DÜMF Mühendislik Dergisi
web: http://dergipark.gov.tr/dumf

Saldırı tespit ve engelleme araçlarının incelenmesi

Muhammet BAYKARA
Fırat Üniversitesi, Yazılım Mühendisliği Bölümü, Elazığ
mbaykara@firat.edu.tr ORCID: 0000-0002-9368-8902, Tel: (424) 237 00 00 (4296)

Resul DAŞ
Fırat Üniversitesi, Yazılım Mühendisliği Bölümü, Elazığ
rdas@firat.edu.tr ORCID: 0000-1234-5678-9012, Tel: (424) 237 00 00 (4305)

Geliş: 30.07.2018 , Kabul Tarihi: 28.09.2018

Öz

Teknolojik gelişmelerle birlikte, yaşanan sayısal bilgi çağında bilgi güvenliğinin önemi gün geçtikçe artmaktadır. Kişi, kurum ve kuruluşlar açısından bilginin saklanması ve mahremiyetinin korunup istenildiğinde sadece yetkili kişiler tarafından erişilebilir olmasının garanti edilmesi oldukça önemlidir. Bilgi sistemlerinde güvenliğin sağlanması için birçok farklı çalışma yapılmış ve yapılmaya devam edilmektedir. Bu çalışmada bilgi güvenliği sistemlerinin vazgeçilmez araçlarından biri olan STS (Saldırı Tespit Sistemi) araçları ayrıntılı bir biçimde incelenmiştir. Yapılan kapsamlı inceleme sonucunda, bu güncel araçlar veri kaynağı, mimari yapı, çalışma zamanı gibi kriterlere göre sınıflandırılmıştır. Ayrıca, saldırı tespit yöntemi ve saldırı tespit sistemi türüne göre karşılaştırılmıştır.

Anahtar Kelimeler: *Bilgisayar güvenliği; Bilgi güvenliği; Saldırı tespit sistemleri; Saldırı engelleme araçları;*

* Yazışmaların yapılacağı yazar

DOI: 10.24012/dumf.449059

Giriş

Bilişim sistemleri ve özellikle İnternet teknolojilerinin yaygınlaşmasıyla birlikte, bu sistemlerdeki açıklıklardan kaynaklanan güvenlik olayları da artmaya başlamıştır. Güncel açıklıkların önlenebilmesi ve güvenliğin sağlanabilmesi amacıyla birçok araç geliştirilmiştir. Bilgisayar ağları kullanılarak gerçekleştirilebilecek kötü amaçlı aktiviteler, bilinçsiz kullanımlar sonucu oluşabilmektedir. Ancak sistemin açıklıklarından faydalanarak sisteme bilerek zarar vermek isteyen saldırı faaliyetlerinin oranı daha fazladır. Özellikle web teknolojilerinin gelişip yaygınlaşması sonucu atakların sayıları ve türleri artmıştır (Baykara vd., 2013). Birçok farklı türü olan saldırılara karşı, kimlik doğrulama, yetkilendirme, antivirüs programları gibi güvenlik çözümleri geliştirilmeye çalışılmıştır. Bilgi güvenliği, kurumsal ve kişisel anlamda önemli olan bilgilerin yetkisiz erişimlere karşı korunmasıdır. Bilgilerin dijital arşivlerde güvenli bir biçimde saklanması, ihtiyaç duyulduğunda sadece yetkili kişiler tarafından erişilebilir ve değiştirilebilir olması, bilgi güvenliğinin temel unsurlarını ifade etmektedir. Bilgi güvenliği, güvenlik gereksiniminin oldukça önemli olduğu günümüz koşullarında bilişim sistemleri açısından birçok olguyu barındıran bir süreçtir. Bu süreç, Şekil 1'de gösterildiği gibi insan, teknoloji, sistem, bilgi, süreç, yöntem ve algoritma bileşenlerini içermektedir.

Şekil 1. Bilgi güvenliği kavramı

Bilinen ilk saldırılar, parola tahmini, basit kod yürütme gibi etki ve olasılığı düşük ataklar olmasına rağmen gelişen teknoloji ile beraber atak karmaşıklığı ve etkisi artmıştır. Buna rağmen atakların gerçekleştirilebilmesi için gereken bilgi düzeyi düşmüştür (Baykara vd., 2013). İnternet üzerinden kontrolsüz bir şekilde yayılan bilgiler ve otonom saldırı araçları bunun en temel sebebidir. Bilgi güvenliği tehditleri, olayın kaynak noktası bakımından temelde ikiye ayrılır. Bu tasnifte ataklar, iç tehditler ve dış tehditler olarak değerlendirilir. Kurum içerisinde çalışan kişilerden kaynaklanan saldırılar "iç tehditler", kurum dışındaki kişilerden kaynaklanan saldırılar ise "dış tehditler" olarak adlandırılır. CSI (Computer Security Institute) tarafından yapılan bir ankete göre katılımcıların %44'lük oranda iç tehdit yaşadığı belirlenmiştir (Şahinaslan vd., 2009). Bu tehditler, virüslerden (%50) sonra ikinci büyük tehdittir. Bu tür bir iç tehdit durumunun tespit edilmesi zordur ve kurum dışına bu gibi kurumsal mahremiyet derecesindeki bilgilerin yayılmaması gerekir. Bu gerçekler ışığında düşünüldüğünde aslında %44'lük oranın daha büyük olduğu da bir gerçektir. Bilişim dünyasında bilinçli veya bilinçsiz kullanımlar sonucu meydana gelebilecek iç ve dış tehditlerin tespit ve engellenmesine yönelik çalışmalar devam etmektedir.

Bu kapsamlı inceleme makale çalışmasında, bilgi güvenliği uygulamalarında ön plana çıkan saldırı tespit ve engelleme araçları incelenmiş, bu güvenlik araçlarının özellikleri karşılaştırmalı olarak sunulmuştur.

Saldırı Tespit Sistemleri

Bilgisayar ve bilişim teknolojilerinin hızlı gelişimi ile elektronik depolama ortamlarının kullanımları da her geçen gün artmaktadır. Bu durumun sağladığı kolaylıklara karşın bulut ortamlarında depolanan bilgilerin korunması da büyük ve çok önemli bir ihtiyaç haline gelmiştir. Bilginin önem derecesine göre kullanılacak olan koruma sistemleri farklılık gösterebilmektedir. Bu sistemlerin temel amacı, kötü niyetli kişi ve ataklara karşı önlem düzeyini arttırarak bilgi güvenliğinin maksimum oranda sağlanmasıdır. Bilişim sistemlerine karşı tehditler ve sistemlerin

sahip olduğu zayıflıklar sürdükçe, bilgi güvenliği sistemlerinde saldırıları tespit etmek önemli rol oynayacaktır. Bilgiyi korumanın yanı sıra, var olan sistemlerin sürekli erişilebilir halde olması da hayati önem taşımaktadır. Sürekliliğin sağlanabilmesi için, yapılan saldırılara karşı alınan önlemlerin güncelliğini koruması gerekmektedir (Güven vd., 2007). Bu güncellik de ancak değişen saldırı ve yöntemlerin bilinmesi ve var olan sisteme eklenmesi ile sağlanabilir. Bu konuda öncelikle "saldırı"nın ne anlama geldiğini bilmek gerekir. Güvenlik konusunda yapılan çalışmalarda saldırının birçok tanımı yapılmıştır. Anderson'a göre (Anderson J.P, 1980), bir saldırı, izinsiz olarak bilgiye ulaşım, değiştirme, sistemi kullanılmaz veya güvenilmez hale getirmektir. Anderson'un 1980'de yapmış olduğu bu tanım hala geçerliliğini koruyan en temel tanımlardan biridir. Günümüzde ise saldırı, "bilginin mahremiyetini, bütünlüğünü ve erişilebilirliğini tehlikeye atabilecek girişimlerin kümesi" olarak tanımlanmaktadır. Saldırı tespiti ise, bir bilgisayar sisteminde veya ağda meydana gelen olayları izleyip analiz ederek, bilginin mahremiyetini, bütünlüğünü ve erişilebilirliğini bozmak ya da sistemin güvenlik mekanizmalarını aşmak için yapılan aktiviteler olarak tanımlanan saldırı işaretlerini yorumlama sürecidir (Yıldız vd., 2010). En basit tanımıyla, saldırı tespiti işini yapmak için geliştirilen sistemlere ise "Saldırı Tespit Sistemleri (STS)" denilmektedir. Konuyla ilgili literatür incelendiğinde, STS için çok farklı tanımlar olduğu da görülmektedir. Yapılan bu tanımlara göre STS'lerin (Güven vd., 2007) birkaç farklı tanımı şöyle ifade edilebilir. Bilgi sistemlerine yapılan saldırıların tespit ve engellenmesine yönelik olarak tasarlanmış sistemlerdir. Çoğunlukla gerçek zamanlı olarak, bilgisayar sistemlerinin yetkisiz, kötüye kullanım ve suistimalini yakalamak için kullanılan sistemlerdir. Diğer bir tanım ile, Saldırıyı durdurma girişiminde bulunmayan ve olası güvenlik istismarı durumlarında, sistem yetkililerine uyarı mesajı (alert) veren sistemlerdir. Sistem kaynaklarına veya verilerine yetkisiz erişimleri belirler. Bilişim sistemlerinde kullanılan, bilgi güvenliğinin sağlanmasındaki "alarm" özelliğinde çalışan sistemlerdir. Bilgisayar veya ağ sistemine gerçekleştirilen sızma faaliyetlerini yakalamak için kullanılan yazılım araçlarıdır. Bilgi güvenliğinin sağlanmasında bizlere yardımcı olan sistemlerdir (Sancak, 2008). Bir ağ veya bir bilgisayara karşı yapılan her türlü saldırının tespit edilmesi ve saldırganın bertaraf edilmesi için geliştirilmiş sistemlerin bütünüdür (Sazlı vd., 2007). Gerçek zamanlı, sistem bütünlüğünü, kullanılabilirliğini ve gizliliğini tehdit eden aktiviteleri ayırt ederek bildiren sistemlerdir (Pasin, 2002).

