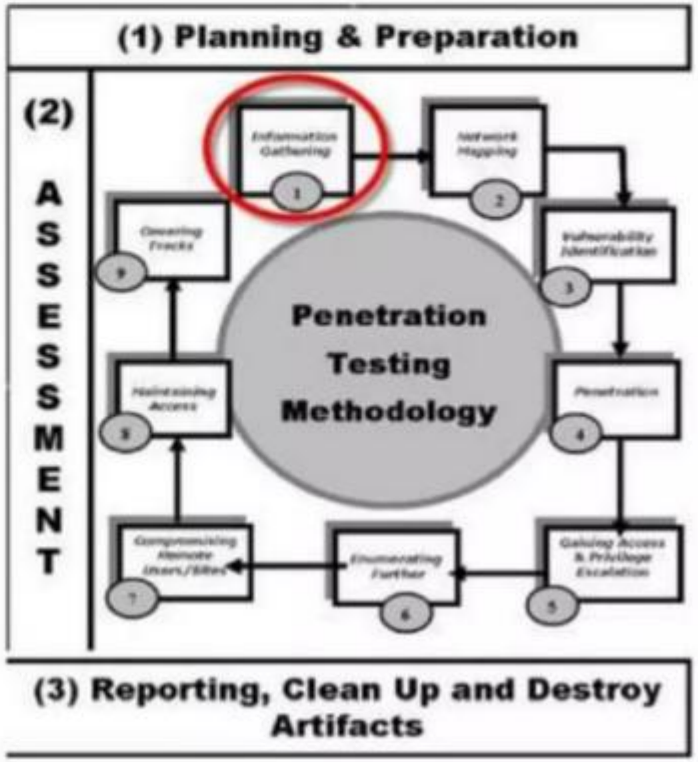
Siber Saldırılar

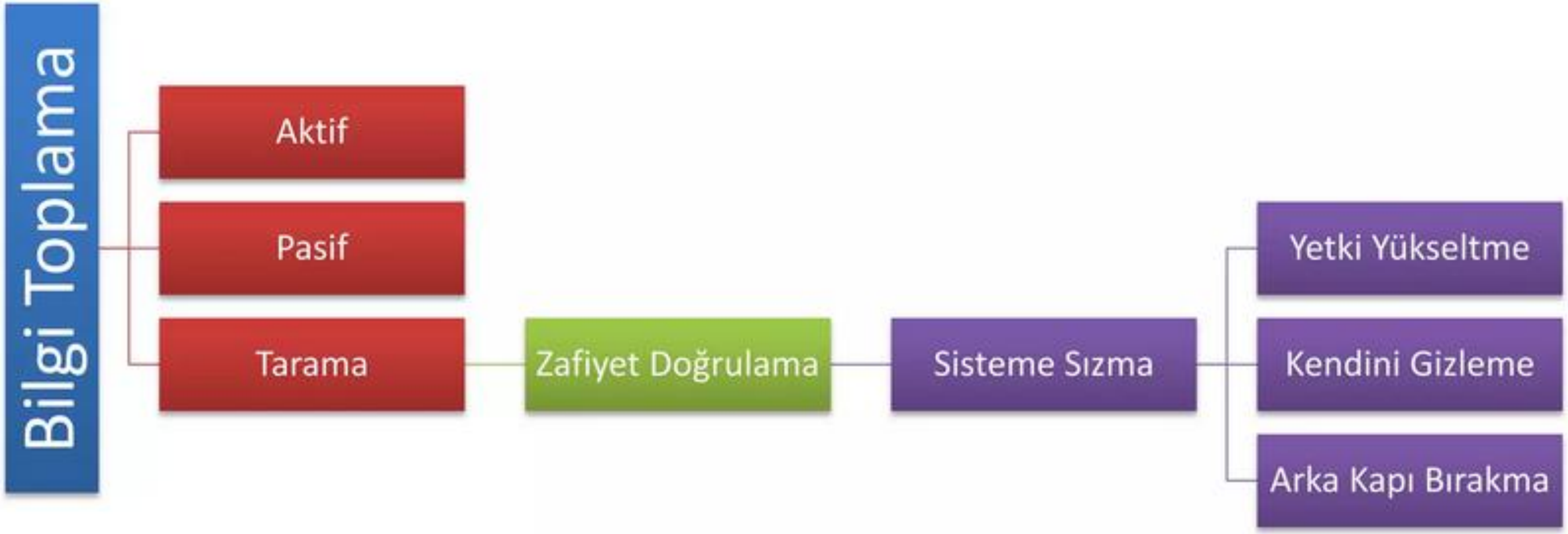
2025

Saldırı Aşamaları

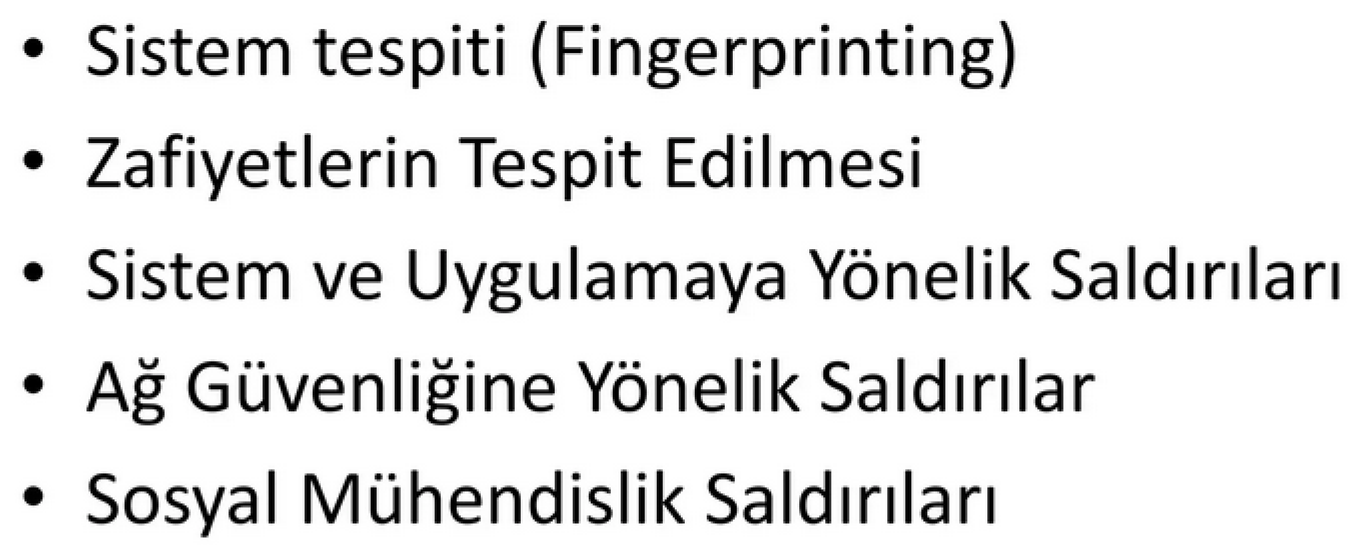
- **Bilgi Toplama**(Veri)
- Hazırlık(Açıklık Tespiti)
- Saldırı(Açıklık Sömürme)
- Erişim
- Yetki Yükseltme
- İzleri Silmek


(1) Planning & Preparation
(2)
ASSESSMENT
Penetration Testing Methodology
Information Gathering
1
Network Mapping
2
Vulnerability Identification
3
Penetration
4
Gaining Access & Privilege Escalation
5
Enumerating Further
6
Compromising Remote Users/Sites
7
Maintaining Access
8
Covering Tracks
9
(3) Reporting, Clean Up and Destroy Artifacts

