

PASİF BİLGİ TOPLAMA



Bilgi toplama;

Hedef sistemle doğrudan iletişime geçerek ve hedef sistemden bağımsız olmak üzere iki türdür.

Aktif Bilgi Toplama

Pasif Bilgi Toplama

Pasif bilgi toplama, penetrasyon testlerinde bilgi toplama bölümünün ilk adımını teşkil etmektedir. **Hedef sistem ile doğrudan iletişime geçilmez, herhangi bir iz bırakmadan internetin imkanları kullanılarak yapılır.** Hedef ile ilgili tüm bilgiler internet üzerinden kuruma ait sistem ve sunuculara erişmeden toplanmaya çalışılır.



pipl



SIK KULLANILAN YÖNTEMLER:

- ▶ Whois: DNS sorgularını yapabileceğimiz ve pasif bilgi toplamak için kullanılan özel web sayfaları
- ▶ Arama motorları (Google, Bing, Yahoo vs.)
- ▶ Sosyal paylaşım ağları (Twitter, Facebook, LinkedIn, Pipl vs.)
- ▶ Bloglar ve tartışma forumları
- ▶ Kariyer siteleri
- ▶ Github

Whois

“

- ▶ Eğer elinizde bir domain varsa <http://www.whois.com.tr/> 'ye girip:
- ▶ Bu domain kime ait?
- ▶ Hangi sunucu bu web hizmetini sağlıyor?
- ▶ Adres ne zaman alındı?
- ▶ Nereden satın alındı?
- ▶ Şirketin IP aralığı ne, sorumlu yöneticisi kim?
- ▶ gibi soruların cevabını bulabilirsiniz.
- ▶ Whois komut kullanımı:
- ▶ Terminal ekranına **sudo apt-get install whois**
- ▶ yazarak kurabilir ve **whois www.blabla.com** yazarak domain name bilgilerine ulaşabilirsiniz.

”

ARIN(American Registry for Internet Numbers)

- <https://www.arin.net/> e girip bulduğunuz IP yi arattığınızda IP aralığını i verir.

The screenshot shows the ARIN website's WHOIS-RWS search interface. The search bar at the top right contains the IP address 50.63.202.28. The search results are displayed in a table format under the heading 'WHOIS-RWS'. The table lists various details about the IP address, including the network range, CIDR, name, handle, parent, net type, origin AS, organization, registration date, last updated date, comments, and RESTful link. A sidebar on the right contains a list of relevant links.

ARIN
American Registry for Internet Numbers

SEARCH WhoisRWS
all requests subject to [terms of use](#) [advanced search](#)

NUMBER RESOURCES | PARTICIPATE | POLICIES | FEES & INVOICES | KNOWLEDGE | ABOUT US

WHOIS-RWS

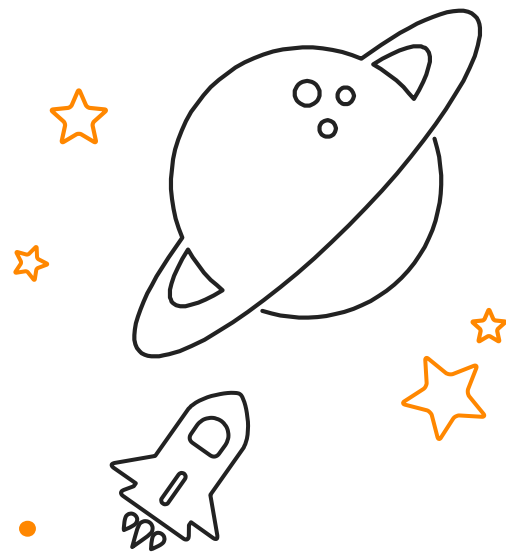
You searched for: 50.63.202.28

Network	
Net Range	50.62.0.0 - 50.63.255.255
CIDR	50.62.0.0/15
Name	GO-DADDY-COM-LLC
Handle	NET-50-62-0-0-1
Parent	NET50 (NET-50-0-0-0-0)
Net Type	Direct Allocation
Origin AS	AS26496
Organization	GoDaddy.com, LLC (GODAD)
Registration Date	2011-02-02
Last Updated	2014-02-25
Comments	Please send abuse complaints to abuse@godaddy.com
RESTful Link	https://whois.arin.net/rest/net/NET-50-62-0-0-1