Yetkisiz kullanma ya da yetkilerini aşan işlemleri yapma girişiminde bulunan kişi veya programları tespit etme çalışmasıdır (Dayıoğlu vd., 2002). Son yıllarda ortaya çıkmış yeni bir ağ teknolojisidir. Yazılım ve donanım kombinasyonundan oluşur. Güvenlik duvarının yetersiz kaldığı durumlarda gerekli koruma ölçütlerini sağlar ve saldırılara karşı etkin bir koruma gücüne sahiptir (Huang vd., 2010). Bilgisayar sistemlerindeki sızmalara karşı, bu sızmaları tespit etmeye çalışan ve sistem izolasyonunu sağlayan yeni bir ağ teknolojisidir (Biermann vd., 2001). Bir ağda düşman (hostile) ve sömürücü (exploit) aktivitelere karşı koruyucu sistemdir (Depren vd., 2005). Bilişim sistemlerine yapılan yetkisiz erişimleri tespit etmek için kullanılan yazılım araçlarıdır. STS'ler, kötü niyetli ağ trafiği ve bilgisayar kullanımını tespit etme yeteneğine sahiptir. Bir STS, olası güvenlik açıklarını belirleyebilmek için bilgisayar veya ağ içerisinde değişik alanlardan bilgileri toplar ve analiz eder. STS'ler, güvenlik duvarının statik izleme kabiliyetini tamamlayan dinamik izleme elemanlarıdır (Patcha vd., 2007).

Literatürde verilen tanımlardan yola çıkarak, STS'leri, bilginin elektronik ortamlarda taşınırken, işlenirken veya depolanırken başına gelebilecek tehdit ve tehlikelerin ortadan kaldırılması amacıyla, bilgiye yetkisiz erişim veya kötüye kullanım gibi girişimleri tespit edebilme ve bu tespiti sistem güvenliğinden sorumlu kişilere iletebilme özelliğine sahip yazılımsal ve/veya donanımsal güvenlik araçları olarak tanımlayabiliriz. Aynı zamanda STS'ler, ağ cihazlarını izleyerek anormal davranışları ve kötüye kullanımı tespit ederler.

Saldırı Tespit Sistemlerinin Güvenlik Açısından Önemi ve Etkisi

Global iletişim araç ve imkânlarının artmasıyla birlikte saldırılabilecek daha çok sistem ortaya çıkmıştır. Bu sistemlere yapılan saldırılar, yeni üretilen sistem ve teknolojilerin açıklıklarından yararlanılarak yapılır. Genel olarak bu saldırıları engellemenin iki farklı yolu vardır: (1) Güvenliği tam sağlanmış bir sistem oluşturmak, (2) Saldırıları tespit edip önlemler almak.

Güvenliği tamamen sağlanmış bir sistem ya da altyapı oluşturmak pratikte çok zor, hatta imkânsızdır denilebilir. Çünkü bilişim dünyasında sürekli olarak yeni teknolojiler üretilmekte ve farklı kategorideki bu teknolojiler birbirleriyle iletişim sağlamak zorundadır. Bu etkileşim mecburiyeti de yeni açıklık noktaları meydana getirebilmektedir. Yukarıda belirtilen (1) tam güvenlikli bir sistem oluşturma zorluğunun gerekçeleri şöyle verilebilir (Güven vd., 2008):

- İşletim sistemlerinde ortaya çıkan açıklıkların saldırganlar tarafından fark edilmesi ve kötücül amaçlarla kullanılması,
- OSI katmanlarında verilerin iletilmesi amacıyla kullanılan bazı protokollerin doğası gereği sahip oldukları bazı kuralların kötücül amaçlı istismar edilebilmesi,
- Şifreleme yöntemlerinin ve şifre anahtarlarının kırılabilmesi ve kullanıcıların şifre yönetimleriyle ilgili olarak yaşadıkları sorunlar nedeniyle yüksek seviyede güvenliğin sağlanamaması,
- Genellikle dış ortamlara karşı korunan bilgi sistemlerinin iç ortamlardan kaynaklanan suiistimaller ile güvenlik zafiyetine uğrayabilmesi,
- Kullanılan güvenlik mekanizmalarının, olası yeni saldırı örüntülerine adapte olabilecek şekilde güncellenmemesi,
- Bilgi güvenliğinin sürekli olarak çalışma gerektiren bir süreç olduğu gerçeğine uygun hareket edilmemesi ve gerçekleştirilmesi gereken güvenlik politikalarının sağlam olarak belirlenip uygulanmaması,
- Güvenlik amacıyla kullanıcı yetkilerinin minimuma indirilmesi sonucu kullanıcı verimliliğinin düşmesi.

Tam güvenlikli bir bilişim sistemi oluşturmak, doğası gereği sahip olduğu karmaşık yapıdaki zorluklarından dolayı tecrübe ve büyük önem gerektiren bir emek ister. Bu sistemleri korumak isteyen kişisel ya da kurumsal kullanıcılar açısından STS'ler oldukça önemli araçlar olarak işlev görürler. STS'lerin normal ağ trafiğinde bekleme pozisyonunda kalması, saldırı geldiğinde ise hızlıca tespit etmesi beklenir. Meydana gelen bir saldırının hangi kaynaktan geldiği bilgisini elde etmek, STS'lerin önemini ortaya koyan temel faktörlerden biridir. STS'ler, detaylı bir şekilde toplayıp depoladığı bilgilerden yararlanarak, kötücül aktiviteleri mümkün olabilen en erken zamanda tespit etme özelliğinde olmalıdır. Benzer şekilde aynı bilgilerin incelenmesi ile daha önce hiç karşılaşılmamış bir saldırıyı da tespit edebilmesi STS'lerin önemini artıran bir özelliktir (Güven vd., 2008).

Yukarıda sıralanan nedenlerden dolayı, tamamen güvenli bir sistem oluşturmanın mümkün olmadığı görülse de, üst düzey güvenliğe sahip bir sistem oluşturmak mümkündür. Bunun için maliyet de göz önünde bulundurularak gerekli olan tüm güvenlik araçlarından faydalanılmalı ve güncel araçlar sürekli takip edilmedir. Ancak saldırganlar, kapatılan açıkların aksine yenilerini bulabilmesi ve önceden tahmin edilemeyen yollara başvurmaları, tamamen güvenli bir ortamın oluşturulamamasına neden olduğu da asla unutulmamalıdır. STS'lerin buradaki önemi, kullanılan yeni teknikler sayesinde önceden bilinmeyen saldırıların da tespit edilebilmesini sağlamasıdır.

Saldırı Tespit Sistemlerinin Sınıflandırılması

Saldırı Tespit Sistemlerinin sınıflandırılmaları için birçok farklı kriter kullanılabilir. STS stratejilerinin de belirlendiği, kullanılan genel kriterler şöylece sıralanabilir:

- Saldırı tespit yöntemi,
- Mimari yapı,
- Korunan sistem türü,

- Veri işleme zamanı,
- Kullanılan bilgi kaynağı.

En çok bilinen sınıflandırma kriteri saldırı tespit yöntemidir. Bu sınıflandırma kriterine göre STS'ler, Anomali Tespiti ve Kötüye Kullanım Tespiti olarak ikiye ayrılmaktadır.

Şekil 2. Saldırı tespit sistemlerinin sınıflandırılması

STS'lerin en çok kullanılan özelliklerine göre sınıflandırılması Şekil 2'de verilmiştir. Bir STS, Şekil 2'de gösterilen sınıflandırma kriterlerinden her biri ile farklı sınıflarda yer alabilir. Bu durum, sınıflandırmanın hangi kritere göre yapıldığına bağlıdır. Örneğin; 1988'de geliştirilen IDES, veri işleme zamanına göre gerçek zamanlı, mimari yapısı bakımından merkezi sistemli, kullanılan bilgi kaynağı açısından sunucu tabanlı, saldırı tespit yöntemi açısından anormallik tespiti, koruduğu sisteme göre ise sunucu temelli sınıfına dahildir. Belirlenen sınıflandırma kriteri sadece saldırı tespit yaklaşımı ise IDES anomali tespiti yaklaşımını kullanan STS sınıfına aittir denir. Bu durumda diğer kriterlerden bahsedilmez. Ancak tüm bu kriterler, aynı zamanda bir STS'nin karakteristiğini ortaya koyması açısından önemlidir (Güven, 2007).

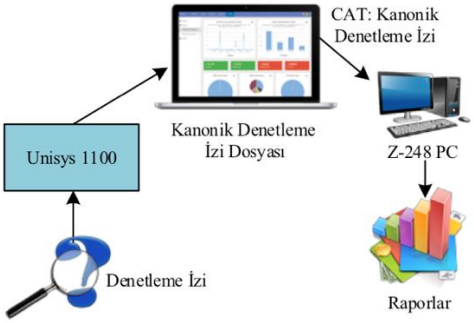
Saldırı Tespit Sistemi Araçları

Haystack

Bu STS, 1988 yılında ABD Hava Kuvvetlerinde kullanılan, OS/1100 işletim sistemini çalıştıran çok kullanıcılı Unisys 1100/60 ana bilgisayarları için geliştirilmiş bir STS'dir. Anderson ve Denning'in konu ile ilgili yayınladıkları makalelerden sonra bu konuda somut olarak atılan ilk adımlardan biridir. Haystack aslında 6 farklı tür saldırının tespiti için geliştirilmiştir [Güven, 2007; Smaha, 1988]. Bunlar:

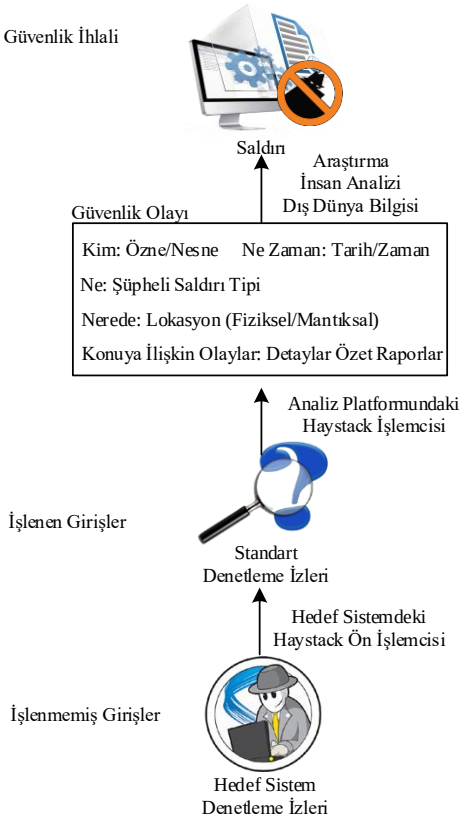
- Kırma girişimleri (attempted break-ins)
- Kılık değiştirilen ataklar (disguised intrusion)
- Güvenlik kontrol sistemine sızma (penetration of the security control system)
- Sızma (leakage)
- Hizmet engelleme (denial of service)
- Kötüye kullanım (malicious use)

Haystack iki bileşene ayrılmıştır. Unisys (Sperry) çalışma sistemi, veri toplamayı denetlemekten sorumlu bileşen, Haystack'in Unisys parçası daha sonra bu denetleme takibini, birleşmiş denetleme takibine dönüştürmektedir. Şekil 3, Haystack STS'nin operasyonel yapısını göstermektedir. Hedef sistem üzerindeki denetleme izleri Haystack ön işlemcisi tarafından kanonik denetleme izlerine dönüştürülür. Daha sonra bu denetleme izleri analiz platformunda incelenerek güvenlik ihlali olup olmadığına karar verilir. Şekil 4 analiz mantığını ve Şekil 5, Haystack STS'nin kavramsal yapısını göstermektedir (Smaha, 1988). Haystack, çok yönlü sistem denetim kayıtlarını, kullanıcı davranışını, anormal olayları ve güvenlik olaylarını kısa özetlerine indirgemektedir. Bu, sistem güvenliği görevlisinin, özellikle içerdeki yani yetkili kullanıcılar tarafından müdahaleleri tespit etmesi ve araştırması için tasarlanmıştır.



