Sinan Göktepeli

Ateşten Duvarlar...

KEVİN Mitnick, bilgisayarlarla oynamaya lise yıllarında başladı. Lise müdürlüğünün bilgisayar sistemine girdi, ancak notları değiştirmedi - sadece bakıyordu. Daha sonra Pacific Bell telefon şirketinin teknik kılavuzlarını çalarken yakalandı. Gözaltındayken, bir üniversitenin bilgisayar sistemine girerken tekrar yakalanınca 6 ay hapis cezası yedi. Ancak hapisten çıktığında, en büyük bilgisayar ağı (yani telefon sistemi) hakkında Pacific Bell'in çalışanları kadar bilgi sahibiydi. Bu sayede, hatlara istediği gibi girip çıkabiliyor, şirketin tüm hizmetlerinden bedavaya yararlanabiliyordu.

1988'de Digital adlı bilgisayar devinden yazılım çalarken yakalanınca bir yıl daha hapis cezası aldı. Hapisten çıktıktan sonra, üç yıl boyunca kaçak olarak yaşadı. Bu yılın başında bilgisayar güvenlik sistemleri konusunda uzman Tsutomu Shimomura'nın bilgisayarına girip bazı bilgileri ondan çalmaya çalıştı. Ancak Shimomura, bilgisayarına giren kişinin peşini bırakmadı ve FBI ile birlikte çalışarak onun yakalanmasına yardımcı oldu. Mitnick, Kuzey Carolina'daki evinde yakalandığında, elinde en az 1 milyon dolarlık yazılım ve birçok kişinin de kredi kartı numaraları ve şifreleri vardı.

Mitnick'in bu hikâyesi geçtiğimiz aylar boyunca basında çok yer aldı. Ancak, onun kadar duyulmasalar da birçok kişi onun yaptıklarını yapıyor. Bu kişiler, İnternet halkı tarafından "hacker" olarak adlandırılıyor. Bu kelimenin tam bir Türkçe karşılığı yok. İngilizce "hack" kelimesi, beceriksiz ve düzensiz vuruşlar ile kesmeye çalışmaktan, uzun yürüş yapmaya ve çok kullanarak işe yaramaz hale getirmeye kadar birçok anlama geliyor.

İnternet, insanların bilgileri diğerlerine zarar vermek amacı gütmeden paylaşmak isteyen kişiler tarafından kullanılıyordu. İlk programlar, bu mentaliteye sahip olmayan insanlara karşı neredeyse hiçbir savunma getirmiyorlardı. Ancak, hacker'ların sayısı arttıkça bazı önlemler alınmaya başlandı. Yine de hacker'ların çok kullandığı bazı yöntemlere karşı hâlâ pek fazla savunma geliştirilemedi. Bunların bazıları şöyle:

Şifre Hırsızları: Bu küçük programlar network üzerinde bazı bilgisayarlara konuluyor. Bu programlar, üzerinden diğer bilgisayarlara yapılan kullanıcı girişlerini ve şifrelerini kütüklere kaydediyorlar. Yapılan araştırmalara göre, bu programlar ile, bugüne kadar onbinlerce şifre çalındı ve kullanılmakta.

Kandırmak: Bu tekniği kullananlar, uzaktaki bir makineye güvenilir bir makinenin Internet adresini vererek, ona girmeye çalışırlar. Böylece makineye girerek sistem yöneticisinin (ya da root kullanıcının) şifresini alarak istediklerini yapmaya çalışırlar. Root şifresini elde edenler, genellikle bir şifre hırsızı veya ona benzer programlar yerleştirir ve sistemden istedikleri bilgileri alırlar.

Web'deki Delik: Şu an dünyanın dört bir yanındaki makinelerde yüklenmiş olan WWW sunucu yazılımlarının bir kısmında bir güvenlik deliği bulunmaktadır. Almanya'dan bir programcı, bu servisi kullananlara bazı sunucular tarafından birçok haklar verildiği konusunda bir uyarı mesajı yayınlamıştı. Bu tip sunucuyu kullanan yerlerde şu an büyük bir risk olduğu düşünülüyor.

Bu tip durumların ve hacker'ların yarattığı risklere karşı birçok önlem geliştirildi bugüne kadar. Bu tip programların en çok kullanılan tipine firewall'lar (ateşten

duvarlar) deniliyor. Firewall'ların kullanımına değinmeden önce bir LAN'ın (Yerel Alan Ağı) yapısına değinmek gerekir.

Bir LAN, aslında bir kablo aracılığı ile birbirine bağlanmış bilgisayarlardan oluşmaktadır. Bu kablo, genellikle bildiğimiz televizyon anten kablolarından 50 ohm'luk koaksiyel, veya kalın ethernet kablosu olabileceği gibi, ikili telefon kablosu da olabilir. LAN, bir başka LAN veya çeşitli farklı network tipleri ile Internet'e bağlanır. LAN ile dış network'ün birbiri ile buluştuğu noktada bir gateway vardır.

