Saldırgan Yaklaşımı

Nebi Şenol YILMAZ
Danışman / Yönetici Ortak
senol.yilmaz@secrove.com

Secrove Information Security Consulting

Hakkımda

- Nebi Şenol YILMAZ, CISA, CEH, 27001 LA
- Secrove Information Security Consulting
  - Bilgi Güvenliği Danışmanlığı
  - Bilgi Sistemleri Denetimi
  - Penetrasyon Testleri
  - Zafiyet Araştırması
  - Exploit Geliştirme
  - Bilgi Güvenliği Ar-Ge (Tubitak Destekli)

Hakkımda

- IT Auditor, HSBC Bank A.Ş.
- Information Security Manager, E-Bay Turkiye
- Info. Security Researcher, Tubitak – UEKAE
- Software Engineer, METU

Ajanda

- Ne Yapıyor ?
- Nasıl Yapıyor ?
- Avantajı...
- Adım Adım...
- Özet

Ne yapıyor ?

- Her zaman zayıf noktaları arıyor...

Nasıl Yapıyor ?

- Saldırgan kurumların içinde de olabiliyor.

Avantajı...

- Kurumlar çoğu zafiyeti gözardı ediyor...

Avantajı...

- Saldırganda zaman kısıtı bulunmuyor !!!

Avantajı...

- Akla gelmeyecek şekilde...
  - Facebook
  - Personel ortak portal
  - Toplantılar, seminerler
- Gözardı edilen her nokta...
  - VoIP, Çağrı sistemi, destek bağlantı hattı, çöp kutuları
- Alternatif giriş yolu

Giriş için her yol mübah...

Adım Adım ?

- Bilgi Toplama
  - Google, Shodan, kurum sitesi, dergi, gazete, whois, nslookup
- Tarama
  - Nmap, nessus, sslscan
- Erişim Sağlama
  - Metasploit, telnet, sslstrip, dnstunnel, ssh, arpspoof
- Erişimi Sürdürme
  - Netcat, ssh
- Saldırı Gizlemek
  - Ssh, dnstunnel

Adım Adım ?

- Bilgi Toplama ve Tarama
  - Google Search
    site:hedefsite.com -www
    inurl, filetype, intext, intitle...

  - Shodan Search
    country:tr
    net, port, server, os

Saldırgan Neler Yapıyor ?

- Erişim Sağlama
  - En zayıf halka her zaman INSAN...
  - Sistemler de saldırgana yardım ediyor :)

