

**Bilgisayar-Bilgi Güvenliği ve Yönetimi/ BM-302**

**Section 2.2.1-2.2.3**

**Hazırlayan:**

**Adı: Ümit**

**Soyadı: SARAÇ**

**Numarası: 140757019**

**Dersi Veren: Prof.Dr. Abdulsamet HAŞILOĞLU**

**Enclaves: The Enterprise as an Extranet**

Bryan T. Koch, CISSP

**1.1 Güvenlik içeriği**

Güvenlik politikaları, prosedürleri ve teknolojilerinin, Girişimcilik sistemleri. Ancak, güvenlik tehditlerinin niteliği ve başarılı olma ihtimalleri Kurumsal sistemlere karşı konuşlandırılmış, değişti. Bu kısmen bilgisayar teknolojisi ve bilgisayar ağlarının işletmelere dağılması ve kısmen de internetin bir sonucudur.

Daha büyük ve daha eski kuruluşlar için, güvenlik açıklarını ve eski anabilgisayar ortamlarındaki tehditler. Daha yeni tehditleri ele almak için eski politikalar tamamlanmıştır bilgisayar virüsleri, uzaktan erişim ve e-posta gibi. Bu yazarın deneyiminde, mevcut politika için nadir ağ tabanlı tehditleri etkin bir şekilde ele almak için çerçeveler. LAN'lar ve PC'ler haline gelenin ilk adımıydı. artan karmaşıklık ve karşılıklı ilişkililik maratonu; intranet (dahili ağlar ve uygulamalara dayalı IP), extranet ve Internet girişimleri bunun en yaygın örnekleridir.

Kısmen “açık” bir ağ olarak başladığı ve kısmen ticari kullanımın patlaması nedeniyle, İnternet

Ayrıca, güvenlik mimarileri, araçları ve

İnternet’in yüksek tehditli ortamı. Bu ortamdan ortaya çıkan araçların örnekleri arasında

güvenlik duvarları, sanal özel ağlar ve katmanlı fiziksel mimariler. Bu araçlar

Internet extranet içine.

**1.2 Bir Büyük Ağ Paradigması**

Günümüzde ağ mimarları, entegre bir ağ ortamının yaratılmasıyla görevlendiriliyor. Bir ağ

mimar bunu “her şeyi her şeye, tam şeffaflıkla bağlamak” için bir görev olarak tanımladı.

Yazar buna One Big Network paradigması olarak atıfta bulunur. Bu yazarın deneyiminde, bazı ağ mimarları

Güvenliği kolun uzunluğunda tutmayı hedefliyoruz - “biz inşa ediyoruz, güvenceye alıyorsunuz ve birbirimizle konuşmak zorunda değiliz”

Bu, birleşme ve satın almalardan kaynaklanan hızlı büyümenin mevcut güvenlik bağlamında savunulamaz.

One Big Network, ağ tasarımcıları, ağ kullanıcıları ve şirket yöneticileri için baştan çıkarıcı bir vizyondur. Bir Büyük Ağ - teorik olarak - tedarikçilerle, iş dünyası ile yeni ve daha iyi etkileşimler sağlayacak müşteriler ve son tüketicilerle. One Big Network’e bağlı herkes - teoride - mükemmel şekilde Minimum altyapı maliyetinden faydalanır. Elektronikten işletmeye ve elektronik-ticaret olacak - teoride - her yerde.

Bununla birlikte, kritik bir unsur bu cesur yeni dünyanın dışında bırakıldı: güvenlik. On yıldan fazla olmasına rağmen ağ oluşturma ve kişisel bilgisayarlarda, birçok kurumsal güvenlik ilkesi mirası hedeflemeye devam ediyor çevre, bir bütün olarak ağ değil. Bu politikalar tek başına güvencenin mümkün olduğunu varsaymaktadır “Sistemler” veya “uygulamalar” sanki kurumun geri kalanından bağımsız bir varlığa sahipler. Varsayıyorlar Saldırganların, İnternet’in çeşitli bölümlerini birbirine bağlayan ağ altyapısı yerine uygulamaları hedefleyeceği birlikte dağıtılmış uygulama. Günümüzün otomatik saldırı araçları, ağı tanımlamak için bir bütün olarak hedeflemekte ve zayıf uygulamalara ve sistemlere saldırın ve daha sonra saldırılar için bu sistemleri kullanın.