Gateway, LAN'ın dışarısıyla iletişimini sağlayan ayrı bir makine olabileceği gibi, bu işi üzerine almış bir bilgisayar da olabilir. Gateway görevini üzerine almış olan bir bilgisayar, çift evli bir bilgisayar olarak adlandırılır. Birinci evi, korumak zorunda olduğu LAN (güvenilir bölge), diğeri ise Internet'tir (güvensiz bölge). Bu bilgisayar üzerinde çalıştırılacak programlar aracılığı ile, güvenilir bölge ve güvensiz bölge arasına bir ateşten duvar örülebilir.

Firewall programlarının tasarımlarında bazı konulara özen gösterilmelidir: (1) Network servisini sunan sistemde bir hata varsa (bazı W3 sunucu programları gibi), bu sisteme zarar vermemelidir; (2) Güvensiz bölgeden, bazı üstünlükleri olan network servisleri kullanılmamalıdır; (3) Network servislerini sunan programlar basit ve kolayca kontrol edilebilir olmalıdır. Bu üç nokta, neredeyse tüm firewall uygulamalarında dikkate alınmaktadır. Ancak, daha önemli bir nokta da bir firewall'un çevresel bir güvenlik sağlamakta olmasıdır. Kötü niyetli biri, firewall'u geçerse, programlar onu durduramaz. Böyle bir sistem, çelik kapılı bir eve benzetilebilir. Kapı açıldıktan sonra hiçbir önlem kalmaz.

Firewall programlarını sistemine yerleştirmekte olan bir sistem yöneticisi de, ilk olarak bir güvenlik politikası belirlemek zorundadır: Ya "açıkça yasaklanmamış herşey serbest olacak" ya da "açıkça serbest bırakılmamış herşey yasaklanacaktır". Birinci yaklaşımda, risk taşıyan servisler tespit edilir ve bunlar durdurulur ya da güvenli hale getirilir. İkincisinde ise, tamamen denenip güvenli olduğu kesinleşmemiş hiçbir servis sunulmaz. Birinci yaklaşımda herşey daha serbesttir. Ancak, sistem yöneticisi ve hacker'lar arasında bir silahlanma yarışına dönüşmesi olasıdır. Geniş bir ağın korunmasına çalışıldığı durumlarda, sistem yöneticisinin her şeyi kontrol etmesi çok zor olacağından, kolayca açık verebilir. İkincisi ise, oldukça konservatiftir. "Bilmediğimiz şeyler bize zarar verebilir", düşüncesinden yola çıkar ve sunulan servislerin tiplerinde ve sayılarında sınırlamalar getirir. Bu düşünceler göz önüne alındığında, ikinci yaklaşımın kullanılması daha iç rahatlatıcı olacaktır.

Yapısal Olarak Firewall'lar

Bir LAN'ı Internete bağlamak için en çok tercih edilen yöntem, iki network'e de bağlı olan bir bilgisayar kullanmaktır. Böylesi hem çok kolay hazırlanabilmekte, hem de çok ucuza malolmaktadır. Bu makine üzerinde iki ayrı network kartı vardır. Bu sayede, makinenin bir yanındaki bir paket, diğer yana gönderilmediyse oradan görülemeyecektir (paketler konusunda daha detaylı bilgi için bkz: Bilim ve Teknik, Mart 1995). Bu, Berkeley temelli Unix sistemlerinin bir özelliğidir. Aradaki trafiğin bütünüyle kesilmesi ve güvenilir bölge ile güvensiz bölge arasında aktarılacak bilgileri sadece aracı programlar kullanarak iletmek, firewall'larda sık sık kullanılan bir yöntemdir. İki network arasında doğrudan iletişim olmayacağından, dışarıdaki makineler için güvenilir bölge görünmez olacaktır.

Buradaki çift evli bilgisayar - yani koruyucu - bir iletici, iletişim kaydedici, ve servis sunucu olarak çalışmaktadır. Bu nedenle onun güvenliğini sağlamak büyük önem taşımaktadır.

Bundan daha az güvenli bir sistem ise, gözetimli makine gateway'i olarak adlandırılan dizilimdir. Burada, bir koruyucu ve bir tane de paket gözlemi yapabilen router bulunmaktadır. Koruyucuda kullanılan yazılımlar, bir çift evli bilgisayarınkiyle aynıdır. Servisler koruyucudan verilmektedir; bir şekilde paket gözlemi yapabilen bir router ise, güvenilir networkle güvensizin arasındaki iletişimi kesmektedir. Sadece dışarıdan sunulan bazı servislere ve güvenilir olduğu kabul edilen servislere izin verilmektedir. Bu durumda dikkat edilmesi gereken iki nokta olduğundan, yönetimi daha zordur.

En emin yöntem ise, gözetimli alt-ağ gateway dizilimidir. Burada güvenilir bir ağ ile güvensizin arasına izole edilmiş küçük bir ağ yerleştirilmektedir. Bu ağa ulaşım, paket gözlemi yapabilen iki router ile sınırlanmaktadır. Arada kalan ağa silahsızlandırılmış bölge de denilmektedir. Bu dizilim ile Internet üzerindekiler, ağ hakkında hiçbir şey öğrenemeyeceklerdir. Aynı şey, güvenilir taraf için de geçerlidir.

