Syn Flood DDoS Saldırıları

SYN

- TCP'e özel bir özelliktir
- TCP oturumlarını başlatmak için kullanılan TCP bayrağı
- Sadece oturumun başlangıç aşamasında görülür
- SYN paketleri veri taşıyamaz
  - İstisna durumlar anormallik olarak adlandırılır
  - Hping –p 8 0-S localhost –d 100 –E data ...

Syn Flood

- Internet dünyasında en sık gerçekleştirilen DDoS saldırı tipi
- Oldukça kolaydır
- Eğer gerekli önlemler alınmamışsa 2Mb hat ile 100Mb hatta sahip olan sistemler devre dışı bırakılabilir
- Saldırı yapması kadar korunması da kolaydır
- Genellikle sahte IP adresleri kullanılarak gerçekleştirilir

Neden Kaynaklanır?

- Temel problem
  - SYN paketini alan tarafta paketi gönderen onaylanmadan kaynak ayrılması
- Paketi gönderen IP adresinin gerçek olduğu belirlenmeden sistemden kaynak ayırılmamalı!

TCP SYN Paketi

Ortalama 60 byte

```
[root@mail ~]# hping -p 80 -S 99.99.99.1 -c 1
HPING 99.99.99.1 (bce1 99.99.99.1): S set, 40 headers + 0 data bytes

--- 99.99.99.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@mail ~]#
```

mail.lifeoverip.net - SecureCRT

File Edit View Options Transfer Script Tools Help

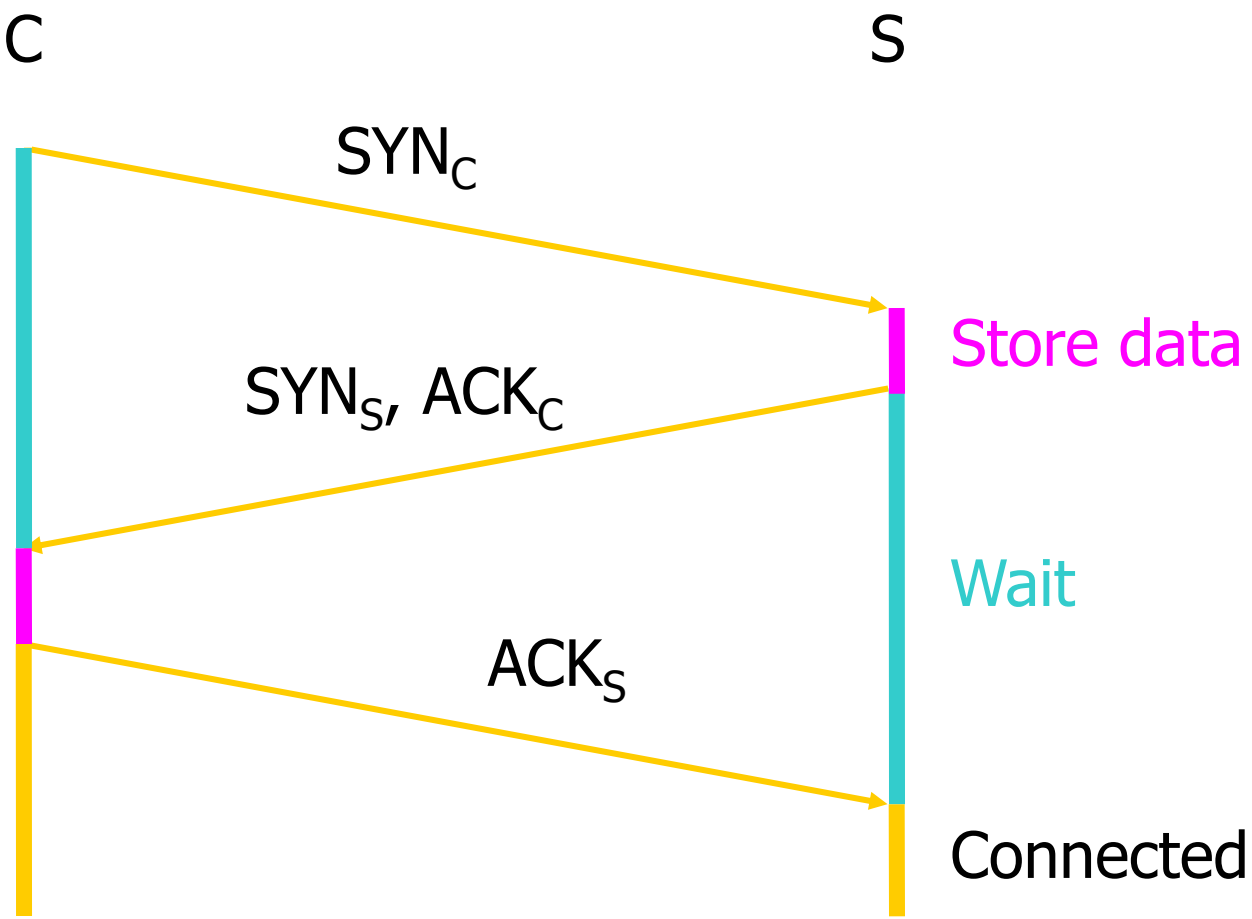
mail.lifeoverip.net

```
[root@mail ~]# tcpdump -i bce1 -v -s0 -tn host 99.99.99.1
tcpdump: listening on bce1, link-type EN10MB (Ethernet), capture size 65535 bytes
IP (tos 0x0, ttl 64, id 16922, offset 0, flags [none], proto TCP (6), length 40)
    91.93.119.80.2636 > 99.99.99.1.80: Flags [S], cksum 0xfeae (correct), seq 156218608, win 512, length 0
```

Gönderilen her SYN paketi için hedef sistem ACK-SYN paketi üretecektir.