Saldırı Metadolojisi

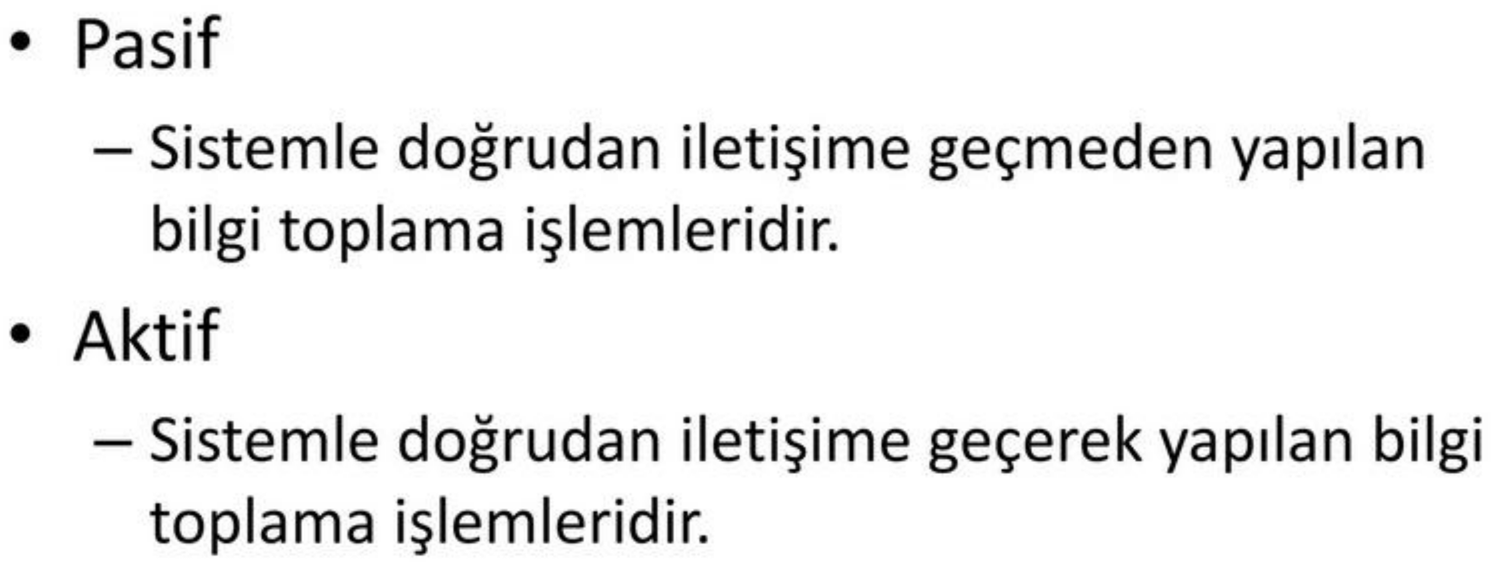


Saldırı Yöntem ve Çeşitleri



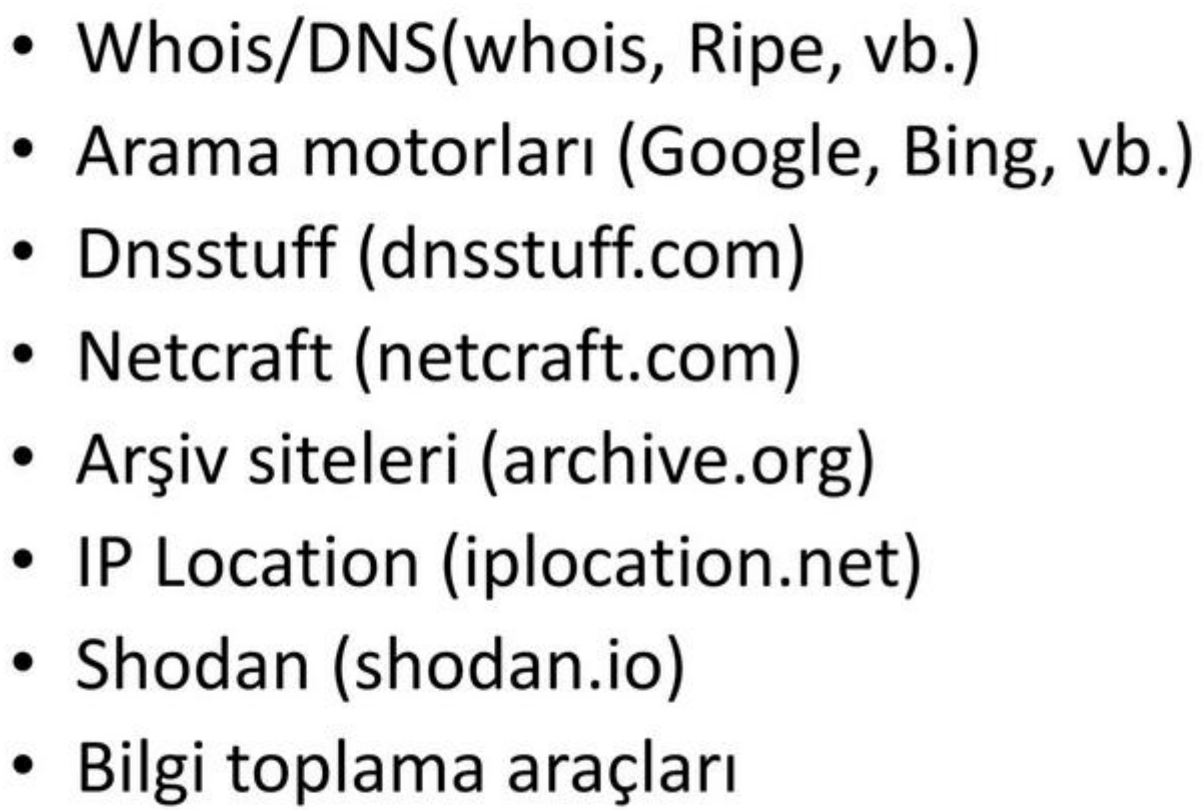
- Sistem tespiti (Fingerprinting)
- Zafiyetlerin Tespit Edilmesi
- Sistem ve Uygulamaya Yönelik Saldırıları
- Ağ Güvenliğine Yönelik Saldırılar
- Sosyal Mühendislik Saldırıları

Bilgi Toplama Yöntemleri



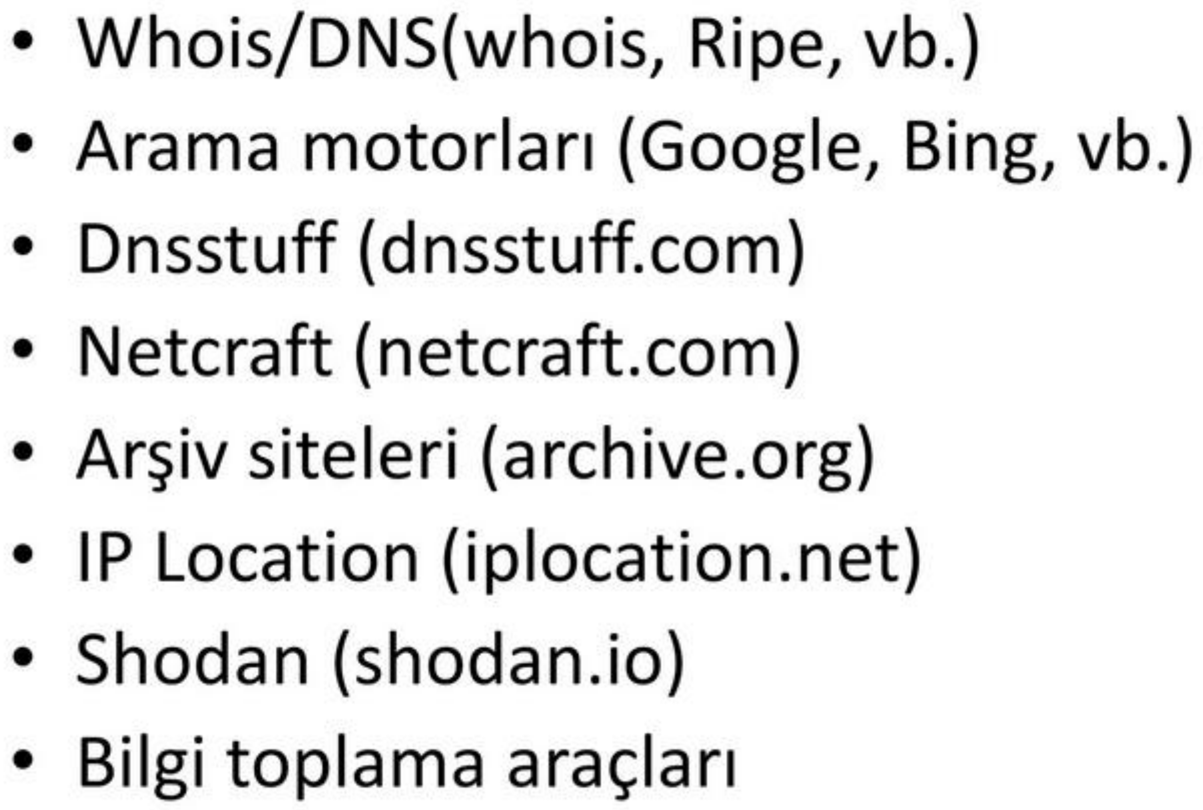
- Pasif
  - – Sistemle doğrudan iletişime geçmeden yapılan bilgi toplama işlemleridir.
- Aktif
  - – Sistemle doğrudan iletişime geçerek yapılan bilgi toplama işlemleridir.

Pasif Bilgi Toplama Araçları



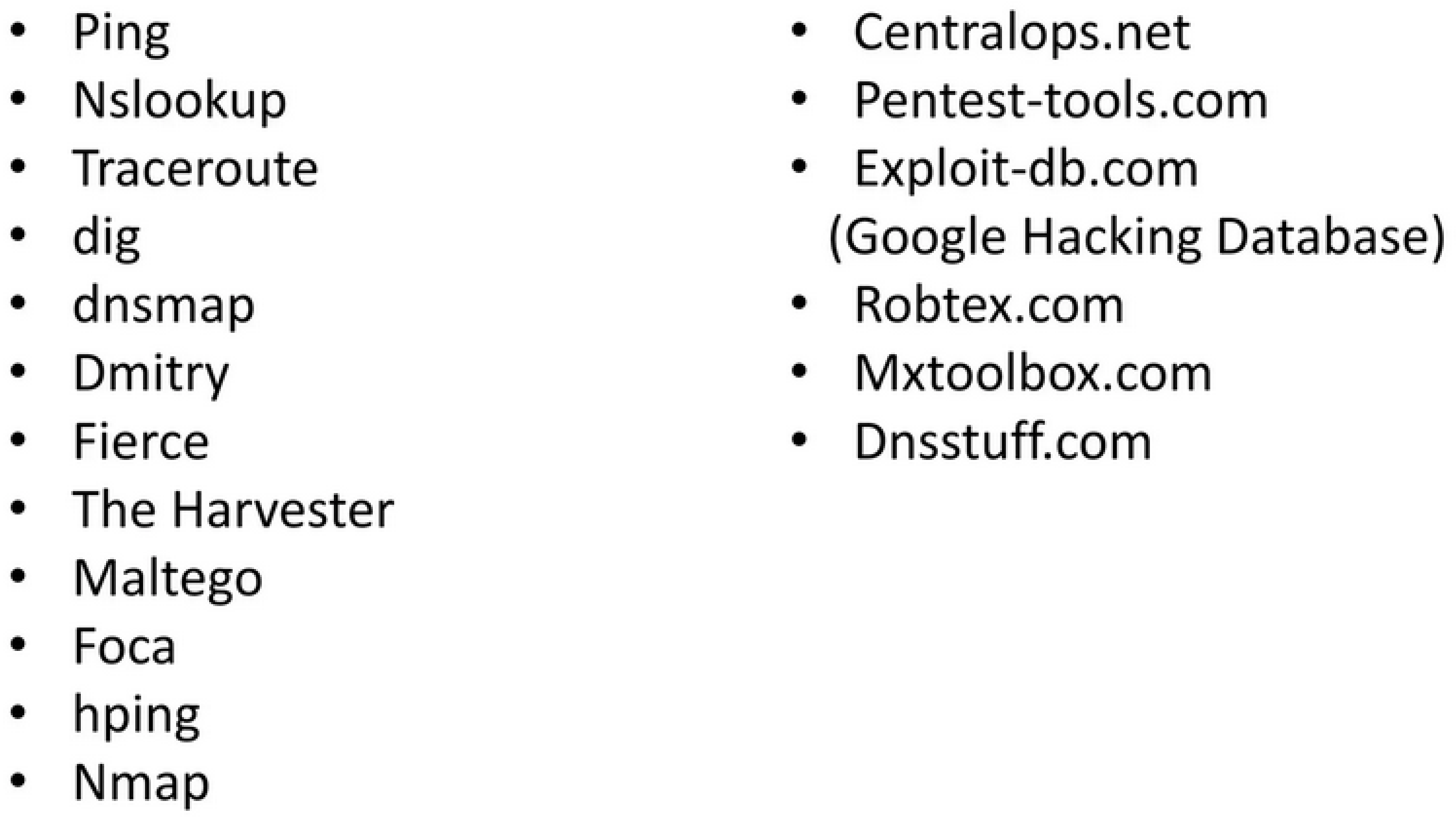
- Whois/DNS(whois, Ripe, vb.)
- Arama motorları (Google, Bing, vb.)
- Dnsstuff (dnsstuff.com)
- Netcraft (netcraft.com)
- Arşiv siteleri (archive.org)
- IP Location (iplocation.net)
- Shodan (shodan.io)
- Bilgi toplama araçları