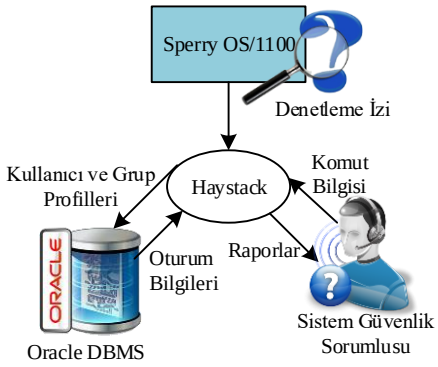
Şekil 3. Haystack operasyonel yapısı

Haystack'in operasyonu temelde, güvenlik politikaları, kullanıcı grupları ve bireysel kullanıcılar için tipik davranış modelleri temeline dayanan davranışsal kısıtlamaları vardır.



Şekil 4. Haystack analiz mantığı

Haystack, "önleme" ipucu ve ilgili verilerin özetlerini sunarak her günün denetim iz dosyalarındaki anormal olaylarla ilgili raporları tutar. Kullanıcı etkinliğini, önceden tanımlanmış güvenlik kısıtlamaları ve tipik kullanıcı davranışının modellerine göre analiz eder. Haystack, sistem güvenliği görevlisi için genel olarak belirsiz denetleme izi verilerinin sayısını, olası bilgisayar saldırılarının daha ayrıntılı incelenmesi için yorumlanan bilgilerin kısa özetlerine indirgemek için operasyonel bir yardımcı olacak şekilde tasarlanmıştır.



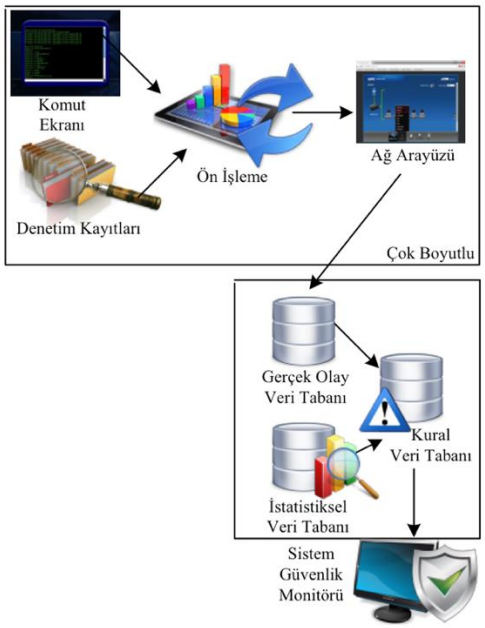
Şekil 5. Haystack kavramsal yapısı

W&S

W&S (Wisdom and Sense – Bilge ve His), Los Alamos Ulusal Laboratuarlarında geliştirilen bir saldırı tespit sistemidir. Saldırı tespitinde kullandığı yönteme göre anormallik tabanlı bir çalışma olup geliştirilmesine 1984 yılında başlanmasına rağmen ilk olarak 1989'da sunulmuştur. W kısmı "Bilge-Hikmet" anlamına gelmektedir ve geçmişteki denetleme verilerini analiz ederek normal davranışı oluşturması anlamına gelir. S kısmı ise "his" anlamına gelmekte ve normal davranışların kural haline getirilip uzman sistem içerisinde kullanılarak sonraki anormal davranışların yakalanması anlamına gelmektedir [Güven, 2007; Erol, 2005).

Midas

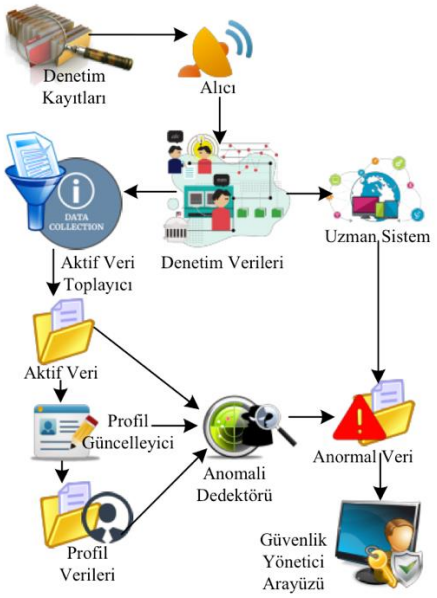
MIDAS (Multics Intrusion Detection and Alerting System), 1988 yılında NCSC (Ulusal Bilgisayar Güvenlik Merkezi), Bilgisayar Bilimleri laboratuvarı (Computer Science Laboratory) ve SRI (Stanford Araştırma Enstitüsü) işbirliği ile NCSC'nin ağa bağlanmış ana bilgisayarı Honeywell DPS-8/70 için saldırı tespiti sağlamak üzere geliştirilmiştir [Güven, 2007; Erol, 2005). MIDAS, sezgisel saldırı tespiti konsepti çevresinde geliştirilmiş uzman sistem tabanlı bir saldırı tespit sistemidir. MIDAS çalışma mimarisi Şekil 6'da verilmiştir.



Şekil 6. MIDAS çalışma mimarisi

Ides

IDES (Intrusion Detection Expert System), Denning ve Neuman'ın 1985'li yıllarda yaptıkları çalışmalar ile gündeme gelmiştir [Güven, 2007; Erol, 2005]. IDES, adından da anlaşılacağı gibi uzman sistem yapısındadır. Denning ve Neuman çalışmalarında IDES için gereksinimleri ve mimari yapıyı ortaya koymuşlardır.



Şekil 7. IDES çalışma mimarisi

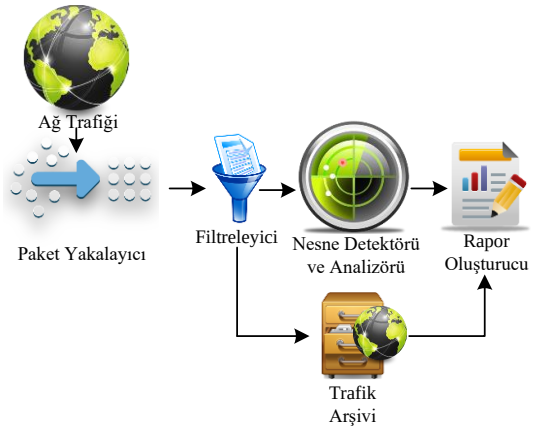
Bu çalışmanın ardından, IDES üzerinde yapılan çalışmalar birçok araştırmacının da katkıları ile 1987-1992 yılları arasında yoğun olarak devam etmiştir. IDES prototipi, kullanıcı davranışlarını denetler ve geçmiş hareket profillerine göre normal ve anormal davranışları tespit eder. Kullanıcı davranışları zaman içerisinde değişebileceğinden kullanıcı hareket profilleri sürekli yenilenir. Bu STS, bir uzman sistem bileşeni içerdiğinden, önceki saldırılardan edinilen bilgilere dayanan özel davranışları, sistemin bilinen açıklıklarını ve kuruluma özel güvenlik politikalarını tanımlayan kurallar içerir. Şekil 7'de görüldüğü üzere IDES, başlangıçta tek bir sunucu için yapılandırılmıştır. Daha sonraki çalışmalarda yeniden tasarlanarak, birden fazla sistem için kullanılabilir hale getirilmiştir. Birçok versiyonu bulunan IDES yazılımı son olarak NIDES (Next-Generation Intrusion Detection Expert System) adını almıştır.

Nadir

NADIR (The Network Anomaly Detection and Intrusion Reporter) 1991-1993 yılları arasında Los Alamos Ulusal Laboratuarlarında (LANL-Los Alamos National Laboratory) bilgisayar ağları mühendisliği grubu tarafından geliştirilmiştir. NADIR, istatistiklere dayalı uzman sistem temelli bir saldırı tespit sistemidir. Çalıştığı sistemin kullanıcıları hakkında haftalık istatistikler tutar, her hafta gerçekleştirilen bu profil analizlerinin sonucunda elde edilen detaylı istatistik raporları uzman sistem kurallarıyla karşılaştırır ve kurallarla çelişen durumlar saldırı olarak değerlendirilir (Güven, 2007).

Nsm

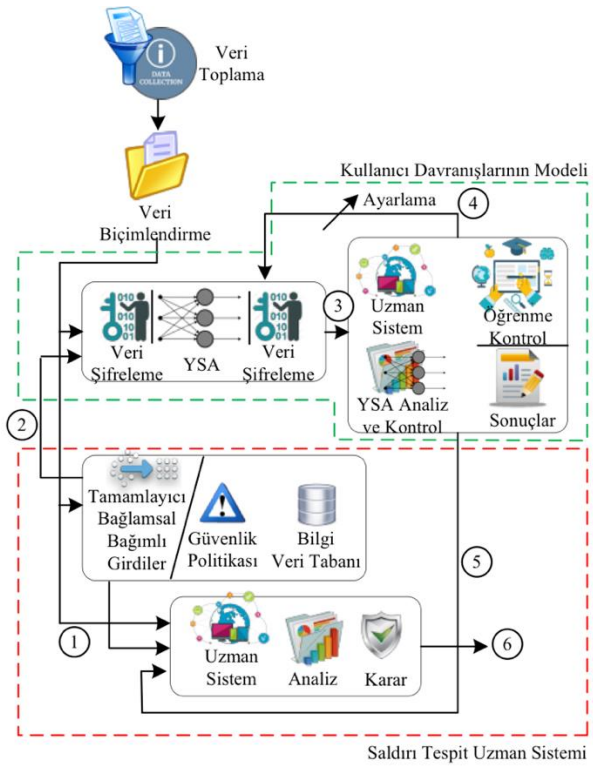
NSM (Network Security Monitoring) ağ güvenlik görüntüleyicisi anlamına gelen bir saldırı tespit sistemidir. NSM de IDES gibi çeşitli düzenlemelerden geçmiştir. 1990-1994 yılları arasında geliştirilen bir saldırı tespit sistemidir. Şekil 8'de çalışma mimarisi verilen NSM, ağı dinleyerek ağın kullanımıyla ilgili bir profil geliştirir ve geçerli kullanımı gerçek zamanlı olarak geliştirdiği profille karşılaştırır. Elde edilen veriler beklenen bağlantı verisiyle karşılaştırılır ve beklenen değerlerden sapma gösteren her veri anormal olarak kabul edilir (Güven, 2007).



