MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(8. Hafta)

İçerik

- 2.Bilgisayar Güvenliği Teknolojisi ve İlkeleri
  - 2.1 Şifreleme Araçları
  - 2.2 Kullanıcı doğrulama
  - 2.3 Giriş/Erişim Kontrolu
  - 2.4 Veritabanı ve Veri Merkezi Güvenliği
  - 2.5 Kötü amaçlı yazılımlar
  - 2.6 Hizmet Reddi Saldırıları
  - 2.7 İzinsiz giriş tespiti
  - 2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.7 İzinsiz Giriş Tespiti

2.7. İçerik

- Davetsiz Misafirler
- İzinsiz giriş tespiti
- Analiz Yaklaşımları
- Ana Bilgisayar Tabanlı Saldırı Tespiti
- Ağ Tabanlı Saldırı Tespiti
- Dağıtılmış veya Hibrit İzinsiz Giriş Tespiti
- İzinsiz Giriş Tespiti Değişim Formatı
- Bal küpleri (Honeypots)
- Örnek Sistem: Snort

Davetsiz misafir sınıfları – Siber Suçlular

- Mali kazanç amacı olan bir organize suç grubunun bireyleri veya üyeleri
- Faaliyetleri şunları içerebilir:
    - Kimlik Hırsızlığı
    - Finansal kimlik bilgilerinin çalınması
    - Kurumsal casusluk
    - Veri hırsızlığı
    - Veri fidyesi
- Tipik olarak genç, genellikle Web'de iş yapan Doğu Avrupalı, Rus veya Güneydoğu Asyalı bilgisayar korsanlarıdır.
- İpuçları ve verileri değiş tokuş etmek ve saldırıları koordine etmek için yeraltı forumlarında buluşuyorlar.

Davetsiz misafir sınıfları – Aktivistler

- Genellikle içeriden biri olarak çalışan bireyler veya sosyal veya politik nedenlerle motive olan daha büyük bir dış saldırgan grubunun üyeleridir.
- Hacktivists o larak da bilinir
- Beceri seviyesi genellikle oldukça düşüktür
- Saldırılarının amacı genellikle amaçlarını tipik olarak aşağıdakiler aracılığıyla tanıtmak ve duyurmaktır:
    - Web sitesi tahrifatı
    - Hizmet reddi saldırıları
    - Olumsuz tanıtım veya hedeflerinin tehlikeye atılmasıyla sonuçlanan verilerin çalınması ve dağıtılması
    - Anonymous and LulzSec

Davetsiz misafir sınıfları – Devlet Destekli Kuruluşlar

Casusluk veya sabotaj faaliyetleri yürütmek için hükümetler tarafından desteklenen bilgisayar korsanı gruplarıdır

Bu sınıftaki herhangi bir saldırının gizli doğası ve uzun süreler boyunca devam etmesi nedeniyle Gelişmiş Israrlı Tehditler (APT'ler) olarak da bilinir.

Çin'den ABD'ye, İngiltere'ye ve onların istihbarat müttefiklerine kadar geniş bir yelpazedeki ülkeler tarafından bu faaliyetlerin yaygın niteliği ve kapsamı vardır

Davetsiz misafir sınıfları – Diğerleri

- Daha önce listelenenlerden farklı motivasyonlara sahip bilgisayar korsanlarıdır
- Teknik başarı veya akran grubu itibarı ile motive olan klasik bilgisayar korsanlarını içine alır
- Yeni arabellek taşması güvenlik açıkları kategorilerini keşfetmekten sorumlu olanların çoğu, bu sınıfın üyeleri olarak kabul edilebilir.
- Saldırı araç setlerinin geniş kullanılabilirliği göz önüne alındığında, sistem ve ağ güvenliğini keşfetmek için bunları kullanan bir "hobi bilgisayar korsanları" havuzu vardır.

Davetsiz Misafir Beceri Seviyeleri – Çırak

- Öncelikle mevcut saldırı araç setlerini kullanan, minimum teknik beceriye sahip bilgisayar korsanlarıdır
- Suçlu ve aktivist saldırganlar da dahil olmak üzere muhtemelen en fazla sayıda saldırganı oluşturur
- Bilinen mevcut araçları kullanmaları göz önüne alındığında, bu saldırganlara karşı savunması en kolay olanlardır.
- Mevcut scriptleri (araçları) kullanmaları nedeniyle "script-kiddies" olarak da bilinirler.

Davetsiz Misafir Beceri Seviyeleri – Kalfa

- Yeni keşfedilen veya satın alınan güvenlik açıklarını kullanmak için saldırı araç setlerini değiştirmek ve genişletmek için yeterli teknik beceriye sahip bilgisayar korsanlarıdır
- Halihazırda bilinenlere benzer yeni güvenlik açıklarını bulabilirler.
- Bu tür becerilere sahip bilgisayar korsanları muhtemelen tüm davetsiz misafir sınıflarında bulunur.
- Araçları başkaları tarafından kullanılmak üzere uyarlarlar

Davetsiz Misafir Beceri Seviyeleri – Usta

- Yepyeni güvenlik açıkları kategorileri keşfedebilen üst düzey teknik becerilere sahip bilgisayar korsanlarıdır
- Yeni güçlü saldırı araçları yazarlar
- İyi bilinen klasik bilgisayar korsanlarından bazıları bu seviyededir.
- Bazıları devlet destekli kuruluşlar tarafından istihdam edilmektedir.
- Bu saldırılara karşı savunma yapmak en zor olanıdır.

İzinsiz Giriş Örnekleri

NIST SP 800-61 (Computer Security Incident Handling Guide , Ağustos 2012) aşağıdaki izinsiz giriş örneklerini listeler:

- Bir e-posta sunucusunun uzaktan kök güvenliği ihlali
- Web sunucusu tahrifatı
- Parolaları tahmin etme/kırma
- Kredi kartı numaraları içeren veritabanlarının kopyalanması
- Hassas verileri yetkilendirme olmadan görüntüleme
- Paket dinleyicisi çalıştırma
- Korsan yazılım dağıtma
- Dahili ağa erişmek için güvenli olmayan bir modem kullanma
- Bilgi almak için bir yöneticiyi taklit etmek
- Açık bırakılmış bir iş istasyonu kullanma

Davetsiz misafir davranışı

Hedef belirleme ve bilgi toplama	**İlk erişim**	**Ayrıcalığı yükseltme**
Bilgi toplama veya sistemin istismarı	**Erişimi sürdürme**	**İzleri kapatma**

Saldırgan Davranış Örnekleri – Hedef belirleme ve bilgi toplama

- Kurumsal yapı, personel, kilit sistemler ve kullanılan belirli Web sunucusu ve işletim sisteminin ayrıntıları hakkında bilgi için kurumsal web sitesini keşfeder.
- Dig, host ve diğerleri gibi DNS arama araçlarını kullanarak hedef ağ hakkında bilgi toplar; ve WHOIS veritabanını sorgular.
- NMAP gibi araçları kullanarak erişilebilir hizmetler için ağın haritasını çıkarır.
- Müşteri hizmetleri iletişim kişisine sorgu e-postası gönderir, posta istemcisi, sunucu ve kullanılan işletim sistemi hakkında bilgi için yanıtı ve ayrıca yanıt veren kişinin ayrıntılarını inceler.
- Potansiyel olarak savunmasız hizmetleri belirler, örneğin, savunmasız Web CMS.