Daha fazla güvenliğin sağlanması gereken durumlar olacaktır. Örneğin, uzaktaki bir yerden işyerine bağlanmak isteyenler olabilir. Internet aracılığı ile satış yapan şirketlerde de müşterilerinin kredi kartı numaraları kayıtlıdır ve müşteriler şifreleri ile alışveriş yaparlar. Şifre hırsızı programlar ile internet üzerinden aktarılmakta olan şifreler okunabileceğinden, bir kerelik şifre kullanımı en emniyetli sistem olacaktır. Bir kerelik şifre hazırlayan yazılımlara doğrulama (authentication) servisi denilmektedir. Bu servisin kullanıldığı yerlerde, ya kullanıcının önceden belirttiği bir sıraya göre şifresi değiştirilir ya da soru-yanıt hesaplayıcıları kullanılır. Soru-yanıt hesaplayıcılarında, girilmek istenen taraf bir şifre istemeden önce bir soru gönderir. Bu sorunun yanıtı, iki tarafta da bulunan soru-yanıt hesaplayıcısı programlar tarafından hesaplanır ve kullanıcı, sonucu gönderir. Eğer sonuç doğruysa, kullanıcı girme hakkını kazanır. Bu sistem, her şifre sadece bir kere kullanılıyor olacağından çok güvenilir olur.

İzleme

Internet üzerinde bu kadar çok güvenlik önleminin bulunuyor olması insanları şaşırtabilir. Ancak, daha şaşırtıcı olan şey, hacker'ların çalışkanlığı olsa gerek. Çok kullanılan merkezlere hergün birçok basit girme denemesi yapılmasına karşın, her hafta en azından birkaç tane ciddi saldırı ile karşı karşıya geldikleri, tutulan kayıtlarla biliniyor. Ancak, kullanılan programların çoğu, yine de bizlere inceleyebileceğimiz kayıtlar yaratmakta. Bu kayıtların çok detaylı olması, bazı kullanıcıları rahatsız ediyor. Herkesin bilgi ve yazılım alabileceği, ftp.funet.fi gibi anonim ftp'ye açık ve yapılan tüm işlemlerin kaydedildiği bazı merkezlerin yöneticilerine bu nedenle yakınmalar gidiyor.

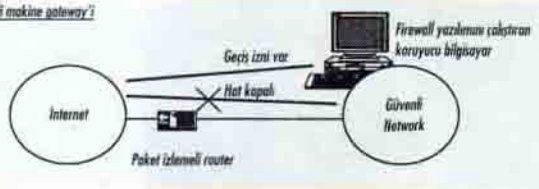
Ancak, merkezlerin yöneticileri bu konudan rahatsızlık duymuyorlar. Herşeyden önce bu merkezler, onların kendi yerleri olduğunu ve buraların kim tarafından nasıl kullanıldığını bilmeye hakları olduğunu savunuyorlar. Yine de önlem olarak, bu tip merkezlere girildiğinde, bir uyarı mesajı ile merkezde yaptığınız her şeyin kaydedileceği size bildiriliyor. Kullanıp kullanmamak ise size kalmış.

Ülkemizin önemli merkezlerinde bile, Internet üzerindeki kötü niyetli kişilere karşı pek fazla önlem alınmamış durumda. Bazı merkezlerin güvenliklerindeki deliklerin varlığından haberdar olunsa da, giderilmiyor olması herhalde genellikle ülkemizde karşılaşılan bir durum olsa gerek. Ancak, Internet'in öneminin hâlâ kavranamadığı ülkemizde de ciddi güvenlik önlemlerine uzun süre ihtiyaç duyulmayabilir. Nitekim, ABD ve birçok Avrupa ülkesi bilgi otobanları oluşturuyor. Buralarda eğlenceden (filmler ve Internet üzerinde oynanan oyunlar), eğitime ve iletişime (görüntülü telefon ve daha birçok yöntem) kadar çeşitli hizmetler sunuluyor. Oysa, ülkemizin telekomünikasyon ağı hâlâ bu tip hizmetleri sunabilecek kadar güçlü değil. Hatta bazı üniversitelerin Internet bağlantıları herhangi bir modem bağlantısından daha az bilgi taşıyabilecek durumda. Bilgisayarların iletişimde getirdikleri kolaylıklardan yeterince yararlanılabilse, birçok kişi güvenlik sorunlarıyla uğraşmayı bir yük olarak görmeyecek, zevk için yapacaktır sanırım.

Kaynaklar:
Bellovin, Steven M., There Be Dragons, AT&T Bell Laboratories
Ranum, Marcus J. Thinking About Firewalls
Newsgroups
Time 27 Subat 1995
TIS Firewall Toolkit, Trusted Information Systems, Inc.

Şekil 1: Çift evli gateway

Şekil 2: Gözetimli makine gateway'i



Şekil 3: Gözetimli alt-ağ gateway'i