Pasif Bilgi Toplama Araçları



- Whois/DNS(whois, Ripe, vb.)
- Arama motorları (Google, Bing, vb.)
- Dnsstuff (dnsstuff.com)
- Netcraft (netcraft.com)
- Arşiv siteleri (archive.org)
- IP Location (iplocation.net)
- Shodan (shodan.io)
- Bilgi toplama araçları

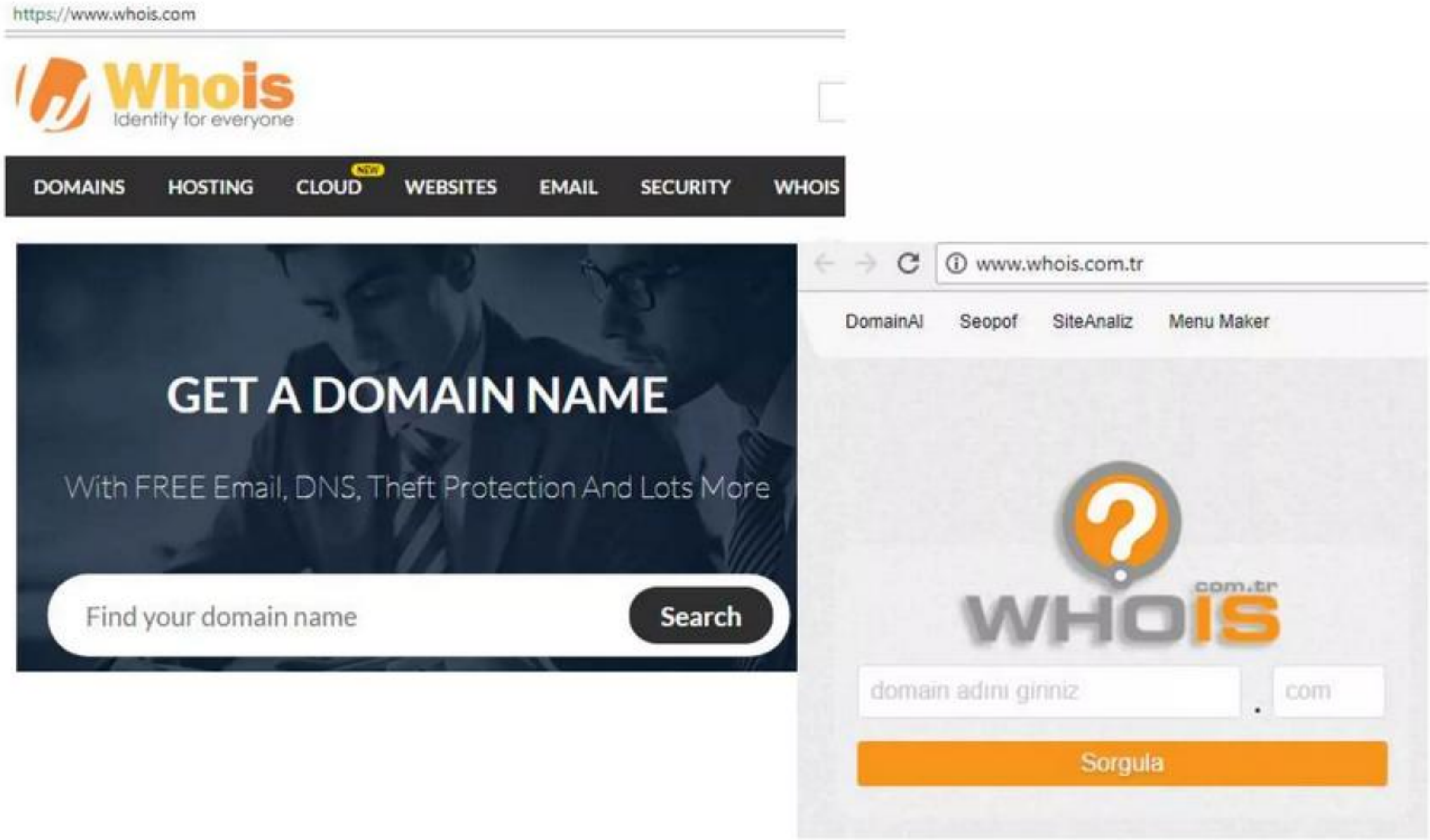
Aktif Bilgi Toplama Araçları



- Ping
- Nslookup
- Traceroute
- dig
- dnsmap
- Dmitry
- Fierce
- The Harvester
- Maltego
- Foca
- hping
- Nmap

- Centralops.net
- Pentest-tools.com
- Exploit-db.com
  (Google Hacking Database)
- Robtex.com
- Mxtoolbox.com
- Dnsstuff.com

