

Denial of Service saldırılarının önlenmesi

İnternet artık her zamankinden daha tehlikeli hale gelmiş durumda. Dis tehlikeler çalışan servisleriniz veya işletim sisteminizdeki açıkları kullanarak “uzaktan super kullanıcı” olarak bağlanma sorunları yanında artık önemli sunucularınızın servisi vermeyi durdurması gibi büyük sorunlar yaratabiliyorlar.İste bu yazıda böyle bir saldırının önlenmesi için neler yapabileceğimizi ve eğer böyle bir saldırı ile karşı karşıya kaldıysanız neler yapabileceğinizi tartışacağız.

Bu teknikler hem FreeBSD 4.x hem de 5.x versiyonları için kullanılabilirlerdir.

Saldırı Cesitleri

Denial of Service (DoS) saldırıları karşı sistemde çalışan servisin durdurulmasını amaç edinir.Web sunucuları artık http servisi veremez, e-posta unucuları artık posta gönderip alamaz hale gelir.

Bu saldırılar iki şekilde servisi durdurmaya çalışırlar:

- İşlemci, hafıza, bant genişliği gibi metaları sonuna kadar tüketerek
- Serviste bulunan bir zayıflığı kullanarak bu servisi durdurmak.

Gectigimiz yıllarda saldirganlar saldiri yontemlerini aciga vurduklari icin artik yazilimcilar daha guvenli ve DoS`a dayanikli yazilimler cikarmaya basladilar.Simdi isterseniz ilk saldiri cesidini inceleyerek baslayalim:

Servislerin en iyi sekilde calistirilmesi

Bu tur saldirilardan korunmanin genel yontemi bir sekilde tum DoS saldirisi yapilabilecek olan metalarinizi son kapasite calisabilecek sekilde ayarlamak gibidir.Ne kadar fazla yuk kaldirabiliyorsaniz o kadar dayanikli olursunuz.

Ornegin web sayfaniz buyuk dosyalari transfer etmek icin ayarlanmis ise ve saldirgan bircok ufak ve az zamanli baglanti kuran dosya gondermeye calisir ise bant genisliginizin ne kadar cabuk doldugunu gorebilirsiniz.Bunun icin inceleyebileceginiz en iyi iki kaynak [tuning FreeBSD for different applications](#) ve [tuning\(7\)](#) man sayfasidir.

Denial of Service saldırılarının analiz ve engellenmesi

Sisteminizi korumanın ilk adımı değişik saldırıları anlamaktan geçmektedir.Daha önce söylediğimiz gibi bu tür saldırılar bitebilen bir kaynağın sonuna kadar tüketilmesi sonucunda ortaya çıkmaktadır. En popüler hedefler ağ bant genişliği, sistem hafızası, ağ stack hafızası, disk I/O, açık olan dosya sayısı limiti gibi işletim sistemi limitleri ve işlemcidir.

Bant genisligi saldirilari

Bant genisliginize yapilan saldirilar savunulmasi gereken en zor yerlerden biridir.Bunlara karsi nasil onlemler alacaginiz tamamen ag yapiniza ve ISP`nizin ne kadar yardimci olmasiyla ilgilidir.Su sorulari sorarak baslayabilirsiniz:

- Saldiri tek bir sisteme mi yoka birden cok sisteme mi yapiliyor?
- Saldirgan sadece belli potlara mi saldiri yapiyor yoksa saldiri hedefi gelisi guzel portlar mi?
- Saldiri saldiri yapilan sunucularda kullanilmayan protokolleri iceriyor mu?

Gunumuzde saldirilarin cogunun basit olmasi islerimizi daha kolaylastirmakta.Saldirganlar birkac Ip adresine bir veya iki saldiri cesidi ile saldirmakta.Bant genisligi saldirilarinda saldirganin bat genisligimizi tuketmesi bizim onu bizim korumamiz kadar zor olmakta.Bunu onlemenin en iyi yolu ag gecidiniz uzerinde daha saldirgan iceriye paket yollayamadan bunu kesmektir.

Sunucularda tcpdump gibi bir yazilim kurulup ayni tur paketlerin, TCP SYN, UDP, veya ICMP, arka arkaya geldigi siralari takip etmek yerinde bir karar olacaktir.Ayni port`a gelen paketlerin tumunu incelemek size bu port`a paketleri gonderen Ip adreslerini gosterecek ve eger bu ip adresleri cok fazla degil ise bunlari bloklamak sorunu ortadan kaldiracaktır..