**1.3 Ağ Güvenliği ve Bir Büyük Ağ Paradigması**

Bir Büyük Ağın yeterince güvenli bir şekilde güvence altına alınabileceği bir zaman olabilir. Eğer varsa, o

gün uzun geçmiş. Bugünün ağları çok daha büyük, çok daha çeşitli, çok daha fazla uygulama çalıştırmak

“Kötü adamların” daha iyi olduğu daha düşmanca bir ortamda daha farklı örgütler bağlayın

her zamankinden daha araçları. Yazar, makul bir güven düzeyinde güvenceye almanın mümkün olmadığını düşünüyor.

ağın tek bir "düz" ağ olarak yönetildiği herhangi bir büyük kuruluş için herhangi bir kurumsal ağ

“herhangi bir şekilde” bağlantısı ile.

Etkili bir iç ağ güvenlik kontrolünün olmadığı bir ortamda, her ağ düğümü bir tehdit oluşturur

diğer her düğüme karşı. (Matematiksel olarak n ağ düğümünün olduğu yerde, tehdit sayısı

yaklaşık n2

.) Kurumun güvenlik duvarı olmadan da internette olması durumunda,

tehditler esasen sonsuz hale gelir (bkz. Ek 31.1).

Etkili kurumsal güvenlik mimarisi, geleneksel, uygulama tabanlı araç setini, ağ tabanlı tehditlere yönelik ağ tabanlı araçlarla genişletmelidir.

**1.4 İnternet Güvenliği Mimarisi Elemanları**

İnternet ve extranet için işletmelerden daha farklı bir tasarım nasıl yapılır? İnternet Nedir / extranet güvenlik mühendisliği ilkeleri?

Basitlik. Karmaşıklık güvenlik düşmanıdır. Karmaşık sistemler daha fazla bileşene sahip, daha tek

başarısızlık noktaları, başarısızlıkların birbiri üzerine basabileceği daha fazla puan ve daha zordur“iyi bilinen” olarak belgelendirmek (nadiren bilinen iyi bileşenlerden yapılmış olsa (bile kendisi) bulunur. Önceliklendirme ve değerleme. İnternet güvenlik sistemleri neyi korumak istediklerini biliyor. Hassasiyet ve her bir öğenin güvenlik açığı hem kendi başına hem de diğeriyle birlikte anlaşılır tasarım unsurları.

Varsayılan olarak reddet, ilke tarafından izin ver. İnternet güvenlik mimarileri, tüm trafiğin olduğu öncülüyle başlar reddedilmek. Yalnızca görevi gerçekleştirmek için açıkça gerekli olan trafik etkinleştirilir ve bu tanımlanmış, belgelenmiş ve analiz edilmiş yollar ve mekanizmalar.

Uçtan uca, yoldan yola analiz. İnternet güvenliği mühendisliği, her ikisi de tüm bileşenlere bakar.

kurumsal taraf ve her işlemin uzak tarafında. Herhangi bir bileşenin arızası veya tehlikesi

tüm sistemin güvenliğini baltalayabilir. Potansiyel zayıf noktalar anlaşılmalı ve eğer

mümkün, başardı. Artık riskler hem işletme hem de işletme tarafından anlaşılmalıdır.

ortaklar ve müşteriler.

**1.5 Enclave Yaklaşımı**

Bu bölüm, işletmeyi bir extranet olarak ele almayı önermektedir. Extranet modeli, bir mimariyi çağırıyor ilk hedefi olarak güvenliği vardır. Bir işletmenin gerçekten neye önem verdiğini belirlemek anlamına gelir: Ne yaşıyor? ya da ölür. Kritik ve güvenli bileşenleri tespit eder ve bunları korunan yerleşim bölgelerine izole eder. Erişim yerleşim bölgeleri ile işletme arasındaki ağ koruyucuları tarafından yönetilir. Yerleşim bölgesi içinde, güvenlik hedefi geleneksel kontrolleri tutarlı ve iyi uygulamaktır. Enklavların dışında, mevcut uygulama (yani güvenlik kontrolleri) resmi güvenlik politikalarına bağlı olarak), teşvik edilmese de, gerçeklik olarak kabul edilmektedir. Bu yeniden yapılanma bazı ağ güvenliği tehditlerini büyüklük sırasına göre azaltabilir. Aşırı ele alındığında, tüm iş biriminden iş birimine etkileşimler enklavlardan geçer.

