Linux Güvenlik NASIL

Çeviren: Tufan Karadere

<tufank (at) gmail.com>

Yazan: Kevin Fenzi

tummy.com, ltd.

<kevin-securityhowto (at) tummy.com>

Yazan: Dave Wreski

linuxsecurity.com

<dave (at) linuxsecurity.com>

v2.4, 26 Ocak 2004

Gelişim

Bu çevirinin sürüm bilgileri:

Sürüm 2.4.1	9 Ekim 2006	Tufan Karadere <tufank (at) gmail.com>

Gelişim

Özgün belgenin sürüm bilgileri:

Sürüm 2.4	26 Ocak 2004	Kevin Fenzi <kevin-securityhowto (at) tummy.com> Dave Wreski <dave (at) linuxsecurity.com>

Özet

Bu belgede, Linux sistem yöneticilerinin yüzyüze geldiği güvenlik konularına genel bir bakış açısı, genel güvenlik felsefesi ile birlikte Linux sisteminizi daha güvenli hale getirebilmeniz için örnekler, ve güvenlik ile ilgili program ve bilgilere daha kolay erişebilmeniz için referanslar bulunmaktadır. Geliştirme, yapıcı eleştiri, ekleme veya düzeltmelerinizi, ve geribildiriminizi her iki yazara da konu kısmında "Security HOWTO" yazan bir e-mektup ile (İngilizce olarak) iletebilirsiniz.[1]

İçindekiler

Giriş

Bu belge Linux güvenliğini etkileyen ana konuları kapsıyor, ve genel felsefe ve İnternet kaynakları tartışılıyor.

Bazı NASIL belgelerinin güvenlik konusunda ortak olarak içerdiği bölümler olabilir, uygun olan yerlerde bu belirtilmiştir.

Bu belge güncel bir güvenlik açıkları listesi *değildir*. Her geçen gün yeni güvenlik açıkları ortaya çıkmaktadır. Bu belge, size daha çok bu güncel bilgilerin nerelerde bulunduğunu söyleyecek, ve güvenlik açıklarını engelleyebilmek için bazı genel yöntemlerden bahsedecektir.

Bu Belgenin Yeni Sürümleri

Bu belgenin yeni sürümleri *comp.os.linux.answers* haber grubuna düzenli olarak postalanacak, ayrıca:

http://www.linuxdoc.org/

gibi sitelere de eklenecektir

Bu belgenin en son sürümü, çeşitli belge biçimlerinde,

- http://scrye.com/~kevin/lsh/
- http://www.linuxsecurity.com/docs/Security-HOWTO
- http://www.tummy.com/security-howto

adreslerinden ulaşılabilir olmalı.[2]

Geribildirim

Bütün yorumlar, hata raporları, ek bilgi ve her çeşit eleştiri:

kevin-securityhowto (at) tummy.com

ve

dave (at) linuxsecurity.com

adreslerine yönlendirilmeli.

Not: Lütfen geribildiriminizi *her iki* yazara da gönderin. Ayrıca, mektubunuzun konu kısmında "Linux", "security", veya HOWTO" kelimelerinin bulunduğundan emin olun ki, Kevin'in reklam süzgecine yakalanmayasınız.

Yasal Sorumluluk Reddi

Bu belgenin içeriği (yazarlara) hiçbir yasal zorunluluk/sorumluluk getirmez. Belgedeki kavramları, örnekleri ve diğer içeriği, tehlikelerini göze alarak kullanın. Ek olarak, belgenin bu sürümü "erken" bir sürüm olup hatalar veya yanlışların bulunması mümkündür.

Belgedeki bazı örnekler ve tanımlamalar RedHat(tm) düzen ve kurulumuna uygun şekilde verilmiştir. Sizin sisteminiz bundan farklı olabilir.

Belgede, bildiğimiz kadarıyla, belirli şartlar altında kullanılabilen veya kişisel kullanım için değerlendirilebilen programlar tanıtılacak. Bir çok program kaynak kodları ile birlikte, GNU şartları altında ulaşılabilir durumda olacaktır.

Copyright Information

Telif Hakkı Bilgisi

Genel Bakış

Bu belge Linux sisteminizi daha güvenli hale getirebilmek için yaygın olarak kullanılan yazılımları ve bazı yordamları açıklamaya çalışacak. Başlamadan önce, öncelikle bazı temel kavramları tartışmak, ve bir güvenlik altyapısı oluşturmak, bu açıdan önemli.

Neden Güvenliğe Gereksinim Duyuyoruz?

Sürekli değişmekte olan küresel iletişim, pahalı olmayan İnternet bağlantıları, ve hızlı adımlarla ilerleyen yazılım gelişimi dünyasında, güvenlik gitgide daha fazla "konu" haline geliyor. Şu anda güvenlik temel bir gereksinim, çünkü küresel bilişim doğal bir güvensizlik içinde. Örneğin, veriniz A noktasından B noktasına İnternet üzerinde giderken, yolu boyunca bir dizi başka noktalardan geçebilir, ve bu şekilde diğer kullanıcılara, gönderdiğiniz verinin yolunu kesebilmek, hatta veriyi değiştiribilmek için fırsatlar verebilir. Hatta sisteminizdeki diğer kullanıcılar, kötü

niyetle, sizin isteğiniz dışında verinizi başka bir şekle sokabilir. "Korsan" [3] da denilen bazı saldırganlar sisteminize izinsiz erişim sağlayabilir, ileri düzey bilgileri kullanarak sizmişsiniz gibi davranabilir, sizden bilgi çalabilir, hatta kendi kaynaklarınıza erişiminizi engelleyebillir. Eğer "Bilgisayar Kurdu" ile "Bilgisayar Korsanı" arasındaki farkı merak ediyorsanız, Eric Raymond tarafından hazırlanan "Nasıl Bilgisayar Kurdu Olunur" belgesini aşağıdaki adreste bulabilirsiniz: http://www.catb.org/~esr/faqs/hacker-howto.html.

"Güvenli", Ne kadar Güvenli?

Öncelikle, hiçbir bilgisayar sisteminin tamamen güvenli olamayacağını aklınızdan çıkarmayın. Bütün yapabileceğiniz, sisteminizi bozmaya çalışan birinin, bu işini gitgide daha zor bir hale getirmek olacaktır. Ortalama bir ev Linux kullanıcısı için "korsan"ları uzak tutmak fazla bir şey gerektirmez. Bununla birlikte, daha Büyük-Ölçek Linux kullanıcıları (bankalar, telekomunikasyon şirketleri vb) için yapılması gereken çok çalışma vardır.

Değerlendirilmesi gereken bir diğer etken de, güvenlik önemleriniz arttıkça, bu güvenlik önlemlerinin kendisi sistemi kullanılmaz hale getirebilmektedir. Bu noktada dengeleri sağlayacak kararlar vermelisiniz, öyleki sisteminiz kullanılabilirliğini yitirmeden amaçlarınıza uygun bir güvenlik içinde olmalı. Örneğin, sisteminize telefon yoluyla bağlanmak isteyen herkese modem tarafından geri-arama yapılması gibi bir güvenlik önleminiz olabilir. Bu daha güvenli olmakla birlikte evinde bulunmayan bir kişinin sisteme giriş yapmasını zorlaştırır. Ayrıca Linux sisteminizin ağ veya İnternet bağlantısı olmayak şekilde de ayarlayabilirsiniz, fakat bu da sistemin yararlı kullanımını sınırlandırmak olacaktır.

Eğer orta büyüklükte veya büyük bir siteyseniz, bir güvenlik politikası oluşturmalı, ve bu politika sitenizin ne kadar güvenliğe gereksinimi olduğunu belirtiyor olmalıdır. Bu politikaya uygun olarak alınan önlemlerin ve yordamların uygulandığından emin olmak için bir izleme yordamı da olmalıdır. Yaygın olarak bilinen bir güvenlik politikası örneğini http://www.faqs.org/rfcs/rfc2196.html adresinde bulabilirsiniz. Bu belge yakın zamanda güncellendi, ve şirketinizin oluşturulacak güvenlik politikası için harika bir iskelet görevi görecek bilgiler içeriyor.

Neyi Korumaya Çalışıyorsunuz?

Sisteminizi güvenli hale getirmeden önce, korunmanız gereken tehditin düzeyine, hangi tehlikeleri dikkate almamak gerektiğine, ve sonuç olarak sisteminizin saldırıya ne kadar açık olduğuna karar vermelisiniz. Koruduğunuz şeyin ne olduğunu, neden korumakta olduğunuzu, değerinin ne olduğunu, ve verinizin ve diğer "değerli"lerinizin sorumluğunun kime ait olduğunu belirlemek amacıyla sisteminizi çözümlemelisiniz..

- *Risk*, bilgisayarınıza erişmeye çalışan bir saldırganın, bunu başarma olasılığıdır. Bir saldırgan, dosyaları okuyabilir veya değiştirebilir, veya zarara yol açacak programlar çalıştırabilir mi? Önemli verileri silebilir mi? Unutmayın: Sizin hesabınıza, veya sisteminize erişim sağlamış biri, sizin kişiliğinize bürünebilir.

  Ek olarak, bir sistemde güvensiz bir hesap bulundurmak bütün ağın güvenliğinin bozulmasıyla sonuçlanabilir. Eğer bir kullanıcıya `.rhosts` dosyasını kullanarak giriş yapma, veya `tftp` gibi güvensiz bir servisi çalıştırma izni verirseniz, bir saldırganın "kapıdan içeri bir adım atması" riskini göze almış oluyorsunuz. Saldırgan bir kez sizin veya bir başkasının sisteminde bir kullanıcı hesabı sahibi olduktan sonra, bu hesabı diğer bir hesaba, veya diğer bir sisteme erişim kazanmak için kullanabilir.

- *Tehdit*, tipik olarak ağınıza veya bilgisayarınıza izinsiz erişim sağlamak için güdülenmiş birinden gelir. Sisteminize erişim için kimlere güveneceğinize, ve ne gibi tehditler ortaya çıkaracaklarına karar vermelisiniz.

  Çeşitli saldırgan tipleri vardır, ve bunların değişik niteliklerini akıldan çıkarmamak, sistemlerinizin güvenliğini sağlamakta yararlı olur:

- *Meraklı* - Bu tip saldırgan genelde ne çeşit bir sisteminiz ve veriniz olduğunu keşfetmek ile ilgilenir.

- *Kötü Niyetli* - Bu tip saldırgan, sisteminizi çalışmaz hale getirmek, www sayfanızın görünüşünü bozmak, ya da yolaçtığı zararı karşılayabilmeniz için sizi zaman ve para harcamaya zorlamak amacıyla ortalarda dolaşır.

- *Büyük-Ölçek Saldırganı* - Bu tip saldırgan, sisteminizi kullanarak tanınıp sevilme ve ün kazanma peşindedir. Büyük ölçekli sisteminizi kullanarak, yeteneklerinin reklamını yapmaya çalışır.

- *Rekabet* - Bu tip saldırgan, sisteminizde hangi verilerin bulunduğu ile ilgilenir. Kendisine, parasal veya diğer yollarla yararlı olabilecek bir şeye sahip olduğunuzu düşünen biri olabilir.

- *Ödünç Alanlar* - Bu tip saldırgan, sisteminize "dükkan açmak" ve kaynaklarını kendi amaçları için kullanmakla ilgilenir. Çoğunlukla sohbet veya IRC servisleri, porno siteleri, hatta DNS servisleri bile çalıştırabilirler.

- *Zıp Zıp Kurbağa* - Bu tip saldırgan, sisteminizle ilgilenir çünkü sisteminizden diğer sistemlere atlamak istemektedir. Eğer sisteminiz diğer sistemlere iyi bir bağlantı sağlıyorsa, veya içerdeki diğer bilgisayarlara bir ağ geçidi niteliğindeyse, bu tip saldırganların sistem güvenliğinizi ihlal etmeye çalıştıklarını görebilirsiniz.

- *Zayıflık*, bilgisayarınızın diğer ağlardan ne kadar iyi korunmakta olduğunu, ve birinin izinsiz erişim sağlaması potansiyelini tanımlar.

  Biri sisteminize girerse tehlikede olan nedir? Elbette, çevirmeli ağ ile PPP bağlantısı sağlayan bir ev kullanıcısı ile makinelerını İnternete bağlayan bir şirketin, veya diğer büyük bir ağın ilgilendikleri farklı olacaktır.

  Kaybolan herhangi bir veriyi yerine koymak/yeniden yaratmak için ne kadar zaman gerekirdi? İşin başında yapılan bir yatırım için harcanan zaman, daha sonra kaybolan veriyi yeniden yaratmak için harcanan zamandan on kat daha az olabilir. Yedekleme stratejinizi gözden geçirdiniz mi? Son zamanlarda verilerinizi doğruladınız mı?

Bir Güvenlik Politikası Geliştirmek

Sisteminiz için kullanıcılarınızın kolayca anlayıp izleyebileceği basit, ve genel bir politika yaratın. Bu politika verinizi koruduğu gibi, kullanıcılarınızın özel hayatlarını da korumalı. Eklenmesi düşünülebilecek bazı şeyler: Kim sisteme erişime sahip (Arkadaşım hesabımı kullanabilir mi?), kim sistem üzerinde yazılım kurma iznine sahip, veri kime ait, felaketten sonra toparlanma, ve sistemin uygun kullanımı.

Genel olarak kabul edilmiş bir güvenlik politikası

" *İzin verilmemiş herşey yasaklanmıştır.* "

ifadesi ile başlar. Bu, herhangi bir servis için bir kullanıcının erişimi onaylanmadığı sürece, o kullanıcı erişim onaylanana kadar o servisi kullanmıyor olmalı anlamına gelir. Politikaların kullanıcı hesapları üzerinde işlediğinden emin olun. Örneğin "Bu erişim hakları probleminin nereden kaynaklandığını bulamıyorum, neyse, root olarak halledeyim" demek, çok bariz güvenlik açıklarına olduğu kadar, henüz hiç keşfedilmemiş olanlarına da yol açabilir.

rfc1244 kendi ağ güvenlik politikanızı nasıl oluşturabileceğinizi açıklayan,

rfc1281 ise her adımı ayrıntılı olarak anlatılmış örnek bir güvenlik politikasını içeren

birer RFC (Request For Comment - Yorum İçin İstek) belgesidir.

Son olarak, gerçek hayatta güvenlik politikaları nasıl oluyor görmek isterseniz, COAST politika arşivine bir göz atmak isteyebilirsiniz: ftp://coast.cs.purdue.edu/pub/doc/policy

Sitenizi Güvenli Hale Getirmenin Yolları

Bu belge, uğrunda çok çalıştığınız değerli şeylerinizi güvenli hale getirebilmeniz için gereken çeşitli yolları tartışacak. Bu değerli şeyler yerel makineniz, veriniz, kullanıcılarınız, ağınız, hatta kendi saygınlığınız olabilir. Kullanıcılarınızın sahip olduğu veriyi bir saldırgan silerse saygınlığınız ne olur? Ya şirketinizin, önündeki üç aylık süredeki proje planlarını yayımlarsa? Bir ağ kurulumu planlıyorsanız, herhangi bir makineyi ağa dahil etmeden önce dikkate almanız gereken bir çok etken vardır.

Tek bir PPP hesabınız dahi olsa, ya da sadece küçük bir siteniz, bu saldırganların sizin sisteminizle ilgilenmeyecekleri anlamına gelmez. Tek hedefler, büyük, büyük ölçekli siteler değildir -- Bir çok saldırgan basitçe, büyüklüğü farketmeden olabildiğince çok sitenin açıklarından yararlanmak ister. Ek olarak, sizin sitenizdeki bir güvenlik açığını, bağlı olduğunuz diğer sitelere erişim kazanmak amacıyla kullanabilirler.

Saldırganların elinde çok zaman vardır, sisteminizi nasıl anlaşılmaz bir hale getirdiğinizi, ya da ne derece gözden sakladığınızı öğrenmek için tahmin yolunu değil, basitçe tek tek bütün olasılısıkları deneme yolunu seçerler. Bir saldırganın sisteminizle ilgileniyor oluşunun bir takım başka nedenleri de vardır, bunları daha sonra tartışacağız.

Bilgisayar Güvenliği

Belki de sistem yöneticilerinin en çok yoğunlaştığı güvenlik alanlarından biri bilgisayar bazında güvenliktir. Bu, tipik olarak, kendi bilgisayarınızın güvenli olduğundan emin olmanız, ve ağınızdaki bütün herkesin de emin olduğunu ümit etmenizdir. İyi parolaların seçilmesi, bilgisayarınızın yerel ağ servislerinin güvenli hale getirilmesi, hesap kayıtlarının iyi korunması, ve güvenlik açıkları olduğu bilinen yazılımın güncellenmesi, yerel güvenlik yöneticisinin sorumlu olduğu işler arasındadır. Bunu yapmak mutlak şekilde gereklidir, fakat ağınızdaki bilgisayar sayısı arttıkça, gerçekten yıldırıcı bir iş haline dönüşebilir.

Yerel Ağ Güvenliği

Ağ güvenliği, en az bilgisayarların güvenliği kadar gerekli olan bir kavramdır. Aynı ağ üzerindeki yüzlerce, binlerce, hatta daha fazla bilgisayarla, güvenliğinizi her birinin tek tek güvenli oluşu üzerine kuramazsınız. Ağınızı sadece izin verilen kullanıcıların kullandığını garanti altına almak, güvenlik duvarları oluşturmak, güçlü bir şifreleme kullanmak, ve ağınızda "yaramaz" (yani güvensiz) makineler bulunmadığından emin olmak, güvenlik yöneticisinin görevlerinin bir parçasıdır.

Bu belgede sitenizi daha güvenli bir hale getirmek için kullanılan teknikleri tartışacağız, ve bir saldırganın korumaya çalıştıklarınıza erişim sağlamasını engellemek için gereken yollardan bazılarını göstermeye çalışacağız.

Karmaşıklaştırma Yoluyla Güvenlik

Tartışılması gereken güvenlik tiplerinden biri "karmaşıklaştırma yoluyla güvenlik"tir. Bunun anlamı, örneğin, güvenlik açıkları bulunan bir servisin standart olmayan bir porta (kapı) taşınmasıdır, saldırganların bu şekilde servisin nerde olduğunu farketmeyerek bu açıktan yararlanamayacağı umulur. Diğerlerinin ise servisin nerde olduğunu bilmeleri, dolayısıyla yararlanabilmeleri gerekir. Sitenizin küçük, veya göreli olarak daha küçük ölçekli oluşu, saldırganların sahip olduklarınızla ilgilenmeyeceği anlamına gelmez. Önüzümüzdeki bölümlerde tartıştıklarımız arasında neyi korumakta olduğunuz da bulunacak.

Bu Belgenin Düzeni

Bu belge, bir takım bölümlere ayrılmıştır. Bu bölümlerde kapsamı geniş olan güvenlik konuları yer almaktır. İlkin, *Fiziksel Güvenlik*, makinenizi fiziksel bir zarar görmekten nasıl korumanız gerektiğini kapsıyor. İkinci olarak, *Yerel Güvenlik*, sisteminizin yerel kullanıcılar tarafından karıştırılmasının nasıl engelleneceğini açıklıyor. Üçüncüsü, *Dosyalar ve Dosya Sistemi Güvenliği*, dosya sistemlerinizi ve dosyalar üzerindeki erişim haklarının nasıl düzenlenmesi gerektiğini açıklıyor. Sonraki bölüm, *Parola Güvenliği ve Şifreleme*, makinenizi ve ağınızı daha iyi bir şekilde güvenli hale getirmek için şifrelemenin nasıl kullanıldığını tartışıyor. *Çekirdek Güvenliği* bölümünde ise daha güvenli bir sistem için farkında olmanız gereken çekirdek seçenekleri anlatılıyor. *Ağ Güvenliği*, Linux sisteminizi ağ saldırılarına karşı nasıl güvenli hale getirebileceğiniz hakkında bilgi içeriyor. *Güvenlik Hazırlığı (Bağlanmadan Önce)*, makine(leri)nizi, ağa bağlı hale getirmeden önce nasıl hazırlamanız gerektiğini anlatıyor. Sonraki bölüm, *Güvenlik İhlali Sırasında ve Sonrasında Neler Yapılabilir*, sistemizi bozmaya çalışma eylemi o an devam etmekte ise, veya böyle bir eylemin yakın zamanda gerçekleştiğini öğrendiğinizde neler yapabileceğiniz konusunu tartışıyor. *Güvenlikle İlgili Kaynaklar*, bölümünde bazı güvenlik ile ilgili bilgilere erişim sağlanabilecek başlıca kaynaklarının neler olduğu sıralanıyor. *Sıkça Sorulan Sorular*, bölümü sık sık sorulan bazı soruların cevaplarını içeriyor, ve son olarak *Sonuç* bölümü yer alıyor.

Bu belgeyi okurken farkında olunması gereken iki ana konu:

- Sisteminizde neler olup bittiğinin farkında olun. `/var/log/messages` gibi sistem kayıtlarınızı düzenli olarak gözden geçirin ve gözünüz daima sisteminizin üzerinde olsun.
- Sisteminizi güncel tutun, yazılımlarınızın en son sürümlerini kurun, ve kullandığınız yazılımla ilgili güvenlik uyarılarını takip ederek gereken güncellemeleri zamanında yapın. Sadece bunu yapmak bile sisteminizi kayda değer şekilde daha güvenli hale getirecektir.

Fiziksel Güvenlik

Güvenliğin dikkate almanız gereken ilk katmanı bilgisayar sistemlerinizin fiziksel güvenliğidir. Makinenize kimler doğrudan erişim sağlayabiliyor? Sağlamalılar mı? Makinenizi kurcalamalarını engelleyebiliyor musunuz? Engellemeli misiniz?

Sisteminizde ne kadar fiziksel güvenliğe gereksinimiz olduğu, durumunuza ve/veya bütçenize bağlıdır.

Eğer bir ev kullanıcı iseniz, büyük olasılıkla çok fazla gereksiniminiz yoktur (tabii ki makinenizi çocuklardan veya rahatsız edici akrabalarınızdan korumanız gerektiğini düşünebilirsiniz). Eğer bir laboratuvardaysanız, ciddi anlamda daha fazlasına ihtiyacınız vardır, ama kullanıcıların da aynı zamanda işlerini makineler üzerinde yapabilmesi gerekir. İzleyen bölümler bu konuda yardım etmeye çalışacak. Eğer bir ofisteyseniz, makinenizi mesai saatleri dışında, veya makinenizin başında değilken daha güvenli hale getirmeye ihtiyacınız olabilir veya olmayabilir de. Bazı şirketlerde, konsolun güvensiz bir durumda bırakılması işten çıkarılma sebebi olabilir.

Kilitler, (elektrikli) teller, kilitli dolaplar, ve kamerayla izleme gibi apaçık fiziksel güvenlik yöntemlerinin hepsi iyi fikir olmakla birlikte bu belgenin konusu ötesindedir. :)

Bilgisayar Kilitleri

Yeni PC'lerin çoğunda bir "kilitleme" özelliği bulunur. Genellikle bu, kasanın önünde yer alan ve beraberinde gelen anahtar kullanılarak açılıp kapanabilir bir kilittir. Kasa kilitleri PC'nizin çalınmasını, ya da kasanın açılarak donanımınıza doğrudan bir müdahele edilmesini veya parçaların çalınmasını engeller. Bazı durumlarda bilgisayarınızın kapatılıp, disket veya başka donanım ile yeniden açılmasının engellenmesini de sağlayabilirler.

Bu kasa kilitleri, ana karttaki desteğe, ve kasanın nasıl yapıldığına göre değişik şeyler de yapabilir. Bazı PC'lerde bu kilitler öylesine yapılmıştır ki kasayı açmak için kırmanız gerekir. Diğer bazı PC'lerde ise, yeni bir klavye ya da fare takmanıza izin vermezler. Bununla ilgili bilgiyi

kasanızın veya ana kartınızın kullanım rehberinde bulabilirsiniz. Kilitler genelde düşük kalitelidir ve uygun bir maymuncukla kolayca açılabilirler, ama buna rağmen bazı durumlarda gerçekten etkili bir koruma yöntemi olabilirler.

Bazı makinelerin (SPARClar ve Mac'ler dikkate değer), arka taraflarında içinden bir telin geçebileceği iki tane delik vardır. İçinden bir tel geçirdiğinizde, saldırganlar kasayı açabilmek için teli kesmek veya kasayı kırmak zorunda kalırlar. Bir asma kilit veya bir şifreli kilit takmak bile makinenizin çalınmasında oldukça caydırıcı olabilir.

BIOS Güvenliği

BIOS, x86 tabanlı donanımızı yönlendiren ve ayarlarını yapan en alt düzeydeki yazılımdır. LILO ve diğer Linux sistem yükleme yöntemleri, Linux makinenizin nasıl açılacağına karar vermek için BIOS'a erişir. Linux'un çalıştığı diğer donanımlarda da benzer bir yazılım bulunur (Mac'lerde OpenFirmware ve yeni Sun'larda Sun boot PROM'u gibi). BIOS'unuzu kullanarak saldırganların bilgisayarınızı kapatıp açmasını, ve Linux sisteminizi yönlendirmesini engelleyebilirsiniz.

Bir çok BIOS bir parola ayarı yapmanıza izin verir. Bu o kadar da çok güvenlik sağlamaz (BIOS sıfırlanabilir, veya kasa açılarak çıkarılabilir), ama iyi bir caydırıcı etken olabilir (yani zaman alacak ve kurcalamanın izleri kalacaktır). Benzer şekilde, s/Linux (SPARC(tm) işlemcili makineler için Linux) sisteminizde, açılış parolası için EEPROM'unuzu kullanabilirsiniz. Bu saldırganları yavaşlatacaktır.