Function	Point of Contact
NOC	NOC124-ARIN (NOC124-ARIN)
Tech	NOC124-ARIN (NOC124-ARIN)

RELEVANT LINKS

- > [ARIN Whois/Whois-RWS Terms of Service](#)
- > [Report Whois Inaccuracy](#)
- > [Whois-RWS API documentation](#)
- > [ARIN Technical Discussion Mailing List](#)
- > [Sample stylesheet \(xsl\)](#)



WaybackMachine

- 1966 dan bu yana web sitelerin önceki kaydedilmiş bilgilerini tutar.

Waybackmachine

INTERNET ARCHIVE

WayBackMachine

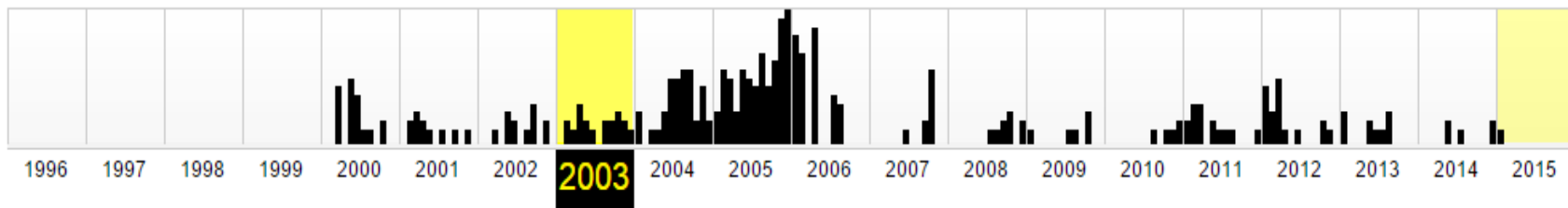
<http://www.mynet.com.tr>

BROWSE HISTORY

<http://www.mynet.com.tr>

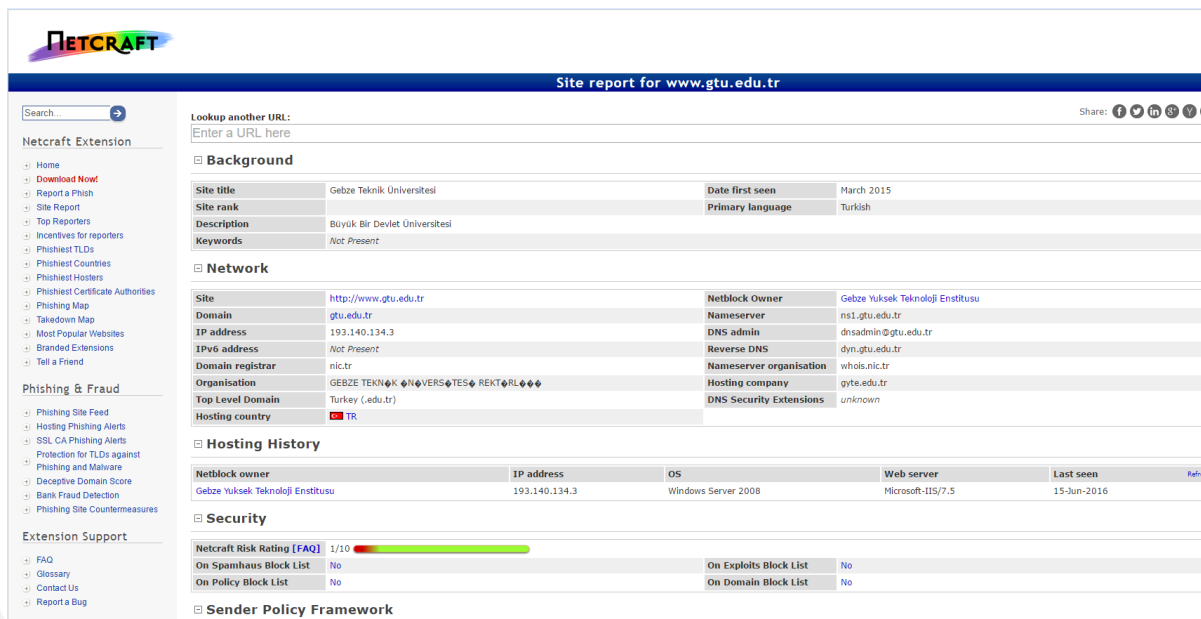
Saved **474 times** between Mart 1, 2000 and Ocak 1, 2015.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



