YMT311 Bilgi Sistemleri ve Güvenliği

Sızma Belirleme ve Testleri

Bölüm - 8

Prof.Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıkları

- Giriş
- Temel İlkeler
- Temel Sızma Belirleme (Pentest)
- Sızma Belirleme Modelleri
- Mimari
- Sızma Belirleme Sistemlerinin Örgütlenmesi
- Sızmaya Tepki

Giriş

- Bilişim güvenliğinin en önemli konularından biri sızma testleri olmaktadır. Kimi zaman bir zorunluluk, kimi zaman güvenliğe olan gerçek ihtiyaç kurum, kuruluş ve firmaları güvenliklerini sızma testleri yapmaya zorlamaktadır.

Temel İlkeler

- Bir sistemdeki kullanıcıların ve süreçlerin hareketleri, genellikle istatistiksel öngörülen bir örüntüye dayanır.
- Bir sistemdeki kullanıcıların ve süreçlerin, hareketleri, sistemin güvenlik politikasını altüst edecek komut veya komutlar dizini içermez.
- Bir sistemdeki kullanıcıların ve süreçlerin hareketleri, sistemde olan ve süreçlerin hareketlerine kısıtlamalar (olumlu veya olumsuz) getiren belirtimler kümesine uyar.

Temel Sızma Belirleme

- Teknolojik gelişmeler arttıkça, sistemlere karşı saldırılar da otomatikleşmeye başlamıştır.
- Otomatik olarak saldırı gerçekleştirme amacına sahip araçlara “saldırı aracı” denmektedir.

Temel Sızma Belirleme

Rootkit nedir?

Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur. Amacı yayılmak değil bulunduğu sistemde varlığını gizlemektir.

Temel Sızma Belirleme

- **Rootkit nasıl kurulur/bulaşır?**

Tipine bağlı olmakla birlikte genelde erişim yetkiniz dahilinde sisteminize kurabileceğiniz rootkit'ler bulmanız mümkündür. Bunun dışında güvenilir bir kaynaktan geldiğine inandığınız bir programı haddinden fazla yetki ile çalıştırmak (Ör: root veya root yetkili bir wheel grubu üyesi) zararlı bir rootkit'in sisteme kurulmasına sebep olur. Aynı şekilde çok kullanıcılı bir sistemde kernel vs açıkları kullanılarak sistemde root yetkisi kazanıp rootkit kurulması en yaygın görülen bulaşma şeklidir.

Temel Sızma Belirleme

- **Rootkit nasıl temizlenir?**

Rootkit çalışırken altında çalıştıracağınız her program rootkit'in yetenekleri doğrultusunda onun verdiği bilgiler ile sistemden aldığı bilgileri ayırd edemez. Dolayısıyla gerçekte hangi dosyaları değiştirdiği, kernele hangi modülü yüklediği, dosya sisteminin neresinde kayıtlı olduğu, hangi ağ servisi üzerinde "sniffer" şeklinde dinleme yaparak uygun komutla harekete geçeceğini tespit etmek kolay değildir. Dolayısıyla rootkit bulaşmış bir sistemin en güzel temizliği içinden hiçbir BINARY dosya alınmadan sadece verilerin alınarak tamamen baştan kurulmasıdır.

Temel Sızma Belirleme

- **Rootkit nasıl tespit edilir?**

Belli zamanlarda en temel komutların ve muhtemel rootkit bulaşma noktalarının **"hash"** değerlerinin saklanarak bunların daha sonra kontrol edilmesi gibi metodlar olmasına rağmen yukarıda belirttiğim gibi rootkit bulaşmış bir sistemin vereceği bilginin gerçekliği bulaşan rootkit'in yeteneğine bağlıdır. Yine de sistemi bir CD ile açarak bu kontrolleri yapan programlar olduğu gibi bu "hash" alma ve kontrol etme işlemi CD ile açıldıktan sonra elle de yapılabilir.

Temel Sızma Belirleme

- **Rootkit'ten nasıl korunulur?**
- Linux ve türevleri için konuşursak kullanılan dağıtımın resmi paket dağıtım sistemi dışına çıkmamak pek çok sorunu çözecektir. Bu paket dağıtım sistemlerinin ele geçirilmesi veya zehirlenmesi ihtimali her zaman mevcut olacaktır.

