Güvenlik Testlerinde Bilgi Toplama

Huzeyfe ÖNAL <huzeyfe@bga.com.tr>

[Bu yazı sızma testlerinde hedef sistemler hakkında detay bilgi toplama yöntem ve araçlarının kullanımını içermektedir. Dökümanın yazım tarihi 2010 yılı olup eski bilgiler içerebilir.]

GÜVENLİK TESTLERİNDE BİLGİ TOPLAMA

Bilgi Neden Değerlidir?

Günümüz dünyasında en değerli varlıklardan biri "bilgi" dir. Bu bilgi kimi zaman bir mal üretmek için kimi zaman da üretilen mala ait detayların, formüllerin saklanması için kullanılabilir. Bilgisayar dünyasında ise bilgi her şey demektir. Tüm iletişimin sayısal olarak gerçeleştiğini düşünülürse her bilgi bir sayısal veridir ve meraklı gözlerden korunmalıdır.

Güvenlik Testlerinde Bilginin Önemi

Güvenlik testlerinde bilgi toplama en önemli adımdır. Yeterli düzeyde toplanmayan veri istenilen sonuçları çıkaramaz. Bilgi toplama esnasında bu gerekli mi değil mi diye sorulmadan alınabilecek tüm bilgiler alınmalı ve bu bilgiler sonraki aşamalarda kullanılmak üzere sınıflandırılmalıdır.

Bilgi Toplama Yöntemleri

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

1. **Pasif Bilgi Toplama**
2. **Aktif 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.

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 ;

Bir IP adresine ait bilgilere en kısa yoldan whois sorgusu ile erişilebilir.

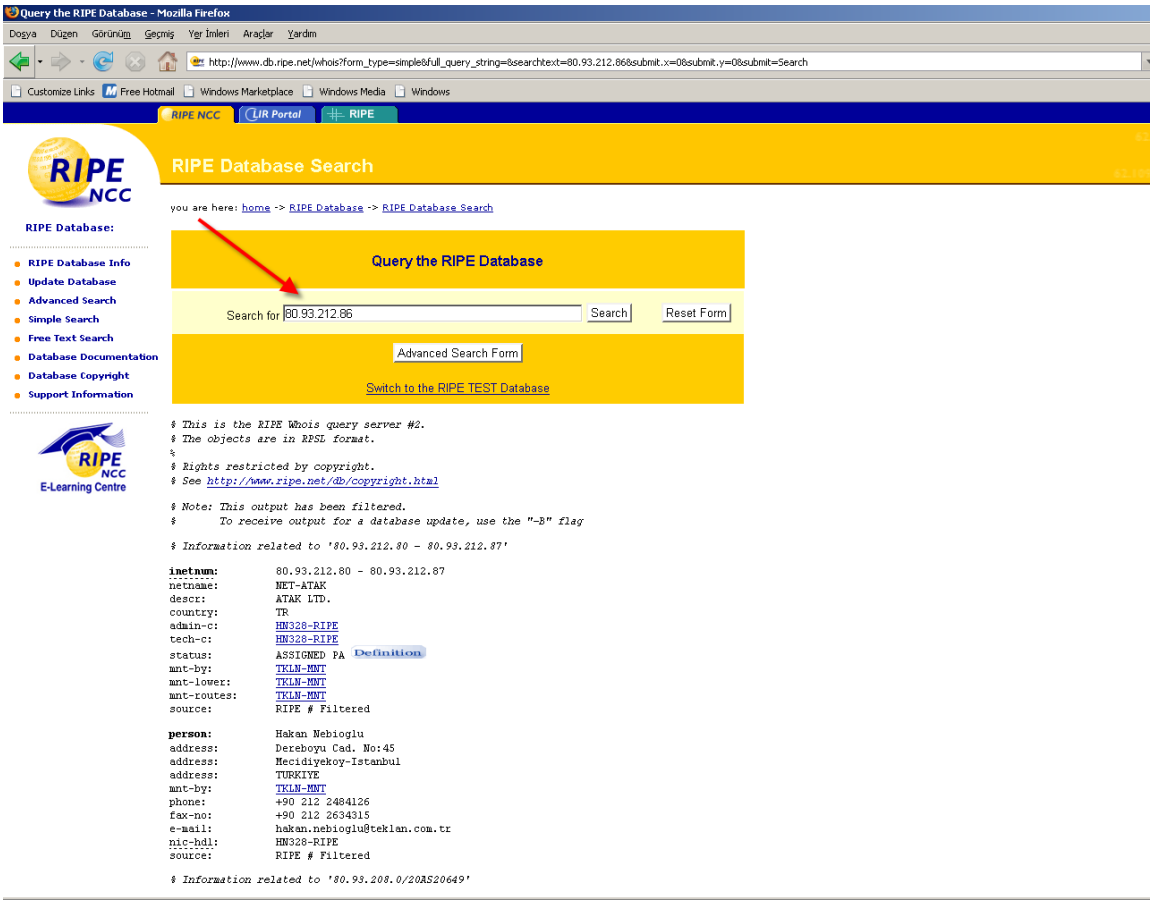
```
# whois 194.27.72.88

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
Parent:
```

```
NetType:    Allocated to RIPE NCC
NameServer: NS-PRI.RIPE.NET
NameServer: NS3.NIC.FR
NameServer: SUNIC.SUNET.SE
NameServer: NS-EXT.ISC.ORG
NameServer: SEC1.APNIC.NET
NameServer: SEC3.APNIC.NET
NameServer: TINNIE.ARIN.NET
Comment:    These addresses have been further assigned to users in
Comment:    the RIPE NCC region. Contact information can be found in
Comment:    the RIPE database at http://www.ripe.net/whois
RegDate:    1993-07-21
Updated:    2005-08-03

# ARIN WHOIS database, last updated 2008-12-04 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '194.27.72.0 - 194.27.72.255'

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 Binasi 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
```

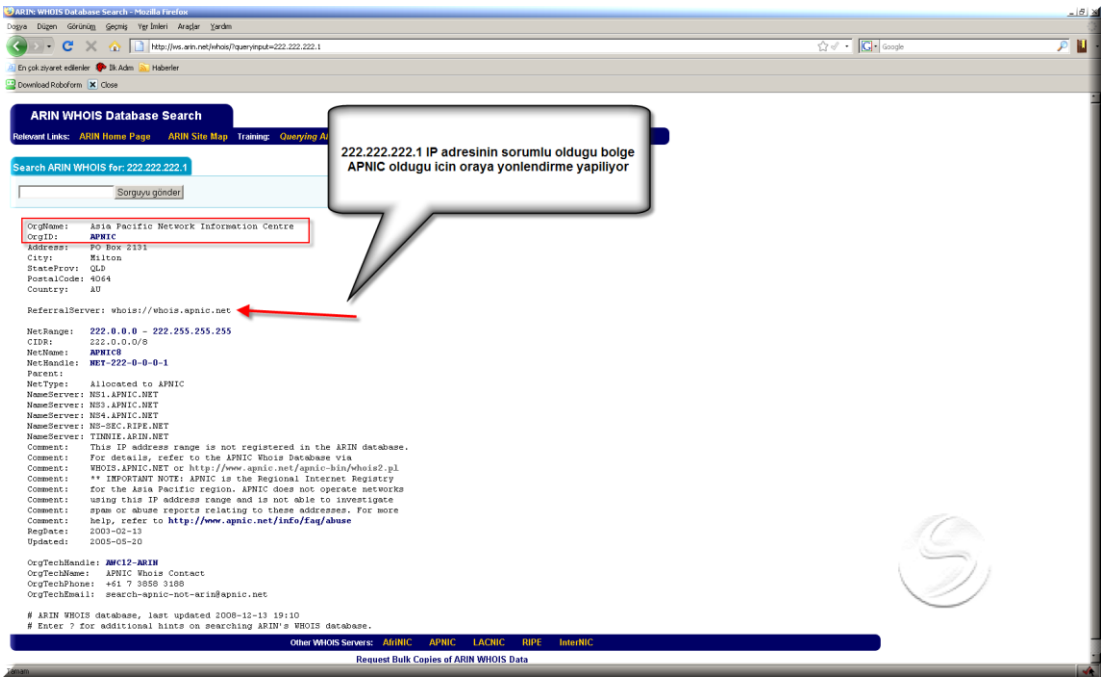
```
source:       RIPE # Filtered

person:      Omur Can
address:     Kocaeli Universitesi
address:     Bilgi Islem Dairesi
address:     Izmit
address:     Turkiye
phone:       +90 262 3313912
fax-no:      +90 262 3313912
nic-hdl:     OC222-RIPE
source:      RIPE # Filtered
```

whois servisi TCP/43 portundan çalışmaktadır ve çoğu sistemde bu port dışarıya doğru açık değildir. Bu sebeple whois hizmetini genelde whois proxyler üzerinden alırız. Whois proxyler basit birer web sayfasıdır ve kullanıcıdan aldığı sorgulamaları whois sunuculara göndererek sonucu kullanıcıya gösterir.

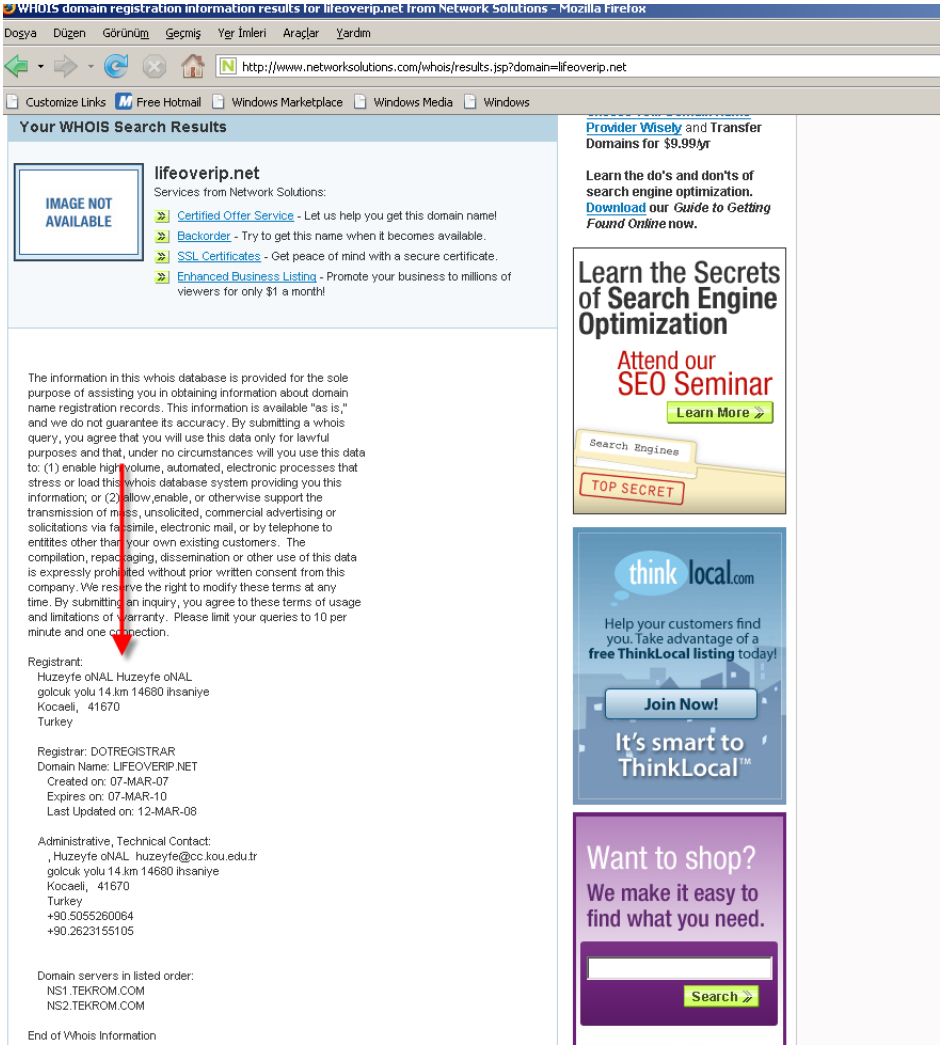
Ripe Üzerinden IP Adresi sorgulama



NOTE: ARIN üzerinden yapılacak IP adresi sorgulamaları eğer ARIN'in kontrolünde değilse size ilgili RIR'in bilgilerini verecektir. Eğer bir IP adresinin hangi bölgede olduğunu bilmiyorsanız ilk olarak ARIN üzerinden sorgulama yaparak hangi whois sunucularda barındığını öğrenebilisiniz