**IPSec Virtual Private Networks**

James S. Tiller, CISA, CISSP

**1.1 Tarihçe**

1994 yılında, İnternet Mimarisi Kurulu (IAB) “İnternet Mimarisinde Güvenlik” üzerine bir rapor yayınladı.

(Yorum İsteği [RFC] 1636). Rapor, İnternet’in daha fazla ihtiyaç duyduğu genel görüş birliğini belirtti.

ve TCP / IP protokol paketindeki doğal güvenlik zayıflıkları nedeniyle daha iyi güvenlik ve

güvenlik iyileştirmeleri için kilit alanlar. IAB ayrıca aynı güvenlik işlevlerinin bir

IP protokolünün gelecek neslin ayrılmaz bir parçası olan IPv6. Yani, baştan beri, bu gelişen standart

Sürekli gelecek nesil IP ve ağ iletişimi teknolojisi ile uyumlu olacak.

VPN çocukluğuna 1995 yılında, kar amacı gütmeyen bir dernek olan AIAG (Otomotiv Endüstrisi Eylem Grubu) ile başlamıştır.

Kuzey Amerika araç üreticileri ve tedarikçileri ile ANX (Otomotiv Ağı)

eXchange) projesi. Proje, alım satımdan oluşan bir TCP / IP ağına duyulan ihtiyacı karşılamak için üretildi.

ortaklar, sertifikalı servis sağlayıcılar ve şebeke değişim noktaları. Gereksinim verimli ve

Güvenli olmayan kanallar üzerinden yalnızca tek bir bağlantıyla aboneler arasında elektronik iletişimin güvenliğini sağlamak.

Bu teknoloji büyüdükçe, güvenli sağlamak isteyen herhangi bir kuruluş için bir çözüm olarak kabul edildi.

ortaklar, müşteriler veya herhangi bir uzak ağla iletişim kurmak. Ancak, büyüme ve kabul

Standartlar ve ürün destek konularının bulunmamasına engel oldu.

**1.2 Standardın Yapı Taşları**

IPSec standardı, IP katmanında gizlilik ve kimlik doğrulama hizmetleri sağlamak için kullanılır. Birkaç RFC

Bu protokol paketini tanımlamak için kullanılır. Belgelerin karşılıklı ilişkisi ve organizasyonu önemlidir

Genel standardın geliştirme sürecinin farkında olmak.

Sergi 32.1'in gösterdiği gibi, ayrı yönlerin birleştirilmesine izin veren yedi belge grubu vardır

İşleyen bir ilişki elde edilirken IPSec protokol paketinin bağımsız olarak geliştirilmesi

yönetilen.

Mimari, genel teknoloji kavramlarını ve güvenliğini kapsayan ana açıklama belgesidir. hususlar. IPSec protokol paketinin ilk anlaşılması için erişim noktası sağlar. ESP (Kapsüllenen Güvenlik Yükü) protokolü (RFC 2406) ve AH (Kimlik Doğrulama Başlığı) protokolü (RFC 2402) belge grupları, paket biçimlerini ve paket yapısı için varsayılan standartları uygulama algoritmaları içerir. Şifreleme Algoritması belgeleri, çeşitli şifreleme kullanımını ayrıntılandıran bir dizi belgedir. ESP için kullanılan teknikler. Belge örnekleri arasında DES (Veri Şifreleme Standardı RFC 1829) bulunmaktadır. ve Triple DES (taslak-simpson-desx-02) algoritmaları ve verilerin şifrelemesindeki uygulamaları.