NETCRAFT

► http://toolbar.netcraft.com/site_report



Site report for www.gtu.edu.tr

Search: →

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Lookup another URL:
Enter a URL here

Share: [f](#) [t](#) [in](#) [g+](#) [v](#)

Background

Site title	Gebze Teknik Üniversitesi	Date first seen	March 2015
Site rank		Primary language	Turkish
Description	Büyük Bir Devlet Üniversitesi		
Keywords	Not Present		

Network

Site	http://www.gtu.edu.tr	Netblock Owner	Gebze Yüksek Teknoloji Enstitüsü
Domain	gtu.edu.tr	Nameserver	ns1.gtu.edu.tr
IP address	193.140.134.3	DNS admin	dnsadmin@gtu.edu.tr
IPv6 address	Not Present	Reverse DNS	dyn.gtu.edu.tr
Domain registrar	nic.tr	Nameserver organisation	whois.nic.tr
Organisation	GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ	Hosting company	gyte.edu.tr
Top Level Domain	Turkey (.edu.tr)	DNS Security Extensions	unknown
Hosting country	TR		

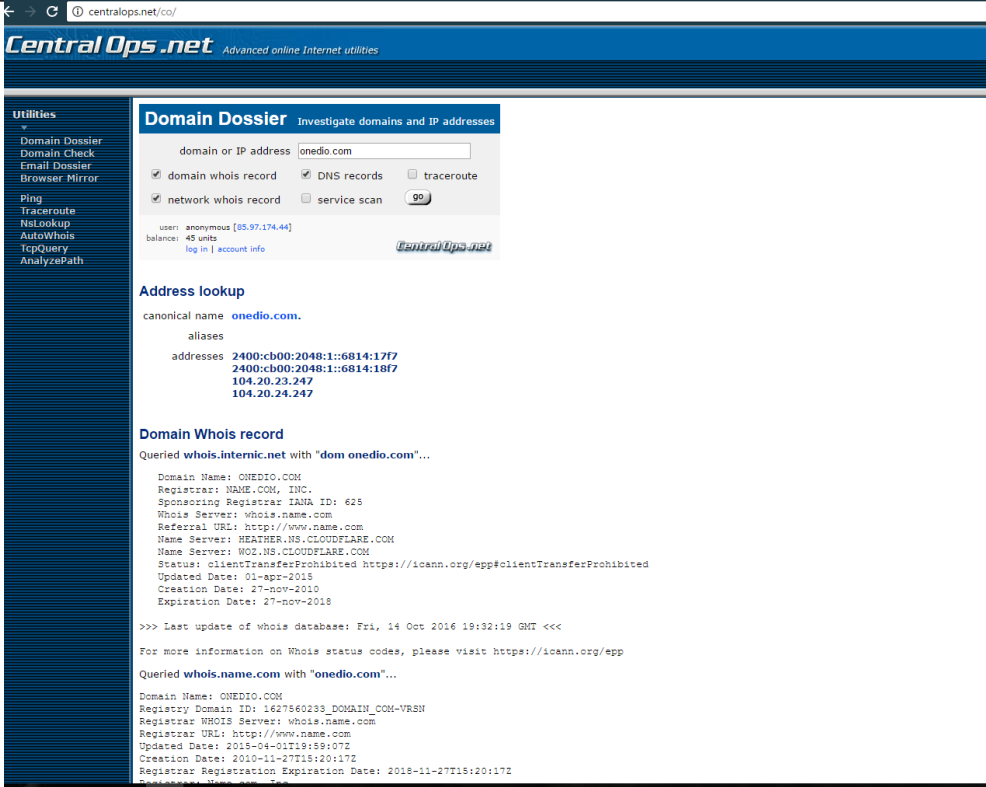
Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Ref
Gebze Yüksek Teknoloji Enstitüsü	193.140.134.3	Windows Server 2008	Microsoft-IIS/7.5	15-Jun-2016	