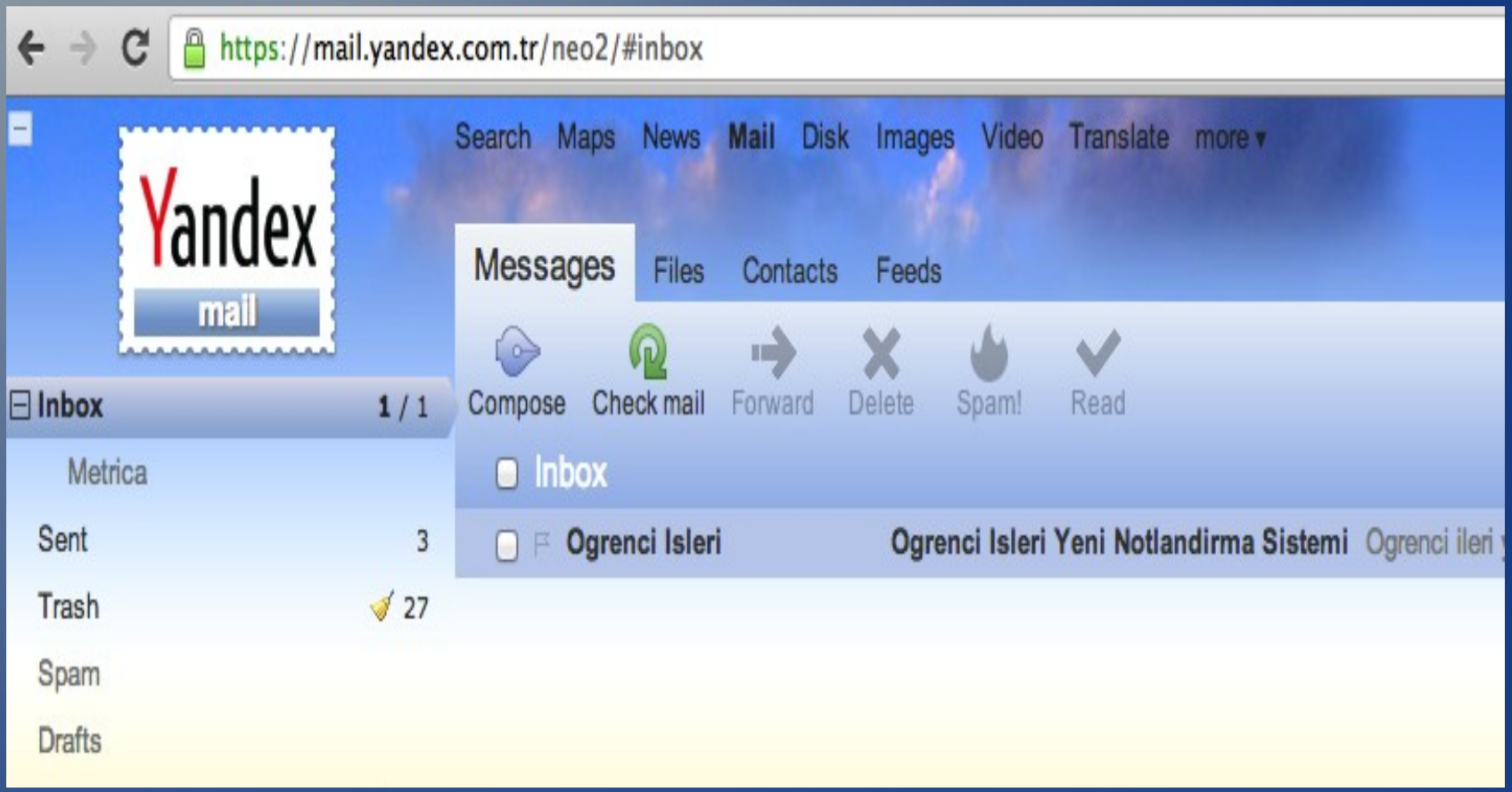
ve herşey bir mail ile başlayabiliyor...

Saldırgan Neler Yapıyor ?