Kimlik Doğrulama Algoritmaları, kullanılan süreç ve teknolojileri tanımlayan bir grup belgedir. AH ve ESP protokolleri için bir kimlik doğrulama mekanizması sağlar. Örnekler HMAC-MD5 (RFC) olacaktır. 2403) ve HMAC-SHA-1 (RFC 2404). Bu belgelerin tümü DOI'ye uyumluluk için birleştirilmesi ve tanımlanması gereken değerleri belirtir, veya Yorumun Yapıldığı Alan (RFC 2407). DOI belgesi IANA tarafından atanan numaralar mekanizmasının bir parçasıdır ve birçok standart için sabittir. Diğer belgelerin değerleri için merkezi depo sağlar. birbirleriyle ilgilidir. DOI, protokolün diğer bölümleri için gereken parametreleri içerir. tanımların tutarlı olduğundan emin olun.

**1.3 Fonksiyonun tanıtımı**

AH bütünlük, kimlik doğrulama, dizi bütünlüğü (tekrarlama direnci) ve reddetme için tasarlanmıştır

- ancak ESP'nin tasarlandığı gizlilik için değil. Kullanımın çeşitli uygulamalar vardır

sadece bir AH gereklidir veya şart koşar. Gizliliğin gerekli olmadığı veya onaylanmadığı uygulamalarda

devletin şifreleme kısıtlamaları ile, kendi içinde olabilen bir bütünlük sağlamak için bir AH kullanılabilir.

Potansiyel saldırganlara karşı güçlü bir düşman. Bu tür bir uygulama bilgileri

yayma ancak bilgilerin bütünlüğünün doğrulanmasına ve

yaratıcısı.

IP başlığının geri kalanı AH güvenlik protokolü ile doğrulamada kullanılmaz. ESP kimlik doğrulaması bundan önce gelen hiçbir IP başlığını kapsamaz. ESP protokolü, AH’nin bazı servislerinin yanı sıra şifreleme de sağlar. Bu iki protokol yapabilir Belirli bir uygulama veya çevresel yapı için gereken servis seviyesini elde etmek için ayrı olarak kullanılabilir veya kombine edilebilir. ESP kimlik doğrulama özellikleri, dahil edilmemesi nedeniyle AH ile karşılaştırıldığında sınırlıdır. kimlik doğrulama işleminde IP başlık bilgisinin. Bununla birlikte, ESP, yalnızca üst katman protokollerinin kimliğinin doğrulanması gerekiyor. Kimlik doğrulama için sadece ESP'nin uygulanması, bütünlük ve üst katmanlara gizlilik, ESP’nin AH. Kimlik doğrulama ve gizlilik her ikisi de isteğe bağlı işlem olsa da, güvenlik protokollerinden biri uygulanmalı. Sadece kimlik doğrulama ile ve şifreleme veya boş şifreleme olmadan iletişim kurmak mümkündür (RFC 2410). ESP'nin ek bir özelliği de büyüklüğü gizleyen yük dolgusu iletilen paketin ve ayrıca iletişimin özelliklerini korur. Bu protokollerin onaylanması süreci, bir güvenlik derneği (SA) oluşturmak için gereklidir. bir IPSec VPN Bir SA, AH veya ESP protokolü tarafından sağlanan kimlik doğrulamasından oluşturulur ve SA'nın sistemler arasında kurulması ve sürdürülmesi için anahtar yönetiminin temel işlevi. SA bir kez Elde edilen verilerin taşınması başlayabilir.

**1.4 Vakfı Anlamak**

Güvenlik birlikleri IPSec'in altyapısıdır. IPSec protokol paketinin tüm bölümleri arasında SA satıcı entegrasyonu ve heterojen sanal özel ağların gerçekleştirilmesi için odak noktası. SA Tüm IPSec uygulamaları arasında ortaktır ve IPSec uyumlu olması için desteklenmesi gerekir. Bir SA neredeyse VPN ile eşanlamlı ancak “VPN” terimi çok daha gevşek bir şekilde kullanılıyor. SA'lar başka güvenliklerde de var protokolleri. Daha sonra açıklandığı gibi, IPSec VPN'lerde kullanılan anahtar yönetimin çoğu, Anahtar yönetiminin diğer formları desteklemesine izin veren, temel güvenlik protokolünü tanımlayan özellikler SA kullanan VPN teknolojisi.