TCP Handshake

- 3'lü el sıkışma olarak da adlandırılır

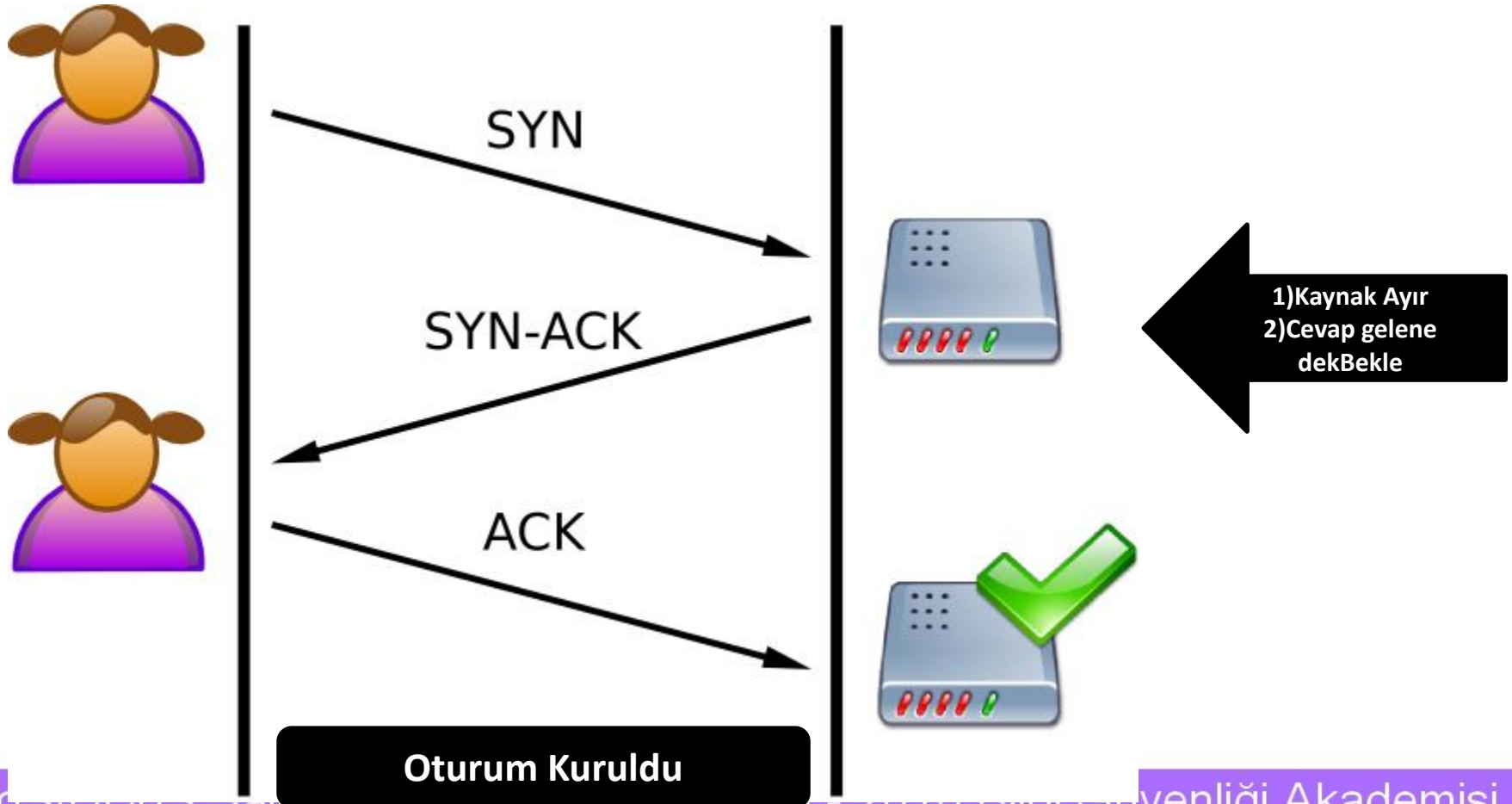


TCP Handshake-II

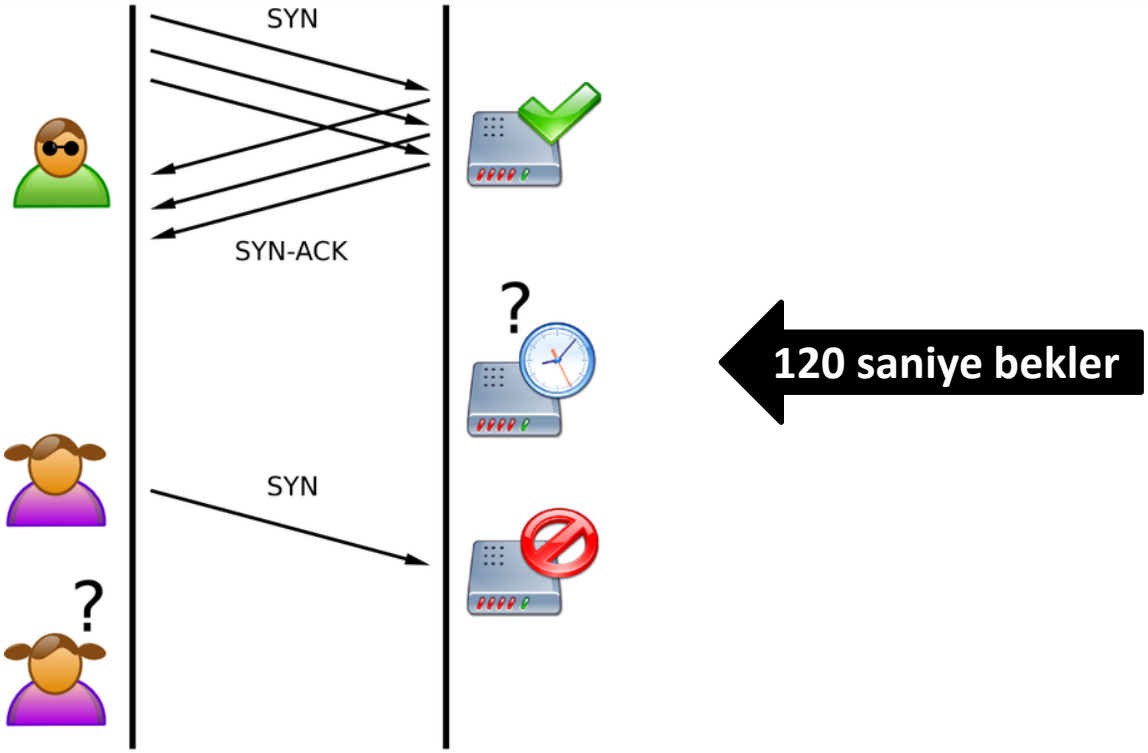
- Handshake esnasında sunucu tarafında hangi bilgiler tutulur?
  - TCP Control Block (TCB) tarafından aşağıdaki bilgileri tutulabilir
    - > 280 byte
    - FlowID, timer info, Sequence number, flow control status, out-of-band data, MSS, ..
  - Half-open TCB verileri zaman aşımına kadar tutulur
- Kaynak yeterli değilse yeni bağlantı kabul edilmeyecektir

SYN Flood Saldırıları

- Normal TCP İşleyişi



SYN Flood



- Bir SYN paketi ortalama 65 Byte
- 8Mb hat sahibi bir kullanıcı saniyede 16.000 SYN paketi üretebilir.