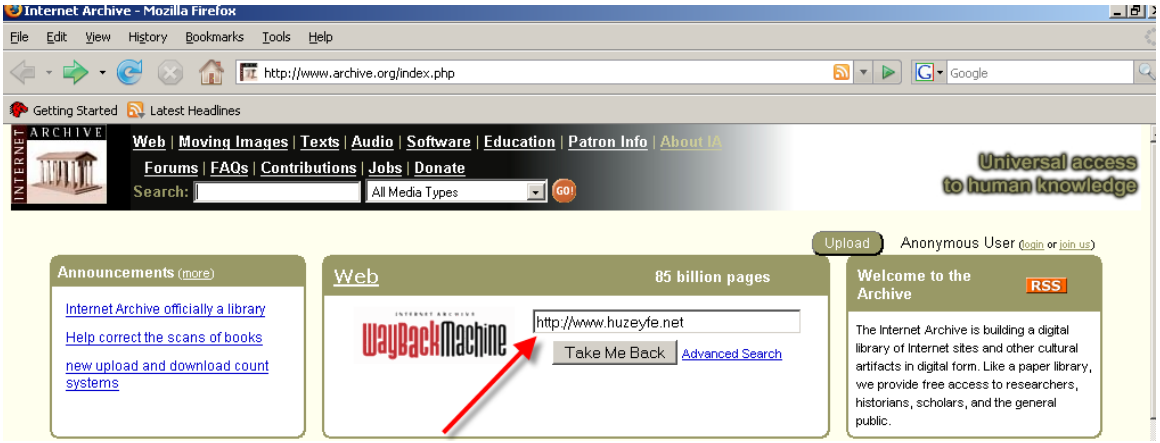


NetworkSolutions Üzerinden Domain Sorgulama

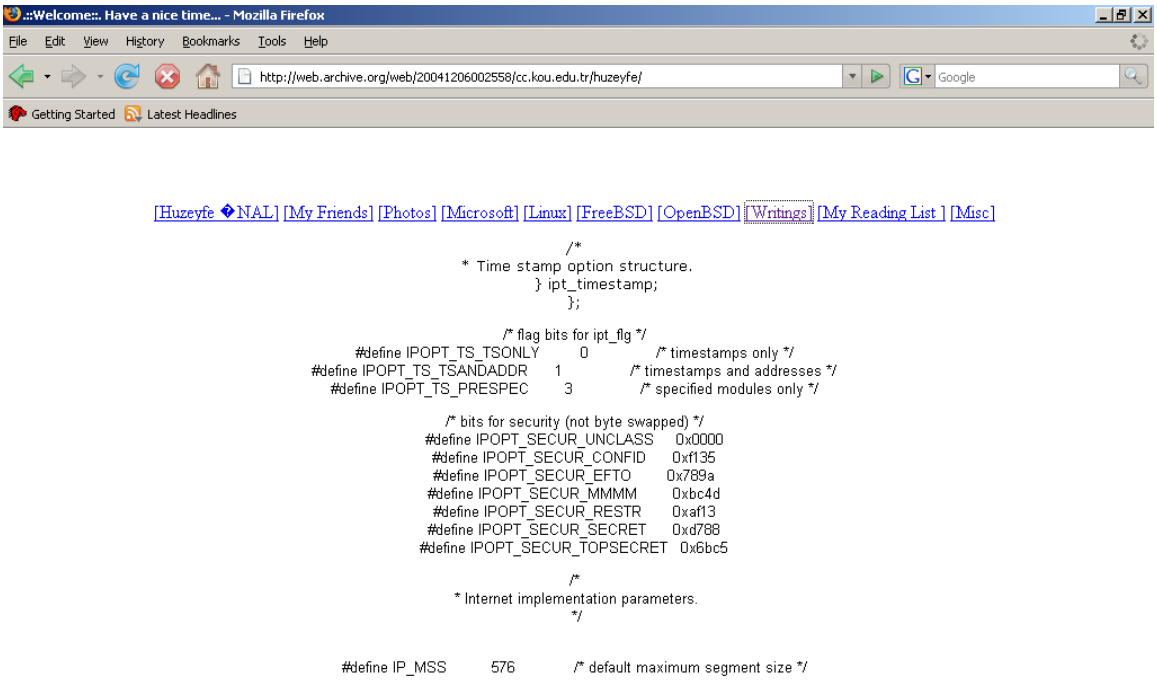


Web Sayfalarının Geçmişini İzleme

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

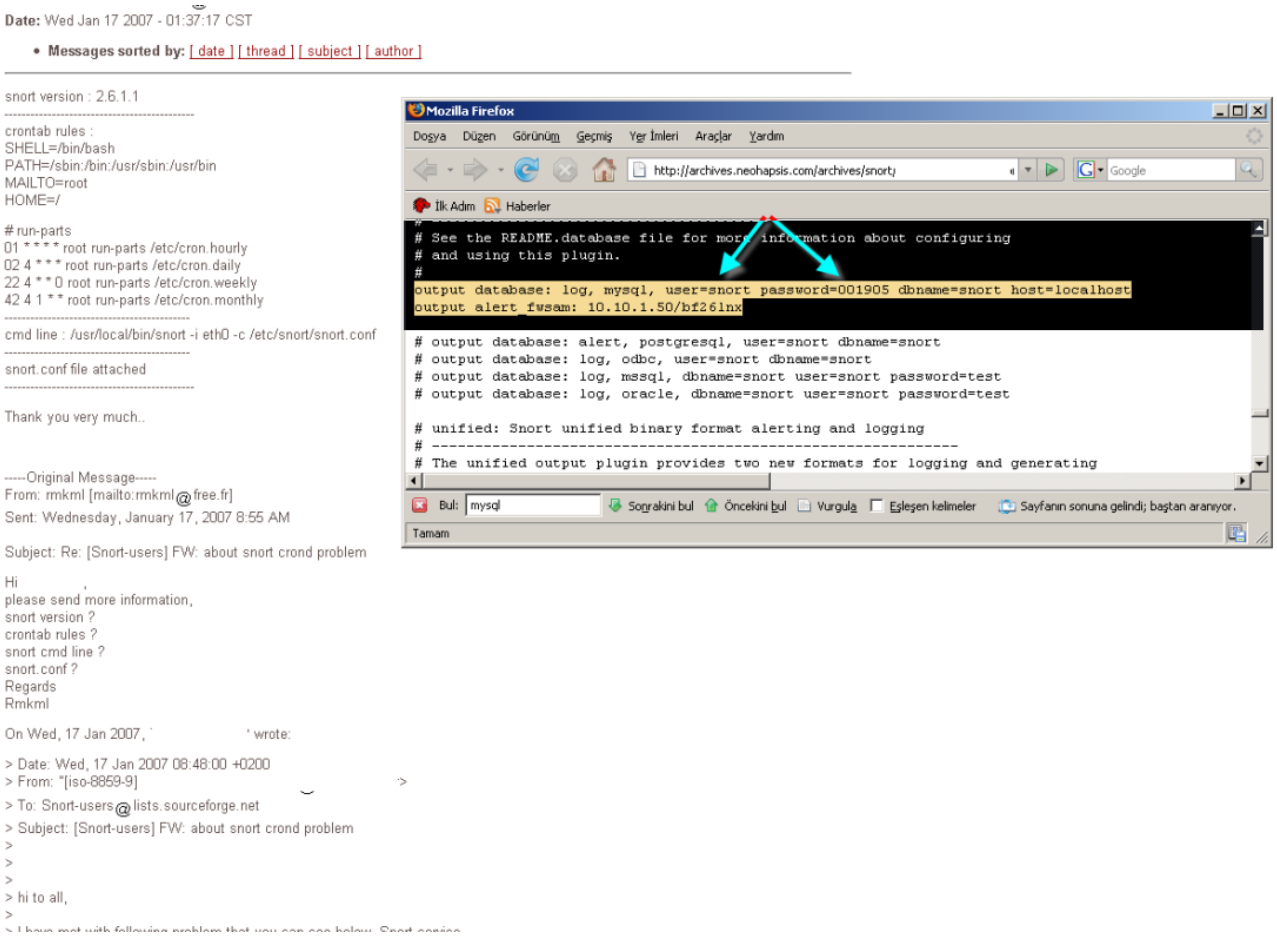


Mesela huzeyfe.net'i sorguladığınızda bu domaine ait hangi devierlerde arşiv alınmış bilgisi ve bu dönemlere ait sitenin görünümünü elde edilebilir.



E-posta Listeleri Arşivleri Aracılığı İle Bilgi Toplama

Ekteki ekran görüntüsü listelere bilgi alma amacı ile sorulan bir sorudan alınmıştır. Soruyu soran detay bilgi olması açısından kullandığı yazılımın yapılandırma dosyasını da göndermiş fakat dosya içerisinde uygulamanın çalışması için gerekli şifreyi silmeyi unutmuştur. Şifre kısmı incelendiğinde maili gönderen kişinin Beşiktaşlı biri olduğu ve şifreleme profili arasında tuttuğu takımın rakkamlarının yer aldığı görülebilir.



Netcraft Aracılığı ile Bilgi Toplama

Netcraft, işletim sistemi, kernel versiyonu ve web sunucu olarak çalışan yazılıma ait detaylı bilgilerin yanı sıra sistemin uptime bilgisini gösterebilen bir sayfadır.

Netcraft nasıl çalışır?

Netcraft hedef sistemin yazılım bilgilerini belirlemek için httprint 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 aracılığı ile Bilgi Toplama

Sorgulanan sisteme ait geçmiş bilgiler(hangi işletim sistemi vs) de yer almaktadır.

Resimde göreceğiniz örnek FreeBSD çalışan bir sunucunun Linux'a geçiş aşamasını belgeliyor. X tarihine kadar FreeBSD üzerinde çalışırken Y tarihinden sonra Linux sistem üzerinde çalışmaya başlamıştır.

Site report for www.gezginler.net

Site	http://www.gezginler.net	**Last reboot**	unknown Uptime graph
Domain	gezginler.net	**Netblock owner**	SoftLayer Technologies Inc.
IP address	74.86.29.219	**Site rank**	90346
Country	US	**Nameserver**	ns1.gezginler.net
Date first seen	March 2002	**DNS admin**	uyduruk@gmail.com
Domain Registry	OnlineNIC.com	**Reverse DNS**	gezginler.net
Organisation	gezginler.net Marmara, Istanbul, 80870, Turkey	**Nameserver Organisation**	gezginler.net Marmara, Istanbul, 80870, Turkey
Check another site:		**Netcraft Site Report Gadget**	Add to Google [More Netcraft Gadgets]

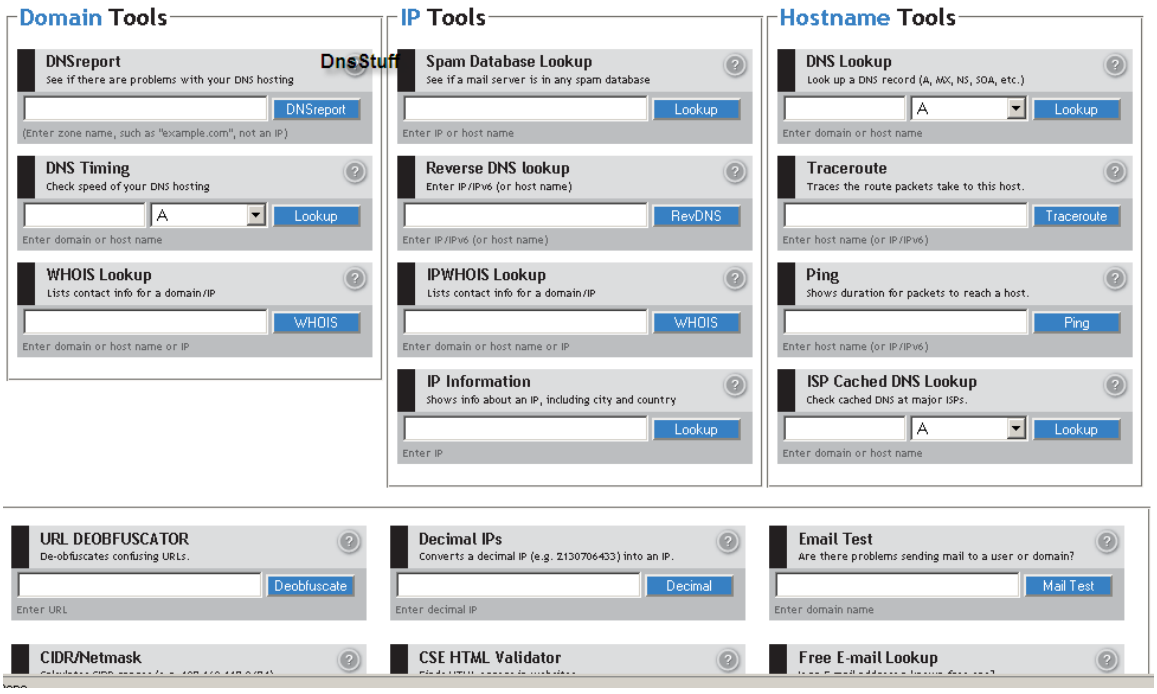
Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	74.86.29.219	Linux	Apache/1.3.37 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.7 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.28 OpenSSL/0.9.7a	4-Jul-2007
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	74.86.29.219	Linux	Apache/1.3.37 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.7 FrontPage/5.0.2.2635.SR1.2	2-Jul-2007
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	74.86.29.219	Linux	Apache/1.3.37 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.7 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.28 OpenSSL/0.9.7a	24-Jun-2007
Layered Technologies, Inc. 18816 Preston Road Suite 100 Dallas TX US 75252	72.232.168.124	FreeBSD	Apache/1.3.37 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.6 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.28 OpenSSL/0.9.7e-p1	14-May-2007

DnsStuff Aracılığı ile Bilgi Toplama

DNSStuff komut satirindan nslookup, host, dig ve whois gibi programları çalıştırarak alınabilecek çıktıları derli toplu ve merkezi bir ortamdan kullanılmasını sağlayan bir araç

Aynı sayfada mail sunucunuzun/IP adresinizin Spam listelere girip girmediği, DNS sunucu yapilandirmaniz gibi bilgiler de alınabilir.