whois.com / whois.com.tr



https://www.whois.com

Whois
Identity for everyone

DOMAINS HOSTING CLOUD NEW WEBSITES EMAIL SECURITY WHOIS

GET A DOMAIN NAME

With FREE Email, DNS, Theft Protection And Lots More

Find your domain name

Search

www.whois.com.tr

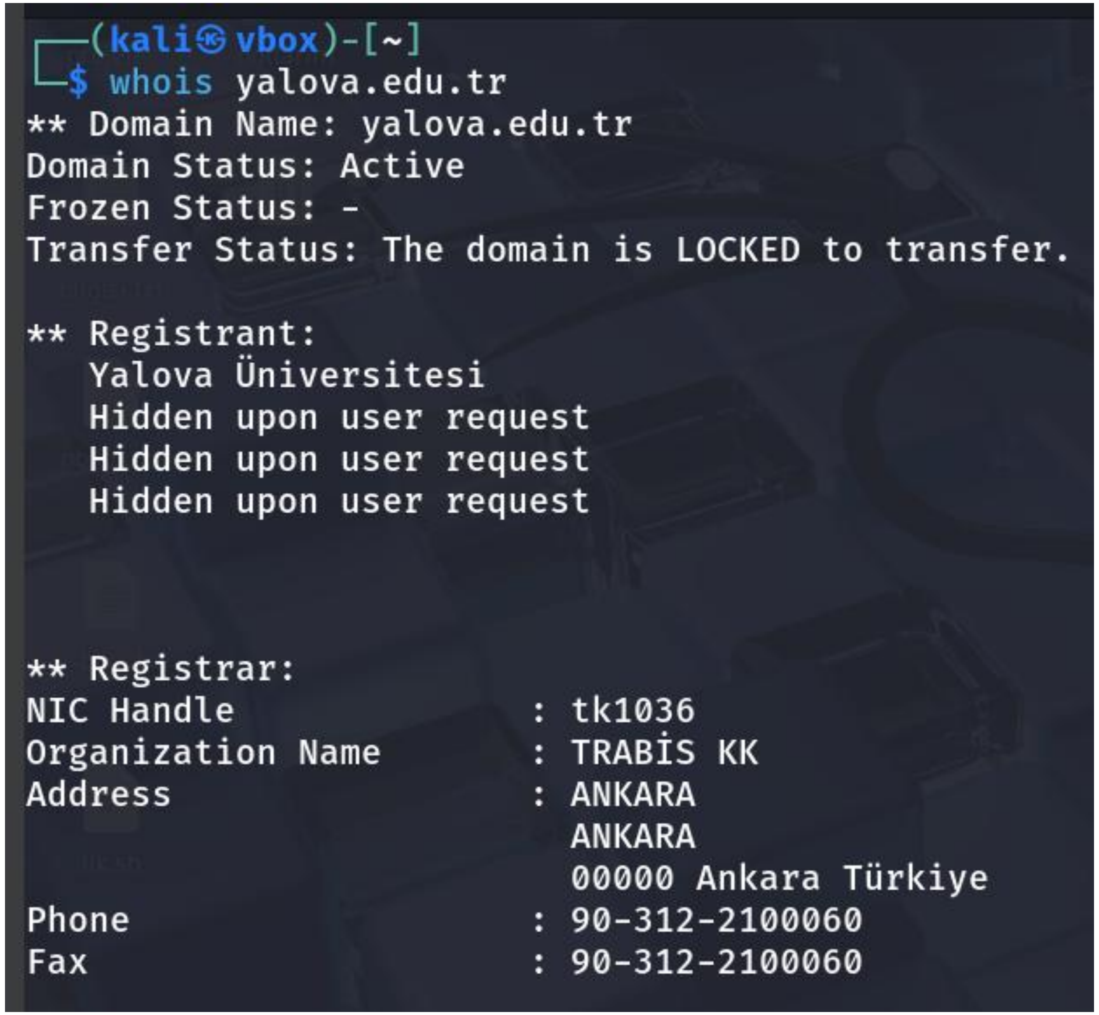
DomainAl Seopof SiteAnaliz Menu Maker

WHOIS com.tr

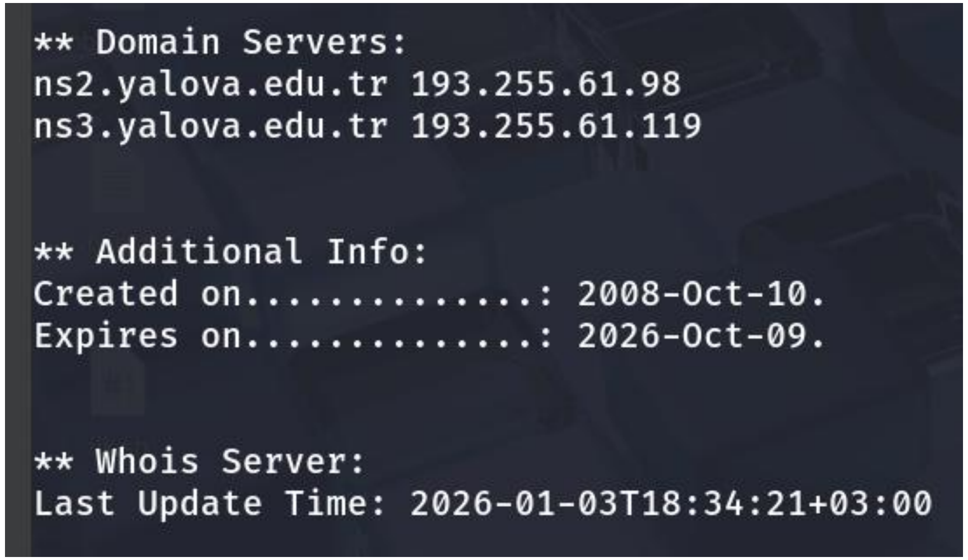
domain adını giriniz . com

Sorgula

whois

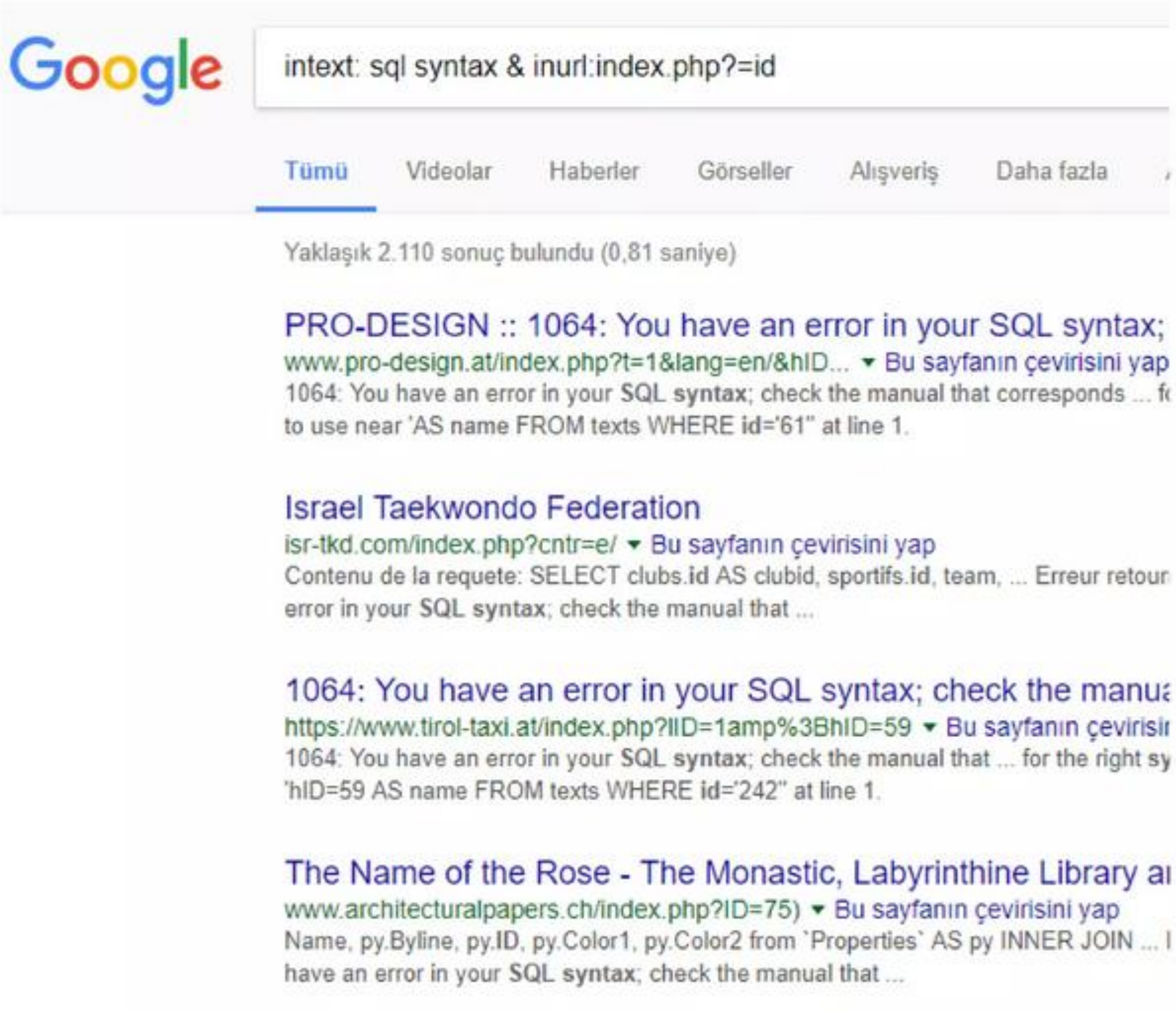


```
┌──(kali㉿vbox)-[~]
└─$ whois yalova.edu.tr
** Domain Name: yalova.edu.tr
Domain Status: Active
Frozen Status: -
Transfer Status: The domain is LOCKED to transfer.

** Registrant:
   Yalova Üniversitesi
   Hidden upon user request
   Hidden upon user request
   Hidden upon user request



** Registrar:
NIC Handle               : tk1036
Organization Name        : TRABİS KK
Address                  : ANKARA
                           ANKARA
                           00000 Ankara Türkiye
Phone                    : 90-312-2100060
Fax                      : 90-312-2100060
```



```
** Domain Servers:
ns2.yalova.edu.tr 193.255.61.98
ns3.yalova.edu.tr 193.255.61.119


** Additional Info:
Created on..............: 2008-Oct-10.
Expires on..............: 2026-Oct-09.


** Whois Server:
Last Update Time: 2026-01-03T18:34:21+03:00
```

google



intext: sql syntax & inurl:index.php?=id

Yaklaşık 2.110 sonuç bulundu (0,81 saniye)

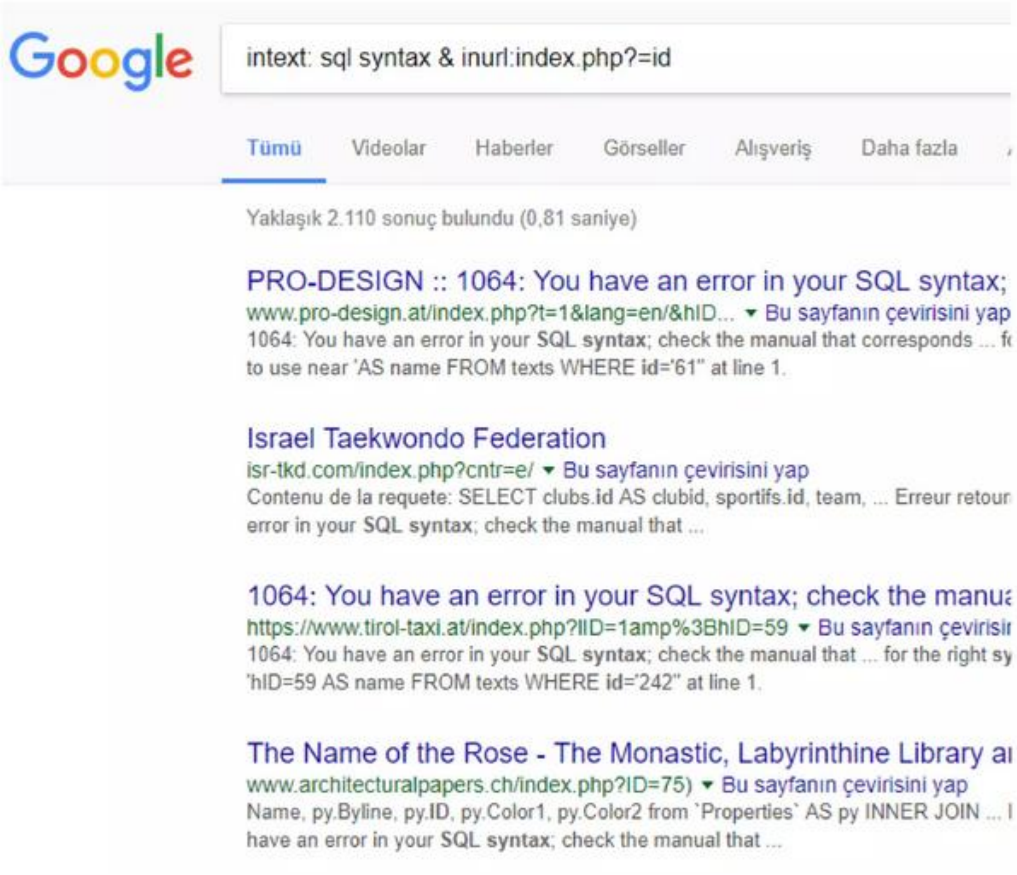
PRO-DESIGN :: 1064: You have an error in your SQL syntax;
www.pro-design.at/index.php?t=1&lang=en/&hID... ▾ Bu sayfanın çevirisini yap
1064: You have an error in your **SQL syntax**; check the manual that corresponds ... f
to use near 'AS name FROM texts WHERE **id**='61'' at line 1.

Israel Taekwondo Federation
isr-tkd.com/index.php?cntr=e/ ▾ Bu sayfanın çevirisini yap
Contenu de la requete: SELECT clubs.**id** AS clubid, sportifs.**id**, team, ... Erreur retour
error in your **SQL syntax**; check the manual that ...

1064: You have an error in your SQL syntax; check the manua
https://www.tirol-taxi.at/index.php?lID=1amp%3BhID=59 ▾ Bu sayfanın çevirisi
1064: You have an error in your **SQL syntax**; check the manual that ... for the right sy
'hID=59 AS name FROM texts WHERE **id**='242'' at line 1.