BIOS parolalarına güvenmenin diğer bir riski varsayılan parola sorunudur. Çoğu BIOS üreticisi, insanların parolalarını unuttuklarında bilgisayarlarını açıp pilleri çıkarmasını beklemediği için, BIOS'lara, seçilen paroladan bağımsız bir parola koymuştur. Bu parolalardan yaygın olarak kullanılanlar:

j262 AWARD_SW AWARD_PW lkwpeter Biostar AMI Award bios BIOS setup cmos AMI!SW1 AMI?SW1 password hewittrand shift + s y x z

Ben Award BIOS için olan AWARD_PW parolasını denedim ve çalıştı. Bu parolalar üreticilerin WWW sayfalarından ve http://astalavista.box.sk adresinden kolaylıkla ulaşılabilir durumdadır ve böyle olduğu için de BIOS parolasının yeterince bilgili bir saldırgana karşı yeterli bir koruma olduğu düşünülemez.

Çoğu x86 BIOS'u, diğer bazı güvenlik ayarlarına sahiptir. BIOS kitapçığınıza bakabilir, veya bir sonraki açılışta BIOS'a girerek ne tür ayarlar olduğunu gözden geçirebilirsiniz. Örneğin, bazı BIOS'lar disket sürücülerden sistem yüklenmesine izin vermez, bazıları da BIOS'un bazı özelliklerinin kullanılması için bir parola gerektirir.

Not: Makineniz sunucu görevi yapıyorsa, ve bir açılış parolası koyduysanız, makineniz başında kimse olmadığı zaman açılmayacaktır. Örneğin bir elektrik kesilmesi durumunda makinenin açılması için başına giderek parolayı girmeniz gerekecek ;(

Sistem Yükleyici Güvenliği

Çeşitli Linux sistem yükleyicileri de bir parola belirlenmesine izin verebilir. Örneğin, LILO'da `password` ve `restricted` ayarları vardır, `password` açılış (sistem yükleme) sırasında bir parola ister,`restricted` ise sadece `LILO` satırında bir seçenek (`single` gibi) belirtirseniz parola ister.

>lilo.conf'un man (yardım) sayfasından:

```
password=password
    Her imge (çekirdek imgesi) için ayarlanabilir olan
    `password=...' seçeneği (aşağıya bakın) bütün imgeler
    için geçerlidir.

restricted
```

```
    Her imge (çekirdek imgesi) için ayarlanabilir olan
    `restricted' seçeneği (aşağıya bakın) bütün imgeler
    için geçerlidir.

  password=password
    İmgeyi bir parola ile korur.

  restricted
    Sadece komut satırında seçenekler belirtilirse
    (örneğin single) bir parola girilmesini gerektirir.
```

Parolaları belirlerken bir gün onları hatırlamanız gerekeceğini aklınızdan çıkarmayın :). Ayrıca bu parolaların kararlı bir saldırganı sadece yavaşlatacağını da unutmayın. Parolalar birinin sistemi disketle açıp sabit disk bölümünüzü bağlamasını engellemez. Eğer açılış bağlamında bir güvenlik uyguluyorsanız, o zaman BIOS'tan disketten açılışı da engelleyip, BIOS'u da bir parola ile koruyabilirsiniz.

Aklınızdan çıkarmamanız gereken bir diğer konu da /etc/lilo.conf dosyasının erişim izinlerinin "600" olması gerektiğidir. Aksi takdirde diğerleri parolanızı okuyabilir!

GRUB bilgi sayfasından: GRUB, sadece yöneticilerin etkileşimli işlemleri başlatabilmesi (örneğin menü girişlerini düzenlemek ve komut-satırı arayüzüne girebilmek) için "password" özelliği sunmaktadır. Bu özelliği kullanmak için, yapılandırma dosyanızda 'password' komutunu aşağıdaki gibi çalıştırmalısınız (*note password::)

password --md5 PASSWORD

Eğer bu belirtilirse, <p> tuşuna basıp doğru parolayı girene dek GRUB tüm etkileşimli denetimlere izni kısıtlar. '--md5' seçeneği GRUB'a 'PASSWORD'ün MD5 formatında olduğunu söyler. Eğer girilmezse, GRUB 'PASSWORD'ün açık metin olduğunu varsayar.

Parolanızı 'md5crypt' komutu ile şifreleyebilirsiniz.(*note md5crypt::). Örneğin, grub kabuğunu başlatın (*note Invoking the grub shell::), parolanızı girin:

grub> md5crypt Password: ********** Encrypted: 1U$JK7xFegdxWH6VuppCUSIb.

Sonra da şifrelenmiş parolayı kopyalayıp yapılandırma dosyanızın içine yapıştırın.

Grub'da aynı zamanda doğru parolayı girmediğinizde disk bölümünü kitlemeye olanak sağlayan 'lock' komutu da vardır. Basitçe 'lock' sözcüğünü ekleyin ve disk bölümünü parola sağlanmadan erişilemez olacaktır.

Eğer farklı bir sistem yükleyici hakkında herhangi biri güvenlikle ilgili bilgiye sahipse duymaktan memnun oluruz (`grub`, `silo`, `milo`, `linload`, vb).

Not: Makineniz sunucu görevi yapıyorsa, ve bir açılış parolası koyduysanız, makineniz başında kimse olmadığı zaman *açılmayacaktır*. Örneğin bir elektrik kesilmesi durumunda makinenin açılması için başına giderek parolayı girmeniz gerekecek ;(

xlock and vlock

Eğer zaman zaman makinenizin başından uzaklaşıyorsanız, konsolu "kilitleyebilmek", böylece hiçkimsenin çalışmanızı kurcalayamamasını, veya bakamamasını sağlamak hoş olur. İki program bu iş için var: `xlock` ve `vlock`.

`xlock` bir X görüntü kilidi. X'i destekleyen tüm Linux dağıtımlarında muhtemelen bulunuyordur. Tüm seçenekler hakkında bilgi almak için man (yardım) sayfasına bir göz atmanız gerekebilir, ama genellikle `xlock`'u konsolunuzdaki herhangi bir xterm'den çalıştırabilirsiniz. `xlock` bir kere çalıştı mı görüntüyü kitler ve kilidin kalkması için parolanızı girmenizi gerektirir.

`vlock` Linux'unuzdaki bazı veya tüm sanal konsolları kilitleyebilmenizi sağlayan küçük bir programdır. O anda çalışmakta olduğunuz konsolu ya da tüm konsolları kilitleyebilirsiniz. Eğer sadece bir tanesini kilitlerseniz, diğerleri geldiğinde konsolu kullanabilir, fakat o an çalışmakta olduğunuz (ve kilitlediğiniz) konsola erişim sağlayamazlar. `vlock` RedHat Linux ile birlikte geliyor, fakat kullandığınız dağıtıma göre değişiklik gösterebilir.

Elbette konsolu kilitlemek, çalışmanızı kurcalamak isteyen birini engeller, fakat makinenizi yeniden başlatmalarını veya bir şekilde çalışmanızı bozmalarını engellemez. Ayrıca makinenize ağdaki başka bir makinenin erişimini ve yol açacağı problemlere de engel olamaz.

Daha önemlisi, birinin X Windows sisteminden tamamen çıkıp, normal bir sanal konsol giriş satırına ulaşmasını, ya da X11'in başlatıldığı sanal konsola gidip askıya almasını ve haklarınıza sahip olmasını da engelleyemez. Bu sebeple, X'i sadece xdm kontrolü altında kullanmayı düşünmeli, veya startx kullanıyorsanız bilgisayarın başından ayrıldığınızda kimsenin bilgisayara ulaşmadığından emin olmalısınız.[4]

Yerel cihazların güvenliği

Sisteminize eklenmiş bir webcam veya mikrofon varsa, bir saldırganın bu cihazlara erişim sağlaması tehlikesini göz önünde bulundurmalısınız. Kullanımda değilken bu tür cihazların kasadan ayırmak veya fişlerini çekmek bir seçenek olabilir. Bu tür cihazlara erişim sağlayan yazılımı da (kullanımı kitapçıklarını/belgelerini okuyarak) çok iyi tanımalısınız.

Fiziksel Güvenlik İhlallerini Belirleme

Dikkat edilmesi gereken ilk nokta bilgisayarınızın ne zaman yeniden başlatıldığıdır. Linux sağlam ve kararlı bir işletim sistemi olduğu için, makinenizi yeniden başlatmanızın gerektirdiği nadir durumlar, *sizin* gerçekleştirdiğiniz işletim sistemi güncellemeleri, veya donanım değişikliği gibi durumlardır. Eğer makineniz böyle bir şey yapmadığınız halde kapanıp açılmışsa, bu, makinenizin güvenliğinin bir saldırgan tarafından bozulduğunun bir işareti olabilir.

Bilgisayarın bulunduğu alanda ve kasada kurcalama işaretleri arayın. Bir çok saldırgan varlıklarının izlerini günlüklerden siler, bütün günlükleri incelemek ve herhangi bir uygunsuzluk olup olmadığını gözden geçirmek, iyi bir fikirdir.

İyi bir fikir olan bir başka şey de, günlük verisini güvenli bir yerde saklamaktır, örneğin, iyi korunmuş bir ağınızdaki bu işe adanmış bir günlük sunucusunda. Makinenin güvenliği bir kere bozuldu mu, günlük verisi çok az yarar sağlar, çünkü saldırgan tarafından değiştirilmiş olması muhtemeldir.

Syslog sunucu programı (daemon), günlükleri merkezi bir syslog sunucusuna göndermek üzere yapılandırılabilir, ama bu bilgi çoğunlukla şifresiz gönderilir, bu da veri aktarılırken bir saldırgan tarafından görülmesine izin vermek anlamına gelir. Bu, ağınız ve herkese açık olmasını düşünmediğiniz konular hakkındaki bilgilerin ortaya çıkmasına yol açabilir. Gönderilen veriyi şifreleyen syslog sunucu programları da vardır.

Farkında olmanız gereken bir diğer durum, sahte syslog mesajları hazırlamanın kolay olduğudur - bunun için yayımlanan bir program vardır. Hatta syslog, ağdan gelen ve gerçek kökenini göstermeden yerel bilgisayardan geldiğini iddia eden günlük satırlarını bile kabul eder.

Günlüklerinizde denetim altında tutmanız gereken bazı şeyler:

- Kısa veya tamamlanmamış günlükler.
- Tarih ve zamanları garip olan günlükler.
- Yanlış erişim hakları veya sahiplikleri olan günlükler.
- Bilgisayarın veya servislerin yeniden başlatılma kaytları.

- Kayıp günlükler.
- su kullanımı kayıtları veya sisteme garip yerlerden yapılan girişler

Sistem günlük verisini, bu belgede daha sonra *Sistem Hesap Verilerinizi Takip Edin* bölümünde tartışacağız.

Yerel Güvenlik

Şöyle bir göz atılması gereken sonraki konu, yerel kullanıcılardan gelen saldırılara karşı sistem güvenliğiniz konusu. Kullanıcıların *yerel* olduğunu söyledik mi? Evet!

Sistem saldırganlarının root hesabına giden yollarındaki ilk şeylerden bir tanesi yerel bir kullanıcı hesabına erişim elde etmektir. Bu saldırganlar, gevşek bir yerel güvenlik ile, kötü ayarlı bir yerel servis veya çeşitli "böceklerden" [5] yararlanarak, normal kullanıcı erişimlerini root erişimine "terfi ettirir". Eğer yerel güvenliğinizin sıkı olduğundan emin olursanız, saldırganın üzerinden atlaması gereken başka bir çit daha oluşturmuş olursunuz.

Yerel kullanıcılar, gerçekten söyledikleri kişi oldukları durumda bile sistem üzerinde fazlaca kargaşa yaratabilir. [6] Tanımadığınız insanlara, veya iletişim bilgilerine sahip olmadığınız birine hesap açmak, gerçekten çok kötü bir fikirdir.

Yeni Hesap Açma

Kullanıcı hesaplarının, kullanıcıların yapması zorunlu işler için asgari gereklerini karşılayacak şekilde açıldığından emin olmalısınız. Eğer (10 yaşındaki) oğlunuza bir hesap açarsanız, erişiminin bir kelime işlemci ya da çizim programıyla sınırlı olmasını, ve kendisinin olmayan veriyi silme yetkisinin olmamasını isteyebilirsiniz.

Diğer kullanıcıların Linux makinenize meşru bir erişim sağlamasına izin verirken esas olarak alınabilecek bazı kurallar:

- Onlara, gereksinim duydukları en az yetkiyi verin.
- Ne zaman ve nereden sisteme giriş yaptıklarına, ya da yapmaları gerektiğine dikkat edin.
- Kullanılmayan hesapların kapandığından emin olun.
- Bütün bilgisayar ve ağlarda aynı kullanıcı isminin kullanılması, hesabın bakımını kolaylaştırması, ve günlük verisinin daha kolay çözümlenmesi açısından tavsiye edilir.
- Grup kullanıcı kimliklerinin yaratılması mutlak surette yasaklanmalıdır. Kullanıcı hesapları sorumluluk mekanizması da sağlar, ve bu birden fazla kişinin kullandığı grup hesaplarıyla mümkün değildir.

Güvenlik ihlallerinde kullanılan bir çok yerel kullanıcı hesabı, aylardır hata yıllardır kullanılmayanlardır. Kimse onları kullanmadığı için, ideal bir saldırı aracıdırlar.

Root Güvenliği

Makinenizdeki, peşinden en fazla koşulan hesap root (üstün kullanıcı) hesabıdır. Bu hesap bütün makine üzerinde yetki sağlamasının yanı sıra, ağdaki diğer makineler üzerinde de yetki sağlıyor durumda olması mümkündür. Unutmayın ki root hesabını, sadece özel işler için ve çok kısa süreliğine kullanmalısınız, geri kalan zamanlarda normal kullanıcı olarak işlerinizi yürütmelisiniz. Root kullanıcısı olarak sisteme giriş yaptığınızda, yaptığınız küçük hatalar dahi sorunlara yol açabilir. Root hesabıyla ne kadar az zaman harcarsanız, o kadar güvende olursunuz.

Diğer kullanıcıların Linux makinenize meşru bir erişim sağlamasına izin verirken esas olarak alınabilecek bazı kurallar:

- Karmaşık bir komut kullanırken, komutu ilk önce yıkıcı olmayan başka bir şekilde kullanmayı deneyin... Özellikle komutun geniş çaplı kullanımında... Örneğin `rm foo*.bak`, yapmak istiyorsanız, önce `ls foo*.bak` komutunu kullanarak, silmek üzere olduğunuz dosyaların, silmeyi düşündüğünüz dosyalar olduğundan emin olun. Bu tür tehlikeli komutların kullanımında, komutlar yerine `echo` kullanmak da zaman zaman işe yarayabilir.

- Kullanıcılarınıza, `rm` komutunun, dosyaları silmeden önce onay almasını sağlayacak, varsayılan bir takma ismini oluşturun. [7]

- Sadece belirli, tek bir işi yapmanız gerektiği zamanlarda root olun. Eğer kendinizi bir şeyin nasıl yapıldığını tahmin etmeye çalışırken bulursanız, normal kullanıcı hesabınıza geri dönüp, root tarafından neyin yapılacağından *emin* olmadan önce root kullanıcısına dönmeyin.

- Root için komut yolu tanımı çok önemli. Komut yolu (yani `PATH` evre değişkeni), girdiğiniz herhangi bir komut ya da programın hangi dizinlerde aranacağını belirtir. Root kullanıcısı için komut yolunu olabildiğince sınırlandırmaya çalışın, ve *asla* `.` dizinini eklemeyin ("geçerli dizin" anlamına gelir [8]. Ek olarak, komut yolunuzda, yazılabilen dizinler bulundurmayın, çünkü bu saldırganların bu dizinler içine, bir sonraki sefer kullandığınızda root erişim izniyle çalışacak olan yeni çalıştırılabilir dosyalar koyabilmesi anlamına gelir.

- Asla rlogin/rsh/rexec araçlarını (r-araçları olarak adlandırılırlar) root olarak kullanmayın. Çünkü bunlar, çok çeşitli saldırılara açık komutlardır, dolayısıyla root olarak çalıştırıldıklarında çok daha tehlikeli hale gelirler. Asla root için `.rhosts` dosyası oluşturmayın. [9]

- `/etc/securetty`dosyası, root olarak giriş yapılabilecek terminalleri belirtir. Bu dosyanın varsayılan ayarları (Red Hat Linux'ta) yerel sanal konsollardır. Bu dosyaya herhangi bir şey eklerken çok tedbirli olun. Root olmanız gerektiğinde uzaktan normal bir kullanıcı hesabına (*ssh (Güvenli Kabuk) ve stelnet* veya diğer şifrelenmiş bir yolla) giriş yapıp `su` komutuyla root olabilirsiniz. Dolayısıyla doğrudan root olarak giriş yapabilmeye gereksiniminiz yoktur.

- Root'u kullanırken daima yavaş ve temkinli davranın. Davranışlarınız bir çok şeyi etkileyebilir. Tuşlara dokunmadan önce düşünün!

Eğer birine (umarız güvenilir biridir), mutlak surette root hesabını kullanması için izin vermeniz gerekiyorsa, yardımcı olabilecek bir kaç araç var. `sudo`, kullanıcıların, parolalarını kullanarak sınırlı sayıda komutu root olarak çalıştırmalarına izin verir. Bu, örneğin, bir kullanıcının, ayrılabilir medyanın bağlanması veya çıkarılması işini, diğer root yetkilerini kullanamadan yapabilmesi anlamına gelebilir. `sudo` aynı zamanda, başarılı ve başarısız `sudo` denemelerinin bir günlüğünü tutar, bu şekilde kimin ne yapmak için bu komutu kullandığını izlemeniz mümkün hale gelir. Bu sebeple `sudo`, birden fazla kişinin root erişimi olduğu yerlerde bile iyi bir iş yapar, çünkü değişikliklerin takip edilmesinde yardım etmiş olur.

`sudo` belirli kullanıcılara belirli yetkiler vermekte yararlı olmasına rağmen, bazı eksiklikleri vardır. Sadece sınırlı bir takım işlerde kullanılmak zorundadır, örneğin bir sunucuyu yeniden başlatmak, veya yeni kullanıcılar eklemek gibi. `sudo` ile çalıştırılan, ve kabuğa çıkmaya izin veren her program, sisteme root erişimi sağlamış olur. Buna örnek olarak bir çok metin düzenleyici gösterilebilir. Ayrıca,`/bin/cat` kadar zararsız bir program bile, dosyaların üzerine yazmakta, ve root erişimi sağlamakta kullanılabilir. `sudo` programını, yapılan işten kimin sorumlu olduğunun izlenilmesi için kullanılan bir programmış gibi düşünün, ve hem root kullanıcısının yerine geçmesini hem de güvenli olmasını beklemeyin.

Dosyalar ve Dosya Sistemi Güvenliği

Sistemlerinizi ağa bağlamadan önce yapılacak bir kaç dakikalık hazırlık ve planlama, sistemlerinizin ve üzerlerinde saklanan verinin korunmasında yardımcı olabilir.

- Kullanıcıların, SUID/SGID programları ev dizinlerinden çalıştırmalarına izin vermek için herhangi bir sebep olmamalıdır. `/etc/fstab` dosyasında, root'tan başkalarının da yazma izninin olduğu disk bölümleri için `nosuid` seçeneğini kullanın. Ayrıca, kullanıcıların ev dizinlerinin bulunduğu bölümlerde, ve `/var` dizininde, program çalıştırılmasını ve karakter veya blok cihazların oluşturulmasını engellemek için (ne de olsa hiçbir zaman böyle bir şey gerekmeyecektir) `nodev` ve `noexec` seçeneklerini kullanabilirsiniz.

- NFS kullanarak dosya sistemlerini dışarı açıyorsanız, `/etc/exports` dosyasında en fazla sınırlandırma sağlayan seçenekleri kullandığınızdan emin olun. Bu, genel karakter kullanılmaması, root kullanıcısına yazma izninin verilmemesi, ve mümkün olduğu yerlerde salt-okunur şekilde dışa açılması anlamına geliyor.

- Kullanıclarınızın dosya yaratma `umask`'ini mümkün olduğu kadar sınırlı tutun. Bkz. *Umask Ayarları*.

- Eğer, NFS gibi bir ağ dosya sistemini kullanarak dosya sistemlerini bağlıyorsanız, `/etc/exports` dosyasında uygun sınırlama ayarlarını yaptığınızdan emin olun. Tipik olarak, `nodev`, `nosuid`, ve belki de `noexec` gerekli olanlardır.

- Dosya sistemlerinin sınırları belirleyin, varsayılan `unlimited` [10] ayarına izin vermeyin. Kullanıcı bazındaki sınırları, kaynak-limitleri PAM modülünü kullanarak, ve `/etc/pam.d/limits.conf`dosyasındaki ayarlar aracılığı ile yapabilirsiniz. Örneğin, `users` grubu için sınırlar şu şekilde olabilir:

```
@users     hard  core    0
@users     hard  nproc   50
@users     hard  rss     5000
```

  Burda söylenen, core dosyalarının yasaklanması, işlem sayısının 50 ile sınırlanması, ve bellek kullanımının 5M ile sınırlandırılmasıdır.

  Aynı sınırlamaları, `/etc/login.defs` dosyasında da belirtebilirsiniz.

- The `/var/log/wtmp` ve `/var/run/utmp` osyaları sisteminizdeki tüm kullanıcıların sisteme giriş bilgilerini içerir. Bu dosyaların bütünlükleri korunmalıdır, çünkü bir kullanıcının (ya da bir saldırganın) ne zaman ve nereden giriş yaptığını belirlemede kullanılabilirler. Bu dosyaların erişim izinleri, olağan işlevlerini gerçekleştirmelerine engel olmayan `644` olmalıdır.

- Korunması gereken bir dosyanın kazara silinmesi veya üzerine yazılmasını önlemek için değişmez biti kullanılabilir. Bu ayrıca, dosyaya bir simgesel bağ oluşturulmasını da engelleyecektir. Değişmez biti ile ilgili daha fazla bilgi için `chattr`(1) man sayfasına bakın.

- Sisteminizdeki SUID ve SGID dosyaları, potansiyel bir güvenlik riski oluşturur ve yakından izlenmelidir. Bu programlar, onları çalıştıran kullanıcıya özel yetkiler verdiği için, güvensiz programların kurulu olmadığından emin olmak gereklidir. Korsanların gözde bir numarası da SUID-root programlarından yararlanarak, bir sonraki girişlerinde arkakapı olarak kullanmak üzere bir SUID programı yerleştirmektir. Bu şekilde asıl açık kapatılsa bile yeni arka kapı sayesinde sisteme giriş yapabilirler.

  Sisteminizdeki bütün SUID/SGID programları bularak ne olduklarını izleyin. Böylelikle, bir değişiklik olduğunda, ki bu değişiklikler potansiyel bir saldırganın göstergesi olabilir, haberiniz olmuş olur. Sisteminizdeki bütün SUID/SGID programları bulmak için aşağıdaki komutu kullanabilirsiniz:

```
root#  find / -type f \( -perm -04000 -o -perm -02000 \)
```

Debian dağıtımı, hangi SUID programlarının bulunduğunu belirlemek için her gece bir iş çalıştırır. Daha sonra bunu bir önceki gece ile karşılaştırır. Bu günlük için `/var/log/setuid*` dosyalarına bakabilirsiniz.

Şüpheli bir programdaki SUID ve SGID erişim izinlerini `chmod` ile kaldırabilir, daha sonra mutlak şekilde gerektiğini hissederseniz tekrar yerine koyabilirsiniz.

- Herkes tarafından yazılabilir dosyalar, özellikle sistem dosyaları, bir korsan sisteminize erişir ve üzerlerinde değişiklik yaparsa bir güvenlik açığı haline gelebilir. Ayrıca herkes tarafından yazılabilir dizinler de tehlikelidir, çünkü bir korsanın istediği gibi dosya ekleme ve silmesine izin verir. Sisteminizdeki herkes tarafından yazılabilen dosyaları bulmak için, aşağıdaki komutu kullanın:

```
root# find / -perm -2 ! -type l -ls
```

ve bu dosyaların neden yazılabilir olduklarını bildiğinizden emin olun. Normal işlevler sırasında, herkes tarafından yazılabilir bir takım dosyalar bulunur, bunlar arasında `/dev` dizinindekiler ve simgesel bağlar da vardır. Bu nedenle yukarıdaki `find` komutunda simgesel bağları dışarıda bırakan `! -type l` seçeneğini kullandık.

- Sahipsiz dosyalar da bir saldırganın sisteminize eriştiğinin bir göstergesi olabilir. Sahibi olmayan veya hiçbir gruba ait olmayan dosyaları aşağıdaki komut ile bulabilirsiniz:

```
root# find / \( -nouser -o -nogroup \) -print
```

- `.rhosts` dosyalarına sisteminiz üzerinde izin vermemelisiniz, dolayısıyla sistem üzerindeki bu dosyaların bulunması düzenli yönetim görevlerinizin bir parçası olmalı. Unutmayın, bir korsan bütün ağınıza erişebilmek için sadece bir güvensiz hesaba gereksinim duyar. Aşağıdaki komutla sistem üzerindeki tüm `.rhosts` dosyalarını bulabilirsiniz:

```
root# find /home -name .rhosts -print
```

- Son olarak, herhangi bir sistem dosyası üzerindeki erişim izinlerini değiştirmeden önce, ne yaptığınızı anladığınızdan emin olun. Sadece bazı işlerin daha kolay olduğunu düşündüğünüz için bir dosyanın erişim izinlerini değiştirmeyin. Daima değiştirmeden önce neden o dosyanın o izinlere sahip olduğunu belirleyin.