SynFlood

- Hedef sisteme kapasitesinin üzerinde SYN paketi göndererek yeni paket alamamasını sağlamaktır
- En sık yapılan DDoS saldırı tipidir
- İlk olarak 1994 yılında “Firewalls and Internet Security “ kitabından teorik olarak bahsi geçmiştir
- İlk Synflood DDoS saldırısı 1996 yılında gerçekleştirilmiştir

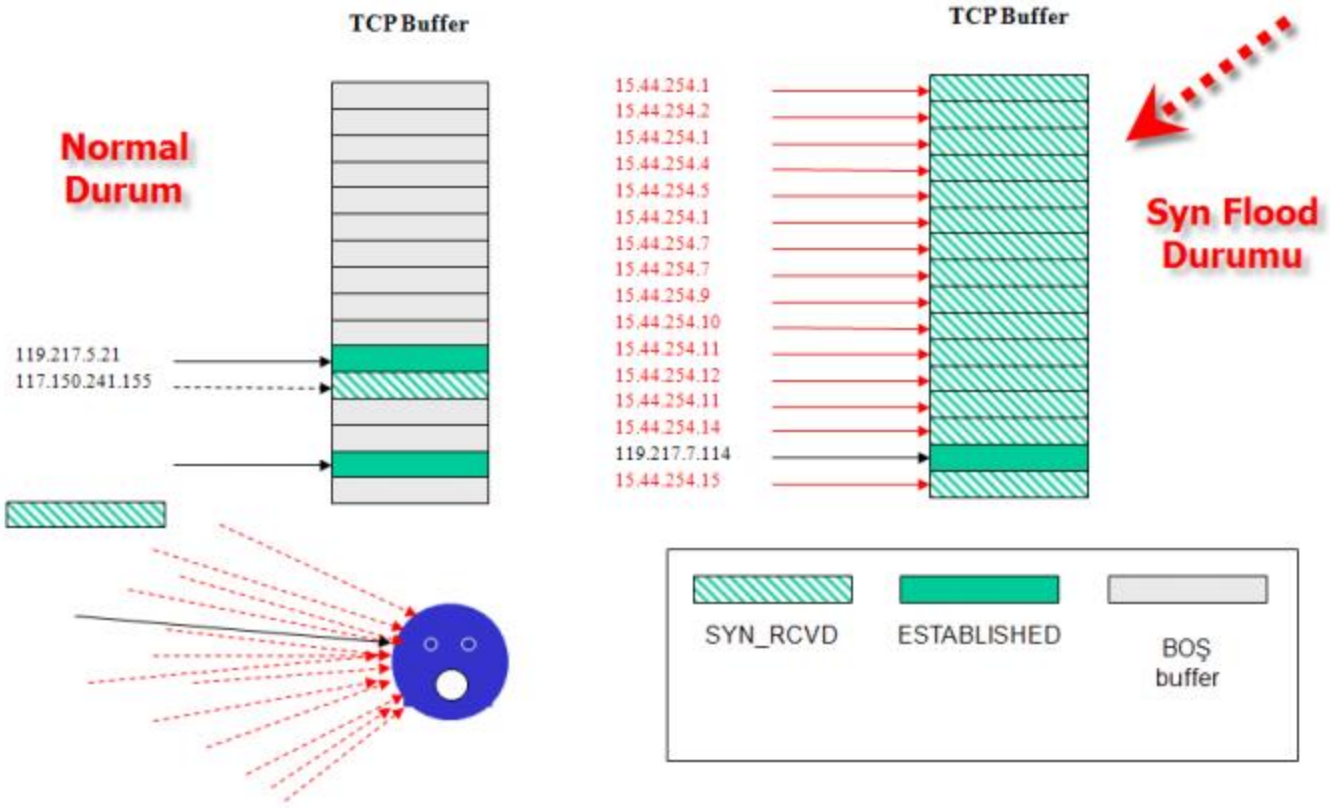
Nasıl Gerçekleştirilir?

- Syn Flood saldırısı basitce açık bir porta hedef sistemin kapasitesinden fazla gönderilecek SYN paketleriyle gerçekleştirilir.
- Buradaki “kapasite” tanımı önemlidir. Teknik olarak bu kapasiteye Backlog Queue denilmektedir.
- Saldırıyı yapan kendini gizlemek için gerçek IP adresi kullanmaz

Backlog Queue Kavramı(Kapasite)

- İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar bellekten bir alan kullanırlar, bu alan TCB olarak adlandırılır
- Bu alanların toplamı backlog queue olarak adlandırılır.
- Başka bir ifadeyle işletim sisteminin half-open olarak ne kadar bağlantı tutabileceğini backlog queue veriyapısı belirler.

Syn Flood Durumu

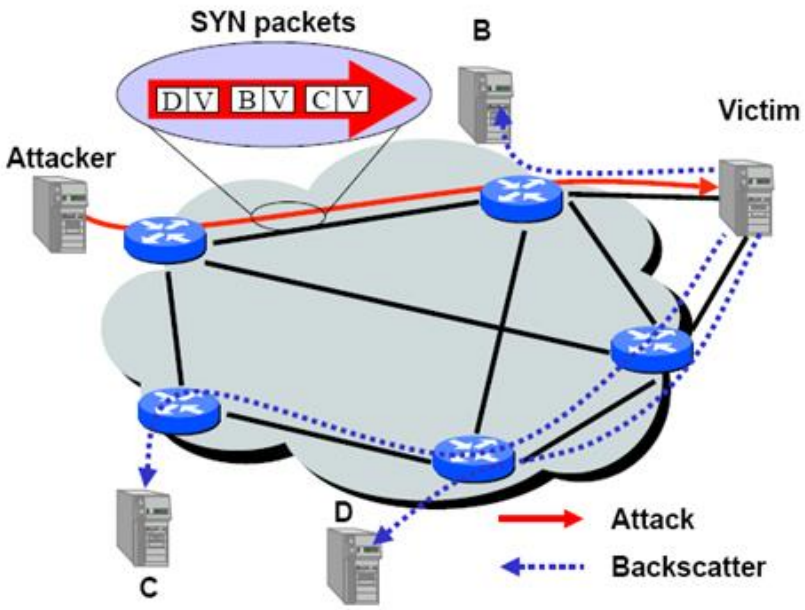


Syn Flood Ne Kadar Kolaydır?

- Tahmin edildiğinden daha çok!
- Örnek:
  - Backlog queue değeri 1000 olan sisteme 1000 adet SYN paketi göndererek servis veremez duruma getirilebilir.
  - 1000 adet SYN paketi=1000*60byte=60.000 byte=468Kpbs
  - Bu değer günümüzde çoğu ADSL kullanıcısının sahip olduğu hat kapasitesine yakındır.

