

Hardening Kavramı

Günümüzde saldırı sayılarındaki artış, güvenlik önlemlerinin artmasına sebep olmuştur. Bir ağ üzerinde çeşitli noktalarda güvenlik önlemleri alınabilir. Hardening bu önlemlerden biridir ve sadece kritik görevlere sahip sistemler üzerinde uygulanması mantıklıdır. Yapılan işlem ; önceden belirlenen bir güvenlik politikasının ilgili sunucu üzerinde uygulanmasıdır. Hardening işlemi, ağa hizmet veren sunuculara uygulanabilmesine ek olarak güvenlik duvarı, saldırı tespit sistemi gibi güvenlik uygulamalarının çalıştığı sistemlere de uygulanabilir.

Bu işlemin yapılmasının amaçları arasında en önemlileri; saldırganların sunucuyu ele geçirmesinin zorlaştırılması ve ele geçirmesi durumunda hareket kabiliyetinin kısıtlanmasıdır. Hardening, tamamen işletim sistemi veya uygulamaya özel olan işlemler dizisinden oluşur. Bu işlemlerden bazıları sunucu üzerinde varolan potansiyel zayıflıkları gidermek, yetki düzenlemeleri yapmak, sistemin çalışma prosedüründe gerekli olmayan bileşenleri eksiltmektir. Yapılabilecek işlemler genel hatlarıyla aşağıda listelenmektedir.

- Üretici Firma veya Yazılım Geliştiricileri tarafından yayınlanan tüm yama ve güncellemelerin belirtildiği şekilde uygulanması gereklidir. Böylece sistemde varolabilecek güvenlik zayıflıkları minimum seviyeye çekilmiş olur.
- Sunucunun vereceği hizmetler önceden belirlenmeli ve bu hizmetlerin sunulması aşamasında gerekli olmayan tüm servisler (ftp, portmap, nfs, telnet vs.) sistemden kaldırılmalıdır. Saldırganların, sunucu için gerekli olmayan hizmetleri ve zayıflıklarını farketmesi , sunucuya erişilebilecek bir arka kapı bulması anlamına gelmektedir. Korunacak sahanın daraltılması, dikkatin gerekli noktalara yoğunlaştırılmasına yardımcı olacaktır.
- İşletim sistemleri üzerinde bulunan kullanıcı sayısı ve yetkileri mümkün olduğunca azaltılmalıdır. Ayrıca doğrulama sistemi olarak harici onaylama sistemleri kullanılmalı (Sertifikalar, S/Key, SecureID, Token vs.) veya düz şifre ile onaylama yapılıyorsa şifre kalitesi ve şifre yaşlandırma politikaları uygulanmalıdır. Saldırganların sisteme yetkisiz erişim istekleri sırasında ilk kullacakları yöntem, sistemdeki zayıf şifrelere sahip kullanıcıları bulmaktır. Harici onaylama yöntemleri ve şifrelerin zor tahmin edilebilir olması yetkisiz erişimi zorlaştırır. Gözden kaçan bir kullanıcı hesabı ile sisteme sızan saldırganın, o kullanıcı haklarıyla sisteme erişebileceği gözönüne alınırsa, sıradan kullanıcıların yetkilerinin ne kadar önem arzettiği daha rahat anlaşılır.
- Dosya sistemi veya donanım üzerinde önemli bileşenlere (özel dizinler, özel programcıklar, güç kaynağı vs.) erişimlerin kısıtlanması ve bu erişimlerin düzenli kontrol edilmesi gereklidir. Dosya sistemi üzerindeki kritik dizinler (/etc, /var, /tmp, c:\windows vs.) üzerinde sadece gerekli olabilecek erişim izinleri bulunmalıdır. Mümkün ise kritik dizinler yalnızca okunabilir şekilde sisteme dahil olmalıdır. Saldırganın sisteme sızabileceği ve bu dizinlerdeki dosyalar üzerinde istediği değişiklikleri yapabileceği gözönüne alınmalıdır. Özel programcıklara (telnet, ping, ftp, tftp, ssh, fdisk vs.) verilen izinlerde, sadece gerekli erişimler doğrultusunda olmalı, mümkün ise bu programcıklar sistemden kaldırılmalıdır. Derleyici/Yorumlayıcılarda (gcc, cc, perl, php vs.) aynı oranda tehlikelidir ve izinleri erişimler doğrultusunda gözden geçirilmeli yada sistemden kaldırılmalıdır. Saldırgan sisteme sızdığında bu araçları kullanarak çeşitli işlemler (ağın haritasının çıkarılması, kötü amaçlı bir yazılımın derlenmesi vs.) yapmak isteyebilir. Donanımların kısıtlanması aynı derecede kritik bir öneme sahiptir. Saldırganın varolan donanımlarda işlemler yapabileceği (com1 portuna bağlı yönlendirici üzerinde değişiklik yapmak, com1 ile iletişimde bulunan güç kaynağına kapanma talimatı vermek vs.) mutlak gözönüne alınmalı ve yetkiler tekrar gözden geçirilmelidir.
- Unix sistemlerinde “suid” ve “sgid” programlar bulunmamalıdır. Bu tür programlarda saldırganın bulabileceği küçük bir zayıflık; saldırganın, programın sahip olacağı (muhtemelen “root”) kullanıcı haklarıyla erişimine izin verecektir. Sistemde, bu tür yetkilerle donatılmış yazılımlar bulunmalı ve bu yetkileri kaldırılmalı yada program gerekmiyorsa silinmelidir.