Security

Netcraft Risk Rating [FAQ]	1/10	On Exploits Block List	No
On Spamhaus Block List	No	On Domain Block List	No
On Policy Block List	No		

Sender Policy Framework



Utilities

Domain Dossier
 Domain Check
 Email Dossier
 Browser Mirror

Ping
 Traceroute
 Nslookup
 AutoWhois
 TcpQuery
 AnalyzePath

```

Registrar Name: ONEDIO
Reseller:
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: Onedio Bilisim
Registrant Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S
Registrant Street: ODTU Teknokent Silikon Blok No:35
Registrant City: Ankara
Registrant State/Province: Cankaya
Registrant Postal Code: 06060
Registrant Country: TR
Registrant Phone: +90.3122101048
Registrant Email: onediocom@gmail.com
Registry Admin ID:
Admin Name: Arsen Nurmagedov
Admin Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S
Admin Street: ODTU Teknokent Silikon Blok No:35
Admin City: Ankara
Admin State/Province: Cankaya
Admin Postal Code: 06060
Admin Country: TR
Admin Phone: +90.5301040767
Admin Email: arsen@onedio.com
Registry Tech ID:
Tech Name: Ekin Koc
Tech Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S
Tech Street: ODTU Teknokent Silikon Blok No:35
Tech City: Ankara
Tech State/Province: Cankaya
Tech Postal Code: 06060
Tech Country: TR
Tech Phone: +90.5327980532
Tech Email: ekin@onedio.com
Name Server: woz.ns.cloudflare.com
Name Server: heather.ns.cloudflare.com
DNSSEC: Unsigned Delegation
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1 7203101849
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2016-10-14T13:32:29-06:00 <<<
  
```

Network Whois record


Queried whois.arin.net with "n 104.20.23.247"...

```

NetRange: 104.16.0.0 - 104.31.255.255
CIDR: 104.16.0.0/12
NetName: CLOUDFLARENET
NetHandle: NET-104-16-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Assignment
OriginAS: AS13335
Organization: CloudFlare, Inc. (CLOUD14)
RegDate: 2014-03-28
Updated: 2015-10-01
  
```

IPAddress.com

onedio.com.ipaddress.com

 **IPAddress.com**
The Best IP Address Tools

[My IP](#) [IP Tools](#) [Email Tools](#) [Speed Test](#) [Articles](#)

My IP: 85.97.174.44

Search for a IP Address, Domain or Hostname


Onedio.com

Onedio Website and Webhosting Information

Advertisements

We found that the organization hosting Onedio.com is CloudFlare in San Francisco, California, United States.

A more detailed IP address report for Onedio.com is below. At the time you pulled this report, the IP of Onedio.com is 104.20.23.247 and is located in the time zone of America/Los_Angeles. The context of Onedio.com is "Onedio" and could reflect the theme of the content available on the resource. More IP details of Onedio.com are shown below along with a map location.

IP Address of Onedio is 104.20.23.247	
Hostname:	onedio.com
IP Address:	104.20.23.247
Organization:	CloudFlare
ISP/Hosting:	CloudFlare
Updated:	10/09/2016 09:06 PM
City:	San Francisco
Country:	United States 
State:	California
Postal Code:	94107
Timezone:	America/Los_Angeles
Local Time:	10/14/2016 12:41 PM

Top of the


Onedio.com Reverse IP | Websites on the same Webhosting

We found 1 hostname for IP Address 104.20.23.247


1	onedio.com
---	----------------------------

Top of the

Map location for Onedio.com | Onedio



onedio.com.ipaddress.com

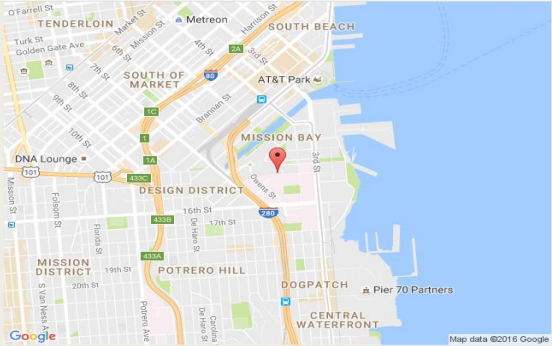
 **IPAddress.com**
The Best IP Address Tools