Şekil 8. NSM çalışma mimarisi

Hyperview

Hyperview 1992 yılında geliştirilmiş olan bir saldırı tespit sistemidir ve diğer saldırı tespit sistemlerinden oldukça farklıdır.

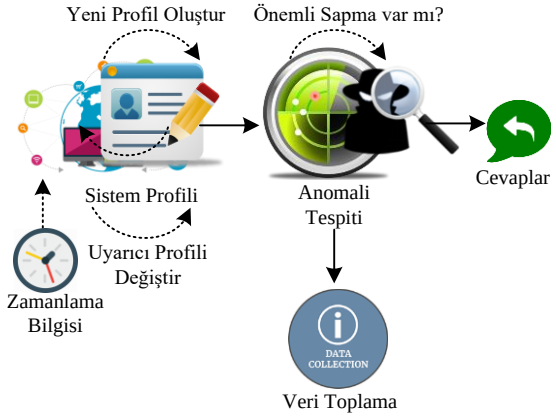


Şekil 9. Hyperview çalışma mimarisi

Çalışma mimarisi Şekil 9'da verilen Hyperview, iki ayrı bölümden oluşmaktadır. Birinci bölüm davranışları izleyen ve bunları sınıflandıran bir uzman sistem içermektedir. İkinci bölümse birinci bölümdeki uzman sistemden öğrendikleri ile eğitilen yapay sinir ağlarını içeren bölümdür (Erol, 2005). Hyperview Şekil 9'da görüldüğü üzere, (1) Denetim verilerinin değişimi ve Formasyonu, (2) Tamamlayıcı bağlamsal bağımlı girdi hesaplama, (3) YSA'nın ham çıktısı, (4) Denetlenen öğrenme ve çıktı yorumlaması, (5) Kullanıcının davranış modelinden girdiler ve (6) Nihai karar ve alarm üretimi olmak üzere altı alt bölümden oluşur.

Ustat

USTAT (State Transition Analysis Technique for Unix Systems), 1993-1995 yılları arasında Unix sistemler için geliştirilmiş bir saldırı tespit sistemidir. Saldırı tespitinde durum geçiş analizi yöntemi kullanılmıştır. Çalışma mimarisi Şekil 10'da verilen bu STS'de, eğer bir davranış saldırı için tanımlı durum geçişlerini yapıyorsa saldırı olarak sınıflandırılmaktadır (Ilgın, 1993).



Şekil 10. Ustat çalışma mimarisi

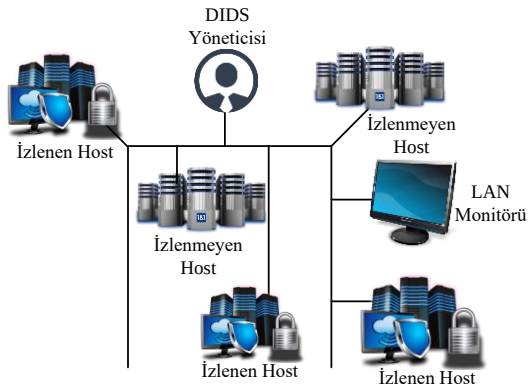
Dids

DIDS (Distributed Intrusion Detection System), 1992 yıllarında geliştirilmiş dağıtık mimarili sistemleri kapsar. Şekil 2'de gösterildiği üzere STS'ler açısından mimari yapıya göre sınıflandırmalardan biri olan dağıtık mimari yapılı sistemler, Şekil 11'de gösterildiği gibi ağın çeşitli noktalarından verilerin toplanıp bir merkezde analiz edilmesi mantığına dayanmaktadır (Güven, 2007; Erol, 2005).

Idiot

IDIOT (Intrusion Detection In Our Time), 1994-1996 yılları arasında CERIAS (Center for Education and Research in Information Assurance and Security)'da Kumar tarafından geliştirilmiş bir saldırı tespit sistemidir. Kumar'ın tasarımı olan IDIOT, saldırı yöntemlerinin eşleştirilmesi ve geçici

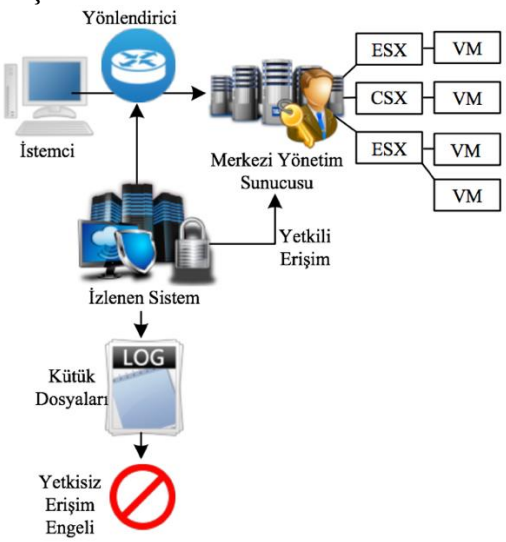
karakteristiklerin karmaşıklığına dayalı olan bir sınıflandırma yöntemi içermektedir (Güven, 2007).



Şekil 11. Dids çalışma mimarisi

Janus

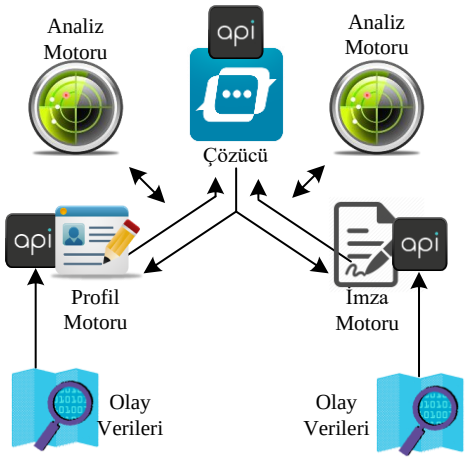
Janus, 1994-1996'da Berkeley Üniversitesi'nde Wagner tarafından tez çalışması sırasında geliştirilmiş bir sistemdir (Güven, 2007; Sazlı vd., 2007). Janus çalışma mimarisi Şekil 12'de verilmiştir.



Şekil 12. Janus çalışma mimarisi

Emerald

EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), 1997-1998 yıllarında geliştirilmiş ölçeklenebilir, dağıtık mimari yapılı bir saldırı tespit sistemidir. Bilgi güvenliği ve saldırı tespit sistemleri alanındaki önemli ve diğer çalışmalar tarafından kaynak olarak kullanılan bir sistemdir (Erol, 2005). Emerald çalışma mimarisi Şekil 13'te verilmiştir.



Şekil 13. Emerald çalışma mimarisi

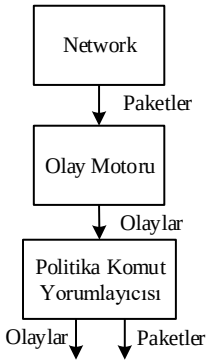
Ripper

Ripper, 1999 yılında geliştirilmiştir. Bu STS, veri madenciliği yaklaşımını kullanır. Ripper, DARPA değerlendirmesine katılmış olan sistemlerden biridir (Erol, 2005).

Bro

Bro, 1998'de Vern Paxson tarafından geliştirilmiş bir saldırı tespit sistemidir. Ağ trafiğini gerçek zamanlı olarak pasif gözetleme mantığı ile izleyerek saldırı tespiti yapmaktadır. Birçok değişik özelliği sağladığı için sıkça kaynak verilen bir STS'dir (Erol, 2005; Axelsson, 2000). Bu STS'yi diğer saldırı tespit sistemlerinden ayıran temel özelliği performansa dayalı analizler ve ağ sorunlarının çözümü için de destek sunmasıdır. Bro bu özelliği ile ağ trafiği analiz aracı olarak nitelendirilebilir. Zaman içerisinde işlevsellik kazanmış olan Bro en güçlü STS yapıları arasına girmiştir. Geliştirilmesine ICSI'da (International Computer Science Institute) devam edilmektedir. Bro, iki temel bileşenden oluşur. Bu bileşenler, (1) "Olay Motoru (event engine)" ve (2) "Politika komut yorumlayıcısı (policy script interpreter)" 'dır. Şekil 14, Bro bileşenlerini göstermektedir. Buradaki olay motoru ağ trafiğindeki paketleri ve protokolleri Bro'nun anlayacağı dile dönüştürür. Bro için belirtilen yaklaşık 320 olay türü vardır. Politika komut yorumlayıcısı ise Bro'nun betik dili ile yazılan olay işleyicilerinin çalıştırılması ile ilgilenir. Bu betikler ile ağ trafiği için oluşturulmuş olay türleri analiz edilir ve herhangi bir anormallik olması durumunda ne tür

işlemlerin gerçekleştirileceği ve bunların kayıt politikaları belirlenir.

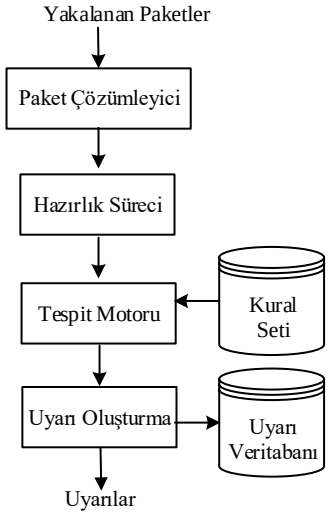


Şekil 14. Bro bileşenleri

Bro'nun genel özellikleri şöyle açıklanabilir.
Linux, FreeBSD, MacOS gibi UNIX tabanlı işletim sistemlerinde çalışabilmektedir. Gerçek zamanlı ya da offline analiz yapabilmektedir. Bro farklı sunucularda da çalışıp birbirleriyle iletişim sağlayabilir. Tüm HTTP trafiğini (sunucu /istemci istek ve cevapları, mime türleri, uri vb.), DNS istek ve cevaplarını, SSL sertifikalarını, SMTP oturumlarını, FTP trafiğini çözümleyerek kaydedebilmektedir. Ayrıca ağ akışını da kayıt altına almaktadır. Kayıtlar rahatça okunabilir şekilde (tab karakteriyle ayrılmış), ASCII formatında metin dosyalarına kaydedilir. Port bağımsız olarak uygulama katmanı protokollerinden DNS, FTP, HTTP, IRC, SMTP, SSH, SSL çözümlenebilmektedir. HTTP, FTP, SMTP, IRC trafiğinden geçen tüm dosyalarla ilgili bilgileri MD5/SHA1 özet değerleriyle birlikte metin formatında kaydedilebilmekte, istenildiği durumda bu dosyalar trafikten çıkarılıp belirtilen bir dizinde saklanabilir. Dış kaynaklar kullanarak (özet değeri eşleştirmeleri, IP itibar tabloları) çeşitli zararlı yazılımları tespit edebilmektedir. IPv6 protokolü kapsamlı bir şekilde desteklenmektedir. Betik dili sayesinde anında e-mail mesajı atabilir ve ağı sonlandırabilir. Libpcap kütüphanesini kullanır.