- Genel kaide olarak dağıtımın resmi paket depoları ile kullanılacak programın resmi internet sitesinden alacağınız kaynak kodlar sizi bir derece koruyacaktır.

- Eğer diğer insanların erişimine açık bir sistem kullanıyorsanız güncellemeleri zamanında yapmak ve sık sık kontrol etmek de unutulmaması gereken bir işlemdir.

Temel Sızma Belirleme

- **Rootkit'in zararı nedir?**

Rootkitin girdiği bilgisayarınız tamamen dışarıdan kontrol edilebilir hale gelecektir. Tipine bağlı olarak ayrı bir "güvenlik duvarı" bile size koruyamayabilir. (İçeriden dışarıya sanki bir web sitesi açar gibi karşı tarafa bağlanan rootkitler). Aynı bilgisayarda yüklü bir güvenlik duvarı ise muhtemelen rootkitin yeteneği ile ters orantılı olarak sizi koruyabilir.

Temel Sızma Belirleme

- Sisteme sızan kötü niyetli kişiler, Rootkit, Trojan veya özel geliştirilmiş araçlar kullanarak sistem kayıtları değiştirilebilir. Böylece hedef bir sistem için veri toplama aşamasıyla başlayan saldırı planı, izleri silme ile sona ermiş olur.
- Ağ dinleme programına ek olarak programın varlığının sistemden gizlenmesi için bazı sistem komutlarının değiştirilmiş versiyonları da sisteme kurulur.
- *netstat, ps, ls, du, ifconfig, login*, ...v.b.

Temel Sızma Belirleme

- Saldırı araçları temel olarak sızma belirlemenin doğasını etkilemez.
- Bütün izler temizlenemez.
- Genel olarak sistemin zarar görebilecek özelliklerinden yararlanmak için komutların normal kullanımlarının dışında anormal olarak kullanılmaları gerekir.

Temel Sızma Belirleme

- Güvenlik ihlalleri ancak anormallikler takip edilerek belirlenebilir.
- Bu anormallikler;
  - Olağanın dışında hareket etme (anomali belirleme)
  - İçeri sızmayı sağlayan süreç hareketleri (kural tabanlı belirleme)
  - Belirlirtimlerin dışında hareket eden yetkili progamlar (belitim-tabanlı belirleme)

Temel Sızma Belirleme

- Bu belirleme işlemlerini yapabilen sistemlere Sızma Belirleme Sistemleri (SBS) denir.
- Amaçlar:
  - Geniş çeşitlilikte sızmaları tespit etmek. İçeriden veya dışarıdan gelebilecek sızmaları belirlemek.

Temel Sızma Belirleme

- Zaman ayarlamalı sızma belirlemek.
- Yapılan analizi en kolay anlaşılabilecek şekilde sunmak.
- Kusursuz bilgi vermek.
  - “yanlış pozitif”
  - “yanlış negatif”

Sızma Belirleme Modelleri

- Sızma belirleme modeli bir dizi durumu veya hareketi sınıflandırarak, yada durum veya hareketleri tanımlayarak iyi (sızma yok) yada kötü (olası sızma) olarak belirtir.
- Pratikte bu modeller birbirleriyle içiçe geçmiş şekillerde de kullanılabilir.

Sızma Belirleme Modelleri

- Anomali Modeli:
  - Beklenmeyen davranışın olası bir sızmanın kanıtı olacağı varsayımı kullanılır.
  - Anomali belirleme sistemleri sistemin tanım kümesindeki eylemleri davranışlarıyla ve beklenen davranışlarıyla karşılaştırarak tespitler yaparlar.

Anomali Belirleme

- Üç çeşit istatiksel yöntem tanımlanmıştır
  - Eşik metriği
  - İstatiksel momentler
  - Markov modelleri

Kural Tabanlı Sızma Belirleme

- Herhangi bir komut dizisinin önceden bilinen ve sistemin güvenlik politikasını ihlal edecek işlemler yapıp yapmadığını tespit eder ve potansiyel sızmaları raporlar.
- Sistemin zarar görebilecek yerlerinin ve buralara karşı yapılabilecek potansiyel saldırıların bilgisinin önceden bilinmesi gerekir.
- Bu sistemler kural kümesinde bulunmayan saldırılara müdahale edemezler.