[My IP](#) [IP Tools](#) [Email Tools](#) [Speed Test](#) [Articles](#)

My IP: 85.97.174.44

Search for a IP Address, Domain or Hostname


Map location for Onedio.com | Onedio





Map data ©2016 Google

Top of the world

Onedio.com Whois

 **Registrar**
Name.com, Inc.

 **Whois Server**
whois.name.com

 **Referral URL**
<http://www.name.com>



Google Hacking

numrange:11111111111-999999999999
ext:pdf intitle:kimlik
inurl:www.onedio.com
filetype:txt
mail:@gtu.edu.tr

“

► **SiteDigger ve Google**

► Google 'ın arama tekniklerini kullanan ve Google 'ın ön belleğinde bulunan sayfalarda yukarıdaki bilgi toplama tekniklerini ve sayfa üzerindeki zafiyetleri raporlayan SiteDigger aracı **pasif bilgi toplamada kullanılması gereken araçlardandır.**

”

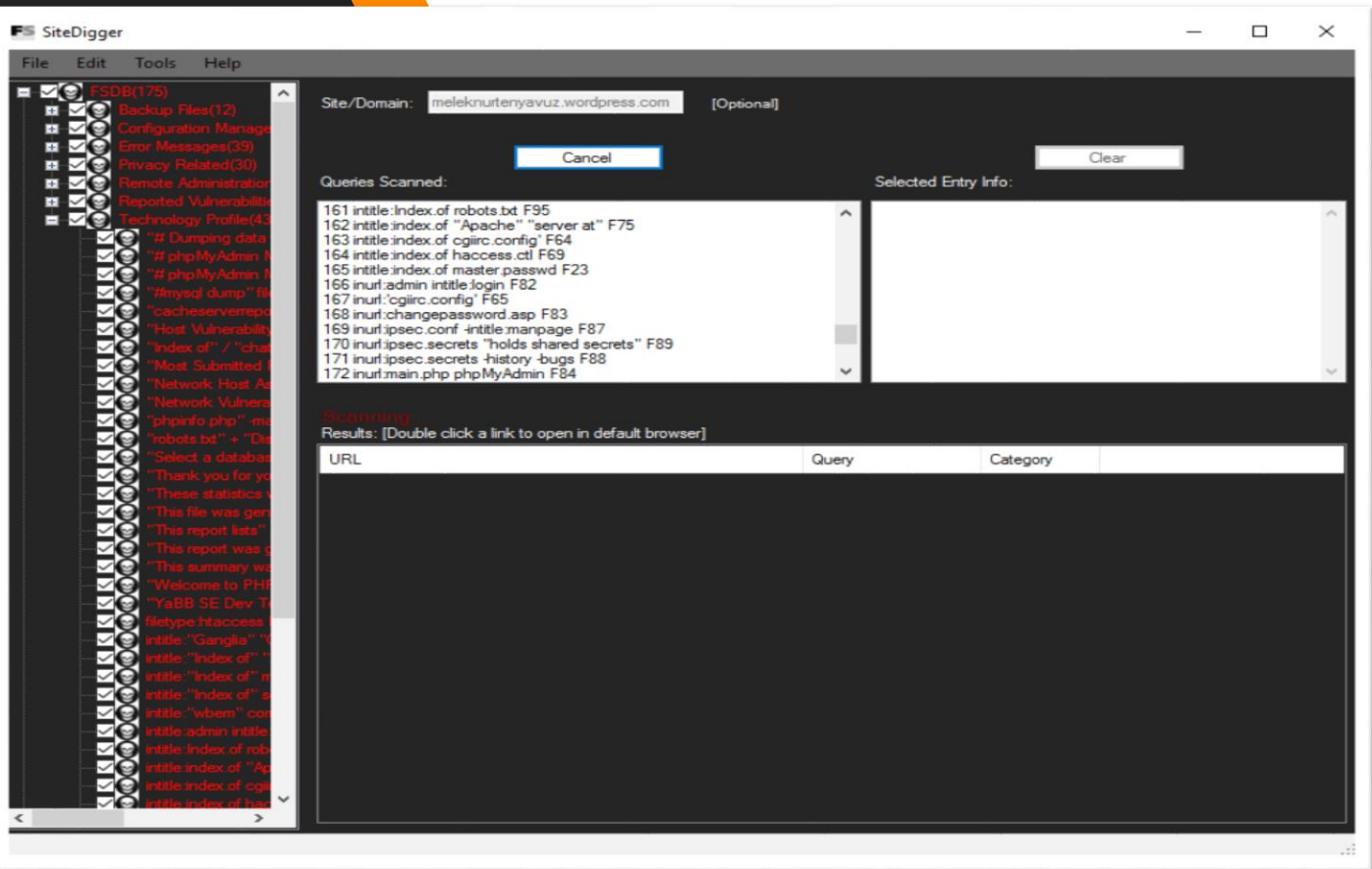
“

► Google ve Google için yazılmış pasif bilgi toplama araçlarını kullanarak **kuruma ait kritik bilgiler, mail adresleri, veritabanı dosyaları, yönetici erişimleri** ve daha bir çok bilgi elde edilebilir. Elde edilen bilgiler penetrasyon testinin diğer aşamaları için ciddi değer ve önem taşır.

► **Linkten indirebilirsiniz:**

<http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx#>

”



Nmap

Nmap, bilgisayar ağları uzmanı Gordon Lyon (Fyodor) tarafından C/C++ ve Python programlama dilleri kullanılarak geliştirilmiş bir güvenlik tarayıcısıdır. Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir.