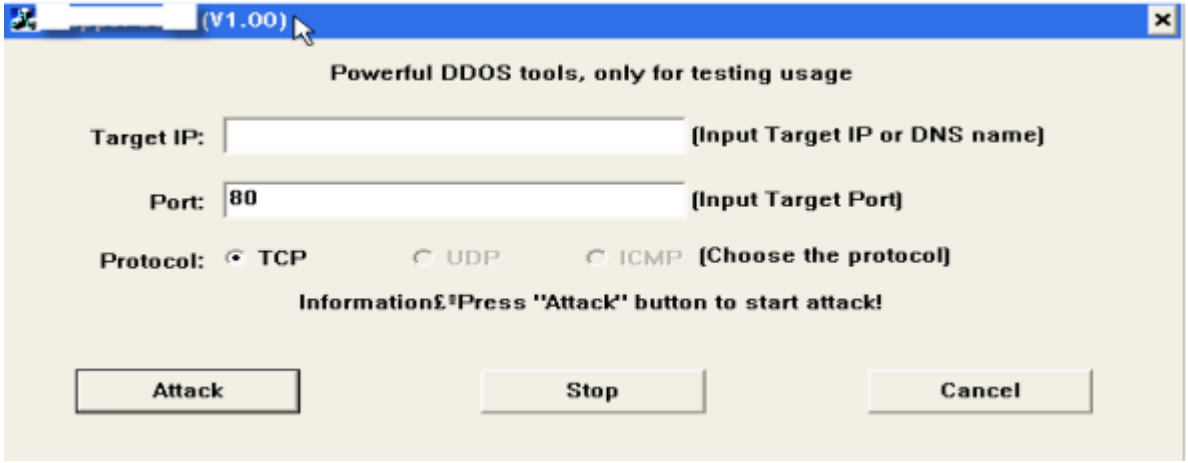
SynFlood Backscatter Tehlikesi

- SYN Flood saldırılarında sahte IP kullanılırsa saldırı yapılan sistemden geriye doğru binlerce SYN+ACK paketi dönecektir
  - Bu da ayrı bir saldırı olarak algılanabilir



Syn Flood Araçları

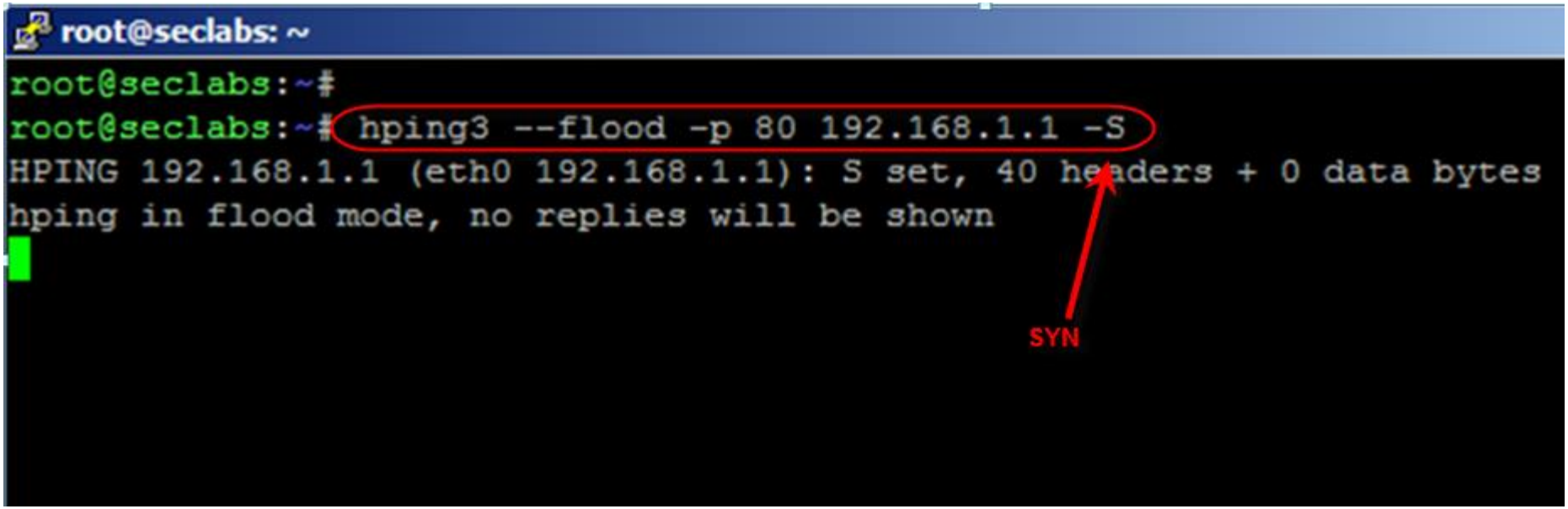
- Netstress
- Juno
- Hping
- Windows tabanlı araçlar
- BotNet yönetim sistemleri



SynFlood Örneği

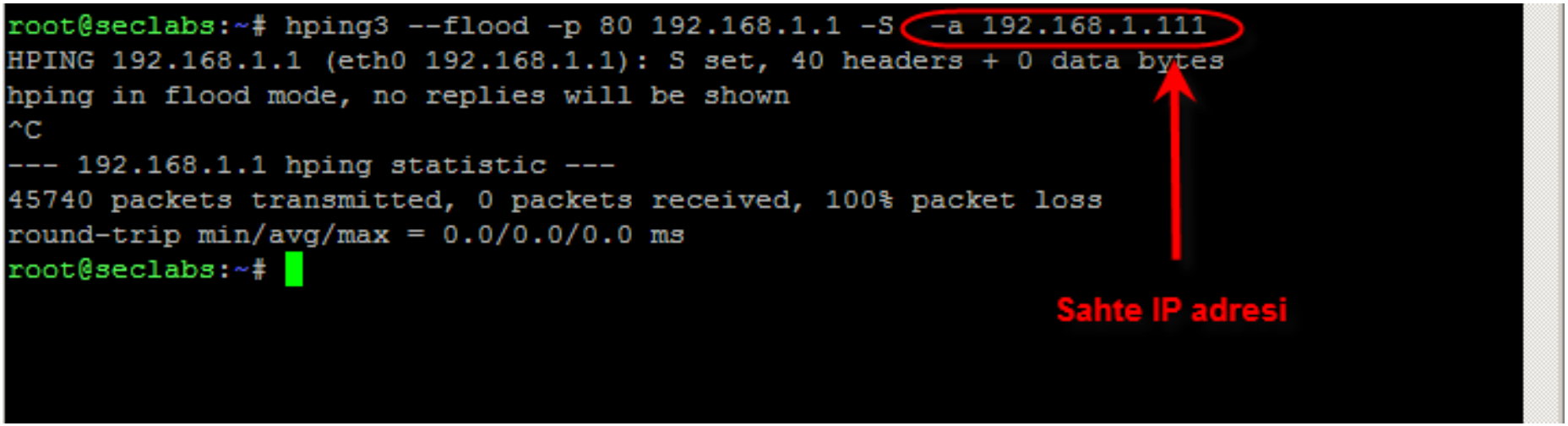
- Amaç:Hedef sisteme tamamlanmamış binlerce TCP SYN paketi gönderip servis verememesinin sağlanması
- Kullanılan araç: Hping

Syn Flood:Gerçek IP Adresleri Kullanarak



Syn Flood:Sahte IP Adresleri Kullanarak

- Kaynak IP adresi seçilen makine açıksa gelen SYN+ACK paketine RST cevabı dönecektir
- Ciddi saldırılarda kaynak ip adresleri canlı olmayan sistemler seçilmeli!