Snort

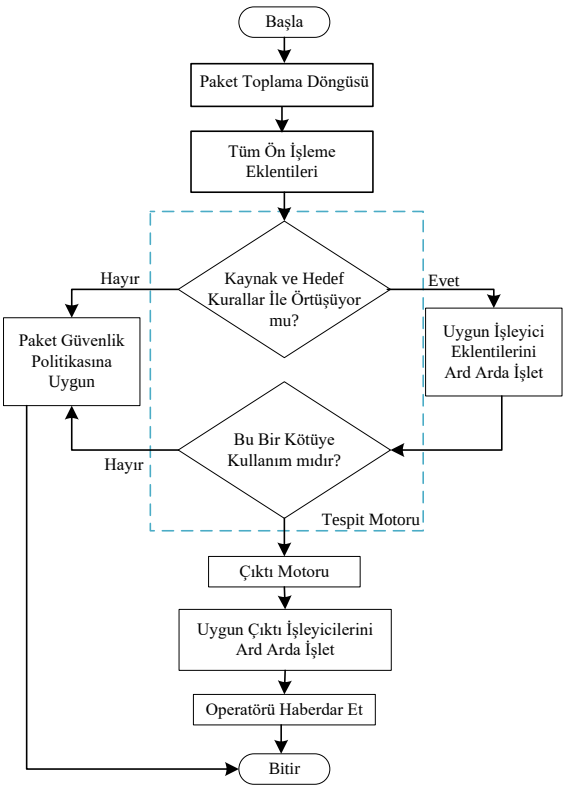
Snort, 1990'ların sonunda Martin Roesch tarafından geliştirilmiştir. Gerçek zamanlı olarak ağ analizi yapabilen ve ağ paketlerini kaydedebilen açık kaynak kodlu, kural tabanlı bir saldırı tespit ve engelleme sistemi olan snort, ticari STS yapıları seviyesine ulaşmış ve oldukça yaygın bir kullanıma sahiptir. Snort, paket çözümleyici, ön işlem, tespit motoru ve uyarı oluşturma şeklinde 4 temel modülden oluşmaktadır. Snort'un sahip olduğu bu modüller ve çalışma mantığı Şekil 15'te verilmiştir.



Şekil 15. Snort çalışma yapısı

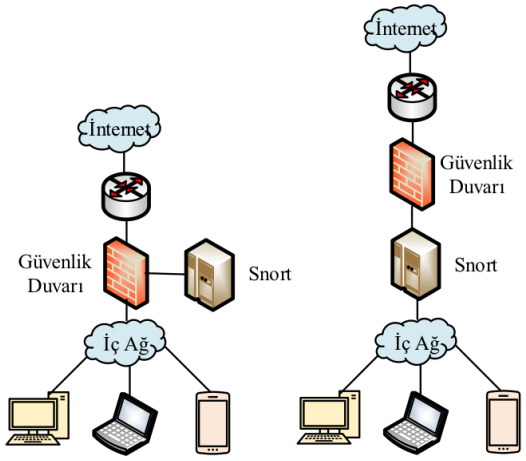
Paket çözümleyici, Libpcap tarafından yakalanan katman 2 paketlerini ayrıştırır ve hazırlık sürecine gönderir. Hazırlık süreci, paketleri tespit motorunun anlayabileceği hale getirir. Tespit motoru Snort'un temel bileşenidir. Saldırı tespitinin yapıldığı kısımdır. Uyarı oluşturma kısmı ise tespit motoru tarafından yakalanan saldırılar için ne tür uyarı oluşturulacağını belirleyen kısımdır.
Snort, imza temelli ve anormallik tespiti yaklaşımlarının avantajlarını üzerinde barındırır. Protokol ve içerik analizleri yaparak birçok saldırı ve sızma girişimini tespit eder ve çeşitli alarm mekanizmaları ile kullanıcıyı uyarır. Saldırı imzalarının düzenli olarak güncellenmesi sayesinde oldukça farklı sayıda ve türde saldırıyı tespit edebilmek mümkündür. Açık kaynak kodlu ve sürekli geliştirilmeye açık olması popülerliğini artırmıştır. Ticari yazılımlarda kaynak kodun açık olmaması, ordu, kamu kuruluşları ve özel sektör gibi üst düzey güvenlik isteyen kuruluşlar tarafından Snort'un daha çok tercih edilmesini sağlamıştır. Farklı kullanım modları sayesinde kullanıcıya kolaylık sağlaması ve yönetilebilir olması ise diğer önemli özelliklerindendir (Güven, 2007).

Snort saldırı tespit sisteminin üç farklı çalışma modu bulunmaktadır. Bunlar, ağ trafiğini izleme modu (packet sniffer), paket kaydedici modu (packet logger) ve ağ temelli saldırı tespit sistemi modu (NIDS)'dur. Paket izleme modu Tcpdump gibi çalışmakta ve bilinen paket izleme programlarına benzer yapıdadır. Paket loglama modu, istenilen türdeki paketlerin loglanıp analiz edilmek üzere saklanmasını sağlar. NIDS modu ise Snort'un asıl kullanım amacını barındırır. Bu mod, gelen paketlerin kullanıcı tanımlı kurallarla analiz edilmesini sağlar. Snort'un çalışma mantığını ve izah edilen farklı çalışma modlarını anlamak açısından Şekil 16'da verilen akış şeması yararlı olacaktır.

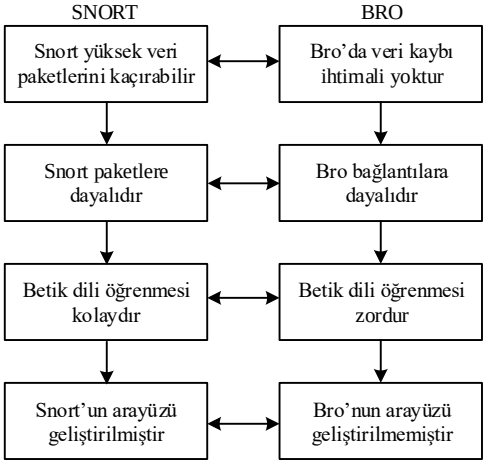


Şekil 16. Snort akış şeması

Snort'un temel olarak bir bilgisayar ağında konumlandırılması Şekil 17'de verildiği gibidir. Snort, güvenlik duvarının pasif izleme yeteneğini dinamik, öğrenen izleme kabiliyeti ile tamamlar. Buradan da anlaşıldığı gibi bilgisayar ağlarında firewall ile birlikte kullanılır ve olmazsa olmaz güvenlik araçlarından biridir. Şekil 18, Snort ve Bro saldırı tespit sistemlerinin bir karşılaştırmasını içermektedir.



Şekil 17. Snort'un konumlandırılma senaryoları



Şekil 18. Snort&Bro karşılaştırılması

SnortSam

Snortsam, Snort sistemine "ses" özelliği katan bir eklentidir. Snortsam iki ana kısımdan oluşmuştur. Bu kısımlardan biri Snort için çıkış sistemidir, diğeri de güvenlik duvarı (GD) üzerinde ajan vazifesi görecek kısımdır. Snortsam kurulumundan sonra Snort kurallarına "fwsam" anahtar kelimesi eklenir. Snortsam'ın kullanımı fwsam anahtar kelimesiyle yapılır. Snort üzerine yazılan kurallar snortsam ajanı aracılığı ile güvenlik duvarına aktarılır ve engellenmesi gereken trafik güvenlik duvarı tarafından durdurulur.

Selks

Debian üzerine, Suricata, Elasticsearch, Logstash, Kibana ve Scirius isimli bileşenlerini kullanarak oluşturulmuş, açık kaynak kodlu bir

saldırı tespit sistemidir. Debian bileşeninin kullanılmış olması Selks'i farklı kılmıştır. Selks, Stamus Networks tarafından geliştirilmiştir ve GPLv3 lisansı ile dağıtılmaktadır. SELKS için tanımlanmış 10'dan fazla varsayılan IDS dashboard (pano) bulunmaktadır (Joshua vd., 2013; McRee, 2011). Bu IDS Panoları, ALL, ALERTS, DNS, FILE-Transactions, FLOW, HTTP, HTTP-Extended-Custom, PRIVACY, SSH ve TLS şeklindedir. Selks STS'yi oluşturan bileşenler ise:

S- Suricata IDPS,
E- Elasticsearch,
L- Logstash,
K- Kibana,
S- Scrius şeklindedir.

Suricata, OISF (Open Information Security Foundation) tarafından geliştirilmiştir ve GPL lisansı ile dağıtılan bir tür saldırı tespit sistemidir.
Elasticsearch, esnek, güçlü ve ölçeklendirilebilir bir (full-text) arama ve analitik motorudur. Suricata üzerinden gelen alarmlar Elasticsearch üzerinde depolanmaktadır. Daha sonra depolanan alarmlar analiz edilmektedir.
Logstash, SELKS mimarisinde Suricata tarafından üretilen ham verinin sorgulanarak analiz edilebilmesine olanak sağlamak amacı ile formatlanması (JSON) ve Elasticsearch'e yazılmasını sağlamaktadır.
Kibana ise, Suricata tarafından üretilmiş bir SELKS bileşenidir. Logstash tarafından formatlanarak Elasticsearch tarafından depolanan verinin analiz edilip görselleştirilmesine imkân sağlar.
Scirius, Stamus Networks tarafından geliştirilen ve Suricata için web tabanlı yönetim arabirimi imkânı sunan bir başka açık kaynak kodlu bir projedir. Selks, eğer nodesktop şeklinde kurulacaksa minimum 4gb bellek, 2gb ram ihtiyacı olacağı düşünülmektedir. Fakat desktop seçeneği ile masaüstü sürümü kullanılacaksa minimum çift çekirdek kullanılması tavsiye edilir.