Şekil 0-1

Passive DNS Replication

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

Çalışma mantığı bir sunucuya kurulan pdr(Passive DNS replication) uygulamasi, sunucudan gecen DNS trafigini dinleyerek dns verilerini bir tabloya yazar sonraki gelen isteklerle karşılaştırılarak bir veritabani olusturulur.

Örnek;

PDS kurulu sistemimiz www.huzeyfe.net icin bir istek gormus olsun, buna ait basit tablomuz su sekilde olacaktir.

www.huzeyfe.net IP 1.2.3.4

sonra www.lifeoverip.net adresine ait bir dns sorgusunu da yakalamis olsun, bunun da IP adresi 1.2.3.4 olsun.

www.lifeoverip.net IP 1.2.3.4

pdr uygulamasi IP adresi ayni olan domain isimlerini veritabanina yerlestirir ve sorgulayanlar o ana kadarki tutulan dns cozumlemeleri verir.

Mesela www.linux.com'un sunuldugu IP adresinde baska hangi isimler host ediliyormus bakalim…

sonuc:
http://cert.uni-stuttgart.de/stats/dns-replication.php?query=66.35.250.177&submit=Query

Bir Domaine Ait E-posta Adreslerinin Bulunması

Bir domaine ait internette dolasan(Arama motrolari vasitasi ile bulunabilecek) e-posta hesaplarini toptan görmek icin arama motorlari ile ugrasmaniza gerek yok, Google ve MSN Search'u bizim icin arayip belirledigimiz kriterlere gore mailleri bulan TheHarvester'i kullanabilirsiniz.

```
$ python theHarvester.py -d lifeoverip.net -b google

**************************************
*TheHarvester Ver. 1.1 *
*Coded by laramies *
*Edge-Security Research *
```

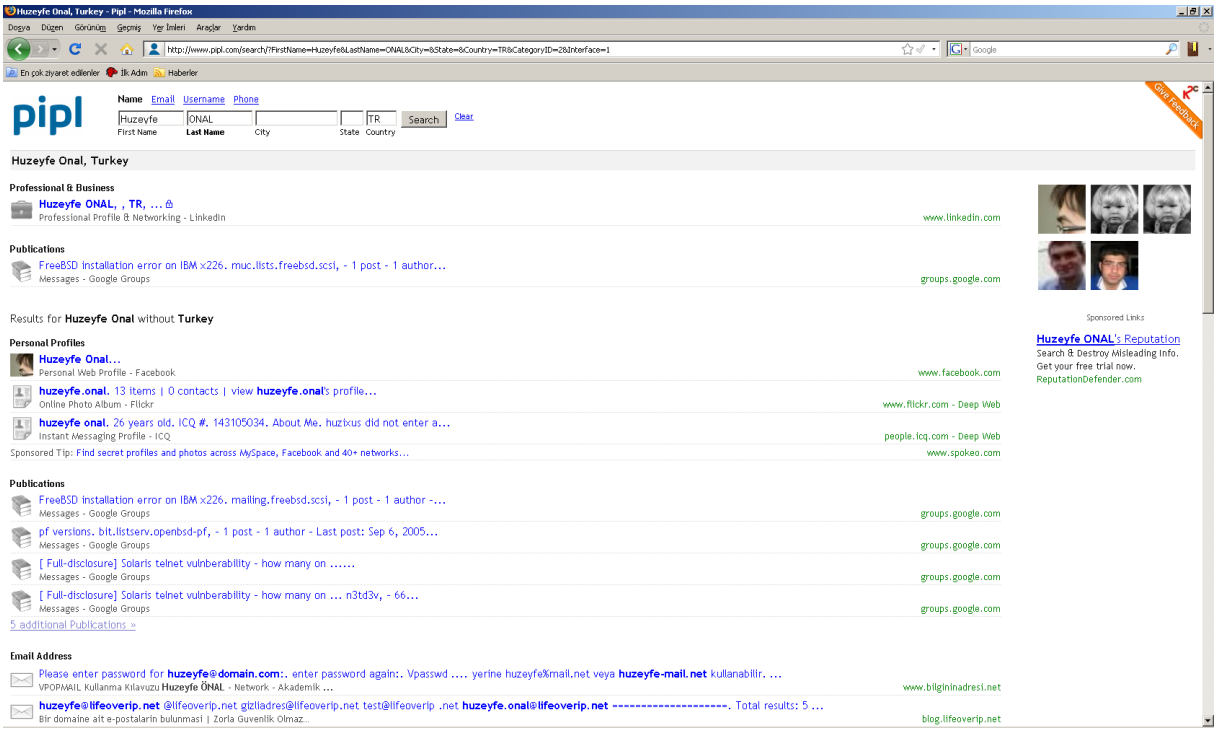
```
*cmartorella@edge-security.com *
************************************

Searching for lifeoverip.net in google
=======================================
Total results: 156
Limit: 100
Searching results: 0

Accounts found:
====================

huzeyfe@lifeoverip.net
@lifeoverip.net

gizliadres@lifeoverip.net
test@lifeoverip.net
huzeyfe.onal@lifeoverip.net
====================

Total results: 5
```

Arama Motoroları Aracılığıyla Bilgi Toplama

Arama motoru denildiğinde akla ilk gelen şüphesiz Google'dur. Fakat Google'un bu ünü zaman geçtikce ticari amaçla kullanılmaya başlandığından arama sonuçları çoğu zaman istem dışı cevaplarla dolabiliyor. Google'daki bu eksikliği iki türlü doldurulabilir: Google'da arama yöntemlerini bilme ya da google'a altternatif , özelleştirilmiş arama motorlarının kullanımı.

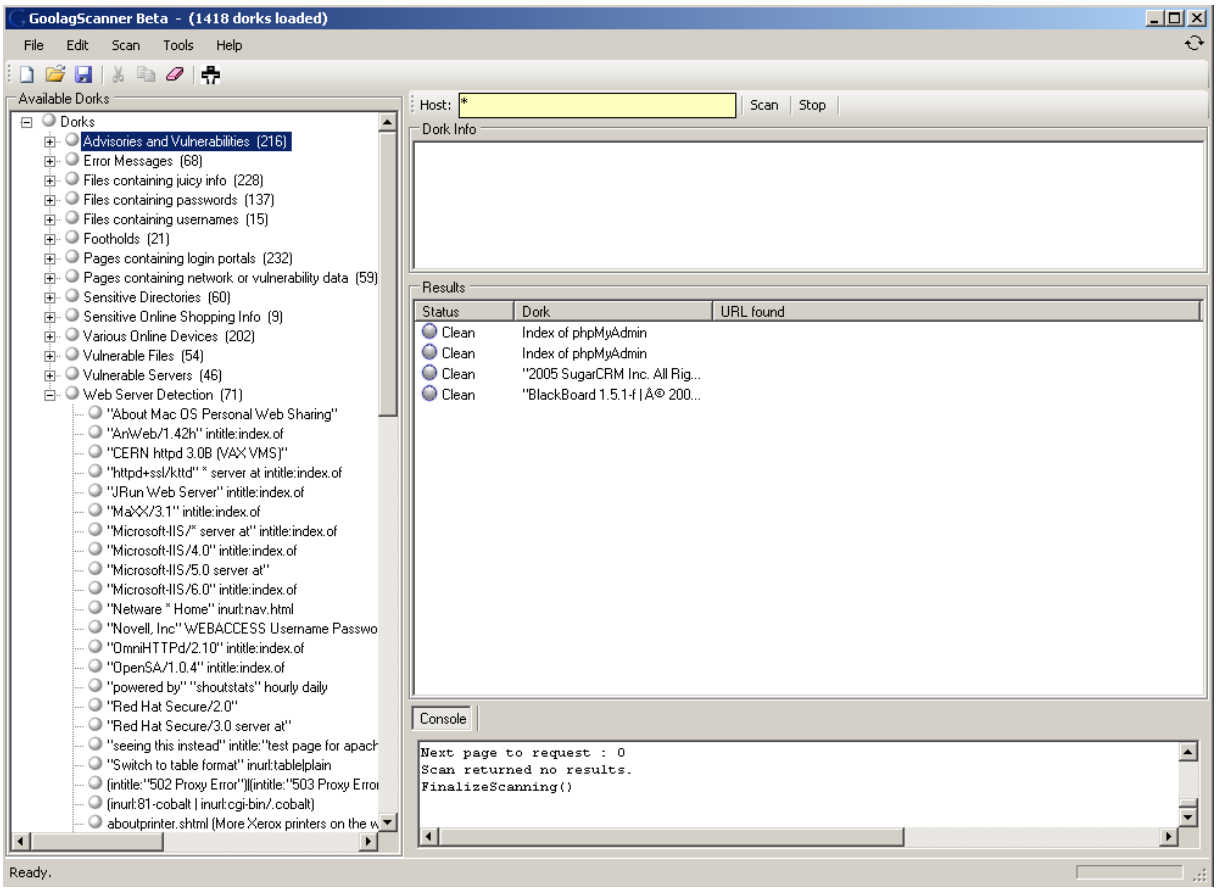
Pipl.com Aracılığı ile Şahıs Arama

Pipl.com kiş arama için en ideal sonuçları bulan bir arama motorudur. Aranan kişi ile ilgili çeşitli bilgileri kategorisel olarak yansıtır.



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 GoolagScanner'dir. İçerisinde 1400 civarı GoogleHack tekniği barındırır.



Aktif Bilgi toplama

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

DNS Protokolü kullanarak Bilgi Toplama

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

DNS sorgu tipleri

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.

Nslookup / dig

Nslookup , UNIX/Linux/Windows ortamlarının klasik dns sorgulama aracıdır. Nslookup kullanarak her tür dns sorgulamasını interaktif bir şekilde yapabilirsiniz.

```
C:\Console2>nslookup
Default Server:  mygateway1.ar7
Address:  192.168.1.1
> www.lifeoverip.net
Server:  mygateway1.ar7
Address:  192.168.1.1
Non-authoritative answer:
Name:    www.lifeoverip.net
Address:  80.93.212.86
```

```
> set type=ns
> huzeyfe.net
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
```

Sorgulama yaptığımız DNS sunucuyu değiştirerek aynı sorguyu tekrarlayalım

```
> server 195.175.39.40
Default Server:  ttdns40.ttnet.net.tr
Address:  195.175.39.40
> huzeyfe.net
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
```

Görüleceği gibi DNS sunucu değiştirildiğinde(server dns_ip_adresi) huzeyfe.net'e ait NS kaydını bulabildik.

Bir başka dns kaydı(Reverse dns) sorgulaması

```
> set type=ptr
> 1.2.3.488
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
```

Dig Aracı ile DNS Sorgulama

Dig, nslookup ve host gibi dns sorgulama araçları yerine kullanılabilen gelişmiş bir araçtır. ISC tarafından geliştirilen BIND DNS sunucusu ile birlikte geliştirilir ve uzun vadede Linux dağıtımlarında nslookup komutunun yerini alması beklenmektedir. Dig komutu domains sorgulama için çalıştırıldığında cevapla birlikte detay bilgiler de döner. Bu detay bilgiler ek parametrelerle gizlenebilir.

```
# dig ns hack2net.com  @195.175.39.40

; <<>> 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     ns2.tr.net.tr.
hack2net.com.         54685  IN     NS     ns1.tr.net.tr.

;; 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
```

Çıktıların Detay açıklaması

Status:NOERROR

sorgulanan domain adının var olduğunu ve bu domainden sorumlu dns sunucunun sorgulara sağlıklı cevap verdiğini gösterir.

