

ÖN BİLGİ

Bu belge

- <https://www.bgasecurity.com/makale/guvenlik-testlerinde-bilgi-toplama/>

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Apache%20htaccess%20G%C3%BCvenlik%20Testleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

Bilgi toplama; hedef sistemle doğrudan iletişime geçerek ve hedef sistemden bağımsız olmak üzere iki türdür.

1. Pasif Bilgi Toplama

- a. IP Adresleri ve Domain Hakkında Bilgi Edinme
 - i) Bir IP adresine ait bilgiler için whois sorgusu
 - ii) Ripe'nin web sitesi üzerinden IP sorgulama
 - iii) Network Solutions Üzerinden Domain Sorgulama
 - iv) Web Sayfalarının Geçmişini İzleme
- b. Eposta Listeleri Arşivleri Aracılığıyla Bilgi Toplama
- c. Netcraft Aracılığıyla Bilgi Toplama
- d. DnsStuff Aracılığıyla Bilgi Toplama
- e. Passive Dns Replication ile Komşu Siteleri Bulma
- f. Bir Domain'e Ait Eposta Adreslerinin Bulunması
- g. Arama Motorları Aracılığıyla Bilgi Toplama
 - i) Pipl.com ile Kişi Bulma
 - ii) GoogleHacking ile Olası Zafiyet Barındıran Linkleri Bulma

2. Aktif Bilgi Toplama

- a. DNS Protokolü Kullanarak Bilgi Toplama
 - i) nslookup ile DNS Sorgulama
 - ii) Dig Aracı İle DNS Sorgulama
 - iii) MX Sorgulama
 - iv) DNS Sunucusunun Versiyonunu Öğrenme
 - v) DNS Zone Transfer Kontrolü
 - vi) DNS Sorgularını İzlemek (DNS Trace)
 - vii) Değişken Kaynak Port ve XID Testleri
 - viii) DNS Sorguları ile Koruma Sistemlerini Atlatma
 - ix) DNS Brute Force Yöntemi ile Bilgi Toplama
- b. Banner Yakalama (Banner Grabbing)
 - i) Mail Sunucusunun Yazılımını Öğrenme
 - ii) Web Sunucularının Yazılımını Öğrenme
 - iii) SSH Sürümünü Sorgulama

3. Diğer Bilgi Toplama Yöntemleri

- a. Web Sayfası Yorum Satırlarından Bilgi Toplama
- b. TCP Sequence Numarasını Tahmin Etme
- c. Hedef Sistemin Uptime Süresini Belirleme
- d. *Hedef Sistemin Saatini Öğrenme*
 - i) HTTP Protokolü İle Hedef Sistemin Saatini Öğrenme
 - ii) SMTP Protokolü İle Hedef Sistemin Saatini Öğrenme
- e. Eposta Başlıkları Aracılığıyla Bilgi Edinme
- f. SMTP Üzerinden Ağ Topolojisini Çıkarma
- g. İnternette İndirilen Dosyanın Metadata'sından Bilgi Toplama
- h. Metagoofil Aracı İle Bilgi Toplama
- i. Ağ Haritalama Yöntemi İle Bilgi Toplama

- i) traceroute Tool'u
- ii) tcptraceroute Tool'u
- j. SNMP Üzerinden Bilgi Toplama
- k. Dimitry ile Bilgi Toplama
- l. Maltego ile Bilgi Toplama

Pasif Bilgi Toplama

Hedef sistem ile doğrudan iletişime geçilmez, herhangi bir iz bırakmadan internetin imkanları kullanılarak yapılır.

Mesela whois sorguları ile şirketin ip aralığı, sorumlu yöneticisi bulunabilir. DNS sorguları ile mail, ftp ve benzeri servislerin hangi ip adreslerinde çalıştığı, ip adresleri ve işletim sistemi bilgilerini hedefle herhangi bir iletişim kurmadan alabiliriz.

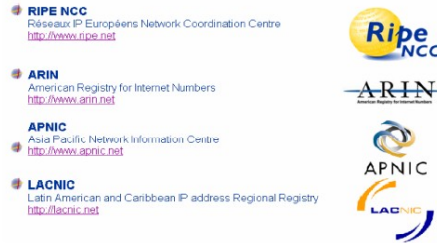
Basit bir whois sorgusundan şu bilgiler edinilebilir; ilgili birimde çalışanların telefon numaraları, e-posta adresleri, şirketin e-posta adresi kullanım profili (isim.soyisim@sirket.com gibi) vb.

a. IP Adresleri ve Domain Adları Hakkında Bilgi Edinme

Tüm dünyada ip adresi ve domain ismi dağıtımı tek bir merkezden kontrol edilir. Bu merkez ICANN(Internet Corporation for Assigned Named and Numbers) adlı bir kurumdur.

ICANN IP adresleri ve domain isimlerinin dağıtımını aşağıdaki gibi düzenlemiştir.

IP Adresleri : RIR(Regional Internet Registrars) lar aracılığı ile.
Domain isimleri : Özel şirketler aracılığı ile IP Adreslerinin bulunduğu bölgeye göre farklı RIR'lardan sorgulanabilir. Dünya üzerinde ip adreslerinin bilgisini tutan dört farklı RIR vardır. Bunlar ;



i) Bir IP adresine ait bilgilere en kısa yoldan whois sorgusu ile erişebiliriz:

> whois 194.27.72.88

Output:

OrgName: RIPE Network Coordination Centre
OrgID: RIPE
Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL
ReferralServer: whois://whois.ripe.net:43
NetRange: 194.0.0.0 - 194.255.255.255
CIDR: 194.0.0.0/8
NetName: RIPE-CBLK2
NetHandle: NET-194-0-0-0-1

inetnum: 194.27.72.0 - 194.27.72.255
netname: KOU-NET
descr: Kocaeli University
country: TR
admin-c: OC222-RIPE
tech-c: OC222-RIPE
status: ASSIGNED PA
mnt-by: ULAKNET-MNT
source: RIPE # Filtered

irt: irt-ULAK-CSIRT
address: National Academic Network
address: and Information Center
address: YOK Binası B5-Blok
address: 06539 Bilkent
address: Ankara-TURKEY
phone: +90 312 298 93 10
fax-no: +90 312 298 93 93
e-mail: csirt@ulakbim.gov.tr
signature: PGPKEY-45F7AD77
encryption: PGPKEY-45F7AD77
admin-c: MS6078-RIPE
tech-c: MS6078-RIPE
auth: PGPKEY-45F7AD77
mnt-by: ULAKNET-MNT

source: RIPE # Filtered
person: Omur Can
address: Kocaeli Universitesi
address: Bilgi İşlem Dairesi
address: İzmit
address: Türkiye

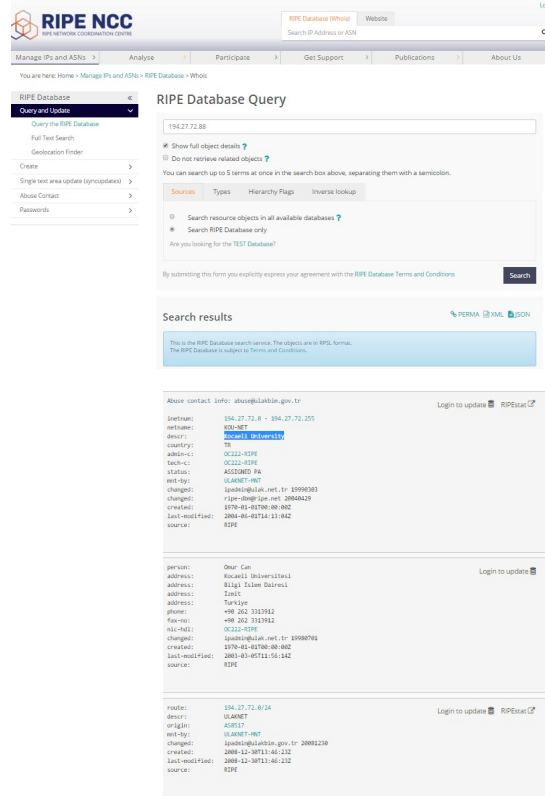
phone: +90 262 3313912
fax-no: +90 262 3313912
nic-hdl: OC222-RIPE
source: RIPE # Filtered

NOT: www.karabuk.edu.tr sitesi RIPE'nin websitesinden sorgulandığında bilgileri göstermiyor. Hata veriyor:

IETF-RESERVED-ADDRESS-BLOCKED

ii) Ripe'nin Websitesi Üzerinden IP Sorgulama

whois'in tool'unun verdiği çıktının aynısı veriyor. Farkı daha derli toplu bir arayüzle sunuyor.



The screenshot shows the RIPE NCC Database Query page. The search bar contains the IP address 194.27.72.88. The search results are displayed in a table format, showing details for the IP address, including its location (Kocaeli University), contact information, and source (RIPE).

Abuse contact info: abuse@dukin.gov.tr	Login to update	RIPEstat
inetnum: 194.27.72.0 - 194.27.72.255		
netname: KDU-NET		
descr: Kocaeli University		
country: TR		
admin-c: OC222-RIPE		
tech-c: OC222-RIPE		
status: ASSIGNED PA		
mnt-by: IRIPE-NET		
changed: iparis@dukin.net.tr 19980903		
changed: iparis@dukin.net.tr 20080229		
created: 1978-01-01T00:00:00Z		
last-modified: 2008-12-30T13:41:44Z		
source: RIPE		

person: Ömer Can	Login to update	RIPEstat
address: Kocaeli Üniversitesi		
address: Bilgi İşlem Dairesi		
address: Zeytin		
address: Turkiye		
phone: +90 262 3313912		
fax-no: +90 262 3313912		
nic-hdl: OC222-RIPE		
changed: iparis@dukin.net.tr 19980701		
created: 1978-01-01T00:00:00Z		
last-modified: 2003-03-05T11:56:34Z		
source: RIPE		

router: 194.27.72.0/24	Login to update	RIPEstat
descr: KDU-NET		
origin: AS6137		
mnt-by: IRIPE-NET		
changed: iparis@dukin.gov.tr 20081230		
created: 2008-12-30T13:46:21Z		
last-modified: 2008-12-30T13:46:21Z		
source: RIPE		

NOTE: Eğer bir IP adresinin hangi bölgede (RIR'da) olduğunu bilmiyorsanız ilk olarak ARIN üzerinden sorgulama yapın. ARIN üzerinden yapılacak IP adresi sorgulaması sonucu ilgili IP eğer ARIN'in kontrolünde değilse size ilgili RIR'ın bilgisini verecektir. Böylece hangi whois sunucusunda barındığını öğrenebileceksiniz ve sorgunuzu o sunucuda yapabileceksiniz.