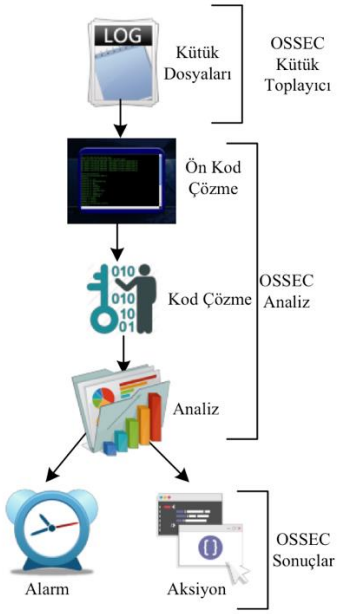
Ossec

Ossec (Open Source Host-based IDS), Trend Micro firmasınca desteklenen Linux, OpenBSD, Windows 2000/XP/2003/, FreeBSD, Vista, Solaris, OSX işletim sistemli bilgisayarlarda herhangi bir sorun oluşturmadan kurulabilen ve bilgisayar üzerinde yüklü olan uygulamaların çalışmalarını kontrol eden, OPEN SOURCE (açık kaynak kodlu) bir STS aracıdır. Ossec, mevcut durumdaki veri paketleri, servis ve onların kaynaklarını kullanarak sistemi inceler ve kullanıcıları bu risklere karşı uyarır. Ossec, tek bir oturumda çalışabilmeye olanak tanıyarak, merkezi yönetim sağlayabilen agent/master yapılı bir host-based STS dir. Ossec, mevcut olan yapısından dolayı SIM/SIEM platformları ile de tümleşik olarak tasarlanabilir. Şekil 19'da çalışma mimarisi verilen Ossec, bu şekilde tanımlar oluşturabilmesinin yanında başka özelliklere de sahiptir (Joshua vd., 2013; Bray vd., 2008). Bu özellikler;

1) Dosya Bütünlük Kontrolü: File Integrity Monitoring (FIM) denen özellik, temelinde sistemde var olan dosyaların belirli aralıklarla kontrol edilmesi kuralını temel almaktadır. Yapılan her kontrolde, var olan dosyaların toplamından MD5 tarzı şifreleme algoritmalarıyla bir şifre oluşturulur. Dosyaların boyutlarında veya diğer özellikler bazında yapılan değişikliklerin tarih ile kayıt altına alınması yoluyla oluşturulan şifre, yapılan kontrollerde bir önceki şifre ile kıyaslanır. Böylelikle dosyalarda herhangi bir değişiklik olup olmadığı gözlemlenir. Değişikliğe uğramış dosyaların tespitini ve yapılan değişikliklerin sistem yöneticisine bildirilmesini temel hedef edinmiştir. Sisteme sızmayı amaçlayan her çeşit saldırının ortak noktasının sistemde mevcut olan dosyalar üzerinde değişiklik yapmak ya da sisteme bir takım dosyalar ilave etmek olduğu biliniyorsa, HIDS'ler açısından dosya bütünlük kontrolünün önemli bir bileşen olduğu söylenebilir. Sistemlerde meydana gelebilecek bu değişiklikleri, değişiklik olduğu an tespit etmek büyük önem arz etmektedir.

2) Rootkit Tespiti (rootkit detection): Rootkit, sistemde mevcut olan süreç/dosya yapılarını gizlemek şartı ile işletim sisteminin gerçeği görmesine engel olmak amacıyla geliştirilmiş olan yazılımlardır. Örnek verilecek olursa; "ps" komutunun görevini değiştirmek için oluşturulan rootkit, sistemdeki kullanıcıların tüm süreci görüntülemesi için verilen izni kaldıracaktır. Bu özellik ile Ossec, sistemdeki mevcut rootkitlerin

tespit edilmesini sağlayarak tehlikelere karşı uyarı verir.



Şekil 19. Ossec çalışma mimarisi

3) Log Monitoring: Değişikliklerin tespit edilmesinin hemen ardından ise kontrolü yapılması gereken log dosyalarıdır. Bu amaca hizmet etmek ve bu soruna çözüm bulmak amacıyla sistem loglarını izleyen OSSEC, analiz işlemini gerçekleştirir ve bir problemin tespitinde hemen alarm oluşturarak sistem yöneticisine bu konuda bilgi verir. Bu duruma örnek vermek gerekirse, sistem üzerinde bir paket kurulduğu vakit ya da web sunucusunun loglarına bir sızma girişimini belirten satırlar gelmeye başladığında, alarm üretilir ve bu durumun farkına varılması, sisteme sızma girişiminin tespitine katkı sağlamış olur. Ossec, bu özellikleri ile rakiplerinden daha fazla ön plandadır. Open Source (açık kaynak kodlu) yazılım olması ve genel kamu lisansı ile dağıtılmasından dolayı da STS araçları arasında en fazla tercih edilenler arasındadır.

Firestorm

Firestorm, son derece yüksek performansa sahip bir ağ saldırı tespit sistemidir. Firestorm son derece esnektir ve bundan dolayı yönetilebilir bir yapıya sahiptir. Bu özelliğiyle diğer sistemlere göre çok daha iyi bir performans gösterir. Firestorm ilk olarak sadece bir sensör niteliğindeydi, daha sonra uzaktan kontrol, raporlama ve analiz için gerekli destekler verilmesi planlanmıştır. Ağ üzerinde şüpheli paketleri belirlemeye yarayan Firestorm, durum bilgilerini analiz edebilir, IP çerçevelerini yeniden oluşturup, TCP bağlantılarını izleyebilir. Firestorm uygulama katmanı üzerinde çalışabilen tüm protokolleri çözebilme kapasitesine ve anomali tespiti modüllerini destekleyebilecek altyapıya sahiptir. Firestorm ayrıca snort gibi ağ trafiğini kontrol eder ve bu analiz sonucu oluşan kayıtları tutar. Firestorm, DOS saldırılarına karşı kendini koruyabilme ve uyarı verme yeteneğine sahiptir (Leach vd., 2003).

Kfsensor

KFSensor, Windows tabanlı honeypot bir STS'dir. KFSensor, honeypot gibi zayıf bir sistem gibi görünerek hacker, solucan ve trojanları tespit eder. Bu tespit işlemini gerçekleştirirken port taramaları yaparak sisteme sızmaya çalışanları belirler ve .txt uzantılı log kaydı tutar. KFSensor Windows tabanlı olarak kurumsal bir ortamda kullanılmak amacıyla tasarlanmış, Snort uyumlu imza motoru, MS Windows ağ protokolleri ve emülasyonlar gibi birçok yenilikçi ve benzersiz özellikler barındırır. KFSensor'un yüklenmesi ve yapılandırılması kolaydır. Hiçbir özel donanım gerekmez ve etkin tasarımı, düşük özellikli Windows makinelerinde bile çalışmasını sağlar. Basit Windows arabirimi tüm işlevleri denetler. Karmaşık yapılandırma dosyalarını düzenlemeye gerek yoktur ve gerekli tüm önemli sistem hizmetleri ile önceden yapılandırılmıştır.
KFSensor, OSI Ağ Modelinin en üst düzeyindeki - uygulama katmanı- sistem servislerini taklit ederek çalışmaktadır. KFSensor çalıştıran bir makine, yönlendiricilere ve güvenlik duvarlarına karmaşık değişiklikler yapmaya gerek kalmadan ağdaki başka bir sunucu gibi davranır. KFSensor, bir ağdaki saldırıların doğasını ve miktarını ortaya çıkarmak için faydalar sağlar. KFSensor'un ürettiği bilgiler, güvenlik duvarı kurallarını iyileştirmek ve ağ saldırı tespit sistemleri için yeni imzalar üretmek için kullanılabilir. KFSensor, ağ güvenlik altyapısını

geliştirmenin son derece uygun maliyetli bir yoludur. Kendine ait olan GUI tabanlı yönetim konsolu, kapsamlı dokümantasyon ve düşük bakım maliyeti nedeniyle KFSensor bir kuruluşun ağ güvenliğini sağlamak için uygun bir çözüm sunar (Kfsensor, 2003).

Suricata

Suricata, ticari kaygı barındırmayan bir oluşum olan OISF (Open Information Security Foundation) tarafından geliştirilmiş Open Source (Açık Kaynak Kod) bir saldırı tespit sistemidir. İmza/kural tabanlı olarak çalışan Suricata, gelen saldırıları tespit etmesinin (IDS) yanında bu saldırıları engelleme (IPS) özelliğine de sahiptir. Bu özellik (IPS) ile yakalanan paketlerin çalıştırılması, reddedilmesi ve istatistiksel bilgilerinin tutulmasına da imkân sağlar. Suricata tarafından sistem çalışması yapılırken kullanılacak yeni mod, başlangıçta verilecek parametreler ile düzenlenmektedir. Çalışma sürecinde ise kural ekleme-çıkarma işlemi yapılmasına olanak tanıyan Suricata, IPv6 yapısını da desteklemektedir. Bu özelliklerden farklı olarak Suricata, bazı ek özellikler ile de yenilik getirmiştir. Bu özellikler (Joshua vd., 2011; Manev, 2012): (1)HTTP kütüphanesi: HTTP trafiklerinin ayrıştırılmasına olanak tanıyarak, saldırganların STS'leri atlatarak sisteme sızma girişimlerini engelleyen bir normalizasyon aracıdır.

Çoklu iş parçacıkları: Paket işleme işlevi farklı bölümlerde yapılmaktadır. Yani paketler farklı makinelerde çalışıyormuş gibi dağıtık olarak işlenmekte ve performansta artış sağlanarak yük dengesi yapılmaktadır. Bu işlem Multi-threaded olarak bilinmektedir. Suricata Unix soket modunda işlem görerek ağ trafiğini pcap formatında kayıt edilmesini sağlar. Kaydedilen bu ağ trafiği kayıtları daha sonra offline olarak analiz edilebilmektedir. Ayrıca Suricata, HTTP istekleri, SSH bağlantıları, TLS el sıkışmalarını kaydedebilmeye olanak tanımaktadır. Suricata işleyişinde 4 kısma ayrılmaktadır (Joshua vd., 2011). Bu kısımlar:

Paket Yakalama Modülü: Capture Module olarak bilinen bu modül, belirlenmiş olan paketlerin Ethernet kartından Suricata'ya iletilmesini sağlamaktadır. Bu modül, paketlerin farklı veri bağı çözümleyicileriyle uygun olarak çalıştırılmasını sağlar.

Paket Çözümleme Modülü: Decoding Module denilen bu modül ise paketlerin ara belleğe alınarak Suricata'nın kullanabileceği veri yapısına çevrilmesinden sorumludur. Burada paketler veri linklerine göre ayrılıp, çözümleyiciler tarafından işlenmiş olurlar.

Akış İşlemleri Modülü: Stream Module denilen bu yapı ise temelde 3 görev üstlenmektedir. Bunlar:

- Ağ bağlantılarının doğru olması için akış takibi,
- TCP bağlantılarında tekrar oluşturulan ana akış için paketlerin sıralanması,
- HTTP - DCERPC analiziyle uygulama katmanı denetimi.

Tespit Modülü: Detect Module, yapılandırılmış kuralların belirlenip yüklenmesi, tespitin başlaması ve kuralların paketler ile eşleştirilmesine olanak tanır.