Bir SPI, aynı hedefe son veren farklı SA'lar arasında ayrım yapmak için kullanılan 32-bit bir değerdir ve aynı IPSec protokolünü kullanarak. Bu veri SA'ların tek bir ağ geçidine çoklanmasına izin verir. İlginçtir, hedef IP adresi tek noktaya yayın, çok noktaya yayın veya yayın olabilir; ancak, SA'ların yönetimi için standart şu anda tek noktaya yayın uygulamaları veya noktadan noktaya SA'lar için geçerlidir. Pek çok satıcı, başarılı olmak için birkaç SA kullanacak noktadan çok noktaya bir ortam. Son kimlik - güvenlik protokolü tanımlayıcısı - bunun için kullanılan güvenlik protokolüdür SA. Tek bir SA tarafından sağlanan iletişim için yalnızca bir güvenlik protokolünün kullanılabileceğini unutmayın. Etkinlikte AH ve ESP güvenliğinin her ikisini de kullanarak iletişimin kimlik doğrulama ve gizlilik gerektirdiğini protokoller, iki veya daha fazla SA'nın oluşturulması ve trafik akışına eklenmesi gerekir.

**1.5 İletişim Modları**

IPSec bağlantısı için işlem türü, sistemin VPN'de oynadığı rolle doğrudan ilgilidir veya SA durumu. IPSec VPN'ler için Ek 32.2'de gösterildiği gibi iki çalışma modu vardır: Aktarım modu ve tünel modu.

Aktarım modu, üst katman protokollerini korumak için kullanılır ve yalnızca IP paketindeki verileri etkiler. Daha fazla

dramatik yöntem, tünel modu, güvenli bir iletişim kurmak için tüm IP paketini içine alır

iletişim.

Aktarım modu, uç nokta bir ana bilgisayar olduğunda veya iletişim

bitiş noktaları. Ağ geçidi-ana bilgisayar iletişimindeki ağ geçidi taşıma modunu kullanıyorsa,

bu ağ geçidine doğrudan protokoller için kabul edilebilir olan konak sistemi. Aksi takdirde, tünel modu gereklidir

Ağ geçidi servislerinin dahili sistemlere erişim sağlaması için.

**1.5.1 Taşıma modu**

Aktarım modunda IP paketi, orijinal IP'den sonra bulunan güvenlik protokolünü (AH veya ESP) içerir. başlık ve seçenekler ve pakette bulunan TCP ve UDP gibi herhangi bir üst katman protokolünden önce. Ne zaman ESP güvenlik protokolü için kullanılır, koruma veya karma yalnızca üst katman protokollerine uygulanır. paketin içinde bulunur. IP başlık bilgisi ve seçenekleri, kimlik doğrulama işleminde kullanılmaz. Bu nedenle, kaynak IP adresi verilere karşı bütünlük açısından doğrulanamaz. AH kullanımı ile güvenlik protokolü, koruma, bütünün bütünlüğünü sağlamak için IP başlığına ilerletilir. karma işleminde orijinal IP başlığının kısımlarını kullanarak paketleyin.

**1.5.2 Tünel Modu**

Tünel modu ağ geçidi servisleri için kuruludur ve temelde kimlik doğrulaması olan bir IP tüneli ve şifreleme. Bu en yaygın çalışma şeklidir. Ağ geçidinden ağ geçidine tünel modu gereklidir ve host-to-gateway iletişimi. Tünel modu iletişiminde iki grup IP başlığı bulunur - içeride ve dışarıda.

IP üstbilgisinin TTL’si (Canlı Kullanım Süresi), kapsülleme sistemi tarafından bir Ağ geçidinden geçerken sekme sayımı. Ancak, ağ geçidi kapsülleme sistemi ise, NAT olduğu gibi iç ana bilgisayarlar için uygulanır, iç IP başlığı değiştirilmez. TTL'nin değiştirilmesi durumunda, sağlama toplamı IPSec tarafından yeniden yaratılmalı ve değişikliği yansıtacak şekilde IP'yi koruyarak orijinalin yerine kullanılmalıdır paket bütünlüğü. Dış IP başlığının oluşturulması sırasında, iç başlığın girişlerinin ve seçeneklerinin çoğu eşleştirilir dışarıya. Bunlardan biri şu anda IPv4'te bulunan ToS (Hizmet Türü).