ARIN WHOIS Database Search - Mozilla Firefox
http://www.arin.net/whois/whoisqueryipui=222.222.222.1

ARIN WHOIS Database Search
Relevant Links: ARIN Home Page ARIN Site Map Training Querying A...

Search ARIN WHOIS for: 222.222.222.1
Sorguyu gönder

OrgName: Asia Pacific Network Information Centre
OrgID: APNIC
Address: PO Box 2131
City: Hiloa
StateProv: Qld
PostalCode: 9094
Country: AU

ReferralServer: whois://whois.apnic.net

NetRange: 222.0.0.0 - 222.255.255.255
CIDR: 222.0.0.0/8
NetName: APNIC8
NetHandle: NET-222-0-0-1

222.222.222.1 IP adresinin sorumlu olduğu bölge APNIC olduğu için oraya yönlendirme yapılıyor

iii) Network Solutions Üzerinden Domain Sorgulama

Aşağıdaki adres ile domain kaydı sorgulanabilir.

Sorgulama Sitesi

<http://www.networksolutions.com/whois/index.jsp>

Sorgulanan Site

lifeoverip.net

Sorgu çıktısı şöyle bi'şey:

```
Domain Name: LIFEOVERIP.NET
Registry Domain ID: 859838676_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2015-02-07T17:50:03Z
Creation Date: 2007-03-07T14:01:24Z
Registrar Registration
Expiration Date: 2017-03-07T14:01:24Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Registry Registrant ID:
Registrant Name:
Registrant Organization: huzeyfe onal Lifeoverip
Registrant Street: Istanbul Dünya, 11111 Turkey Last
Updated on: 21-DEC-09
Registrant City:
Registry Admin ID:
Admin Name: huzeyfe onal
```

Bu da çıktıyı aldığım yerin resmi:

```
lfeoverip.net
Is this your domain name? Renew it now.

Domain Name: LIFEVERIP.NET
Registry Domain ID: 859838676_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2015-02-07T17:50:03Z
Creation Date: 2007-03-07T14:01:24Z
Registrar Registration Expiration Date: 2017-03-07T14:01:24Z
Registrar: Godaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1 4806242405
Domain Status: clientTransferProhibited http://www.icann.org/epp/clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp/clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp/clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp/clientDeleteProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization: huseyfe onal Lifeoverip
Registrant Street: Istanbul Dunya, 11111 Turkey Last Updated on: 21-DEC-09
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country:
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: nocontactsfound@secureserver.net
Registry Admin ID:
Admin Organization:
Admin Phone:
Admin Fax:
Admin Email:
```

iv) Web Sayfalarının Geçmişini İzleme

Archive.org 1996'dan beri tüm interneti kayıt altına alan bir yapıdır. Buradan hedef sistemin önceki kaydedilmiş bilgilerine erişim sağlanabilir.

www.archive.org

b. Eposta Listeleri Arşivleri Aracılığıyla Bilgi Toplama

Örn;

Aşağıdaki ekran görüntüsü bir eposta listesine bilgi alma amacı ile sorulan bir sorudan alınmıştır. Soruyu soran kişi detaylı bilgilendirme adına kullandığı yazılımın yapılandırma dosyasını da göndermiş. Fakat yapılandırma dosyası içerisinde uygulamanın çalışması için gerekli şifreyi silmeyi unutmuş. Şifre kısmı incelendiğinde maili gönderen kişinin Beşiktaşlı biri olduğu ve şifre olarak tuttuğu takımın rakamlarının yer aldığı görülebilir.

```
# See the README.database file for more information about configuring
# and using this plugin.
#
output database: log, mysql, user=snort password=001905 dbname=snort host=localhost
output alert fwsam: 10.10.1.50/bf261nx

# output database: alert, postgresql, user=snort dbname=snort
# output database: log, odbc, user=snort dbname=snort
# output database: log, mssql, dbname=snort user=snort password=test
# output database: log, oracle, dbname=snort user=snort password=test

# unified: Snort unified binary format alerting and logging
# -----
# The unified output plugin provides two new formats for logging and generating
```

c. Netcraft Aracılığıyla Bilgi Toplama

Netcraft sitesi hedef sistemin işletim sistemini, kernel versiyonunu, web sunucusu olarak üzerinde çalışan yazılımlara ait detaylı bilgileri ve bunların yanısıra sistemin uptime bilgisini gösterebilen bir sayfadır.

Netcraft hedef sistemin yazılım bilgilerini belirlemek için httpprint ile çeşitli sorgular yapar ve gelen cevaplara göre bir tahminde bulunur. (Burada yapılan hatalı bir istekdir ve dönen hata cevaplarından web sunucu yazılımı belirlenir).

Netcraft'ın sitesi : <http://www.netcraft.com/>
Sorgulanacak site: <http://www.karabuk.edu.tr>

Site	http://www.karabuk.edu.tr	Netblock Owner	Karabuk Universitesi
Domain	karabuk.edu.tr	Nameserver	ns1.karabuk.edu.tr
IP address	193.140.9.45	DNS admin	hostmaster@karabuk.edu.tr
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	nic.tr	Nameserver organisation	whois.nic.tr
Organisation	Karabuk Üniversitesi	Hosting company	unknown
Top Level Domain	Turkey (.edu.tr)	DNS Security Extensions	unknown
Hosting country	TR		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Karabuk Universitesi Turkey	193.140.9.6	Windows Server 2012	Microsoft-IIS/8.5	29-Nov-2015	
Karabuk Universitesi Turkey	193.140.9.6	Windows Server 2003	Microsoft-IIS/6.0	28-Jul-2014	
Karabuk Universitesi Turkey	193.140.9.4	Windows Server 2003	Microsoft-IIS/6.0	18-Apr-2009	

Görüldüğü üzere üniversitenin sunucusunun işletim sistemi Windows Server 2003'ten Windows Server 2012'ye terfi ettirilmiş. Dolayısıyla web sunucusu yazılımını da IIS/6.0'dan IIS/8.5'ye çıkılmış.

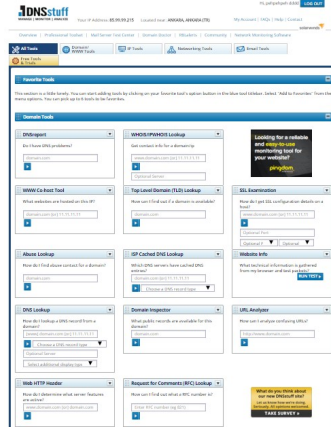
Netcraft ile bu tip saptamalarda bulunabiliyoruz.

d. DnsStuff Aracılığıyla Bilgi Toplama

DNSStuff komut satırından nslookup, host, dig ve whois gibi programları çalıştırarak alınabilecek çıktıları derli toplu ve merkezi bir ortamdan kullanılmasını sağlayan bir araçtır (websitesidir).

DnsStuff aynı sayfada mail sunucunuzun/IP adresinizin spam listelere girip girmediğini, DNS sunucu yapılandırmanız gibi bilgileri ve dahasını öğrenebilme imkanı sunmaktadır.

DnsStuff Sitesi Şu: <http://www.dnsstuff.com/tools#>



e. Passive DNS Replication ile Komşu Siteleri Bulma

Passive Dns replication(PDR) bir tür pasif dns analiz aracıdır. Piyasada daha çok "bir" IP adresine ait domainleri bulmaya çalışırken faydalanılır.

Passive DNS Replication işlemi dig aracı ile yapabilirsin:

```
> dig -x IPNUMBER
```

İşe yaramazsa bing arama motorunu kullanabilirsin. Bing'e şunu gir:

```
ip: 188.124.10.40
```

Bu ip'ye düşen tüm domain'ler (websiteleri) sıralanacaktır. Bir başka çözüm ise aşağıdaki sitedir:

<https://majestic.com/reports/neighbourhood-checker>

Bu siteye dilediğin websitenin adını ya da IP'sini girerek aynı ip'yi paylaşan domain'leri görebilirsin.

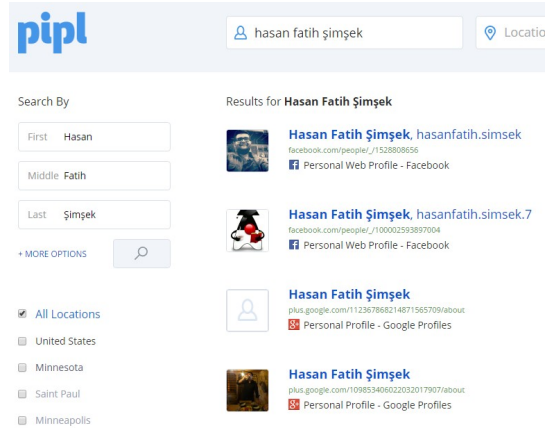
f. Bir Domain'e Ait Eposta Adreslerinin Bulunması

Bir domaine ait internette dolan (arama motorları vasıtası ile bulunabilecek) e-posta hesaplarını toptan görmek için arama motorları ile uğraşmanıza gerek yoktur. Google ve MSN Search'u bizim için arayip belirlediğimiz kriterlere göre mailleri bulan TheHarvester adlı tool'u kullanabilirsiniz. Veyahut bir windows uygulaması olan FreeEmailExtractor adlı yazılımı da kullanabilirsiniz.

g. Arama Motorları Aracılığıyla Bilgi Toplama

i) Pipl.com Aracılığı ile Şahıs Arama

Pipl.com kişi arama için en ideal sonuçları bulan bir arama motorudur. Aranılan kişi ile ilgili çeşitli bilgileri kategorik olarak ekrana yansıtır.

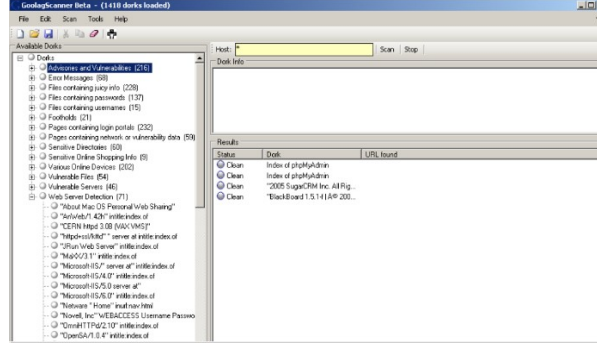


The screenshot shows the Pipl.com search interface. The search bar contains 'hasan fatih şimşek' and a location filter is set to 'Location'. The search results are displayed in a grid format. The first result is 'Hasan Fatih Şimşek, hasanfath.simsek' with a Facebook profile link. The second result is 'Hasan Fatih Şimşek, hasanfath.simsek.7' with a Facebook profile link. The third result is 'Hasan Fatih Şimşek' with a Google profile link. The fourth result is 'Hasan Fatih Şimşek' with a Google profile link. The search criteria are set to 'First: Hasan', 'Middle: Fath', and 'Last: Şimşek'. The location filter is set to 'All Locations'.

ii) Google Aracılığıyla Bilgi Toplama

Google üzerinden arama yapmak için çeşitli teknikler bulunmaktadır. Bu tekniklere GoogleHacking adı verilir. Bu teknikler çeşitli özel kelimelerden oluşur ve genelde akılda kalmaz. Bunun için çeşitli googleHacking programları yazılmıştır.