Tabiki eger Ip adresleri cok fazla olmasi durumunda, ki bu ip adreslerinin saldirgan tarafından spoofing veya forging yontemi ile kullanildiginiz gosterir, oaketlerde diger benzerlikleri aramamiz gerekecektir. Bu paket header`i, pencere buyuklugu, fragmantasyon vs. olabilir. Eger bu tur paketleri bu tur parametrelere gore bloklayamiyorsaniz burada daha fazla arastirma yapmaniz gerekecektir.

Kendinizin olusturacagi bir system yaninda ISP`nizin yardimi da cok ise yarayacaktır. Saldiriye analiz ettikten sonra ISP`nizi arayip iki tur filtreleme isteyebilirsiniz. Bunlardan birincisi saldiri yapilan sunuculara gelen tum paketlerin kapatilmasi veya saldirganlarin filtrelenmesi olabilir.

Eger internet ag gecidinizde Border Gateway Protocol (BGP) ip`nizi internet ortamina duyurursa ucuncu bir seceneginiz ortaya cikacaktır.Bu yontemde bircok ISP kullanicilarin /32 bitlik bir route`i belli bir public string ile alip kendi border router`larinin bu route`a gelen tum paketleri dusurmelerini salgayabilmelerine olanak vermekteler.Tabiki bu tabiki eger saldirilan sistemler sayici az is eve ISP`niz bu tur bir uygulamaya izin veriyorsa saglanmaktadır.

Genel olarak aginiz uzerinde sadece cok gerekli olan servisleri acik tutmak en genel guvenlik onlemidir.Http sunuculariniza guncellemeleri yapmak ve sistemlerini uzerinde calismalari icin ssh ile ancak belli ip adreslerinin baglanabileceklerinden emin olmak alacaginiz onlemler arasinda olacaktir.

Sistem ve servis saldırıları

Bu tür saldırılar tüm ağdan çok tek veya birkaç sisteme yönelik olarak gerçekleştirilmektedir. Saldırı çeşitleri ise şöyledir:

- Ağ alt sistem sınırlamaları (saniye bazında çok yüksek paket sayısı)
- İşletim sistemi veya hafıza sınırlamaları (Hafıza yeneği)
- Dis veya işlemci sınırlamaları (Yüksek sayıda geçerli istek)

Sistemleri hedef alan saldırılar gerçekten savunulması zor saldırılar arasında sayılsa bile FreeBSD bunun için önlemini almış olarak gelmektedir.

Standart olarak ağ kartınızın paket aldığı her seferde IRQ'su üzerinde işlemcinize bir interrupt (istek) yaratır. İşlemci bunu yakalar ve belli bir süreyle bu paketi ağ kartından almak için zaman ayırır. Normal zamanlarda birkaç bin defa gerçekleşen bu işlem eski işlemcilerin bile kapasitesini aşmamaktadır. Eski modem işlemciler ancak 25.000 – 50.000 arasında performans sorunu yaratmaya başlayabilir. Paket büyüklüklerinin 1,500 byte'tan olduğunu düşünürsek bu 40Mbytes/sn'den 75Mbytes/sn'ye kadar değişen bir büyüklüğe erişir ki bu çoğu eski işlemcinin kapasitesini zorlar. Çoğunlukla bu sınır noktası 1Ghz işlemciler için 75.000 paket'tir. Problemi kötülestiren iki faktör şunlardır:

- TCP SYN paketleri, sistem kaynak adresine SYN ACK paketlerini cevap olarak göndermeden önce tam işlem gerektirir. Kapalı port'lara gelen TCP ve UDP paketleri ve ayrıca ICMP paketleri de, SYN kadar olmasa da zaman ve işlemci gücü yemektir.
- Ayrıca paket büyüklüğü de büyük bir rol oynamaktadır. Bant genişliğine büyük paketlerden daha çok ufak paketleri sigdirabilirsiniz. Bu yüzden daha fazla paket alınması daha fazla işlemci gücü olacağından paket büyüklüğünün büyük olması pek bir şey degistirmeyecektir.