Saldırgan Davranış Örnekleri – İlk erişim

- Bir kullanıcının Web içerik yönetim sistemi (CMS) parolasını kaba kuvvetle (tahmin edir) bulur.
- Sistem erişimi kazanmak için Web CMS eklentisindeki güvenlik açığından yararlanır.
- Önemli kişilere Web tarayıcı istismarına bağlantı içeren hedef odaklı kimlik avı e-postası gönderir.

Saldırgan Davranış Örnekleri – Ayrıcalığı yükseltme

- Yerel istismara sahip uygulamalar için sistemi tarar.
- Yükseltilmiş ayrıcalıklar elde etmek için savunmasız herhangi bir uygulamadan yararlanır.
- Yönetici parolalarını yakalamak için algılayıcıları yükler.
- Ayrıcalıklı bilgilere erişmek için yakalanan yönetici parolasını kullanır.

Saldırgan Davranış Örnekleri – Bilgi toplama veya sistemin istismarı

- İstenen bilgiler için dosyaları tarar.
- Çok sayıda belgeyi harici depoya aktarır.
- Ağdaki diğer sunuculara erişmek için tahmin edilen veya yakalanan parolaları kullanır.

Saldırgan Davranış Örnekleri – Erişimi sürdürme

- Daha sonra erişim için uzaktan yönetim aracını veya arka kapılı rootkit'i kurar.
- Daha sonra ağa erişmek için yönetici şifresini kullanır.
- Sistemde çalışan anti-virüs veya IDS programlarını değiştirir veya devre dışı bırakır.

Saldırgan Davranış Örnekleri – İzleri kapatma

- Sistemde yüklü dosyaları gizlemek için rootkit'i kullanır.
- İzinsiz giriş sırasında oluşturulan girişleri kaldırmak için log dosyalarını düzenler.

Tanımlar

- Güvenlik İhlalleri:

  Bir sistemin güvenlik mekanizmalarını yetkisiz bir şekilde aşma eylemidir

- İzinsiz giriş tespiti:

Olası güvenlik ihlallerini belirlemek için bir bilgisayar veya ağ içindeki çeşitli alanlardan bilgi toplayan ve analiz eden bir donanım veya yazılım işlevidir.

Saldırı Tespit Sistemi (IDS)

- Ana bilgisayar tabanlı IDS (HIDS)
  - Şüpheli etkinlik için tek bir ana bilgisayarın özelliklerini izler
- Ağ tabanlı IDS (NIDS)
  - Ağ trafiğini izler ve şüpheli etkinliği belirlemek için ağ, aktarım ve uygulama protokollerini analiz eder
- Dağıtılmış veya hibrit IDS
  - Saldırı etkinliğini daha iyi tanımlayabilen ve bunlara yanıt verebilen merkezi bir analizörde, genellikle hem ana bilgisayar hem de ağ tabanlı bir dizi sensörden gelen bilgileri birleştirir.

Üç mantıksal bileşenden oluşur:

- **Sensörler (algılayıcılar) - veri toplar**
- **Analizörler - izinsiz giriş olup olmadığını belirler**
- **Kullanıcı arabirimi - çıktıyı görüntüler veya sistem davranışını kontrol etmek için kullanılır**

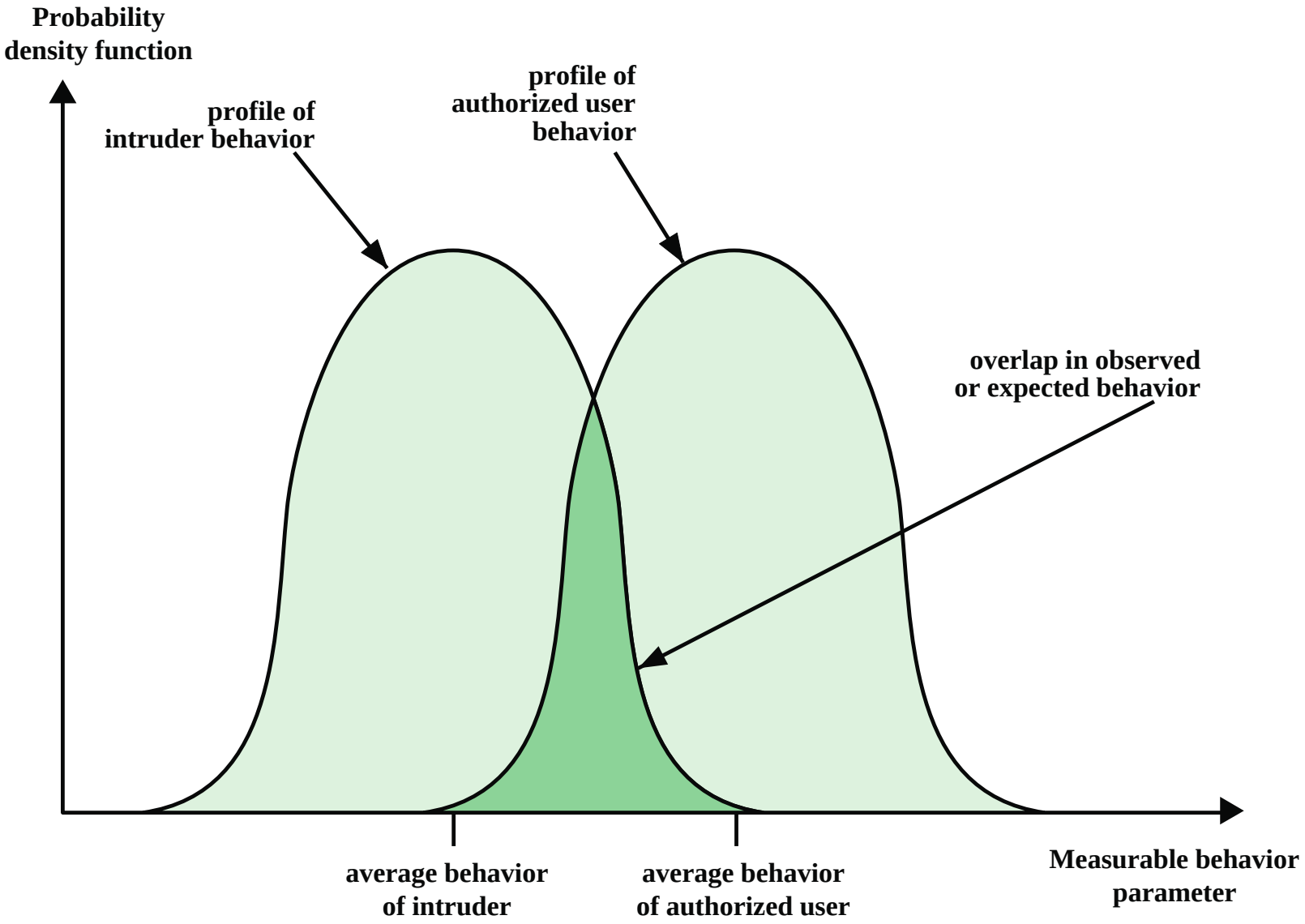

Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

IDS Gereksinimleri

Asgari düzeyde insan gözetimi ile sürekli çalışır

Hata toleranslı olur. Sistem çökmelerinden kurtulabilmelidir

Yıkıma dirençlidir. IDS kendini izleyebilmeli ve bir saldırgan tarafından değiştirilip değiştirilmediğini tespit edebilmelidir