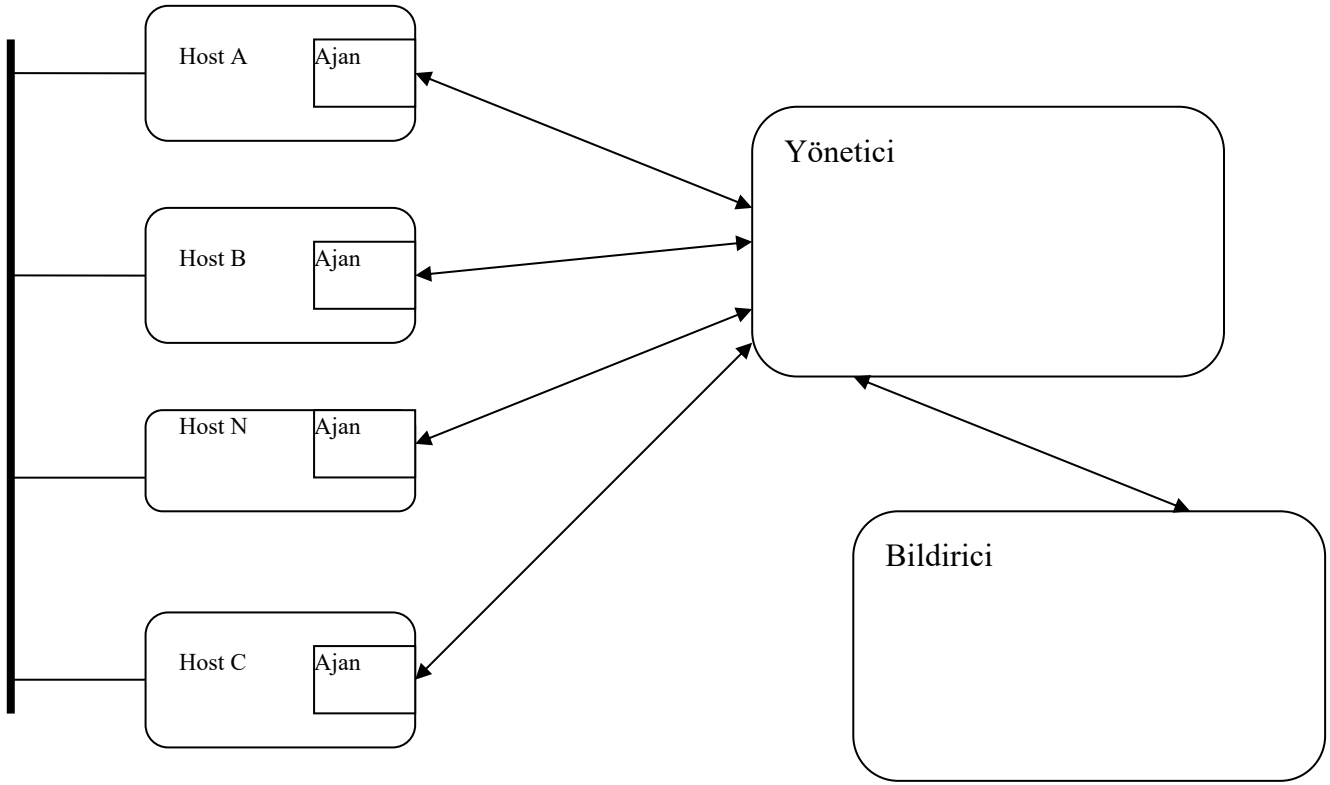
Belirtim Tabanlı Sızma Belirleme

- Bir dizi komutun bir programın yada sistemin çalışma şekline zarar verip vermediğini belirler.
- Sistemin güvenlik durumunu değiştirebilecek programların belirlenmesi ve kontrol edilmeleri gerekmektedir.