Daha önce tartıştiğimiz gibi her interrupt (istek) belli bir işlemci zamanını doldurmaktadır. Yeteri kadar IRQ üretildiği takdirde CPU'nun başka hiçbir işlem yapmaya zamanı kalmayacak ve sadece bu isteklere cevap verecektir. İc paketler beklemeye alınıp, sistem üzerinde kullanılan yazılımlar için gerekli hiç işlemci gücü kalmayacaktır. Paketler ağ üzerinden gelmeyi kestiginde işlemci arka planda biriktirdiği tüm paketleri işleyecek ve bunun ile dakikalar hatta saatler harcayacaktır.

Yeni donanım harcamaları yapmadan yüksek paket geliş oranını sınırlayabileceğiniz bazı yöntemler bulunmaktadır. Bunları hemen hepsi `sysctl(8)` komutunu kullanarak sisteminizde yapılandırılabilir. Şimdi ise hangi parametreleri `/etc/sysctl.conf` dosyasına ekleyeceğimize bakalım:

- `net.inet.tcp.msl=7500`

`net.inet.tcp.msl` Maximum Segment Life (En yüksek segment hayat süresi). Bu süre SYN-ACK veya FIN-ACK paketine verilecek ACK paketini bekleme

surecini milisaniye cinsinden belirler. Eger system ACK`yi bu zaman icinde almaz ise segment`i kaybolmus olarak Kabul ederek ag genisligini acar.

Burada dikkat edilmesi gereken iki nokta bulunmakta. Bir baglantiyi kapatmaya calistiginizda eger son ACK kaybolmus veya gec kalmis ise socket daha cabuk kapanacaktır. Bunun yaninda eger istemci size bir baglanti yaratmak istiyor ise eve istemcinin ACK`si 7,500 ms`den daha uzun suruyorsa baglanti kurulmayacaktır. RFC 753 bu sureyi 120 saniye (120,000) olarak belirlemis olsa bile yazildigi yilin 1979 oldugunu goz alarak artik bu surenin cok daha kisaldigini soyleyebilirsiniz. Gunumuzde FreeBSD`nin standard`i 30,000 ms`dir. Cogu DoS saldirisini onlemek icin yeterli olan bu rakami eger isterseniz 7,500 ms`ye indirip daha guclu bir DoS guvenligi saglayabilirsiniz.

- `net.inet.tcp.blackhole=2`

`net.inet.tcp.blackhole` sistemin kapali bir port`a TCP paketi almasi sonucunde ne yapacagini ayarlamak icjn kullanilir. `_1` olarak ayarlandiginda kapali port`a gelen SYN paketi RST gonderilmeden dusurulecek, `2` olarak ayarlandiginda ise yine tum TCP paketleri RST gonderilmeden dusurulecektir. Bu paketlerin geri gonderilmesini engelledigi icin islemci zamani kazandiracaktır.

- `net.inet.udp.blackhole=1`

`net.inet.udp.blackhole` `net.inet.tcp.blackhole` parametresini animsattmaktadır. Bu parametre `1` olarak ayarlandiginda TCP yerine UDP paketlerini tamamen dusurecektir.

- `net.inet.icmp.icmplim=50`

`net.inet.icmp.icmplim` her saniye geri gonderilen TCP RST paket sayisini ve gonderilebilecek maximum ICMP "Ulasilamaz" mesajlarini saniye bazinda kontrol eder. Sisteminizin cok fazla cevap yaratmaya calisip tikanmasi olasiligini ortadan kaldirir.

- `kern.ipc.somaxconn=32768`

`kern.ipc.somaxconn` maksimum acik socket sayisini belirlemektedir. Buradaki standart 128 olarak belirtilmistir. Eger saldirgan kisa zamanda yeteri kadar SYN paketini size yollayabilir ise tum ag baglantilarinizi kullanip diger kullanicilarin size baglanmasini engelleyebilir. Dolayisiyla sisteminiz disariya hicbir hizmet veremez hale gelebilir.

Bu degerleri isteginiz ve ag yapinizi goze alarak degistirebilirsiniz.

Son olarak eger asagidaki ag kartlarindan birisine sahipseniz kernel`inizda `DEVICE_POLLING` parametresini aktif hale getirebilirsiniz:

- dc
- em
- fxp
- nge
- rl
- sis

`DEVICE_POLLING` parametresi ile kernel interrupt (istek) servis verilme seklini degistirmekte. Bazi zamanlarda islemci ag kartini cagirip islem icin bekleyen paketleri alacak ve isleyecektir. Bu ic agdaki trafik icin kullanılan islemci zamanini buyuk bir seviyede indirecektir. Yalnız bu parametre ancak yukarıdaki kartlardan biri ve `DEVICE_POLLING` secenegini destekleyen suruculeri ile calisabilmektedir.