Umask Ayarları

The `umask` komutu, sistem üzerinde varsayılan dosya yaratma kipini belirlemek amacıyla kullanılabilir. İstenen dosya kipinin sekizli sayı düzeninde tümleyicisidir. Eğer dosyalar, erişim ayarlarına bakmaksızın oluşturulursasa, kullanıcı dikkatsizce, okuma veya yazma izni olmaması gereken birine bu izinleri verebilir. Tipik `umask` ayarları, `022`, `027`, ve `077` (en fazla sınırlama budur) ayarlarıdır. Normal olarak, umask `/etc/profile` dosyasında belirlenir, dolayısıyla bütün kullanıcılar için geçerlidir. Ortaya çıkan izin şu şekilde hesaplanabilir: kullanıcı/grup/diğerleri için olan varsayılan izin (dizinler için 7, dosyalar için 6), umask'in mantıksal DEĞİLi ile bit bazında VE mantıksal işlemine sokulur.[11]

Örnek 1:

dosya, varsayılan 6, ikili : 110 umask, (örn. 2): 010, DEĞİL: 101

ortaya çıkan izin, VE: 100 (eşittir 4, r__)

Örnek 2:

dosya, varsayılan 6, ikili : 110 umask, (örn. 6): 110, DEĞİL: 001

ortaya çıkan izin, AND: 000 (eşittir 0, ___)

Örnek 3:

dizin, varsayılan 7, ikili : 111 umask, (örn. 2): 010, DEĞİL: 101

ortaya çıkan izin, VE: 101 (eşittir 5, r_x)

Örnek 4:

dizin, varsayılan 7, ikili : 111 umask, (örn. 6): 110, DEĞİL: 001

ortaya çıkan izin, VE: 001 (eşittir 1, __x)

```
# Set the user's default umask
umask 033
```

root kullanıcısının umask'ini `077` yaptığınızdan emin olun. Böylelikle root tarafından oluşturulan dosyaların/dizinlerin varsayılan olarak diğer kullanıcılara okuma, yazma ve çalıştırma izinleri, `chmod` komutuyla değiştirilmedikleri sürece kapalı olacaktır. which will disable read, write, and execute permission for other users, unless explicitly changed using `chmod` . Yukarıdaki örnekte, yeni oluşturulan dizinlerin izinleri, 777 - 033 = 744 olacaktır. Yeni oluşturulan dosyaların ise bu maske ile erişim izinleri 644 olur.

Eğer Red Hat kullanıyorsanız, ve onların kullanıcı ve grup ID oluşturma düzenlerine bağlı kalıyorsanız, `umask` için gereken sadece `002` değeridir. Bunun sebebi, Red Hat'te varsayılan ayarın her kullanıcı için ayrı bir grup olmasıdır. [12]

Dosya İzinleri

Sistem dosyalarınızın, kullanıcılar tarafından, ve sistem dosyalarının bakımından sorumlu olmayan kişiler tarafından açılmadığını garanti altına almak önemlidir.

Unix, dosya ve dizinlerdeki erişim denetiminde üç ayrı özelliğe göre sağlar: sahip, grup, ve diğer. Bir dosyanın her zaman bir sahibi ve grubu vardır, geriye kalan herkes "diğer" özelliğine sahiptir.

Unix izinlerini kısaca açıklayacak olursak:

Sahiplik - Hangi kullanıcı(lar) ve grup(lar), dosyanın (veya dizin/üst dizinin) izin haklarını denetim altında tutuyor?

İzinler - Kimi erişim tiplerine müsade etmek için 1 veya 0 olabilen bitler. Dosyaların izinleri, dizinlerinkinden farklı anlamlar taşır.

Okuma:

- Dosyanın içeriğini görebilme
- Dizini okuyabilme. [13]

Yazma:

- Bir dosya üzerinde değişiklik veya ekleme yapabilme

- Bir dizindeki dosyaları silebilme veya taşıyabilme

Çalıştırma:

- İkili yapıdaki bir programı veya kabuk betiğini çalıştırma [14]

- Bir dizinde arama yapabilme, okuma izinleri ile birlikte [15]

Metin Sakla Niteliği: (Dizinler için)
"Yapışkan bit" dizinlere ve dosyalara uygulandığında farklı anlamlar taşır. Eğer bir dizinin yapışkan biti 1 ise, bir kullanıcı o dizinde yeni bir dosya oluşturabilir, fakat dizindeki diğer dosyaları, kendine ait olmadığı veya açık bir şekilde izin verilmediği sürece silemez. Bu bit, `/tmp` gibi herkesin yazabileceği, ama diğer hiçbir kullanıcının başkalarının dosyalarını silmemesinin sağlanması gereken dizinler için tasarlanmıştır. Uzun dizin listesinde yapışkan bit `t` olarak görünür. [16]

SUID Niteliği: (Dosyalar için)
Bu, dosyanın "kullanıcı-kimliği-belirle" izinleriyle ilgilidir. Eğer sahip izinleri bölümünde bu bit 1 ise, ve dosya çalıştırılabilir bir dosya ise, çalışan süreçler sistem kaynaklarına, işlemi başlatan kişinin değil, dosya sahibinin kimliğinde erişim sağlar. Bu, bir çok "tampon taşması" açıklarının da sebebidir. [17]

SGID Niteliği: (Dosyalar için)
Bu bit grup izinlerinde 1 ise, dosyanın "grup-kimliği-belirle" durumunu denetler. Bu kullanıcı-kimliği-belirle biti ile aynı şekilde çalışır, fakat bu kez grup kimliği etkilenir. Bu bitin etkili olabilmesi için dosyanın çalıştırılabilir olması şarttır.[18]

SGID Niteliği: (Dizinler için)
Eğer bir dizinin bu bitini 1 yaparsanız (`chmod g+s dizin` ile), bu dizinde yaratılan dosyaların grupları, bu dizinin grubu ile aynı olacaktır.

Siz - Dosyanın sahibi

Grup - Ait olduğunuz grup

Herkes - Sizin ve grubunuzun diğer üyelerinin dışında kalan herkes.

Dosya Örneği:

```
   -rw-r--r--  1 kevin  users         114 Aug 28  1997 .zlogin
  1. bit - dizin mi?                        (hayır)
   2. bit - sahibi okuyabilir mu?             (evet, kevin )
    3. bit - sahibi yazabiliyor mu?            (evet)
     4. bit - sahibi çalıştırabiliyor mu?       (hayır)
      5. bit - grup üyeleri okuyabilir mu?        (evet, users)
       6. bit - grup üyeleri yazabiliyor mu?      (hayır)
        7. bit - grup üyeleri çalıştırabiliyor mu? (hayır)
         8. bit - herkes okuyabiliyor mu?           (evet)
          9. bit - herkes yazabiliyor mu?            (hayır)
           10. bit - herkes çalıştırabiliyor mu?      (hayır)
```

Aşağıdaki satırlar, dosyalar için açıklanan erişim izinlerinin uygulanabilmesi için verilmesi gereken en az izinlerin örnekleridir. Herhangi birine burdakilerden daha fazla izin vermek isteyebilirsiniz, fakat bunların en azları açıklanmaktadır:

```
-r-------- Sahibinin dosyayı okumasına izin verir.

--w------- Sahibinin dosyayı değiştirmesine veya silmesine izin verir.
           (Dosyanın içinde bulunduğu dizine yazma hakkı olan herkes,
dosyanın üzerine yazabilir, dolayısıyla dosyayı silebilir)
```

```
---x------ Sahibi programları çalıştırabilir. Kabuk betiklerini
           çalıştıramaz, çünkü onlar için de okuma izni olmalıdır.

---s------ Etkin kullanıcı kimliğini dosya sahibinin kullacı kimliği
haline getirir.

--------s- Etkin grup kimliğini dosyanın grup kimliği haline getirir.

-rw------T "Son değiştirilme zamanı" güncellenmez. Genelde takas
dosyaları için kullanılır.

---t------ Etkisi yoktur. (Önceleri yapışkan bit olarak kullanılırdı)
```

Dizin Örneği:

```
        drwxr-xr-x  3 kevin  users         512 Sep 19 13:47
.public_html/
        1. bit - dizin mi?               (evet, bir çok dosyaya sahip)
         2. bit - sahibi okuyabilir mu?             (evet, kevin)
          3. bit - sahibi yazabiliyor mu?            (evet)
           4. bit - sahibi çalıştırabiliyor mu?      (evet)
            5. bit - grup üyeleri okuyabilir mu?       (evet, users)
             6. bit - grup üyeleri yazabiliyor mu?      (hayır)
              7. bit - grup üyeleri çalıştırabiliyor mu? (evet)
               8. bit - herkes okuyabiliyor mu?           (evet)
                9. bit - herkes yazabiliyor mu?            (hayır)
                 10. bit - herkes çalıştırabiliyor mu?      (evet)
```

Aşağıdaki satırlar, dosyalar için açıklanan erişim izinlerinin uygulanabilmesi için verilmesi gereken en az izinlerin örnekleridir. Herhangi birine burdakilerden daha fazla izin vermek isteyebilirsiniz, fakat bunların en azları açıklanmaktadır:

```
dr-------- Dizin içeriği listelenebilir, fakat dosya nitelikleri
okunamaz.

d--x------ Dizine girilebilir, ve tam çalıştırma yollarında
kullanılabilir [19]

dr-x------ Dosya nitelikleri sahip tarafından okunabilir.

d-wx------ Dosyalar, dizinin içine girilmeksizin
yaratılabilir/silinebilir.

d------x-t Dosyaların yazma hakkı olan diğerlerince silinmesini
engeller. /tmp dizininde kullanılır.
d---s--s-- Bir etkisi yoktur.
```

Sistem yapılandırma dosyaları (genelde `/etc` içinde) , genelde `640`kipindedir (`-rw-r-----`), ve sahipleri root'tur. Sitenizin güvenlik gereksinimlerine bağlı olarak, bunun üzerinde değişiklik yapmak isteyebilirsiniz. Asla herhangi bir sistem dosyasını grup veya herkes tarafından yazılabilir durumda bırakmayın. Bazı yapılanış dosyaları, `/etc/shadow` da buna dahildir, sadece root tarafından okunabilir durumda olmalı. `/etc` içindeki bazı dizinler de en azından diğer kullanıcılar tarafından erişilemez olmalı.

SUID Kabuk Betikleri

SUID kabuk betikleri, ciddi bir güvenlik riskidir, ve bu sebeple çekirdek tarafından hoş karşılanmazlar. Bir kabuk betiğinin ne kadar güvenli olduğunu düşünürseniz düşünün, bir korsan ondan yararlanarak bir root kabuğuna erişebilir.

Bütünlük Denetimi

Yerel (ve ağ) saldırılarını ortaya çıkarmanın çok iyi bir yolu da bir bütünlük denetleyici, örneğin `Tripwire`, `Aide` veya `Osiris`. gibi bir program çalıştırmaktır. Bu bütünlük denetleyiciler, bütün önemli ikili dosyalarınızın üzerinde bir sağlama toplamı hesaplar, ve dosyalar iyi durumda olduklarındaki toplamlarla karşılaştırır. Sonuç olarak, dosyalardaki değişiklikler farkedilebilir.

Bu tür programları bir diskete kurmak, ve disketin yazma korumasını kapatmak iyi bir fikirdir. Bu yolla saldırganlar bütünlük denetleyicisinin kendisini veya veritabanını kurcalayamazlar. Bir kere bunun gibi bir düzeneğiniz olduktan sonra, bu düzeneği normal yönetim görevleriniz arasında kullanmak, ve değişen bir şeyler olup olmadığını görmek de iyi bir fikirdir.

Hatta, `crontab` 'a denetleyicinizin her gece disketten çalışması için bir girdi ekleyebilir, ve sabaha sonuçlarını gözden geçirebilirsiniz. Aşağıdaki gibi bir şey size her sabah 5:15'te bir raporu mektup olarak yollar:

```
# set mailto
MAILTO=kevin
# run Tripwire
15 05 * * * root /usr/local/adm/tcheck/tripwire
```

Bütünlük denetleyicileri, aksi takdirde farkedilmesi zor olan saldırganları ortaya çıkarmak konusunda bir nimettir. Ortalama bir sistemde çok fazla dosya değiştiği için, hangisinin bir korsan tarafından, hanginizin kendiniz tarafından değiştirildiği konusunda dikkatli olmak zorundasınız.

`Tripwire`'ın açık kaynak sürümünü, ücretsiz olarak http://www.tripwire.org adresinde bulabilirsiniz. Kitapçıklar ve destek ise satın alınabilir.

`Aide` http://www.cs.tut.fi/~rammer/aide.html adresinde,

`Osiris` ise http://www.shmoo.com/osiris/ adresinde bulunabilir.

Truva Atları

Truva Atlarının ismi Virgil'in "Aenid"indeki ünlü numaradan gelmektedir. Bunun arkasındaki fikir, bir korsanın, kulağa çok hoş gelen bir program veya ikili dosya dağıtıp, diğer insanların dosyayı indirmesi ve root olarak çalıştırmasını teşvik etmesidir. Çalıştırılan program, sistem güvenliğini dikkat çekmeden ihlal eder. İnsanlar indirdikleri ve çalıştırdıkları dosyanın tek bir şey yaptığını (ve bunu çok iyi yapıyor da olabilir) düşünürler, ama program bir taraftan güvenliğe de zarar vermekle meşguldür.

Makinenize hangi programları kurduğunuza dikkat edin. Red Hat, RPM dosyaları için, programın gerçeğini kurduğunuzu doğrulayabilmeniz amacıyla, MD5 sağlama toplamları ve PGP imzaları sağlar. Diğer dağıtımlar da benzer yöntemler kullanır. Asla bilmediğiniz, kaynak kodu elinizde bulunmayan bir ikili dosyayı, root olarak çalıştırmayın! Çok az saldırgan kaynak kodlarını halka açık hale getirir.

Karmaşık olabilir, fakat bir programın kaynak kodunu gerçek dağıtım sitesinden aldığınıza emin olun. Eğer program root olarak çalışacaksa, güvendiğiniz birinin kaynak koduna bakmasını ve doğrulamasını sağlayın.

Parola Güvenliği ve Şifreleme

Bugün en önemli güvenlik özelliklerinden biri parolalardır. Hem sizin hem de tüm kullanıcılarınız için, güvenli, tahmin edilemeyen parolalara sahip olmak önemli bir konudur. Yakın zamanlı Linux dağıtımlarının çoğu, kolay tahmin edilebilir bir parola belirlemenizi engelleyen `passwd` programları ile birlikte gelir. `passwd` programınızın güncel ve bu özelliklere sahip olduğundan emin olun.

Şifrelemenin derinlemesine tartışılması bu belgenin konusu ötesindedir, ama bir giriş yapılabilir. Şifreleme gerçekten yararlıdır, hatta bu zaman ve çağda gereklidir de. Şifrelemenin bir çok yöntemi vardır ve her biri kendi özellikler kümesini birlikte getirir.

Bir çok Unix (ve Linux bir istisna değil), parolalarınızı şifrelemek için çoğunlukla tek yönlü, DES (Data Encryption Standard - Veri Şifreleme Standardı) adında bir algoritma kullanır. Şifrelenmiş parola (tipik olarak)`/etc/passwd` veya (daha az sıklıkla) `/etc/shadow`dosyasının içinde tutulur. Sisteme giriş yapmaya kalktığınızda, girmiş olduğunuz parola tekrar şifrelenir, ve parola dosyalarının içindeki ile karşılaştırılır. Eğer uyarsa, o zaman aynı parola olmalı demektir, ve erişime izin verilir. DES aslında iki yönlü bir şifreleme algoritmasıdır (doğru anahtar olduğunda, bir mesajı şifreleyebilir veya şifreli bir mesajın şifresini çözebilirsiniz). Bununla beraber, DES'in Unixler üzerindeki değişik biçimi tek yönlüdür. Bunun anlamı, `/etc/passwd` (veya `/etc/shadow`) dosyasının içindeki şifrelenmiş parolaya bakarak, şifreleme algoritmasını tersine çevirmek yoluyla parolayı bulmak mümkün olmamalıdır.

"Crack" veya "John the Ripper" (Bkz. *"Crack" ve "John the Ripper"*) programlarında olduğu gibi kaba kuvvet saldırıları, parolanızı yeterince rastgele değilse bulabilir. PAM modülleri (aşağıda), parolalarınız ile birlikte başka bir şifreleme algoritmasının kullanılmasına izin verir (MD5 vb.). Crack programını kendi lehinizde de kullanabilirsiniz. Kendi parola veritabanınızı, güvensiz parolalara karşı Crack programını çalıştırarak düzenli olarak denetlemeyi düşünün. Güvensiz parolaya sahip kullanıcıyla iletişim kurarak, parolasını değiştirmesini isteyebilirsiniz.

İyi bir şifrenin nasıl seçildiği hakkında bilgi almak için http://consult.cern.ch/writeup/security/security_3.html adresine gidebilirsiniz.

PGP ve Açık Anahtarlı Şifreleme

Açık anahtarlı şifreleme, örneğin PGP'de kullanılan gibi, bir anahtarı şifreleme, diğer bir anahtarı da şifre çözme için kullanır. Geleneksel şifreleme tekniklerinde, şifreleme ve şifre çözme için aynı anahtar kullanılır. Bu anahtarın, her iki tarafta da bulunması, dolayısıyla bir şekilde bir tarafdan diğer tarafa güvenli şekilde aktarılmış olması gerekir.

Şifreleme anahtarının güvenli aktarımını kolaylaştırmak için, açık anahtarlı şifreleme iki ayrı anahtar kullanır: bir açık anahtar ve bir de özel anahtar. Herkesin açık anahtarı diğerlerine şifreleme yapabilmesi amacıyla "açık"tır, ama herkes özel anahtarını, doğru açık anahtarla yapılmış şifreyi açabilmek için diğerlerinden gizli tutar.

Açık anahtarlı ya da gizli anahtarlı şifrelemenin kendine has bazı avantajları vardır. İkisi arasındaki farklar hakkında bilgi edinmek için the the RSA Cryptography FAQ (RSA Şifreleme SSS) belgesine göz atabilirsiniz.

PGP (Pretty Good Privacy, Oldukça İyi -Kişisel- Gizlilik) Linux'ta iyi desteklenir. 2.6.2 ve 5.0 sürümlerinin iyi çalıştığı biliniyor. İyi bir PGP tanıtımı ve nasıl kullanıldığı ile ilgili bilgiyi PGP SSS içermektedir: http://www.pgp.com/service/export/faq/55faq.cgi

Ülkeniz için uygun sürümü kullandığınızdan emin olun. ABD Hükümetinin dışsatım sınırlamalarından dolayı, güçlü şifrelemenin elektronik yollarla ülke dışına aktarılması yasaktır.

ABD dışsatım denetimleri, artık ITAR tarafından değil, EAR (Export Administration Regulations - Dışsatım Yönetim Düzenlemeleri) tarafından idare edilmektedir.

Ayrıca, Linux üzerinde PGP yapılandırmasını adım adım anlatan bir rehber http://mercury.chem.pitt.edu/~angel/LinuxFocus/English/November1997/article7.html adresinde bulunmaktadır. Bu rehber PGP'nin uluslararası sürümleri için yazılmıştır, ama ABD sürümü için de uyarlanabilir. Bunun yanısıra Linux'un son sürümleri için bir yamaya ihtiyacınız olabilir. Bu yamaya ftp://metalab.unc.edu/pub/Linux/apps/crypto adresinden ulaşabilirsiniz..

PGP'nin ücretsiz ve açık kaynak şekliyle yeniden hayata geçirme amacını taşıyan bir proje var. GnuPG, PGP'nin yerini alacak tamamlanmış ve ücretsiz bir yazılım. IDEA veya RSA'yı kullanmadığı için sınırlandırma olmaksızın kullanılabilir. GnuPG OpenPGP ile uyumludur. Daha fazla bilgi için GNU Gizlilik Nöbetçisi ana sayfasına bakabilirsiniz: http://www.gnupg.org/.

Şifreleme ile ilgili daha fazla bilgi RSA Şifreleme SSS'ında bulunabilir: http://www.rsa.com/rsalabs/newfaq/. Burda, "Diffie-Hellman", "Açık-Anahtarlı Şifreleme", "Sayısal Sertifika" vb. konular hakkında bilgi bulabilirsiniz.

SSL, S-HTTP ve S/MIME

Kullanıcılar sık sık çeşitli güvenlik ve şifreleme protokolleri arasındakı farkları, ve nasıl kullanıldıklarını sorar. Bu bir şifreleme belgesi olmamakla birlikte her bir protokolün ne olduğunu ve daha fazla bilginin nerde bulunabileceğini açıklamak iyi bir fikir olabilir.

- *SSL:* - SL, veya Secure Sockets Layer (Güvenli Soket Katmanı), Netscape tarafından İnternet üzerinde güvenlik sağlamak amacıyla geliştirilen bir şifreleme yöntemidir. SSL veri aktarım katmanında işlev görür, güvenli bir şifreli veri kanalı oluşturduğu için bir çok veri tipini şifreleyebilir. Bu en yaygın olarak, Communicator güvenli bir WWW sitesine bağlandığı, ve güvenli bir belgeyi görüntülemek istediğinde görülür. SSL, Netscape Communications şirketinin diğer veri şifrelemelerinin olduğu kadar, Communicator'ın da güvenli iletişim temellerini oluşturur. Daha fazla bilgi için http://www.consensus.com/security/ssl-talk-faq.html adresine bakabilirsiniz. Netscape'in güvenlikle ilgili hayata geçirdiği diğer örnekler, ve bu protokoller için iyi bir başlangıç noktası da http://home.netscape.com/info/security-doc.html adresinde bulunabilir. SSL protokolü diğer bir çok protokolü "sararak" güvenlik sağlayabilir. http://www.quiltaholic.com/rickk/sslwrap/ adresinde ayrıntılı bilgi bulabilirsiniz.

- *S-HTTP:* - S-HTTP, İnternet üzerinde güvenlik servislerini sağlayan bir diğer protokoldür. Tasarlanma amacı gizlilik, kimlik doğrulama, bütünlük, ve inkar edememe (kendisinden başkası olduğunu söyleyememe) olan S-HTTP, aynı zamanda birden çok anahtar-yönetimi mekanizmasını ve şifreleme algoritmasını, taraflar arasındaki aktarımda yer alan seçenek kararlaştırılması yoluyla destekler. S-HTTP, kendisini hayata geçirmiş olan belirli yazılımlarla sınırlıdır, ve her bir mesajı ayrı ayrı şifreler (RSA Şifreleme SSS, Sayfa 138)

- *S/MIME:* - S/MIME, veya Güvenli Çokamaçlı İnternet Mektup Uzantısı (Secure Multipurpose Internet Mail Extension), elektronik mektup ve İnternet üzerindeki diğer mesajları şifrelemek için kullanılan bir şifremele standardıdır. RSA tarafından geliştirilen açık bir standarttır, dolayısıyla bir gün Linux üzerinde görme olasılığımız yüksektir. S/MIME ile ilgili daha fazla bilgi http://home.netscape.com/assist/security/smime/overview.html adresinde bulunabilir.

Linux IP Güvenliği'nin (IPSec) Hayata Geçirilmesi

CIPE ve diğer veri şifreleme biçimlerinin yanında, IPSEC'in de Linux için bir kaç hayata geçirilme örneği vardır. IPSEC, IP ağ düzeyinde şifreli-güvenli iletişimler yaratmak, ve kimlik doğrulama, bütünlük, erişim denetimi ve gizlilik sağlayabilmek amacıyla IETF tarafından gösterilen bir çabadır. IPSEC ve İnternet taslağı üzerinde daha fazla bilgiye http://www.ietf.org/html.charters/ipsec-charter.html adresinden ulaşabilir, ayrıca anahtar yönetimini içeren diğer protokollere, ve bir IPSEC mektuplaşma (haberleşme) listesi ve arşivlerine ulaşabilirsiniz.

Arizona Üniversitesi'nde geliştirilen, Linux için x-çekirdek (x-kernel) uygulaması, x-çekirdek adı verilen ağ protokollerinin hayata geçirilmesi için nesne tabanlı bir iskelet kullanır. Bununla ilgili bilgi http://www.cs.arizona.edu/xkernel/hpcc-blue/linux.htmladresinde bulunabilir. En basit anlatımla, x-çekirdek, mesajların çekirdek düzeyinde aktarılması yöntemidir, ki bu hayata geçirilmesini kolaylaştırır.

IPSEC'in ücretsiz bir diğer uygulaması da Linux FreeS/WAN IPSEC'tir. WWW sayfalarında belirtildiğine göre,“"Bu servisler, güvenmediğiniz ağların içinde güvenli tüneller oluşturmanızı sağlar. Güvenilmeyen ağdan geçen herşey IPSEC ağ geçidi tarafından şifrelenir ve diğer uçtaki ağ geçidinde şifresi çözülür. Sonuç bir Sanal Özel Ağ, yani VPN'dir (Virtual Private Network). Bu, bir takım farklı sitelerdeki güvensiz İnternet ile birbirine bağlı bulununan makineler içerdiği halde, etkin anlamda özel bir ağdır."”

Bilgisayarınıza indirmek isterseniz, http://www.xs4all.nl/~freeswan/, adresinden ulaşabilirsiniz.

Bu belge yazıldığı sırada sürüm 1.0 henüz çıkmıştı.

Diğer şifreleme biçimleri gibi, bu da dışsatım sınırlamaları nedeniyle çekirdek ile birlikte dağıtılmıyor.

`ssh` (Güvenli Kabuk) ve `stelnet`

`ssh` ve `stelnet` uzak sistemlere giriş yapabilmenizi, ve şifreli bir bağlantı kurabilmenizi sağlayan programlar grubudur.

`openssh` ise for `rlogin`, `rsh` ve `rcp`'nin yerine geçen güvenli bir programlar grubudur. Kullanıcıların kimliğini doğrulamak için ve iki bilgisayar arasındaki iletişimi şifrelemek için açık anahtarlı şifreleme tekniğini kullanır. Uzaktaki bir bilgisayara güvenli şekilde giriş yapmak veya bilgisayarlar arasında veri kopyalama yapmak, ama bu sırada gelebilecek ortadaki-adam (oturum kaçırma) ve DNS taklit saldırılarını engellemek amacıyla kullanılabilir. Bağlantılarınız arasındaki verileri sıkıştırır, ve bilgisayarlar arasındaki X11 iletişimini güvenli hale getirir.

Şu anda bir çok `ssh` uygulaması mevcut. Data Fellows tarafından hayata geçirilen özgün ticari sürümü http://www.datafellows.com adresinde bulunabilir.