Sisteme minimum bir ek yük yükler

Sistem güvenlik politikalarına göre yapılandırılır

Zaman içinde sistemlerdeki ve kullanıcı davranışlarındaki değişikliklere uyum sağlar

Çok sayıda sistemi izlemek için ölçeklendirilir

Hizmetin zarif bir şekilde bozulmasını sağlar. IDS'nin bazı bileşenleri herhangi bir nedenle çalışmayı durdurursa, geri kalanı mümkün olduğunca az etkilenir

Dinamik yeniden yapılandırmaya izin verir. IDS'yi yeniden başlatmaya gerek kalmadan yeniden yapılandırma yeteneği olur.

Analiz Yaklaşımları

Anomali tespiti

- Belirli bir süre boyunca yasal kullanıcıların davranışlarına ilişkin verilerin toplanmasını içerir.
- Mevcut gözlemlenen davranış, bu davranışın yasal bir kullanıcıya mı yoksa davetsiz misafire mi ait olduğunu belirlemek için analiz edilir.

İmza/Sezgisel algılama

- Geçerli davranışla karşılaştırılan bir dizi bilinen kötü amaçlı veri modeli veya saldırı kuralı kullanır
- Kötüye kullanım tespiti olarak da bilinir
- Yalnızca kalıpları veya kuralları olan bilinen saldırıları tanımlayabilir

Anomali tespiti

Çeşitli sınıflandırma yaklaşımları kullanılır:

İstatistiksel	Bilgiye dayalı	Makine öğrenmesi
• Gözlemlenen metriklerin tek değişkenli, çok değişkenli veya zaman serisi modellerini kullanarak gözlemlenen davranışın analizidir	• Yaklaşımlar, gözlemlenen davranışı meşru davranışı modelleyen bir dizi kurala göre sınıflandıran bir uzman sistem kullanır	• Yaklaşımlar, veri madenciliği tekniklerini kullanarak eğitim verilerinden uygun bir sınıflandırma modelini otomatik olarak belirler

Makine öğrenmesi

Farklı başarı oranlarına sahip çeşitli makine öğrenimi yaklaşımları denenmiştir.

Bayes ağları	Markov modelleri	Sinir ağları	Bulanık Mantık	Genetik algoritmalar	Kümeleme ve aykırı değer tespiti
• Gözlemlenen metrikler arasındaki olasılıksal ilişkileri kodlar	• Geçiş olasılıklarıyla birbirine bağlı, bazıları muhtemelen gizli olan durum kümeleriyle bir model geliştiriir	• Gözlenen verileri sınıflandıran nöronlar ve aralarındaki sinapslarla insan beyninin işleyişini simüle eder	• Akıl yürütmenin yaklaşık olduğu ve belirsizliği barındırabileceği bulanık küme teorisini kullanır	• Evrimsel biyolojiden ilham alan teknikleri kullanır	• Gözlemlenen verileri, bazı benzerlik veya mesafe ölçülerine göre kümeler halinde gruplandırır ve ardından sonraki verileri bir kümeye ait veya bir aykırı değer olarak tanımlar

İmza veya Sezgisel Tespit

İmza yaklaşımları

- **Bilinen kötü amaçlı veri kalıplarından oluşan geniş bir koleksiyonu, bir sistemde depolanan veya bir ağ üzerinden aktarılan verilerle eşleştirir**
- **İmzaların, kötü amaçlı verilerin yeterince büyük bir kısmını tespit etmeye devam ederken yanlış alarm oranını en aza indirecek kadar büyük olması gerekir**
- **Anti-virüs ürünlerinde, ağ trafiği tarama proxy'lerinde ve NIDS'de yaygın olarak kullanılır**

Kural tabanlı buluşsal/sezgisel tanımlama

- **Bilinen sızmaları veya bilinen zayıflıklardan yararlanacak sızmaları belirlemek için kuralların kullanılmasını içerir**
- **Davranış yerleşik kullanım kalıplarının sınırları içinde olsa bile şüpheli davranışı tanımlayan kurallar da tanımlanabilir**
- **Tipik olarak kullanılan kurallar belirlidir**
- **SNORT, kural tabanlı bir NIDS örneğidir**

Ana Bilgisayar Tabanlı Saldırı Tespiti (HIDS)

- Savunmasız veya hassas sistemlere özel bir güvenlik yazılımı katmanı ekler
- Şüpheli davranışı tespit etmek için etkinliği izler
  - Birincil amaç izinsiz girişleri tespit etmek, şüpheli olayları loga kaydetmek ve uyarılar göndermektir.
  - Hem harici hem de dahili izinsiz girişleri tespit edebilir
- Anomali veya imza ve buluşsal yaklaşımları kullanabilir

Veri Kaynakları ve Sensörler

İzinsiz giriş tespitinin temel bir bileşeni, verileri toplayan sensördür

Yaygın veri kaynakları şunları içerir:

- Sistem çağrı izleri
- Denetim (log dosyası) kayıtları
- Dosya bütünlüğü sağlama toplamları
- Registery erişimi