Nmap kullanarak ağa bağlı herhangi bir **bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılımların sürüm numaraları, bilgisayarın güvenlik duvarına sahip olup olmadığı, ağ kartının üreticisinin adı gibi bilgiler** öğrenilebilmektedir.

Nmap Port Selection

Scan a single Port	<code>nmap -p 22 192.168.1.1</code>
Scan a range of ports	<code>nmap -p 1-100 192.168.1.1</code>
Scan 100 most common ports (Fast)	<code>nmap -F 192.168.1.1</code>
Scan all 65535 ports	<code>nmap -p- 192.168.1.1</code>

Nmap Port Scan types

Scan using TCP connect	<code>nmap -sT 192.168.1.1</code>
Scan using TCP SYN scan (default)	<code>nmap -sS 192.168.1.1</code>
Scan UDP ports	<code>nmap -sU -p 123,161,162 192.168.1.1</code>
Scan selected ports - ignore discovery	<code>nmap -Pn -F 192.168.1.1</code>

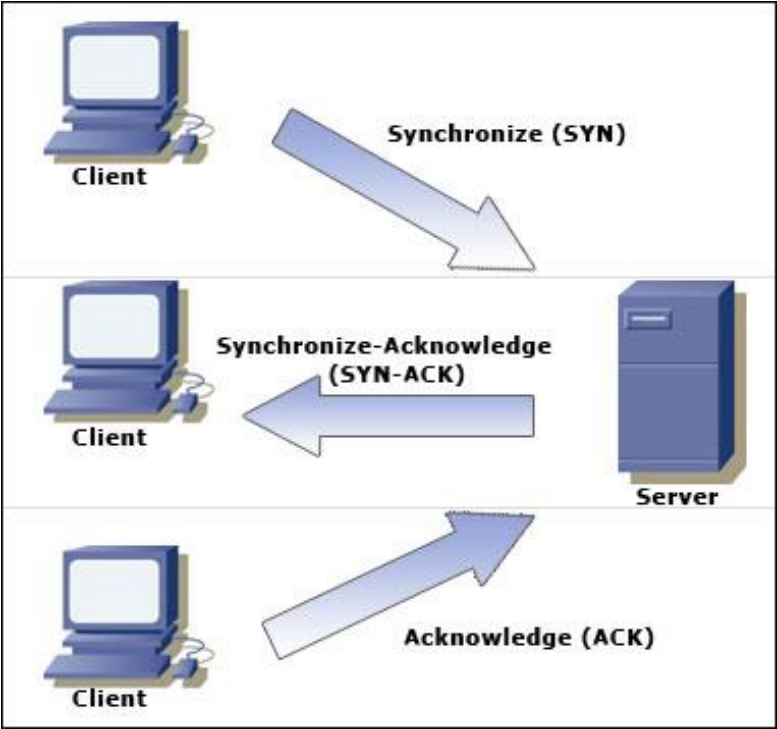
Privileged access is required to perform the default `SYN` scans. If privileges are insufficient a TCP connect scan will be used. A TCP connect requires a full TCP connection to be established and therefore is a slower scan. Ignoring discovery is often required as many firewalls or hosts will not respond to `PING`, so could be missed unless you select the `-Pn` parameter. Of course this can make scan times much longer as you could end up sending scan probes to hosts that are not there.