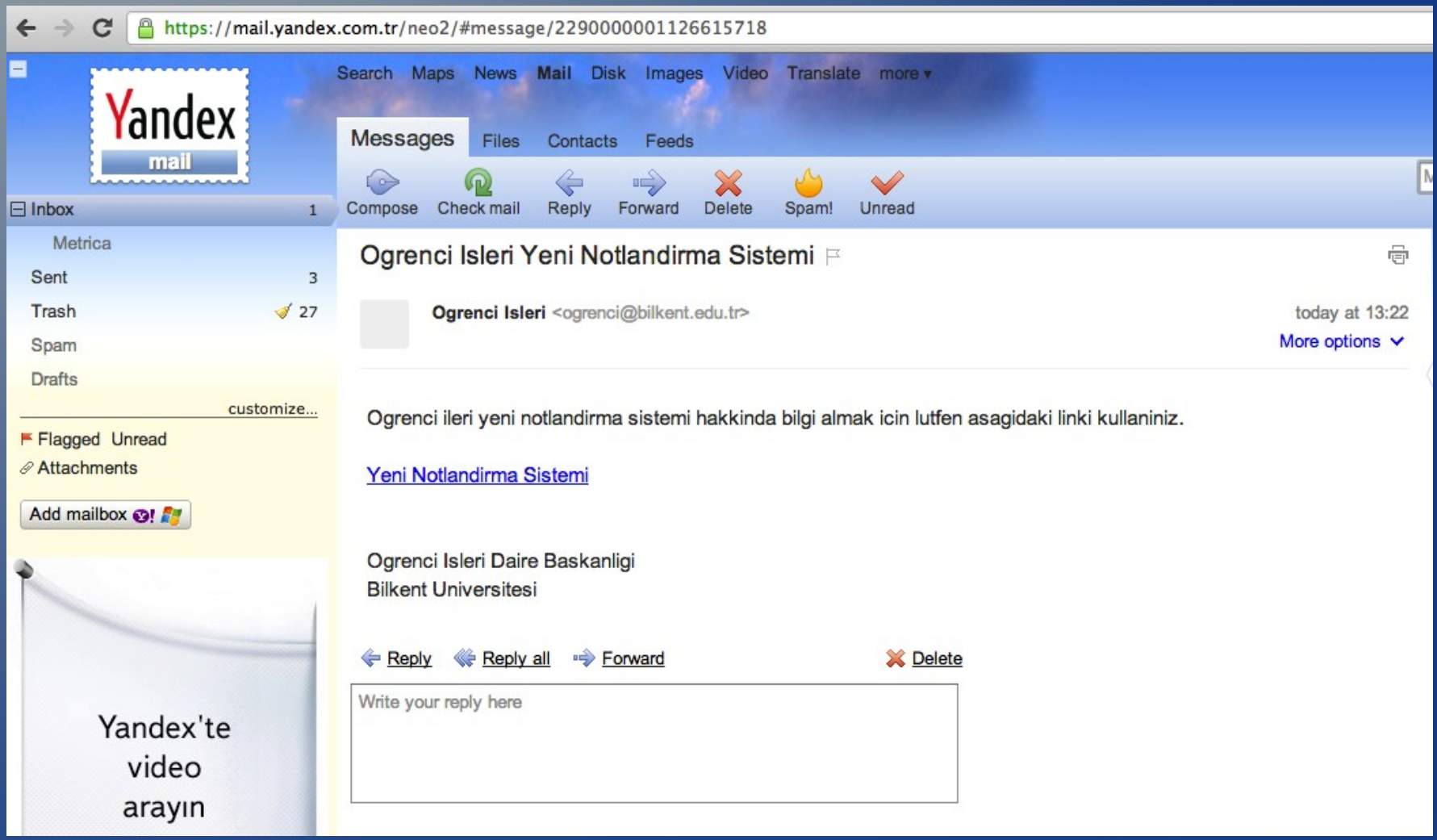
nsyilmaz — e139837@divan: /home/ms1/e139837 — ssh — 18

```
e139837@divan:~$ telnet mx.yandex.ru 25
Trying 213.180.193.89...
Connected to mx.yandex.ru.
Escape character is '^]'.
220 mxfront6h.mail.yandex.net (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
helo test
250 mxfront6h.mail.yandex.net
mail from:yok@yok.com
250 2.1.0 <yok@yok.com> ok
rcpt to:nsyilmaz@yandex.com
250 2.1.5 <nsyilmaz@yandex.com> recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: Ogrenci Isleri Yeni Notlandirma Sistemi
From:Ogrenci Isleri <ogrenci@bilkent.edu.tr>
To:nsyilmaz@yandex.com
Content-Type: text/html;


Ogrenci ileri yeni notlandirma sistemi hakkinda bilgi almak icin lutfen asagidaki linki kullaniniz. <br> <br>

<a href='http://www.secrove.com/'> Yeni Notlandirma Sistemi</a> <br> <br>


<br>
Ogrenci Isleri Daire Baskanligi <br>
Bilkent Universitesi

.
250 2.0.0 Ok: queued on mxfront6h.mail.yandex.net as IpK4eZXA-J2KGAmQ2
```

Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?

Görüntüde tamamen doğruymuş gibi görünen mail, aslında hedef aldığı kişiyi malware bulaştıracak bir siteye yönlendirebilmektedir.

Maili alan kişinin linke tıklaması, bilgisayarın ele geçirilmesi için yeterli olacaktır.

POC: 0-day exploit ile bilgisayarın ele geçirilmesine ilişkin örnek.

http://www.youtube.com/watch?v=IKsdHQTD34w

Neden DoS/DDoS?