Mükemmel Openssh uygulamasında, Data Fellows ssh'ının önceki sürümlerinden biri taban oluşturmuş, ve patentli veya tescilli herhangi bir parça bulunmaması için tamamen yeniden bir çalışma yapılmıştır. BSD lisansı altında ücretsiz olarak dağıtılmaktadır: http://www.openssh.com.

ssh'ı sıfırdan yeniden yazmak amacıyla, "psst..." adıyla başlatılan bir açık kaynak kodlu bir proje daha mevcut. Daha fazla bilgi için: http://www.net.lut.ac.uk/psst/

`ssh`'ı Windows iş istasyonunuzdan Linux `ssh` sunucunuza bağlanmak amacıyla da kullanabilirsiniz. Ücretsiz olarak dağıtılan bir çok Windows istemcisi de mevcut, bunlardan birine http://guardian.htu.tuwien.ac.at/therapy/ssh/ adresinden ulaşabilirsiniz. Data Fellows'un ticari bir uygulamasına ise aşağıdaki adresten ulaşılabiliyor olmalı: http://www.datafellows.com.

SSLeay, Netscape'in Güvenli Soket Katmanı protokol uygulamasının, Eric Young tarafından yazılan ücretsiz bir sürümü. Güvenli telnet gibi bazı uygulamalar, Apache için bir modül, bir takım veritabanları, ve DES, IDEA, ve Blowfish algoritmaları SSLeay'in içinde bulunabilir.

Bu kütüphaneyi kullanarak, telnet bağlantısı üzerinde şifreleme yapan güvenli bir telnet uygulaması oluşturuldu. SSH'nin tersine, stelnet SSL'yi, Netscape tarafından geliştirilen Güvenli Soket Katmanı'nı kullanıyor. Güvenli telnet ve Güvenli FTP hakkında bilgiyi SSLeay SSS'ından başlayarak bulabilirsiniz: http://www.psy.uq.oz.au/~ftp/Crypto/.

Bir diğer güvenli telnet/ftp uygulaması ise SRP. WWW sayfalarından:

“"SRP projesi, dünya çapında ücretsiz kullanım için güvenli İnternet yazılımı geliştiriyor. Tamamen güvenli bir Telnet ve FTP dağıtımından başlayarak, ağ üzerindeki zayıf kimlik doğrulama sistemlerini değiştirmeyi, bunu yaparken de güvenlik uğruna kullanıcı-dostluğunu kurban etmemeyi amaçlıyoruz. Güvenlik, varsayılan olmalı, bir seçenek değil!"”

Daha fazla bilgi için: http://www-cs-students.stanford.edu/~tjw/srp/

PAM - Takılabilir Kimlik Doğrulama Modülleri

Red Hat Linux dağıtımlarının yeni sürümleri, "PAM" adı verilen birleşmiş bir kimlik doğrulama tasarımı ile birlikte geliyor. PAM, kimlik doğrulama yöntem ve gereksinimlerinizi çalışma kesilmeksizin değiştirmenize izin veriyor, ve ikililerinizin yeniden derlenmesine gerek bırakmaksızın bütün yerel kimlik doğrulama yöntemlerinizi çevreliyor. PAM yapılandırması, bu belgenin konusu dışında, bununla birlikte daha fazla bilgi için PAM sitesini şöyle bir gözden geçirmeyi ihmal etmeyin: http://www.kernel.org/pub/linux/libs/pam/index.html.

PAM ile yapabileceklerinizden sadece bir kaçı:

- Parolalarınız için DES'ten başka bir şifreleme kullanma (Böylelikle kaba kuvvet saldırılarını daha da zorlaştırma)
- Tüm kullanıcılarınızın üzerinde, kaynak sınırlandırmaları koyabilme, böylelikle servis-reddi saldırılarını engelleme (işlem sayısı, bellek miktarı vb.)
- Çalışma kesilmeksizin gölge parolaya geçiş olanağı (aşağıya bakın)
- Belirli kullanıcıların, sadece belirli zamanlarda ve belirli yerlerden giriş yapmalarına izin verme

Sisteminizi bir kaç saat içinde kurduktan ve yapılandırdıktan sonra, bir çok saldırıyı gerçekleşmeden durdurabilirsiniz. Örneğin, kullanıcıların ev dizinlerindeki `.rhosts` dosyalarının kullanımını engellemek için, sistem genelinde `/etc/pam.d/rlogin` dosyasına aşağıdaki satırları ekleyerek PAM'i kullanabilirsiniz:

```
#
# Kullanıcılar için rsh/rlogin/rexec kullanımını yasakla
#
login auth required pam_rhosts_auth.so no_rhosts
```

Şifreli IP Sarma (CIPE)

Bu yazılımın birincil amacı (gizlice dinleme, trafik çözümlemesi ve araya sahte mesaj sokmaya karşı), İnternet gibi güvensiz paket ağı boyunca oluşturulan alt ağ bağlantılarını güvenli hale getirmede bir kolaylık sağlamaktır.

CIPE veriyi ağ düzeyinde şifreler. Bilgisayarlar arasında ağ üzerinde seyahat eden paketler şifrelenir. Şifreleme motoru, paketleri alan ve gönderen sürücüye yakın bir yerdedir.

Bu, verileri soket düzeyinde bağlantılara göre şifreleyen SSH'den farklıdır. Farklı bilgisayarda çalışan programlar arası mantıksal bağlantılar şifrelenir.

CIPE, Sanal Özel Ağ yaratmak amacıyla tünellemede kullanılabilir. Düşük-düzey şifrelemenin, uygulama yazılımında değişiklik yapmaksızın VPN'de bağlı iki ağ arasında şeffaf şekilde çalıştırılabilme getirisi vardır.

CIPE belgesinden özet:

"IPSEC standartları, (diğer şeyler arasında) şifrelenmiş VPN'ler oluşturmak için kullanılabilecek protokoller kümesini tanımlar. Bununla birlikte, IPSEC, bir çok seçeneği olan ağır ve karışık bir protokol kümesidr, protokolün bütün olarak hayata geçirilebildiği durumlar nadirdir ve bazı konular (anahtar idaresi gibi) tam olarak çözülmemiş durumdadır. CIPE, değiştirgelenebilen bir çok şeyin (kullanılan asıl şifreleme algoritmasının seçimi gibi) kurulum zamanındaki sabit bir seçim olduğu daha basit bir yaklaşım kullanır. Bu esnekliği kısıtlar, ama daha basit (ve dolayısıyla daha etkili, böcek ayıklamasını kolaylaştıran) bir uygulama olanağı sağlar."

Daha fazla bilgi http://www.inka.de/~bigred/devel/cipe.html adresinde bulunabilir.

Diğer şifreleme biçimleri gibi, dışsatım kısıtlamaları yüzünden çekirdek ile birlikte dağıtılmamaktadır.

Kerberos

Kerberos, MIT'teki [20] Athena Projesi tarafından geliştirilen bir kimlik doğrulama sistemidir. Kullanıcı sisteme giriş yaptığında, Kerberos kullanıcının kimliğini doğrular (bir parola kullanarak),

ve kullanıcıya ağa dağılmış diğer sunucular ve bilgisayarlara kimliğini kanıtlamak için bir yol sağlar.

İşte bu kimlik doğrulama `rlogin` gibi programlar tarafından kullanılır (`.rhosts` dosyası yerine), ve kullanıcıya diğer bilgisayarlara parolasız girebilmesi için izin verilir. Bu kimlik doğrulama yöntemi posta sistemi tarafından da mektubun doğru kişiye dağıtıldığından emin olmak, ve gönderen kişinin iddia ettiği kişi olduğunu garanti altına almak amacıyla kullanılabilir.

Kerberos ve birlikte gelen diğer programlar, kullanıcıların başka birini "taklit" yoluyla sistemi yanıltmasını engeller. Ne yazık ki, Kerberos'u kurmak kökten değişiklik ister, bir çok standard programın yenileriyle değiştirilmesini gerektirir.

Kerberos hakkında daha fazla bilgi almak için Kerberos SSS'a, kodu almak içinse http://nii.isi.edu/info/kerberos/ adresine bakabilirsiniz.

[Kaynak: Stein, Jennifer G., Clifford Neuman, and Jeffrey L. Schiller. "Kerberos: An Authentication Service for Open Network Systems (Kerberos: Açık Ağ Sistemleri için Bir Kimlik Doğrulama Servisi") USENIX Konferans Tutanakları, Dallas, Texas, Winter 1998.]

Kerberos, bilgisayarınızın güvenliğini iyileştirmede ilk adımınız olmamalı. Oldukça kapsamlı olduğu gibi, örneğin SSH kadar yaygın olarak da kullanılmamaktadır.

Gölge Parolalar

Gölge parolalar, şifrelenmiş parola bilgilerinizi normal kullanıcılardan gizli tutmanın bir yoludur. Hem Red Hat hem de Debian Linux dağıtımlarının yeni sürümleri, gölge parolaları var sayılan yapılandırmada kullanıyor, fakat diğer sistemlerde, şifrelenmiş parolalar, herkesin okuyabileceği şekilde `/etc/passwd`dosyasında saklanıyor. Herhangi biri bunlar üzerinde parola-tahmin programları kullanarak ne olduklarını bulmaya çalışabilir. Gölge parolalar ise tam tersine `/etc/shadow`, dosyasında saklanır, ve sadece yetkili kullanıcılar okuyabilir. Gölge parolalar, kullanılabilmek için, parola bilgisine erişime gereksinim duyan bütün yararlı programlar tarafından destekleniyor olmalıdır. PAM (yukarıda) de bir gölge modülünün takılmasına izin verir, ve çalıştırabilir dosyaların yeniden derlenmesini gerektirmez. Daha fazla bilgi için Shadow-Password HOWTO (Gölge-Parola NASIL) dosyasına başvurabilirsiniz: http://metalab.unc.edu/LDP/HOWTO/Shadow-Password-HOWTO.html Yalnız oldukça eski olabilir ve PAM'ı zaten destekleyen dağıtımlar için gerek yoktur.

"Crack" ve "John the Ripper"

Herhangi bir nedenle `passwd` programı tahmini-zor parolalar seçmeye zorlayamıyorsa, bir parola-kırıcı program çalıştırmak, ve kullanıcılarınızn parolalarının güvenli olduğundan emin olmak isteyebilirsiniz.

Parola kıran programlar basit bir düşünceye dayanarak çalışır: Sözlükteki her sözcüğü, ve sözcüklerden türeyen ifadeleri dener. Önce bunları şifreler, daha sonra sistemdeki şifrelenmiş parola ile karşılaştırır. Eğer birbirini tutarsa, parolayı bulmuş olurlar.

En dikkate değer ikisi "Crack" ve "John the Ripper" olmak üzere (http://www.openwall.com/john/) ortalarda dolaşan bir kaç program mevcuttur. Bu programlar çok fazla işlemci zamanı alırlar, fakat önce kendiniz çalıştırarak ve zayıf parolası olan kullanıcıları farkederek herhangi bir saldırganın bunları kullanarak sisteme girip giremeyeceğini öğrenebilirsiniz. Dikkat edilmesi gereken bir nokta, bir saldırganın bu programları kullanabilmesi için, önce başka bir açık kullanarak`/etc/passwd` dosyasını okumuş olması gerekir ve bu tür açıklar düşündüğünüzden daha yaygındır.

Güvenlik, en güvensiz bilgisayar kadar güçlü olduğundan, belirtilmelidir ki, eğer ağınızda Windows makineler varsa L0phtCrack programına da bir göz atmak isteyebilirsiniz. L0phtCrack Windows için bir parola kırma uygulamasıdır: http://www.l0pht.com

CFS - Şifreli Dosya Sistemi ve TCFS - Şeffaf Şifreli Dosya Sistemi

CFS bütün dizin ağaçlarını şifrelemenin, ve kullanıcıların bu dizinlerde şifreli dosyalar saklayabilmesini sağlamanın bir yoludur. Yerel makinede çalışan bir NFS sunucusundan yararlanır. RPM dosyalarını, http://www.zedz.net/redhat/ adresinden, ve nasıl çalıştığı hakkında daha fazla bilgiyi ise ftp://ftp.research.att.com/dist/mab/ adresinden bulabilirsiniz.

TCFS, dosya sistemine daha fazla bütünlük katarak CFS'in geliştirilmiş halidir, böylece dosya sisteminin şifrelenmiş olduğu kullanıcılara şeffaf olur. Daha fazla bilgi: http://www.tcfs.it/.

Ayrıca tüm dosya sistemleri üzerinde de kullanılabilir. Dizin ağaçları üzerinde de çalışılabilir.

X11, SVGA ve Görüntü Güvenliği

X11

Saldırganların parolalarınızı yazarken çalmasını, ekranda okuduğunuz belge ve bilgileri okumasını, hatta root erişimi sağlama için bir açık kullanmasını engellemek amacıyla, çizgesel görüntünüzü güvenli hale getirmeniz önem taşır. Ağ üzerinde uzak X uygulamaları çalıştırmak da, koklayıcıların uzak sistemle olan tüm etkileşiminizi görmeleri açısından, tehlike dolu olabilir.

X bir takım erişim-denetim mekanizmalarına sahiptir. Bunların en basiti bilgisayar bazında olandır. Görüntünüze erişmesine izin verdiğiniz bilgisayarlar için `xhost` programını kullanırsınız. Bu kesinlikle çok güvenli değildir, çünkü biri makinenize erişim sağlarsa, `xhost + saldırganın makinesi` aparak rahatlıkla girebilir. Ayrıca, güvensiz bir makineden erişime izin verirseniz, oradaki herhangi biri görüntünüzü bozabilir.

Giriş yapmak için `xdm` (X Display Manager, X Görüntü Yöneticisi) kullanırken, çok daha iyi bir erişim yönteminiz vardır: MIT-MAGIC-COOKIE-1. 128 bitlik bir çerez üretilir ve `.Xauthority` dosyanızda saklanır. Eğer uzak bir makineye görüntü erişim izni vermek isterseniz, `xauth` komutunu ve `.Xauthority` dosyanızdaki bilgiyi bunu sağlamak için kullanabilirsiniz. Remote-X-Apps mini-howto (Uzak-X-Uygulamaları Mini-NASIL) belgesine bir göz atabilirsiniz: http://metalab.unc.edu/LDP/HOWTO/mini/Remote-X-Apps.html.

Güvenli X bağlatıları için `ssh` (see *ssh (Güvenli Kabuk) ve stelnet* da kullanabilirsiniz. connections. unun son kullanıcıya şeffaf olması avantajı vardır, ve ağda şifrelenmemiş hiç bir veri akışının olmadığı anlamına gelir.

Ayrıca, X sunucunuzu '-nolisten tcp' seçeneği ile çalıştırarak, uzaktan erişimi tamamen kapatabilirsiniz. Bu, sunucunuza tcp soketleri üzerinden herhangi bir ağ bağlantısına engel olacaktır.

X güvenliği ile ilgili daha fazla bilgi için `Xsecurity` man page for more information on X security. man sayfasına bir göz atın. En güvenilir yol, konsola giriş yapmak için `xdm` , üzerinde X programları çalıştırmak istediğiniz uzak sitelere gitmek içinse `ssh` kullanmaktır.

SVGA

SVGAlib programları, Linux makinenizin video donanımına erişmek için tipik olarak SUID-root'tur. Bu onları çok tehlikeli yapar. Eğer göçerlerse, kullanılır bir konsol almak için tipik olarak makinenizi yeniden başlatmak zorunda kalırsınız. SVGA programlarınızın düzgün olduğundan, en azından bir şekilde güvenilir olduğundan emin olun. Daha da iyisi, hiç çalıştırmayın.

GGI GGI (Genel Çizgesel Arabirim Projesi)

Linux GGI projesi, Linux'ta video arabirimlerinden kaynaklanan bir takım problemleri çözmeyi deneyen bir projedir. CGI, bir parça video kodunu Linux çekirdeğine taşır, sonra video sistemine erişimi denetler. Bu, çekirdeğinizin iyi bir durumunun herhangi bir zamanda tekrar çağrılabileceği anlamına gelir. Verdikleri güvenli anahtar sayesinde, konsolunuzda çalışan bir Truva atı `login` programının olmadığından emin olabilirsiniz. http://synergy.caltech.edu/~ggi/

Çekirdek Güvenliği

Bu bölümde güvenlikle ilgili çekirdek yapılandırma seçeneklerini açıklayacak, ne işe yaradıklarını ve nasıl kullanıldıklarını anlatılıyor.

Çekirdek, bilgisayarnızın ağını denetim altında tuttuğu için, çok güvenli olması ve bozulmaması önemli. En yeni ağ saldırılarını engellemek için, çekirdek sürümünüzü güncel tutmaya çalışmalısınız. Çekirdeklerinizi ftp://ftp.kernel.org adresinden, veya dağıtıcınızdan bulabilirsiniz.

Ana Linux çekirdeğine, birleştirilmiş bir şifre yaması sağlayan uluslararası bir grup var. Bu yama, dışsatım kısıtlamaları yüzünden ana çekirdeğe dahil edilemeyen şeyler ve bazı şifreli alt sistemler için destek sağlıyor. Daha fazla bilgi için: http://www.kerneli.org

2.0 Çekirdek Derleme Seçenekleri

2.0.x çekirdekleri için izleyen seçenekler geçerli. Bu seçenekleri çekirdek yapılandırma işlemi sırasında görürsünüz. Buradaki yorumların çoğu `./linux/Documentation/Configure.help`, belgesinden, aynı belge çekirdeğin `make config` aşamasında Help (Yardım) kısmında da kullanılıyor.

- Ağ Güvenlik duvarları (CONFIG_FIREWALL)

  Bu seçenek, eğer Linux makinenizde güvenlik duvarı kullanacaksanız, veya maskeleme yapacaksanız açık olmalı. Eğer sıradan bir istemci makine olacaksa, kapata da bilirsiniz.

- IP: yönlendirme/ağ geçidi (CONFIG_IP_FORWARD)

  IP yönlendirmesini açarsanız, Linux kutunuz bir yöneltici haline gelir. Eğer makineniz ağ üzerinde ise, bir ağdan diğerine veri yönlendiriyor olabilirsiniz, belki de bunun olmasını engelleyen bir güvenlik duvarını devre dışı bırakarak. Normal çevirmeli ağ kullanıcıları bunu kapatmak isteyecektir, diğer kullanıcılar ise bunun güvenlik yan etkileri üzerinde düşünmelidir. Güvenlik duvarı görevi yapacak makineler bu seçeneğin açık olmasını, ve güvenlik duvarı yazılımıyla uyum içinde kullanılmasını gerektirir.

  IP yönlendirmeyi şu komutu kullanarak dinamik şekilde açabilir:

```
root#  echo 1 > /proc/sys/net/ipv4/ip_forward
```

  ve şu komutu kullanarak da kapatabilirsiniz:

```
root#  echo 0 > /proc/sys/net/ipv4/ip_forward
```

  proc dizini içindeki dosyaların "sanal" dosyalar olduğunu ve gösterilen boyutun dosyadan alınabilecek veri miktarını yansıtmadığını aklınızdan çıkarmayın.

- IP: syn çerezleri (CONFIG_SYN_COOKIES)

"SYN Saldırısı", makinenizdeki tüm kaynakları tüketen bir servis reddi (DoS) saldırısıdır, sistemi yeniden başlatmak zorunda kalırsınız. Normal olarak bu seçeneği açmamanızı gerektirecek bir sebep düşünemiyoruz. 2.2.x çekirdek serisinde bu yapılandırma seçeneği "syn çerez"lerini açmaya izin verir, fakat onları açmaz. Açmak için aşağıdaki komutu kullanmalısınız:

```
root# echo 1 > /proc/sys/net/ipv4/tcp_syncookies <P>
```

- IP: Güvenlik duvarı (CONFIG_IP_FIREWALL)

  Makinenizi bir güvenlik duvarı olarak yapılandıracaksanız, veya maskeleme yapacaksanız, veya PPP çevirmeli ağ arabirimini kullanarak çevirmeli ağ iş istasyonunuza birinin girmesine engel olmak istiyorsanız bu seçeneği açmanız gerekir.

- IP: Güvenlik duvarı paket günlüğü (CONFIG_IP_FIREWALL_VERBOSE)

  Bu seçenek güvenlik duvarınızın paketler hakkında aldığı gönderici, alıcı, port gibi bilgileri verir.

- IP: Kaynaktan yönlendirilen çerçeveyi düşür (CONFIG_IP_NOSR)

  Bu seçenek etkinleştirilmelidir. Kaynaktan yönlendirilen çerçeveler, gidecekleri yeri paketin içinde bulundurur. Bu, paketin içinden geçtiği yöneltici tarafından incelenmemesi, ve sadece yönlendirmesi anlamına gelir. Bu, potansiyel açıklardan yararlanmak isteyen verinin sisteminize girebilmesine olanak tanıyabilir.

- IP: Maskeleme (CONFIG_IP_MASQUERADE)

  Linux'unuzun güvenlik duvarı rolünü üstlendiği yerel ağınızdaki bilgisayarlardan biri dışarı bir şey göndermek isterse, Linux'unuz kendini o bilgisayar olarak "maskeleyebilir", yani trafiği istenen hedefe göndererek, kendisinden geliyormuş gibi görünmesini sağlayabilir. Daha fazla bilgi için http://www.indyramp.com/masq adresine bakın.

- IP: ICMP Maskeleme (CONFIG_IP_MASQUERADE_ICMP)

  Bu seçenek, sadece TCP ve UDP trafiğinin maskelenmesi anlamına gelen bir önceki seçeneğe ICMP maskelemesini de ekler.

- IP: şeffaf vekil desteği (CONFIG_IP_TRANSPARENT_PROXY)

  Bu, Linux güvenlik duvarınızın, yerel ağdan çıkan ve uzaktaki bir bilgisayara gidecek olan tüm trafiği, "şeffaf vekil sunucu" adı verilen yerel bir sunucuya yönlendirebilir. Bu, yerel kullanıcıların uzak uç ile konuştuklarını sanmalarına yol açar, halbuki yerel vekile bağlanmış durumdadırlar. Daha fazla bilgi için http://www.indyramp.com/masq adresindeki IP-Masquerading HOWTO (IP Maskeleme NASIL) belgesine göz atın.

- IP: parçaları daima birleştir (CONFIG_IP_ALWAYS_DEFRAG)

  Genellikle bu seçenek kapalı durumdadır, fakat bir güvenlik duvarı veya maskeleyen bir bilgisayar oluşturuyorsanız, etkin hale getirmek isteyeceksiniz. Veri bir bilgisayardan diğerine giderken, her zaman tek bir paket halinde değil, bir kaç parçaya ayrılarak gönderilir. Buradaki sorun birinin kalan paketlere orada olması beklenmeyen bazı bilgileri sokmasıdır. Bu seçenek ayrıca, gözyaşı saldırısına karşı yama uygulanmamış içerdeki bir bilgisayara yapılan bu saldırıyı da engelleyebilir.

- Paket İmzaları (CONFIG_NCPFS_PACKET_SIGNING)

  Bu, 2.2.x çekirdek dizisinde yer alan ve daha güçlü güvenlik için NCP paketlerinin imzalanmasını sağlayan bir seçenektir. Olağan durumlarda kapalı bırakabilirsiniz, ama

gereksinim duyarsanız orda duruyor.

- IP: Güvenlik duvarı paket ağbağlantısı aygıtı (CONFIG_IP_FIREWALL_NETLINK)

  Bu, bir paketin meşruluk durumuna bakarak kabul edilip edilmeyeceğini belirlemek amacıyla, kullanıcı uzayında çalışan herhangi bir programındaki paketlerin ilk 128 baytını inceleyebilmenizi sağlayan etkileyi bir seçenektir.

2.2 Çekirdek Derleme Seçenekleri

2.2.x çekirdekleri için, seçeneklerin çoğu aynı, fakat yeni bir kaç seçenek daha var. Buradaki açıklamaların çoğu, çekirdeği derlerken ki `make config` aşamasında kullanılan Yardım bölümünün referans aldığı `./linux/Documentation/Configure.help` belgesiyle aynıdır[21]. Gereken seçeneklerin bir listesi için 2.0 açıklamalarına başvurun. 2.2 çekirdekteki en anlamlı değişiklik IP güvenlik duvarı kodudur. Artık güvenlik duvarı oluşturmak için, 2.0 çekirdeğindeki `ipfwadm` programının yerine `ipchains` programı kullanılıyor. [22]

- Soket Süzümü (CONFIG_FILTER)

  Çoğu insan için bu seçeneğe hayır demek güvenlidir. Bu seçenek, tüm soketlere kullanıcı uzayında bir süzgeci bağlamanızı, ve bu yolla paketlerin geçişine izin verilip verilmeyeceğini belirlemenizi sağlar. Çok özel bir gereksinim duyuyor olmadıkça ve böyle bir süzgeç programlayabilir bilgiye sahip olmadıkça hayır demelisiniz. Ayrıca bu belgenin yazılışı sırasında TCP dışındaki tüm protokoller destekleniyordu.

- Port Yönlendirme

  Port Yönlendirme, güvenlik duvarındaki belirli portlarda, dışarı giden veya içeri gelen paketlerde bazı yönlendirmelerin yapılabilmesini sağlar. Bu, örneğin bir WWW sunucusunu güvenlik duvarının veya maskeleme bilgisisayarının arkasında çalıştıracağınız halde o WWW sunucusunun dış dünyadan ulaşılabilir durumda olması gerektiği durumlarda yararlıdır. Bir dış istemci güvenlik duvarının 80. portuna bir istek yollar, güvenlik duvarı bu isteği WWW sunucusuna yönlendirir, WWW sunucusu istekle ilgilenir ve sonuçları güvenlik duvarının üstünden tekrar özgün istemciye gönderir. İstemci güvenlik duvarının kendisinin WWW sunucusu olarak çalıştığını düşünür. Bu, eğer güvenlik duvarının arkasında bir WWW sunucu çiftliği bulunduruyorsanız, yük dengelemede de kullanılabilir.

  Bu özellik hakkında daha fazla bilgiyi http://www.monmouth.demon.co.uk/ipsubs/portforwarding.html adresinden bulabilirsiniz. Genel bilgi için lütfen ftp://ftp.compsoc.net/users/steve/ipportfw/linux21/ adresine göz atın.