Bu programlardan en kullanışlı olanı Goolag Scanner'dir. İçerisinde 1400 civarı GoogleHack tekniği barındırır.



Bu yazılımın sitesi göçük. Başka hiçbir yerde de yok maalesef (!)

Aktif Bilgi Toplama

Aktif bilgi toplama yöntemlerinde hedef ile iletişime geçilerek olabildiğince fazla ve işe yarayan bilgi edinilmeye çalışılır.

a. DNS Protokolü Kullanarak Bilgi Toplama

DNS Protokolü internetin temel yapıtaşdır. Genel olarak www hizmetlerinde ve e-posta servislerinde kritik rol oynar. Düzgün yapılandırılmamış bir DNS sunucu dışarıya oldukça fazla bilgi verebilir.

DNS Query Types

A	Host Address	32-bit IP address
CNAME	Canonical Name	Canonical Domain Name for an alias
HINFO	CPU & OS	Name of CPU and Operating System
MINFO	Mailbox Info	Information about a Mailbox or Mail List
MX	Mail Exchanger	16-bit Preference and Name of Host that acts as Exchanger for the Domain
NS	Name Server	Name of Authoritative Server for Domain
PTR	Pointer	Pointer from IP address to Domain Name
SOA	Start of Authority	Multiple fields that specify which parts of the naming hierarchy a server implements
TXT	Arbitrary Text	Uninterpreted string of ASCII text

Nslookup (Windows/Linux) ve Linux sistemler için dig komutu ile her tür dns sorgulama işlemi yapılabilir.

i) nslookup ile DNS Sorgulama

Site artık mevcut değil ama örneği görmek adına huzeyfe.net'i ele alalım. Bu sorguda sorgu tipi olarak yukarıdaki resimde yer alan DNS sorgu tiplerinden (A, CNAME, MX,...) NS'yi kullanalım. Bunun için set type=ns dememiz gerekir.

```
C:\Console2> nslookup  
> set type=ns  
> huzeyfe.net
```

Output:

```
Server: mygateway1.ar7  
Address: 192.168.1.1  
DNS request timed out.  
timeout was 2 seconds.  
DNS request timed out.  
timeout was 2 seconds.  
*** Request to mygateway1.ar7 timed-out
```

Görüldüğü üzere yanıt alamadık. huzeyfe.net sitesinin dns bilgisine ulaşamadık. Şimdi DNS sorgusu yaparken ki kullandığımız DNS sunucumuzu değiştirelim ve ttdns40.ttnet.net.tr (195.175.39.40) yapalım. Bunun için nslookup'ın server komutu kullanılır.

```
C:\Console2> nslookup  
> server 195.175.39.40  
> huzeyfe.net
```

Output:

```
Server: ttdns40.ttnet.net.tr  
Address: 195.175.39.40  
Non-authoritative answer:  
huzeyfe.net nameserver = ns1.tekrom.com  
huzeyfe.net nameserver = ns2.tekrom.com  
ns1.tekrom.com internet address = 67.15.122.30  
ns2.tekrom.com internet address = 67.15.122.225
```

Görüldüğü üzere kullanılan DNS sunucusu değiştirildiğinde huzeyfe.net'e ait NS'yi (name server'ı) bulmuş olduk.

Eğer ters DNS sorgusu yapmak isteseydik, yani domain adı verip IP'sini öğrenmek değil de IP'sini verip domain'ini öğrenmek isteseydik DNS Sorgu Tiplerinden (A, CNAME, MX,...) PTR'yi kullanmamız gerekirdi. Bu durumda aşağıdakiler girilirdi.

```
C:\Console2> nslookup
```

```
> 1.2.3.488 // IP girilir, domain bulunur.
```

```
Output:
```

```
Server: ttdns40.ttnet.net.tr
Address: 195.175.39.40
Non-authoritative answer:
88.72.27.194.in-addr.arpa name = open.edu.tr
88.72.27.194.in-addr.arpa name= kocaeli2007.open.edu.tr
72.27.194.in-addr.arpa nameserver = bim.open.edu.tr
bim.open.edu.tr internet address = 1.2.3.42
```

ii) Dig Aracı İle DNS Sorgulama

Dig tool'u nslookup ve host gibi dns sorgulama araçları yerine kullanılabilen gelişmiş bir araçtır. Uzun vadede Linux dağıtımlarında nslookup komutunun yerini alması beklenmektedir. Dig komutu domains sorgulama için çalıştırıldığında cevapla birlikte detay bilgiler de döndürür. Bu detay bilgiler ek parametrelerle gizlenebilir.

```
> dig ns hack2net.com @195.175.39.40
```

```
Output:
```

```
; <<>> DiG 9.4.1 <<>> ns hack2net.com
@195.175.39.40
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status:
NOERROR, id: 52488
;; flags:qr rd ra;QUERY:1,ANSWER:2,AUTHORITY:0,
ADDITIONAL: 2

;; QUESTION SECTION:
;hack2net.com. IN NS

;; ANSWER SECTION:
hack2net.com. 54685 IN NS
```

ns1.tr.net.tr.

hack2net.com. 54685 IN NS

```
;; ADDITIONAL SECTION:
ns2.tr.net.tr. 2319 IN A 195.155.11.4
ns1.tr.net.tr. 1014 IN A 195.155.1.3

;; Query time: 22 msec
;; SERVER: 195.175.39.40#53(195.175.39.40)
;; WHEN: Sun Aug 10 18:32:33 2008
;; MSG SIZE rcvd: 103
```

Output'un Detaylı Açıklaması

- ➔ Status:NOERROR
Sorgulanan domain adının var olduğunu ve bu domainden sorumlu dns sunucusunun sorgulara sağlıklı cevap verdiği anlamına gelir.
- ➔ Status:SERVFAIL
Domainin var olduğunu, fakat domain'den sorumlu DNS sunucusunun sorgulara sağlıklı cevap veremediği anlamına gelir. Yani sorun domain'den sorumlu olan DNS sunucusundandır.
- ➔ Status:NXDOMAIN
Domain ile ilgili ana DNS sunucularının bilgisinin olmadığını gösterir. Yani ya sorgulanan domain mevcut değildir ya da çeşitli sebeplerden ötürü root dns sunucusu yanıt verememiştir manasına gelir.

Aynı işlemi nslookup kullanarak da yapabildik:

```
C:\> nslookup
> set type=ns           // type yerine q da konabilir.
                        // Aynı şeyi yapar
> hack2net.com
```

Output:

```
Server:                192.168.2.1
Address:               192.168.2.1#53
```

Non-authoritative answer:

```
hack2net.com  nameserver=ns1w.name.com  
hack2net.com  nameserver=ns4jp.name.com,  
hack2net.com  nameserver=ns3dt.name.com,  
hack2net.com  nameserver=ns2fl.name.com,
```

Authoritative answers can be found from:

```
n1sjp.name.com internet address=98.124.217.1  
ns3dt.name.com internet address=98.124.246.2  
ns1w.name.com  internet address=184.172.60.1  
ns1w.name.com has AAAA  
address=2507:f0d0:1101:16f:24  
ns2fl.name.com internet address=98.124.246.1
```

iii) MX Sorgulama

DNS sorgu tiplerinden MX mail exchanger'ın kısaltılmışıdır. MX tipinde DNS sorgusu yaparak bir domain'e ait smtp sunucularını belirleyebiliriz.

```
> dig @195.175.39.40 -t mx hack2net.com
```

Output:

```
...  
;; QUESTION SECTION:  
;hack2net.com. IN MX  
  
;; ANSWER SECTION:  
hack2net.com. 86400 IN MX 10  
mail.hack2net.com.
```

...

iv) DNS Sunucusunun Versiyonu

DNS sunucu versiyon bilgisini öğrenmek bir saldırganın o dns sunucuda "DNS cache Poisoning" açıklığının olup olmadığı konusunda bilgi verebilir. Aşağıdaki dns sunucu bilgisi bir saldırgan için hedef olacak kadar açıklık barındırmaktadır.

```
> dig @10.180.8.115 version.bind chaos txt
```

Output:

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6  
<<>> @10.180.8.115 version.bind chaos txt
```

```
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
37376
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;version.bind. CH TXT

;; ANSWER SECTION:
version.bind. 0 CH TXT "9.8.2rc1-RedHat-9.8.2-
0.17.rc1.el6_4.6"

;; AUTHORITY SECTION:
version.bind. 0 CH NS version.bind.

;; Query time: 2 msec
;; SERVER: 10.180.8.115#53(10.180.8.115)
;; WHEN: Fri Oct 18 16:20:20 2013
;; MSG SIZE rcvd: 95
```

Tüm Türkiye'nin kullandığı DNS sunucusunun (195.175.39.40) versiyon bilgisini sorgulayalım(*Dilersen nslookup 195.175.39.40 ile ters dns sorgusu yaparak dns sunucularının adlarını öğrenebilirsin (rdns2.turktelekom.com.tr, rdns1.turktelekom.com.tr, rdns3.turktelekom.com.tr)).*

```
> dig @195.175.39.40 version.bind chaos txt
```

Output:

```
; <<>> DiG 9.4.1 <<>> @195.175.39.40
version.bind chaos txt
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status:
NOERROR, id: 61452
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0
;; WARNING: recursion requested but not available
;; QUESTION SECTION:
;version.bind. CH TXT
;; ANSWER SECTION:
version.bind. 0 CH TXT "Versiyon bilgisi guvenlik
nedeniyle gizlenmistir. Geregi durumunda
```


ipg@turktelekom.com.tr adresine basvurunuz."
;; AUTHORITY SECTION:
version.bind. 0 CH NS version.bind.
;; Query time: 24 msec
;; SERVER: 195.175.39.40#53(195.175.39.40)
;; WHEN: Sun Aug 10 18:40:15 2008
;; MSG SIZE rcvd: 167

v) DNS Zone Transfer Kontrolü

DNS'in yapısı gereği ikincil dns sunucular kendilerinde tanımlı birincil dns sunucunun verilerini dinamik olarak alırlar ve aldıkları veriye göre de gelen istekleri cevaplarlar. Burada transfer edilen veri, yedekleme maksadıyla transfer edilir. Bir DNS sunucu göçtü mü diğeri devreye girsin diyedir. Tabi bu transfer sürecinde transfer edilen domain kayıtları yabancı gözlerden uzak tutulmalıdır. Bu konudaki önlem master DNS sunuculara sadece yetkili ip adresleri için zone transfer izni vermeyeyle gerçekleştirilir.

Sisteme sızmak isteyen birinin yapacağı keşiflerden biri de DNS sunucunuzdan zone transferi yapmaktır. Bunun için nslookup ya da dig araçları kullanılabilir.

→ Dig Aracı İle Zone Transferi

If the name server which hosts the target's domain zone is vulnerable to a zone transfer attack. A simple AXFR query will display all saved DNS records

Example:

```
numb@soldierx.com:~$ dig shadow.net axfr
```

AXFR is a type for dns transaction.

[Bunu araştır. Pdf'deki ls -d komutu çalışmıyor. Page 23-24]

vi) DNS Sorgularını İzlemek (DNS Trace)

Domainize ait DNS sorgularının hangi DNS sunuculardan geçtiğini sorgulamak için dig komutuna +trace parametresini verebilirsiniz. Bu parametre ile iterative

sorgu yapılarak root sunuculardan sizin domaininizin tutulduğu DNS sunucusuna kadar olan yollar belirlenir.