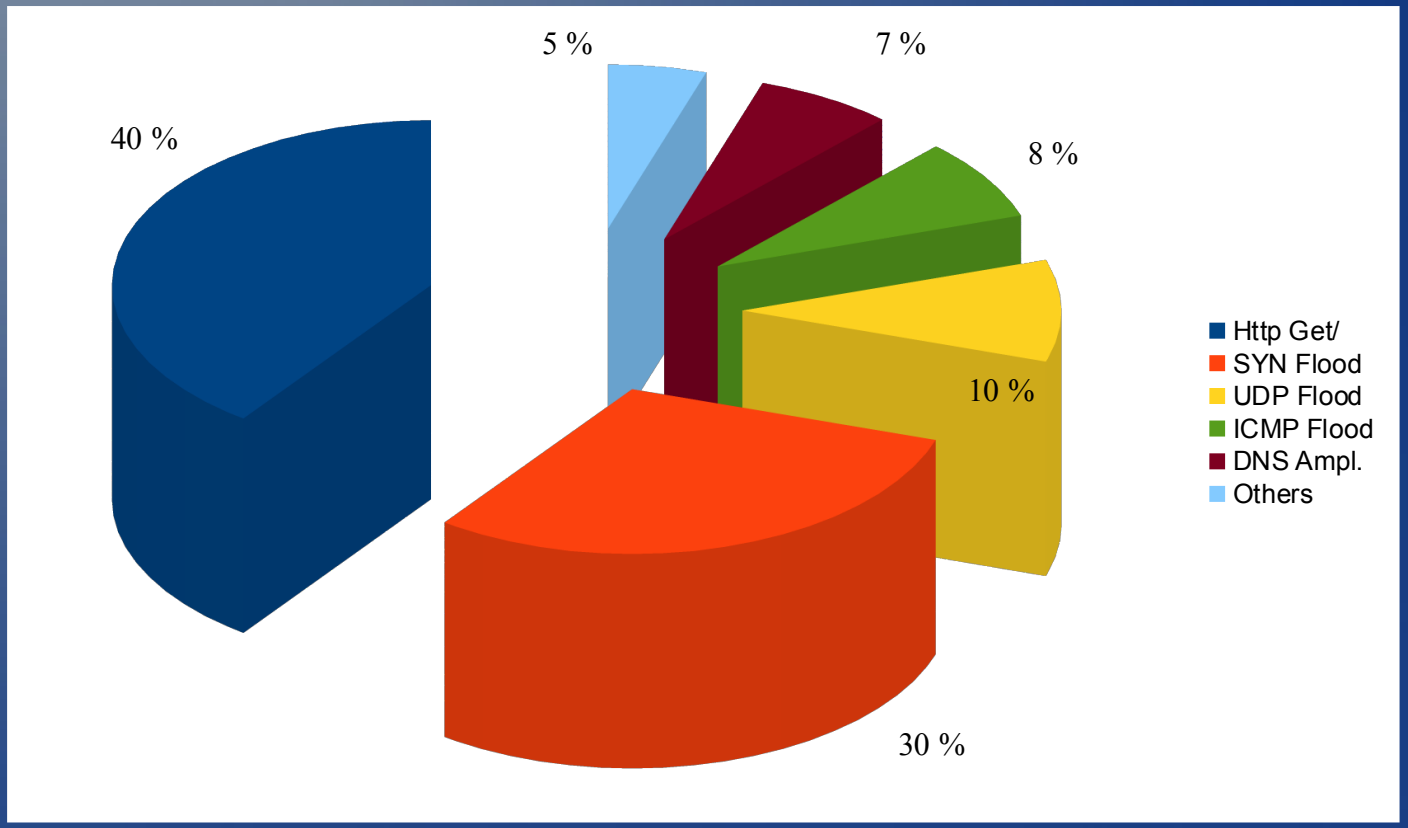
Neden DoS/DDoS?

Artık hayatımızın bir parçası oldu...