- Soket Süzümü (CONFIG_FILTER)

  Bu seçeneği kullanarak, kullanıcı uzayındaki programları tüm soketlere bir süzgeç ekleyebilir, dolayısıyla çekirdeğe belirli tipteki verinin soket içinden geçip geçemeyeceğini bildirebilir. Linux soket süzümü şimdilik TCP dışındaki tüm soket tiplerinde çalışıyor. Daha fazla bilgi için `./linux/Documentation/networking/filter.txt` dosyasına göz atın.

- IP: Maskeleme

  2.2 çekirdek maskeleme geliştirilmiş durumda. Özel protokollerin maskelenmesi için ek destek sağlıyor vb. Daha fazla bilgi için Ipchains NASIL belgesine göz atın.

Çekirdek Aygıtları

Linux üzerinde güvenlik konusunda yardımcı olabilecek bir kaç blok ve karakter aygıtı mevcuttur.

`/dev/random` ve `/dev/urandom` aygıtları, rastgele veri sağlama amacını taşır.

Hem `/dev/random` hem de `/dev/urandom`, PGP anahtarlarının üretilmesinde, `ssh` bağlantılarında, ve rastgele sayıların gerektiği diğer uygulamalarda kullanılmak için yeteri kadar güvenli olmalıdır. Verilen herhangi bu kaynaklardan çıkan herhangi bir sayı dizisi için saldırganlar bir sonraki sayıyı tahmin edememeli. Bu kaynaklardan elde edilen verinin kelimenin tam anlamıyla rastgele olması için çok fazla çaba ortaya konmuştur.

Bu iki cihaz arasındaki tek fark, `/dev/random` cihazının elindeki rastgele baytların tükenmesi, ve yenileri toplanması için beklemek zorunda oluşunuzdur. Yani kullanıcı tarafından üretilen entropinin sisteme girmesi için beklemesi durumunda uzun bir süre çalışması durabilir. Dolayısıyla `/dev/random`'ı kullanırken dikkatli olmak zorundasınız. (Belki de yapılacak en iyi şey bu cihazı hassas anahtarlama bilgisini üretirken kullanmak, ve kullanıcıya "Tamam, yeterli" denilene kadar klavyesindeki tuşlara rastgele basmasını söylemektir.)

`/dev/random` yüksek kalitede entropi sağlar, kesmeler arasındaki farklı zamanları ölçme vb. şeylerden elde edilir. Yeterli bitte rastgele veri var olana kadar çalışması durur.

`/dev/urandom` benzeri bir aygıttır, fakat depolanmış entropi azalmaya başladığında, olan kadarının, güçlü bir şifresel hash değerini döndürür. Bu, rastgele veri kadar güvenli olmasa da çoğu uygulama için yeterli derecede güvenlidir.

Bu aygıtlardan okuma yapmak için aşağıdaki gibi bir şey kullanabilirsiniz:

```
root#  head -c 6 /dev/urandom | mimencode
```

Bu, konsola sekiz rastgele karakter yazar, örneğin parola üretimi için kullanılabilir. You can find `mimencode` programını `metamail` paketi içinde bulabilirsiniz.

Algoritmanın açıklaması için `/usr/src/linux/drivers/char/random.c` dosyasına bi göz atın.

Bu konuda bana yardımcı olan, Theodore Y. Ts'o, Jon Lewis, ve Linux çekirdek grubundan diğerlerine teşekkürler.

Ağ Güvenliği

Ağ güvenliği, insanların bağlı olduğu süre arttıkça, daha önemli hale gelmektedir. Ağ güvenliğini ihlal etmek, fiziksel veya yerel güvenliği ihlal etmekten çok daha kolay, ve çok daha yaygındır.

Ağ güvenliğine yardımcı olan iyi araçlar var, ve Linux dağıtımlarıyla birlikte gelenlerin sayısı gittikçe artıyor.

Paket Koklayıcılar

Saldırganların, ağınız üzerinde daha fazla sisteme erişim kazanmasının en yaygın yollarından biri, güvenliği ihlal edilen bilgisayarlardan birinin üzerinde bir paket koklayıcı çalıştırmasıdır. Bu "koklayıcı", paket akışı içinde `passwd`, `login` ve `su` gibi programlar için Ethernet portunu dinler ve günlük tutar. Bu yolla saldırganlar, girmeye hiç kalkışmadıkları sistemlerin parolalarına dahi erişebilirler. Açık metin parolalar bu saldırıya karşı çok korunmasızdırlar.

Örnek: A Bilgisayarının güvenliği ihlal edilmiş durumda. Saldırgan bir koklayıcı kurar. Koklayıcı,

B Bilgisayarından C Bilgisayarına giriş yapan sisyön (sistem yöneticisi) parolasını ele geçirir. Sonra, sisyön bir sorunu çözmek için `su` yapar. Saldırganlar böylelikle B Bilgisayarındaki root parolasına da sahip olur. Daha sonra sisyön, herhangi bir kişiye, hesabile bağlanmasına izin verir. Artık saldırgan Z Bilgisayarında da bir parola/giriş bilgisine sahiptir.

Günümüzde bir saldırganın bunu yapabilmesi için bir sistemin güvenliğini ihlal etmesine dahi gerek yoktur: Kendi kişisel veya dizüstü bilgisayarlarını bir binaya getirip ağınıza saplanabilirler.

Using `ssh` veya diğer şifreli parola yöntemlerini kullanarak, bu saldırının önüne geçilebilir. POP hesapları iin APOP gibi şeyler bu saldırıyı engeller (Olağan POP girişleri, ağ üzerinde açık metin parola gönderen herşey gibi, bu saldırıya karşı çok korunmasızdır).

Sistem servisleri ve tcp_wrappers

Linux sisteminizi *HERHANGİ* bir ağ üzerine koymadan önce, bakmanız gereken ilk şey hangi servisleri sunmanız gerektiğidir. Sunmanız gerekmeyen servisler kapatılmalı, ki her gereksiz servisin kapatılışı, endişelenmeniz gereken ve saldırganların açık arayacağı şeylerin bir azalması anlamına gelir.

Linux'ta servisleri kapatmanın bir kaç yolu vardır. `/etc/inetd.conf` dosyasına bakarak `inetd` tarafından hangi servislerin sunulduğunu görebilirsiniz. Gereksinim duymadıklarınızı açıklama haline getirerek (o satırın başına `#` koyarak), ve sonrasında `inetd` işlemine bir SIGHUP sinyali göndererek kapatabilirsiniz.

Bunun yanısıra, `/etc/services` dosyasındaki servisleri silebilirsiniz (ya da açıklama haline getirebilirsiniz). Bu, yerel istemcilerin de servisi kullanamaması anlamına gelir (yani `ftp`,satırını siler, sonra o makineden uzaktaki bir siteye Genellikle `ftp` bağlantısı yapmaya çalışırsanız, işlem "bilinmeyen servis" mesajı vererek başarısız olacaktır. Genellikle `/etc/services` dosyasındaki servisleri kaldırarak çıkacak sorunlarla uğraşmaya değmez, çünkü ek bir güvenlik getirisi yoktur. Eğer yerel bir kullanıcı, kaldırmış olmanıza rağmen ftp kullanmak isterse, yaygın `ftp` portunu kullanan kendi istemcisini yapıp bunu başarabilir.

Çalışır durumda olmasını isteyebileceğiniz servislerden bazıları:

- `ftp`
- `telnet` (veya `ssh`)
- mail, örneğin `pop-3` veya `imap`
- `identd`

Eğer belirli bir paketi kullanmayacağınızdan eminseniz, toptan kaldırma yolunu da seçebilirsiniz. Red Hat Linux altında `rpm -e paket_ismi` komutu ile bütün paketi silmeniz mümkündür. Debian altında`dpkg --remove` komutu aynı işi görecektir.

Ek olarak, gerçekten rsh/rlogin/rcp gereçlerini `/etc/inetd.conf` dosyasını kullanarak kapatmak isteyebilirsiniz; buna login (`rlogin` rlogin tarafından kullanılan), shell (`rcp` tarafından kullanılan), ve exec (`rsh` tarafından kullanılan) de dahildir. Bu protokoller aşırı derecede güvensizdir ve geçmişte bir çok açığın sebebi olmuştur.

`/etc/rc.d/rc[0-9].d` (Red Hat) veya`/etc/rc[0-9].d` (Debian) başlangıç dizinlerini kontrol ederek, herhangi bir sunucunun çalıştırılıp çalıştırılmadığını görebilirsiniz. Bu dizindeki dosyalar aslında`/etc/rc.d/init.d` (Red Hat) veya `/etc/init.d` (Debian) dizinindeki dosyalara simgesel bağlardır. `init.d` dizinindeki dosyaların isimlerini değiştirmek, o dosyaya bağlı olan simgesel bağları etkisiz hale getirir. Eğer belirli bir çalışma düzeyindeki servisi kapatmak istiyorsanız, ilgili simgesel bağın ismindeki büyük `S` harfini küçük `s` harfiyle değiştirebilirsiniz:

```
root#  cd /etc/rc6.d
root#  mv S45dhcpd s45dhcpd
```

Eğer BSD-tarzı `rc` dosyalarınız varsa, ihtiyacınız olmayan programlar için `/etc/rc*` dizinlerini kontrol etmek isteyebilirsiniz.

Çoğu Linux dağıtımı, tüm TCP servislerinizi "örten" tcp_wrappers ile birlikte gelir. Gerçek sunucunun yerine `inetd` içinden bir tcp_wrapper (`tcpd`) çalıştırılır, `tcpd` servisi isteyen bilgisayarı kontrol eder, ya gerçek sunucuyu çalıştırır, veya o bilgisayardan erişimi reddeder. `tcpd` , TCP servislerinize erişimi kısıtlamanızı sağlar. Bir `/etc/hosts.allow` dosyası oluşturmalı, ve sadece makinenize erişime gereksinim duyan bilgisayarları eklemelisiniz.

Evden bağlanan bir çevirmeli ağ kullanıcı iseniz, önerimiz her bağlantıyı reddetmenizdir. `tcpd` aaynı zamanda başarısız olan bağlantı girişimlerinin de günlüğünü tutar, bu şekilde bir saldırı geldiğinde haberiniz olur. Eğer yeni TCP-tabanlı servisler eklerseniz, tcp_wrappers kullanacak şekilde yapılandırmalısınız. Örneğin, olağan çevirmeli ağ kullanıcıları dışarıdakilerin kendi makinelerine bağlanmasını engelleyebilir, ama aynı zamanda mektup alma, ve İnternete ağ bağlantısı kurma işlemlerini de gerçekleştirebilir. Bunu yapmak için, `/etc/hosts.allow` dosyanıza:

ALL: 127.

satırını ekleyebilirsiniz. Elbette /etc/hosts.deny dosyanız da

ALL: ALL

satırını bulundurmalı. Bu şekilde makinenize dışarıdan gelen tüm bağlantıları engeller, bununla birlikte içerde İnternetteki servislere bağlanmanıza izin verirsiniz.

tcp_wrappers'ın diğer bir kaç diğer servis dışında, sadece`inetd` tarafından çalıştırılan servisleri koruduğunu unutmayın. Makinenizde çalışan pekala diğer servisler de olabilir. `netstat -ta` komutunu kullanarak makinenizde sunulan tüm servislerin bir listesini görebilirsiniz.

DNS Bilginizi Doğrulayın

Ağınızdaki bütün bilgisayarların DNS bilgisinin güncel tutulması, güvenliğin artırılmasında yardımcı olabilir. Eğer izinsiz bir bilgisayar ağınıza bağlanırsa, DNS girişinin olmamasından tanyabilirsiniz. Bir çok serviste, sadece geçerli bir DNS girişi olduğunda bağlantıya izin verilmesi şeklinde bir yapılandırma gerçekleştirmek mümkündür.

identd

`identd`,`inetd` sunucunuzun dışında çalışan küçük bir programdır. Hangi kullanıcının hangi TCP servisini çalıştırdığını izler, ve istendiğinde rapor verir.

Bir çok kişi `identd`'nin yararlılığını yanlş anlamakta, dolayısıyla kapatmakta veya site dışı tüm isteklerin önünü kesmektedir. `identd`, uzak sitelere yardım etmek için değildir. Uzak `identd` servisinden alınan verinin doğru olup olmadığını bilmenin bir yolu yoktur. `identd` isteklerinde kimlik doğrulama yoktur.

O zaman neden çalıştırmak isteyebilirsiniz? Çünkü yardım ettiği *sizsinizdir*, ve izlemede diğer bir veri-noktasıdır. Eğer bozulmamışsa, bilirsiniz ki `identd` servisiniz uzak sitelere TCP servisini kullanan kullanıcı ismi ya da kullanıcı kimliğini bildirmektedir. Uzak sitenin sisyönü gelir ve sisteminizdeki kullanıcının sitelerini kırmaya çalıştığını söylerse, kolaylıkla bu kullanıcıya karı tavır alabilirsiniz. `identd`, çalıştırmıyorsanız, çok ama çok fazla günlük dosyasına bakmanız, ve o anda kimin sistemde olduğunu bulmanız gerekir, genelde bu, kullanıcının kim olduğunun belirlenmesini çok daha uzatır.

Çoğu dağıtımla birlikte gelen `identd` , bir çok kişinin tahmin ettiğinden çok daha yaplandırılabilir durumdadır. Belirli kullanıcılar için kapatabilir (bir `.noident` dosyası yaratabilirler), bütün`identd` isteklerinin günlüğünü tutabilir (öneriyoruz), hatta `identd` tarafından döndürülen bilginin kullanıcı ismi yerine kullanıcı kimliği olmasını ya da NO-USER [23] olmasını sağlayabilirsiniz.

Postfix MTA'nın[24] yapılandırılması ve güvenli hale getirilmesi

Postfix posta sunucusu, Postfix ile beraber diğer İnternet güvenlik ürünlerinin yazarı olan Wietse Venema tarafından, yaygın olarak kullanılan Sendmail programına bir alternatif sağlamak amacıyla yazılmıştır. Postfix'in temel hedefi, hızlı, kolay yönetilebilen ve güvenli olması umulan, bunları sağlarken de kullanıcıların rahatı açısından olabildiğince sendmail ile uyumlu bir posta dağıtım aracı olmaktır.

Postfix hakkında daha fazla bilgi için Postfix Ana sayfası ve Postfix'i Yapılandırmak ve Güvenli Hale Getirmek adreslerine göz atmak isteyebilirsiniz.

SATAN, ISS, ve Diğer Ağ Tarayıcıları

Makinelerde veya ağlarda port ve servis tabanlı tarama yapan bir kaç farklı yazılım paketleri mevcut. SATAN, ISS, ve Nessus, iyi bilinenlerden bazıları. Bu yazılımlar hedef makineye bağlanır, ve hangi servisin çalıştığını belirlemeye çalışır. Bu bilgiye dayanarak, makinedeki servislerin bir açığı olup olmadığını söyleyebilirsiniz.

SATAN (Security Administrator's Tool for Analyzing Networks - Ağların Çözümlenmesi İçin Güvenlik Yöneticisi Aracı). Herhangi bir makine veya ağda hafif, orta, veya güçlü kontroller yapmak üzere yapılandırılabilir. SATAN ile makinenizi veya ağınızı tarayarak bulduğu sorunları düzeltmek iyi bir fikirdir. SATAN'ı metalab'dan dan veya bilindik başka bir FTP veya WWW sitesinden aldığınızdan emin olun. Çünkü SATAN'ın İnternet üzerinde dolaşan bir de truva atı kopyası mevcut: http://www.trouble.org/~zen/satan/satan.html. SATAN oldukça uzun bir süredir güncellenmiyor ve aşağıdaki diğer bazı araçlar daha çok işe yarayabilir.

ISS (Internet Security Scanner - İnternet Güvenlik Tarayıcı), başka bir port-tabanlı tarayıcıdır. Satan'dan daha hızlıdır, dolayısıyla büyük ağlar için daha uygun olabilir. Bununla birlikte SATAN daha fazla bilgi verme eğilimindedir.

Abacus, bilgisayar-tabanlı güvenlik ve izinsiz giriş belirleme aracıdır. İnternet sayfasında daha fazla bilgi bulabilirsiniz: http://www.psionic.com/abacus/

SAINT, SATAN'ın güncellenmiş bir sürümü. WWW-tabanlı ve SATAN'dan daha çok güncel testlere sahip. Daha fazla bilgi için: http://www.wwdsi.com/~saint

Nessus, ücretsiz bir güvenlik tarayacıdır. GTK çizgesel arabirimi ile kolay kullanıma sahiptir. Ayrıca yeni port-tarayan testler için çok hoş bir eklenti ayar sitemi birlikte tasarlanmıştır. Daha fazla bilgi için: http://www.nessus.org

Port Taramalarını Algılama

SATAN, ISS ve diğer tarayıcı yazılımların yoklamaları durumunda sizi uyaracak bazı araçlar da vardır. Bununla birlkite, eğer tcp_wrappers kullanıyor ve günlük dosyalarınıza düzenli olarak bakıyorsanız, bu tür yoklamaları farketmeniz zor olmaz. En düşük ayarda bile SATAN Red Hat günlüklerinde iz bırakır.

Ayrıca "gizli" port tarayıcıları da vardır. TCP ACK biti 1 olan bir paket (bağlantı kurulurken yapıldığı gibi) büyük olasılıkla paket-süzen bir güvenlik duvarını aşacaktır. *Kurulmuş hiçbir bağlantısı olmayan* bir porttan döndürülen RST paketi, o portta hayat olduğunun bir kanıtı olarak görülebilir. TCP örtü programlarının bunu farkedeceğini sanmıyorum.

Ayrıca, serbest bir IDS (Intrusion Detection System - Saldırı Belirleme Sistemi) olan SNORT'a da bir göz atabilirsiniz. SNORT, ağa yapılan diğer bazı izinsiz girişleri/saldırıları da belirleyebilir: http://www.snort.org

sendmail, qmail and MTA'lar

Sağlayabileceğiniz en önemli servislerden biri posta servisidir. Ne yazık ki, saldırıya en korumasız olanlardan biri de budur. Bunun sebebi basitçe yerine getirmek zorunda olduğu görevlerin sayısı ve bunlar için gereken yetkilerdir.

`sendmail` kullanıyorsanız, güncel sürümlerini takip etmek çok önem taşıyor. `sendmail`'in güvenlik açıkları konusunda çok uzun bir tarihi var. Daima en güncel sürümünü çalıştırdığınızdan http://www.sendmail.org adresine bakarak emin olun.

Unutmayın ki mektup atabilmeniz için sendmail'in çalışıyor olması gerekmiyor. Ev kullanıcı iseniz, sendmail'i bütünüyle kapatabilir, ve posta istemcinizi mektup göndermek amacıyla kullanabilirsiniz. Sendmail başlangıç dosyasındaki "-bd" bayrağını kaldırarak posta için dışarıdan gelen istekleri engellemeniz de mümkün. Diğer bir deyişle, başlangıç dosyanızda sendmail'i aşağıdaki komut ile çalıştırabilirsiniz:

```
# /usr/lib/sendmail -q15m
```

Bu, sendmail'in mektup kuyruğunda bekleyen ve ilk girişimde dağıtılamayan tüm mesajların 15 dakikada bir boşaltmasını sağlar.

Bir çok yönetici sendmail yerine diğer posta dağıtım araçlarını kullanmayı tercih ediyor. Siz de sendmail yerine `qmail` kullanmayı düşünebilirsiniz. `qmail`, temelde güvenlik düşüncesi ile sıfırdan tasarlanmıştır. Hızlı, kararlı, ve güvenlidir. Qmail http://www.qmail.org adresinde bulunabilir.

Qmail ile doğrudan rekabet içinde olan bir başka program da, tcp_wrappers ve diğer güvenlik araçlarının yazarı tarafından yazılmış olan "postfix". Önceki vmailer isimli, ve sponsorluğu IBM tarafından yapılan bu program da sıfırdan güvenlik düşünülerek yazılmış bir posta dağıtım aracı. Postfix hakkında daha fazla bilgiyi http://www.postfix.org adresinden bulabilirsiniz.

Servis Reddi Saldırıları

Bir "Servis Reddi" saldırısı, saldırganın bazı kaynakları aşırı meşgul etmesi yoluyla servisin meşru isteklere cevap verememesini, veya meşru kullanıcıların makineye erişimlerinin reddedilmesini sağlamasıdır.

Servis reddi saldırıları son yıllarda oldukça fazlalaştı. Bazı yeni ve gözde olanları aşağıda listelenmiştir. Unutmayın ki bunlar sadece bir kaç örnek, her geçen gün yenileri ortaya çıkıyor. Daha güncel bilgi için Linux güvenlik ve bugtraq listelerine ve arşivlerine göz atın.

- *SYN Seli* - SSYN seli, bir ağ servis reddi saldırısıdır. TCP bağlantılarının oluşturulma şeklindeki bir boşluktan yararlanır. Yeni Linux çekirdekleri (2.0.30 ve yukarısı) SYN seli saldırılarının insanların makinenize ya da servislerine erişimini reddetmesini engellemek için yapılandırılabilir seçeneklere sahiptir. Uygun çekirdek koruma seçenekleri için *Çekirdek Güvenliği* bölümüne bakın.

- *Pentium "F00F" Böceği* - Yakın zamanda, gerçek bir Intel Pentium işlemcisine gönderilen bazı Assembly programlama dili kodlarınının makineyi yeniden başlatabileceği keşfedildi. Bu, çalışan işletim sisteminin ne olduğu farketmeksizin, Pentium işlemcili (Pentium Pro, Pentium III, veya Pentium benzeri işlemciler değil) her makineyi etkiliyor. Linux çekirdeklerinin 2.0.32 ve yukarısı sürümlerinde bu böceğin makineyi kilitlemesini engelleyen bir önlem mevcut. Kernel 2.0.33, bu çekirdek çözümünün gelişmiş bir

sürümünü içeriyor, 2.0.32'ye tercih edilmesi önerilir. Eğer Pentium işlemci üzerinde çalışıyorsanız, hemen güncellemelisiniz!

- *Ping Seli* - Ping seli, basit bir kaba-kuvvet servis reddi saldırısı. Saldırgan makinenize ICMP paketlerinden oluşan bir "sel" gönderir. Eğer bunu bant genişliği sizinkinden daha iyi olan bir bilgisayardan yapıyorsa, makineniz ağ üzerine hiçbir şey yollayamaz hale gelecektir. Bu saldırının bir değişik şekli, "şirince", dönüş adresi *sizin* makinenizin IP adresi olan ICMP paketleri gönderir, böylelikle yollanan sel baskınının kimin tarafından olduğunun belirlenmesi de güçleşir. "Şirin" saldırısı ile ilgili daha fazla bilgiyi http://www.quadrunner.com/~chuegen/smurf.txt adresinde bulabilirsiniz.[25]

  Eğer bir ping seli saldırısına maruz kalırsanız, paketlerin nerden geldiğini (ya da nerden geliyor gibi göründüğünü) belirlemek için `tcpdump` gibi bir araç kullanın, ve servis sağlayıcınızla bu bilgi ile birlikte iletişim kurun. Ping selleri, en kolay şekilde yöneltici düzeyinde veya bir güvenlik duvarı kullanarak durdurulabilir.

- *Ölüm Pingi* - Ölüm pingi saldırısı, çekirdekte bulunan, ICMP ECHO REQUEST paketlerini tutmakla görevli veri yapısına uymayacak kadar büyük bir paket gönderir. Tek ve büyük bir paket (65,510 bayt) göndererek çoğu sistemin kilitlenmesine, hatta göçmesine yol açan bu sorun kısa zamanda "Ölüm Pingi" olarak adlandırılmıştır. Bu sorun çok uzun süre önce çözülmüştür, ve artık endişelenecek bir şey yoktur.

- *Gözyaşı / Yeni Gözyaşı* - En yeni açıklardan birisi, Linux ve Windows platformlarındaki IP parçalama kodunda bulunan bir böcektir. Çekirdek 2.0.33 sürümünde onarılmış, ve onarımdan yararlanmak için herhangi bir çekirdek derleme-zamanı seçeneğini seçmeye gerek yoktur. "Yeni Gözyaşı" açığına karşı ise, Linux'ta görünüşte böyle bir tehlike yoktur.

Açıklardan yararlanan kodları, ve nasıl çalıştıkları konusundaki detaylı açıklamaları http://www.rootshell.com adresinde, arama motorunu kullanarak bulabilirsiniz.

NFS (Ağ Dosya Sistemi) Güvenliği

NFS, yaygın olarak kullanılan bir paylaşım protokolüdür. `nfsd` ve `mountd` çalıştıran sunucuların dosya sistemlerinin tamamının, çekirdeklerinde NFS dosya sistemi desteği bulunan (veya Linux makine değilse diğer istemci desteği bulunan) diğer makinelere ihraç edilmesini sağlar. `mountd`, `/etc/mtab` dosyasındaki bağlanmış dosya sistemlerini takip eder, ve `showmount` komut ile bunları görüntüler.

Çoğu site NFS'i kullanıcılara ev dizinleri vermek için kullanır, böylelikle bilgisayar demetindeki hangi makineye giriş yaparlarsa yapsınlar, evlerindeki dosyalara ulaşabilirler.

Dosya sistemlerinin dışa açılmasında küçük bir miktar güvenliğe izin verilir. `nfsd`sunucunuzun uzak root kullanıcısını (uid=0) `nobody` kullanıcısına karşılık getirmesini, böylelikle dışa açılan tüm dosyalara erişiminin reddedilmesini sağlayabilirsiniz. Bununla birlikte, bireysel kullanıcılar kendi dosyalarına (en azından uid'si aynı olanlara) erişebileceği için uzak root kullanıcısı, kullanıcıların hesaplarına giriş veya `su` yaparak onların dosyalarına erişebilir. Bu, dışa açtığınız dosya sistemlerini bağlayabilen bir saldırgan için sadece küçük bir engeldir.

Eğer kaçınılmaz şekilde NFS kullanmanız gerekiyorsa, dosya sistemlerini gerçekten sadece gereken makinelere açtığınıza emin olun. Asla kök dizininizin tamamını dışa açmayın; sadece gereken dizinleri açın.