The Name of the Rose - The Monastic, Labyrinthine Library a
www.architecturalpapers.ch/index.php?ID=75) ▾ Bu sayfanın çevirisini yap
Name, py.Byline, py.**ID**, py.Color1, py.Color2 from `Properties` AS py INNER JOIN ... I
have an error in your **SQL syntax**; check the manual that ...

google



intext: sql syntax & inurl:index.php?=id

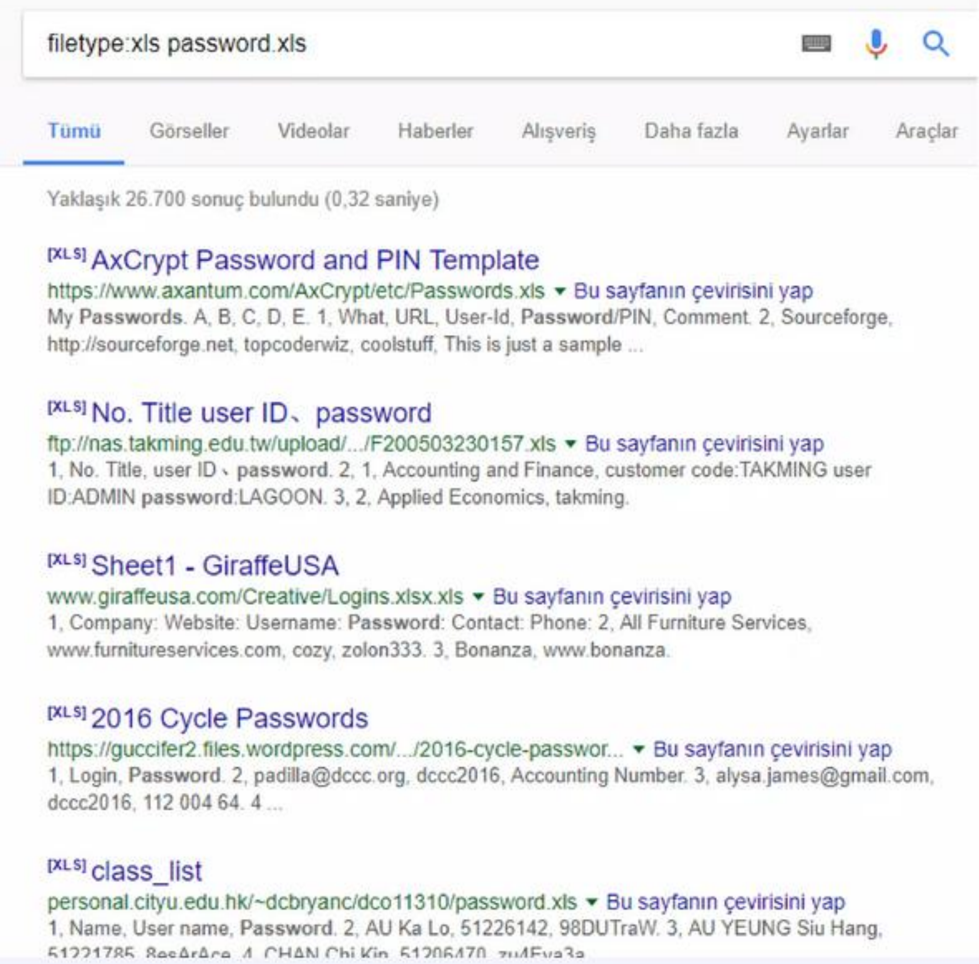
Yaklaşık 2.110 sonuç bulundu (0,81 saniye)

PRO-DESIGN :: 1064: You have an error in your SQL syntax;
www.pro-design.at/index.php?t=1&lang=en/&hID... ▾ Bu sayfanın çevirisini yap
1064: You have an error in your **SQL syntax**; check the manual that corresponds ... fo
to use near 'AS name FROM texts WHERE **id**='61'' at line 1.

Israel Taekwondo Federation
isr-tkd.com/index.php?cntr=e/ ▾ Bu sayfanın çevirisini yap
Contenu de la requete: SELECT clubs.**id** AS clubid, sportifs.**id**, team, ... Erreur retour
error in your **SQL syntax**; check the manual that ...

1064: You have an error in your SQL syntax; check the manua
https://www.tirol-taxi.at/index.php?lID=1amp%3BhID=59 ▾ Bu sayfanın çevirisi
1064: You have an error in your **SQL syntax**; check the manual that ... for the right sy
'hID=59 AS name FROM texts WHERE **id**='242'' at line 1.

The Name of the Rose - The Monastic, Labyrinthine Library ar
www.architecturalpapers.ch/index.php?ID=75) ▾ Bu sayfanın çevirisini yap
Name, py.Byline, py.**ID**, py.Color1, py.Color2 from `Properties` AS py INNER JOIN ... I
have an error in your **SQL syntax**; check the manual that ...



filetype:xls password.xls

Yaklaşık 26.700 sonuç bulundu (0,32 saniye)

[XLS] AxCrypt Password and PIN Template
https://www.axantum.com/AxCrypt/etc/Passwords.xls ▾ Bu sayfanın çevirisini yap
My **Passwords**. A, B, C, D, E. 1, What, URL, User-Id, **Password**/PIN, Comment. 2, Sourceforge, http://sourceforge.net, topcoderwiz, coolstuff, This is just a sample ...

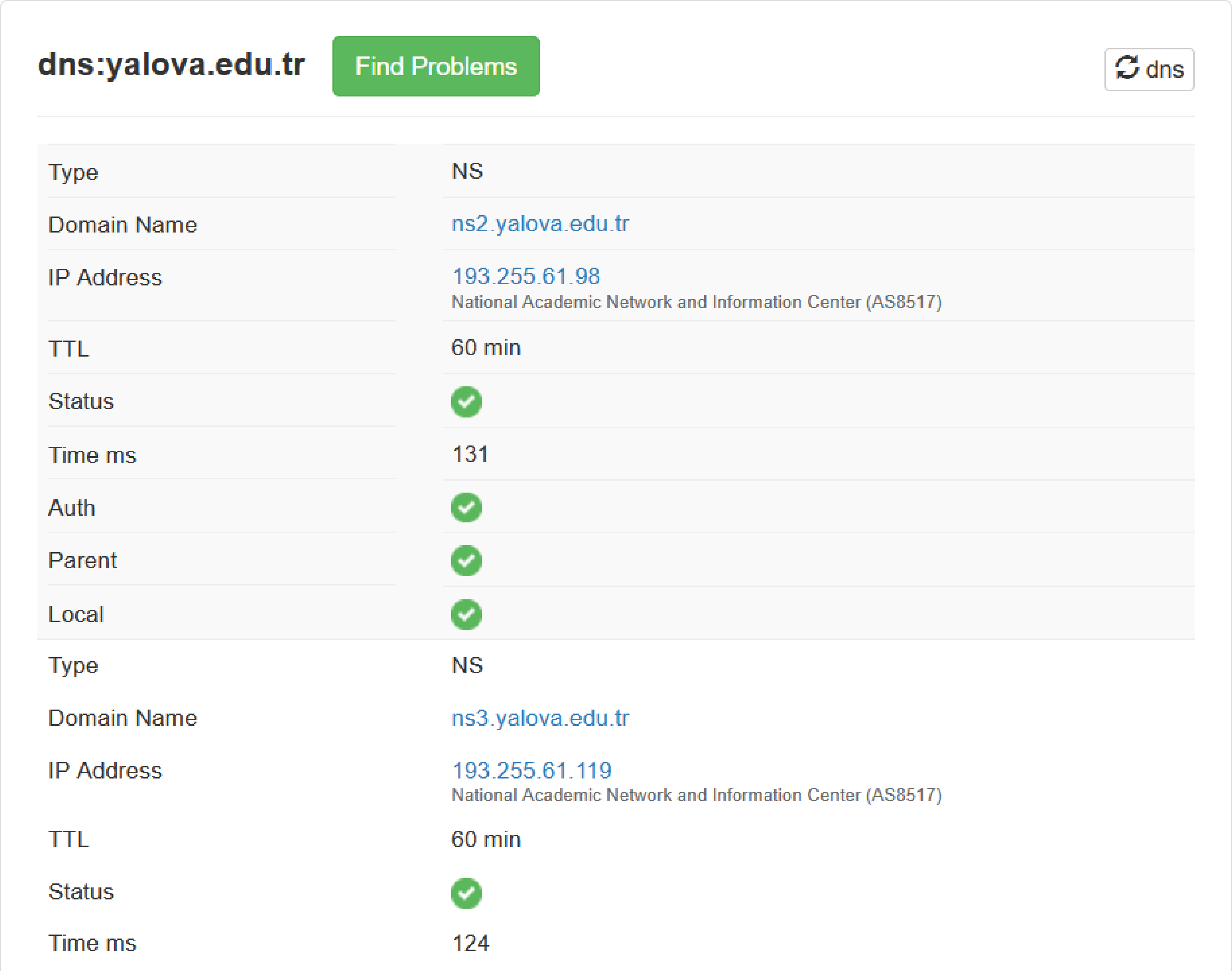
[XLS] No. Title user ID、password
ftp://nas.takming.edu.tw/upload/.../F200503230157.xls ▾ Bu sayfanın çevirisini yap
1, No. Title, user ID、**password**. 2, 1, Accounting and Finance, customer code:TAKMING user ID:ADMIN **password**:LAGOON. 3, 2, Applied Economics, takming.

[XLS] Sheet1 - GiraffeUSA
www.giraffeusa.com/Creative/Logins.xlsx.xls ▾ Bu sayfanın çevirisini yap
1, Company: Website: Username: **Password**: Contact: Phone: 2, All Furniture Services, www.furnitureservices.com, cozy, zolon333. 3, Bonanza, www.bonanza.

[XLS] 2016 Cycle Passwords
https://guccifer2.files.wordpress.com/.../2016-cycle-passwor... ▾ Bu sayfanın çevirisini yap
1, Login, **Password**. 2, padilla@dccc.org, dccc2016, Accounting Number. 3, alysa.james@gmail.com, dccc2016, 112 004 64. 4 ...

