

Tripwire ile Bütünlük Denetimi

Mücahit Karatekin

(Linux Güvenlik Semineri-1)



Tripwire Nedir?

- Tripwire; bütünlük denetçisidir.
- Sisteminizin bilinen bir durumdaki durumunu saklar(fotoğrafını çeker). Böylece farklılıkları ortaya çıkarmak için dosyaları bu durum bilgisi ile karşılaştırabiliriz.



İki Ana Bileşen: Politika ve VeriTabanı

- Politika:
 - İhlal durumları(beklenmedik değişiklikler) tanımlama kuralları.
 - Tripwire' in fotoğrafını çekmesi gereken tüm dosya ve dizinlerin listesi.
-
-

Bütünlük Denetim Raporu

- VeriTabanı:
 - Politika ile dosya sistemlerini değerlendirerek oluşturulan fotoğrafları tutar.
 - Bu veritabanı ile dosya sistemimiz herhangi bir zamanda karşılaştırılabilir.
 - Tripwire tüm farklılıkları bildirecektir.
-
-

Yapılandırma Dosyası

- Tripwire' in davranışının genel noktalarını denetleyen bir yapılandırma dosyasına sahiptir.
- Veritabanının, politika dosyasının, tripwire çalıştırılabilirinin yerini belirtir.



Site Anahtarı ve Yerel Anahtar

- Tripwire ile ilgili önemli dosyalar müdahalelere karşı şifrelenmiştir.
 - Site anahtarı:
 - Politika dosyası ile yapılandırma dosyası
 - Yerel Anahtar:
 - Veritabanı ve raporları
-
-

Tripwire Üzerinde Tehditler

- Tripwire veritabanı silinebilir.
 - Tripwire şifreleri ele geçirilip politika ve yapılandırma dosyası değiştirilebilir.
 - Tripwire çalıştırılabilirliği kırılabilir ya da müdahale edilebilir.
 - Periyodik kontrollerde ki fırsat penceresi.
-
-

Tripwire' in Yorucu Yanları

- Uzun ve yorucu çıktısı güvenlik ihlallerini bulmayı zorlaştırıyor.
- Kritik dosyalarınızı sık güncelliyorsanız(tavsiye edilen budur) veritabanını da sıkça güncellemek zorunda kalacaksınız.



Tavsiyeler ve Önermeler

- Herhangi bir linux makinesini **bir ağa bağlamadan ve diğer kullanıcılara açmadan önce, Bir Fotoğrafını Alın.**
 - İlk fotoğraf durumun geçerli ve kırılmamış bir fotoğrafı olmak zorundadır, yoksa bir işe yaramaz.
 - Tripwire raporunun çıktısının grafiksel bir arayüze kavuşturulması, kritik değişikliklerin denetim sırasında uyarılarla kullanıcılara gösterilmesi.
-
-

Salt Okunur Bütünlük Denetimi

- Tripwire' in önemli dosyalarını kırılmaya karşı korumak için CD-ROM gibi yazmaya karşı korumalı salt okunur ortamda depolamak.
 - Site anahtarı, yerel anahtar, tripwire ikilisi
 - Veritabanı(?), politika dosyası(?) ve yapılandırma dosyası(?)
 - Saldırılarda silinme olasılığı sebebi ile yedek almak faydalıdır.
 - CD-ROM' a kopyalamadan, tripwire ikilisinin static executable olduğundan emin olalım.
-
-

Yerel ve Site Anahtarlarının Oluşturulması

- #YER=/etc/tripwire
 - #SITE_KEY=\$YER/site.key
 - #LOCAL_KEY=\$YER/'hostname'-local.key
 - **Site anahtarını oluşturalım:**
 - #twadmin --generate-keys --site-keyfile \
\$SITE_KEY
 - #twadmin --generate-keys --local-keyfile \
\$LOCAL_KEY
-
-

Politika ve Yapılandırma Dosyalarının Şifrelenmesi

- #twadmin –create-cfgfile –cfgfile \$YER/tw.cfg
 \ --site-keyfile \$SITE_KEY \$YER/twcfg.txt
 - #twadmin –create-polfile –polfile \$YER/tw.pol
 \ --site-keyfile \$SITE_KEY \$YER/twpol.txt
 - Uygun İzinlerin Ayarlanması
 - cd \$YER
 - chown root:root \$SITE_KEY \$LOCAL_KEY \
 tw.cfg tw.pol
 - chmod 600 \$SITE_KEY \$LOCAL_KEY \
 tw.cfg tw.pol
-
-

Son Ayarlar ve Veritabanının Oluşturulması

- `#cd $YER`
 - `#rm twpol.txt`
 - `#rm twcfg.txt`
 - `#tripwire -init`
-
-

Politika, Yapılandırma ve Veritabanının Görüntülenmesi

- #cd \$YER
 - #twadmin -print-(cfgfile, polfile) > dosya adı
 - #twprint -print-dbfile -dbfile \
/var/lib/tripwire/'hostname'.twd
 - #tripwire -check
 - #tripwire -check -severity 40
-
-

Otomatik Bütünlük Denetimi ve Veritabanını Güncelleme

- **crontab dosyası: /etc**
 - **0 3 * * * /usr/sbin/tripwire -check**
 - **sabaha karşı :) 3:00**
 - **tripwire -update -twrfile \$ LAST_REPORT”**
-
-

Politika Dosyasına Kural Ekleme

- (
 - rulename = "My important files"
 - severity = 100
 -)
 - {
 - /root/Desktop/şifrelerim.txt -> \$(SEC_CRIT);
 - }
 - #tripwire -check -rulename "My important files"
-
-

Kaynaklar

- <http://sourceforge.net/projects/tripwire/>
- Linux Security Cookbook O' Reilly
- Linux Güvenliđi Pusula Yayınları (Türkçe Çevirisi).



Teşekkürler

Gene Kim ve Gene Spafford

-
-
-
- HOŞ OLARAK KALIN !
-
-
-