Status:SERVFAIL

domainin olduğunu fakat domainden sorumlu DNS sunucunun sorgulara sağlıklı cevap veremediğini gösterir. Yani sorun domainden sorumlu DNS sunucusundadır.

Status:NXDOMAIN

Domain ile ilgili ana DNS sunucuların bilgisinin olmadığını gösterir. Bu da ya o domain yoktur ya da bazı sebeplerden dolayı root dns sunuculara yayınlanmamıştır manasına gelir.

Aynı işlemi Nslookup kullanarak yapmak için;

C:\>Nslookup

>set q=ns

>hack2net.com

MX Sorgulama

MX Kayıtlarını sorgulayarak bir domaine ait smtp sunucuları belirleyebiliriz.

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

; <<>> DiG 9.4.1 <<>> @195.175.39.40 -t mx hack2net.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38034
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

;; AUTHORITY SECTION:
hack2net.com.           52855   IN      NS      ns2.tr.net.tr.
hack2net.com.           52855   IN      NS      ns1.tr.net.tr.

;; ADDITIONAL SECTION:
mail.hack2net.com.      86400   IN      A       195.142.133.68
ns2.tr.net.tr.          2124    IN      A       195.155.11.4
ns1.tr.net.tr.          2124    IN      A       195.155.1.3

;; Query time: 28 msec
;; SERVER: 195.175.39.40#53(195.175.39.40)
;; WHEN: Sun Aug 10 18:43:12 2008
;; MSG SIZE  rcvd: 140
```

DNS Sunucu Versiyon Bilgisi

DNS sunucu versiyon bilgisini öğrenmek bir saldırgana 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 @195.155.1.3  version.bind chaos txt

; <<>> DiG 9.4.1 <<>> @195.155.1.3 version.bind chaos txt
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3385
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

```
;; ANSWER SECTION:
version.bind.        0     CH     TXT    "9.2.3"

;; Query time: 41 msec
;; SERVER: 195.155.1.3#53(195.155.1.3)
;; WHEN: Sun Aug 10 18:40:30 2008
;; MSG SIZE  rcvd: 48
```

Tüm Türkiye'nin kullandığı DNS sunucunun versiyon bilgisini sorgulayalım

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

; <<>> 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
```

Zone Transferi Kontrolü

DNS'in yapısı gereği ikincil dns sunucular kendilerinde tanımlı birincil dns sunucunun verilerini alırlar ve bunlara göre gelen istekleri cevaplarlar. Burada transfer edilen veri tamamen bizim domain kayıtlarımıza aittir ve yabancı gözlerden uzak tutulmalıdır. Bunu da master DNS sunucularda sadece yetkili ip adreslerine zone transfer izni vererek yapılır.

Sisteme sızmak isteyen birinin yapacağı keşiflerden biri de domain sunucunuzdan zone transferi yapmaktır. Bunun için nslookup ya da dig araçlarını kullanabilir.

Dig Aracı ile Zone Transferi

Öncelikle master sunucudan bölge(zone) transferi yapabilmeniz icin master sunucuda allow-transfer ile slave sunucuya izin verilmis olmalidir.

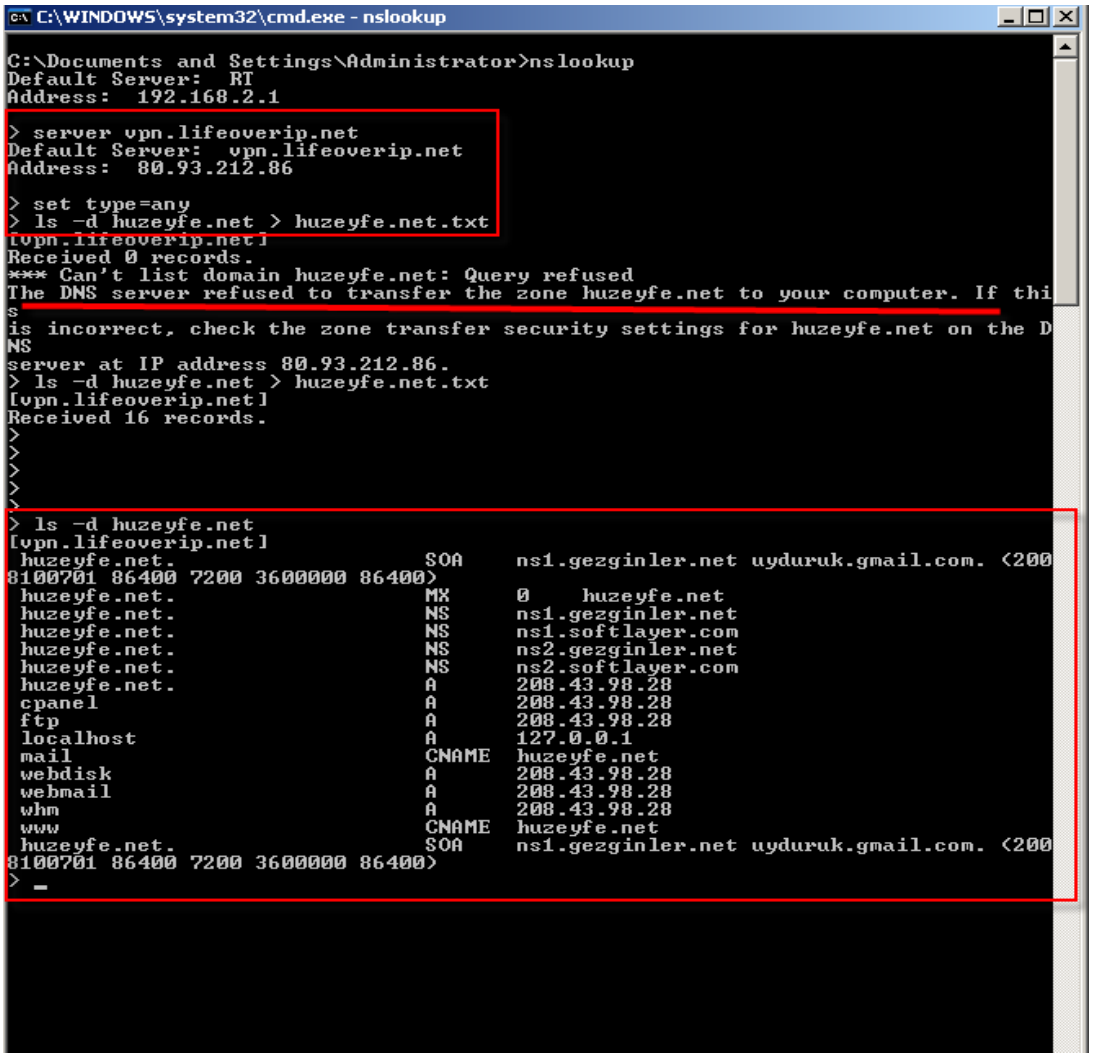
Master(1.2.3.4) sunucudaki huzeyfe.net(1.2.3.5) alani icin slave sunucuya transfer izni verelim;
/etc/named.conf dosyamda asagidaki satirlara slave sunucu icin izin veriyorum

```
zone "huzeyfe.net"
{
type master;
file "fhosts/huzeyfe.net.hosts";
allow-transfer { 1.2.3.5; };
};
```

allow-transfer { 1.2.3.5; }; satiri ile 1.2.3.5 ip sine sahip slave sunucuma benden(master sunucu)zone dosyalarini almasini sagliyorum. bu degisiklikleri yapip named prosesini yeniden baslatalim.

1.2.3.5 makinesine gecip ilk denememizi yapalim.

$dig @1.2.3.4 axfr huzeyfe.net
bu komutun ciktisi huzeyfe.net alanina ait bilgileri gosterecektir.



Zone Transfer işlemi

Dig kullanarak

```
# dig @auth100.ns.uu.net ucia.gov axfr
```

Nslookup kullanarak

Nslookup>

Ls –d domain.adi.

```
# host -l -t any ucia.gov
```

```
# host -l ibm.com
```

Server failed: Query refused

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 tutuldugu sunucuya kadar olan yollar belirlenir.

```
#dig +trace open.edu.tr @195.175.39.39

; <<>> DiG 9.3.4 <<>> +trace open.edu.tr @195.175.39.39
; (1 server found)
;; global options: printcmd
. 248 IN NS K.ROOT-SERVERS.NET.
. 248 IN NS L.ROOT-SERVERS.NET.
. 248 IN NS M.ROOT-SERVERS.NET.
. 248 IN NS A.ROOT-SERVERS.NET.
. 248 IN NS B.ROOT-SERVERS.NET.
. 248 IN NS C.ROOT-SERVERS.NET.
. 248 IN NS D.ROOT-SERVERS.NET.
. 248 IN NS E.ROOT-SERVERS.NET.
. 248 IN NS F.ROOT-SERVERS.NET.
. 248 IN NS G.ROOT-SERVERS.NET.
. 248 IN NS H.ROOT-SERVERS.NET.
. 248 IN NS I.ROOT-SERVERS.NET.
. 248 IN NS J.ROOT-SERVERS.NET.
;; Received 356 bytes from 195.175.39.39#53(195.175.39.39) in 12 ms

tr. 172800 IN NS ns1.nic.tr.
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.
tr. 172800 IN NS ns-tr.ripe.net.
;; Received 252 bytes from 193.0.14.129#53(K.ROOT-SERVERS.NET) in 84
ms

open.edu.tr. 43200 IN NS bim.open.edu.tr.
open.edu.tr. 43200 IN NS ns.ulak.net.tr.
;; Received 110 bytes from 144.122.95.51#53(ns1.nic.tr) in 14 ms

open.edu.tr. 3600 IN A 1.2.3.488
open.edu.tr. 3600 IN NS alfa.open.edu.tr.
open.edu.tr. 3600 IN NS ns.ulak.net.tr.
open.edu.tr. 3600 IN NS bim.open.edu.tr.
;; Received 161 bytes from 1.2.3.42#53(bim.open.edu.tr) in 2 ms
```

Yolu izleyecek olursak;

ilk olarak resolv.conf'ta tanımlı DNS sunucudan ROOT DNS sunucuların listesi alınır. Gelen sorgudaki ilk dns sunucuya .tr uzantılarından sorumlu olan dns sunucu sorulur ve cevap olarak ns1.nic.tr döner. Sonra ns1.nic.tr'y2 open.edu.tr'den sorumlu dns sunucu sorulur dönen cevap bim.open.edu.tr'dir . son olarak bim.open.edu.tr'ye open.edu.tr ismi sorulur ve cevap 1.2.3.488 olarak döner.

Değişken Kaynak Port ve XID DeğeriTestleri

Rekursif DNS sunucular başka dns sunuculardan istekde bulunurken kaynak port numarasını değiştirmeyebilirler. Bu, 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) değişkenine bağlıdır. Bu iki değişken ne kadar kuvvetli olursa dns üzerinden yapılacak cache poisoning türü ataklar o kadar başarısız olacaktır.

Kaynak port değeri yeterli derecede kuvvetli olan dns sunucunun verdiği cevap

```
# dig +short @195.175.39.40  porttest.dns-oarc.net txt
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 değeri yeterli derecede kuvvetli olmayan dns sunucunun verdiği cevap

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

DNS sorguları ile koruma sistemlerini atlatma

Sistem ve ağ yöneticileri test amaçlı çeşitli 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 MX kayıtlarını spam&virus koruma sisteminin ip adresi olacak şekilde yayınlaması gerekir.

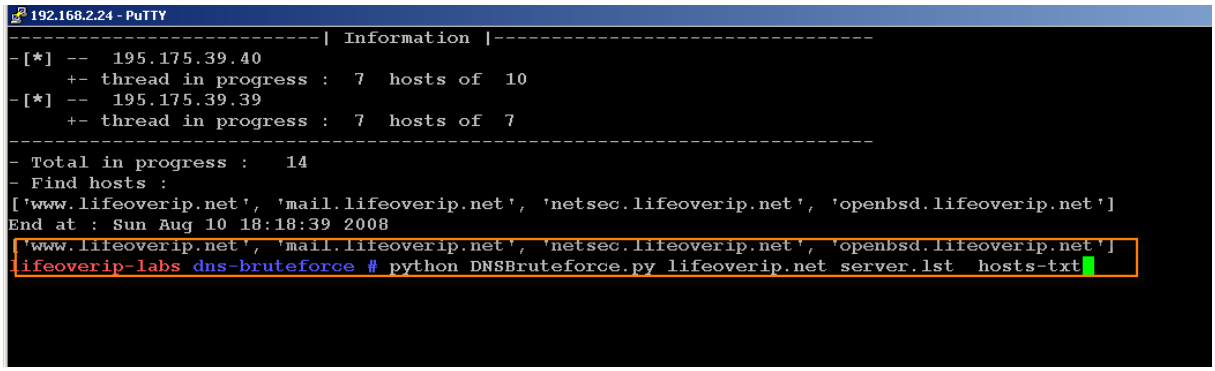
```
$ nslookup
> set querytype=mx
> bankofengland.co.uk
Server: 213.228.193.145
Address: 213.228.193.145#53
Non-authoritative answer:
bankofengland.co.uk mail exchanger = 10 cluster2.eu.messagelabs.com.
bankofengland.co.uk mail exchanger = 20 cluster2a.eu.messagelabs.com.
```

Dışardaki bir saldırgan da bu firmaya ait dns isimlerisi sözlük saldırısı ile bulmaya çalışsın.