[XLS] class_list
personal.cityu.edu.hk/~dcbryanc/dco11310/password.xls ▾ Bu sayfanın çevirisini yap
1, Name, User name, **Password**. 2, AU Ka Lo, 51226142, 98DUTraW. 3, AU YEUNG Siu Hang, 51221785, 8esArAce. 4, CHAN Chi Kin, 51206470, zu4Eva3a

DNS Report

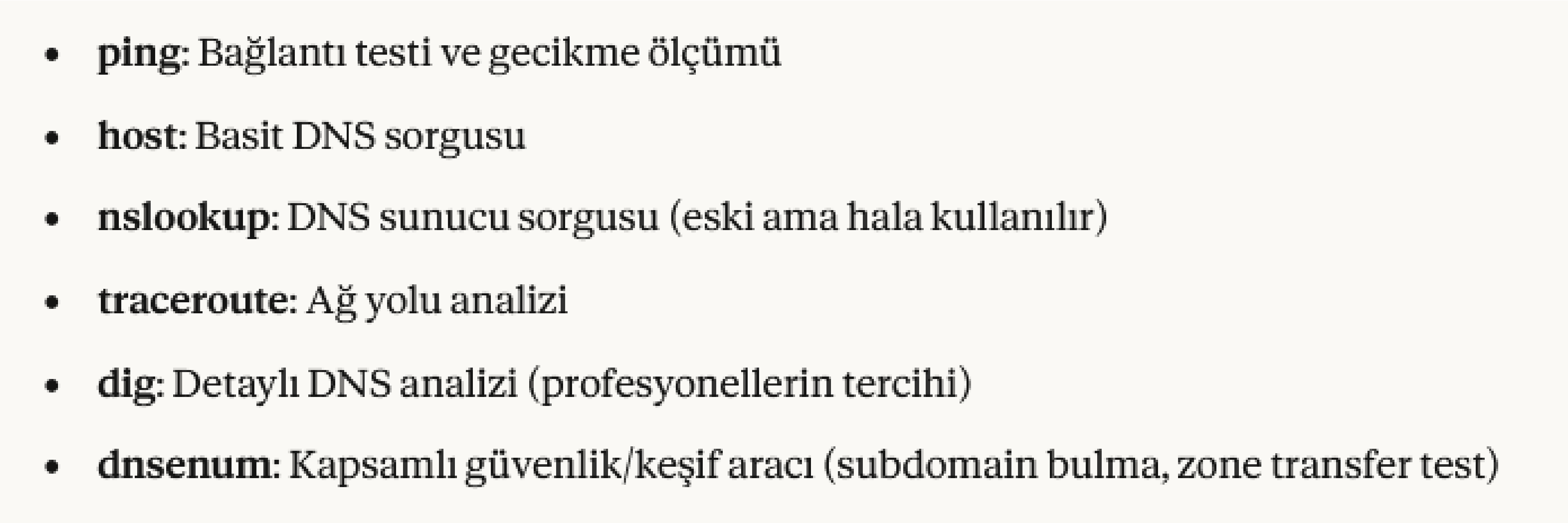


dns:yalova.edu.tr

Type	NS
Domain Name	ns2.yalova.edu.tr
IP Address	193.255.61.98 National Academic Network and Information Center (AS8517)
TTL	60 min
Status	✓
Time ms	131
Auth	✓
Parent	✓
Local	✓
Type	NS
Domain Name	ns3.yalova.edu.tr
IP Address	193.255.61.119 National Academic Network and Information Center (AS8517)
TTL	60 min
Status	✓
Time ms	124

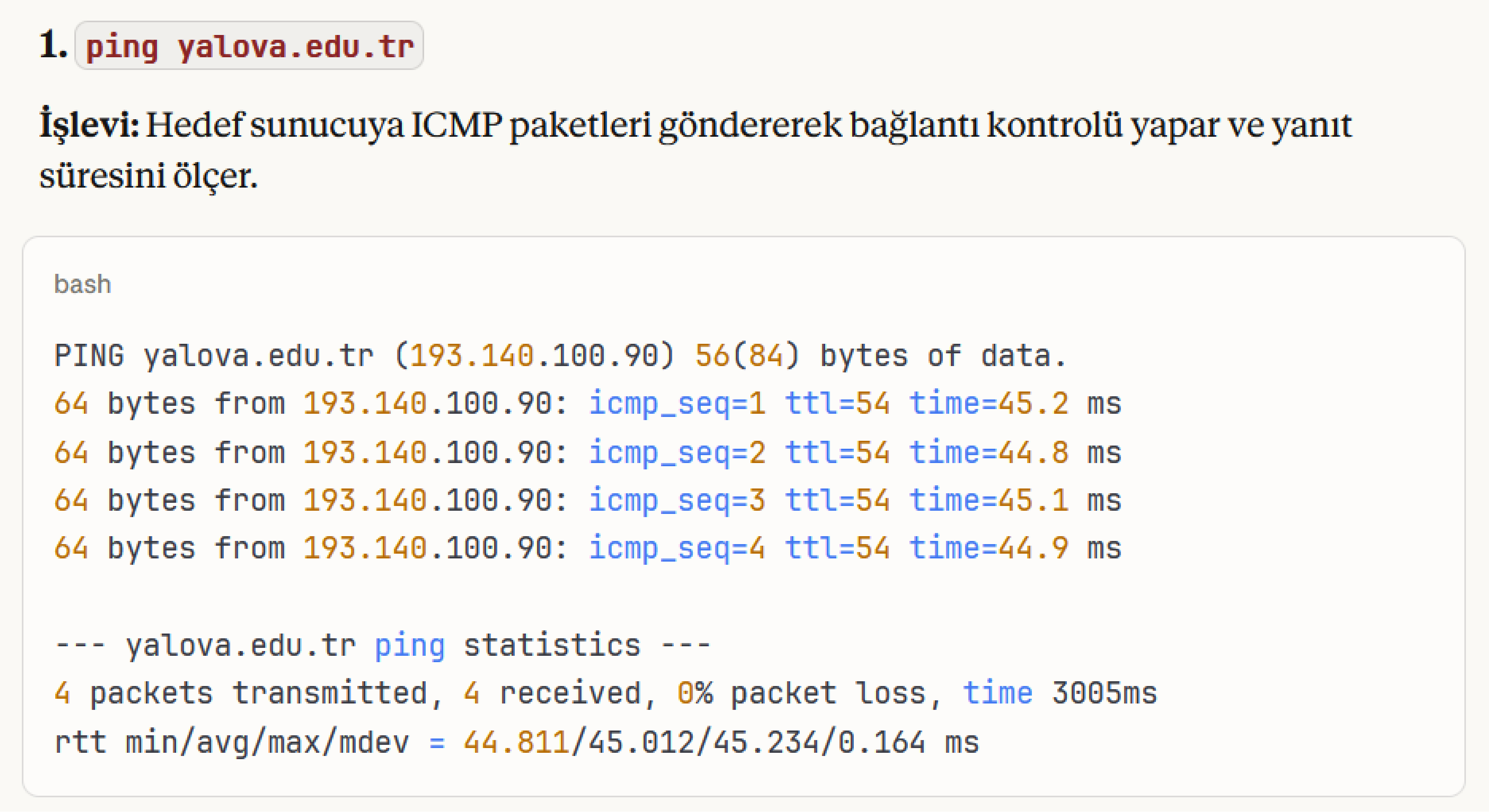
Konsol Komutları

Konsol Komutları



- **ping**: Bağlantı testi ve gecikme ölçümü
- **host**: Basit DNS sorgusu
- **nslookup**: DNS sunucu sorgusu (eski ama hala kullanılır)
- **traceroute**: Ağ yolu analizi
- **dig**: Detaylı DNS analizi (profesyonellerin tercihi)
- **dnsenum**: Kapsamlı güvenlik/keşif aracı (subdomain bulma, zone transfer test)

Konsol Komutları



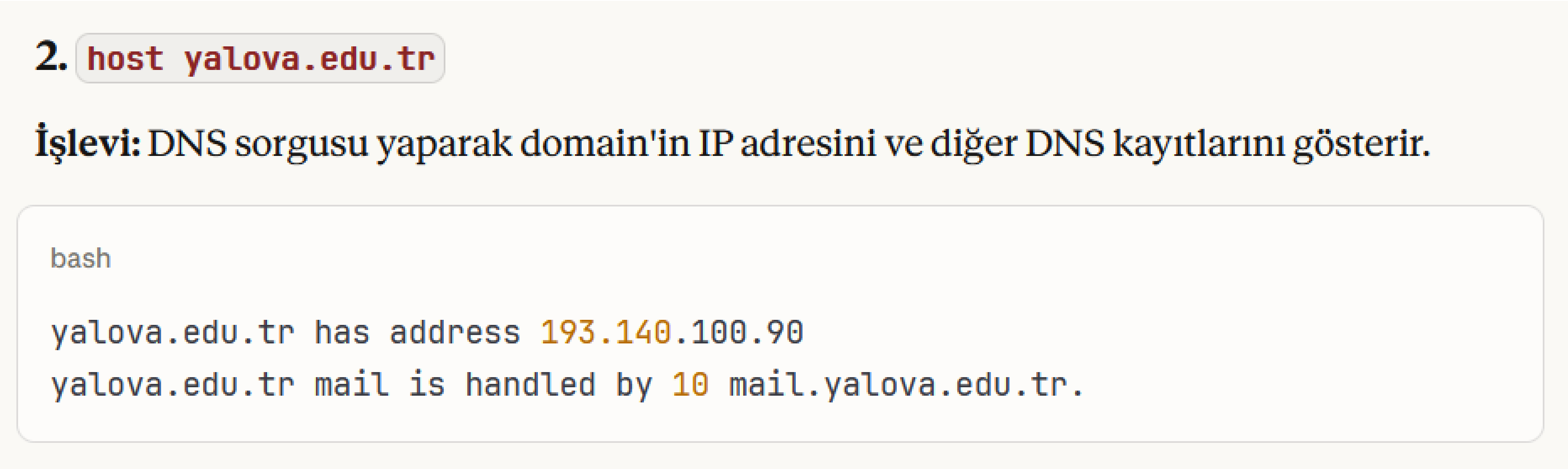
1. `ping yalova.edu.tr`

İşlevi: Hedef sunucuya ICMP paketleri göndererek bağlantı kontrolü yapar ve yanıt süresini ölçer.

bash

```bash
PING yalova.edu.tr (193.140.100.90) 56(84) bytes of data.
64 bytes from 193.140.100.90: icmp_seq=1 ttl=54 time=45.2 ms
64 bytes from 193.140.100.90: icmp_seq=2 ttl=54 time=44.8 ms
64 bytes from 193.140.100.90: icmp_seq=3 ttl=54 time=45.1 ms
64 bytes from 193.140.100.90: icmp_seq=4 ttl=54 time=44.9 ms

--- yalova.edu.tr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 44.811/45.012/45.234/0.164 ms
```