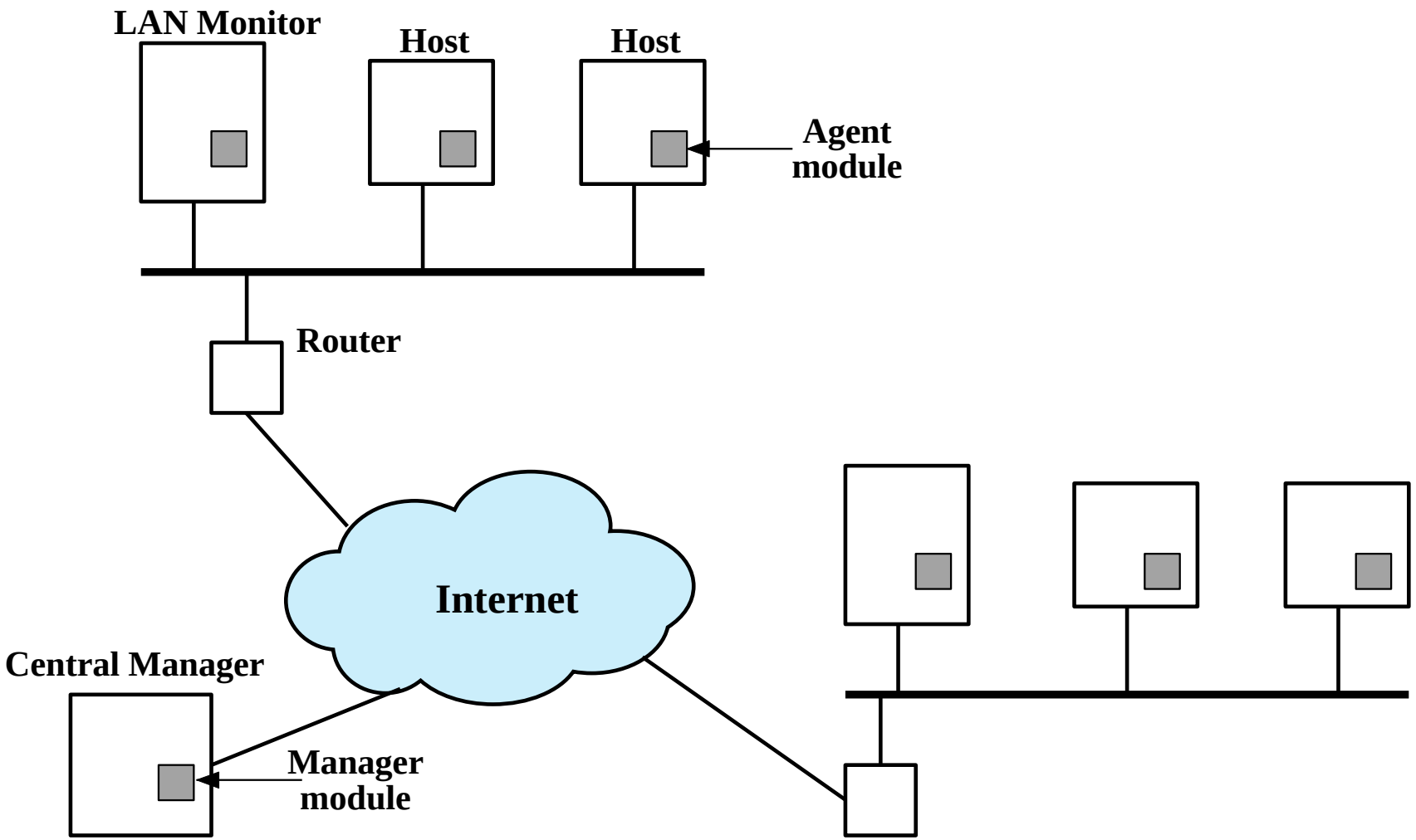

Figure 8.2 Architecture for Distributed Intrusion Detection

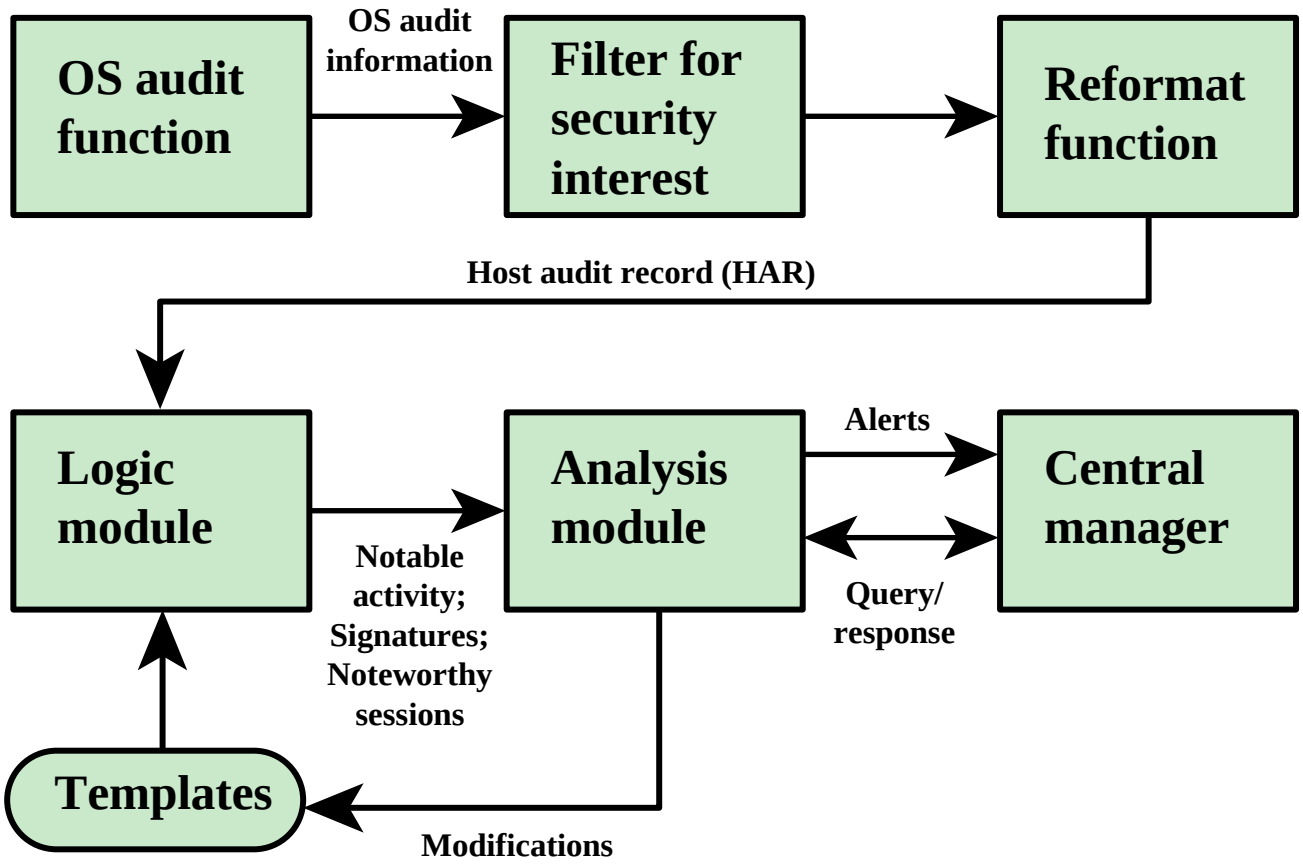

Figure 8.3 Agent Architecture

Ağ Tabanlı Saldırı Tespiti (NIDS)

Bir ağ üzerinde seçilen noktalardaki trafiği izler

Trafik paketini paket bazında gerçek veya gerçek zamana yakın olarak inceler

Ağ, aktarım ve/veya uygulama düzeyinde protokol etkinliğini inceleyebilir

Bir dizi sensörden, NIDS yönetim işlevleri için bir veya daha fazla sunucudan ve insan arayüzü için bir veya daha fazla yönetim konsolundan oluşur

Trafik paternlerinin analizi sensörde, yönetim sunucusunda veya ikisinin bir kombinasyonunda yapılabilir