```
> dig +trace karabuk.edu.tr @195.175.39.39
```

Yukarıdaki 195.175.39.39 adresi türk telekomun DNS sunucusunun adresidir (İstersen nslookup 195.175.39.39 diyerek görebilirsin). dig +trace ile root dns server'dan karabuk.edu.tr'ye ait dns server'ına kadar giden yolları trace edeceğiz.

```
root@kali:~/Desktop# dig +trace karabuk.edu.tr @195.175.39.39
; <<>> DiG 9.8.4-rpz2+r1005.12-P1 <<>> +trace karabuk.edu.tr @195.175.39.39
;; global options: +cmd
.          41105  IN      NS      b.root-servers.net. 1
.          41105  IN      NS      h.root-servers.net.
.          41105  IN      NS      g.root-servers.net.
.          41105  IN      NS      c.root-servers.net.
.          41105  IN      NS      j.root-servers.net.
.          41105  IN      NS      k.root-servers.net.
.          41105  IN      NS      m.root-servers.net.
.          41105  IN      NS      a.root-servers.net.
.          41105  IN      NS      l.root-servers.net.
.          41105  IN      NS      f.root-servers.net.
.          41105  IN      NS      i.root-servers.net.
.          41105  IN      NS      d.root-servers.net.
.          41105  IN      NS      e.root-servers.net.
;; Received 508 bytes from 195.175.39.39#53(195.175.39.39) in 896 ms

tr.        172800  IN      NS      ns1.nic.tr. 2
tr.        172800  IN      NS      ns2.nic.tr.
tr.        172800  IN      NS      ns3.nic.tr.
tr.        172800  IN      NS      ns4.nic.tr.
tr.        172800  IN      NS      ns5.nic.tr.
;; Received 206 bytes from 199.7.83.42#53(199.7.83.42) in 788 ms

karabuk.edu.tr. 43200  IN      NS      ns1.karabuk.edu.tr. 3
;; Received 66 bytes from 213.248.162.131#53(213.248.162.131) in 493 ms

karabuk.edu.tr. 10800  IN      A      193.140.9.6 4
karabuk.edu.tr. 10800  IN      NS      ns1.ulak.net.tr.
karabuk.edu.tr. 10800  IN      NS      ns1.karabuk.edu.tr.
;; Received 109 bytes from 193.140.9.2#53(193.140.9.2) in 43 ms

root@kali:~/Desktop#
```

İlk olarak resolv.conf'ta tanımlı DNS sunucudan ROOT DNS sunucularının listesi alınır. Gelen listedeki ilk dns sunucusuna .tr uzantılarından sorumlu olan dns sunucu sorulur ve cevap olarak ns1.nic.tr döner. Sonra ns1.nic.tr'ye karabuk.edu.tr'den sorumlu dns sunucu sorulur. Dönen cevap ns1.karabuk.edu.tr'dir . Son olarak ns1.karabuk.edu.tr'ye karabuk.edu.tr ismi sorulur ve cevap 193.140.9.6 olarak döner.

vii) Değişken Kaynak Port ve XID Değeri Testleri

Recursive DNS sunucular (Back and forth yapan dns sunucular) başka dns sunuculardan istekte bulunurken

kaynak port numarasını deęiřtirmeyebilirler. Bu sayede kaynak portun öğrenilmesine imkan vermiş olurlar ve dns protokolünün kötüye kullanılmasına sebep olabilir.

DNS sorgulamaları UDP üzerinden çalıştığı için IP spoofing yapmak kolaydır. Bu sebeple dns protokolünün güvenliği kaynak port numarası ve transaction ID (XID) deęişkenine baęlıdır. Bu iki deęişken ne kadar kuvvetli olursa dns üzerinden yapılacak cache poisoning türü ataklar o kadar başarısız olacaktır.

- Kaynak port deęeri yeterli derecede kuvvetli olan dns sunucusunun verdięi cevap: *[TurkTelekom]*

```
> dig +short @195.175.39.40 porttest.dns-oarc.net txt
```

Output:

```
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.  
"195.175.39.228 is GREAT: 26 queries in 6.3 seconds from 26 ports with std dev 16123"
```

- Kaynak port deęeri yeterli derece kuvvetli olmayan dns sunucusunun verdięi cevap: *[vpn.lifeoverip.net]*

```
> dig +short @vpn.lifeoverip.net porttest.dns-oarc.net txt
```

Output:

```
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.  
"80.93.212.86 is POOR: 26 queries in 5.5 seconds from 1 ports with std dev 0"
```

vii) DNS Sorguları ile Koruma Sistemlerini Atlatma

Sistem ve aę yöneticileri test amaçlı çeřitli sistemler kurarlar ve bunlara kolay erişim için dns kaydı girerler. Bu kayıtlar dışarda başkaları tarafından bilinirse farklı amaçlar için kullanılabilir.

Mesela X firması kendisine gelen tüm mailleri spam ve virus koruma sistemlerinden geçiriyor olsun. Bunu

yapabilmesi için spam&virus koruma sisteminin ip adresini Dns sunucusunda MX kaydı olarak yayınlaması gerekir.

```
$ nslookup  
> set querytype=mx  
> bankofengland.co.uk
```

Output:

```
Server: 213.228.193.145  
Address: 213.228.193.145#53  
Non-authoritative answer:  
bankofengland.co.uk mail exchanger = 10  
cluster2.eu.messagelabs.com.  
bankofengland.co.uk mail exchanger = 20  
cluster2a.eu.messagelabs.com.
```

Yukarıdan da görülebileceği gibi firma iki adet mx kaydı yayınlamıştır. Diyelim ki dışarıdaki bir saldırgan bu firmaya ait dışarıya anons etmediği dns isimlerini sözlük saldırısı ile bulmaya çalışsın.

```
C:\tools> txdns -f mailDictionary.txt bankofengland.co.uk
```

Output:

```
-----  
TXDNS (http://www.txdns.net) 2.0.0 running STAND-  
ALONE Mode  
-----
```

```
> mail.bankofengland.co.uk - 217.33.207.254  
> mail2.bankofengland.co.uk - 194.201.32.153  
> mailhost.bankofengland.co.uk - 194.201.32.130  
-----
```

```
Resolved names: 3  
Failed queries: 95  
Total queries: 98
```

Sonuçlardan görüleceği üzere firma dışarıya anons etmediği fakat kullandığı başka smtp sunuculara sahiptir. Gönderilecek bir virus ya da zararlı programcık bu adresler kullanılarak gönderilebilir.

viii) DNS Brute Force Yöntemi İle Bilgi Toplama

DNS sunucularına hedef sisteme ait olası subdomainlerin yer aldığı sözlük dosyası ile brute force yaparak hedef site hangi subdomain'lere sahip belirleyebiliriz. Teker teker elle denemektense böyle çoklu olarak denemek daha uygundur. Bu iş için PDF'de bahsedilen dnsbruteforce.py kullanılacaktır. dnsenum.pl script'i ya da dnsnmap script'i de kullanılabilirdi. Bu işi yapacak birçok tool mevcuttur.

```
$ python DNSBruteforce.py www.lifeoverip.net  
dnsServers.txt sub-domainWordlist.txt
```

Output:

```
-----| Information |-----  
-[*] -- 195.175.39.40  
      +- thread in progress : 7 hosts of 10  
-[*] -- 195.175.39.39  
      +- thread in progress : 7 hosts of 7  
-----  
- Total in progress : 14  
- Find hosts :  
['www.lifeoverip.net', 'mail.lifeoverip.net',  
'netsec.lifeoverip.net', 'openbsd.lifeoverip.net']  
End at : Sun Aug 10 18:18:39 2008  
['www.lifeoverip.net', 'mail.lifeoverip.net',  
'netsec.lifeoverip.net', 'openbsd.lifeoverip.net']  
-----
```

dnsServers.txt dosyası sorguların gönderileceği dns sunucu adreslerini barındırmaktadır. subdomainWordlist.txt dosyası ise tarayacağımız siteye has subdomain'lerin yer aldığı bir wordlist'i temsil etmektedir.

NOT: Bu örnekte kullanılan tool Kali'de mevcut değildir. Sen sadece bilgi toplama aşamasında subdomain'lerin de böyle otomatik şekilde toplanması gerektiğini bil yeter. Eğer bu işi yapacak bir tool Kali'de ararsan dnsrecon ihtiyacına göre.

<http://tools.kali.org/information-gathering/dnsrecon>

b. Banner Yakalama (Banner Grabbing)

Çalışan servis hakkında detaylı bilgi almanın en basit yolu o porta telnet/netcat ile bağlanarak uygun komutu vermektir. Bazı servisler için herhangi bir komut vermenize gerek kalmadan gerekli bilgiyi size verir. Banner yakalama oldukça eski bir yöntemdir ve bilgi toplamanın ilk adımlarından sayılır.

i) Mail Sunucusunun Yazılımını Öğrenme

Mesela Microsoft.com sistemi üzerinde çalışan SMTP yazılımının ne olduğunu bulmaya çalışalım. Bunun için önce MX kaydını, yani mail sunucusunu bulmamız gerekir.

```
$ dig MX Microsoft.com
```

```
Output:
```

```
; <<>> DiG 9.3.3 <<>> MX microsoft.com
```

```
...
```

```
:: QUESTION SECTION:
```

```
;microsoft.com. IN MX
```

```
:: ANSWER SECTION:
```

```
microsoft.com. 2678 IN MX 10
```

```
mail.global.frontbridge.com.
```

```
...
```

Ardından bulunan SMTP sunucusunun, yani mail sunucusunun TCP/25 portuna telnet çekerek dönen banner'dan sunucunun kullandığı SMTP yazılımını öğrenebiliriz.

