Denial of Service saldirilarinin onlenmesi

Internet artik her zamankinden daha tehlikeli hale gelmis durumda. Dis tehlikeler calisan servisleriniz veya isletim sisteminizdeki aciklari kullanarak “uzaktan super kullanici” olarak baglanma sorunlari yaninda artik onemli sunucularinizin servis vermeyi durdurmasi gibi buyuk sorunlar yaratabiliyorlar.Iste bu yazida boyle bir saldirinin onlenmesi icin neler yapabilecegimizi ve eger boyle bir saldiri ile karsi karsiya kaldiysaniz neler yapabileceginizi tartisacagiz.

Bu teknikler hem FreeBSD 4.x hem de 5.x versiyonlari icin kullanilabilmektedir.

Saldiri Cesitleri

Denial of Service (DoS) saldirilari karsi sistemde calisan servisin durdurulmasini amac edinir.Web sunuculari artik http servisi veremez, e-posta unuculari artik posta gonderip alamaz hale gelir.

Bu saldirilar iki sekilde servisi durdurmaya calisirlar:

- Islemci, hafiza, bant genisligi gibi metalari sonuna kadar tuketerek
- Serviste bulunan bir zayifligi kullanarak bu servisi durdurmak.

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

Servislerin en iyi sekilde calistirilmasi

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 saldirilarinin analiz ve engellenmesi

Sisteminizi korumanin ilk adimi degisik saldirilari anlamaktan gecmektedir.Daha once soyledigimiz gibi bu tur saldirilar bitebilen bir kaynagin sonuna kadar tuketilmesi sonucunda ortaya cikmaktadir. En popular hedefler ag bant genisligi, system hafizasi, ag stack hafizasi, disk I/O, acik olan dosya sayisi limiti gibi isletim sistemi limitleri ve islemcidir.

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 kaldiracaktir..

Tabiki eger Ip adresleri cok fazla olmasi durumunda, ki bu ip adreslerinin saldirgan tarafindan 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 yarayacaktir. Saldiriyi 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 cikacaktir.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 saglanmaktadir.

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 saldirilari

Bu tur saldirilar tum ag dan cok tek veya birkac sisteme yonelik olarak gerceklestirilmektedir.Saldiri cesitleri ise soyledir:

- Ag alt sistem sinirlamalari (saniye bazinda cok yuksek paket sayisi)
- Isletim sistemi veya hafiza sinirlamalari (Hafiza yenmesi)
- Dis veya islemci sinirlamalari (Yuksek sayida gecerli istek)

Sistem`leri hedef alan saldirilar gercekten savunulmasi zor saldirilar arasinda sayilsa bile FreeBSD bunun icin onlemini almis olarak gelmektedir.

Standart olarak ag kartinizin paket aldigi her seferde IRQ`su uzerinde islemcinize bir interrupt(istek) yaratir.Islemci bunu yakalar ve belli bir sureyi bu paketi ag kartindan almak icin zaman ayirir.Normal zamanlarda birkac bin defa gerceklesen bu islem en eski islemcilerin bile kapasitesini asmamaktadir.Eski modem islemciler ancak 25.000 – 50.000 arasinda performans sorunu yaratmaya baslayabilir.Paket buyukluklerinin 1,500 byte`tan oldugunu dusunursek bu 40Mbytes/sn den 75Mbytes/sn`ye kadar degisen bir buyukluge erisir ki bu cogu eski islemcinin kapasitesini zorlar.Cogunlukla bu sinir noktasi 1Ghz islemciler icin 75.000 paket`tir.Problemi kotulestiren iki factor sunlardir:

- TCP SYN paketleri, system kaynak adresine SYN ACK paketlerini cevap olarak gondermeden once tam islem gerektirir.Kapali port`lara gelen TCP ve UDP paketleri ve ayrica ICMP paketleri de, SYN kadar olmasa da zaman ve islemci gucu yemektedir.
- Ayrica paket buyuklugu de buyuk bir rol oynamaktadir.Bant genisligine buyuk paketlerden daha cok ufak paketleri sigdirabilirsiniz. Bu yuzden daha fazla paket alinmasi daha fazla islemci gucu olacagindan paket buyuklugunun buyuk olmasi pek birsey degistirmeyecektir.

Daha once tartistigimiz gibi her interrupt (istek) belli bir islemci zamanini doldurmaktadir.Yeteri kadar IRQ uretildigi taktirde CPU`nun baska hicbir islem yapmaya zamani kalmayacak ve sadece bu isteklere cevap verecektir.Ic paketler beklemeye alinip, system uzerinde kullanilan yazlimlar icin gerekli hic islemci gucu kalmayacaktir.Paketler ag uzerinden gelmeyi kestiginde islemci arka planda biriktirdigi tum paketleri isleyecek ve bunun ile dakikalar hatta saatler harcayacaktir.

Yeni donanim harcamalari yapmadan yuksek paket gelis oranini sinirlayabileceginiz bazi yontemler bulunmakta. Bunlari hemen hepsi `sysctl(8)` komutunu kullanarak sisteminizde yapilandirilabilinmektedir.Simdi ise hangi parametreleri `/etc/sysctl.conf` dosyasina ekleyecegimize bakalim:

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

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

suresini 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 soket daha cabuk kapanacaktir.Bunun yaninda eger istemci size bir baglanti yaratmak istiyor is eve istemcinin ACK`si 7,500 ms`den daha uzun suruyorsa baglanti kurulmayacaktir.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 kazandiracaktir.

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

  `net.inet.udp.blackhole` `net.inet.tcp.blackhole` parametresini animsatmaktadir.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 soket 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 kullanilan islemci zamanini buyuk bir seviyede indirecektir.Yalniz bu parametre ancak yukaridaki kartlardan biri ve DEVICE_POLLING secenegini destekleyen suruculeri ile calisabilmektedir.

FXP kartlari genel olarak bu ozellik ile performansli sekilde calisabilemktedir.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 hakkinda daha fazla bilgiye DEVICE_POLLING sayfasindan bulabilirsiniz.

Saldiri kaynaginin tespiti

Saldirilar bildiginiz gibi hem ic hem de disaridan gelebilmektedir. Saldirinin kaynaginin tespiti tcpdump, ngrep, ve ethereal gibi paket sniffing (koklama) yazilimlari hakkinda 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 olacaktir.Denial of Service saldirilarinin isaretcileri “Internet yavas” veya “E postalarimi alamiyorum” olarak alinabilmekte. Iki gercegi anlamaniz gerekmekte:

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

Peki bun e demek? Eger aginizdaki kisiler e –posta alamiyor veya internetin yavasligindan 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 belirttiginiz <*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 noktalarina 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 hakkinda 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 olacaktir.

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.