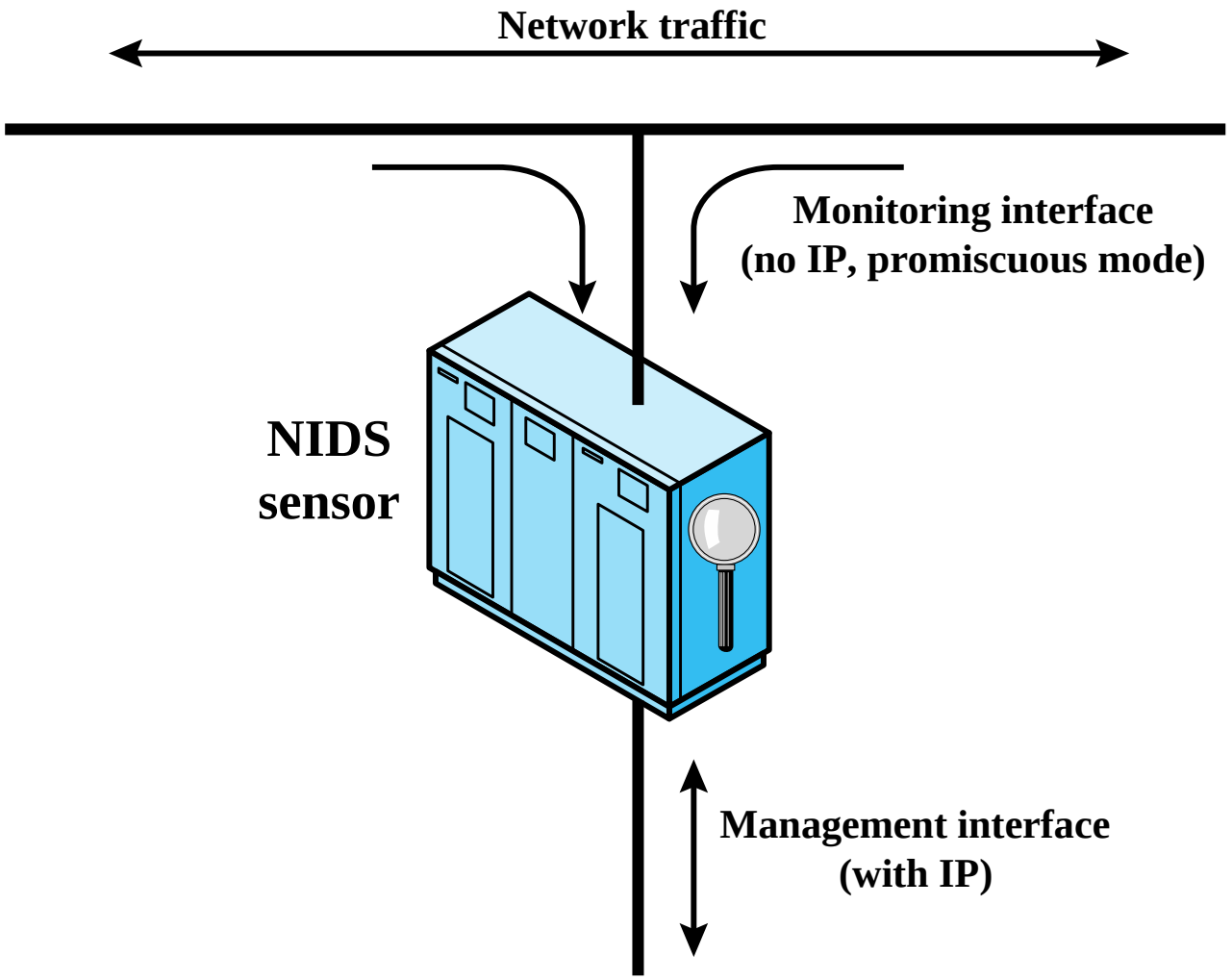

Figure 8.4 Passive NIDS Sensor

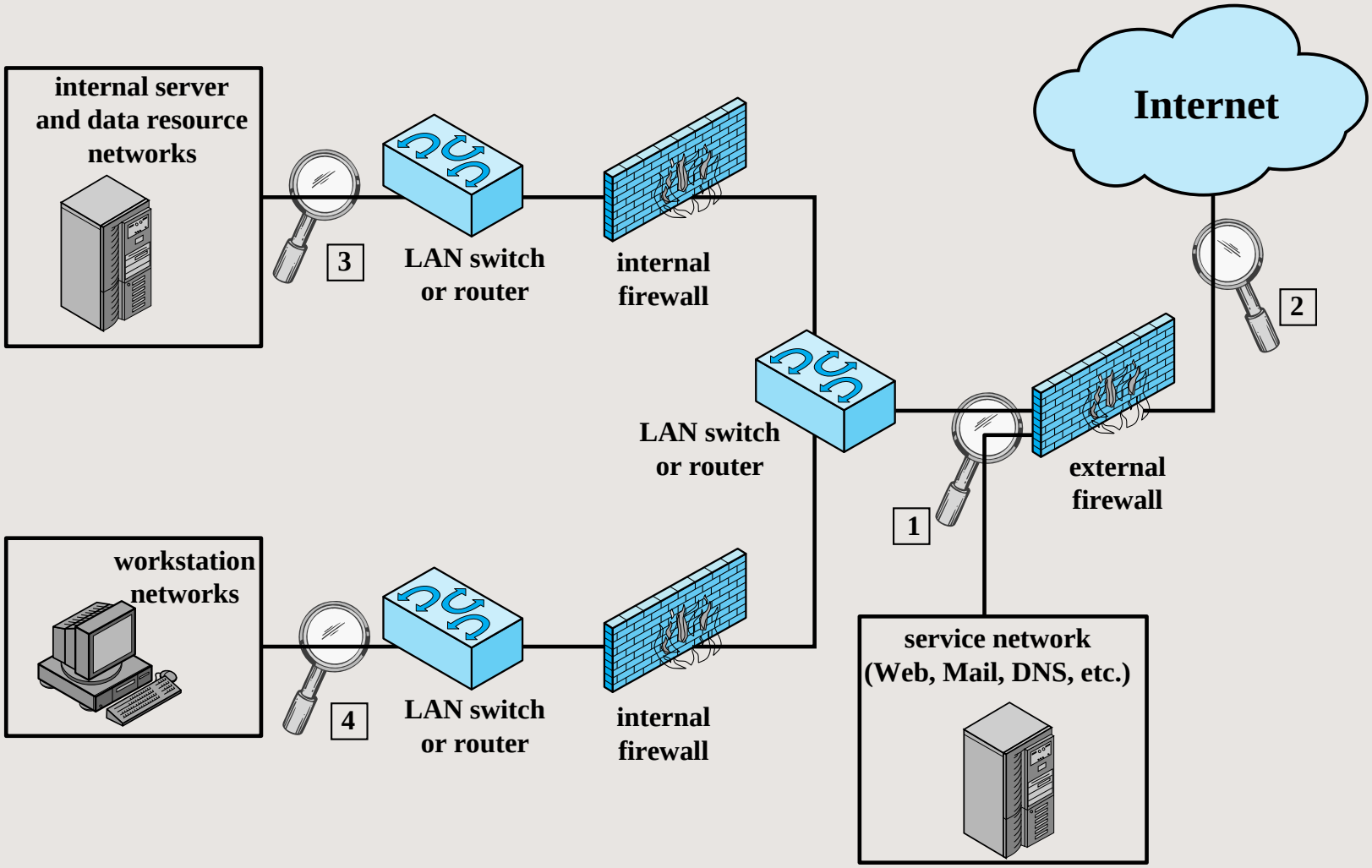

Figure 8.5 Example of NIDS Sensor Deployment

İzinsiz Giriş Tespit Teknikleri

İmza tespiti için uygun saldırılar

- Uygulama katmanı keşif ve saldırıları (DNS, FTP, HTTP vb.)
- Taşıma katmanı keşif ve saldırıları(TCP, UDP)
- Ağ katmanı keşif ve saldırıları (IP v4/v6, ICMP)
- Beklenmeyen uygulama hizmetleri
- Politika ihlalleri