```
$ telnet mail.global.frontbridge.com. 25
```

```
Output:
```

```
Trying 216.32.181.22...
```

```
Connected to mail.global.frontbridge.com.
```

```
Escape character is '^]'.  
220 mail40-wa4.bigfish.com ESMTP Postfix EGG5 and  
Butter help
```

Görüldüğü üzere Microsoft'un mail'leri yönettiği ana MX sunucusu Postfix yazılımı üzerinde çalışıyormuş.

ii) Web Sunucularının Yazılımını Öğrenme

Web sunucularına gönderilen talepler sonucu dönen yanıtların başlık bilgisinden çoğu zaman web sunucunun kullandığı yazılım öğrenilebilmektedir. Örnek başlık bilgileri olarak aşağıdakiler verilebilir:

Apache kullanan sunucunun başlığı:

```
HTTP/1.1 200 OK
Date: Mon, 22 Aug 2005 20:22:16 GMT
Server: Apache/2.0.54
Last-Modified: Wed, 10 Aug 2005 04:05:47 GMT
ETag: "20095-2de2-3fdf365353cc0"
Accept-Ranges: bytes
Content-Length: 11746
Cache-Control: max-age=86400
Expires: Tue, 23 Aug 2005 20:22:16 GMT
Connection: close
Content-Type: text/html; charset=ISO-8859-1
```

IIS kullanan sunucunun başlığı:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 22 Aug 2005 20:24:07 GMT
Connection: Keep-Alive
Content-Length: 6278
Content-Type: text/html
Cache-control: private
```

Sun One kullanan sunucunun başlığı:

```
HTTP/1.1 200 OK
Server: Sun-ONE-Web-Server/6.1
Date: Mon, 22 Aug 2005 20:23:36 GMT
Content-length: 2628
Content-type: text/html
Last-modified: Tue, 01 Apr 2003 20:47:57 GMT
Accept-ranges: bytes
Connection: close
```

Eğer ki IIS kullanan ile Sun One kullanan'ların başlık bilgisinde Server header'ı olmasaydı bu ikisi arasındaki farka Content-Length ile Content-length'te L'lerin büyük ve küçük olma durumuna bakarak banner bilgisine vakıf olabilirdik.

Başlık bilgilerini nc ya da telnet komutlarını kullanıp hemen ardından

```
HEAD / HTTP/1.0
```

kodunu girerek öğrenebiliriz.

```
$ nc www.lifeoverip.net 80 -vv
```

```
www.lifeoverip.net [80.93.212.86] 80 -vv
```

```
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
```

```
Date: Sun, 29 Jul 2007 03:15:51 GMT
```

```
Server: Apache/2.2.4 (FreeBSD) DAV/2 mod_ssl/2.2.4  
OpenSSL/0.9.7e-p1
```

```
X-Pingback: http://blog.lifeoverip.net/xmlrpc.php
```

```
$ telnet www.ebay.com 80
```

```
Trying 66.135.208.88...
```

```
Connected to www.ebay.com.
```

```
Escape character is '^['.
```

```
HEAD / HTTP/1.0
```

```
HTTP/1.0 200 OK
```

```
Age: 44
```

```
Accept-Ranges: bytes
```

```
Date: Mon, 26 May 2003 16:10:00 GMT
```

```
Content-Length: 47851
```

```
Content-Type: text/html
```

```
Server: Microsoft-IIS/4.0
```

```
Content-Location: http://10.8.35.99/index.html
```

```
Last-Modified: Mon, 26 May 2003 16:01:40 GMT
```

```
ETag: "04af217a023c31:12517"
```

```
Via: 1.1 cache16 (NetCache NetApp/5.2.1R3)
```


Ekstra bilgi almak için telnet'ten sonra OPTIONS /HTTP/1.0 kodu girilebilir.

```
# telnet www.nasdaq.com 80
```

```
Trying 206.200.251.71...
```

```
Connected to www.nasdaq.com.
```

```
Escape character is '^['.
```

```
OPTIONS / HTTP/1.0
```

```
HTTP/1.1 200 OK
```

```
Allow: OPTIONS, TRACE, GET, HEAD
```

```
Content-Length: 0
```

```
Server: Microsoft-IIS/6.0
```

```
Public: OPTIONS, TRACE, GET, HEAD, POST
```

```
X-Powered-By: ASP.NET
```

```
Date: Sat, 08 Nov 2008 20:34:08 GMT
```

```
Connection: close
```

```
Connection closed by foreign host.
```

iii) SSH Sürümünü Sorgulama

```
C:\netcat>nc www.lifeoverip.net 2000 -vvv
```

```
www.lifeoverip.net [80.93.212.86] 2000 (?) open
```

```
SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110
```

NOT: Bu yöntem denediğim sitelerde işe yaramadı.

Diğer Bilgi Toplama Yöntemleri

a. Web Sayfası Yorum Satırlarından Bilgi Toplama

Bazen yazılımcılar geliştirme sürecinde kaynak koda çeşitli bilgiler yazarlar ve bunları sonra unuturlar. Buradaki notlar çok basit ve işe yaramaz olabileceği gibi yazılan uygulamaya ait username/password bilgilerini de barındırıyor olabilir.

```
File Edit View Help
this.a0 = new Array("username", "Kullanıcı Adı boş bırakılamaz.", new F
this.a1 = new Array("phoneNumber", "Kullanıcı Telefon Numarası boş bira
this.a2 = new Array("verifCode", "Onaylama Kodu boş bırakılamaz.", new
)

function userPasswordRemainderForm_mask () {
this.a0 = new Array("phoneNumber", "Geçersiz mobil numara formatı. Mobi
)

//End -->
</script>

<!-- End of Validator Javascript Function-->

</BODY>
</HTML>
<script language="JavaScript" type="text/JavaScript">
document.getElementsByName("username")[0].focus();
//document.getElementsByName("username")[0].value="admin";
//document.getElementsByName("password")[0].value="123456";
</script>
```

b. TCP Sequence Numarasını Tahmin Etme

Saldırgan aynı subnet'te olduğu kurbanın paketlerini izleyerek bir sonraki gönderilecek paketin TCP Sequence numarasını saptar ve bunun üzerine bir paket hazırlar. Bu paketin kaynak IP'sini kurbanınki, sequence numarasını ise kurbanın bir sonraki göndereceği pakete ait sequence numarasından yapar. Bu şekilde paketi hedefe yollar. Yani saldırgan kurbanın TCP Stream'ine bir enjeksiyon yapmış olur. Bu işlem hping tool'u ile yapılabilmektedir.

```
$ hping2 --seqnum -p 80 -S -i u1 192.168.1.1
```

```
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
1734626550 +1734626550
1733715899 +4294056644
1731604480 +4292855876
1736090136 +4485656
1730089804 +4288966963
1736532059 +6442255
1730574131 +4289009367
1735749233 +5175102
1725002138 +4284220200
1725076236 +74098
1729656540 +4580304
1721106365 +4286417120
1728255185 +7148820
1726183881 +4292895991
1722164576 +4290947990
```

1720622483 +4293425202

c. Hedef Sistemin Uptime Süresini Belirleme

Uptime demek sistemin açık kaldığı süre demektir. Şimdi www.ubys.net'in barındığı sunucunun ne kadar süredir açık durduğunu öğrenelim.

```
$ hping3 -S --tcp-timestamp -p 80 -c 2 www.ubys.net
```

Output:

```
HPING 1.2.3.488 (eth0 1.2.3.488): S set, 40 headers + 0 data bytes
```

```
len=56 ip=1.2.3.488 ttl=56 DF id=28012 sport=80 flags=SA seq=0  
win=65535 rtt=104.5 ms
```

```
TCP timestamp: tcpts=55281816  
len=56 ip=1.2.3.488 ttl=56 DF id=28013 sport=80 flags=SA seq=1  
win=65535 rtt=99.1 ms
```

```
TCP timestamp: tcpts=55281917  
HZ seems hz=100
```

System uptime seems: 53 days, 7 hours, 31 minutes, 6 seconds

```
--- 1.2.3.488 hping statistic ---  
2 packets tramitted, 2 packets received, 0% packet loss  
Round-trip min/avg/max = 99.1/101.8/104.5ms
```

NOT:

Cisco router'larda timestamp'i aşağıdaki şekilde aktif ve pasif hale getirebiliriz.

```
ip tcp timestamp           // aktif hale getirir  
no ip tcp timestamp        // pasif hale getirir.
```

d. Hedef Sistemin Saatini Öğrenme

Hedef sistemin saatini öğrenmenin çeşitli yolları vardır. Bu yöntemlerden en etkili olanları HTTP ve SMTP protokolleri üzerinden yapılır.

i) HTTP Protokolü İle Hedef Sistemin Saatini Öğrenme

telnet ile 80 portuna bağlantı kurup

HEAD / HTTP/1.1

yazarsak hedef sistemin saatini öğrenebiliriz.

```
$ telnet mail.lifeoverip.net 80
```

Output:

```
Trying 80.93.212.86...
Connected to mail.lifeoverip.net.
Escape character is '^]'.
```

```
HEAD / HTTP/1.1
```