Belirtim Tabanlı Sızma Belirleme

- Yeni bir yaklaşım.
- Sistemde ne olabileceği şekillendirilir.
- Bilinmeyen saldırılara karşı çözüm.
- Zor kısmı; belirtimlerinin çıkarılması gereken programları iyi seçme.

Mimari


Host A
Ajan
Host B
Ajan
Host N
Ajan
Host C
Ajan
Yönetici
Bildirici

Ajan

- Veri kaynaklarından bilgi toplar.
- Anında gönderme – Önişlemeli gönderme
- Yönetici potansiyel bir saldırıdan şüphelenmesi halinde ajanların çalışma şekillerini değiştirmelerini sağlayabilir.
- Tek bir konak, birçok konak, ağ.

Ajan

- Konak Tabanlı Bilgi Toplama
  - Sistem ve uygulama kayıtları üzerinde çalışırlar.
  - Olabildiğince sade bir tasarım.
- Ağ Tabanlı Bilgi Toplama
  - Ağdaki çeşitli araçlardan ve yazılımlardan faydalanırlar.
  - İçerik incelemesi
  - Yerleştirilme yerleri iyi seçilmeli

Yönetici

- Analiz motoru ile herhangi bir saldırı veya saldırı başlangıcı olup olmadığını kontrol eder.
- Bir veya birden fazla analiz modeli kullanabilir.
- Ayrı bir sistem üzerinde bulunur.
- Birçok yönetici üzerinde çalıştıkları kural kümelerini ve profilleri değiştirebilme özeliğine sahiptir.

Bildirici

- Yöneticiden aldığı bilgilere göre hareket eder.
- Sistem yöneticisine bir saldırının yapılmakta olduğunun haber vermek.
- Saldırıya karşılık vermek.

Sızma Belirleme Sistemlerinin Örgütlenmesi

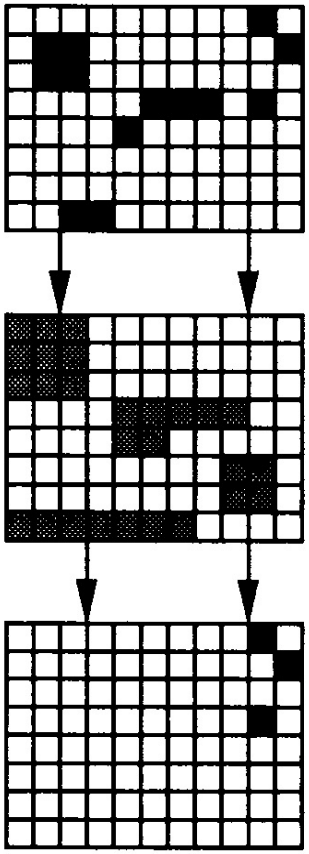
Üç temel yaklaşım var

- Ağ Trafiğini İzlemek (NSM)
- Konakları ve Ağları Birlikte İzlemek (DIDS)
- Özerk Aracılar Kullanmak

Ağ Trafiğini Sızmalara Karşı İzlemek

- Kaynak, varış ve hizmet üçlüsü izlenir.
- Elde edilen bilgiler üç eksene yerleştirilerek bir matris oluşturulur.
- Beklenen değerler matrisi ile maskelenerek terslikler ortaya çıkarılır.
- Matrisler sıradüzeni ile aşım engellenir.
- *İmzalar* da yapıya eklenebilir.

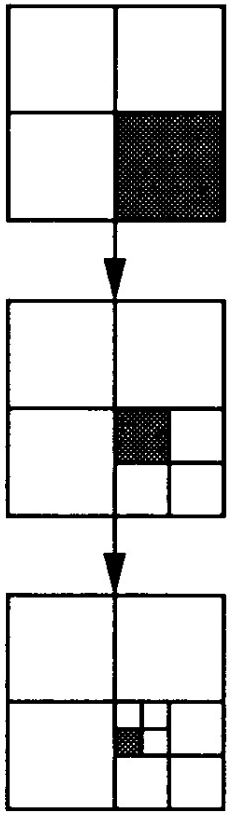
Ağ Trafiğini Sızmalara Karşı İzlemek



current data

data mask

Anomalous data



Searching from a coarse grain matrix analysis to a fine grain analysis.