Anomali tespiti için uygun saldırılar

- Hizmet reddi (DoS) saldırılar
- Tarama
- Solucanlar

Durum Bilgili Protokol Analizi (SPA)

- NIST SP 800-94, gözlemlenen ağ trafiğini önceden belirlenmiş evrensel satıcı tarafından sağlanan iyi huylu protokol trafiği profilleriyle karşılaştıran bu anormallik algılama alt kümesini ayrıntılarıyla açıklar
  - Bu, onu kuruluşa özgü trafik protokolleriyle eğitilmiş anomali tekniklerinden ayırır.
- Beklendiği gibi ilerlemelerini sağlamak için ağ, aktarım ve uygulama protokolü durumlarını anlar ve izler
- Gerektirdiği yüksek kaynak kullanımı önemli bir dezavantajdır.

Uyarıların Loglanması

- Bir NIDS sensörü tarafından kaydedilen tipik bilgiler şunlardır:
  - Zaman Damgası
  - Bağlantı veya oturum kimliği
  - Olay veya uyarı türü
  - Derecelendirme
  - Ağ, taşıma ve uygulama katmanı protokolleri
  - Kaynak ve hedef IP adresleri
  - Kaynak ve hedef TCP veya UDP bağlantı noktaları veya ICMP türleri ve kodları
  - Bağlantı üzerinden iletilen bayt sayısı
  - Uygulama istekleri ve yanıtları gibi kodu çözülmüş yük verileri
  - Durumla ilgili bilgiler

IETF İzinsiz Giriş Tespiti Çalışma Grubu

- Amaç, izinsiz giriş tespit ve müdahale sistemleri ile bunlarla etkileşime girmesi gerekebilecek yönetim sistemleri ile ilgili bilgileri paylaşmak için veri formatlarını ve değişim prosedürlerini tanımlamaktır.
- Çalışma grubu 2007'de aşağıdaki RFC'leri yayınlamıştır:

İzinsiz Giriş Tespit Mesajı Değişimi Gereksinimleri (RFC 4766)

- Belge, İzinsiz Giriş Tespit Mesajı Değişim Biçimi (IDMEF) için gereksinimleri tanımlar
- Ayrıca, IDMEF ile iletişim kurmak için bir iletişim protokolü için gereklilikleri belirtir

İzinsiz Giriş Tespit Mesajı Değişim Formatı (RFC 4765)

- Belge, izinsiz giriş tespit sistemleri tarafından dışa aktarılan bilgileri temsil eden bir veri modelini açıklar ve bu modeli kullanmanın gerekçesini açıklar.
- Genişletilebilir Biçimlendirme Dili'ndeki (XML) veri modelinin bir uygulaması sunulur ve XML Belge Türü Tanımı geliştirilir ve örnekler sağlanır

İzinsiz Giriş Tespiti Değişim Protokolü (RFC 4767)

- Belge, izinsiz giriş algılama varlıkları arasında veri alışverişi için uygulama düzeyinde bir protokol olan Saldırı Tespiti Değişim Protokolünü (IDXP) açıklar.
- IDXP, bağlantı yönelimli bir protokol üzerinden karşılıklı kimlik doğrulama, bütünlük ve gizliliği destekler