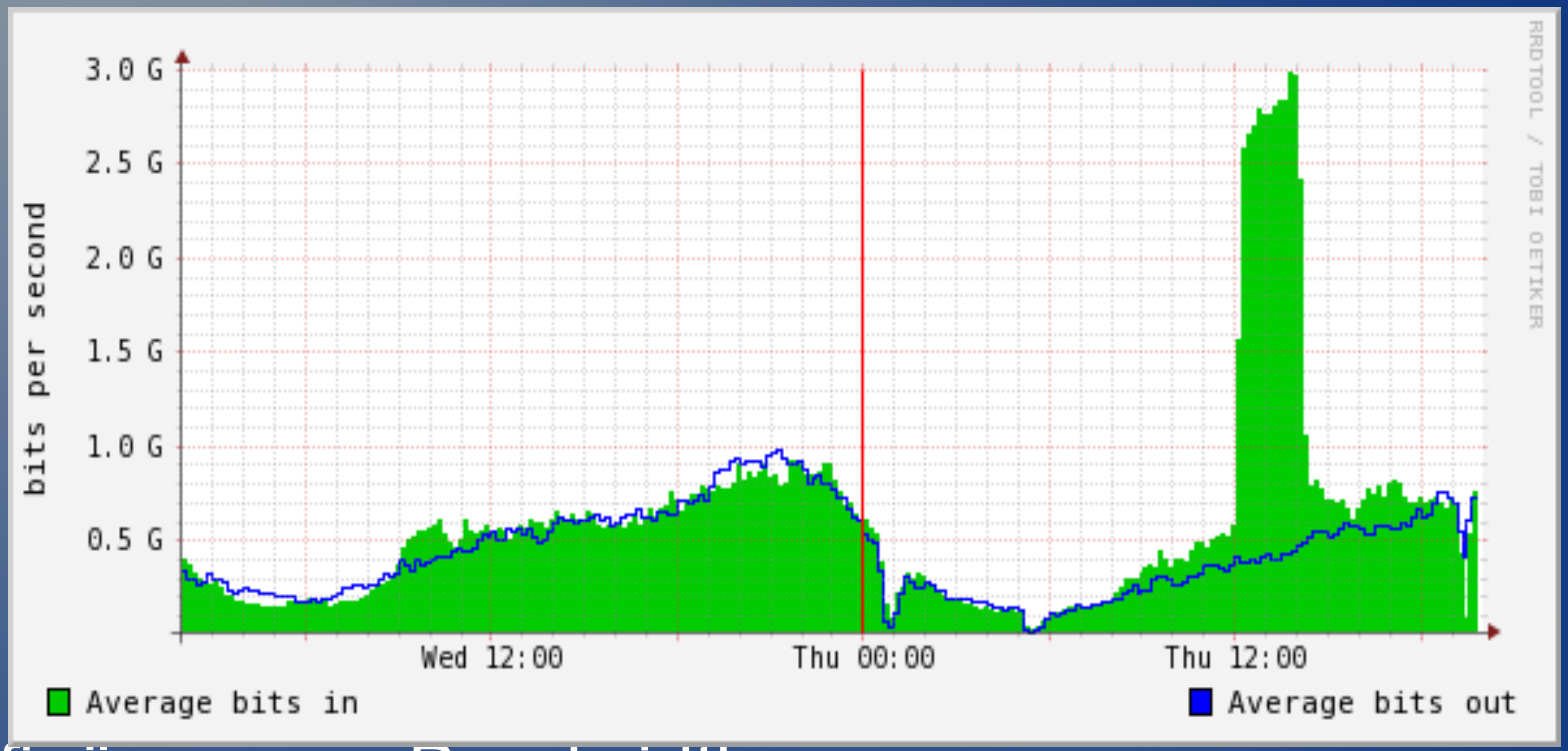
- WikiLeaks, VISA, MasterCard and PayPal
- Amazon, E-Bay
- Sony PlayStation, WordPress
- Borsaya yapılan saldırılar (Hong-Kong)
- Saldırı ile protesto (US, Israel, TR)
- Off-line olmak... (TTNet)

Neden DoS/DDoS?

Peki nasıl...?



Neden DoS/DDoS?



Konfigürasyon - Bandwidth

Neden DoS/DDoS?

DoS / DdoS sadece konfigürasyon ya da bandwidth problemi değildir...