Random Sahte IP Adresi Kullanarak Syn Flood

```
root@seclabs:~# hping3 --flood -p 80 192.168.1.1 -S --rand-source
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.1 hping statistic ---
38910 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@seclabs:~#
```

Her biri farklı sahte IP adresleri

```
root@seclabs:~# tcpdump -i eth0 -n -c 10  not tcp port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:32:00.873729 IP 38.229.94.208.1131 > 192.168.1.1.80: S 1430370877:1430370877(0) win
512
15:32:00.874169 IP 51.156.106.34.1132 > 192.168.1.1.80: S 1541065602:1541065602(0) win
512
15:32:00.874496 IP 242.107.203.163.1133 > 192.168.1.1.80: S 467335447:467335447(0) win
512
15:32:00.875104 IP 51.5.104.198.1134 > 192.168.1.1.80: S 545020726:545020726(0) win 512
15:32:00.875434 IP 15.107.198.252.1135 > 192.168.1.1.80: S 1327699439:1327699439(0) win
 512
15:32:00.875686 IP 105.30.208.236.1136 > 192.168.1.1.80: S 1854543872:1854543872(0) win
 512
15:32:00.876281 IP 112.31.252.123.1137 > 192.168.1.1.80: S 148664490:148664490(0) win 5
12
15:32:00.876528 IP 51.99.83.148.1138 > 192.168.1.1.80: S 2016110487:2016110487(0) win 5
12
15:32:00.876748 IP 21.84.230.195.1139 > 192.168.1.1.80: S 577132950:577132950(0) win 51
2
15:32:00.877154 IP 160.184.35.181.1140 > 192.168.1.1.80: S 1478357594:1478357594(0) win
 512
```

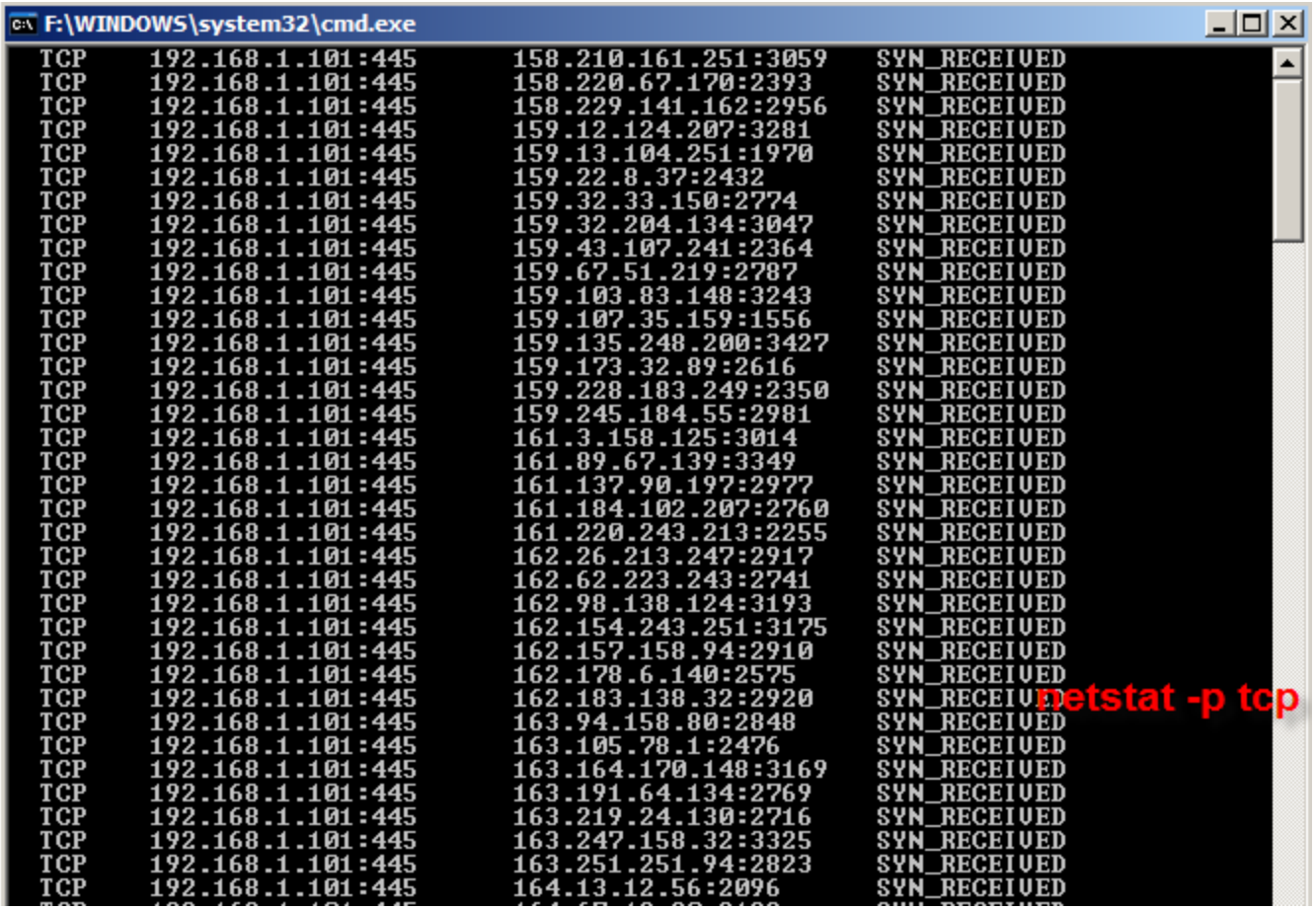
SynFlood DDoS Saldırıları Nasıl Anlaşılır?