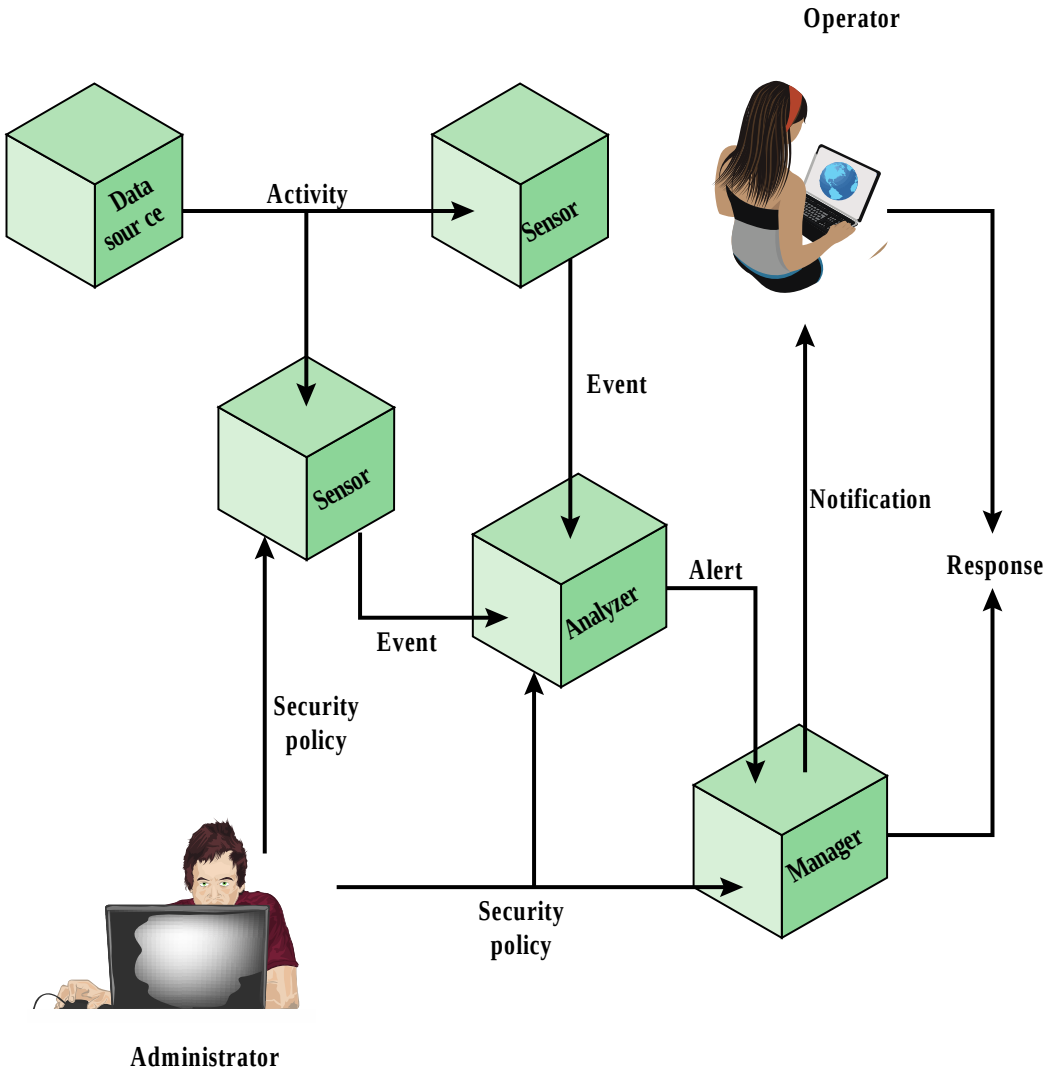

Figure 8.7 Model For Intrusion Detection Message Exchange

Bal küpleri/Honeypots

- Aşağıdakiler için tasarlanmış tuzak sistemleridir:
  - Potansiyel bir saldırganı kritik sistemlerden uzaklaştırır
  - Saldırganın etkinliği hakkında bilgi toplar
  - Saldırganın, yöneticilerin yanıt vermesine yetecek kadar sistemde kalması için teşvik eder
- Sistemler, sistemin meşru bir kullanıcısının erişemeyeceği uydurma bilgilerle doludur.
- Üretim değeri olmayan kaynaklar
  - Bu nedenle, gelen iletişim büyük olasılıkla bir araştırma, tarama veya saldırıdır.
  - Başlatılan giden iletişim, sistemin muhtemelen tehlikeye girdiğini gösterir

Bal Küpü /Honeypot Sınıflandırmaları

- Düşük etkileşimli Bal küpü
  - Gerçekçi bir ilk etkileşim sağlamak için belirli BT hizmetlerini veya sistemlerini yeterince iyi taklit eden, ancak bu hizmetlerin veya sistemlerin tam sürümünü yürütmeyen bir yazılım paketinden oluşur.
  - Daha az gerçekçi bir hedef sağlar
  - Yaklaşan bir saldırı konusunda uyarmak için dağıtılmış bir IDS'nin bir bileşeni olarak kullanım için genellikle yeterlidir.
- Yüksek etkileşimli Bal küpü
  - Saldırganlar tarafından erişilebilecekleri yerlerde araçlanmış ve dağıtılmış eksiksiz bir işletim sistemi, hizmetler ve uygulamalar içeren gerçek bir sistem
  - Bir saldırganı uzun süre meşgul edebilecek daha gerçekçi bir hedeftir.
  - Ancak, önemli ölçüde daha fazla kaynak gerektirir
  - Ele geçirilirse, diğer sistemlere saldırı başlatmak için kullanılabilir