```
C:\tools> txdns -f mail-dict.txt bankofengland.co.uk
-------------------------------------------------------------------------------
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 sunucularda bulunmaktadır. Gönderilecek bir virus ya da zararlı programcık bu adresler kullanılarak gönderilebilir.

DNS Bruteforce Yöntemi ile Bilgi Toplama



lifeoverip-labs dns-bruteforce # **python DNSBruteforce.py lifeoverip.net server.lst hosts-txt**

----------| 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']

Server.lst dosyası sorgulama yapılacak dns cache sunucular

Host-txt domain üzerinde deneme yapılacak alt alan adları.

Yine aynı iş için dnsenum.pl scripti de kullanılabilir. Burada önemli olan sözlük dosyası ve sorgulama yapan araçın kullandığı yöntem. Zira teker teker yapılacak sorgulama ile çoklu yapılacak sorgulamaların sonuçları farklı olacaktır.

DNSMAP

Bir domaine ait subdomainleri bulmak için bruteforce yöntemi ile deneme yapar. Eğer parameter olarak ayrı bir wordlist verilmezse kendi içinde barındırdığı standart listesini domain üzerinde denemeye başlar ve sonuçlarını ekrana basar.

netsec-egitim ~ # dnsmap

dnsmap - DNS Network Mapper by pagvac
(http://ikwt.com, http://foro.elhacker.net)
Usage: dnsmap <target-domain> [dictionary-file]
Examples:

dnsmap yourtarget.com
dnsmap yourtarget.com yourwordlist.txt

netsec-egitim ~ # dnsmap lifeoverip.net dnslistesi

dnsmap - DNS Network Mapper by pagvac
(http://ikwt.com, http://foro.elhacker.net)
Searching subhosts on domain lifeoverip.net

netsec.lifeoverip.net
IP Address #1:80.93.23.83

blog.lifeoverip.net
IP Address #1:80.93.23.83

openbsd.lifeoverip.net
IP Address #1:194.27.72.88

egitim.lifeoverip.net
IP Address #1:80.93.23.83

Lan.lifeoverip.net
IP Address #1:192.138.2.1

5 subhost(s) found

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.

Mesela X sistemi üzerinde çalışan SMTP yazılımının ne olduğunu bulmaya çalışalım

Öncelikle dns sorguları kullanılarak ilgili domaine ait MX kaydı(yani SMTP sunucu) bulunur.

```
# dig MX microsoft.com

; <<>> DiG 9.3.3 <<>> MX microsoft.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20996
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 6

;; QUESTION SECTION:
;microsoft.com.              IN      MX

;; ANSWER SECTION:
```

```
microsoft.com.      2678   IN    MX    10 mail.global.frontbridge.com.

;; AUTHORITY SECTION:
microsoft.com.      163558 IN    NS    ns4.msft.net.
microsoft.com.      163558 IN    NS    ns5.msft.net.
microsoft.com.      163558 IN    NS    ns1.msft.net.
microsoft.com.      163558 IN    NS    ns2.msft.net.
microsoft.com.      163558 IN    NS    ns3.msft.net.

;; ADDITIONAL SECTION:
mail.global.frontbridge.com. 3  IN    A     216.32.180.22
ns1.msft.net.       157431 IN    A     207.68.160.190
ns2.msft.net.       157431 IN    A     65.54.240.126
ns3.msft.net.       157431 IN    A     213.199.161.77
ns4.msft.net.       157431 IN    A     207.46.66.126
ns5.msft.net.       157431 IN    A     65.55.238.126

;; Query time: 3 msec
;; SERVER: 195.175.39.40#53(195.175.39.40)
;; WHEN: Fri Dec  5 21:47:12 2008
;; MSG SIZE  rcvd: 265
```

Sonra bulunan SMTP sunucusunun TCP/25 portuna telnet çekilerek dönecek banner ile yazılımı öğrenilebilir.

```
# telnet mail.global.frontbridge.com. 25
Trying 216.32.181.22...
Connected to mail.global.frontbridge.com.
Escape character is '^]'.
220 mail40-wa4.bigfish.com ESMTP Postfix EGGS and Butter
help
```

Görüleceği üzere Microsoftun maillerinin yönlendirildiği ana MX sunucu Postfix üzerinde çalışıyor.

Web Sunuculardan Banner Yakalama Yöntemi ile Bilgi Toplama

http fingerprint aşamasında sunucu sisteme beklenmeyen anormal istekler gondererek dönen cevabı incelemek çoğu durumda sunucuya ait net bilgiler verir. Bu yöntem sunucunun uzerinde çalışan web servisine ait bilgilerin özellikle saklandığı durumlarda geçerlidir.

Örnek

Sun One Web Server	IIS 5.x
$ nc sun.site.com 80	**$ nc iis5.site.com 80**
PUT / HTTP/1.0	**PUT / HTTP/1.0**

Host: sun.site.com	**Host: iis5.site.com**
HTTP/1.1 401 Unauthorized	HTTP/1.1 403 Forbidden
Server: Sun-ONE-Web-Server/6.1	**Server: Microsoft-IIS/5.1**
IIS 6.0	Apache 2.0.x
$ nc iis6.site.com 80	**$ nc apache.site.com 80**
PUT / HTTP/1.0	**PUT / HTTP/1.0**
Host: iis6.site.com	**Host: apache.site.com**
HTTP/1.1 411 Length Required	HTTP/1.1 405 Method Not Allowed
Server: Microsoft-IIS/6.0	**Server: Apache/2.0.54**
Content-Type: text/html	

Bu yönteme ek olarak sunucunun döndürdüğü cevaplar da izlenerek servis yazılımı hakkında bilgi edinilebilir. Mesela

Apache 2.x icin dönen cevap:

```
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 5.1 için dönen cevap

```
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 için

```
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
```

Sun One ve IIS için dönen cevaplar benzer gözükse de dikkatli bir göz ikisi arasındaki farkı görecektir.

IIS icin Content-Length

Sun ONE için Content-**length**

Görüleceği gibi Length kelimelerinden biri büyük harfle basliyor digeri isi küçük harfle...

Bu ve buna benzer yöntemler kullanarak bir servisin tam sürümü belirlenebilir. Bu tip testleri elle yapulabileceği gibi otomatize araçlar kullanılarak da yapılır.

Httprint bunlardan en sık kullanılanı.

C:\netcat>nc www.lifeoverip.net 80 -vv

www.lifeoverip.net [80.93.212.86] 80 (?) open

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

```
Connection: close

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

sent 17, rcvd 236: NOTSOCK
```

```
# telnet www.trustmatta.com 80

Trying 62.232.8.1...

Connected to www.trustmatta.com.

Escape character is '^]'.

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Mon, 26 May 2003 14:28:50 GMT

Server: Apache/1.3.27 (Unix) Debian GNU/Linux PHP/4.3.2

Connection: close

Content-Type: text/html; charset=iso-8859-1
```

Bazen web sunucunun çalıştığı iç IP adresini almak içinde kullanılır.

```
# 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)
```

Bazı değerleri almak için HTTP OPTIONS komutu kullanılır

```
# 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.
```

ASp .net çalışan web sunucuları test aracı

dnascan.pl

```
# ./dnascan.pl http://www.example.org
[*] Sending initial probe request...
[*] Sending path discovery request...
[*] Sending application trace request...
```

```
[*] Sending null remoter service request...


[ .NET Configuration Analysis ]


       Server    -> Microsoft-IIS/6.0
  Application    -> /home.aspx
     FilePath    -> D:\example-web\asproot\
   ADNVersion    -> 1.0.3705.288
```

SSH Sürümünü Sorgulama

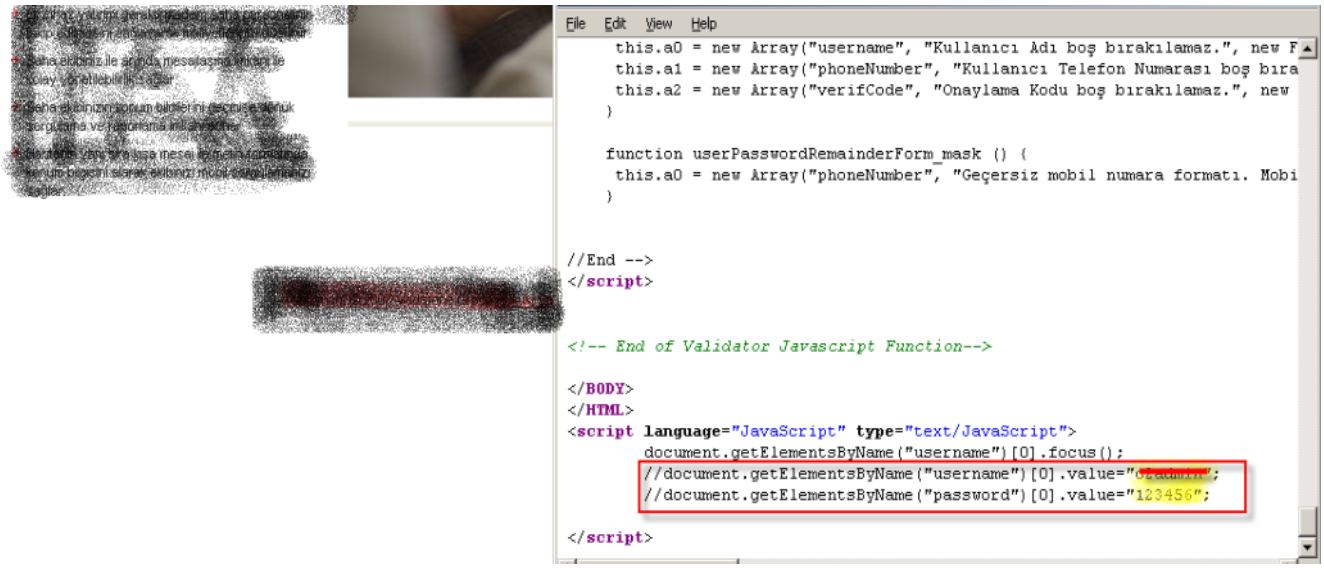
```
C:\netcat>nc www.lifeoverip.net 2000 -vvv
www.lifeoverip.net [80.93.212.86] 2000 (?) open
SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110
```

Banner yakalamnın bir adım ötesi bu işi otomatize araçlara teslim etmektir. Nmap ve THC Amap bu hizmeti en iyi sağlayan iki araçtır.

Diğer Bilgi Toplama Yöntemleri

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.



Hedef Sistem Hakkında Ek Bilgi Edinmek

Sequence numarası tahmini

```
# 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
```

Hedef Sistemin Uptime Süresinii Belirleme

```
# hping3 -S --tcp-timestamp -p 80 -c 2 1.2.3.488

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: 6 days, 9 hours, 33 minutes, 39 seconds




--- 1.2.3.488 hping statistic ---

2 packets tramitted, 2 packets received, 0% packet loss

round-trip min/avg/max = 99.1/101.8/104.5 ms
```

NOT-I : Windows XP SP2'lerle birlikte güvenlik amaçlı* timestamp sorgularına cevap

dönmez.

NOT-II : Cisco Routerlarda timestamp'i aşağıdaki şekilde aktif/pasif hale getirebiliriz

ip tcp timestamp -> aktif hale getirmek için
no ip tcp timestamp

Hedef Sistemin Saatini Öğrenme

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

HTTP Protokolü üzerinden hedef sisteme ait zaman tespiti

```
# telnet mail.lifeoverip.net 80
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.
```

GMT olarak verilen zaman dilimine +2 ekleyerek sunucunun gerçek zamanına ulaşılabilir.

SMTP Protokolü Üzerinden Hedef Sisteme Ait Zaman Tespiti

Hedef sistemin üzerinde bir SMTP sunucu çalıştığı varsayılarak yapılır. Hedef e-posta sistemi üzerinde olmadığı bilinen bir kullanıcıya mail atılır ve sistemin bu mail karşılık olarak hata dönmesi beklenir. Hedef sistem hata dönerse(bounce maili) dönen mailin başlıkları incelenerek zaman tespiti yapılır.

Intrace

Gelişmiş traceroute uygulamasıdır. NAT arkasındaki local ipli sistemleri bulma olasılığı var.