**1.6 Verileri Koruma ve Doğrulama**

AH ve ESP protokolleri veriler için kimlik doğrulama veya bütünlük sağlayabilir ve ESP sağlayabilir

veri için şifreleme desteği. Güvenlik protokolünün başlığı, cihazınız için gerekli bilgileri içerir.

beraberindeki paket. Sergi 32.3, her başlığın biçimini gösterir.

**1.7 Bağlantıları Yönetme**

Daha önce de belirtildiği gibi, SA'lar IPSec protokol paketinin temel amacını ve ağ geçitleri ve ana bilgisayarlar. Birkaç uygulama ve standart katmanı kontrol etmek, yönetmek, ve SA'ların izlenmesi. Çeşitli uygulamalar, servislerin birleştirilmesini gerektirebilir; gerekli taşıma. Örnek olarak, kimlik doğrulama ve gizlilik gerektiren bir uygulama olabilir. AH ve ESP'yi kullanmak ve daha fazla SA grubunun hiyerarşik iletişim sağlamasını gerektirir. Bu süreç iletişimin katmanlı bir etkisini sağlayabilen bir SA Paketi olarak adlandırılır. SA paketlerinden yararlanılabilir iki formatta uygulamalar: ince tanecik ve kaba tanecik. İnce ayrıntı düzeyi, her iletişim süreci için SA'ların atanmasıdır. Tek bir üzerinden iletilen veriler SA tek bir güvenlik protokolü ile korunmaktadır. Veriler, bir AH veya ESP tarafından korunur, ancak her ikisi de SA'lar nedeniyle korunmaz sadece bir güvenlik protokolüne sahip olabilir.

**1.8 Çok Katmanlı Güvenlik Akışı Sağlama**

Ayrıcalık sağlamak için çok katmanlı güvenlik (MLS) veya veri etiketlemesi yapan birçok sistem vardır. ağ üzerinde iken verebileceği sistem ve verilere dayalı güvenlik. Bu operasyon modeli Zorunlu Erişim Kontrolü (MAC) olarak adlandırılabilir. Bu güvenlik modelinin bir örneği Bell-LaPadula'dır. Hassas bilgilerin izinsiz iletilmesine karşı koruma sağlamak için tasarlanmış bir modeldir. Çünkü veri Transit olarak incelenmek üzere kendisi etiketlendi, çeşitli güvenlik katmanları uygulanabilir. Diğer güvenlik biçimleri erişim denetim listelerini veya filtreleri kullanabilecek İsteğe Bağlı Erişim Kontrolü (DAC) gibi modeller çok katmanlı güvenliği desteklemek için yeterli. AH ve ESP gerekli güvenliği sağlamak için birleştirilebilir MAC ortamında çalışan MLS sistemleri için gerekli olabilecek politika.

Bu, güvenliği bağlamak için AH güvenlik protokolünün kimliği doğrulayan özellikleri kullanılarak gerçekleştirilir Orijinal IP başlığındaki yüklerin yük ile eşleştirilmesi. AH’nin bu şekilde kullanılması, Başlığa karşı veri. Şu anda, IPv4 yükü başlık ile doğrulamıyor. Duyarlılığı veri sadece başlığın varsayılanı olarak kabul edilir. Bu işlemi gerçekleştirmek için, her SA veya SA Paketi, diğer güvenlik seviyelerinden ayırt edilebilir olmalıdır. bilgi iletiliyor. Örnek: “SENSITIVE” etiketli veriler SA veya SA ile eşlenecek Paket, “SINIFLANDIRILMIŞ” etiketli veriler başkalarına eşlenecek. SAD ve SPD bir parametre içerir Verilerin elde edilmesini sağlamak için çeşitli uygulamalar tarafından erişilebilen Hassasiyet Bilgisi olarak adlandırılır. Aktarılan uygun şifreleme seviyesi ve ilgili SA'lara iletilir.

**Denial-of-Service Attack**

**1.1 Gözyaşı Saldırısı Nedir?**

Denial of Service (DoS saldırısı) olarak da bilinir. İnternete bağlı bir hostun hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır.