Suricata'da tanımlanmış 3 profil mevcuttur. "yüksek, orta ve düşük" olmak üzere oluşturulmuş bu profiller içerisinde, varsayılan profil, bellek kullanımı ile performans arasında bir denge sağlayan "orta" dır.

Snorby

Snorby, Snort, Suricata gibi popüler saldırı tespit sistemli uygulamalar gibi ağ güvenliğini izlemek amacıyla, Ruby Dili ile yazılmış bir uygulamadır [26]. Ruby ile bir deneyim kazanmadan, çalışma yapılmadan Snorby ile uğraşmak zor olabilmektedir. Saldırı tespit sistemimizde doğru ayar ve güncellemeleri yapmak için Snorby'i iyi bir şekilde kavramak önemlidir. Snorby, sensörlerden gelen IDS/IPS alertlerini toplayan, merkezi bir konsol olarak da kabul edilebilir. Snorby'nin diğer STS uygulamalarından farkı daha fonksiyonel olmasıdır (Snorby, 2010).

Phpids

PHPIDS, PHP web uygulamalarında kullanılan açık kaynak kodlu, hızlı, kullanımı kolay, iyi yapılandırılmış ve güvenilir bir saldırı tespit sistemidir. PHPIDS web uygulamaları üzerinde

çapraz site betikleme (XSS), SQL Enjeksiyonu (SQL Injection), başlık enjeksiyonu (Header Injection), Dizin atlama (Directory Traversal), RFI/LFI, hizmet engelleme (DOS) gibi saldırı türlerini analiz edebilmektedir (Phpids, 2007).

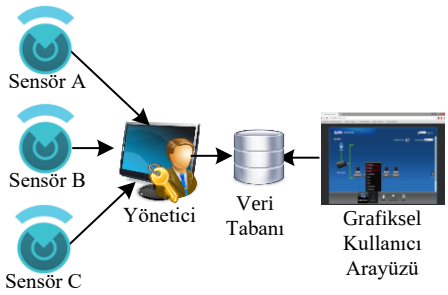
PHPIDS kötü bilinen uygulamaları tespit etmek için birkaç düzenli uygulama ile çalışır. Bunu yapmak için temelde kara liste yaklaşımını, bilinmeyen saldırı örüntülerini yakalamak için sezgisel yaklaşımlar ile birleştirir. Özel dönüşüm algoritmaları sayesinde PHPIDS, siteme sızan saldırıların tespit edilmesi ve bunların kayıtlarının tutulmasını sağlar.

.Net Ids

.NETIDS olarak isimlendirilen bu araç, web tabanlı .NET uygulamalarını korumanın diğer bir yoludur. Bu araç, web uygulamalarına karşı yapılan saldırıları tespit yeteneğine sahiptir. .NETIDS ile oluşturulan saldırı tespit sisteminin dosyaları, mümkün olan saldırılarla etkileşime geçmek için filtreleme kuralları ve fonksiyonlar barındırır. .NetIDS, daha önce var olan PHPIDS'in .Net framework için geliştirilmiş olan bir türüdür. .NETIDS'in kütüphanesi, CLS uyumludur ve PHP versiyonundaki filtreleme sistemleri benzer şekilde uygulanmıştır. .NETIDS sistemleri ile kullanılan herhangi bir .Net uygulaması için ek koruma katmanları oluşturmak temel amaçtır. Bunun yanında .NETIDS, XSS'in belirlenmesi, SQL Injection, zararlı JS nesne ve metotlarına karşı koruma, gelişmiş loglama fonksiyonları, filtreleme kuralları ve arayüzleri kategorize etme ve etiketleme özelliklerini içerir (.Netids, 2007).

Prelude

Prelude bir SIEM (Bilgi Güvenliği Tehdit ve Olay Yönetimi) yani güvenlik kontrol aracıdır. Prelude, merkezi bir yönetim noktası sağlamak amacıyla ağın güvenlik bilgilerini toplar ve bu bilgileri merkezileştirir. Günlük dediğimiz kütük dosyalarının analizi ve ilişkilendirilmesi sayesinde Prelude, ağdaki gerçek zamanlı saldırı girişimlerini tespit eder ve tehditler konusunda uyarı verir. Şekil 20'de basit mimari yapısı verilen Prelude, büyük veriler üzerinde gelişmiş kalıcı tehditlerin (APT) önlenmesini sağlayabilecek zayıf sinyalleri tanımlamak için birkaç araştırma ve raporlama aracı sunar. Sonuç olarak, Prelude, güvenlik konusunda; operatörlerin işini ve risk yönetimini basitleştirmek için operasyona yardımcı olacak tüm araçlara sahiptir (Prelude, 2012).



Şekil 20. Prelude basit mimari yapısı

Aide

AIDE, gelişmiş izinsiz giriş algılama ortamı adıyla bilinen, bir dosya ve dizin bütünlüğü denetleyicisidir. AIDE, çalışma mantığı olarak temelde, yapılandırma dosyasından bulduğu düzenli ifade kurallarından bir veri tabanı oluşturur. Bu veri tabanı başlatıldığında, dosyaların bütünlüğünü doğrulamak için kullanılabilmektedir. Dosyanın bütünlüğünü kontrol etmek için ise kullanılan birkaç mesaj özet algoritmasına sahiptir. Genel olarak işleyişte yer alan her zamanki dosya özeliklerinin tümü de tutarsızlıklar açısından kontrol edilebilmektedir. Eski veya daha yeni sürümlerden veri tabanlarını okuyabilme özelliğine de sahip olan AIDE: md5, sha1, rmd160, tiger, crc32, sha256, sha512, whirlpool (ek olarak libmhash: gost, haval, crc32b) gibi mesaj özet algoritmalarını da desteklemektedir. Ayrıca: Dosya türü, İzinler, Inode, Uid, Gid, Bağlantı adı, Boyut, Blok sayısı, Bağlantıların sayısı, Mtime, Ctime ve Atime gibi dosya öznitelikleri de desteklenmektedir (Aide, 2004).

Samhain

Host tabanlı bir saldırı tespit sistemi (HIDS) özelliği taşımaktadır. Samhain dosya bütünlüğünün denetimi ve günlük dosyası izleme/analizinin yanı sıra rootkit algılama, bağlantı noktası izleme, sahte SUID

çalıştırılabilir dosyalarını algılama gibi özellikleri sahip olmakla birlikte sistem üzerindeki gizli süreçleri de tespit etme olanağı sağlar. Samhain, tek bir ana bilgisayarda bağımsız uygulama olarak kullanılabilir olmasına rağmen, merkezi olarak günlüğe (log) kaydetme ve bakım sağlayarak potansiyel olarak farklı işletim sistemleri olan birden çok ana bilgisayarı izlemek üzere tasarlanmıştır. Ayrıca, POSIX sistemleri (Unix, Linux, Cygwin / Windows) için açık kaynak kodlu çoklu platform uygulamasıdır (Samhain, 2001).

Acarm-ng

Bilgisayar ağlarındaki trafik analizlerini önemli ölçüde kolaylaştırabilen bir uyarı korelasyon yazılımıdır. Sırasıyla NIDS ve HIDS olarak da bilinen ağ ve ana sensörler tarafından gönderilmiş olan toplama ve korelasyon uyarılarından sorumludur. Gerçekleştirilmek istenen korelasyon süreci, benzer olayları kötü amaçlı etkinliğin mantıksal parçalarını temsil eden grupları birleştirerek, bir sistem yöneticisi tarafından görüntülenmesi gereken toplam mesaj sayısını olabildiğince aza indirmeyi amaçlar. Bu tür uyarı gruplarına meta-uyarılar denir ve tek bir makinedeki bir grup başarısız kullanıcı girişinden, servis tanıma, ardından giriş girişimi veya bir bot ağı kurma gibi daha karmaşık saldırı senaryolarına kadar değişebilir (Acarm-ng, 1991).

Tablo 1. Saldırı tespit yöntemine göre güncel STS araçlarının karşılaştırılması

STS	Saldırı Tespit Yöntemi	STS Türü
Snort	Anormallik Tespiti, Kötüye Kullanım	IDPS, NIDS
Bro	İmza, Kötüye Kullanım	NIDS
Selks	İmza, Kötüye Kullanım	NIDS
Suricata	İmza, Kötüye Kullanım	IDPS, NIDS
Ossec	Anormallik Tespiti, Kural Eşleştirme	HIDS
Kfsensor	İmza, Kural Tabanlı	Honeypot IDS
PhpIDS	Anormallik Tespiti, İmza, Kural Tabanlı	HIDS
.NetIDS	İmza, Kural Tabanlı	HIDS
Firestorm	Anormallik Tespiti, İmza, Kural Tabanlı	NIDS

Bilgisayar kümesinin ve/veya ağ saldırılarının hedefi olan bir ağın operatörü olarak çalışan yöneticiler için bu araç, olaylara tepki süresini azaltarak, sistem güvenliğine daha fazla zaman tanıyacak şekilde yararlı olabilme özelliğine de sahiptir. Tablo 1, mevcut saldırı tespit sistemlerinin karşılaştırılmasını içermektedir. Karşılaştırma kriteri olarak saldırı tespitinde kullanılan yöntem ve çalışma mantığını içerecek şekilde STS türü nitelikleri kullanılmıştır. Tablo 2 ise saldırı tespit sistemlerinin çalışma zamanı, kullanılan veri ve mimari yapı özellikleri bazında sınıflandırılmasını sunmaktadır.

Tablo 2. Bazı STS araçlarının sınıflandırılması

STS	Çalışma Zamanı	Kullanılan Veri	STS Mimarisi
Snort	Gerçek Zamanlı	Ağ	Hibrit
Bro	Gerçek Zamanlı	Ağ	Merkezi
Selks	Gerçek Zamanlı	Ağ	Merkezi
Emerald	Gerçek Zamanlı	Ağ, Sunucu	Dağıtık
Suricata	Gerçek Zamanlı	Ağ	Merkezi
Haystack	Gerçek Zamanlı Değil	Sunucu	Merkezi
Ossec	Gerçek Zamanlı	Sunucu	Dağıtık
Kfsensor	Gerçek Zamanlı	Ağ	Merkezi
PhpIDS	Gerçek Zamanlı	Ağ	Merkezi
.NetIDS	Gerçek Zamanlı	Ağ	Merkezi
Firestorm	Gerçek Zamanlı	Ağ	Merkezi
DIDS	Gerçek Zamanlı	Ağ, Sunucu	Dağıtık
Tripwire	Gerçek Zamanlı Değil	Sunucu	Merkezi
FIRE	Gerçek Zamanlı Değil	Ağ	Merkezi
Snorby	Gerçek Zamanlı	Ağ	Merkezi

Sonuç

Günümüz dünyasında ticari ve resmi kurum/kuruluşlar çalışmalarında yoğun olarak bilgi kullanımına ihtiyaç duymaktadırlar.