Konakları ve Ağı Birlikte İzlemek

- Konakların ve ağın izlenmesini içiçe koyarak ayrı ayrı izlemeyle belirlenemeyen saldırıları belirleyebilir.
- *Director* adında merkezi bir uzman sistem kullanır.
- Uzman sistemnin altı katmanlı bir yapısı vardır.
- DIDS üzerine kurulan GrIDS sıradüzensel bir yapıyla bu yaklaşımın geniş alan ağlarına uygulanmasını sağlar.

Özerk Aracılar

- *Director*, tekil hata noktası oluşturur.
- Bu yaklaşımda uzman sistem her bir ayrı bir izleme ile görevli aracı parçalara ayrılır.
- Parçalardan biri çalışmazsa diğerleri onun boşluğunu doldurabilir.
- Parçalardan birine yapılan saldırı tüm ağın güvenliğini etkilemez.
- Yapısı gereği ölçeklenebilir.

Sızmaya Tepki

Sızmanın gerçekleştiği algılandıktan sonra korunan ağı en az hasarla eski durununa getirmek için sızmaya karşı tepkiler geliştirilmelidir.

- Engelleme
- Sızma Yönetimi

Engelleme

İdeal şartlarda sızma denemeleri henüz başında engellenir.

- *Hapsetme*, saldırganları saldırılarının başarılı olduğuna inandırarak sınırlı bir alana sıkıştırmaktır. Hapiste gerçek dosya yapısına çok benzer bir dosya yapısı kullanılır, iyice kısıtlanmış saldırganın davranışları böylece gözlenebilir.
- Bu kavram, ayrıca, çok güvenlik seviyeli ağlarda da kullanılabilir.

Engelleme

- Bir başka örnekte sistem çağrılarında bir terslik olması durumunda sistem çağrıları özellikle geciktiriliyor.
- Normal kullanıcılar bundan etkilenmezken, saldırganlar kısa sürede iki saati aşkın bekleme sürelerine erişiyorlar.

Sızma Yönetimi

- Bir sızma gerçekleştiğinde ağı korumak, korunan ağı eski durumuna getirmek ve ilkeler doğrultusunda tepkiler vermektir.
- Altı aşamadan oluştuğu düşünülebilir.

Sızma Yönetimi

- **Hazırlık** aşamasında henüz bir saldırı belirlenmemiştir. Gerekli ilkeleri ve düzenekleri kurma aşamasıdır.
- **Tanıma aşaması,** bundan sonra gelen aşamaları ateşleyen aşamadır.
- **Yakalama aşaması** hasarı en aza indirmek içindir.
- **Temizleme aşaması** saldırıyı durduran ve benzer saldırıları engelleyen aşamadır.
- **Kurtarma aşaması**, ağı eski durumuna getimek içindir.
- **Kovalama aşaması** saldırgana karşı alınacak tepkileri, saldırganın davranışlarının incelenmesini ve kazanılan bilgilerin ve derslerin kaydedilmesini içerir.

Sızma Yönetimi - Yakalama

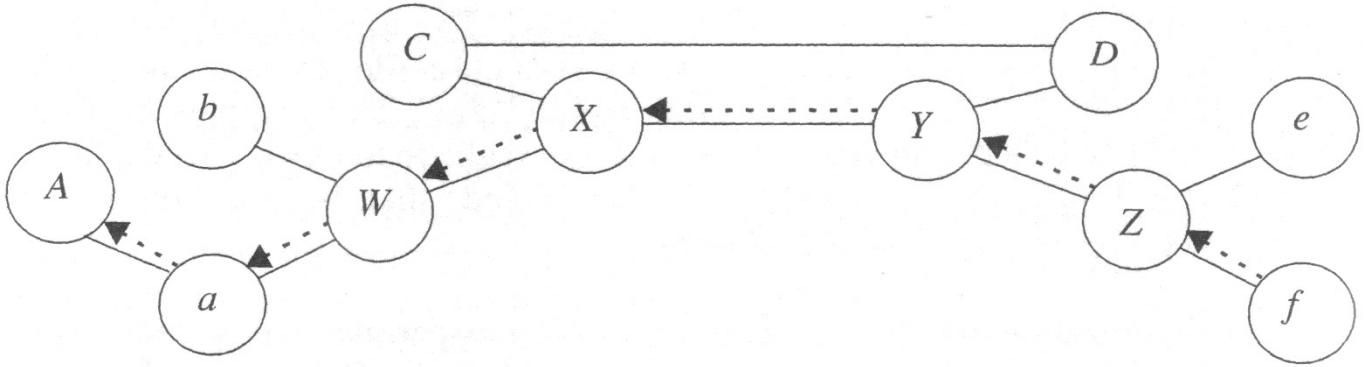
- Pasif izleme ve erişimi sınırlandırmak olarak ikiye ayrılabilir.
- Pasif izleme, basitçe saldırgan davranışlarının kaydedilmesidir. Saldırgan davranışları hakkında bilgi verir.
- Erişimi sınırlandırmak, saldırganın amacına ulaşmasını engellerken, ona en küçük alanı vermektir.
  - Bal küpleri yaklaşımında saldırganın ilgisini çekecek sahte hedeflerle gerçek hedefe ulaşması engellenebilir. sistem bir saldırı belirlediğinde saldırganı küpe düşürmeye çalışır.