- Temel mantık
  - Normalin üzerinden SYN paketi geliyorsa veya normalin üzerinde SYN_RECV durumu gözüküyorsa SYN Flood olma ihtimali vardır

Netstat ile SynFlood Belirleme

```
[root@hackme ~]# netstat -ant|grep SYN_RECV
tcp        0      0 91.93.119.77:80             87.67.208.159:2550          SYN_RECV
tcp        0      0 91.93.119.77:80             222.7.139.211:2553          SYN_RECV
tcp        0      0 91.93.119.77:80             84.126.171.37:2541          SYN_RECV
tcp        0      0 91.93.119.77:80             23.3.218.61:2545            SYN_RECV
tcp        0      0 91.93.119.77:80             61.156.167.224:2538         SYN_RECV
tcp        0      0 91.93.119.77:80             197.68.120.6:2533           SYN_RECV
tcp        0      0 91.93.119.77:80             75.217.84.238:2546          SYN_RECV
tcp        0      0 91.93.119.77:80             199.139.67.162:2555         SYN_RECV
tcp        0      0 91.93.119.77:80             108.60.179.141:2552         SYN_RECV
tcp        0      0 91.93.119.77:80             88.65.103.236:2540          SYN_RECV
tcp        0      0 91.93.119.77:80             141.6.36.83:2554            SYN_RECV
tcp        0      0 91.93.119.77:80             183.152.167.29:2556         SYN_RECV
tcp        0      0 91.93.119.77:80             51.220.145.73:2535          SYN_RECV
tcp        0      0 91.93.119.77:80             53.180.0.25:2542            SYN_RECV
tcp        0      0 91.93.119.77:80             26.155.106.211:2559         SYN_RECV
tcp        0      0 91.93.119.77:80             162.190.171.87:2561         SYN_RECV
tcp        0      0 91.93.119.77:80             112.38.199.120:2544         SYN_RECV
tcp        0      0 91.93.119.77:80             106.152.221.42:2537         SYN_RECV
tcp        0      0 91.93.119.77:80             85.172.27.202:2557          SYN_RECV
tcp        0      0 91.93.119.77:80             194.145.35.130:2548         SYN_RECV
tcp        0      0 91.93.119.77:80             198.55.236.250:2560         SYN_RECV
tcp        0      0 91.93.119.77:80             113.248.199.145:2549        SYN_RECV
tcp        0      0 91.93.119.77:80             98.87.167.160:2534          SYN_RECV
tcp        0      0 91.93.119.77:80             8.248.218.198:2563          SYN_RECV
tcp        0      0 91.93.119.77:80             85.127.141.187:2564         SYN_RECV
```

Netstat İle SynFlood Belirleme-Windows



Sahte IP Kullanımının Dezavantajları

- Synflood saldırısında sahte IP adresleri kullanılırsa
  - Her gönderilen SYN paketine karşılık hedef sistem sahte IP adreslerine SYN ACK paketi dönecektir.
  - Bu durumda sahte IP adreslerinin gerçek sahipleri sizden ACK flood saldırısı geliyormuş zannedebilir
  - Saldırgan belirli bir firmanın IP Adresinden geliyormuş gibi SynFlood Saldırısı gönderebilir

SynFlood Saldırılarını Engelleme

- Syn Flood Saldırısı gerçekleştirme çok kolaydır
- Syn flood saldırılarını engellemek çok kolaydır
- Syn flood saldırıları için tüm dünya iki temel çözümü kullanır
  - Syn cookie
  - Syn proxy
- Bu iki çözüm haricinde endüstri standartı haline gelmiş başka çözüm bulunmamaktadır
  - Farklı adlandırmalar kullanılabilir(syn authentication gibi)

Klasik TCP Bağlantısı

- Normal TCP bağlantılarında gelen SYN bayraklı pakete karşılık ACK paketi ve SYN paketi gönderilir.
- Gönderilen ikinci(sunucunun gönderdiği) SYN paketinde ISN değeri random olarak atanır ve son gelecek ACK paketindeki sıra numarasının bizim gönderdiğimizden bir fazla olması beklenir.
- Son paket gelene kadar da sistemden bu bağlantı için bir kaynak ayrılır(backlog queue)
  - Eğer SYN paketine dönen ACK cevabı ilk sny paketininin ISN+1 değilse paket kabul edilmez.

SynCookie Aktifken TCP Bağlantısı

- Syncookie aktif edilmiş bir sistemde gelen SYN paketi için sistemden bir kaynak ayrılmaz
- SYN paketine dönecek cevaptaki ISN numarası özel olarak hesaplanır (kaynak.ip+kaynak.port+.hedef.ip+hedef.port+x değeri) ve hedefe gönderilir
- Hedef son paket olan ACK'i gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı kurulur
  - Değilse bağlantı iptal edilir

SYN Cookie Değeri

cookie = hash(saddr, daddr, sport, dport) + sseq

where
saddr : Source IP Address
daddr : Destination IP Address
sport : Source Port
dport : Destination Port
sseq : Source Sequence Number.

Sny Cookie-II

- Böylece spoof edilmiş binlerce ip adresinden gelen SYN paketleri için sistemde bellek tüketilmemiş olacaktır ki bu da sistemin SYNflood saldırıları esnasında daha dayanıklı olmasını sağlar.
- Syncookie mekanizması backlogqueue kullanmadığı için sistem kaynaklarını daha az kullanır
- Syncookie aktif iken hazırlanan özel ISN numarası cookie olarak adlandırılır.

SynCookie Dezavantajları

- Syncookie'de özel hazırlanacak ISN'ler için üretilen random değerler sistemde matematiksel işlem gücü gerektirdiği için CPU harcar
- Eğer saldırının boyutu yüksekse CPU performans problemlerinden dolayı sistem yine darboğaz yaşar
- DDOS Engelleme ürünleri(bazı IPS'ler de) bu darboğazı aşmak için sistemde Syncookie özelliği farklı CPU tarafından işletilir

SynCookie Dezavantajları-II

- Syncookie özelliği sadece belirli bir sistem için açılamaz.
  - Ya açıktır ya kapalı
  - Bu özellik çeşitli IPS sistemlerinde probleme sebep olabilir.
- Syncookie uygulamalarından bazıları TCP seçeneklerini tutmadığı için bazı bağlantılarda sorun yaşatabilir.