NFS hakkında daha fazla bilgi için, http://metalab.unc.edu/mdw/HOWTO/NFS-HOWTO.htmladresindeki NFS NASIL belgesine bakabilirsiniz.

NIS (Ağ Bilgi Servisi) (Önceki Sarı Sayfalar, YP).

Ağ Bilgi Servisi (YP), bir makineler grubu arasında bilginin dağıtılması için bir yoldur. NIS sunucusu bilgi tablolarını tutar ve onları NIS harita dosyalarına çevirir. Bu haritalar daha sonra

ağ üzerinde NIS istemci makinelerinin giriş, parola, ve ev dizinleri ile kabuk bilgilerinin (hepsi standart bir `/etc/passwd` dosyasındadır) alınmasına hizmet eder. Bu, kullanıcının bir makinede parolasını değitirdiğinde diğer bütün NIS alanındaki makinelerde de bu değişikliğin geçerli olmasını sağlar.

NIS kesinlikle gvenli değildir. Hiç bir zaman olması düşünülmemiştir. Kolay kullanılır ve yararlı olması amacı güdülmüştür. NIS alanınızın adını tahmin edebilen (İnternette herhangi bir yerdeki) herkes `/etc/passwd` dosyasınızın bir kopyasını alabilir, ve "Crack" ve "John the Ripper" programlarını kullanıcılarınızın parolaları üzerinde kullanabilir. Ayrıca, NIS'i taklit etmek ve her çeşit yaramaz numaralar yapmak mümkündür. Eğer NIS'i kullanmak zorundaysanız, tehlikelerinin de farkında olduğunuzdan emin olun.

NIS'in yerine geçen çok daha güvenli bir program vardır: NIS+ Daha fazla bilgi için NIS HOWTO (NIS NASIL)belgesine bir göz atın: http://metalab.unc.edu/mdw/HOWTO/NIS-HOWTO.html

Güvenlik Duvarı

Güvenlik duvarı, yerel ağınızın içine giren ve dışına çıkan bilgiyi denetim altında tutmanın bir yoludur. Tipik bir güvenlik duvarı, İnternete ve yerel ağınıza bağlanmış durumdadır, ve yerel ağınızdan İnternete tek çıkış yolu güvenlik duvarının içinden geçmektir. Bu yolla güvenlik duvarı yerel ağdan İnternete ya da İnternetten yerel ağa nelerin geçtiğini denetleyebilir.

Bir kaç güvenlik duvarı ve kurma yöntemi vardır. Linux makinelerden oldukça iyi güvenlik duvarı olur. Güvenlik duvarı kodu, 2.0 ve daha yukarı sürüm çekirdeğin içine tümleşik olabilir. Kullanıcı araçları, 2.0 çekirdek için `ipfwadm` , ve 2.2 çekirdek için `ipchains`, [26] izin verdiğiniz ağ trafiği tiplerini çalışma kesilmeksizin değiştirebilmenizi sağlarlar.

Güvenlik duvarları, ağınızı güvenli hale getirmede çok yararlı ve önemli bir tekniktir. Bununla birlikte, bir güvenlik duvarınız varsa, arkasındaki makinelerin güvenliğini sağlamak gerekmediğini asla düşünmeyin. Bu ölümcül bir hatadır. Güvenlik duvarları ve Linux hakkında daha fazla bilgi için metalab arşivindeki http://metalab.unc.edu/mdw/HOWTO/Firewall-HOWTO.html belgesine bir göz atın.

Daha fazla bilgi için IP-Maskeleme mini-nasıl belgesine de göz atabilirsiniz: http://metalab.unc.edu/mdw/HOWTO/mini/IP-Masquerade.html

`ipfwadm` hakkında daha fazla bilgiyi (güvenlik duvarınızın ayarlarını yapabileceğiniz bir araç) http://www.xos.nl/linux/ipfwadm/

Eğer güvenlik duvarları ile daha önce hiç tecrübeniz yoksa, ve basit bir güvenlik politikasından daha fazlası için kurmayı planlıyorsanız, "O'Reilly and Associates"in "the Firewalls (Güvenlik duvarları)" kitabını, ya da İnternette bulunan diğer belgeleri okumanız şarttır. Daha fazla bilgi için http://www.ora.com adresine bir göz atın. NIST (The National Institute of Standards and Technology - Ulusal Standard ve Teknoloji Enstitüsü), güvenlik duvarları üzerine harika bir belge hazırlamıştır. 1995 tarihli olmasına rağmen, hala iyidir. Bu belgeyi http://csrc.nist.gov/nistpubs/800-10/main.html adresinde bulabilirsiniz. Ayrıca ilgili olarak:

- The Freefire Project (Serbest Ateş Projesi) -- Serbest güvenlik duvarı araçlarının bir listesi: http://sites.inka.de/sites/lina/freefire-l/index_en.html

- SunWorld Güvenlik duvarı Tasarımı -- O'Reilly kitabının yazarları tarafından hazırlanan bu belge farklı güvenlik duvarı tipleriyle ilgili başlangıç düzeyinde bilgi niteliğini taşıyor: http://www.sunworld.com/swol-01-1996/swol-01-firewall.html

- Mason - Linux için otomatik güvenlik duvarı oluşturucusu. Bu, ağınızda yapmanız gereken şeyleri siz yaptıkça öğrenen bir güvenlik duvarı betiğidir. Daha fazla bilgi: http://www.pobox.com/~wstearns/mason/

IP Chains - Linux 2.2.x Çekirdek Güvenlik duvarı

Linux IPChains, Linux 2.0 güvenlik duvarı sisteminin 2.2 çekirdek için güncellenmiş halidir. Önceki uygulamadan çok daha fazla özelliği vardır, bunların arasında:

- Daha esnek paket yönetimi
- Daha karmaşık muhasebe
- Basit politika değişikliklerinin otomatik olarak değiştirilebilmesi
- Parçaların açıkça engellenebilmesi, reddedilebilmesi vb.
- Şüpheli paketlerin günlüğünün tutulması
- ICMP/TCP/UDP dışındaki diğer protokolleri de idare edebilmesi.

sayılabilir.

Şu anda 2.0 çekirdeğinizde`ipfwadm` kullanıyorsanız, `ipfwadm` komut biçimini `ipchains`'de kullanılabilecek biçime dönüştüren betikler mevcuttur.

Daha fazla bilgi için IP Chains NASIL belgesini okuduğunuzdan emin olun: http://www.adelaide.net.au/~rustcorp/ipfwchains/ipfwchains.html

Netfilter - Linux 2.4.x Çekirdek Güvenlik duvarı

Çekirdek IP paket süzüm kodu için bir başka gelişme de, netfilter programı tarafından kullanıcıların 2.4 çekirdeğinde paket süzümünün kurulum, bakım ve denetleme işlemlerini yapabilmesine olanak sağlanmasıdır.

Netfilter alt sistemi ipchains ve ipfwadm dahil olmak üzere tüm paket süzüm uygulamalarının yeniden yazılmış halidir. Netfilter çok sayıda geliştirilmiş özellik sunar, ve geniş şirket ağlarını korumada artık daha olgun ve kararlı bir çözüm olmuş durumdadır.

```
iptables
```

komutunu kullanarak çekirdek içindeki güvenlik duvarı tablolarını yönetebilirsiniz.

Netfilter, paketleri çekirdeğin çeşitli bölümlerinden geçerken yönetmenize olanak sağlayan ham bir çalışma ortamı sağlar. Bu çalışma ortamınının bir bölümü maskeleme, standart paket süzümü, ve ağ adres çevirisi için destek sağlar. Netfilter, aynı zamanda güvenlik duvarının arkasındaki bir grup sunucuda çalışan hizmet programlarına yönelik yapılan yük dengeleme istekleri için bile daha gelişmiş bir desteğe sahiptir.

Durum denetleme özellikleri gerçekten çok yararlı. Durum denetleme özelliği süzeçten geçen iletişim akışının izlenmesi ve denetlenmesine olanak tanır. Oturum hakkında durum ve bağlam bilgisinin izlenebilmesi kural koyma işlemini basitleştirir ve daha yüksek düzeydeki protokollerin yorumlamaya çalışır.

Ayrıca, paketlerin kullanıcı uzayındaki programlara geçirilip ilendikten sonra tekrar paket akışı içine geri döndürülmesi gibi belirli ek işlevleri yerine getirmek üzere küçük modüller geliştirilebilir. Bu programların kullanıcı uzayında geliştirilebilmesi, daha önceki bir zorunluluk olan çekirdek düzeyindeki değişikliğin yol açtığı karmaşıklığın azaltılmasını sağlar.

Diğer IP Tables referansları arasında:

- *Oskar Andreasson IP Tables Dersi* -- Oskar Andreasson, LinuxSecurity.com ile giriş düzeyinde IP Tables dersinin sağlam bir güvenlik duvarı oluşturmak için nasıl kullanılabileceği hakkında konuşuyor.

- *Hal Burgiss Introduces Linux Güvenliği Hızlı-Başlama Rehberleri* -- Hal Burgiss, Linux'un güvenliğini sağlama üzerine güvenlik duvarlarının yönetimini de içine alan iki yetkin rehber yazmış durumda.

- *Netfilter Ana Sayfası* -- Netfilter/iptables ana sayfası.

- *2.4 Linux Çekirdeği Güvenlik duvarı olgunlaşıyor: netfilter* -- Bu LinuxSecurity.com makalesinde paket süzümünün temelleri, iptables kullanarak işe nasıl başlanabileceği, ve Linux için yeni nesil güvenlik duvarlarında ne gibi yeni özelliklerin bulunduğu açıklanıyor.

VPN'ler - Sanal Özel Ağlar

VPN'ler, var olan bir ağın üstüne "sanal" bir ağ kurmanın bir yoludur. Bu sanal ağ, bazı durumlarda şifreli olup, sadece ağa katılmış olan ve kim olduğu bilinen bilgisayarlar arasındaki trafiğe izin verir. VPN'ler, çoğunlukla evde çalışan birini, herkese açık İnternet üzerinden dahili bir şirket ağına bağlamak için kullanılır.

Eğer bir Linux maskeleme güvenlik duvarınız varsa ve MS PPTP paketleri (Microsoft'un VPN noktadan-noktaya ürünü) geçirmeniz gerekiyorsa, bunu yapabilmeniz için gereken bir çekirdek yaması mevcut: ip-masq-vpn.

Linux'taki VPN çözümlerinden bir kaçı:

- vpnd. Bkz. http://sunsite.dk/vpnd/.

- Free S/Wan, http://www.xs4all.nl/~freeswan/

- ssh, bir VPN oluşturmak için kullanılabilir. Daha fazla bilgi için VPN mini-nasıl belgesine bakın.

- vps (sanal özel sunucu): http://www.strongcrypto.com.

- yawipin http://yavipin.sourceforge.net

Daha fazla bilgi ve referans için IPSEC ile ilgili bölüme de bakın.

Güvenlik Hazırlığı (Bağlanmadan Önce)

Tamam, sisteminizi gözden geçirdiniz, ve olabildiğince güvenli olduğunu belirlediniz, ve bağlanmaya hazırsınız. Sisteminize yapılacak olası izinsiz giriş durumunda, giren kişiyi çabucak etkisiz hale getirerek sisteminizi tekrar çalışır duruma döndürebilmek için şimdi yapmanız gereken bir kaç hazırlık var.

Makinenizin Tam Yedeğini Alın

Yedekleme yöntemleri ve depolama hakkında bir tartışma bu belgenin konusu ötesinde, ama yedekleme ve güvenlik ile ilgili bir kaç söz söylenebilir:

Eğer bir sabit disk bölümünde 650 MB veriden daha azı varsa, verinizi CD-R üzerine kopyalamak iyi bir yoldur (daha sonra kurcalanması da zordur, hem uygun şekilde saklanırsa uzun süreli bir ömrü vardır). Manyetik bant ve diğer yeniden-yazılabilir ortamlar, yedekleme tamamlanır tamamlanmaz yazmaya karşı korunmalı, ve değiştirilmenin engellenmesi için doğrulanmalıdır. Yedeklerinizi, güvenli ve bağlı olmayan bir alanda sakladığınızdan emin olun. İyi bir yedeğin

anlamı, sistemi iyi bir noktadan tekrar yerine koyabilir olmanızdır.

İyi Bir Yedekleme Çizelgesi Seçimi

A six-tape cycle is easy to maintain. This includes four tapes for during the week, one tape for even Fridays, and one tape for odd Fridays. Perform an incremental backup every day, and a full backup on the appropriate Friday tape. If you make some particularly important changes or add some important data to your system, a full backup might well be in order.

Yedeklerizinin Denenmesi

6-bantlık bir dönüşümün bakımı kolaydır. 4 bant hafta içi, 1 bant çift Cumalar için, bir bant da tek Cumalar için olabilir. Her gün bir artımlı yedekleme uygulayın, ve uygun Cuma bandında tam yedek alın. Sisteminizde özellikle önemli değişiklikler yapar veya bazı önemli veri eklemesi yaparsanız da tam yedek almak iyi olabilir..

RPM ve Debian Dosya Veritabanınızı Yedekleyin

Bir izinsiz giriş durumunda, RPM veritabanınızı, aynı `tripwire`, gibi kullanabilirsiniz, veritabanının da değiştirilmediğinden emin olmanız durumunda elbette. RPM veritabanınızı bir diskete kopyalamalı, ve daima bağlantısız şekilde tutmalısınız. Debian dağıtımında da benzer bir şeyler olması muhtemeldir.

The files `/var/lib/rpm/fileindex.rpm` ve `/var/lib/rpm/packages.rpm` mdosyaları büyük olasılıkla tek bir diskete sığmayacaktır, fakat sıkıştırılırlarsa, her biri bir diskete sığabilir.

Şimdi, sisteminizin güvenliği ihlal edildiğinde,

```
root#  rpm -Va
```

komutunu, sistem üzerindeki her bir dosyayı doğrulamak amacıyla kullanabilirsiniz. `rpm` man sayfasına bir bakın, bir kaç diğer seçenek sayesinde bu işlemi daha az şey söyleyerek yapmasını sağlayabilirsiniz. Unutmayın ki bunu yaparken RPM programınızın da bozulmadığından emin olmalısınız.

Bunun anlamı, sisteminize her yeni RPM eklendiğinde, RPM veritabanının da yeniden arşivlenmesi gerekecek. Getirileri ve götürüleri karşılaştıracak ve karar verecek olan sizsiniz..

Sistem Hesap Verilerinizi Takip Edin

`syslog` 'dan gelen bilginin bozulmaması çok önemlidir. `/var/log` altındaki dosyaların sadece sınırlı sayıda kullanıcı tarafından okunabilmesi ve yazılabilmesi iyi bir başlangıçtır.

Gözünüz orda yazılı olanlar, özellikle `auth` kısmındakiler üstünde olsun. Örneğin birden çok giriş başarısızlıkları, bir kırma girişiminin göstergesi olabilir.

Günlük dosyanızın nerde olduğu dağıtımınıza bağldr. "Linux Dosya Sistemi Standart"ına uyan bir Linux sisteminde, örneğin Red Hat'te, `/var/log` 'un altına bakabilir, `messages`,`mail.log`, ve diğer dosyaları gözden geçirebilirsiniz.

Kendi dağıtımızın nereye günlük tuttuğunu `/etc/syslog.conf` dosyasına bakarak bulabilirsiniz. Bu dosya `syslogd`'ye (sistem günlük sunucu programı) çeşitli mesajların günlüğünün nerelerde tutulması gerektiğini söyler.

Ayrıca günlükleri başa döndüren betik veya sunucu programı logları daha uzun süre tutması için yapılandırabilirsiniz, böylelikle onları incelemek için daha fazla zamanınız olur. Red Hat dağıtımında `logrotate` paketine bir göz atın. Diğer dağıtımlar da muhtemelen benzer bir işleme sahiptirler.

Günlük dosyalarınız kurcalandıysa, tam olarak ne çeşit şeylerin ne zaman kurcalanmaya başladığını belirlemeye çalışın. Hesap bilgilerine ulaşılamayan geniş zaman aralıkları var mı? Kurcalanmamış günlük dosyaları için yedekleme verinize (eğer varsa) bakmak iyi bir fikirdir.

Sisteme izinsiz girenler, tipik olarak izlerini saklamak için günlük dosyalarını değiştirir, yine de garip olguları belirlemek amacıyla göz atmak gerekir. İzinsiz giren kişinin, root hesabı için giriş kazanmaya çalıştığını, ya da bir programdan yararlandığını belirleyebilirsiniz belki de. Belki de izinsiz giren kişinin, günlük dosyalarını değiştirmeye zaman bulamadığı kısımları görebilirsiniz.

Ayrıca, `su` kullanarak kullanıcı değiştirme girişimleri, sisteme giriş girişimleri, ve diğer kullanıcı hesap bilgileri de dahil olmak üzere tüm `auth` verisini diğer günlük verisinden ayrı tutmalısınız.

Mümkünse `syslog` 'u, verinin bir kopyasını güvenli bir sisteme göndermek üzere yapılandırın. Bu, izinsiz giren kişinin, login/su/ftp/vb girişimlerinin izlerini ortadan kaldırmasını engelleyecektir. `syslog.conf` man sayfasında `@` seçeneğine bir göz atın.

İnternette daha gelişmiş `syslogd` programları da vardır: http://www.core-sdi.com/ssyslog/ adresinde Secure Syslog (Güvenli Syslog) programı mevcuttur. Secure Syslog, syslog verinizi şifreleyebilmenizi ve kimsenin değiştirmediğinden emin olmanızı sağlar.

Daha fazla özellikli bir diğer `syslogd` ise syslog-ng sayfasında yer almaktadır. Günlük tutmada daha fazla esnekliğe sahiptir ve ayrıca uzak syslog akışınızın da değiştirilmesini engeller.

Son olarak, eğer okuyan kimse yoksa günlük dosyalarının da fazla bir yararı yoktur. Arada bir günlük dosyalarınıza bakmak için zaman ayırın, ve olağan bir günde nasıl göründükleri hakkında bir fikir sahibi olun. Bunu bilmek, olağan dışı şeyleri farketmede oldukça yardımcı olacaktır.

Bütün Yeni Sistem Güncellemelerini Uygulayın

Çoğu kullanıcı Linux'u bir CD-ROM'dan kurar. Güvenlik onarımlarının hızlı doğası sebebiyle, sürekli yeni (onarılmış) programlar çıkar. Makinenizi ağa bağlamadan önce, dağıtımınızın ftp sitesine göz atmak ve CD-ROM'dan beri güncellenen tüm paketleri almak iyi bir fikirdir. Çoğu zaman bu paketler önemli güvenlik onarımlarını içerir, dolayısıyla bu güncelleme paketlerini kurmak iyi bir fikirdir..

Güvenlik İhlali Sırasında ve Sonrasında Neler Yapılabilir[27]

Evet, burdaki (veya başka bir yerdeki) önerileri dinlediniz ve bir sistem kırılma durumunu belirlediniz. İlk yapılacak şey, soğukkanlılığı korumaktır. Aceleci davranışlar saldırganın neden olduğundan daha çok zarara yol açabilir.

Güvenlik İhlali Sırasında

Güvenlik ihlalini, olduğu sırada belirlemek ağır bir yükümlülük olabilir. Vereceğiniz tepki büyük sonuçlar doğurabilir.

Gördüğünüz ihlal fiziksel ise, olasılıklar, birinin evinize, ofisinize veya laboratuvarınıza girmiş olabileceğidir. Yerel yetkililere haber vermelisiniz. Bir laboratuvarda, birinin kasayı açmaya veya makineyi yeniden başlatmaya çalıştığını belirlemiş olabilirsiniz. Yetkileriniz ve yordamlarınıza bağlı olarak, engel olmaya çalışabilir veya yerel güvenlik görevlilerinizle iletişime geçebilirsiniz.

Eğer yerel bir kullanıcının güvenliğinizi ihlal ettiğini farkettiyseniz, ilk yapılacak şey, onların

aslında sandığınız kişi olduklarının doğrulanmasıdır. Sisteme nerden giriş yaptıklarını kontrol edin. Olağan durumlarda giriş yaptıkları yer ile aynı mı? Hayır mı? O zaman temasa geçmenin elektronik olmayan bir yolunu kullanın. Örneğin, telefon ile arayın ya da konuşmak için ofislerine/evlerine gidin. Eğer sistemde oldukları konusunda anlaşmaya varabilirseniz, ne yaptıklarını açıklamalarını veya yaptıkları şeye son vermelerini isteyebilirsiniz. Eğer sistemde değillerse, ve ne söylediğiniz hakkında bir fikirleri yoksa, olasılıkla bu olayın daha fazla araştırılması gerekecek. Bu tür olayları iyice araştırın, ve bir suçlama yapmadan önce fazlasıyla bilgi sahibi olun..

Eğer bir ağ güvenliği ihlali belirlediyseniz, ilk yapılacak şey (yapabiliyorsanız), ağınızın bağlantısını kesmektir. Modem ile bağlanıyorlarsa, modem kablosunu çıkarabilir, Ethernet yoluyla bağlanıyorlarsa Ethernet kablosunu çıkarabilirsiniz. Bu onların daha fazla zarar vermesini engelleyecek, ve yakalandıklarından çok bir ağ problemi olduğuna inanmalarına yol açacaktır.

Eğer ağın bağlantısını kesemiyorsanız (yoğun kullanımlı bir siteniz varsa, veya makinelerinizin fiziksel denetimi elinizde değilse), en iyi diğer bir adım, izinsiz giriş yapan kişinin sitesinden erişimi `tcp_wrappers` veya `ipfwadm` kullanarak reddetmektir.

Eğer izinsiz giren kişinin sitesinden erişimi reddedemeyecek durumda iseniz, kullanıcının hesabını kilitlemek zorunda kalabilirsiniz. Unutmayın ki hesabı kilitlemek kolay bir iş değildir. Düşünmeniz gerekenler arasında `.rhosts` dosyaları, FTP erişimi ve olası başka arka kapılar sayılabilir.

Yukarıdakilerden birini yaptıktan sonra (ağın bağlantısını kestiniz, siteden erişimi yasakladınız ve/veya hesaplarını etkisiz hale getirdiniz), yapmanız gereken o kullanıcının çalıştırdığı tüm işlemleri öldürmek ve sistem dışına çıkarmaktır.

Sonraki bir kaç dakika için sitenizi izleyebilirsiniz, çünkü saldırgan tekrar girmeyi deneyecektir. Belki de farklı bir hesap kullanarak ve/veya farklı bir ağ adresinden.

Güvenlik İhlali Sonrasında

Evet, diyelim ki gerçekleşmiş bir güvenlik ihlalini veya bozukluğunu belirlediniz ve saldırganı sisteminiz dışına (umarım) attınız. Sırada ne var?

Açığı kapatmak

Eğer saldırganın sisteminize ne şekilde girdiğini belirleyebildiyseniz, o açığı kapatmayı denemelisiniz. Örneğin, kullanıcı giriş yapmadan önce belki de günlükte bir takım FTP kayıtları gördünüz. FTP servisini kapatıp güncel bir sürümünün olup olmadığına bakabilir, veya listelerde herhangi bir onarım arayabilirsiniz..

Bütün günlük dosyalarınızı gözden geçirin, ve güvenlik liste ve sayfalarınızı bir ziyaret ederek onarabileceğiniz herhangi bir yeni açık olup olmadığını belirleyin. Caldera güvenlik onarımlarını http://www.caldera.com/tech-ref/security/adresinde bulabilirsiniz. Red Hat henüz güvenlik onarımlarını böcek onarımlarından ayırmadı, fakat dağıtım hata düzelten belgeleri http://www.redhat.com/errata adresinden ulaşılabilir durumda.

Debian artık bir güvenlik mektup listesi ve WWW sayfasına sahip. Daha fazla bilgi için: http://www.debian.org/security/ adresine bakın.

Eğer bir dağıtımcı firma bir güvenlik güncellemesi çıkardıysa, diğer çoğu Linux dağıtımcılarının da çıkarması olasılığı çok yüksektir.

Artık bir Linux güvenlik izleme projesi var. Düzenli bir şekilde bütün kullanıcı gereçlerini deniyor ve olası güvenlik açıkları ve taşmalarını araştırıyorlar. Duyurularından:

“"OpenBSD kadar güvenli olabilme bakış açısıyla bütün Linux kaynaklarını sistemli bir şekilde izleme girişimimiz var. Bazı problemleri belirlemiş (ve onarmış) durumdayız, fakat daha fazla yardıma da açığız. Liste kısıtlı bir liste değil ve aynı zamanda genel güvenlik

tartışmaları için de yararlı bir kaynak. Liste adresi: security-audit@ferret.lmh.ox.ac.uk. Abone olmak için security-audit-subscribe@ferret.lmh.ox.ac.uk adresine bir mektup gönderin"”

Saldırganın girişini kilitleyerek engellemezseniz, muhtemelen geri gelecektir. Dönüşü sadece sizin makinenize değil, ağınızdaki herhangi bir yere olabilir. Eğer bir paket koklayıcı çalıştırıyorduysa, diğer makinelere erişim sağlamış olmaları da muhtemeldir.

Hasar Tespiti

Yapılacak ilk iş hasarın tespit edilmesidir. Tam olarak bozulan nedir? `Tripwire`gibi bir bütünlük inceleyici çalıştırıyorsanız, bir bütünlük taraması için kullanabilirsiniz; neyin bozulduğunu bulmanıza yardımcı olacaktır. Kullanmıyorsanız, tüm önemli verinizi kendiniz incelemek zorunda olacaksınız.

Linux sistemlerinin gün geçtikçe daha kolay kuruluyor olması nedeniyle, yapılandırma dosyalarınızı saklamayı, disklerinizi temizleyip, yeniden kurmayı, sonra da kullanıcı ve yapılandırma dosyalarınızı yedeklerden yerine koymayı düşünebilirsiniz. Bu yeni ve temiz bir sisteme sahip olduğunuzdan emin olmanızı sağlayacaktır. Eğer bozuk sistemden bazı dosyalar almak durumunda kalırsanız, çalıştırılabilir dosyalar konusunda özellikle dikkatli olun, çünkü izinsiz giriş yapan kişi tarafından konulmuş truva atları olabilir.