Konsol Komutları



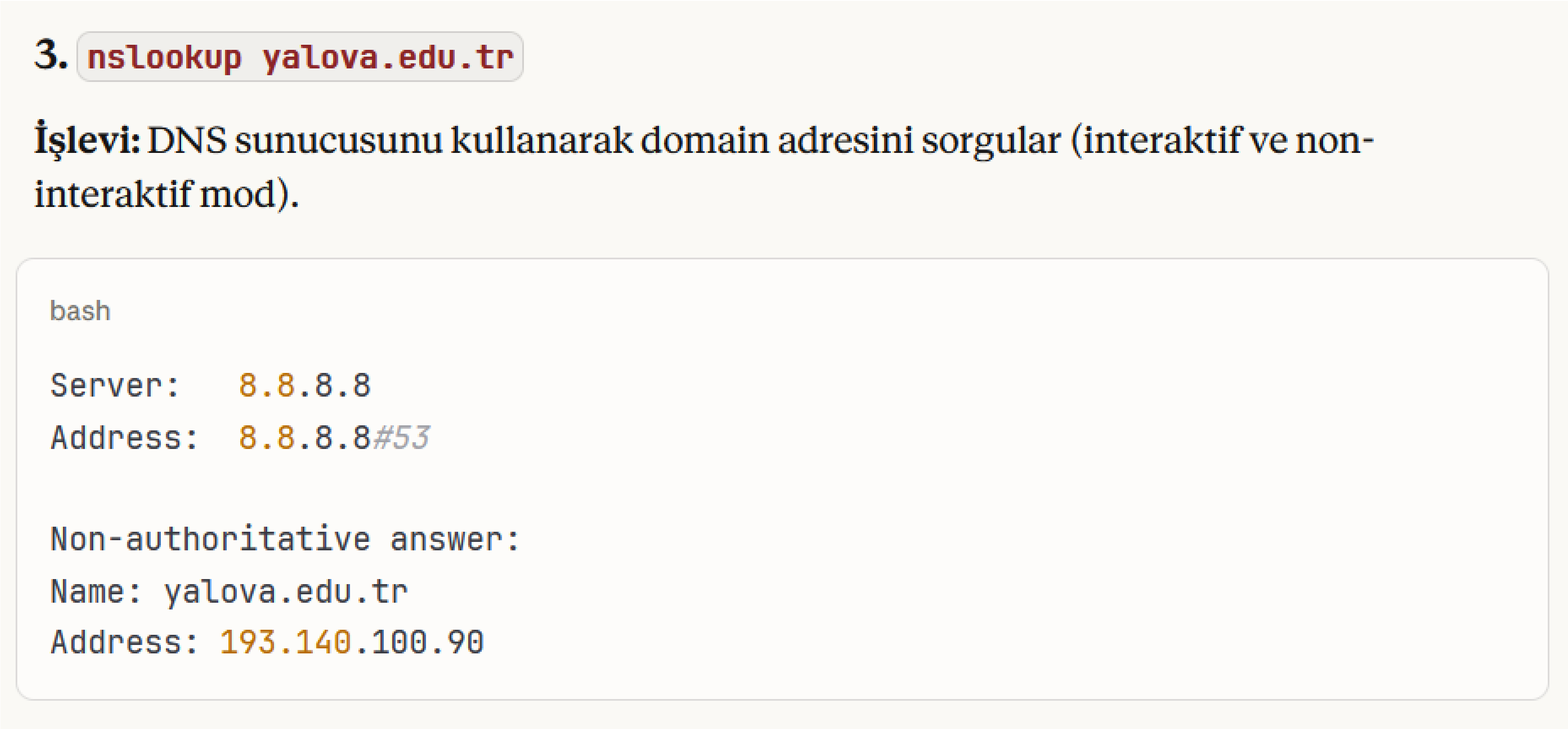
2. `host yalova.edu.tr`

İşlevi: DNS sorgusu yaparak domain'in IP adresini ve diğer DNS kayıtlarını gösterir.

bash

```bash
yalova.edu.tr has address 193.140.100.90
yalova.edu.tr mail is handled by 10 mail.yalova.edu.tr.
```

Konsol Komutları



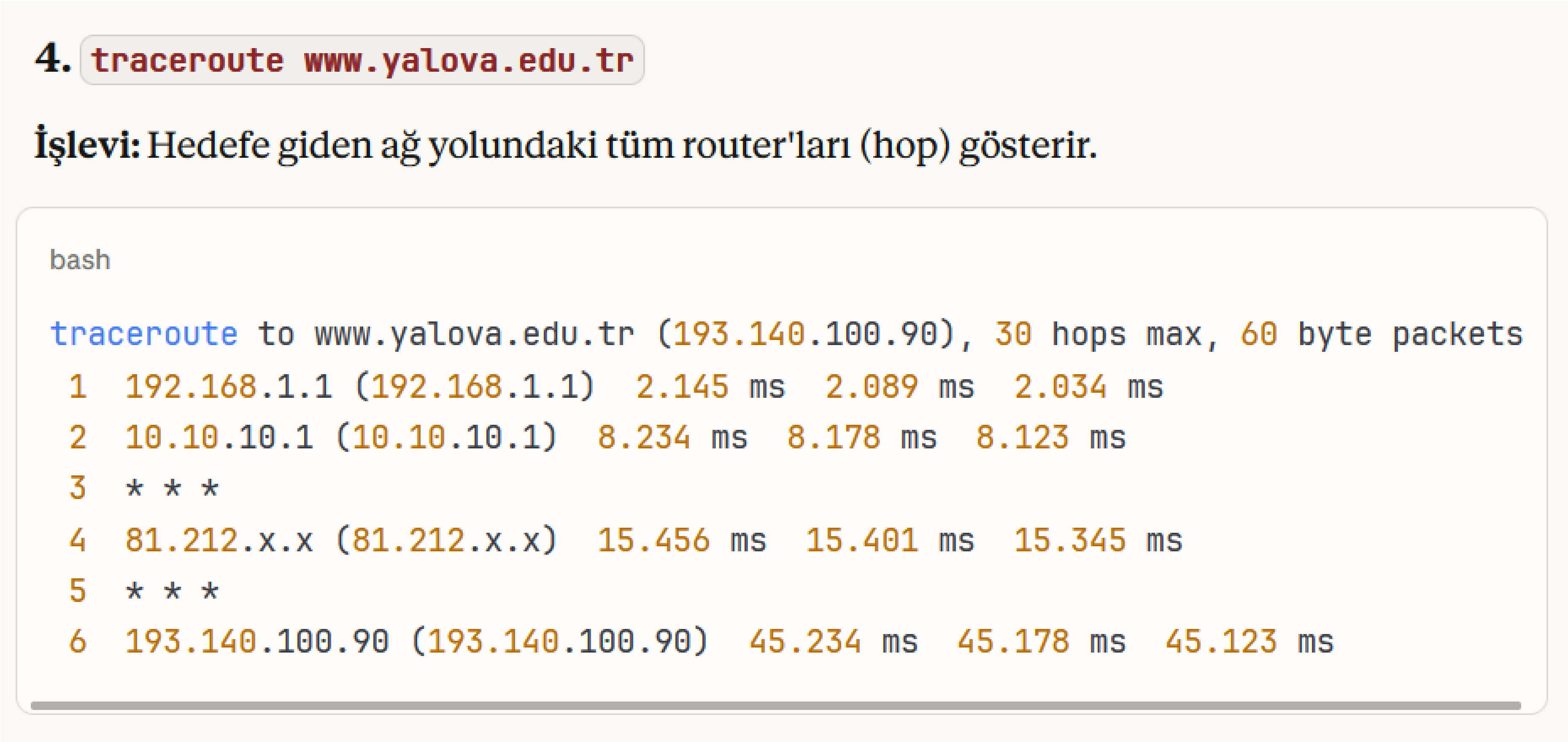
3. `nslookup yalova.edu.tr`

İşlevi: DNS sunucusunu kullanarak domain adresini sorgular (interaktif ve non-interaktif mod).

bash

```
Server:    8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
Name: yalova.edu.tr
Address: 193.140.100.90
```

Konsol Komutları



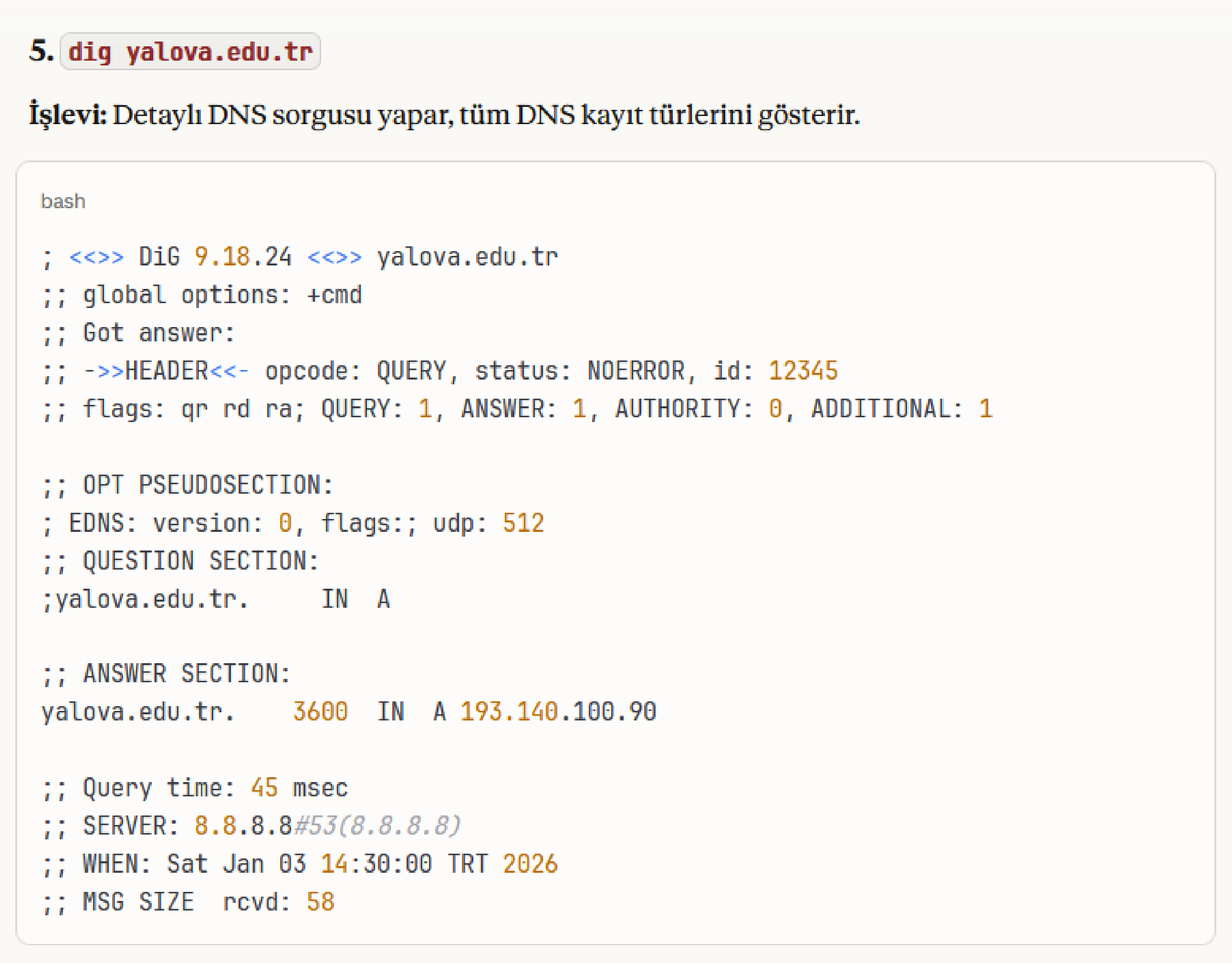
4. `traceroute www.yalova.edu.tr`

İşlevi: Hedefe giden ağ yolundaki tüm router'ları (hop) gösterir.