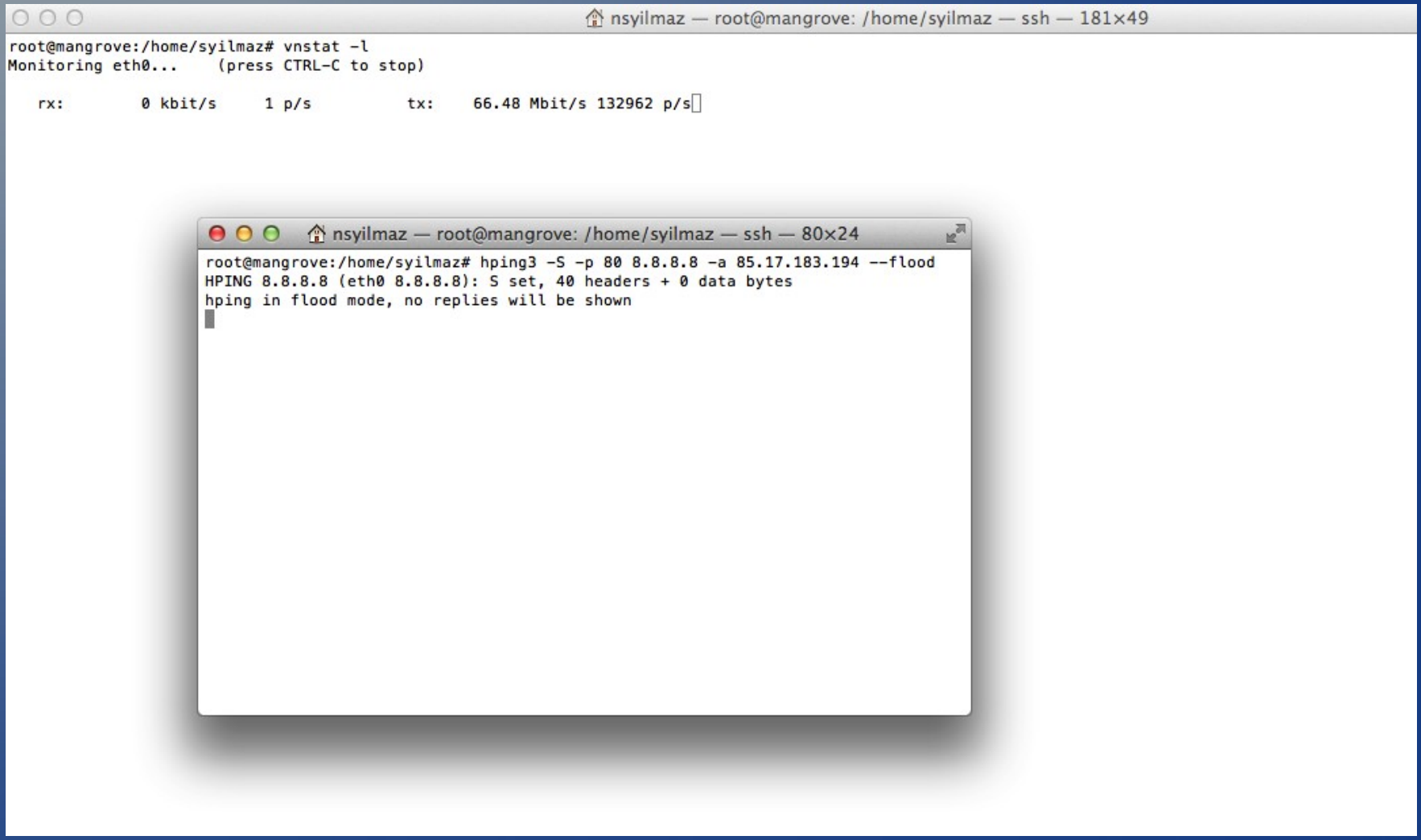
- Farkındalık
- Teknik altyapı
- Teknik bilgi birikimi

Geleneksel IPS veya güvenlik duvarı cihazları haricinde spesifik DDoS çözümlerinin kullanılması gerekmektedir.

Neden DoS/DDoS?

Gerçekleştirmesi çok kolay, kullanabildiğiniz kaynak kapsamında tek komut ile saldırı gerçekleştirilebiliyor.

Neden DoS/DDoS?



Neden DoS/DDoS?

```
# hping3 -S -p 80 8.8.8.8 -a 85.17.183.194 --floood
```

hping komutu, TCP/IP paketleri oluşturmak için geliştirilen bir programdır. Kullandığınız parametreler ile bunu bir saldırı aracı olarak kullanabilirsiniz.

Neden DoS/DDoS?

```
# hping -S -p 80 8.8.8.8 -a 85.17.183.194 --floood
```

-S : Syn paketi
-p 80 : TCP 80 portu
-a 85.17.183.194 : Spoof edilecek source IP addr.
--flood : Pketleri flood olarak arbitrary gönder

Sonuç: Basit bir sunucu ile ~60 Mbit/s SYN flood saldırısı gerçekleştirilmiş olur.
Ayrıca IP spoof ile de kimliğimiz gizlenmiş olur.

Önleme

- Packet Accounting
- Syn Cookies (into seq. num.)
- Syn Caches (160 vs 736 bytes TCB)
- Syn Proxy
- TCP Backlog
- SYN-Received Timer

Özet

- Saldırgan genellikle bir adım önümüzdedir...
- Sistemlere girmek için her yolu deneyecektir.
- Motive olmak için büyük beklentileri olmayabilir.
- En zayıf halka genellikle insandır.
- Sistemler fazlaca yardımcı olur.

Teşekkürler !

senol.yilmaz@secrove.com

@nsyilmaz

nsyilmaz