DoS genellikle hedef makine veya kaynağın, gereksiz talepler ile aşırı yüklenmesi ve bazı ya da bütün meşru taleplere doluluktan kaynaklı engel olunması şeklinde gerçekleştirilir. DoS saldırısını; bir grup insanın, bir dükkân veya işyerindeki kapıları tıkayıp, meşru tarafların mağazaya veya işletmeye girmesine izin vermeyerek normal işlemleri aksatması şeklinde örnekleyebiliriz.

**1.2 Gelişmiş Kalıcı DoS**

Gelişmiş Kalıcı DoS(APDoS), gelişmiş bir kalıcı tehdit(APT) tarafından işgal edilme olasılığı yüksektir. Gelişmiş kalıcı tehdit iyi kaynaklara sahip, son derece yetenekli ve önemli derecede ticari nitelikli bilgisayar kaynakları ve kapasitesine erişen aktörlerdir. APDoS saldırıları özel izleme ve olay tepki hizmetlerine ve özel DDoS azaltma servis sağlayıcılarının savunma yeteneklerine ihtiyaç duyan açık ve yeni bir tehdit oluşturur.

Bu saldırı türü uygulama katmanı(HTTP) floodlarına kadar geniş ağ katmanlı DDoS saldırılını ve (değişken aralıklarla) SQL'i ve XSS saldırılarını içerir. Suçlular genellikle saniyede on milyondan fazla talep içeren 2 den 5'e kadar saldırı vektörünü eş zamanlı kullanabilirler.Bu saldırıların çoğu kurbana saldırmakla kalmaz, aynı zamanda herhangi bir DDoS azaltma yönetimi sağlayan herhangi bir servis sağlayıcıya SYN flood'ları eşlik eder. Bu saldırılar birkaç hafta devam edebilir. Şu ana kadarki en uzun süre 38 gün sürmüştür. Bu APDoS saldırıları yaklaşık 50+ petabits (50,000+ terabits) zararlı trafik içeriyordu.

Saldırganlar bu senaryoda(çoğu kez) taktiksel olarak birçok hedef arasında geçiş yapar.Bunu DDoS defanslarından kurtulmak için oluşturmuştur. Ancak tüm bunlar sonunda saldırının ana gücünü tek bir kurban üzerinde yoğunlaştırdı.

**1.3 Servis Olarak DoS**

Bazı satıcılar basit web tabanlı ön uçlara sahip olan ve web üzerinden ödeme kabul eden "booter" veya "stresser" hizmetleri sunar. Stres test araçları olarak satılır ve geliştirilirler. Yetkisiz DoS saldırıları yapılmasına ve teknik olarak ileri düzeyde bilgisi olmayan saldırganların, gelişmiş saldırı araçlarına saldırganın kullanımını anlamasına gerek kalmadan erişmesine olanak sağlar.

**1.4 Korunma Yolları**

DoS saldırılarına karşı savunmalar, genellikle, saldırı tespiti, trafik sınıflandırması ve yanıt araçları kombinasyonunun kullanılmasını içerir. Bunlar, meşru olduklarını belirledikleri trafik akışına izin vermeyi ve diğer trafikleri engellemeyi  amaçlar.

**1.4.1 Uygulama Ön Uç Donanımı**

Uygulama ön uç donanımı, trafik sunucularına ulaşmadan önce ağa yerleştirilen akıllı bir donanımdır. Anahtarlar ve yönlendiriciler ile birlikte ağlarda kullanılabilir. Uygulama ön uç donanımı sisteme girerken veri paketlerini analiz eder ve sonra bunları öncelikli, normal veya tehlikeli olarak tanımlar. 25'den fazla bant genişliği yönetimi sağlayıcısı bulunmaktadır.

**1.4.2 Kara Delik ve Sinkholing**

Kara Delik yönlendirmesiyle, saldırıya uğramış DNS veya Ip adresine bir "kara delik"'e(boş arayüz veya mevcut olmayan bir sunucuya) tüm trafik yollanır.Daha verimli olmak ve ağ bağlantısını etkilemekten kaçınmak için, ISS tarafından yönetilebilir.