Çalışması için bir pencereden INtrace komutu çalıştırılmaı aynı anda hedef sistemin ilgili portuna very gönderecek işlemler yapılmalı.

```
netsec-egitim ~ # intrace  -i eth0 -h www.vodafone.com.tr -p 443 -d 4
InTrace, version 1.3
2008/11/11 18:11:41.469769 <INFO> Resolving 'www.vodafone.com.tr'

InTrace 1.3 (C)2007 Robert Swiecki <robert@swiecki.net>
-------------------------------------------------------
R: 74.125.77.147/80 (80) L: 192.168.2.24/58007
Last rcvd SEQ: 0xaa2b850e, ACK: 0x5bcf4388
Press ENTER to start sending packets

  1.    192.168.2.1       [ICMP TTL-EXCEEDED]
  2.    85.96.186.1       [ICMP TTL-EXCEEDED]
  3.    212.156.203.54    [ICMP TTL-EXCEEDED]
  4.    212.156.118.253   [ICMP TTL-EXCEEDED]
  5.    212.156.117.245   [ICMP TTL-EXCEEDED]
  6.    212.156.102.9     [ICMP TTL-EXCEEDED]
  7.    212.156.102.14    [ICMP TTL-EXCEEDED]
  8.    209.85.254.250    [ICMP TTL-EXCEEDED]
  9.    72.14.233.114     [ICMP TTL-EXCEEDED]
 10.    209.85.255.166    [ICMP TTL-EXCEEDED]
 11.    209.85.255.106    [ICMP TTL-EXCEEDED]
 12.    74.125.77.147          [TCP RST]
```

RelayScanner

SMTP Üzerinden e-posta sisteminin Relay'a açık olup olmadığını control eder.
netsec-egitim relayscanner # perl RelayScanner.pl -l host_info.txt

```
****************************************
****************************************
```

```
***  CIRT.DK SMTP Relay Scanner    ***
***        Version 1.7         ***
****************************************
******* (c)2007 by Dennis Rand *********
****************************************
****************************************
```

[X] Checking for updates - NO UPDATES
[X] Loading scanner - DONE
[X] Checking for service - DONE
[X] Checking for SMTP service - DONE
[X] Total testcases to run - 16416
[X] Delay between tests - 2 seconds
[X] Relay scan started - Tue Nov 11 18:40:33 2008

[X] Relay Checking in progress: => 0/10

Bir SMTP sunucunun üzerinde test edilebilecek tüm relaying olasılıkları taker taker denenir. Programın düzgün çalışabilmesi için host_info.txt içerisinde yazılacak bilgilerin doğru olması gerekir. Program çalıştığında hedef mail adresine bir adet mail gönderir ve bu maile cevap dönülmeden testlere başlamaz.

Spam Göndermeye Açık Web Sunucuların Keşfi

WEB Servis Güvenlik Açıklarını Tarama

HTTP CONNECT

```
# telnet www.example.org 80
Trying 192.168.0.14...
Connected to 192.168.0.14.
Escape character is '^]'.
CONNECT maila.microsoft.com:25 HTTP/1.0

HTTP/1.0 200 Connection established
220 inet-imc-02.redmond.corp.microsoft.com Microsoft.com ESMTP Server
```

A failed HTTP CONNECT bounce

```
# telnet www.example.org 80
Trying 192.168.0.14...
Connected to 192.168.0.14.
Escape character is '^]'.
CONNECT maila.microsoft.com:25 HTTP/1.0

HTTP/1.1 405 Method Not Allowed
Date: Sat, 19 Jul 2003 18:21:32 GMT
Server: Apache/1.3.24 (Unix) mod_jk/1.1.0
Vary: accept-language,accept-charset
Allow: GET, HEAD, OPTIONS, TRACE
Connection: close
Content-Type: text/html; charset=iso-8859-1
Expires: Sat, 19 Jul 2003 18:21:32 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>405 Method Not Allowed</TITLE>
</HEAD><BODY>
<H1>Method Not Allowed</H1>
The requested method CONNECT is not allowed for the URL<P><HR>
<ADDRESS>Apache/1.3.24 Server at www.example.org Port 80</ADDRESS>
</BODY></HTML>
```

A successful HTTP GET bounce

```
# telnet cacheflow.example.org 80
Trying 192.168.0.7...
Connected to 192.168.0.7.
Escape character is '^]'.
GET / HTTP/1.1
HOST: mx4.sun.com:25
```

```
HELO .

MAIL FROM: spammer@alter.net

RCPT TO: target@unsuspecting.com

DATA

Subject: Look Ma! I'm an open relay

Hi, you've been spammed through an open proxy, because of a bug in

The CacheOS 4 platform code. Have a great day!

-Spammer
```

E-posta Başlıkları Aracılığı ile 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.

E-posta Başlık Bilgileri

From:
From: Mailin kimden geldiğini gösteren elemandır. Çok kolay spoof edilebileceği için en az güvenilir başlık alanıdır denilebilir.

From: "Huzeyfe Onal" Huzeyfe.Onal@xyz.com.tr

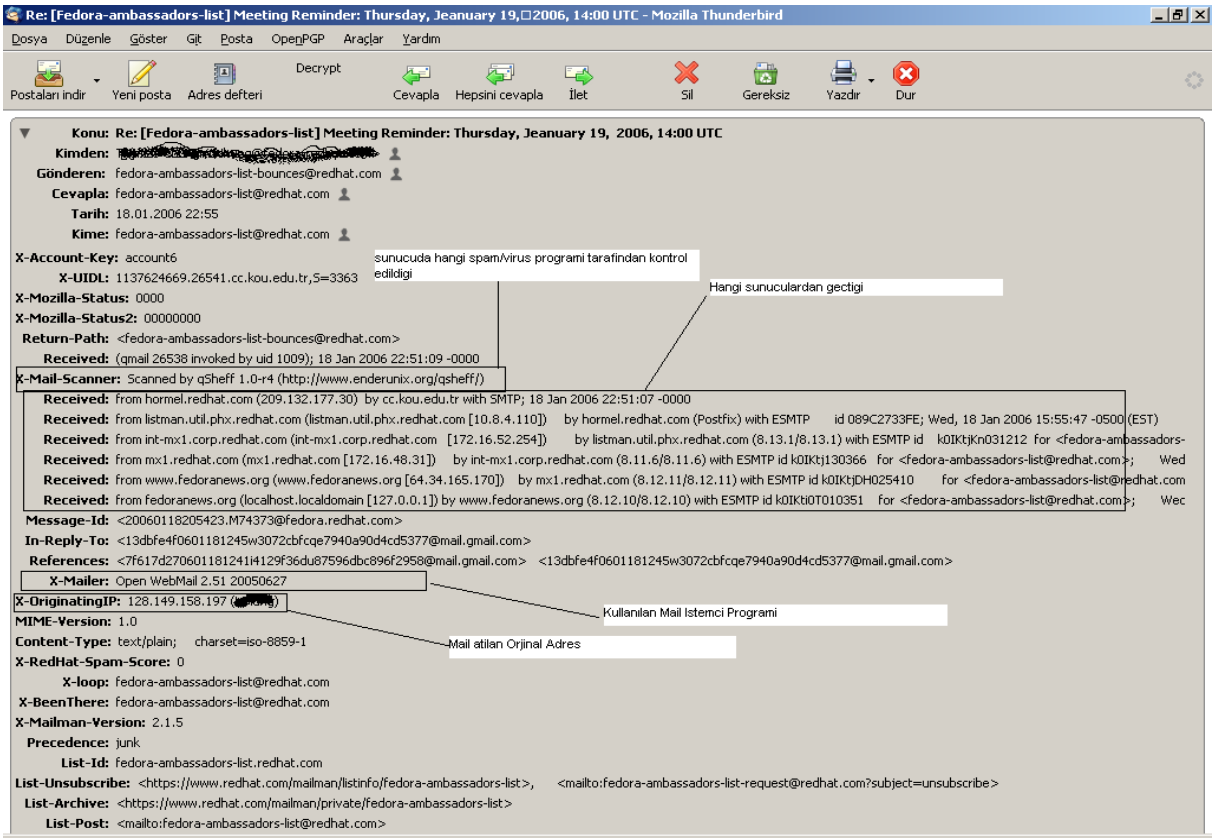
Bir de From(From: değil) alani vardir ki bu standart mail başlığı değildir, bazı yazılımların mail alındığında eklediği bir başlık türüdür.

Reply-To:

Dönen cevabın hangi adrese gönderileceğini bildirir.

Return-path

Reply-to benzeri bir başlıktır.



Received

Received başlığı mail iletilişimi ile ilgili verdiği detaylı ve gerçekci bilgiden dolayı oldukça önemlidir . Kullanıcı ile MTA, MTA ile MTA arasındaki iletişimi geriy dönük takip edebilmek içi Recevied alanı kullanılır.

Postayı her teslim alan mta bir received başlığı ekler. Aşağıdan yukarı takip ederek gönderilen mailin hangi SMTP sunucularindan geçtiği belirlenebilir.

Received: from string (hostname [host IP address])

by recipient host (MTA Bilgisi)

with protocol id message ID

for recipient;

timestamp

string ile hostname(gönderici MTA/host) genelde aynı olur fakat string kısmı farklı olabilir.

Hostname, gonderici MTA'nin ters DNS kaydi ile elde edilir. String degistirilebilir oldugu icin dikkate alınmayabilir.

recipient host: Maili teslim alan MTA

MTA Bilgisi : Maili teslim alan MTA yazılım bilgileri. Bu alan kullanılan yazılıma ve yapılan ayarlara göre çok detaylı bilgi de verebilir, sadece yazılım ismi de.

Örnek MTA Bilgisi.

Received: from defiant.ddtechcg.com ([72.90.237.196])

by vms044.mailsrvcs.net (Sun Java System Messaging Server 6.2-6.01 (built Apr

3 2006))

Sendmail

by shear.ucar.edu (8.14.1/8.13.6) with ESMTP id l4K4heF4002161;

Postfix örneği:

by mail4.barnet.com.au (Postfix) with ESMTP id 5EEE242931F

esmtp id maili alan sunucunun kendi içerisinde kullanılabilecek bir değerdir.

Message ID: Mailin ilk çıktığı makine tarafindan oluşturulan başlık değeri. Kullanılan mta'ya göre ufak tefek farklılıklar gösterse de genel tanım itibari ile id@smtp_sunucu formatındadır.

<1168358378.14189.ezmlm@huzeyfe.net>

Bu ID mail istemcisi tarafindan olusturulur ve mail sunucuda belirli bir mesajin aranmasinda kolaylik saglar.

timestamp: mesajin alici taraftaki MTA'ya ulastigi zaman. Ilk ve son timestamp bilgilerine bakılarak e-posta sunucularin performanslarına dair bir fikir edinilebilir.

Received: (from rapsodi@localhost)

by synack.anonim.net (8.13.8/8.13.8/Submit) id l4JNzXCJ032364;

Sat, 19 May 2007 16:39:34 -0700

-0700 Greenwitch'in 7 saat gerisinde manasindadir.

For recipient: alıcı mail adresi. Mailin kim için olduğu bilgisi.

Received: from smtp2.abc.com.tr (HELO smtp2.xyz.com.tr) (2.1.1.7)

by gelisimplatformu.org with SMTP; 29 Dec 2006 13:12:24 -0000

from satırında maili gönderen sunucunun smtp2.abc.com.tr olduğu gözüküyor, fakat aynı adrese dns sorgulaması yaptığımızda farklı bir isim çözüyorsa bu başlığın değiştirilmiş olduğundan şüphelenilebilir.

Bazen de maili gönderen makinenin DNS ismi ile kendi üzerinde tanımlanmış ismi farklı olur ve Received kısmında iki farklı isim gözükür . Yukarıdaki örnek aslında tam da bugu göstermektedir.

Makinenin ismi smtp2.xyz.com.tr olarak tanımlanmış fakat dns kaydı smtp2.abc.com.tr şeklindedir.