FXP kartlari genel olarak bu ozellik ile performansli sekilde calisabilmektedir. Donanim dizayn ve kalitesi daha dusuk olan RL kartlari 1Ghz`den dusuk islemcilerde tam 100MB/s performansini malesef yakalayamamaktadirlar. Eger yeni bi rag karti alacaksaniz bu noktaya dikkat etmelisiniz.

`DEVICE_POLLING` hakkında daha fazla bilgiye [DEVICE_POLLING](#) sayfasından bulabilirsiniz.

Saldiri kaynaginın tespiti

Saldirilar bildiginiz gibi hem ic hem de disaridan gelebilmektedir. Saldirinin kaynaginın tespiti tcpdump, ngrep, ve ethereal gibi paket sniffing (koklama) yazilimlari hakkında biraz bilgi sahip olmanizi gerektirmekte. Eger sisteminizi birkac ay boyunca inceleyerek ve hangi tur paketlerin normal hangilerinin anormal oldugunu gormediyseniz denial of service saldirilarini yakalama sansiniz cok dusuk olacaktır. Denial of Service saldirilarinin isaretcileri “Internet yavas” veya “E postalarimi alamiyorum” olarak alinabilmekte. Iki gercegi anlamaniz gerekmektedir:

- Saldirilar hem iceriden hem disaridan gercekleliyor olabilir
- Ne tum servis hedefli saldirilar DoS saldirisina yol acar ne de tum DoS saldirilari servisin durmasına yol acar.

Peki bun e demek? Eger aginizdaki kisiler e –posta alamiyor veya internetin yavasligından sikayet ediyorsa sorun sizing sisteminizdeki bir yanlis konfigrasyon veya bozuk bir sunucu olabilir.

Baslangic icin bakilacak en iyi nokta cikis noktanizdir (bottleneck). Bu HTTP Proxy`nizdeki veya ag gecidinizdeki islemci olabilir. Eger siteminiz proxy islemi

gerceklestiriyorsa gunlukleri inceleyin.Buyuk istekleri tek bir system mi yoksa birden cok system mi yapmakta?

Eger cikis noktaniz ag gecidiniz ise (FreeBSD oldugunu farzediyoruz) sisteminizden gecen ip paketlerini gormke icin asagidaki komutu calistirabilirsiniz:

```
router# tcpdump -n -i <interface> -c 100
```

Bu komut belirttiğiniz <arayuz> (-i <arayuz>)`den gecen ilk 100 paketin bir genellemesini ip adreslerini isimlere cevirmeden (-n), gosterecektir:

```
04:59:53.915324 192.168.0.3.2327 > 192.168.0.10.1214:  
S 3199611726:3199611726(0) win 16384 <mss 1460,nop,nop,sackOK>  
(DF)
```

Bazi noktalarına goz atalim. Bize yararli olabilir:

- 04:59:53.915324

Bu paketin islendigi zamani belirtmektedir

- 192.168.0.3.2327

Bu ise kaynak Ip adresini ve sondaki 2327 ise port numarasini bildirir.

- 192.168.0.10.1214

Burasi gonderilen Ip adresini ve son bolumdeki 1214 varis port`unu belirtir.

- S

Paket tipini belirtir.Su anda bir SYN paketini belirtmekte.Diger cesit paketler ve TCP paketlerinin olusumu hakkında bilgi icin [Daryl's TCP/IP Primer](#) sayfasina ulasabilirsiniz.

Bu yazida tartistigimiz DoS saldirilari her sekil ve buyuklukte olusabilmekte.Her sekilde DoS saldirisi olsun veya olmasin aginizi izlemek saldirilar yaninda olumus olan ve farkedemediniz veya olusacagina dair isaretler veren sorunlari da teshis edip buyumeden cozmenize yardimci olacaktır.

Ozgur Ozdemircili

ozgur@enderunix.org

<http://www.enderunix.org>

<http://www.enderunix.org/ozgur/blog>

KAYNAKLAR

Avleen Vig` in “Preventing Denial of Service Attacks” yazisindan derlenmistir.Orjinal metne http://www.onlamp.com/pub/a/bsd/2004/06/24/anti_dos.html adresinden ulasabilirsiniz.