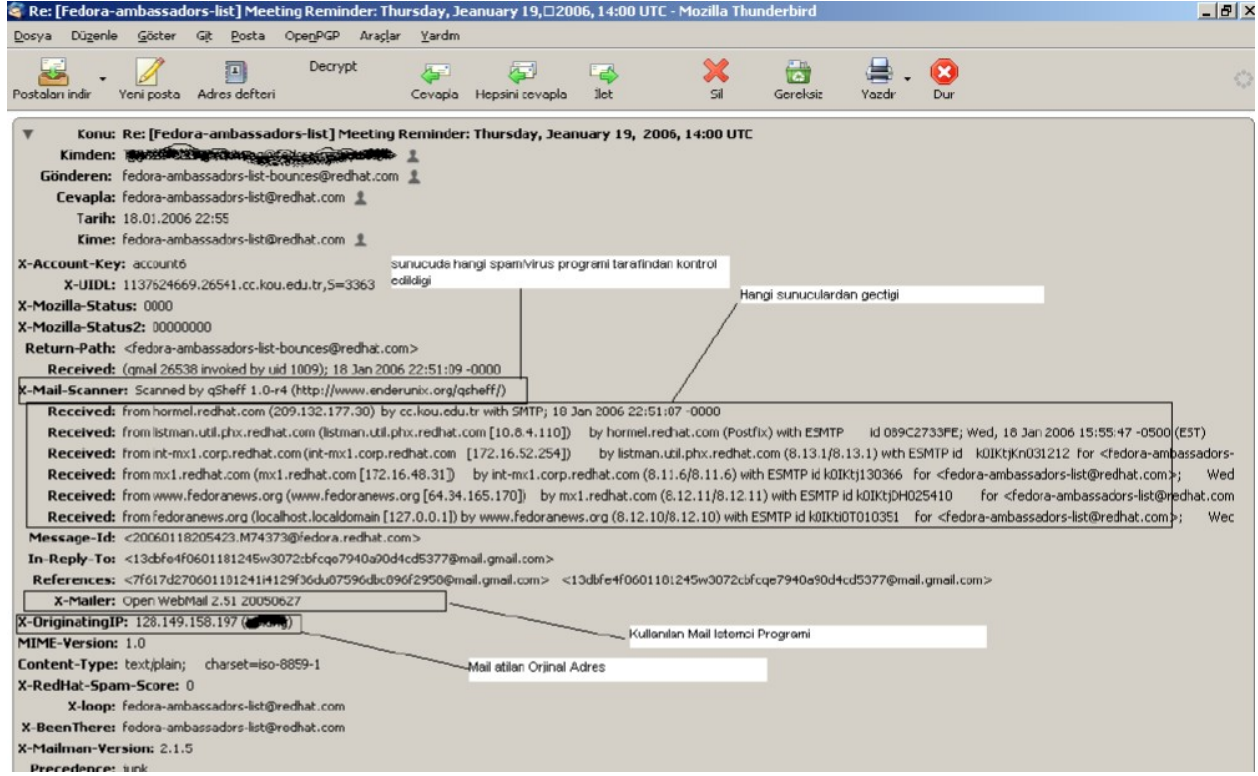
```
HTTP/1.1 400 Bad Request
Date: Mon, 28 Jan 2008 17:49:06 GMT
Server: Apache/2.2.4 (FreeBSD) DAV/2 mod_ssl/2.2.4
OpenSSL/0.9.7e-p1
Connection: close
Content-Type: text/html; charset=iso-8859-1
Connection closed by foreign host.
```

ii) SMTP Protokolü İle Hedef Sistemin Saatini Öğrenme

Hedef sistemin üzerinde bir SMTP sunucusu, yani mail sunucusu çalışıyorsa bu durumda sunucuda kayıtlı olmayan bir mail adresine mail gönderip dönen hata mesajının başlıkları incelenerek hedef sistemin saati öğrenilebilir.

e. Eposta Başlıkları Aracılığıyla Bilgi Edinme

Mail başlıklarını doğru okuyabilmek forensic analiz ve bilgi toplama açısından oldukça önemlidir. Üzerinde dikkatle uğraşılmamış bir mail takip edilerek sahibine ait oldukça detaylı bilgiler edinilebilir.



From:

Mail'in kimden geldiğini gösteren elemandır. Kolaylıkla manipüle edilerek karşı tarafa mail'in başkasından geldiği yönünde aldatma yoluna gidilebilir.

Reply-To:

Dönen cevabın hangi adrese gönderileceğini bildirir.

Return-path

Reply-To benzeri bir başlıktır.

Received

Received başlığı mail iletişimi sırasında mail'in hangi ara sunuculardan geçtiği bilgisini verir. Verdiği detaylı

ve gerçekçi bilgidan dolayı önemli bir eposta başlığıdır. Yukarıdaki resimde Received kısmını yukarıdan aşağıya doğru okuyarak mail'in sırayla hangi SMTP sunucularından geçtiği tespit edilebilir.

Recipient Host

Mail'i teslim alan kişi bilgisini barındırır.

İstemci ve mta (message transfer agent) yazılımı harici yardımcı yazılımların eklediği başlıklar gerçek başlık değerleri ile karışmaması için X- ile başlar.

f. SMTP Üzerinden Ağ Topolojisi Çıkarma

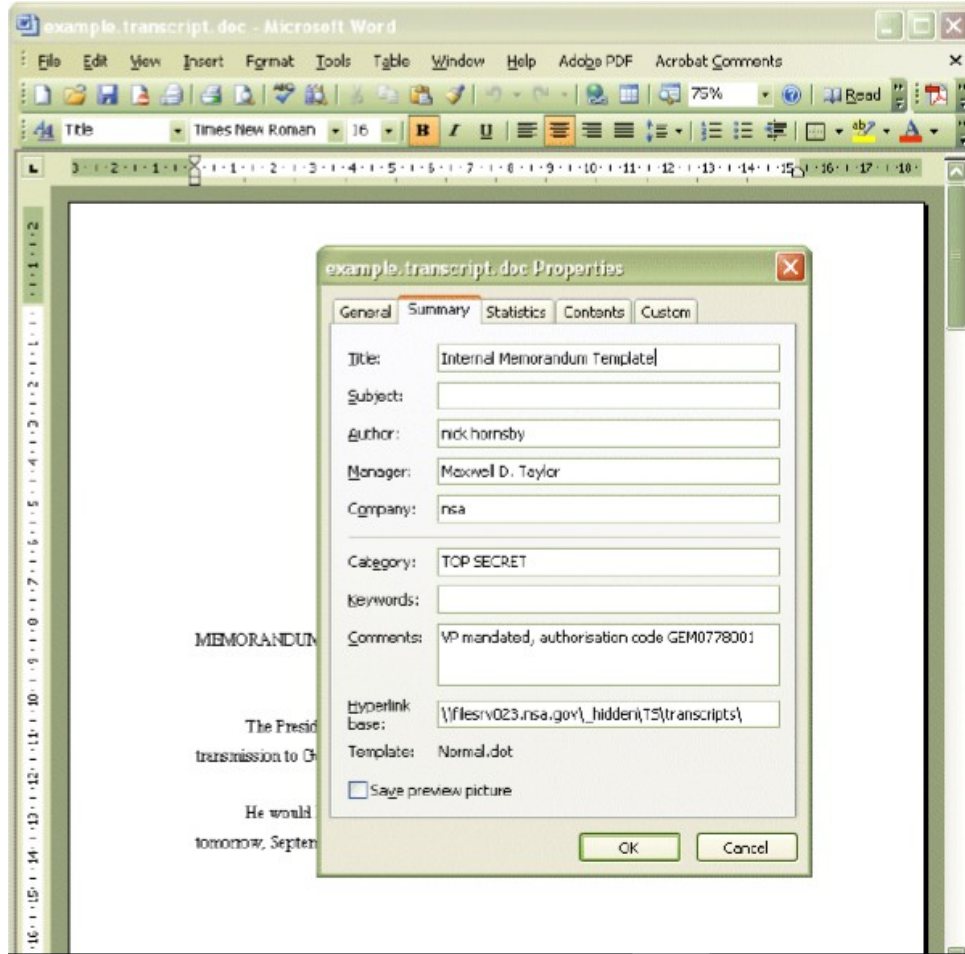
SMTP yazılımları eğer özel olarak düzenlenmemişse buldukları ağ hakkında oldukça fazla bilgi verirler. Bu bilgilerden biri de hedef ağın haritasıdır. Aşağıdaki çıktı bir e-posta listesine gönderilen mailden alıntılanmıştır ve açıkça görüleceği üzere - iç ağ ip adresleri de dahil olmak üzere - hedef sistemin ağ yapısını ortaya çıkarmaktadır.

```
Received-SPF: pass (google.com: domain of sentto-8295402-1229-1217329328-huzeyfe.onal@gmail.com@returns.groups.yahoo.com designates 66.163.168.185 as permitted sender)
DomainKey-Status: good
Authentication-Results: mx.google.com; spf=pass (google.com: domain of sentto-8295402-1229-1217329328-huzeyfe.onal@gmail.com@returns.groups.yahoo.com designates 66.163.168.185 as permitted sender)
Comment: DomainKeys? See http://antispam.yahoo.com/domainkeys
DomainKey-Signature: a=rsa-sha1; q=dns; c=noftvs; s=lima; d=yahogroups.com;
    b=USSHE30SSk7firUSDba18J3zEzNTqlx0B3aa4zuFiIvaihFBEPiR7GoOKwnOH+2fd5Lct/j4SdxW8mEeKvu1SHZ8F6e1RJK18vntT/XAe2E5M2La0BwKMUWzps/xrt8hZ;
Received: from [216.252.122.216] by n51.bullet.mail.sp1.yahoo.com with NNFP; 29 Jul 2008 11:02:09 -0000
Received: from [66.218.69.6] by t1.bullet.sp1.yahoo.com with NNFP; 29 Jul 2008 11:02:09 -0000
Received: from [66.218.67.91] by t6.bullet.scd.yahoo.com with NNFP; 29 Jul 2008 11:02:09 -0000
X-Yahoo-Newman-Id: 8295402-m1229
Received: (qmail 58228 invoked by uid 7800); 29 Jul 2008 11:02:04 -0000
X-Sender:
X-Apparently-To: bilgiguvenligi@yahoo.com
X-Received: (qmail 90819 invoked from network); 29 Jul 2008 08:51:55 -0000
X-Received: from unknown (66.218.67.96)
    by m14.grp.scd.yahoo.com with QWOP; 29 Jul 2008 08:51:55 -0000
X-Received: from unknown (HELO NEWW.turkcell.com.tr) (212.252.168.230)
    by m1a17.grp.scd.yahoo.com with SMTP; 29 Jul 2008 08:51:53 -0000
X-Received: from exi3401.turkcell.entp.tgc ([10.200.123.125]) by NEWW.turkcell.com.tr with InterScan Message Security Suite; Tue, 29 Jul 2008 11:54:30 +0300
X-Disclaimer-Added-By: turkcell.com.tr
X-Received: from HUB3401.turkcell.entp.tgc ([10.200.123.127]) by exi3401.turkcell.entp.tgc with Microsoft SMTPSVC(6.0.3790.3959); Tue, 29 Jul 2008 11:51:52 +0300
Importance: normal
Priority: normal
X-Received: from exhmbx03.turkcell.entp.tgc ([10.200.125.25]) by HUB3401.turkcell.entp.tgc with Microsoft SMTPSVC(6.0.3790.3959); Tue, 29 Jul 2008 11:51:52 +0300
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.3959
Content-class: urn:content-classes:message
Message-ID: <f802d73cd4cad440af999db0a27551fa032c9337@exhmbx03.turkcell.entp.tgc>
In-Reply-To: <66024ce0807271402i701da05f1d1b17e403b535de5@mail.gmail.com>
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
Thread-Topic: =?iso-8859-9?Q?=5Bbilgiguvenligi=5D_TI_6ns_a=E7=FD=FD=FD?=>
```

Eğer başlık Received olsaydı bu durumda derdik ki ara SMTP sunuculardan geçiyor. Fakat dikkat ederseniz vurgulanmış başlıklar X-Received'dir. Demek ki SMTP sunucusu kendi network'ündeki ara yazılımlar içeren makinelerden mail'i geçiriyor. Bu sayede SMTP sunucusunun yer aldığı network hakkında bilgi toplanmış olur.

