors/rfcs/rfc1119.txt

(B45) http://cryptnet.net/mirrors/rfcs/rfc1059.txt

(B46) http://cryptnet.net/mirrors/rfcs/rfc958.txt

(B47) http://www.amazon.com/exec/obidos/tg/detail/-«/0471117099/qid%3D1085516723/sr%3D11-«1/ref%3Dsr%5F11%5F1/103-«3431487-«6727030?v=glance

(B48) http://mailman.mit.edu/mailman/listinfo/kerberos

(B49) http://mailman.mit.edu/pipermail/kerberos/

(B50) news:comp.protocols.kerberos

(B51) http://www.cybersafe.ltd.uk/

(B52) http://www.e-«techservices.com/solutions/kerberos/

(B53) http://cryptnet.net/mirrors/rfcs/rfc1510.txt

Bu dosya (kerberos-howto.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

23 Ocak 2007