bash

```bash
traceroute to www.yalova.edu.tr (193.140.100.90), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  2.145 ms  2.089 ms  2.034 ms
 2  10.10.10.1 (10.10.10.1)  8.234 ms  8.178 ms  8.123 ms
 3  * * *
 4  81.212.x.x (81.212.x.x)  15.456 ms  15.401 ms  15.345 ms
 5  * * *
 6  193.140.100.90 (193.140.100.90)  45.234 ms  45.178 ms  45.123 ms
```

Konsol Komutları



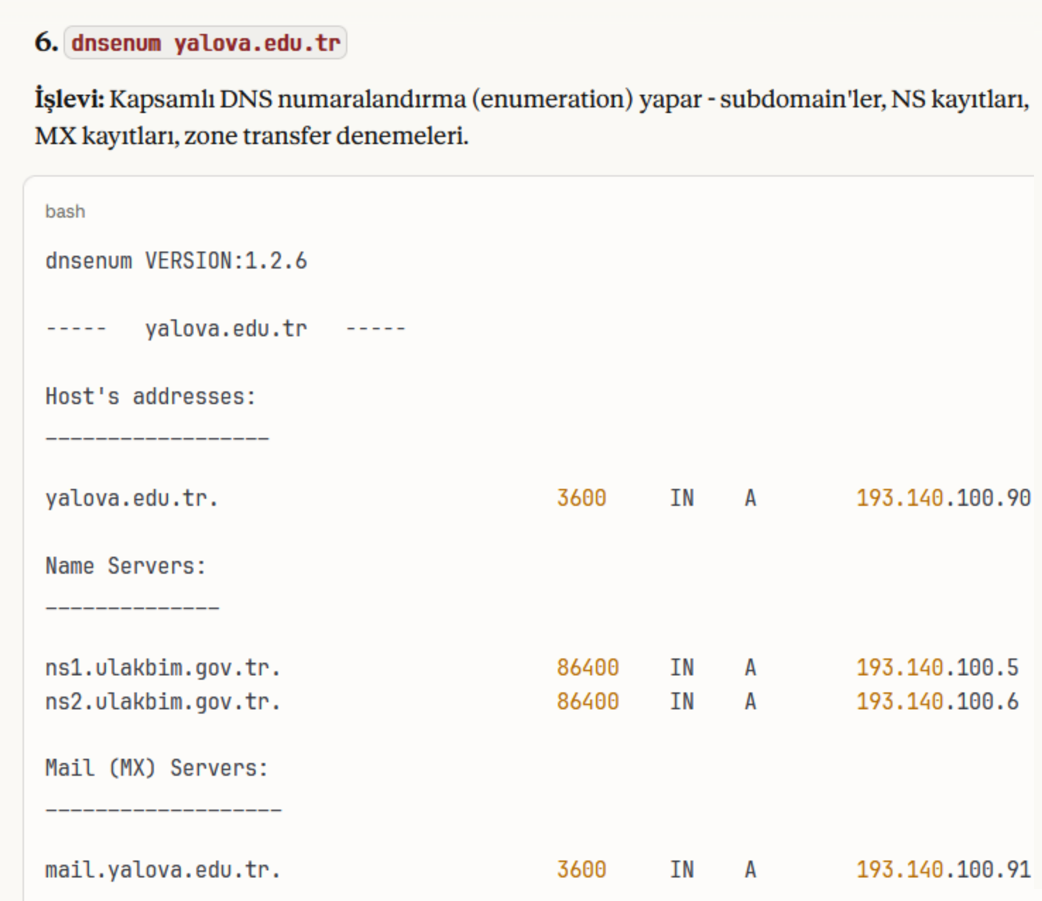
5. `dig yalova.edu.tr`

İşlevi: Detaylı DNS sorgusu yapar, tüm DNS kayıt türlerini gösterir.

bash

```
; <<>> DiG 9.18.24 <<>> yalova.edu.tr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12345
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;yalova.edu.tr.     IN   A

;; ANSWER SECTION:
yalova.edu.tr.    3600   IN   A 193.140.100.90

;; Query time: 45 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Jan 03 14:30:00 TRT 2026
;; MSG SIZE  rcvd: 58
```

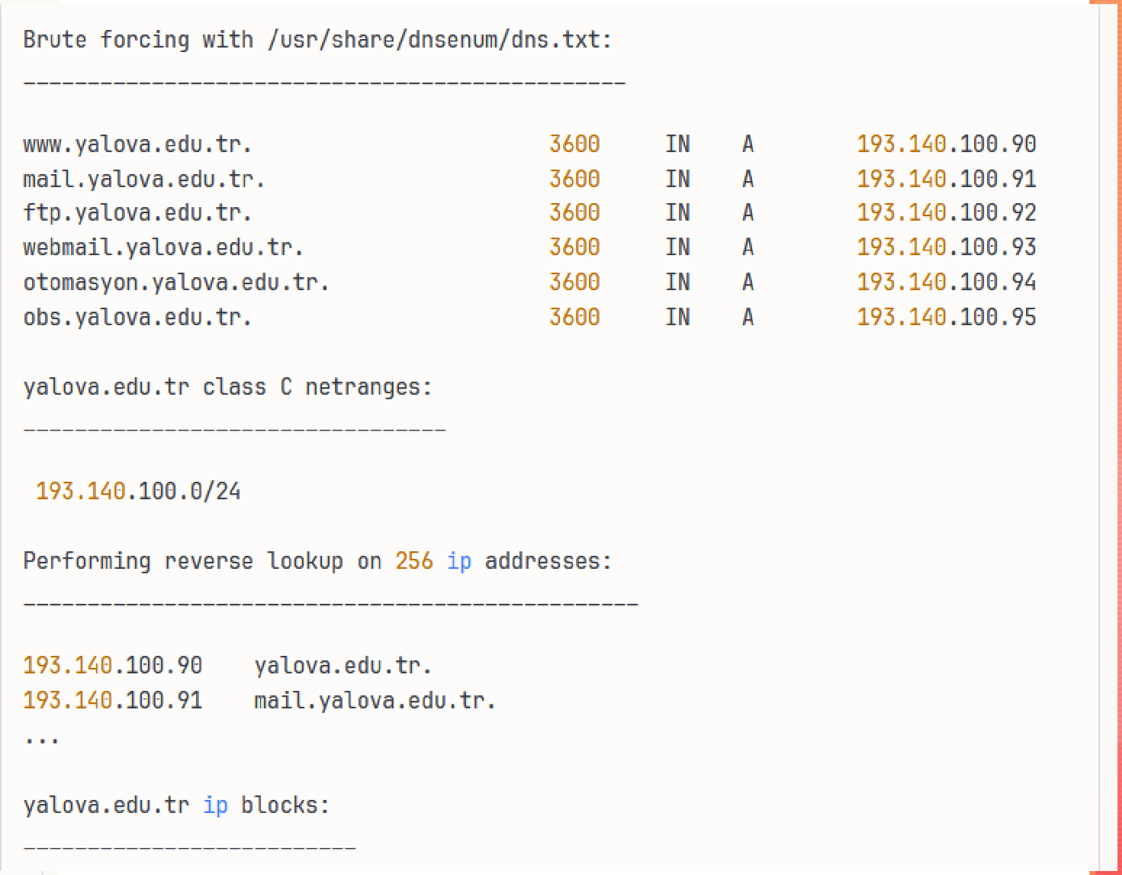
Konsol Komutları



6. `dnsenum yalova.edu.tr`

İşlevi: Kapsamlı DNS numaralandırma (enumeration) yapar - subdomain'ler, NS kayıtları, MX kayıtları, zone transfer denemeleri.

```bash
dnsenum VERSION:1.2.6

-----   yalova.edu.tr   -----

Host's addresses:
__________________

yalova.edu.tr.                          3600     IN     A        193.140.100.90

Name Servers:
______________

ns1.ulakbim.gov.tr.                     86400    IN     A        193.140.100.5
ns2.ulakbim.gov.tr.                     86400    IN     A        193.140.100.6

Mail (MX) Servers:
___________________

mail.yalova.edu.tr.                     3600     IN     A        193.140.100.91
```



```
Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

www.yalova.edu.tr.                        3600     IN    A         193.140.100.90
mail.yalova.edu.tr.                       3600     IN    A         193.140.100.91
ftp.yalova.edu.tr.                        3600     IN    A         193.140.100.92
webmail.yalova.edu.tr.                    3600     IN    A         193.140.100.93
otomasyon.yalova.edu.tr.                  3600     IN    A         193.140.100.94
obs.yalova.edu.tr.                        3600     IN    A         193.140.100.95

yalova.edu.tr class C netranges:
_________________________________

 193.140.100.0/24

Performing reverse lookup on 256 ip addresses:
_______________________________________________

193.140.100.90    yalova.edu.tr.
193.140.100.91    mail.yalova.edu.tr.
...

yalova.edu.tr ip blocks:
__________________________
```