İzinsiz giren kişinin root erişimi sağlaması durumunda yeniden kurulum zorunlu olarak düşünülmelidir. Ek olarak, var olan kanıtları saklamak isteyebilirsiniz, dolayısıyla yedek bir disk bulundurmak mantıklıdır.

Düşünmeniz gereken bir diğer konu da güvenlik ihlalinin ne kadar zaman önce gerçekleştiği, ve yedeklerdeki bilgilerin hasarlı çalışmaları içerip içermediğidir. Şimdi yedekler konusu.

Yedekler, Yedekler, Yedekler!

Düzenli yedekleme, güvenlik konularında bir nimettir. Sisteminizin güvenliği ihlal edildiyse, gereken veriyi yedeklerden yerine koyabilirsiniz. Elbette, bazı veri saldırgan için de değerlidir, sadece yok etmek değil, bilgiyi çalma ve kendi kopyalarını oluşturma eylemlerini de gerçekleştirebilirler. Ama en azından verinin bir kopyasını elinizde bulundurmuş olursunuz..

Kurcalanan bir dosyayı yerine koymadan önce, bir kaç yedek öncesine de bakmalısınız. Saldırgan dosyalarınızı uzun süre önce bozmuş olabilir ve bozulan dosyaların yedeğini almış olabilirsiniz!

Elbette, yedeklerle ilgili bir takım güvenlik konuları da vardır. Yedeklerinizi güvenli bir yerde sakladığınızdan emin olun. Kimlerin erişimi olduğunu bilin (Eğer bir saldırgan yedeklerinize ulaşırsa, haberiniz bile olmadan tüm verinize ulaşabilir).

Saldırganı İzleme

Tamam, saldırganı dışarı attınız, ve sisteminizi iyileştirdiniz, ama işiniz henüz bitmiş sayılmaz. Çoğu saldırganın yakalanma olasılığı düşük olmakla birlikte, saldırıyı rapor etmeliniz.

Saldırıyı, saldırganın sitesindeki yöneticilere bildirmelisiniz. Bu yönetici bilgisine `whois` komutuyla ya da Internic veritabanından ulaşabilirsiniz. Onlara bütün uygun günlük satırlarıyla tarih ve saat bilgilerini içeren bir e-mektup atabilirsiniz. Saldırgan hakkında ayırt edici başka herhangi bir şey de belirlediyseniz, bunu da onlara bildirin. Mektubu gönderdikten sonra (dilerseniz) bir telefon konuşması da yapabilirsiniz. Eğer o yönetici sizin saldırganınızı belirlerse, o siteye giriş yaptığı diğer sitenin yöneticisiyle konuşabilir, ve bu şekilde sürer.

İyi korsanlar, arada pek çok site kullanırlar, bunlardan bazıları (veya çoğu) güvenliklerinin ihlal edildiğinden dahi habersizdirler. Bir korsanı ev sistemine kadar izlemeyi denemek zor bir iş olabilir. Konuştuğunuz sitelerin yöneticilerine karşı nazik olmak, yardım alma konusunda oldukça yol almanızı sağlayabilir.

Ayrıca, Linux sistem dağıtıcınızı olduğu kadar, bir parçası olduğunuz (CERT ve benzeri), güvenlik örgütlerini de bu konuda uyarmalısınız.

Güvenlikle İlgili Kaynaklar

Genel olarak Unix güvenliği, ve özel olarak da Linux güvenliği ile ilgili ÇOK SAYIDA iyi site vardır. Bir (veya daha fazla) güvenlik mektup listelerine abone olmak ve güvenlik onarımları hakkında güncel bilgiye sahip olmak önemlidir. Bunların çoğu çok yoğun olmayan ve çok bilgilendirici listeler.

LinuxSecurity.com Atıfları

The LinuxSecurity.com WWW sitesinde, LinuxSecurity personeli ve dünyanın çeşitli bölgelerinden insanları tarafından hazırlanmış çok sayıda açık kaynak güvenlik referanslarını bulabilirsiniz.

- *Linux Tavsiye İzleme* -- Hafta boyunca duyrulan güvenlik zayıflıklarının taslaklarını içeren haberler. Her bir zayıflığın betimlemesi ve güncellenen paketlere linkleri de içeriyor.
- *Haftalık Linux Güvenliği* -- Bu belgenin amacı, her hafta okuyuculara en önemli Linux güvenlik başlıklarının bir özetini sunmak.
- *Linux Güvenliği Tartışma Listesi* -- Bu mektup listesi, genel güvenlik soruları ve yorumları için.
- *Linux Güvenlik Haberleri* -- Tüm haberler için abonelik bilgisi.
- *comp.os.linux.security SSS* -- comp.os.linux.security haber grubu için yanıtlarıyla birlikte Sıkça Sorulan Sorular.
- *Linux Güvenlik Belgeleri* -- Linux ve Açık Kaynak Güvenlik için harika bir başlangıç noktası.

FTP Siteleri

CERT (Computer Emergency Response Team) Bilgisayar Acil Durum Yanıt Takımı'dır. Çoğunlukla güncel saldırı ve onarımlar hakkında uyarılarda bulunurlar. Daha fazla bilgi için ftp://ftp.cert.org adresine bakabilirsiniz.

ZZEDZ (önceki Replay) (http://www.zedz.net) arşivi bir çok güvenlikle ilgili program bulundurur. ABD'nin dışında oldukları için ABD şifre kısıtlamalarına uymaları da gerekmiyor.

Matt Blaze CFS'nin yazarı ve mükemmel bir güvenlik danışmanı. Matt'in arşivi ftp://ftp.research.att.com/pub/mab adresinde bulunabilir.

`tue.nl` Hollanda'da bulunan büyük bir güvenlik FTP sitesi: ftp.win.tue.nl

WWW Siteleri

- The Hacker FAQ, Bilgisayar kurtları hakkında bir SSS: The Hacker FAQ

- COAST arşivi çok sayıda Unix güvenlik program ve bilgisini bulunduruyor: COAST
- SuSe Güvenlik Sayfası: http://www.suse.de/security/
- Rootshell.com, korsanlar tarafından kullanılan güncel açıkların neler olduğunu görmek için harika bir site: http://www.rootshell.com/
- BUGTRAQ, güvenlik konularında tavsiyeler veren bir site: BUGTRAQ archives
- CERT, Bilgisayar Acil Durum Yanıt Takımı, Unix ile ilgili yaygın saldırılar konusunda tavsiyeler veriyor: CERT home
- Dan Farmer, SATAN'ın ve diğer bir çok güvenlik aracının yazarı. Ev sitesinde ilginç bazı araştırma bilgileri, ve diğer güvenlik araçları var: http://www.trouble.org
- The Linux security WWW (Linux Güvenlik WWW Sayfası), Linux güvenliği ile ilgili bilgiler için iyi bir site: Linux Security WWW
- Infilsec, hangi platformun hangi açıklara karşı korunmasız olduğunu söyleyecek bir motora sahip: http://www.infilsec.com/vulnerabilities/
- CIAC, yaygın açıklar konusunda düzenli güvenlik bültenleri yayımlıyor: http://ciac.llnl.gov/cgi-bin/index/bulletins
- Linux PAM için iyi bir başlangıç noktası: http://www.kernel.org/pub/linux/libs/pam/.
- Debian projesi, güvenlik onarımları ve bilgi için bir WWW sayfasına sahip: http://www.debian.com/security/.
- Lincoln Stein tarafından yazılan WWW Security FAQ (WWW Güvenlik SSS), harika bir WWW güvenliği referansı: http://www.w3.org/Security/Faq/www-security-faq.html

Mektup Listeleri

Bugtraq: Abone olmak için, listserv@netscape.org adresine, gövde kısmında subscribe bugtraq yazan bir mektup atın (arşivler için aşağıdaki linklere bakın)

CIAC: majordomo@tholia.llnl.gov adresine mektup atın. Mesajın GÖVDE kısmında (Subject, yani Konu kısmında değil) şunlar bulunmalı: subscribe ciac-bulletin

Red Hat'te de bir takım mektup listeleri var, en önemlisi redhat-announce (redhat-duyuru listesi). Güvenlik (ve diğer şeylerin) onarımları hakkında, çıktıkları anda haber alabilirsiniz. redhat-announce-list-request@redhat.com adresine, Konu kısmında Subscribe yazılı olan bir mektup atın. Daha fazla bilgi ve arşivler için https://listman.redhat.com/mailman/listinfo/ adresine bir göz atın.

Debian, güvenlik onarımlarını kapsayan bir mektup listesine sahip: http://www.debian.com/security/

Kitaplar - Basılı Eserler

Güvenlikle ilgili bir çok iyi kitap da mevcut. Bu bölümde bir kaç tanesini sıralayacağız. Güvenlikle ilgili kitaplara ek olarak, sistem yönetiminin anlatıldığı ve güvenlik konusunda da bilgilerin yer aldığı kitaplar mevcut.[28]

- Building Internet Firewalls By D. Brent Chapman & Elizabeth D. Zwicky, 1st Edition

September 1995, ISBN: 1-56592-124-0

- Practical UNIX & Internet Security, 2nd Edition By Simson Garfinkel & Gene Spafford, 2nd Edition April 1996, ISBN: 1-56592-148-8
- Computer Security Basics By Deborah Russell & G.T. Gangemi, Sr., 1st Edition July 1991, ISBN: 0-937175-71-4
- Linux Network Administrator's Guide By Olaf Kirch, 1st Edition January 1995, ISBN: 1-56592-087-2
- PGP: Pretty Good Privacy By Simson Garfinkel, 1st Edition December 1994, ISBN: 1-56592-098-8
- Computer Crime A Crimefighter's Handbook By David Icove, Karl Seger & William VonStorch (Consulting Editor Eugene H. Spafford), 1st Edition August 1995, ISBN: 1-56592-086-4
- Linux Security By John S. Flowers, New Riders; ISBN: 0735700354, March 1999
- Maximum Linux Security : A Hacker's Guide to Protecting Your Linux Server and Network, Anonymous, Paperback - 829 pages, Sams; ISBN: 0672313413, July 1999
- Intrusion Detection By Terry Escamilla, Paperback - 416 pages (September 1998), John Wiley and Sons; ISBN: 0471290009
- Fighting Computer Crime, Donn Parker, Paperback - 526 pages (September 1998), John Wiley and Sons; ISBN: 0471163783

Sözlük

Aşağıda bilgisayar güvenliği ile ilgili en sık kullanılan terimleri bulacaksınız. Daha geniş bir sözlüğe LinuxSecurity.com Sözlüğü'nden erişebilirsiniz.[29]

- *authentication (kimlik doğrulama):* Verinin, asıl gönderilen veri olduğunu, ve veriyi göndermiş gibi görünen kişinin, gerçekten gönderen kişi olduğunun bilinmesi.
- *bastion host (sur bilgisayar):* İnternete açık ve içerdeki kullanıcılar için ana bir iletişim noktası olduğundan dolayı saldırılara uğrama tehlikesinin çok fazla oluşu nedeniyle yüksek derecede güvenli hale getirilmesi gereken bilgisayar sistemi. İsmi, ortaçağ kalelerinin dış duvarlarındaki yüksek derecede güçlendirilmiş yapılardan gelmektedir. Kale surları, savunmada kritik alanlara yukarıdan bakan, genelde güçlü duvarlı, fazladan asker için geniş alanlı, saldırganlara kızgın yağın dökülerek uzaklaştırıldığı yerlerdir.
- *buffer overflow (tampon taşması):* Yaygın programlama tarzında, asla yeteri büyüklükte tamponlar ayrılmaz, ve taşmaların olup olmadığı gözden geçirilmez. Bu tür taşmalar olduğunda, çalışan program (sunucu program ya da suid program) başka şeyler yapmak üzere kandırılabilir. Genelde bu, fonksiyonun yığındaki dönüş adresini değiştirerek başka bir yere yönlendirme yoluyla yapılır.
- *denial of service (servis reddi):* Bilgisayarınızın, yapmasını düşünmediğiniz şeylerle fazlaca meşgul olup kaynaklarının saldırgan tarafından tüketilmesi yoluyla, meşru kullanıcılar için ayrılmış ağ kaynaklarının olağan kullanımının engellenmesi.[30]
- *dual-homed host (çift evli bilgisayar):* En az iki ağ arabirimi bulunan genel amaçlı bilgisayar sistemi.

- *firewall (güvenlik duvarı):* İnternet ve korunan bir ağ arasında, ya da diğer ağ kümeleri arasında, erişimi kısıtlayan bileşen, veya bileşenler kümesi.

- *host (bilgisayar):* Ağa dahil olmuş bir bilgisayar sistemi.

- *IP spoofing (IP taklidi):* IP taklidi, bir takım bileşenlerden oluşan karmaşık teknikli bir saldırıdır. Bilgisayarlara, olmadığınız bir kişi gibi görünerek güvenlerini kazanmanıza yol açan bir güvenlik açıdır. Bu konuda "Phrack Magazine", 7. Cilt, 48. Konuda, daemon9, route, ve infinity tarafından yazılmış kapsamlı bir makale vardır.[31]

- *non-repudiation (inkar edememe):* Bir alıcının, bir veriyi göndermiş gibi görünen kişinin gerçekten veriyi gönderen kişi olduğunu, gönderen kişi daha sonra inkar etmeye kalksa dahi kanıtlayabilmesi[32]

- *packet (paket):* İnternet üzerindeki haberleşmenin temel birimi.

- *packet filtering (paket süzme):* Bir ağdaki içe ve dışa olan veri akışının bir cihaz tarafından seçici olarak gerçekleştirilmesi davranışı. Paket süzgeçleri, genelde bir ağdan bir başkasına yöneltme yaparken paketlerin geçişine izin verir veya engel olur (çoğunlukla İnternet'ten içerideki ağa, veya tam tersi). Paket süzgecinin başarılı olması için, hangi paketlere (IP adreslerine ve portlarına göre) izin verileceğine ve hangilerine engel olunacağına karar veren kuralları belirlemeniz gerekir.

- *perimeter network (çevre ağ):* Ek bir güvenlik katmanı oluşturabilmek amacıyla korunan bir ağ ile dışardaki bir ağ arasına eklenen ağ. Çevre ağ bazen DMZ olarak da adlandırılır.

- *proxy server (vekil sunucu):* İçerdeki istemcilerin adına dışarıdaki sunucularla iletişim kuran bir program. Vekil istemciler, vekil sunucuya konuşur, vekil sunucular onaylanmış istemcilerin isteklerini gerçek sunucuya nakleder, gelen cevapları da tekrar istemcilere nakleder.

- *superuser (üstün kullanıcı):* `root`'un resmi olmayan isimlerinden biri.

Sıkça Sorulan Sorular

1. Sürücü desteğini doğrudan çekirdeğe tümleşik olarak derlemek, modül olarak derlemekten daha mı güvenlidir?

   Yanıt: Bazı insanlar, cihaz sürücülerini modüller yoluyla yüklenememesinin daha iyi olacağını düşünürler, çünkü sisteme izinsiz giren biri, bir Truva atı ya da sistem güvenliğini etkileyebilecek bir modül yerleştirebilir.

   Bununla birlikte, modülleri yükleyebilmek için root olmanız gerekir. Modül nesne dosyaları da sadece root tarafından yazılabilir dosyalardır. Bunun anlamı, izinsiz girenin bir modülü sokmadan önce root erişimine gereksinimi olduğudur. Eğer izinsiz giren kişi root erişimi kazanırsa, modül yüklemesinden çok daha fazla endişelenilmesi gereken, daha ciddi şeyler vardır.

   Modüller, sık kullanılmayan belirli bir cihaz için desteğin dinamik olarak yüklenmesi amacını taşır. Sunucu makinelerde, veya örneğin güvenlik duvarlarında, bunun olma olasılığı dşüktür. Bu sebeple, sunucu makineler için desteği doğrudan çekirdeğe tümleşik derlemek daha mantıklıdır. Ayrıca modüller, çekirdeğe tümleşik derlenmiş destekten daha yavaştırlar.

2. Uzak bir makineden root olarak giriş yapmak neden hep başarısızlıkla sonuçlanıyor?

   Yanıt: Bakınız: *Root Güvenliği*. Bu, uzak kullanıcıların makinenize `telnet` yoluyla `root`olarak bağlanma girişimlerini engellemek amacıyla kasıtlı olarak yapılan bir şeydir. Uzaktan root olarak bağlanabilmek ciddi bir güvenlik açığıdır, çünkü bu durumda root parolası ağ boyunca açık metin olarak iletilmektedir. Unutmayın: potensiyel saldırganların vakti vardır, ve parolanızı

bulmak için otomatik programlar çalıştırabilirler.

3. Linux makinemde gölge parolaları nasıl etkin hale getirebilirim?

   Yanıt:

   Gölge parolaları etkin hale getirmek için, `pwconv`rogramını root olarak çalıştırın. Böylelikle `/etc/shadow` dosyası yaratılır ve uygulamalar tarafından kullanılmaya başlar. RH 4.2 ve üstü kullanıyorsanız, PAM modülleri otomatik olarak olağan `/etc/passwd` dosyasından gölge parolalara geçişe, başka bir değişikliğe gerek kalmaksızın uyum sağlayacaktır.

   Bazı temel bilgiler: Gölge parola mekanizması, parolalarınızı olağan `/etc/passwd` dosyasınından başka bir dosyada tutar. Bunun bir takım getirileri vardir. Birincisi, gölge dosyası, `/etc/shadow`, herkes tarafından okunabilen `/etc/passwd`,dosyasının aksine, sadece root tarafından okunabilen bir dosyadır. Diğer bir getiri, yönetici olarak, diğer kullanıcıların haberi olmadan bir kullanıcı hesabını etkisiz veya etkin hale getirebilirsiniz.

   The `/etc/passwd` dosyası, kullanıcı ve grup isimlerini tutmak için, örneğin `/bin/ls` programı tarafından bir dizin listesindeki dosyaların uygun kullanıcı ve grup isimlerini bulmak amacıyla kullanılır.

   The `/etc/shadow` dosyası ise kullanıcı ismi ve parolasını, ve örneğin hesabın ne zaman süresinin dolduğu gibi hesap bilgilerini içerir.

   Parolalarınızı güvenli hale getirmekle ilgilendiğinize göre, belki iyi parolalar üretmeye başlamakla da ilgili olabilirsiniz. Bunun için PAM'in bir parçası olan `pam_cracklib` modülünü kullanabilirsiniz. Parolanızı Crack kütüphanelerini kullanarak gözden geçirir, böylelikle parola-kıran programlar tarafından kolaylıkla tahmin edilebilir parolaları belirlemenizi sağlar.

4. Apache SSL uzantılarını nasıl etkin hale getirebilirim?

   Yanıt:

   a. ftp://ftp.psy.uq.oz.au/pub/Crypto/SSLadresinden SSLeay 0.8.0 veya daha yukarı sürümünü indirin

   b. Derleyin, deneyin, ve kurun!

   c. Apache kaynak dosyasını indirin.

   d. Burdan SSLeay uzantılarını indirin

   e. Apache kaynak dizininde sıkıştırılmış dosyayı açın ve README dosyasında yazdığı gibi yamayı uygulayın.

   f. Yapılandırın ve derleyin.

   Ayrıca, bir sürü önceden derlenmiş paketlere sahip olan ve ABD'nin dışında bulunan ZEDZ net'i de deneyebilirsiniz.

5. Kullanıcı hesaplarını idare ederken güvenliği nasıl sağlayabilirim?

   Yanıt: Red Hat dağıtımı, özellikle RH5.0, kullanıcı hesaplarının özelliklerini değiştirebilmeyi sağlayan bir çok araçla birlikte gelir.

   a. `pwconv` ve `unpwconv` programları gölge ve olağan parolalar arasında geçiş yapmak amacıyla kullanılabilir.

   b. `pwck` ve `grpck` programları, `passwd` ve `group` dosyalarının uygun düzende olduğunun doğrulanması için kullanılabilir.

c. `useradd`, `usermod`, ve `userdel`programları kullanıcı eklemek, silmek, ve değişiklik yapmak amacıyla kullanılabilir. `groupadd`,`groupmod`, ve `groupdel` programları aynı şeyleri gruplar için yapar.

d. Grup parolaları `gpasswd` kullanılarak yaratılabilir.

Bütün bu programlar "gölgenin farkında" olan programlardır, yani gölge parolaları etkin hale getirdiğinizde parola bilgisi için `/etc/shadow` osyasını kullanırlar, getirmezseniz kullanmazlar.

Daha fazla bilgi için ilgili man sayfasına bakabilirsiniz.

6. Apache'yi kullanarak belirli HTML belgelerini nasıl parola-korumalı hale getirebilirim?

   Yanıt: Bahse girerim http://www.apacheweek.org adresini bilmiyordunuz değil mi?

   Kullanıcı kimlik doğrulaması hakkında bilgiyi http://www.apacheweek.com/features/userauth adresinden, WWW sunucusu hakkında güvenlik ipuçlarını ise http://www.apache.org/docs/misc/security_tips.html adresinden bulabilirsiniz.

Sonuç

Güvenlik uyarı mektup listelerine üye olarak, ve güncel olayları takip ederek, makinenizi güvenli hale getirmeye doğru çok adım atabilirsiniz. Günlük dosyalarınıza ilgi gösterir ve `tripwire` gibi bir programı düzenli olarak çalıştırırsanız, daha fazlasını da yapabilirsiniz.

Evdeki bir makinede akla yatkın düzeyde bilgisayar güvenliğini kurmak ve idare etmek zor değildir. İş makineleri için daha fazla çaba gerekir, fakat Linux gerçekten güvenli bir platform haline gelebilir. Linux gelişiminin doğası gereği, güvenlik onarımları ticari işletim sistemlerinde olduğundan çok daha hızlı ortaya çıkar, bu da güvenliğin şart olduğu durumlarda Linux'u ideal bir platform haline getirir.

Teşekkürler

Burdaki bilgiler bir çok kaynaktan toplanmıştır. Aşağıda bulunan ve doğrudan veya dolaylı olarak katkıda bulunan herkese teşekkürler:

Rob Riggs
rob (at) DevilsThumb.com

S. Coffin
scoffin (at) netcom.com

Viktor Przebinda
viktor (at) CRYSTAL.MATH.ou.edu

Roelof Osinga
roelof (at) eboa.com

Kyle Hasselbacher
kyle (at) carefree.quux.soltec.net

David S. Jackson
dsj (at) dsj.net

Todd G. Ruskell
ruskell (at) boulder.nist.gov

Rogier Wolff
R.E.Wolff (at) BitWizard.nl

Antonomasia ant (at) notatla.demon.co.uk

Nic Bellamy sky (at) wibble.net

Eric Hanchrow offby1 (at) blarg.net

Robert J. Berger
rberger (at) ibd.com

Ulrich Alpers
lurchi (at) cdrom.uni-stuttgart.de

David Noha dave (at) c-c-s.com

Pavel Epifanov. epv (at) ibm.net

Joe Germuska. joe (at) germuska.com

Franklin S. Werren fswerren (at) bagpipes.net

Paul Rusty Russell
Paul.Russell (at) rustcorp.com.au

Christine Gaunt cgaunt (at) umich.edu

lin bhewitt (at) refmntutl01.afsc.noaa.gov

A. Steinmetz astmail (at) yahoo.com

Jun Morimoto morimoto (at) xantia.citroen.org

Xiaotian Sun sunx (at) newton.me.berkeley.edu

Eric Hanchrow offby1 (at) blarg.net

Camille Begnis camille (at) mandrakesoft.com

Neil D neild (at) sympatico.ca

Michael Tandy
Michael.Tandy (at) BTInternet.com

Tony Foiani tkil (at) scrye.com

Matt Johnston mattj (at) flashmail.com

Geoff Billin gbillin (at) turbonet.com

Hal Burgiss hburgiss (at) bellsouth.net

Ian Macdonald ian (at) linuxcare.com

M.Kiesel m.kiesel (at) iname.com

Mario Kratzer
kratzer (at) mathematik.uni-marburg.de

Othmar Pasteka pasteka (at) kabsi.at

Robert M rom (at) romab.com

Cinnamon Lowe clowe (at) cinci.rr.com

Rob McMeekin blind_mordecai (at) yahoo.com

Gunnar Ritter g-r (at) bigfoot.de

Frank Lichtenheld
frank (at) lichtenheld.de

Björn Lotz
blotz (at) suse.de

Othon Marcelo Nunes Batista
othonb (at) superig.com.br

Carlo Perassi
carlo (at) linux.it

Aşağıdaki insanlar bu HOWTO belgesini çeşitli diğer dillere çevirdiler. Linux mesajının yayılmasına yardım eden sizlerin hepinize özel bir teşekkür ediyoruz:

Polonyaca: Ziemek Borowski
ziembor (at) FAQ-bot.ZiemBor.Waw.PL

Japonca: FUJIWARA Teruyoshi
fjwr (at) mtj.biglobe.ne.jp

Endonezce: Tedi Heriyanto
22941219 (at) students.ukdw.ac.id

Korece: Bume Chang Boxcar0001 (at) aol.com

İspanyolca: Juan Carlos Fernandez
piwiman (at) visionnetware.com

Hollandaca: "Nine Matthijssen"
nine (at) matthijssen.nl

Norveççe: ketil@vestby.com
ketil (at) vestby.com

Türkçe: Tufan Karadere
tufank (at) gmail.com

Çeviri Hakkında - About Translation

In this additional page to the translation of the Linux Security HOWTO, I wish to make some additional explanations about the translation procedure for Turkish speaking people, which I hope to be helpful in following up the document. These explanations include the difficulty in translating a technical document, choosing the right terms/words for a given event/technology, and an English-Turkish vocabulary, which I hope to function as a map for not being lost in the Turkish terminology.

I wanted to translate Linux Security HOWTO for mainly two reasons:

- I think this HOWTO is an outstanding document for those who want to secure their Linux systems but don't know where to begin, in that this document includes nearly all of the issues generally relating to the security and where to find more information; and for those who has a general understanding of the terms of security, but want to know what exact implementations exist, and where to find more information about them. Although original HOWTO is dated a bit and some of the links may possibly be broken/changed, it's still a great source for general purpose security reading. Thanks to Kevin Fenzi and Dave Wreski for such a good contribution to the Linux community. I thought such a document should be translated into Turkish as well, so that Turkish people who can't speak English (if any, :)) can make use of the document.