Detaylı Başlık Analizi

Delivered-To: huzeyfe.onal@gmail.com

Received: by 10.114.153.8 with SMTP id a8cs349808wae;

Sat, 19 May 2007 21:44:46 -0700 (PDT)

Received: by 10.114.156.1 with SMTP id d1mr1825769wae.1179636286474;

Sat, 19 May 2007 21:44:46 -0700 (PDT)

Return-Path: <owner-advocacy+M1030@openbsd.org>

Received: from shear.ucar.edu (lists.openbsd.org [192.43.244.163])

by mx.google.com with ESMTP id a8si2499671poa.2007.05.19.21.44.42;

Sat, 19 May 2007 21:44:46 -0700 (PDT)

Received-SPF: pass (google.com: manual fallback record for domain of owner-advocacy+M1030@openbsd.org designates 192.43.244.163 as permitted sender)

Received: from openbsd.org (localhost.ucar.edu [127.0.0.1])

by shear.ucar.edu (8.14.1/8.13.6) with ESMTP id l4K4heF4002161;

Sat, 19 May 2007 22:43:40 -0600 (MDT)

Received: from mail4out.barnet.com.au (mail4.barnet.com.au [202.83.178.125])

by shear.ucar.edu (8.14.1/8.13.6) with ESMTP id l4K4gwhT025317 (version=TLSv1/SSLv3 cipher=DHE-DSS-AES256-SHA bits=256 verify=NO)

for <advocacy@openbsd.org>; Sat, 19 May 2007 22:43:00 -0600 (MDT)

Received: by mail4out.barnet.com.au (Postfix, from userid 1001) id 8AF9F37D73E; Sun, 20 May 2007 14:42:52 +1000 (EST)

X-Viruscan-Id: <464FD1CC0000E45F9685CD@BarNet>

Received: from mail4auth.barnet.com.au (mail4.barnet.com.au [202.83.178.125]) (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits)) (Client did not present a certificate)

by mail4.barnet.com.au (Postfix) with ESMTP id 5EEE242931F

for <advocacy@openbsd.org>; Sun, 20 May 2007 14:42:52 +1000 (EST)

Received: from mail1.test (mail1.test.org [10.251.1.18])

by mail4auth.barnet.com.au (Postfix) with ESMTP id 2E9F937D731

for <advocacy@openbsd.org>; Sun, 20 May 2007 14:42:52 +1000 (EST)

Received: by mail1.test (Postfix, from userid 1001) id 0DE621A3; Sun, 20 May 2007 14:42:52 +1000 (EST

Date:

Mailin ilk kaynakta oluşturulma zamanı.

Date: Sat, 19 May 2007 10:31:37 -0400

X-Başlıkları

İstemci ve mta harici yardımcı yazılımların eklediği başlıklar gerçek başlık değerleri ile karışmaması için X- ile başlar.

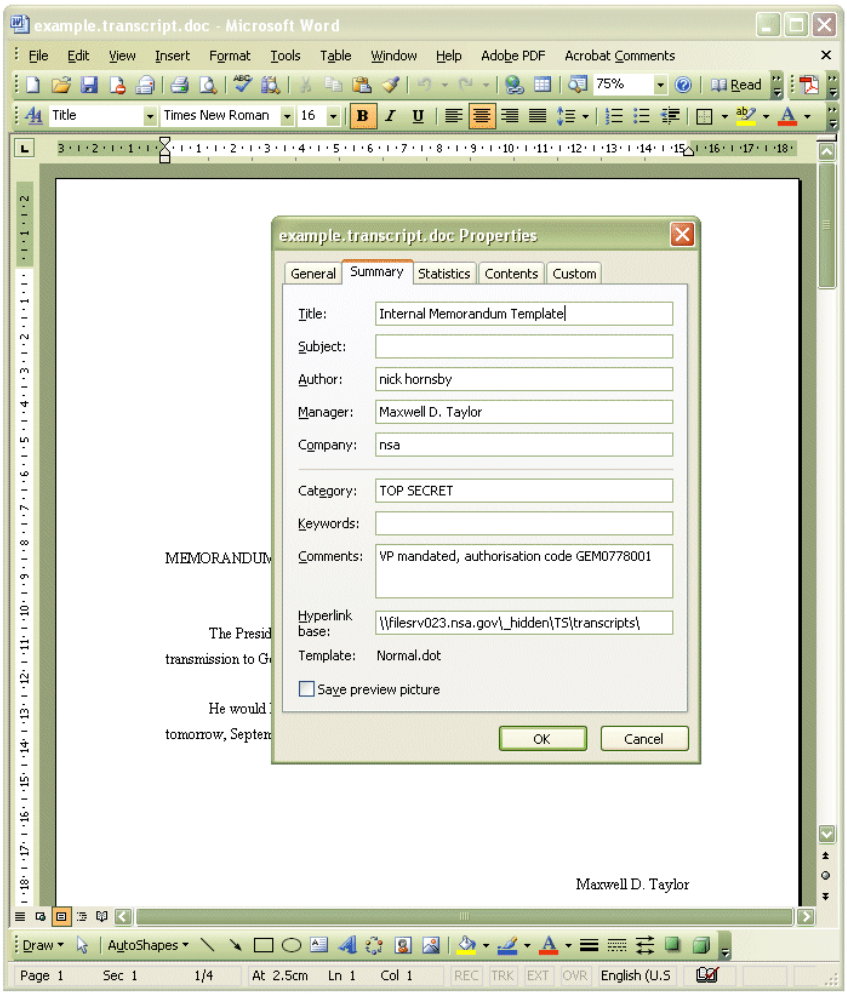
SMTP Üzerinden Ağ Topolojisi Çıkarma

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

```
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) client-ip=66.163.168.185;
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 send
Comment: DomainKeys? See http://antispam.yahoo.com/domainkeys
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=lima; d=yahoogroups.com;
        b=US5HE3OSSk7frUSDbA8J3zEzNTqlxoB3aa4zuFiIwaiihFBBpiR7GoOKwnOH+2fd5LCt/j4SdxW8mEeKvu1SHX8F6elRJKi8vmtT/XAe2E5M2LAoBwKMUWzpS/xrt8hZ;
Received: from [216.252.122.216] by n51.bullet.mail.sp1.yahoo.com with NNFMP; 29 Jul 2008 11:02:09 -0000
Received: from [66.218.69.6] by t1.bullet.sp1.yahoo.com with NNFMP; 29 Jul 2008 11:02:09 -0000
Received: from [66.218.67.91] by t6.bullet.scd.yahoo.com with NNFMP; 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@yahoogroups.com
X-Received: (qmail 90819 invoked from network); 29 Jul 2008 08:51:55 -0000
X-Received: from unknown (66.218.67.96)
  by m44.grp.scd.yahoo.com with QMQP; 29 Jul 2008 08:51:55 -0000
X-Received: from unknown (HELO NEWVW.turkcell.com.tr) (212.252.168.230)
  by mta17.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 NEWVW.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: <F8D2D73CD4CAD440AF999D80A27651FA032C9337@exhmbx03.turkcell.entp.tgc>
In-Reply-To: <68024ce0807271402i701da06f1d1b17e403b535de6@mail.gmail.com>
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
Thread-Topic: =?iso-8859-9?Q?=5Bbilgiguvenligi=5D_TT_dns_a=E7=FD=FO=FD?=
Thread-Index: AcjwZ9IrwZoZWoJ2SmamWziRBWJ1RAA7wA/A
References: <68024ce0807271402i701da06f1d1b17e403b535de6@mail.gmail.com>
To: <bilgiguvenligi@yahoogroups.com>
X-OriginalArrivalTime: 29 Jul 2008 08:51:52.0120 (UTC) FILETIME=[58515380:01C8F158]
X-Originating-IP: 212.252.168.230
X-eGroups-Msg-Info: 2:2:2:0:3
From: <okyar.tahaoglu@turkcell.com.tr>
X-Yahoo-Profile: okyartaha
X-eGroups-Approved-By: deniztuncalp <deniz.tuncalp@turkcell.com.tr> via email; 29 Jul 2008 11:02:04 -0000
Sender: bilgiguvenligi@yahoogroups.com
MIME-Version: 1.0
Mailing-List: list bilgiguvenligi@yahoogroups.com; contact bilgiguvenligi-owner@yahoogroups.com
Delivered-To: mailing list bilgiguvenligi@yahoogroups.com
List-Id: <bilgiguvenligi.yahoogroups.com>
Precedence: bulk
List-Unsubscribe: <mailto:bilgiguvenligi-unsubscribe@yahoogroups.com>
Date: Tue, 29 Jul 2008 11:51:07 +0300
Subject: =?iso-8859-9?Q?RE:_=5Bbilgiguvenligi=5D_TT_dns_a=E7=FD=FO=FD?=
X-Yahoo-Newman-Property: groups-email-ff-m
Reply-To: bilgiguvenligi@yahoogroups.com
Content-Type: multipart/related;
 boundary="----=_NextPart_000_51941F_01C8F171_7DB87C20"
```

Internetten İndirilen Dosyalar Üzerinden Bilgi Toplama

Bu yöntem özelde office dosyalari için kullanılsa da genelde tüm metadata içeren belgeler için geçerlidir. Mesela bir word dosyası aşağıdaki bilgileri barındırabilir ve bu bilgiler temizlenmeden internete koyulan bir belge birçok bilginin sızmasına sebep olabilir.

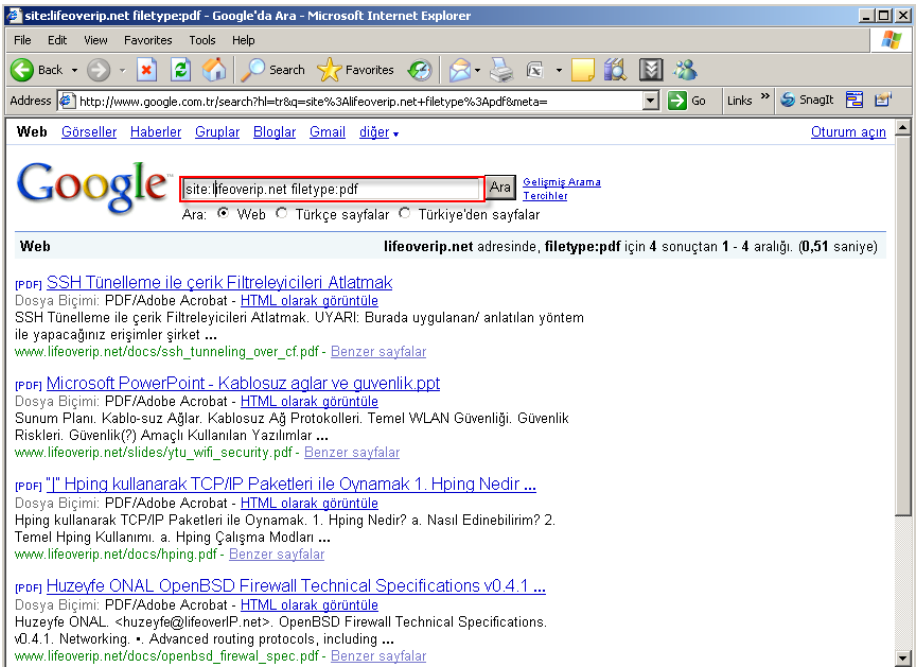


Metagoofil Aracı ile Bilgi Toplama

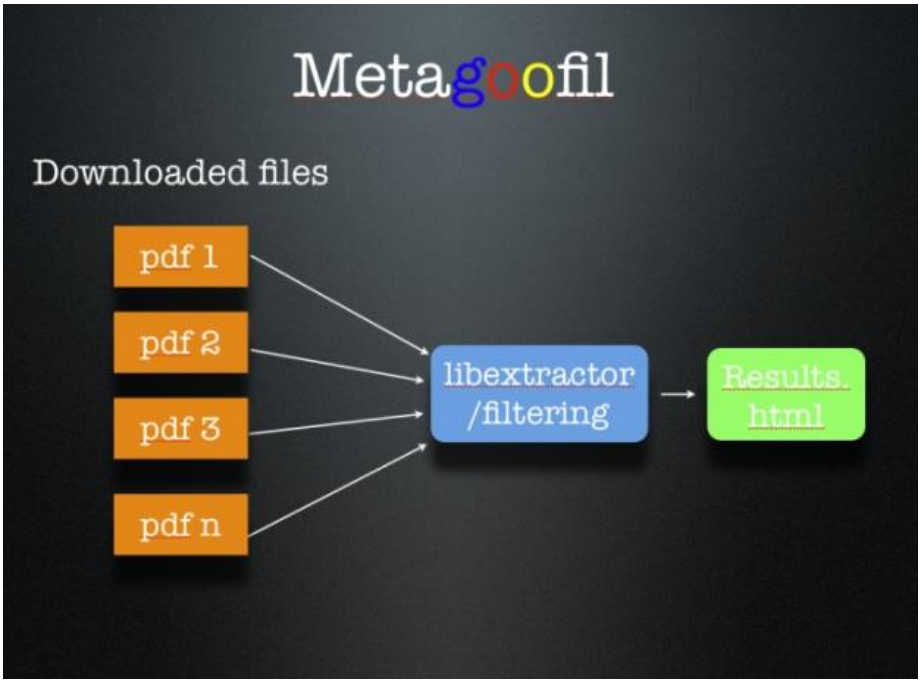
Metagoofil, google aracılığı ile çeşitli dökümanları (pdf, doc, jpg)araştırıp bunlar üzerinde –normalde görünmeyen- metadata bilgilerini ayrıştıran ve raporlayan bir araçtır.

MetaGoofil nasıl çalışır?

