Ağ Güvenliği Konusunda Kendinizi Yetiştirmek

12. 2006, v1.0
Ar. Gör. Enis Karaarslan,
ULAK-CSIRT
Ege Üniversitesi Kampüs Network Yöneticisi

Güvenlik konusunda, özellikle ağ yönetimi ve ağ güvenliği konusunda kendini yetiştirmek isteyen arkadaşlardan e-posta'lar alıyorum. Elimden geldiğince onlara yardımcı oluyorum, bu yazıda güvenlik konusunda nasıl kendinizi yetiştirebileceğiniz konusunu ele almaya çalışacağım. Yazıya yorumlarıyla katkıda bulunan Hüzeyfe Önal'a teşekkürler.

Öncelikle Ağ Güvenlik Uzmanı (Network Security Analyst) kimdir ve ne yapar? Sistem güvenlik uzmanı, sistemin güvenli olması için şu süreçleri yerine getiren kişidir:

- Var olan tehditleri sürekli olarak takip etmek ve analiz etmek,
- Bu tehditlere karşı alınabilecek önlemleri incelemek, mümkünse bir test ortamı içerisinde bunları denemek,
- Gerekli önlemleri devreye almak,
- Önlemlerin düzgün çalıştığını sürekli olarak kontrol etmek (log ve trafik analizi - saldırı programlarıyla sistemi test etmek)

Ağ güvenliği konusunda kendinizi yetiştirmek için ne yapmalısınız? Bunu öğrenmek, denemek ve uzmanlaşmak alt konularında inceleyeceğiz.

Öğrenmek

Güvenlik konusunda çalışabilmek için, öncelikle ağın nasıl çalıştığı ve kullanılan protokoller hakkında bilgi sahibi olmak gerekmektedir. Öncelikle TCP/IP protokolleri çok iyi bilinmelidir. Güvenlik uzmanı, sorun yaşandığında sorunun nedenini tespit etmek için ağ trafiğini ve logları analiz edebilecek bir kabiliyete sahip olmalıdır. Bunun için Cisco Network Akademi programının güzel bir başlangıç olduğunu düşünüyorum. Bunun mümkün olmadığı durumlarda, internet ortamındaki bilgi kaynakları kullanılmalı ve Ethereal gibi paket analiz programları ile analiz denemeleri yapılmalıdır.

Herşeyin başı bilgidir. Bilgiyi en yoğun olarak internet ortamında bulabilirsiniz. Öncelikle, ULAK-CSIRT bünyesinde hazırladığımız Türkçe dökümanlar (http://csirt.ulakbim.gov.tr/dokumanlar/), ağ güvenliğinin sağlanması konusunda ciddi bir referans kaynağı olacaktır. Bu adresteki dökümanların sayısını ve çeşitliliğini arttırmak için çalışmalarımız devam etmektedir. Linux konusunda kendinizi yetiştimek için http://www.belgeler.org adresi iyi bir başlangıç olacaktır. Güvenlik açıklarından haberdar olmak için Olympos http://www.olympos.org adresini takip edilebilir ve çeşitli e-posta listelerine üye olabilirsiniz. Güvenlik konusunda kullanabileceğiniz bilgi kaynaklarının bir listesi için http://csirt.ulakbim.gov.tr/link.uhtml kullanılabilir.

Güvenlik uzmanı, işletim sistemleri hakkında bilgili olmalıdır. Özellikle açık kaynak kodlu güvenlik programlarını kurabilmek ve kullanabilmek için, iyi bir seviyede Linux bilmesi gerektiğini düşünüyorum. Bazen scriptler üzerinde oynaması gerekebilecektir, o yüzden en azından program kodlarını okuyup anlayabilmesi ve gerektiğinde değişiklikler yapabilmesi de gerekebilecektir. Bu nedenle, C dilini, Perl gibi script dillerini bilmesi de önemli bir artı olacaktır.