Bir DNS sinkhole trafiği analiz eden ve hatalı paketleri reddeden geçerli bir IP adresine yönlendirilir.Sinkholing, en güçlü saldırılar için etkili değildir.

**1.4.3 IPS Tabanlı Savunma**

Saldırı önleme sistemleri (IPS), saldırıların kendileri ile ilişkili imzaları olması durumunda etkilidir. Fakat, saldırılar arasındaki eğilim meşru içeriğe sahip olmakla birlikte kötü niyetlidir. İçerik tanıma üzerinde çalışılan saldırı önleme sistemleri davranış temelli DoS saldırılarını engelleyemez.

**1.4.4 Güvenlik Duvarları**

Basit bir saldırı durumunda, güvenlik duvarları saldırganlardan gelen tüm trafiği, protokollere, portlara veya kaynak IP adreslerine dayanarak reddetmek için basit bir kurala sahip olabilir.

Ancak basit kurallarla daha karmaşık saldırıların engellenmesi zor olacaktır. Örneğin, 80. portta(web hizmeti) devam eden bir saldırı varsa, bu porta gelen bütün trafiği engellemek mümkün değildir, çünkü meşru trafikleri de engellemiş oluruz.[[44]](https://tr.wikipedia.org/wiki/Denial-of-service_attack) Ayrıca, ağ hiyerarşisinde güvenlik duvarları çok derinde olabilir, bu yüzden trafik güvenlik duvarına gelmeden önce yönlendiriciler olumsuz etkilenmiş olabilir.

**1.4.5 Yönlendiriciler**

Yönlendiriciler de , anahtarlar gibi bazı hız sınırlayıcı ve ACL özelliklerine sahiptir.Yönlendiriciler de el ile ayarlanır. Çoğu yönlendirici , bir hizmet reddi saldırısı altında kolayca ezilebilir. Cisco IOS , isteğe bağlı olarak floodların etkisini azaltabilen özelliklere sahiptir.

**REFERANSLAR**

İnternet Mühendisliği Görev Gücü (IETF) Yorum İsteği (RFC) belgeleri: İnternet Mühendisliği Görev Gücü (IETF) Yorum İsteği (RFC) belgeleri:

RFC-1089 SNMP over Ethernet

RFC-1157 SNMP over Ethernet

RFC-1187 Bulk Table Retrieval with the SNMP

RFC-1215 Convention for Deﬁning Traps for Use with the SNMP RFC-1227 SNMP MUX Protocol and MIB

RFC-1228 SNMP-DPI: Simple Network Management Protocol Distributed Program

RFC-1270 SNMP Communications Services

RFC-1303 A Convention for Describing SNMP-Based Agents

RFC-1351 SNMP Administrative Model

RFC-1352 SNMP Security Protocols

RFC-1353 Deﬁnitions of Managed Objects for Administration of SNMP

RFC-1381 SNMP MIB Extension for X.25 LAPB

RFC-1382 SNMP MIB Extension for the X.25 Packet Layer

RFC-1418 SNMP over OSI

RFC-1419 SNMP over AppleTalk

RFC-1420 SNMP over IPX

RFC-1461 SNMP MIB Extension for Multiprotocol Interconnect over X.25

RFC-1503 Algorithms for Automating Administration in SNMPv2 Managers

RFC-1901 Introduction to Community-Based SNMPv2

RFC-1909 An Administrative Infrastructure for SNMPv2

RFC-1910 User-Based Security Model for SNMPv2

RFC-2011 SNMPv2 Management Information Base for the Internet Protocol

RFC-2012 SNMPv2 Management Information Base for the Transmission Control Protocol

RFC-2013 SNMPv2 Management Information Base for the User Datagram Protocol

RFC-2089 V2ToV1 Mapping SNMPv2 onto SNMPv1 within a Bi-Lingual SNMP Agent

RFC-2273 SNMPv3 Applications

RFC-2571 An Architecture for Describing SNMP Management Frameworks

RFC-2573 SNMP Applications

RFC-2742 Deﬁnitions of Managed Objects for Extensible SNMP Agents

RFC-2962 An SNMP Application-Level Gateway for Payload Address

CERT Advisory CA-2002–03