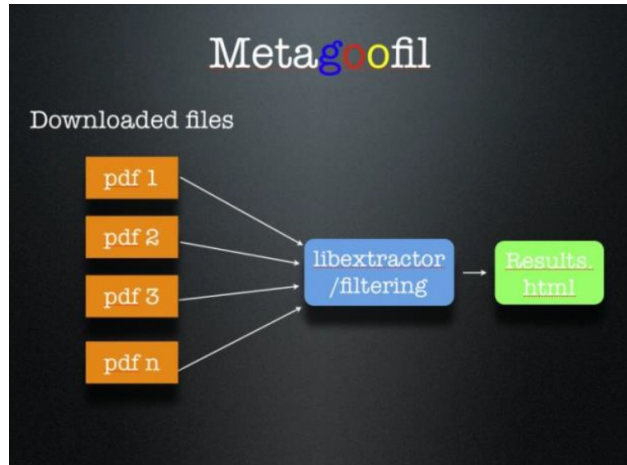
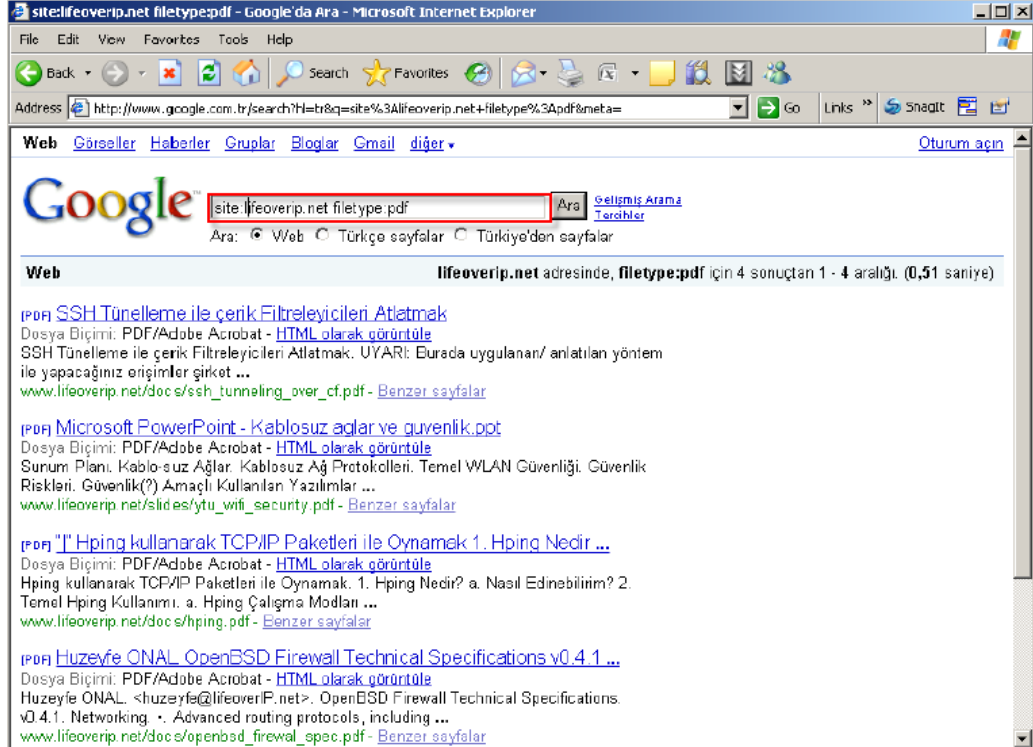
g. İnternette İndirilen Dosyalar Üzerinden Bilgi Toplama

Bu yöntem özelde office dosyaları için kullanılsa da genelde tüm metadata içeren belgeler için geçerlidir. Örneğin bir word belgesi hazırlayan kimse gereğinden fazla detay veri dökümana metadata olarak aşağıdaki resimde olduğu gibi ekleyebilir. Bu şekilde internete servis edilen dökümanı inceleyen bir kimse hedef hakkında kritik bilgilere kavuşabilir.



h. Metagoofil Aracı İle Bilgi Toplama

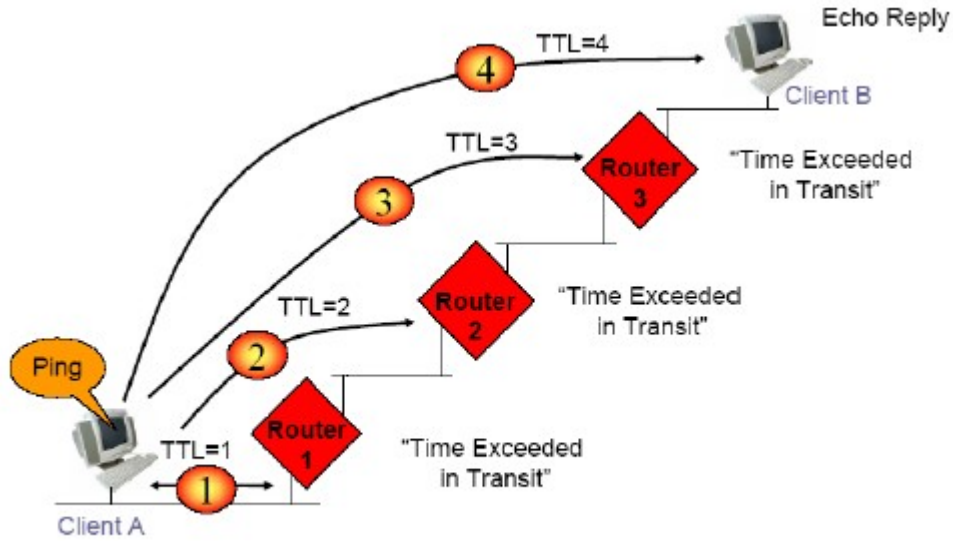
Metagoofil tool'u google aracılığı ile çeşitli dökümanları (pdf, doc, jpg) araştırıp bunların üzerinde normalde görünmeyen metadata bilgilerini ayrıştırır ve raporlar. Çalışma şekli şöyledir: Öncelikle google'a dork girer ve bulduğu dökümanları indirir. Ardından indirdiği dökümanları bir süzgeçten geçirip metadata'ları ayrıştırarak html olarak raporlar.



i. Ağ Haritalama Yöntemi İle Bilgi Toplama

I) Traceroute

Traceroute tool'u paketin hedefe giderkenki uğradığı router'ların tespit eder. Bunu şöyle yapar. Öncelikle TTL değeri 1 olan paketi hedefe doğru gönderir. TTL değeri 1 olduğu için denkle geldiği ilk router TTL değerini azaltacaktır ve TTL değeri 0 olacağı için paketi düşürecektir. Geri bildirim olarak da TTL Expired cevabını göndericiye gönderecektir. Böylece yol üstündeki ilk router'ı öğrenmiş olduk. Ardından TTL değeri 2 olan paket gönderilir ve bu paket yol üstündeki 2nci Router tarafından düşürülerek gelen bildirim ile 2nci router'ı da tespit etmiş oluruz. Bu böyle devam eder. Böylelikle yol üstündeki tüm router'ları tespit etmiş oluruz.



II) TcpTraceroute

*Linux ve Windows sistemlerinde trace tool'u farklı protokolleri kullanmaktadır.

*Hedef sistemde icmp ve udp portları kapalı ise klasik traceroute çalışmaları sağlıklı sonuçlar vermeyecektir.

*Hedef sistem üzerinde açık bir port üzerinden TCPTraceroute çalıştırsak yol üstündeki router'ları ve "sistem önündeki güvenlik duvarını" belirleyebiliriz. Güvenlik duvarını anlamak için bir traceroute tool'u ile yol üstündeki cihazların tespit sonucuna bak bir de tcptraceroute tool'u ile yol üstündeki cihazların tespit sonucuna bak.

Hedef sisteme yapılan klasik bir traceroute çalışması sonucu çıktı:

\$ traceroute www.open.edu.tr

traceroute to www.open.edu.tr (111.112.113.114), 64 hops max, 40 byte packets

```
1 172.16.10.1 (172.16.10.1) 0.599 ms 0.522 ms 0.333 ms
2 1.2.3.41 (1.2.3.41) 0.823 ms 0.711 ms 1.169 ms
3 193.255.0.61 (193.255.0.61) 51.837 ms 61.271 ms 67.060 ms
4 195.175.51.65 (195.175.51.65) 71.319 ms 77.868 ms 77.057
5 * 212.156.118.161 (212.156.118.161) 459.421 ms 667.286 ms
6 212.156.118.5 (212.156.118.5) 66.180 ms 65.540 ms 58.033
7 212.156.118.38 (212.156.118.38) 69.980 ms 212.156.118.21
8 * * *
9 212.156.117.146 (212.156.117.146) 107.342 ms 94.551 ms
10 usr-4993.dial-in.ttnet.net.tr (212.156.147.130) 55.633 ms
63.031 ms 77.537 ms
11 * * *
12 * * *
13 * *
```

Hedef sisteme yapılan klasik bir TCPtraceroute çalışması sonucu çıktı:

\$ tcptraceroute www.open.edu.tr 80

Selected device fxp0, address 172.16.10.2, port 58582 for outgoing packets

Tracing the path to www.open.edu.tr (111.112.113.114) on TCP port 80, 30 hops max

```
1 172.16.10.1 (172.16.10.1) 0.872 ms 9.832 ms 9.905 ms
2 1.2.3.41 (1.2.3.41) 9.925 ms 0.721 ms 9.741 ms
3 193.255.0.61 (193.255.0.61) 83.745 ms 31.317 ms 27.939 ms
4 195.175.51.65 (195.175.51.65) 25.453 ms 28.686 ms 28.104
5 212.156.118.161 (212.156.118.161) 384.850 ms 742.354 ms
6 212.156.118.5 (212.156.118.5) 18.064 ms 24.648 ms 23.109
7 212.156.118.21 (212.156.118.21) 32.347 ms 48.208 ms
8 212.156.117.10 (212.156.117.10) 61.678 ms 54.749 ms
9 212.156.117.146 (212.156.117.146) 73.028 ms 97.067 ms
10 usr-4993.dial-in.ttnet.net.tr (212.156.147.130) 112.622 ms
ms 75.954 ms
11 111.112.113.114 (111.112.113.114) 64.054 ms 46.363
ms 43.193 ms
12 111.112.113.114 (111.112.113.114) [open] 52.160 ms
44.720 ms 31.919 ms
```

Yukarıdaki kırmızı ile vurgulanmış son iki satıra dikkat edecek olursan aynı adres iki kere TTL Expired cevabı vermiş. Bu, hedef sistemin önünde NAT yapan bir güvenlik duvarının çalıştığını gösterir.

j. SNMP Üzerinden Bilgi Toplama

SNMP ağ cihazlarında yönetimsel türden bilgi alışverişlerinin yapılabilmesi için oluşturulmuş bir uygulama katmanı protokolüdür. Ağ yöneticilerinin ağ performansını arttırmasına, ağ problemlerini bulup çözmesine ve ağlarda genişleme durumu söz konusu olduğunda planlama yapabilmelerine olanak sağlar.