Son zamanlarda kullanımı artan sanal makinalar, çeşitli denemeler için idealdir. VMware (http://en.wikipedia.org/wiki/Vmware), Cooperative Linux (http://en.wikipedia.org/wiki/Colinux) gibi programlarla sanal makinalar kurup programlar denenebilir, saldırı/savunma uygulamaları

çalıştırılabilir. Sanal makina pogramlarının karşılaştırılması için (http://en.wikipedia.org/wiki/Comparison_of_virtual_machines) adresi incelenebilir.

Ağ güvenliğini sağlamak için Güvenlik duvarları, Saldırı Tespit/Engelleme Sistemleri, zafiyet tarama sistemleri ve birçok güvenlik önlemi bulunmakta. Ürün tabanlı olmadan, sadece hangi önlemin, ne için gereçekleştirildiği ve nasıl etkin olduğunu bilmek iyi bir başlangıç olacaktır. Ürün bazlı çalışma daha çok kullanım kitapçıklarını (manual) okumak ve uygulama anında geçerli olacaktır. Bu da ancak öyle bir çözüm kullanıyorsanız veya deniyorsanız geçerlidir.

Ağ güvenliği konusunda piyasada çeşitli kurslar olduğunu duyuyorum. Bazıları "Hacker Eğitimi" gibi ilginç adlarla da ortaya çıkıyorlar. Bu kurslar hakında en iyi yorumu, daha önceden bu kursa gitmiş bir kişiden alabileceğinizi düşünüyorum.

Denemek

Deneyim çok önemlidir. Bir test ortamı yaratabilirseniz kendiniz de saldırı/savunma süreçlerini gerçekleştirebilirsiniz. Biz Ege Üniversitesi Ağ Güvenlik Laboratuvarı'nda bunu gerçekleştiriyoruz. Kendi içinde bir ağ olan bu ortamda; saldırgan, hedef makina (kurban) ve saldırı tespit sistemleri bulunmaktadır. Böylece saldırıların gücü ve savunma yöntemleri hakkında denemelerde bulunabiliyoruz. Siz de kendiniz daha küçük çaplı da olsa bu tür denemeler yapabilirsiniz. Bir uyarıda bulunmak istiyorum, bu tür denemelerin izinsiz olarak başka ağlarda kullanılması yasal ve etik olmadığı gibi, ciddi sorunlara yol açabilir. Bu nedenle, bu tür denemeler mutlaka ağdan yalıtılmış/ayrık ortamlarda yapılmalıdır.

Uzmanlaşmak

Güvenlik konusu gerçekten de geniş bir alan. Bilgisayar dünyasında olduğu gibi, güvenliğin her alt konusunda uzman olmak imkansız. Örneğin kablosuz ağ güvenliği, kriptografi (cryptography), bilgisayar adli bilimleri (computer forensics), nüfuz deneyi (penetration test) ... vb konularının herhangi birinde uzmanlaşmak bir hedef olarak alınabilir. Hüzeyfe Önal'ın yorumuyla yazıyı bitireyim; "Güvenlik konusuna bozma penceresinden değil de yapma penceresinden bakmak her zaman sizin için daha öğretici olur. Güvenlik konusunda zevk, aslında oyanan bir piyesin perde arkasını bilmekte yatar. Bir başkası için birşey ifade etmeyen garip paketler, size aslında yaklaşan bir tehlikeyi haber veriyordur."

Kitap İncelemesi

Ağ Güvenliği konusunda Türkçe döküman açığı bulunmakta. Elimize bu konudaki kitaplar geçtikçe, incelemeye çalışıyoruz. **"Ağ Güvenliği İpuçları"** kitabı, **Açık Akademi Yayınları**'ndan çıkan bir tercüme kitap. Bu kitapta, sisteminizi basit bir hedef olmaktan çıkaracak 100 etkin güvenlik tekniği sunulmakta. Bunlar, daha çok konfigürasyon önerileri ve kurulabilecek açık kaynak kodlu yazılımları içeriyor. İncelediğinizde, uygulayabileceğiniz çeşitli ipuçlarına ulaşabileceğinizi ve yararlı olacağını düşünüyorum. (http://www.acikakademi.com)