Sızma Yönetimi - Temizleme

- Saldırıyı durdurmak anlamına gelir. En basiti saldırganın sistemye tüm erişimini kesmektir. (Ağ kablosunu çıkarmak?)
- Sık kullanılan bir yaklaşım örtülerle olası hedeflerin etrafını sarmaktır. Örtüler çoğunlukla işletim sisteminin çekirdeğine gömülür.

Sızma Yönetimi - Temizleme

- Güvenlik duvarları saldırganın bağlantısını hedefe gelmeden önce süzmek için kullanılabilir.
- IDIP (Intrusion Detection and Isolation Protocol) kullanılarak ağda bir sızma olduğunda komşu ağlara haber verilebilir. Böylece komşu ağlar da saldırının süzülmesine yardım edebilirler.



Sızma Yönetimi - Kovalama

- Saldırının yerini belirlemek gerekecektir. İki ayrı yaklaşım önerilebilir.
- İzbasma (Thumprinting)
  - Olabildiğince az yer kaplamalı.
  - İki bağlantının içeriği farklıysa farklı izleri olmalı.
  - İletişim hatalarından etkilenmemeli.
  - Toplanabilir olmalı.
  - Hesaplaması ve karşılaştırması ucuz olmalı.

Sızma Yönetimi - Kovalama

- IP başlığı işaretleme (IP header marking)
  - Paket seçimi gerekirci ya da rastgele olabilir. Rastgele seçim daha ekonomik ve güvenlidir.
  - Paket işaretleme içsel ya da genişletilebilir olabilir. İçsel işaretlemede başlığın boyu değişmez.

Sızma Yönetimi - Kovalama

- Karşı saldırı yasal ya da teknik olabilir.
  - Yasal saldırı uzun zaman gerektirir. Kanunlar yerli yerinde değil ve oldukça karışık. Ayrıcı yabancı ülkelerden saldırı gelirse uluslararası kanunlar yetersiz.
  - Teknik saldırı masumlara zarar verebilir. Saldırganlar masum bir ağı ele geçirdikten sonra orayı üs olarak kullanmış olabilirler.
  - Kendi ağımızdaki haberleşmeye zarar verebilir.
  - Paylaşılan bir ağın her ne sebeple olursa olsun saldırı için kullanılması etik değil.
  - Karşı saldırı da saldırı gibi dava edilebilir.

Sonuç

- Bilgi Güvenliği **ürün veya hizmet değildir.**
- İnsan faktörü, teknoloji ve eğitim unsurları üçgeninde **yönetilmesi zorunlu olan karmaşık süreçlerden oluşan, süreklilik arz eden bir süreçtir.**
- Üç unsur arasında tamamlayıcılık olmadığı sürece **yüksek seviyede bir güvenlikten bahsedebilmek mümkün değildir.**
- Yüksek seviyede E-Devlet güvenliğinden bahsedebilmek için **Kurumsal ve Bireysel anlamda Bilgi Güvenliğinin gerekleri yerine getirilmelidir.**

Sorular

Kaynaklar