- Sistemler üzerinde kaydı tutulacak işlemler belirlenmeli, bir izleme politikası oluşturulmalı ve kayıtlar mümkün ise sunucu dışında bir sistemde tutulmalıdır. Saldırıları erken farketmede veya zarar boyutu tespitinde, saldırganların ilk olarak değiştirmek isteyeceği bu raporlar kullanılacaktır.
- Sistemde sunulacak servisler başlatılırken özel bir kullanıcı kullanılmalı ve bu kullanıcının hakları gereklilikler ölçüsünde kısıtlanmalıdır. “root” yada “administrator” kullanıcısı haklarıyla çalışan bir uygulamada bulunabilecek güvenlik zayıflıklarının sonucunda, sistemde çalıştırılabilecek komutlar, bahsi geçen kullanıcıların hakları ile çalışacaktır.
- Windows temelli sistemlerde Netbios/SMB servisi ; eğer gerekmiyorsa (Active Directory, PDC, BDC) kapatılmalıdır. Bu servis çeşitli sebepler ile gerekli ise boş kullanıcının haklarıyla erişim hakları, doğrulama mekanizması gibi kritik ayarlar gözden geçirilmelidir. Windows temelli sistemlerin bilinen en büyük zayıflığı olan bu servis sebebiyle saldırgan, sunucu paylaşımları, kullanıcılar/gruplar, şifre yaşlandırmaları gibi bir çok kritik bilgiye sahip olacak veya bu bilgileri değiştirme hakkı elde edecektir.
- Unix temelli sistemlerde mümkünse, “kernel” ihtiyaçlar doğrultusunda tekrar derlenmeli ve gerekli olabilecek güvenlik yamaları uygulanmalıdır. Varsayılan “kernel”, yerel kullanıcıların yetkilerini yükseltebileceği çeşitli zayıflıkları içerebileceği gibi, uzak kullanıcıların sistemin hizmetini durdurmaya yönelik saldırılarından da etkilenebilir.
- Windows temelli sistemlerde registry kayıtlarındaki yetkilerin elden geçirilmesi ve kritik kayıtların yetkilerinin kısıtlanması gereklidir. Varsayılan kurulumlarda, Windows temelli sistemler, uzaktan registry erişimine izin vermektedirler. Uzaktan registry erişimi mutlak suretle kapatılmalıdır. Registry üzerinde yapılabilecek değişiklikler tüm sistem üzerinde etkili olacağından, bu adım atlanması en tehlikeli adımlardan biridir.

Hardening yapılan sistem üzerinde, tamamlayıcı bazı işlemler yapabilmek için çeşitli yazılımlar üretilmiştir. Bütünlük doğrulama yazılımları ve zayıflık tarama yazılımları, bu yazılım gruplarının önemli örneklerindedir. Bütünlük doğrulama yazılımları sunucu sistemde bulunan önemli dosya ve dizinlerin çeşitli özelliklerini (dosya boyu, yetkileri, değiştirilme tarihi vs.) bir dosya içerisinde kaydederek dosyayı şifrelemektedir. Daha sonraki zamanlarda kontrol amaçlı olarak kullanılacak bu dosyanın sistem üzerinde bulunamaması gereklidir. Düzenli aralıklar ile yapılabilecek bu işlem, dosya sistemindeki değişiklikleri, saldırganın yaptığı işlemlerin neler olduğunu ve bırakılabilecek arka kapıların yerlerini saptamada faydalı olmaktadır. Zayıflık tarama sistemleride, yerel/uzak erişimler ile sunucu üzerinde bulunabilecek, bilinen güvenlik zayıflıklarını taramayı ve raporlamayı sağlar. Düzenli olarak yapılacak taramalar sonucu üretilen bu raporlarda, bulunan güvenlik zayıflıklarının nasıl giderilebileceğide ayrıntılı olarak açıklanmaktadır. Sunucu üzerinde yapılması gereken son işlem olan zayıflık tarama, sistemi son bir gözden geçirme olarakta nitelendirilebilir.

Saldırganların, hedef gözetmeksizin saldırılar düzenlediği internet ortamında, %100 güven ve girilemeyecek sistem kavramlarından söz etmek mümkün değildir. Bu doğrultuda, her türlü hizmet sunucu sistem üzerinde güvenlik önlemleri artırılmalı, saldırganların tüm ağ sistemini ele geçirmesini engelleyecek yapılar kurulmalı ve işleri mümkün olduğunca zorlaştırılmalıdır. Kritik sistemler üzerinde yapılacak her zorlaştırıcı hareket, saldırganları daha kolay farketmeyi veya daha az zarar görmeyi sağlayacaktır.

Fatih Özavcı
Security Analyst

holden@siyahsapka.com
<http://www.siyahsapka.com>
<http://www.dikey8.com>