TCP SYN Scan

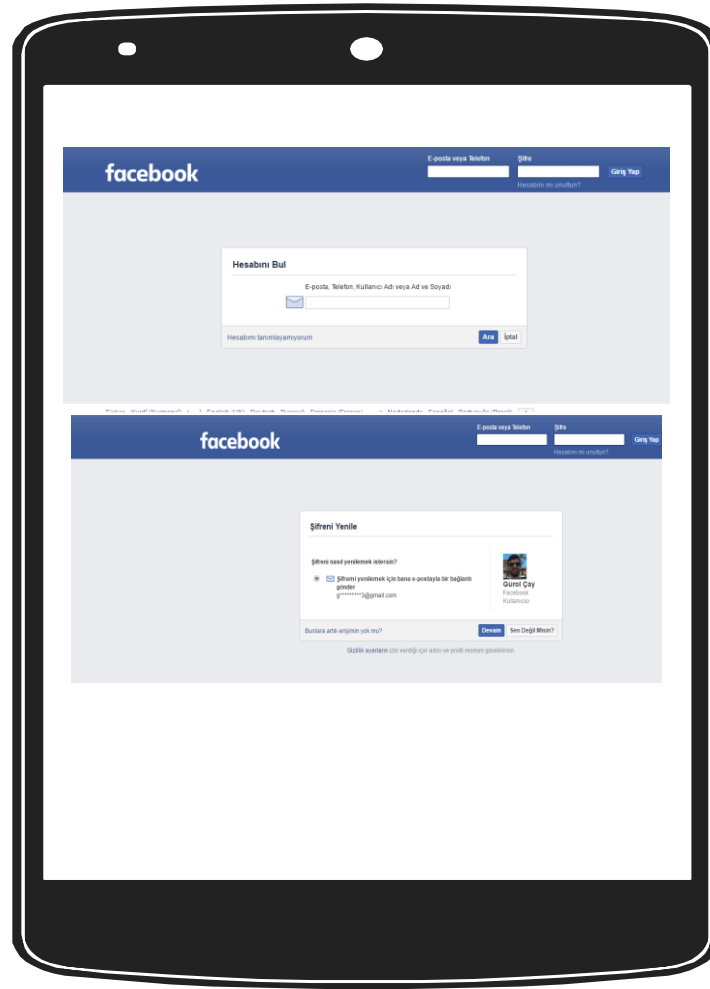
Terminal Komutu:

```
nmap -sS 192.168.109.0/24 | grep «192» | awk {'print +5'}
```

TCP SYN Scan Kaynak bilgisayarın hedef bilgisayara TCP SYN bayraklı paket gönderilerek yapılan bir tarama şeklidir. Eğer taranan portlar kapalı ise hedef makinadan kaynak makinaya RST + ACK bayraklı paket döndürülür. Eğer taranan portlar açık ise SYN + ACK bayraklı paket döndürülür. Daha sonra kaynak bilgisayarda RST bayraklı paket göndererek bağlantı kopar.