SYN Cookie Alt etme

- Sunucu tarafında kullanılan syncookie özelliği istemci tarafında da kullanılarak sunucudaki syncookie özelliği işe yaramaz hale getirilebilir.
- Böylece istemci kendi tarafında state tutmaz, sunucu tarafında da 3'lü el sıkışma tamamlandığı için bağlantı açık kalır(uzuun süre)
- Sockstress, scanrand araçları

TCP Connection Flood

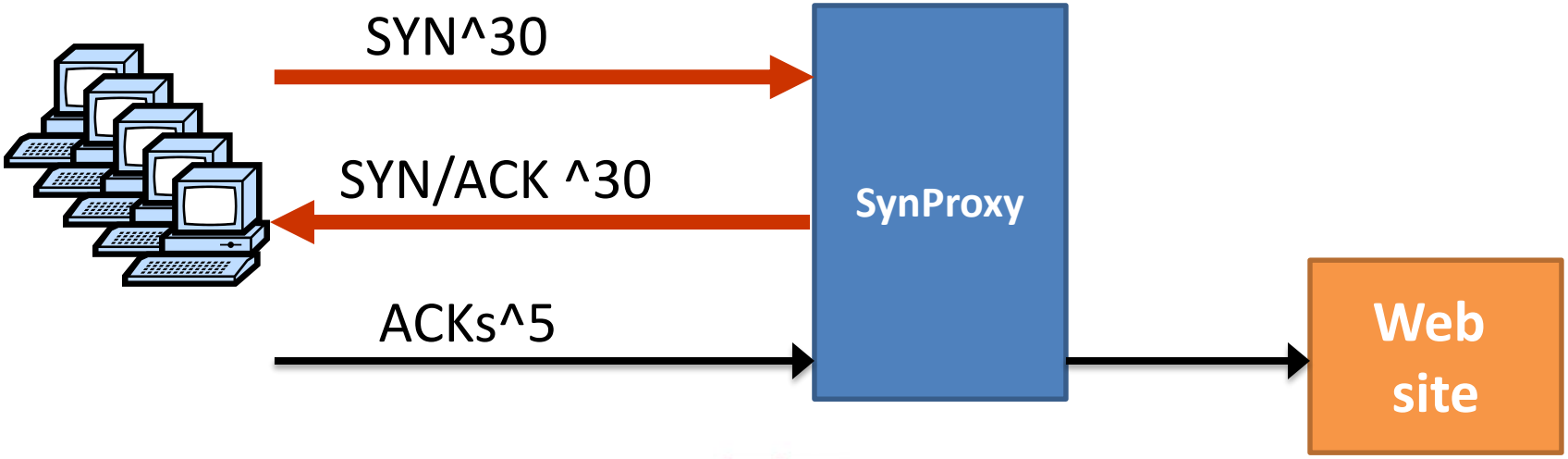
- Hedef sisteme 1000 adet SYN paketi gönder
- Gelen SYN+ACK paketlerindeki ISN numarasını al
  - Bir fazlasını ekleyerek ACK paketi gönder
  - Hedef sistemde 3'lü el sıkışma tamamlanmış ve Syncookie devreden çıkmıştır
- Aynı işlemi tekrarla
  - Hedef sistemin state tablosu dolunca bırak!
- Syncookie atlatma için etkili bir saldırı yöntemidir
- Rate limiting uygulayan Firewall/IPS'ler tarafından rahatlıkla yakalanabilir

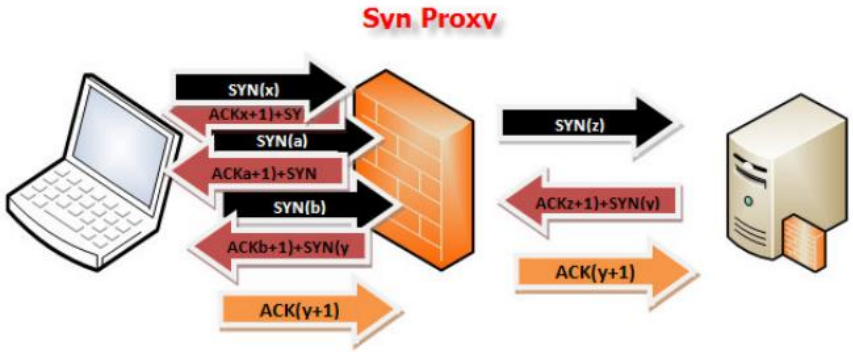
SynProxy

- SynProxy, adından da anlaşılacağı üzere SYN paketlerine karşı proxylik yapmaya yarayan bir özelliktir.
- Güvenlik duvarlarında ve Syncookie'nin kullanımının sıkıntılı olduğu durumlarda rahatlıkla kullanılabilir.
- Syncookie gibi arkasında korumaya aldığı sistemlere gelecek tüm SYN paketlerini karşılar ve üçlü el sıkışma tamamlandıktan sonra paketleri koruduğu sistemlere yönlendirir.
-

SynProxy Mantığı

- Sadece oturum kurulmuş TCP bağlantılarını sunucuya geçir!





SynProxy Dezavantajları

- Synproxy'de proxylik yapan makine state bilgisi tuttuğundan yoğun saldırılarda state tablosu şişebilir
- Synproxy ya hep açıktır ya da kapalı
  - Belirli değerin üzerinde SYN paketi gelirse aktif et özelliği yoktur

Stateless SynProxy

- Syncookie ve synproxy özelliklerinin birleştirilmiş hali
- Syncookie'nin avantajı olan state tutmama özelliği
- Synproxy'nin esnekliği alınarak oluşturulmuştur
- En ideal çözüm olarak bilinir.

SYN Flood Koruma-1

- Tcp timeout değerlerini düşürme

```
TIMEOUTS:
tcp.first                    120s
tcp.opening                   30s
tcp.established            86400s
tcp.closing                  900s
tcp.finwait                   45s
tcp.closed                    90s
tcp.tsdiff                    30s
udp.first                     60s
udp.single                    30s
udp.multiple                  60s
icmp.first                    20s
icmp.error                    10s
other.first                   60s
other.single                  30s
other.multiple                60s
frag                          30s
interval                      10s
adaptive.start         60000 states
adaptive.end          120000 states
src.track                      0s
```

Syn Flood Engelleme

- Synflood engelleme standartı:Syncookie/SynProxy
- Linux sistemlerde Syncookie ile yapılabilir
  - Syncookie STATE tutmaz, state tablosunu kullanmaz
- OpenBSD PF Synproxy
  - En esnek çözüm: ip, port, paket özelliklerine göre aktif edebilme ya da kapatabilme özelliği
  - pass in log(all) quick on $ext_if proto tcp to $web_servers port {80 443} **flags S/SA synproxy state**
  - (((Loglama sıkıntı çıkarabilir)))

SynFlood Engelleme-II

- TCP timeout değerleriyle oynama
  - Default değerler yüksektir...
  - Saldırı anında dinamik olarak bu değerlerin 1/10'a düşürülmesi saldırı etkisini azaltacaktır.
- Linux için sysctl ile (manuel)
- OpenBSD PF için
  - set timeout {tcp.first 10, tcp.opening 10 tcp.closing 33, tcp.finwait 10, tcp.closed 20} gibi... Ya da
- Packet Filter adaptive timeout özelliği!
  - State tablosu dolmaya başladıkca timeout değerlerini otomatik azalt!