- A second simple reason is to contribute to the Turkish terminology, by translating the terms of Computer Security issues, specifically in Linux Security. I think one of the most difficult tasks ever, is to provide translations of the fresh technical terms into one's own language (perhaps more difficult than securing Linux :)).

The rest of this page continues in Turkish to explain the difficulties in choosing the words, and make a little discussion about which words have been recommended, and why.

Türkçe Çeviri Üzerine Açıklamalar

Daha önce yapmış olanlar bilir, teknik bir belgeyi Türkçe'ye çevirmek zor bir iştir. Bu zorlukların sebeplerinin başında, seçilen sözcüğün ilk kez duyanlara "komik" gelmesi yer alıyor sanırım. Devlet memurluğunu milletçe çok sevdiğimiz için, seçilen sözcüklerin de devlet kurumu ciddiyetinde olmasını bekliyoruz belki de. Oysa İngilizce'deki, özellikle de bilgisayar dünyasındaki terimlerin Türkçe'deki tam karşılıkları kadar, İngilizce'deki anlamları da "komik", en azından "eğlenceli" şeylerdir.

"Türkçe'nin hali ne olacak?" şeklindeki tartışma çok uzun süreden beri devam ediyor. Çeviri yapmak için bu tartışmanın sonucunu beklersek, öyle sanyorum ki kendimizi bu tartışmayı İngilizce yaparken bulacağız. Bu çeviride "yaşayan Türkçe'yi" kullanmaya özen gösterdiğimi söyleyebilirim. Bunun anlamı şu: otobüse "oturgaçlı götürgeç" demedim ama "construction" sözcüğünü de konstrüksiyon şeklinde çevirmedim. En azından temel düşüncem belgenin anlaşılabilir olmasıydı. Bilmeyen kişilere bu konuları anlatırken kullandığım sözcükleri kullanmaya özen gösterdim.

Sözcüklerin çevirisinde Türk Bilişim Derneği'nin "önerdiği" sözcükleri de zaman zaman kullandım. Bununla beraber, açıkça söylemeliyim ki TBD'nin sözcük karşılıklarının çok yetersiz veya "yanlış" olduğunu düşündüğüm zamanlar da olmadı değil. Bunun en güzel örneği "key" için kullanılan "şifre" sözcüğüydü. Eğer önerilen sözcükleri aynen kullanmaya kalkarsam, örneğin "encryption key" ifadesini "şifreleme şifresi" ve "key encrypting key" ifadesini ise "şifre şifreleyen şifre" gibi garip bir Türkçe ile çevirmek zorunda kalabilirdim.

Eğer güvenlik ile ilgili her terimin başına "güvenlik" (güvenlik duvarında olduğu gibi), şifre ile ilgili her terimin başına da "şifre" koyarak Türkçe karşılık bulmaya kalkarsak, sanırım işimiz hiç kolay olmaz. Er geç düzeltilmesi gerekecektir. Yeni yeni düzeltilmeye başlanan, password sözcüğüne karşılık "şifre" yerine doğru karşılığı olan "parola"yı kullanmak gibi.

İşin içinden çıkılamayan sözcükler de oluyor elbette: Hacker, cracker, encapsulation, daemon, web, "on the fly" vb. Bu sözüklere ise olabildiğince karşılık bulmaya çalıştım, encapsulation gibi bazılarını TBD'den alıntı ile "sarma" (yaprak sarma gibi oldu ama n'apalım :)), cracker gibi bazılarını ise tam yaptıkları işi anlatan şekilde "korsan" olarak çevirdim (krakere tercih ettim). Bilgisayar teknolojisi yaygınlaşmadan önce de "hacker" sözcüğünün tam karşılığı, fiil ile birlikte kullanılıyordu: "Kurt" veya "bir şeyin kurdu olmak" şeklinde. Nedense "kurt" sözcüğü artık "bir şeyi iyi bilen" veya "bir şeyle çok uğraşan" anlamında daha seyrek kullanılmaya başlandı. Belki de "Kurt" sözcüğünün belirli bir siyasi görüşü/kimliği çağrıştırmasının da bununla bir ilgisi vardır. Halbuki "hacker", nerdeyse tam anlamıyla "bilgisayar kurdu"nun İngilizce'sidir.

E-mail sözcüğünü "e-posta" yerine "e-mektup" şeklinde çevirmeyi daha uygun bulduğumu da burda belirtmek istiyorum. Buna karşılık MTA'daki "Mail"in de posta şeklinde çevrildiğini, ama "to send a mail"in "posta göndermek"ten çok "mektup göndermek" olduğunu düşündüğümü de ekleyim. E-posta'nın çoğu kimse tarafından cümle içinde akıcı biçimde kullanıl(a)madığını, bir şekilde "mail" veya "email" ile desteklenerek kullanıldığını, ya da bu sözcüğü kullanmamak için sadece "email" kullanıldığını gözlemlemem üzerine böyle bir tercihte bulunduğumun altını çizmeliyim. "E-posta"nın, bu kadar uzun süredir kullanılmasına rağmen yeteri kadar yerleşmemiş bir sözcük olduğunu düşünüyorum. Bence bunun en önemli nedenlerinden biri, benzerleri gibi Türkçe'de çok yaygın olarak kullanılan deyimlerden oluşturulmamış olmasıdır. Oysa İngilizce'deki tüm bilimsel terimler, (artık) insanların günlük hayatta kullandığı sözcüklerden, ya da bunların kısaltmasından oluşturulmaya çalışılıyor.

Yukarıda söylediğim gibi, temel amaç konu hakkında bilgisi olmayan kişilerin en iyi anlayabileceği şekilde çeviri yapabilmek idi. Konuşurken bir yabancı sözcük yerine birkaçını kullanabilirsiniz, ama yazılı belgelerde bu çok işe yarar bir yöntem olmuyor ne yazık ki.

Bu kadar açıklamayı yapmamın sebebi, bu belgedeki terimlerin, tartışmaya ve önerilere açık olduğunu daha iyi anlatabilmek içindi. Tüm yapıcı öneri ve eleştirilerinizi, tufank@gmail.com adresine, konu kısmında "Guvenlik NASIL" yazan bir mektup atarak iletebilirsiniz (mektupların bana ulaştığından emin olmak için ü ile değil u ile yazmanızı rica ediyorum).

Belgenin özgün biçimi, Linux Security HOWTO, güvenlik konusunda, özellikle başlangıç, taslak oluşturma ve referans bakımından, en iyi belgelerden ve NASIL'lardan biri. Çeviri yapmak istememin de iki sebebinden biri, böyle bir belgeden İngilizce bilmeyen kişilerin de

yararlanmasını sağlayabilmek; diğeri ise güvenlik konusunda yavaş yavaş da olsa uyanmaya başlayan güzide yurdumun, güzide dilini "Kriptoloji, kriptografi, enkripşın, diimın, meyl, dos atak, hek, krek, şadov, veb, transparan, trojan-troyan-trocın hors, pablik, snifır, spuf" gibi sayısı sonsuz gibi görünen ingliş sözcüklerden temizleme çabasına katkıda bulunmaktı.

Her iki açıdan da yararlanmanız dileği ile...

Sözcük Karşılıkları

Alışık olunmadığını ya da farklı olduğunu düşündüğüm sözcüklerin kullandığım karşılıklarını belirtmenin, belgeyi takip etmeyi kolaylaştıracağını düşündüm.

- `account`: hesap
- `alias`: takma isim
- `brute force attack`: kaba kuvvet saldırısı
- `bug`: böcek
- `boot`: (bilgisayarı) başlatmak
- `cracker`: Bilgisayar sistemlerini "kıran" kişi, kırıcı, korsan.
- `reboot`: (bilgisayarı) yeniden başlatmak
- `attack`: saldırı
- `attacker`: saldırgan
- `buffer overflow`: tampon taşması
- `checksum`: sağlama toplamı
- `cluster`: demet
- `compromise`: (güvenliğini) bozmak/ihlal etmek
- `cookie`: çerez / kurabiye
- `cryptology`: şifrebilim
- `cryptography`: şifreleme
- `cryptanalyst`: şifreçözümleyici
- `encrypt`: şifrelemek
- `decrypt`: şifresini çözmek/açmak
- `exploit`: (güvenlik açıklarından) yararlanmak, (güvenlik açıkları anlamında da kullanılır)
- `display`: görüntü

- `file`: dosya
- `filesystem`: dosya sistemi
- `firewall`: güvenlik duvarı / yangın duvarı
- `frame`: çerçeve
- `free`: ücretsiz, özgür
- `free software`: özgür yazılım (çoğunlukla ücretsizdir de, ama asıl kastedilen yazılımı kullanabilme özgürlüğüdür, GPL lisansında ayrıntılı bilgi bulabilirsiniz)
- `gateway`: ağ geçidi
- `graphic(s)`: çizgesel
- `hacker`: Özellikle bilişim teknolojileriyle ilgili, belirli bir alanda (örneğin güvenlik alanında) tüm ayrıntıları öğrenmeye çalışmaktan zevk duyan kişi, bilgisayar canavarı, bilgisayar kurdu.
- `host`: bilgisayar (aslında çoğunlukla, ftp, www, news gibi bir hizmet veren bilgisayar)
- `image`: resim
- `intrude`: izinsiz girmek
- `intruder`: izinsiz giren (kişi).
- `intrusion`: izinsiz giriş
- `link`: bağ
- `symbolic link`: simgesel bağ
- `log`: günlük, günlük tutmak, günlüğünü tutmak.
- `login`: (sisteme) giriş
- `mail`: mektup
- `e-mail (electronic mail)`: elektronik mektup, e-mektup
- `mail transfer agent`: posta dağıtım aracı
- `mailbox`: posta kutusu
- `mailing list`: mektup listesi (haberleşme listesi veya elektronik liste olarak da kullanılır)
- `mail server`: posta sunucusu
- `malicous`: kötü niyetli
- `man-in-the-middle attack`: ortadaki adam saldırısı

- masquerading: maskeleme
- mount: (sabit disk bölümünü bir dizine) bağlama, bağlanma
- node: uç
- netlink: ağbağlantısı
- parameter: değiştirge
- parameterize: değiştirgelemek
- partition: sabit disk bölümü
- password: parola
- shadow password: gölge parola
- policy: politika
- router: yöneltici
- script: betik (İçinde komutların toplu halde bulunduğu, çalıştırılabilir olduğu halde ikili yapıda değil de metin yapısında olan dosya)
- server: sunucu (makine veya program)
- sniff: koklamak
- sniffer: koklayıcı
- spam: reklam (Tam olarak "spam mail", İnternet'te çoğunlukla reklam, çoğunlukla da ticari reklam amacıyla, istek yapılmadığı halde gönderilen mektuplar anlamında kullanılır)
- spoof: taklit etmek, taklit
- spoofing: taklit etme
- site: site (Belgede hem bir bilgisayarı, örneğin WWW, FTP sitesi gibi, hem de bir şirketin WWW, FTP, NEWS gibi sunucularının hepsini birden, yani tüm bilgisayarlar topluluğunu ifade etmek için kullanılmış)
- smurf: şirin (Aslında anlamı şirin değil, fakat smurf sözcüğü Türkiye'deki ismi "Şirinler" olan "Smurfs" isimli çizgi filmden geliyor, smurf sözcüğü İngilizce'de de bu çizgi filmden önce kullanılan bir anlama sahip değil)
- sticky bit: yapışkan bit
- swap: takas
- text: metin
- trojan horse: truva atı
- vulnerability: (saldırılara karşı) korunmasız olmak, saldırıya açık olmak

Kısaltma Karşılıkları

Belge içinde ekleri olabildiğince Türkçe okunuşlarına eklemeye çalıştım. Yaygın İngilizce okunuşlarını ve anlamlarını ise aşağıda bulabilirsiniz.

- BIOS: (bayos) - Basic Input/Output System - Temel Girdi/Çıktı Sistemi
- CIPE: (sayp) - Cryptographic IP Encapsulation - Şifreli IP Sarma
- DOS: (dos) - Disc Operating System - Disk İşletim Sistemi
- DoS: (dos) - Denial of Service - Servis Reddi
- DDoS: (di dos) - Distributed Denial of Service - (Birden çok bilgisayara) Yayılmış Servis Reddi
- FTP: (ef ti pi) - File Transfer Protocol - Dosya Aktarım Protokolü
- IP: (ay pi) - Internet Protocol - İnternet Protokolü
- IPSec: (ay pi sek) - IP Security - IP Güvenliği
- man: (men) - Manual - El Kitabı, Kitapçık (Unix benzeri işletim sistemlerinin yardım sistemi)
- MIME: (maym) - Multipurpose Internet Mail Extension - Çokamaçlı İnternet Mektup Uzantısı
- NIS: (nis) - Network Information System - Ağ Bilgi Sistemi
- NFS: (en ef es) - Network File System - Ağ Dosya Sistemi
- PAM: (pem) - Pluggable Authentication Modules - Takılabilir Kimlik Doğrulama Modülleri
- PGP: (pi ci pi) - Pretty Good Privacy - Oldukça İyi (Kişisel) Gizlilik
- SSL: (es es el) - Secure Sockets Layer - Güvenli Soket Katmanı
- ssh: (es es eyc, ama Türkçe'de es es aş) - Secure Shell - Güvenli Kabuk
- CFS: (si ef es) - Cyrptographic File System - Şifreli Dosya Sistemi
- TCFS: (ti si ef es) - Transparent Cyrptographic File System - Şeffaf Şifreli Dosya Sistemi
- SATAN: (seytın)- Security Administrator's Tool for Analyzing Networks - (Şeytan) - Ağ Çözümlemesi İçin Yöneticinin Güvenlik Aracı
- VPN: (vi pi en) - Virtual Private Network - Sanal Özel Ağ
- WWW: (bunun telafuzu çok uzuuun bi tartışma :), Türkçe'de çoğunlukla" ve ve ve" şeklinde, Amerikan İngilizce'sinde çok hızlı ve yutarak bir "dabyu dabyu dabyu" :)) - World Wide Web - Dünya Çapında Örümcek Ağı
- Web: (Cem Yılmaz'ın mukawwa deyişindeki "w" gibi :), web) - Web (Kısaltma değil) - Örümcek Ağı

[1] (Çeviri konusundaki eleştirilerinizi, eklemek istediklerinizi, ya da yanlış çeviriler konusudaki önerilerinizi tufank (at) gmail.com adresine gönderebilirsiniz. Konu kısmına "Guvenlik NASIL" yazın ki, benim reklam süzgecime de yakalanmayasınız :). Cevap alma konusunda da lütfen sabırlı olun :))

[2] Çevirinin güncel bir haline de http://www.belgeler.org adresinden ulaşabilirsiniz.

[3] cracker = çatlatan, çatırtadan, argoda sistemleri "kıran" kişi, "korsan", aynı zamanda bildiğimiz kraker anlamına da gelir. Türkçe'de kanımca buna en iyi karşılık gelen ifade "Bilgisayar Korsanı" olsa gerek.

Hacker ise, İngilizce günlük konuşmada bilgisayar teknolojisinin gelişmesinden önce çok yaygın olarak kullanılmayan bir sözcük. Bilgisayar teknolojosinin yaygınlaşması ile birlikte, argoda "Bilgisayar ile ilgili bütün konuları en ince ayrıntısına kadar öğrenmeye çalışmaktan derin bir zevk duyan kişi" anlamında kullanılmaya başlandı. Yine kanımca Hacker'a en iyi karşılık gelen ifade "Bilgisayar Kurdu". Cracker"lar kendilerinin kraker olarak anılmasından hoşlanmamış olacak ki bir süre sonra cracker ve hacker sözcükleri aynı anlamı ifade edecek şekilde kullanılmaya başlandı. Daha doğrusu hacker sözcüğü cracker için kullanılmaya başlandı. Bilgisayar dünyasındaki terimlerle resmi olmayan şekilde anlatacak olursak: Hacker her şeyi bilen, cracker ise sisteme (izinsiz) girendir.

Bir sisteme izinsiz girebilmek, yani o sistemi "kırabilmek" için o sistemin bütün teknik ayrıntılarını bilmek gerekmez. Açık kapının, ya da zayıflıkların nerde olduğunu bilmek yeterlidir. Bununla birlikte, bir sistemin bütün teknik ayrıntılarını biliyorsanız, muhtemelen zayıf noktalarını da bilirsiniz, bu yüzden en iyi "cracker"lar genelde "hacker"lardan çıkar. "Lamer" (lame = topal, aksak) ise, zayıf noktanın bile neresi olduğunu anlamadan sisteme girmeye çalışan kişiye denir :).

[4] Eğer X Windows'u `startx` komutuyla başlattıysanız, muhtemelen bunu yapmadan önce sisteme metin konsollarından birini (ayarları değiştirmediyseniz 6 tane) kullanarak girmişsiniz demektir. `startx` komutu, X Windows'u çoğunlukla 7. konsolda açar, fakat giriş yaptığınız konsol kapanmaz. Gelen herhangi birisi <**Control**>-<**Alt**> ile birlikte Fonksiyon tuşlarından birini kullanarak (<**Control**>-<**Alt**>-<**F1**>'den <**Control**>-<**Alt**>-<**F12**>'ye kadar) diğer metin konsollara, ve `startx` ile X Windows'u başlattığınız konsola geçiş yapabilir. Bu konsolda <**Ctrl**>-<**C**> veya <**Ctrl**>-<**Z**> tuş kombinasyonunu kullanarak X Windows'u tümden kapatıp daha önce giriş yapmış olduğunuz konsolun kabuğuna erişim sağlayabilir. Bunu önlemek için, `xdm`, `kdm`, veya `gdm` kullanabilirsiniz. Giriş yaptıktan sonra `startx` komutunu değil,

```
xdm; exit
```

komutunu yazarak X Windows'u başlatabilir, daha sonra `xdm` giriş ekranından giriş yapabilirsiniz. Veya bilgisayarınızın daha açılışta `xdm`'i yüklemesini sağlayabilirsiniz. Bunun için `/etc/inittab` dosyasıyla ilgili bilgi araştırmasında bulunmanız gerekebilir. `xdm` komutunu kullanmak çoğunlukla o sistemde root olmayı, ve diğer bazı ayarları yapmış olmayı gerektirebilir. Bunun için Linux dağıtımınızla birlikte gelen belgelere, man sayfalarına, veya Linux-NASIL belgelerine göz atabilirsiniz.

[5] İngilizce bug (böcek) kelimesi, bilgisayar dünyasında, yazılımların, yazarları tarafından önceden tahmin edemedikleri, "çalışma zamanında", yani "çalışırken" ortaya çıkan hataları kastetmek için kullanılır. Bununla ilgili anlatılan bir hikaye, bilgisayarların henüz bir oda büyüklüğünde olduğu zamanlarda, bir böceğin bilgisayarın içine girerek kısa devreye sebep olduğu, böylelikle o anda çalışmakta olan "yazılım"ın görevini yerine getirememesine yol açtığı şeklindedir. Bu olay, ilk "yazılım böceği" olarak anılır. Genelde "böcek" kelimesi, yazılımların çalışırken, çoğunlukla beklemedikleri veya kontrol etmedikleri bir girdi karşısında ne yapacaklarını bilememeleri, yahut da kendilerine

işletim sistemi tarafından yasaklanmış olan bazı şeyler yapmaya kalkmaları yüzünden "göçmesi" ile sonuçlanan "yazılım hataları" için kullanılır. Bu yazılım hataları, önemli bir oranda denetimin yazılım dışına çıkmasına ve işletim sistemine devredilmesine yol açar. Bunu bilen bir saldırganın, yazılımın bıraktığı yerde, işletim sistemi henüz devreye girmemişken, denetimi devralarak kendi yararına olan yazılım kodu parçacıklarını sistem üzerinde çalıştırmasına olanak sağlar. Bu yüzden daha önce bahsedilen, yazılım sürümlerinin güncel tutulması özellikle önem kazanmaktadır. Çünkü bir yazılımın bulunmuş böcekleri, bir sonraki sürüm çıkmadan önce temizlenir. Hatta bazı güncellemeler, yazılımın sadece böceklerden temizlenmiş olması için yayınlanan güncellemelerdir.

Bizzat hesabın meşru sahibi tarafından zarar verilmek istenebilir.

[7] Bir çok Linux sistemde bunu `alias rm="rm -i"` komutuyla, örneğin sistem genelindeki başlangıç dosyalarının (`/etc/profile` gibi) içinde gerçekleştirebilirsiniz.

[8] tek bir nokta olan geçerli dizin, o anda içinde bulunduğunuz dizindir.

[9] Bu dosya başka bilgisayarlardan çoğunlukla parolasız bağlantı için kullanılır. Sadece oluşturmamakla kalmayıp, özellikle root için böyle bir dosyanın olmadığından emin olun.

Bir çok saldırı, root'un ev dizinine, içinde `+ +` satırı bulunan bir `.rhosts` dosya oluşturulması ile sonuçlanır, ki bu makinenize her hangi bir bilgisayardan herhangi bir kullanıcının parola girmeden root olarak bağlanabileceği anlamına gelir.

[10] sınırsız

[11] bit, binary digit (ikili sayı düzenindeki rakam) ifadesinin kısaltmasıdır. İkili sayı düzeninde iki rakam vardır, 1 ve 0.

[12] Red Hat dağıtımında, yeni bir kullanıcı açtığınız zaman, grubunu belirtmediğiniz sürece, kullanıcı ismiyle aynı yeni bir grup açılır ve kullanıcı bu grupta yer alır.

[13] Dizinde hangi dosyaların bulunduğunu görebilme

[14] Betikler, ikili dosya türünde olmayıp, bildiğimiz okunabilir metin dosyalarıdır. Diğer metin dosyalarından farkları çalıştırılabilme özellikleridir. Bu özellikleri, betiklerin ikili dosya tipleri, yani programlar tarafından yorumlanması şeklindedir. Örneğin bash kabuğu için yazılmış bir kabuk betiği `bash` programı tarafından, bir perl betiği `perl` programı (veya modülü) tarafından, ve bir php betiği ise `php` programı (veya modülü) tarafından okunarak, içindeki komutlar yerine getirilir.

[15] Bir dizin için çalıştırma bitinin durumu, o dizine `cd` veya `chdir` komutlarıyla girilip

girilemeyeceğini de belirler.

[16] Bir başka örnek, dosya göndermenize izin verilen ftp sunucularıdır. Burda aynı dizine herkes dosya aktarımı yapabilir, ama bir kullanıcının koyduğu dosyayı diğer bir kullanıcı silemez.

[17] Normalde Unix sistemlerde bir bir programı veya kabuk betiğini çalıştırarak bir işlem başlattığınızda, o işlemin kullanıcı kimliği ve izinleri, başlatan kişininkiyle aynıdır. Söz konusu dosyanın sahip izinleri bölümünde SETUID (Set User ID) biti 1 ise, bu, dosya sahibinin kullanıcı kimliğinin, işlemin etkin kullanıcı kimliği haline getirilmesini sağlar, ve işlem o dosya sahibinin erişim izinleri ile çalışır. Bunun pratik olarak anlamı şudur: Bir dosyanın sahibi root ise, ve SETUID biti 1 ise, o dosya çalıştırıldığında, çalıştıran kişi işlemin çalışması boyunca root olur, işlem bittiğinde eski kullanıcı kimliğine (gerçek kullancı kimliği) geri döndürülür. Tampon taşmaları, programın "göçmesine" ve yarım kalmasına sebep olan böceklerdir. Program henüz bitmemiş olduğu için çalıştıran kullanıcı hala root erişim iznindedir. Bu noktada bir kabuk çalıştırılabilirse bu kişi pratik anlamda root'un yapabileceği herşeyi yapabilir anlamına gelir.

[18] SGID - set group id, grup kimliğini belirle

[19] Dizin içindeki dosyalar listelenmez, ama dosyanın ismini biliyorsanız, ve dosyanın izinleri uygunsa dizinle birlikte dosyanın tam yolunu yazdığınız takdirde dosyaya erişmeniz mümkündür.

[20] Massachusetts Institute of Technology - Massachusetts Teknoloji Enstitüsü

[21] Çekirdek kaynak dosyaları genelde `/usr/src/linux` altında bulunur, `make config` komutu da bu dizine girdikten sonra verilir. Bahsedilen dosya da `make config` komutunun verildiği dizine göre genelde `./Documentation/` altındadır.

[22] 2.4 çekirdek sürümünden itibaren artık bu iki programın yerine iptables kullanılmaktadır.

[23] NO-USER: KULLANICI-YOK

[24] MTA: Mail Transfer Agent, Posta Dağıtım Aracı

[25] Şirin sözcüğü için bkz. *Sözcük Karşılıkları*

[26] 2.4 ve 2.6 çekirdekler için `iptables`

[27] Kırıldığınızı Nasıl Anlarsınız, Sonrasında Ne Yaparsınız? bu konudaki bir başka Türkçe belge, ve diğer güvenlikle ilgili belgeler ile birlikte http://www.ulakbim.gov.tr/dokumanlar/guvenlik/sunumlar.uhtml adresinde duruyor.

[28] Kitaplar İngilizce olduğu için, ulaşmak istemeniz durumunda İngilizce referansların bulunması daha iyi olacaktır. Bu yüzden referans bilgilerini çevirmeden bırakmanın daha iyi olabileceğini düşünüyorum

[29] Bu çeviride kullanılan İngilizce sözcükler için önerdiğim Türkçe karşılıkları *Sözcük Karşılıkları* bölümünde bulabilirsiniz. En azından bir göz attığınızdan emin olun :)

[30] Bilgisayar, saldırgana servis vermekle o kadar meşguldür ki meşru kullanıcılara servis vermeyi reddeder

[31] Temel olarak, bağlantı yapmaya çalıştığınız bilgisayara, IP bilgilerinizi yanlış iletmek olarak özetlenebilir

[32] Yani veriyi gönderen kişinin veriyi gönderdiğini daha sonra inkar edememesi