Facebook



→ C Pipl, Inc [US] | https://pipl.com/search?q=halil+öztürkçi&l=&sloc=&ln=6

pipl

Search By

First Last

+ MORE OPTIONS


☒ All Locations


☐ Turkey



☐ Istanbul


☐ United States


Results for **Halil Öztürkçi**



 **Halil Ozturkci**
Istanbul, Turkey
SPONSORED: [Contact Details](#) | [Username Report](#)
Partner at ADEO IT Consulting Services and 3 more jobs

 **Halil Öztürkci**
Istanbul, Turkey
SPONSORED: [Social Profile](#) | [Username Report](#)
Known online as halilozturkci

 **Halil Öztürkci, halilozturkci**
soundcloud.com/halilozturkci
 Member's Profile - SoundCloud

 **Halil Öztürkci**
Associated with Uğur Güngör
SPONSORED: [Vital Records](#) | [Contact Details](#)

 **Halil Öztürkci**
Istanbul, Turkey
SPONSORED: [Contact Details](#)

 **Halil Öztürkci, halil.ozturkci**
facebook.com/people/_/100003080037125
 Personal Web Profile - Facebook

<https://www.shodan.io>

Shodan, çevrimiçi bulunan belirli cihazları ve cihaz türlerini bulmak için kullanılan bir arama motorudur. En popüler aramalar web kamerası, linksys, cisco, netgear, SCADA vb. Şeyler içindir.

Shodan

Developers

Book

View All...

SHODAN

default password country:tr

Q

Explore

Downloads

Reports

Enterprise Access

Contact Us

Exploits

Maps

Share Search

Create Report

TOP COUNTRIES

Turkey	80
--------	----

TOP CITIES

Istanbul	10
Ankara	6
Kocaeli	3
Sanayi	2
Mugla	1

TOP SERVICES

Telnet	48
HTTP	13
8081	6
8880	2
GlassFish Server	2

TOP ORGANIZATIONS

Turk Telekom	40
Vodafone Net Iletisim Hizmetleri A.s	12
Telcom Iletisim Hizmetleri A.s.	4
TurkNet Iletisim Hizmetleri A.S	3
Vodafone Turkey 3G IP Pool	2

TOP PRODUCTS

nginx	7
TP-LINK WR841N WAP http config	1
TP-LINK WR740N WAP http config	1
Microsoft IIS httpd	1

Total results: 79

213.254.131.44

Telcom Iletisim Hizmetleri A.s.

Added on 2016-11-20 10:55:23 GMT

Turkey

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Nov 2016 10:55:22 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Set-Cookie: iMSCP_Session=4ucncohpigkb53v2dkbh48scd0; path=

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Cont...

46.197.117.21

mail.bioartmed.com

Turksat Uydu-Net Internet

Added on 2016-11-20 07:14:20 GMT

Turkey

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Nov 2016 07:14:06 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Last-Modified: Sun, 20 Nov 2016 07:14:05 GMT

X-Frame-Options: SAMEORIGIN

Set-Cookie: PHPSESSID=7h381j0utqmtffv3co32ivc1tph2ojms; path=...

78.186.175.34

78.186.175.34.static.ttnet.com.tr

Turk Telekom

Added on 2016-11-20 07:13:45 GMT

Turkey, Kocaeli

Details

<HTML>

<HEAD>

<META http-equiv="Pragma" content="no-cache">

<META http-equiv="Content-Type" content="text/html; charset=utf-8">

<title>Tenda ADSL2/2+ Modem with Wireless Router</title>

<script language="javascript" src="translate.js"></script>

<SCRIPT language=JavaScript>

TranslateDictio...

IoT Hack

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

Friday, October 21, 2016 Mohit Kumar

90 9.8K 5188 669 157 6112



A massive Distributed Denial of Service (DDoS) [attack against Dyn](#), a major domain name system (DNS) provider, broke large portions of the Internet on Friday, causing a significant outage to a ton of websites and services, including Twitter, GitHub, PayPal, Amazon, Reddit, Netflix, and Spotify.

But how the attack happened? What's the cause behind the attack?

Exact details of the attack remain vague, but Dyn reported a huge army of hijacked internet-connected devices could be responsible for the massive attack.

Yes, the same method recently employed by hackers to carry out [record-breaking DDoS attack](#) of over 1 Tbps against France-based hosting provider OVH.

Teşekkürler...

Melek Nurten YAVUZ