SynFlood engelleme-III

- Rate limiting(bir ip adresinden 500'den fazla istek geldiyse engellenecekler listesine ekle ve o ip adresine ait oturum tablosunu boşalt)
- OpenBSD Packet Filter
  - ... flags S/SA synproxy state (max-src-conn 500, max-src-conn-rate 100/1, overload <ddos_host> flush global)
- Linux iptables modülleri
  - -m limit, recent vs

SynFlood engelleme-IV

- Beyaz liste, kara liste uygulaması
  - Daha önce state oluşturmuş, legal trafik geçirmiş ip adresleri
- Ülkelerin IP bloklarına göre erişim izni verme
  - Saldırı anında sadece Türkiye IP'lerine erişim açma

(((IP spoofing kullanıldığı için çoğu zaman işe yaramaz)))

- DNS round-robin & TTL değerleriyle oynayarak engelleme

Linux Syncookie dezavantajları

- Donanım iyiyse yeterli koruma sağlar
  - Syncookie CPU'ya yüklendiği için CPU %100'lere vurabilir
  - Ethernet kartının üreteceği IRQ'lar sistemi zora sokabilir
- Sadece kendisine syncookie koruması sağlar
- 1/0 . Aç - kapa özelliğindedir, çeşitli uygulamalarda SYNcookie sıkıntı çıkartabilir. Bir port/host için kapama özelliği yoktur

SynProxy Dezavantajları

- SynProxy=State=Ram gereksinimi
- State tablosu ciddi saldırılarda çok çabuk dolar
  - 100Mb~=200.000 SYN=200.000 State
    - 40 saniyede 8.000.000 state = ~5GB ram ...
  - Tcp timeout değerlerini olabildiğince düşürmek bir çözüm olabilir
    - Timeout süresi 5 saniye olursa ?

(((Genel Çözüm: Stateless SynProxy çözümü)))

Rate limiting dezavantajları

- Akıllı saldırganın en sevdiği koruma yöntemidir☺
- Neden ?

Diğer TCP Flood Saldırıları

- Sık görülmese de FIN, ACK ve RST Flood saldırıları da DDoS amaçlı kullanılmaktadır

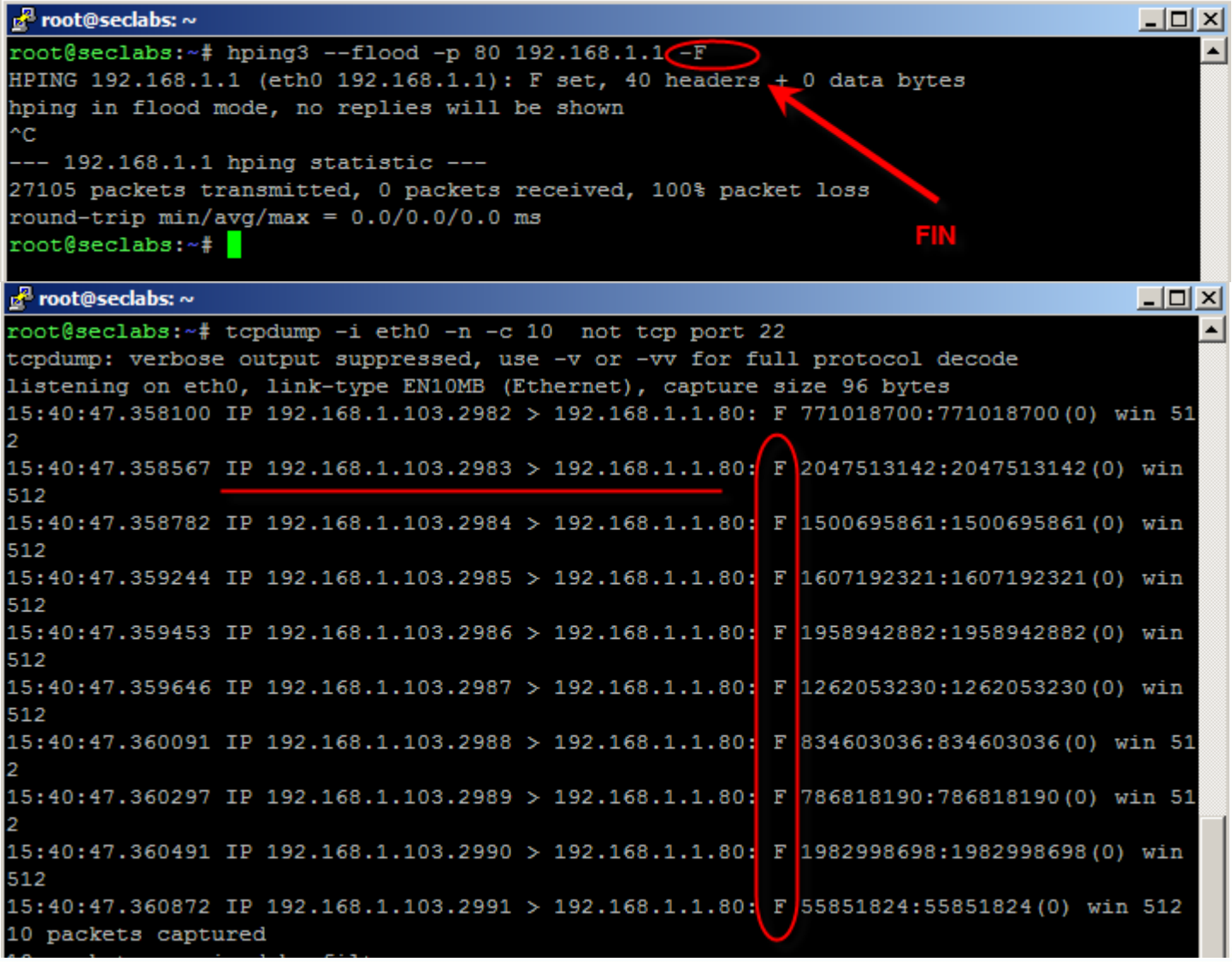
ACK, FIN, PUSH Flood Saldırıları

- SynFlood'a karşı önlem alınan sistemlerde denenir.
- Hedef sisteme ACK, FIN, PUSH bayraklı TCP paketleri göndererek güvenlik cihazlarının kapasitesiniz zorlama
- Diğer saldırı tiplerine göre engellemesi oldukça kolaydır
- Etki düzeyi düşüktür

ACK,FIN,PUSH Saldırıları Engelleme

- Gelen ilk paketin SYN paketi olma zorunluluğu, oturum kurulmamış paketleri düşürme
- OpenBSD Packet Filter
  - scrub all
- Linux
  - İptables kuralları

FIN Flood Saldırısı



ACK Flood Saldırısı

```
root@seclabs:~#
root@seclabs:~# hping3 --flood -p 80 192.168.1.1 -A
HPING 192.168.1.1 (eth0 192.168.1.1): A set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.1 hping statistic ---
22661 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@seclabs:~#
```