Snm aracılığıyla bir sistemden her türlü bilgi edinilebilir.

```
$ perl snmpenum.pl 192.168.2.20 public windows.txt
```

```
-----  
INSTALLED SOFTWARE  
-----
```

```
hMailServer 4.4.3-B285  
Update for Windows Server 2003 (KB911164)  
Microsoft .NET Framework 2.0  
Microsoft SQL Server 2005  
..
```

```
-----  
HOSTNAME  
-----
```

```
LIFEOVER-W2K3
```

```
-----  
USERS  
-----
```

```
Guest  
honal  
krbtgt  
Administrator  
SUPPORT_388945a0  
IUSR_LIFEOVER-W2K3  
IWAM_LIFEOVER-W2K3  
....  
-----
```

RUNNING PROCESSES

System Idle Process
System
appmgr.exe
dfssvc.exe
dns.exe
elementmgr.exe
svchost.exe

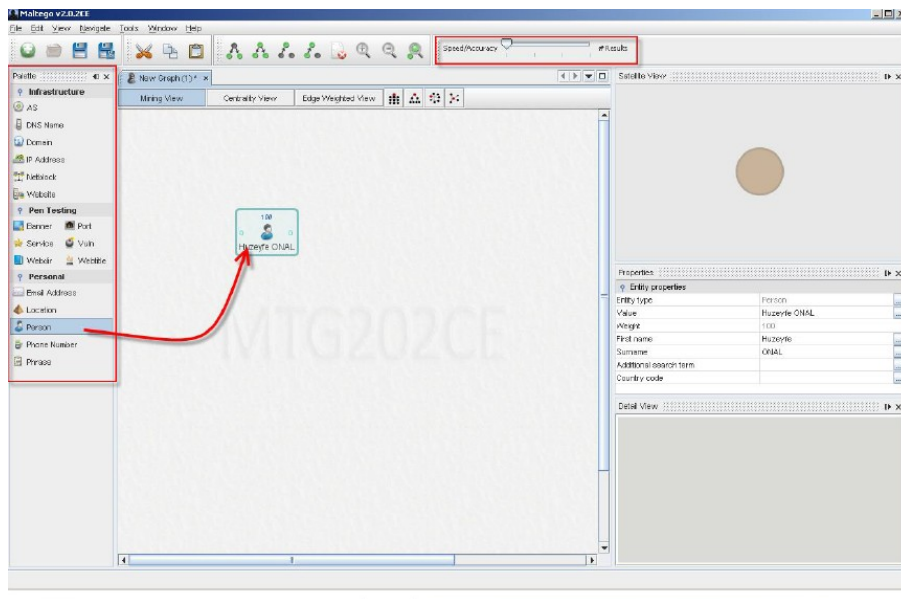
Dmitry İle Bilgi Toplama

Dmitry tool'u ile verilen bir domain/ip adresi hakkında whois sorgusu, Netcraft'tan alınma bilgiler, subdomain bilgileri, o domain'e ait eposta adresleri, açık TCP portları ve bu portlarda çalışan servislere ait banner bilgileri alınabilmektedir. Yani kısacası buraya kadar ayrı ayrı yaptığımız bu işlemleri tek bir tool ile yapabilmekteyiz.

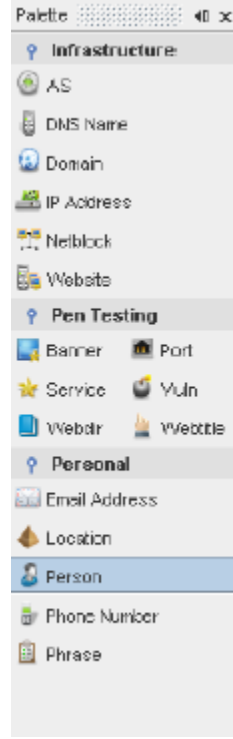
```
$ dmitry -winsefb www.lifeoverip.net -o rapor.txt // Tüm bulduğu veriler  
// rapor.txt'e yazılır
```

Yeni Nesil Bilgi Toplama Aracı (Maltego)

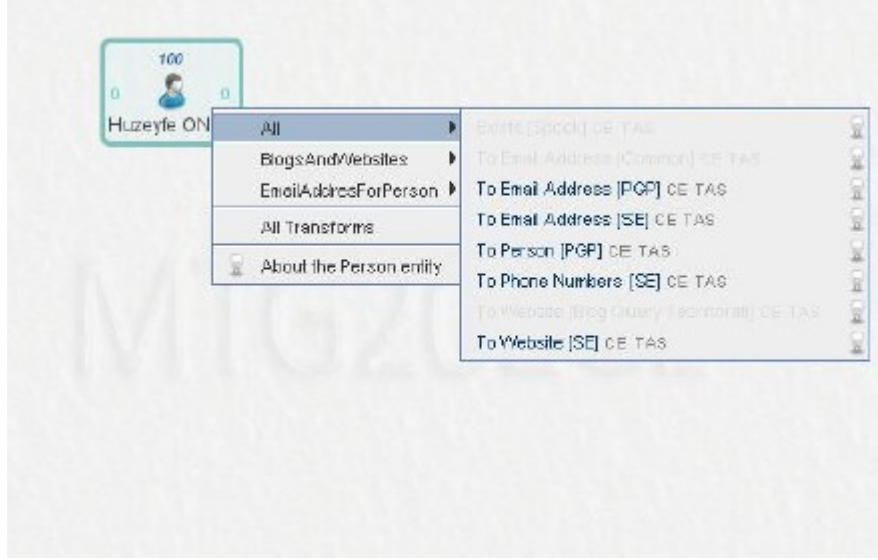
Maltego, bildiğimiz tüm klasik bilgi toplama yöntemlerini birleştirerek merkezi bir yerden kontrol ve raporlama imkanı sunar. Bu sebeple yeni nesil (ikinci nesil) bilgi toplama aracı olarak sınıflandırılır.



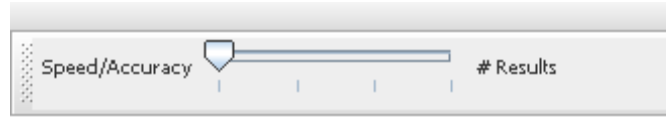
Yukarıdaki resmin sol tarafındaki menüden arama kriterleri belirlenir. Sol menüdeki arama kriterleri şunlardır:



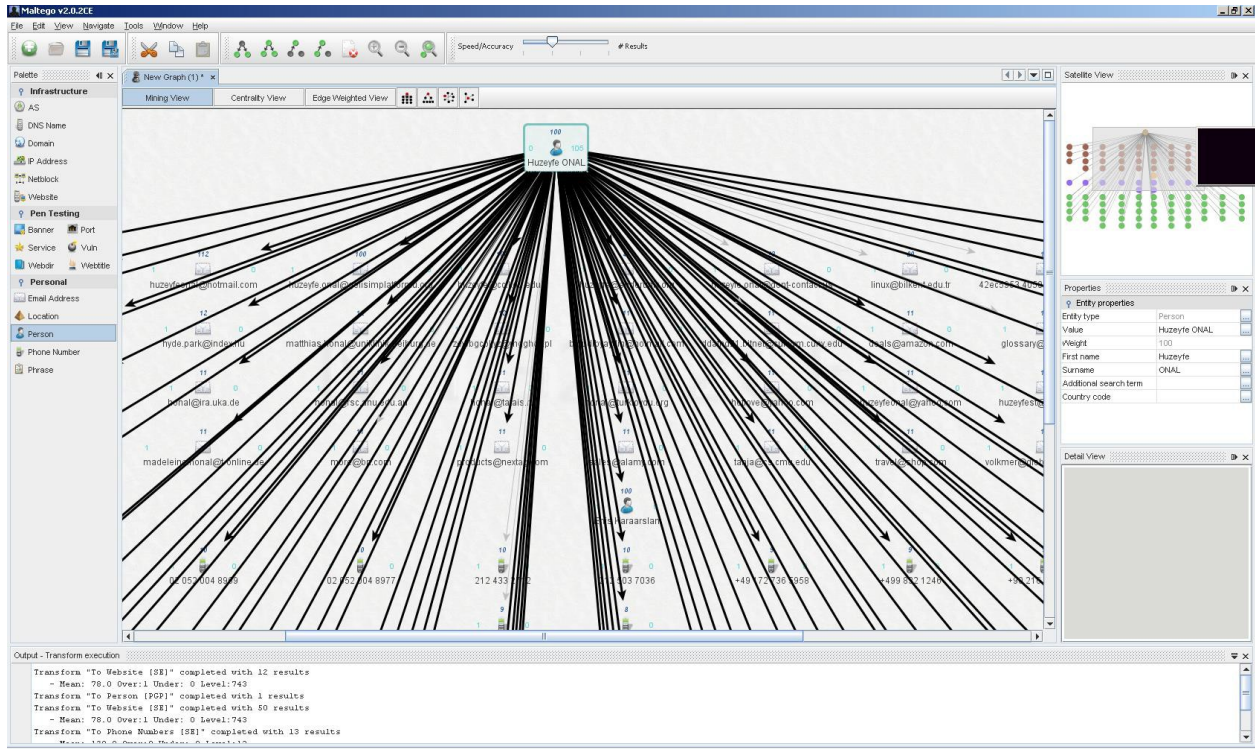
Belirlenen arama kriteri ekranın ortadaki bölümüne doğru sürüklenir. Sonra ortadaki alanda arama yapılacak kritere ait özellikler simgeye çift tıklayarak girilir ve son olarak da simgenin üzerine sağ tıklayıp ne tür aramalar yapılsın bilgisi seçilir.



Arama sonuçlarını ilgilendiren önemli bir husus aramanın hızlı bir arama mı yoksa yavaş bir arama şeklinde olacağıdır. Hızlı arama çabuk sonuç döner fakat çok sağlıklı olmaz. Yavaş arama ise sağlıklı sonuçlar döner fakat çok uzun sürebilir. Dolayısı ile Speed/Accuracy değerini ortada tutmak uygun bir çözüm olacaktır.



Arama sonrası sonuçlar orta ekranda gösterilecektir. Herhangi bir sonuç objesi üzerine gelirse o objeye ait özellikler ekranın sağ kısmında belirir.



<http://blog.btpro.net/aktif-bilgi-toplama/>