Gelişen teknoloji ile birlikte, geçmişe dair bilgilerin önemi de artmakta ve bu veriler istatistiksel olarak çeşitli araştırma sonuçları için kullanılmaktadır. Bu sebeple bilginin güvenli bir şekilde saklanması ve istenildiği zaman, yetkili kişiler tarafından kullanılabilir durumda olması oldukça önemli bir hal almıştır. Bilginin önem düzeyinin artması ve bu sebeple bilgiye olan bu bağımlılığın yükselmesi bilginin korunması için kullanılması gerekli olan sistemleri de zorunlu kılmaktadır. Bu sistemler bilgiye yönelik olası tehditlerin veya saldırıların tespit ve engellenmesinde kullanılırlar. Ayrıca saldırılar sonucu oluşabilecek bilgi tahribi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, sistem altyapısının bozulması ve dolayısıyla meydana gelebilecek maddi manevi kayıpların önlenmesi açısından önem arz ederler. Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin başarılı bir şekilde sağlanabilmesi, bilginin gizliliği, bütünlüğü ve kullanılabilirliği etmenlerinin tam anlamıyla korunması ile mümkündür. Bu amaçla kullanılabilecek güvenlik sistemlerinin vazgeçilmez temel bileşenlerinden biri de saldırı tespit sistemleridir. Bilgi güvenliği bir süreçtir. Bu sürecin her bir unsuru tek başına yeterli değildir. Dolayısıyla bu çalışma kapsamında incelenen saldırı tespit ve engelleme sistemleri de bütün bir ağ veya sistemin güvenliğini sağlayabilir demek afaki bir görüş olacaktır. Diğer ağ güvenliği sistemleri ile birlikte kullanılan saldırı tespit ve engelleme sistemleri, bilgi güvenliğini tamamlayıcı bir unsur olarak oldukça yararlı olacaktır.

Bu makale çalışmasında, bilgi güvenliği sistemlerinde yaygın olarak kullanılan STS'ler incelenmiştir. Özellikle veri tabanlarından veri ambarlarına, veri ambarlarından ise "büyük veri" olarak literatüre giren veri yığınlarının kullanıldığı günümüzde STS'ler bilgi güvenliği sistemlerinin olmazsa olmaz bir parçası olarak karşımıza çıkmaktadır. Yapılan incelemeler sonucunda, yeni geliştirilen saldırı örüntülerini de yakalama potansiyeline sahip olan akıllı-öğrenen saldırı tespit sistemlerinin geliştirilmesi gerektiği açıktır. Ayrıca özellikle STS'lerin olumsuz özelliği olan yanlış alarm seviyesinin düşük olduğu yeni sistemlere de ihtiyaç duyulmaktadır. Bu inceleme çalışmasında, özellikle geçmişten günümüze yeni nesil saldırı tespit sistemleri üzerinde durulmuş ve bu sistemlerin bir karşılaştırılması da sunulmuştur. Yapılan araştırmalar, bilgisayar ağ güvenliğinin en önemli yapılarından birisi olan saldırı tespit ve engelleme sistemlerinin önemini açıkça ortaya koymaktadır. Bu önem sebebiyledir ki, saldırı tespit ve engelleme sistemleri sürekli olarak güncellenmekte ve yeni tür saldırı tespit yazılım ve donanımları geliştirilmektedir.

Teşekkür

Bu çalışma, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Biriminin (FÜBAP) TEKF.15.04 numaralı projesi ile desteklenmiştir.

Kaynaklar

ACARM-ng. "Alert Correlation, Assessment and Reaction Module-Next Generation". http://www.acarm.wcss.wroc.pl (28.02.2018).

AIDE. "Advanced Intrusion Detection Environment". http://aide.sourceforge.net/ (24.02.2018).

Ağ Güvenliği. "Sızma Belirlemede Anormallik Tespiti Kullanımı". http://web.itu.edu.tr/orencik/SizmaBelirlemedeAnormallikTespitiKullanimi.pdf (01.02.2018).

Anderson J.P. "Computer Security Threat Monitoring and Surveillance", *Technical Report*. James P. Anderson Co., Fort Washington, PA, 1980.

Axelsson, S. "Intrusion detection systems: A survey and taxonomy", Technical Report 99- 15, Dept. of Computer Eng. Chalmers University of Technology, Göteborg, Sweden, 1-23 (2000).

Baykara M, Daş R, Karadogan İ. "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", *1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli*

Bilişim ve Güvenlik Sempozyumu)", 231-239, 20-21 Mayıs 2013, Elazığ - Turkey.

Biermann, E. Cloete, L. M. Venter. "A Comparison of Intrusion Detection Systems", *Computers & Security*, vol. 20 pp. 676-683, 2001.

Bray R, Cid D. Hay A. "OSSEC Host-Based Intrusion Detection Guide". Foreword by Stephen Northcutt, President The SANS Technology Institute, 2008.

Dayıoğlu B, Özgit A. "Internet'de Saldırı Tespiti Teknolojileri", *İletişim Teknolojileri I. Sempozyumu ve Fuarı,* 17-21 Ekim 2001, Ankara.

Depren O, Topallar M, Anarim E, Ciliz, M.K. "An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks", *Expert System with Applications*, vol. 29 pp. 713-722, 2005.

Ilgun K. "Ustat: A real-time intrusion detection system for Unix", *Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy*, Oakland, California, 16-28, (1993).

Fisch, Eric A. and Gregory B. White. "Secure computers and networks: analysis, design, and implementation", CRC Press, 1999.

Güven, E. N. Sağıroğlu Ş. "Saldırı Tespit Sistemleri Üzerine Bir İnceleme", *3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 2008.

Güven E. N. "Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2007.

Joshua, S. Whitea, Thomas T. Fitzsimmonsb, Jeanna N. Matthewsc, "Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata", Wallace H. Coulter School of Engineering Department of Computer Science, 2011.

Kfsensor. "Advanced Windows Honeypot System". http://www.keyfocus.net/kfsensor (06.01.2018).

Manev, P. "Windows Installation Guide for Suricata IDS/IPS". Open Information Security Foundation, Document Version 1.3, 2012.

McRee R. "BroIDS with Logstash and Kibana", ISSA Journal pp. 37-39, September 2013.

NETIDS. "Intrusion detection system for .NET based on phpids". https://code.google.com/p/dotnetids/ (12.02.2018).

Pasin Ş. "Çok Algılayıcılı Saldırı Tespit Sistemleri", Gebze Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü, Veri ve Ağ Güvenliği Dersi Projesi, 2002.

Patcha A. Park J.M. "An overview of anomaly detection techniques: Existing solutions and latest technological trends", *Computer Networks*, 51(12): pp.3448-3470, 2007.

Phpids. "PHP-Intrusion Detection System". https://github.com/PHPIDS/PHPIDS (12.06.2016).

Prelude."Prelude Security Information & Event Management". http://www.prelude-siem.com/en (24.02.2018).

Samhain. "File integrity / host-based intrusion detection system". http://www.la-samhna.de/samhain/ (25.02.2018).

Sancak, S. "Saldırı Tespit Sistemi Tekniklerinin Karşılaştırılması", Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, 2008.

Sazlı H, M Tanrıkulu. "Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması", *XII. Türkiye'de İnternet Konferansı*, 8-10 Kasım, Ankara, 2007.

S. E. Smaha, "Haystack: an intrusion detection system," *Aerospace Computer Security Applications Conference*, Fourth, Orlando, FL, pp. 37-44, 1988.

Snorby. "Ruby On Rails Application for Network Security Monitoring". https://github.com/Snorby/snorby (02.01.2018).

Şahinaslan E, Kantürk, A, Şahinaslan, Ö, Borandağ, E. "Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri", *Akademik Bilişim*, *9*, 11-13, 2009.

Weijian Huang, Yan An, Wei Du. "A Multi-Agent-Based Distributed Intrusion Detection System", *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol.3, pp.141-143, 20-22 Aug. 2010.

Yıldız E, Arıcı N. "Gerçek Zamanlı Bir Saldırı Tespit Sistemi Tasarımı Ve Gerçekleştirimi", *E-Journal of New World Sciences Academy Engineering Sciences*, 1A0072, 5, (2), 143-159, 2010.

Investigation of intrusion detection and prevention tools

Extended abstract

The importance of information security in the digital information age with technological developments, is increasing day by day. In terms of individual and institutional, storage of information, protection privacy and guarantee reaching by authorized persons only to the accessibility is very important. Many different studies carried out in order to ensure security in information systems and are continuing to do. In this study, one of the indispensable tools of information security intrusion detection systems have been examined in detail. After detailed review, these tools have been classified according to data source, architectural structure and working time. In addition, these tools have been compared according to the type of intrusion detection system and intrusion detection method.

In today's world, commercial and official institutions/ organizations need to use intensive information in their work. With the developing technology, the importance of past information also increases, this data is used statistically for various research results. For this reason, it has become very important that the information is stored safely and when it is requested, it can be used by the authorized persons. Increased level of importance of the information for this reason rise of the addiction of information makes compulsory the systems that are required to be used for the protection of information. These systems are used to detect and prevent possible threats to information. In addition, the consequences of the attacks are important in terms of the destruction, deletion, destruction of integrity and / or confidentiality, the deterioration of the system infrastructure and thus the material moral losses that may occur. Information is an asset like other assets in the organization, that is important to the organization and must be best protected for this reason. Information security; ensuring continuity of the work in the institution, reducing business interruptions, and protecting information from widespread threats to increase future benefits. Whatever form the information is in, it must be preserved in an appropriate manner. The availability of information security is only possible if the privacy of the information, its integrity and its availability are at a sufficient level. One of the indispensable parts of the security systems that can be used for this purpose is intrusion detection systems.

In this paper, intrusion detection systems are examined which commonly used in information security systems. As a result of the investigation made, it is clear that intelligent-learning intrusion detection systems with potentiation of newly developed attack patterns should be developed. In addition, new systems are also needed where the false alarm level, which is a negative feature of intrusion detection systems, is low.

This study focuses on the next generation intrusion detection systems, especially from past to present and a comparison of these systems is also presented. The researches clearly demonstrate the importance of intrusion detection and prevention systems which one of the most important structures of computer network security. According to this importance, intrusion detection and prevention systems are constantly being updated and new types of attack detection software and hardware are being developed.

Information security is a process. Each element of this process is not enough for alone. Therefore, the intrusion detection and prevention systems which examined in the scope of this study will be an unnecessary opinion that it can provide security of an entire network or system. Intrusion detection and prevention systems used in conjunction with other network security systems will be useful as a complement to information security.

Keywords: *Computer security, information security, intrusion detection system, intrusion prevention system*