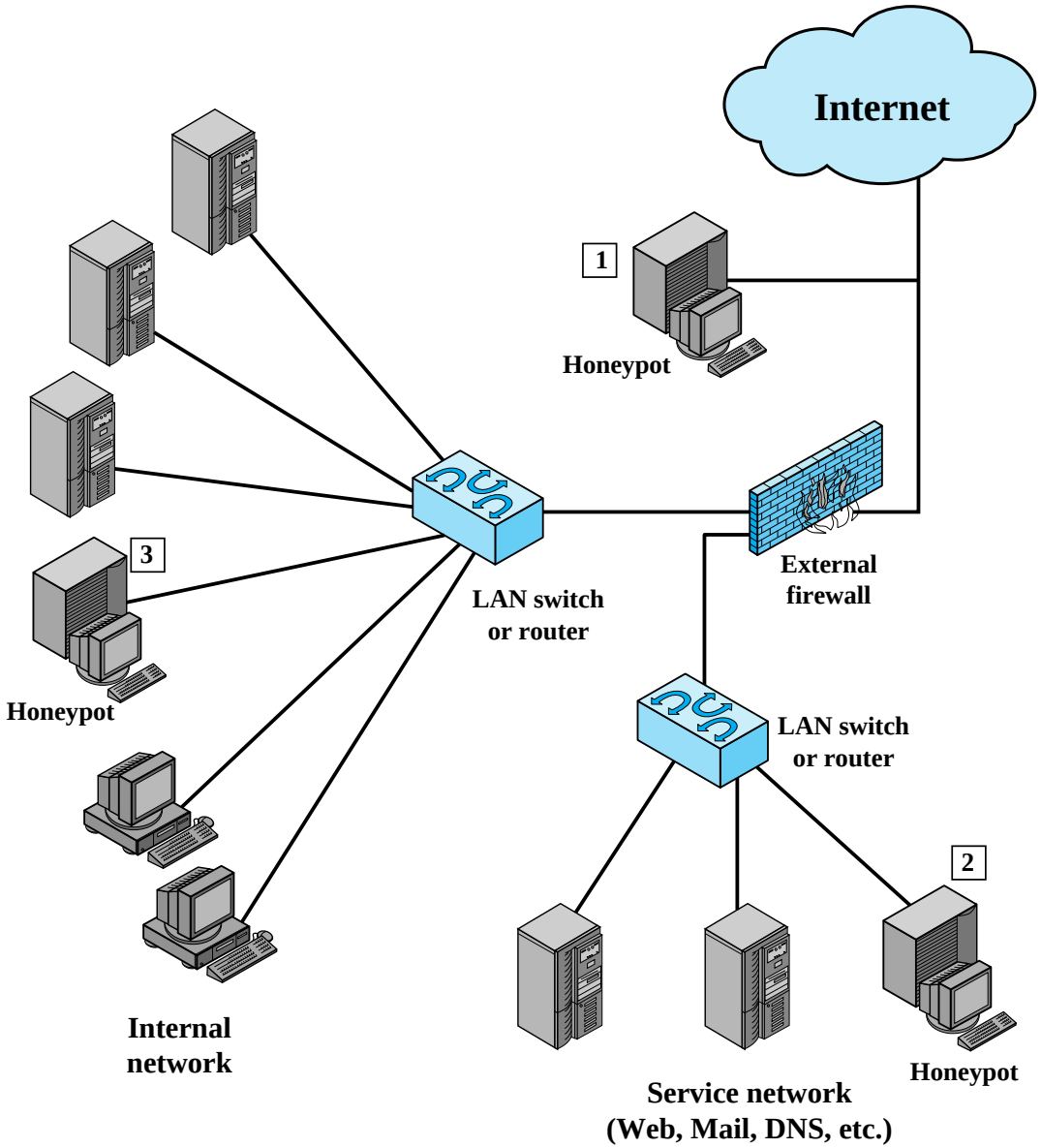

Figure 8.8 Example of Honeypot Deployment

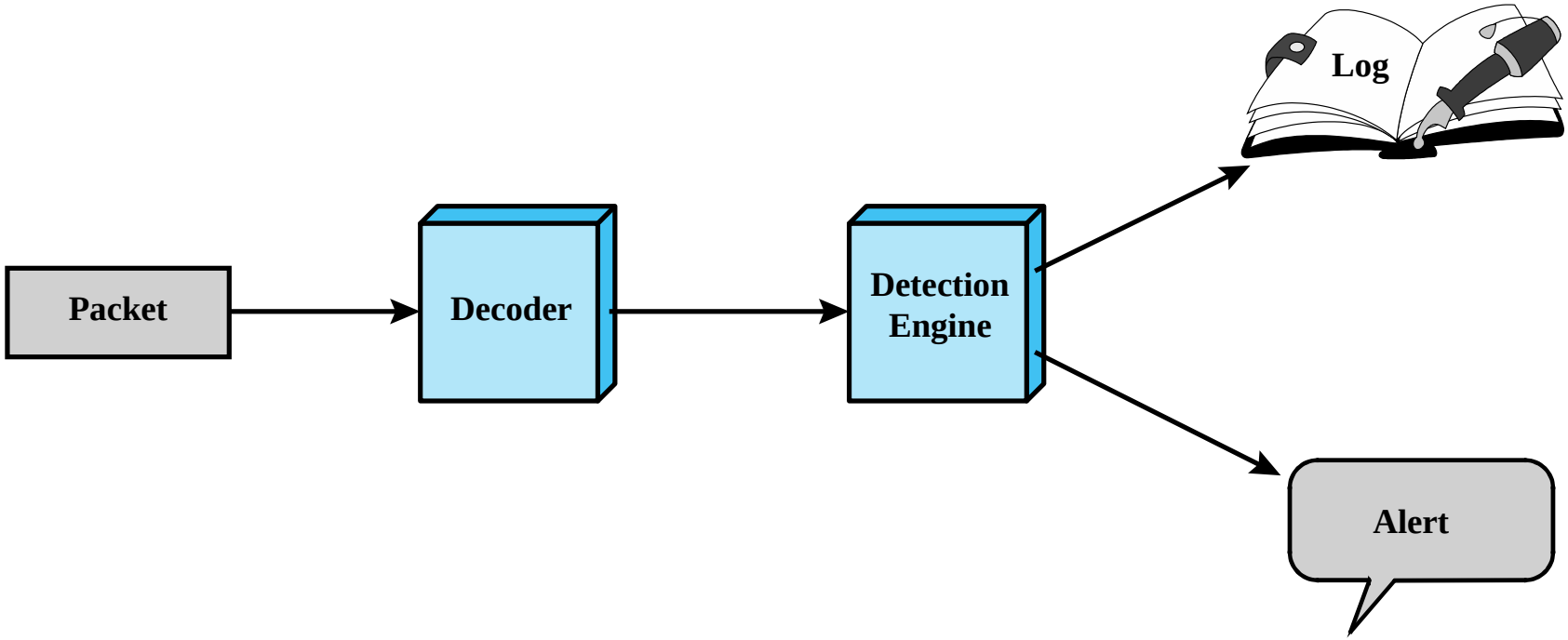

Figure 8.9 Snort Architecture

- Snort, açık kaynaklı, yüksek düzeyde yapılandırılabilir ve taşınabilir ana bilgisayar tabanlı veya ağ tabanlı bir IDS'dir.
- Snort, hafif bir IDS olarak adlandırılır
  - Bir ağın çoğu düğümüne (ana bilgisayar, sunucu, yönlendirici) kolayca dağıtılır
  - Az miktarda bellek ve işlemci süresi kullanan verimli çalışma sağlar
  - Belirli bir güvenlik çözümünü kısa sürede uygulaması gereken sistem yöneticileri tarafından kolayca yapılandırılır
- Snort, gerçek zamanlı paket yakalama, protokol analizi ve içerik arama ve eşleştirme gerçekleştirebilir

Action	Protocol	Source IP address	Source Port	Direction	Dest IP address	Dest Port

(a) Rule Header

Option Keyword	Option Arguments	• • •

(b) Options

Figure 8.10 Snort Rule Formats

Snort Kural İşlemleri

Eylem	Tamım
alert	Seçilen uyarı yöntemini kullanarak bir uyarı oluşturur ve ardından paketi loglar.
log	Paketi loglar
pass	Paketi dikkate almaz
activate	Uyarır ve ardından başka bir dinamik kuralı etkinleştirir
dynamic	Bir etkinleştirme kuralı tarafından etkinleştirilene kadar boşta kalır, ardından bir log kuralı olarak hareket eder
drop	Iptables'a paketi bıraktırır/attırır ve atılan paketi loglar.
reject	iptables'a paketi bıraktırır/attırır, loglanan ve ardından protokol TCP ise bir TCP sıfırlaması veya protokol UDP ise bir ICMP bağlantı noktasına erişilemiyor mesajı gönderier
sdrop	iptables'a paketi bıraktırır/attırır, ancak paketi loglamaz

Snort Kural Seçeneklerine Örnekler 1/2

meta-data	
msg	Bir paket bir olay oluşturduğunda gönderilecek mesajı tanımlar
reference	Ek bilgi sağlayan harici saldırı tanımlama sistemine bir bağlantı tanımlar
classtype	Paketin ne tür bir saldırı denediğini gösterir
yük/payload	
content	Snort'un paket yükündeki belirli içerik (metin ve/veya ikili) için büyük/küçük harfe duyarlı bir arama gerçekleştirmesini sağlar
depth	Snort'un belirtilen modeli bir paketin ne kadar içinde araması gerektiğini belirtir. Derinlik, kuraldaki önceki içerik anahtar sözcüğünü değiştirir
offset	Bir paket içinde bir kalıp aramaya nereden başlayacağınızı belirtir. Ofset, kuraldaki önceki içerik anahtar sözcüğünü değiştirir
nocase	Snort, durumu yok sayarak belirli bir modeli aramalıdır. Nocase, kuraldaki önceki içerik anahtar sözcüğünü değiştirir

Snort Kural Seçeneklerine Örnekler 2/2

Yük barındırmayan/non-payload	
ttl	IP yaşam süresi değerini kontrol edin. Bu seçenek, traceroute girişimlerinin algılanmasında kullanılmak üzere tasarlanmıştır
id	Belirli bir değer için IP Kimliği alanını kontrol edin. Bazı araçlar (istismarlar, tarayıcılar ve diğer garip programlar) bu alanı özellikle çeşitli amaçlar için ayarlar; örneğin, 31337 değeri bazı bilgisayar korsanları arasında çok popülerdir.
dsize	Paket yük boyutunu test eder. Bu, anormal boyuttaki paketleri kontrol etmek için kullanılabilir. Çoğu durumda, arabellek taşmalarını saptamak için kullanışlıdır
flags	Belirtilen ayarlar için TCP bayraklarını test eder
seq	Belirli bir TCP başlık sıra numarası arar
icmp-id	Belirli bir ICMP ID değeri olup olmadığını kontrol edin. Bazı gizli kanal programları iletişim kurarken statik ICMP alanları kullandığından bu yararlıdır. Bu seçenek, stacheldraht DDoS aracısını algılamak için geliştirilmiştir.
tespit sonrası/post detection	
logto	Kuralla eşleşen paketleri belirtilen dosya adıyla günlüğe kaydeder
session	Kullanıcı verilerini TCP oturumlarından çıkarır. Kullanıcıların telnet, rlogin, ftp ve hatta web oturumlarında ne yazdıklarını görmenin çok yararlı olduğu birçok durum içerir