İlk olarak Google aracılığı ile belirtilen özelliklerdeki domainleri arar. Tıpkı bizim browser üzerinden google yöntemlerini kullanarak yaptığımız aramalar gibi.



Bulduğu dökümanları diske kaydeder ve bir ayrıştırıcıdan geçirip dökümanlar üzerindeki metadatalardan işe yarayacak bilgileri raporlar.

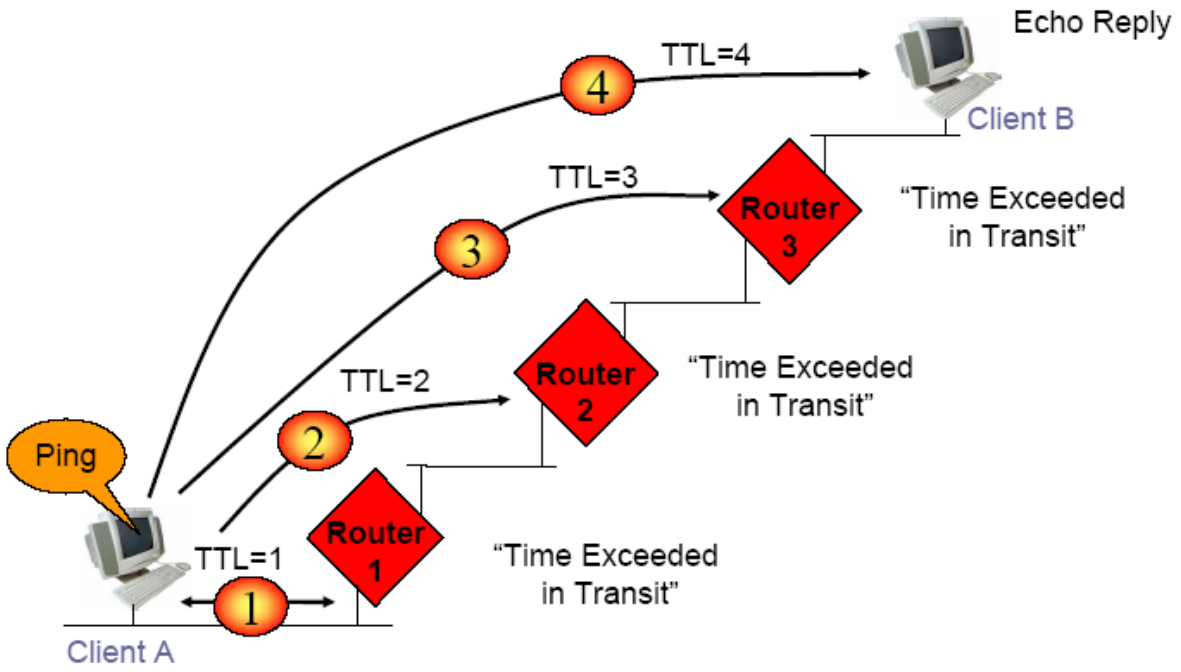


Ağ Haritalama Yöntemi ile Bilgi Toplama

Traceroute

Traceroute IP başlığındaki TTL(Time To Live) alanını kullanır. Amaç Hedef sisteme giden yolları öğrenmektir ve bunun için TTL değerini 1 den başlatarak her seferinde bir arttırır.

TTL değerini 1 olarak alan host paketi çöpe atarak geriye TTL Expired cevabı döner. Trace çeken bilgisayarda bu şekilde önündeki yolun tarifini çıkarır.




```
# traceroute www.google.com

traceroute: Warning: www.google.com has multiple addresses; using 64.233.183.103
traceroute to www.l.google.com (64.233.183.103), 64 hops max, 40 byte packets
 1  host-80-93-212-81.teklan.com.tr (80.93.212.81)  0.625 ms  20.543 ms  0.242 ms
 2  88.255.65.17 (88.255.65.17)  1.332 ms  28.244 ms  30.353 ms
 3  * * *
 4  * 212.156.118.9 (212.156.118.9)  130.119 ms  213.596 ms
 5  212.156.118.21 (212.156.118.21)  20.435 ms  1.035 ms  1.022 ms
```

NOT: Linux ve Windows sistemlerde trace aracı farklı protokoller kullanır.

Traceroute ve Diğer Protokoller

TcpTraceroute

Hedef sistemde icmp ve udp portlari kapali ise klasik traceroute çalışmaları sağlıklı sonuçlar vermeyecektir.

Hedef sistem üzerinde açık bir port üzerinden TCPTraceroute çalıştırırsak sisteme giden yolları ve sistem önünde güvenlik duvarını belirleyebiliriz.

```
#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 ms
 5  212.156.118.161 (212.156.118.161)  384.850 ms  742.354 ms  336.844 ms
 6  212.156.118.5 (212.156.118.5)  18.064 ms  24.648 ms  23.109 ms
 7  212.156.118.21 (212.156.118.21)  32.347 ms  48.208 ms  64.222 ms
 8  212.156.117.10 (212.156.117.10)  61.678 ms  54.749 ms  52.075 ms
 9  212.156.117.146 (212.156.117.146)  73.028 ms  97.067 ms  109.632 ms
10  usr-4993.dial-in.ttnet.net.tr (212.156.147.130)  112.622 ms  97.923 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
```

Traceroute ve TCPTraceroute Farkını Anlama

www.open.edu.tr önünde sağlam bir güvenlik duvarı ile korunan web sunucusu.

Hedef sisteme yapılan klasik traceroute çalışması çıktısı

```
#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 ms
 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 ms
 7  212.156.118.38 (212.156.118.38)  69.980 ms 212.156.118.21 (212.156.118.21)  90.169 ms
212.156.118.38 (212.156.118.38)  107.029 ms
 8  * * *
```

```
 9  212.156.117.146 (212.156.117.146)  107.342 ms  94.551 ms 212.156.117.142
(212.156.117.142)  76.182 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 TCPtraceroute çalışması çıktısı

```
#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 ms
 5  212.156.118.161 (212.156.118.161)  384.850 ms  742.354 ms  336.844 ms
 6  212.156.118.5 (212.156.118.5)  18.064 ms  24.648 ms  23.109 ms
 7  212.156.118.21 (212.156.118.21)  32.347 ms  48.208 ms  64.222 ms
 8  212.156.117.10 (212.156.117.10)  61.678 ms  54.749 ms  52.075 ms
 9  212.156.117.146 (212.156.117.146)  73.028 ms  97.067 ms  109.632 ms
10  usr-4993.dial-in.ttnet.net.tr (212.156.147.130)  112.622 ms  97.923 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
```

Son iki satıra dikkat edilirse aynı adres iki kere cevap vermiş. Bu hedef sistemin önünde NAT yapan bir güvenlik duvarının çalıştığını gösterir.

SNMP Üzerinden Bilgi Toplama

SNMP Nedir?

SNMP, ağ cihazlarında yönetimsel bilgi alışverişinin sağlanması için oluşturulmuş bir uygulama katmanı protokolüdür. TCP/IP protokolünün bir parçası olan SNMP; ağ yöneticilerinin ağ performansını arttırması, ağ problemlerini bulup çözmesi ve ağlardaki genişleme için planlama

yapabilmesine olanak sağlar. Günümüzde kullanımda olan 3 tane SNMP sürümü mevcuttur.[Wikipedia]

Snmpenum ile bilgi toplama

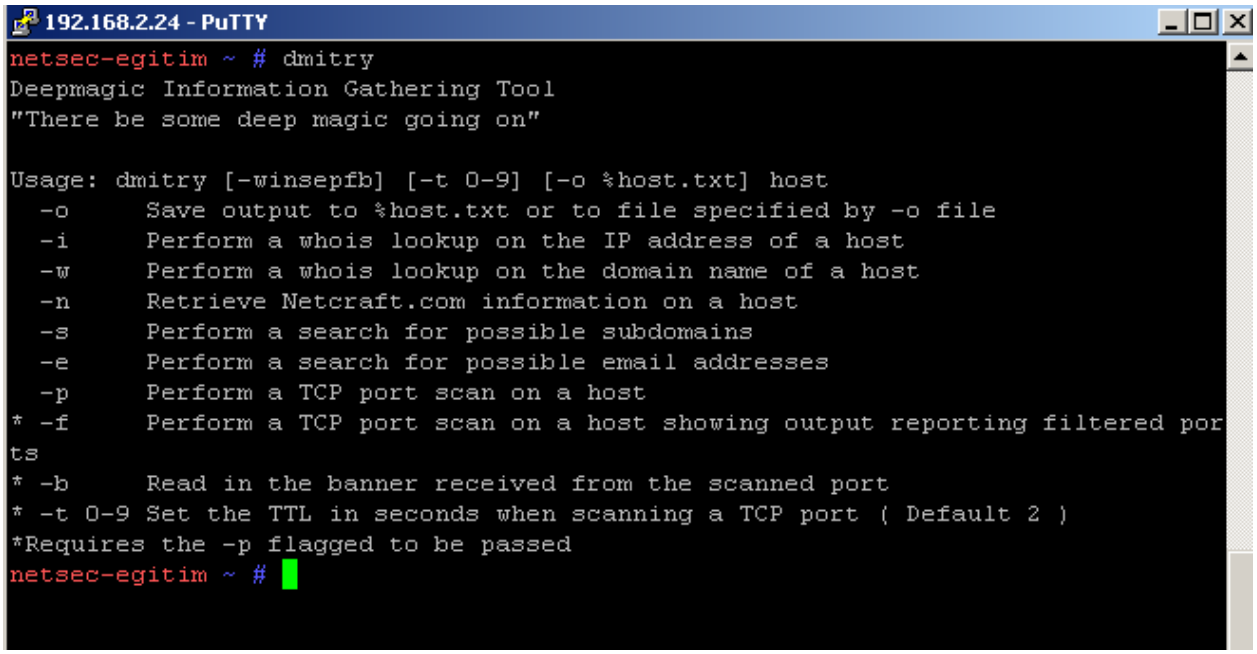
SNMP aracılığı ile bir sistemden hertür bilgi(snmp oidleri bilinerek) edinilebilir. SNMP çalıştıran bir Windows sistem üzerinden bilgi toplama.

```
home-labs snmpenum # 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
```

```
mysqld-nt.exe
inetinfo.exe
...
----------------------------------------
      LISTENING UDP PORTS
----------------------------------------

7
9
13
17
19
161
162
445
500
1029
....
----------------------------------------
      SYSTEM INFO
----------------------------------------

Hardware: x86 Family 16 Model 2 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 5.2
(Build 3790 Uniprocessor Free)


----------------------------------------
      SHARES
----------------------------------------

SYSVOL
NETLOGON
programlar
C:\WINDOWS\SYSVOL\sysvol
C:\WINDOWS\SYSVOL\sysvol\home-labs.lifeoverip.net\SCRIPTS
E:\
```

Dmitry ile Bilgi Toplama

K>Backtrack>Information Gathering>All>Dmitry



Dmitry(Deep Magic Information Gathering Tool) hedef system hakkında olabildiğince fazla bilgi toplayarak bunu raporlar.

Yeni bir özellik sunmamasına rağmen manuel yapılacak çoğu işlemi tek bir adımda yapabilmemize olanak sağlar.

Dmitry ile kısaca ;

Verilen bir domain/ip adresi hakkında whois sorgusu, Netcraft'tan alınma bilgiler, subdomain bilgileri, o domaine ait e-posta adresi, açık TCP portları ve bu portlarda çalışan servislere ait banner bilgileri alınabilir.

netsec-egitim ~ # dmitry -winsepfb www.lifeoverip.net -o rapor.txt
tüm bulduğu bilgileri rapor.txt isimli dosyaya yazar.

Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'rapor.txt'

HostIP:80.93.23.83
HostName:www.lifeoverip.net

Gathered Inet-whois information for 80.93.23.83

....

Gathered Netcraft information for www.lifeoverip.net

Retrieving Netcraft.com information for www.lifeoverip.net
Operating System: FreeBSD
WebServer: Apache/2.2.@4 (FreeBSD) mod_ssl/2.2.4 OpenSSL/0.9.7e-p1 DAV/2
No uptime reports available for host: www.lifeoverip.net
Netcraft.com Information gathered

Gathered Subdomain information for lifeoverip.net

Searching Google.com:80...
HostName:blog.lifeoverip.net
HostIP:80.93.23.83
HostName:netsec.lifeoverip.net
HostIP:80.93.23.83
HostName:www.lifeoverip.net
HostIP:80.93.23.83
Searching Altavista.com:80...
Found 3 possible subdomain(s) for host lifeoverip.net, Searched 0 pages containi
ng 0 results

Gathered E-Mail information for lifeoverip.net
…

Gathered TCP Port information for 80.93.23.83

Port State

21/tcp open
>> 220 Welcome to LifeoverIP FTP service.

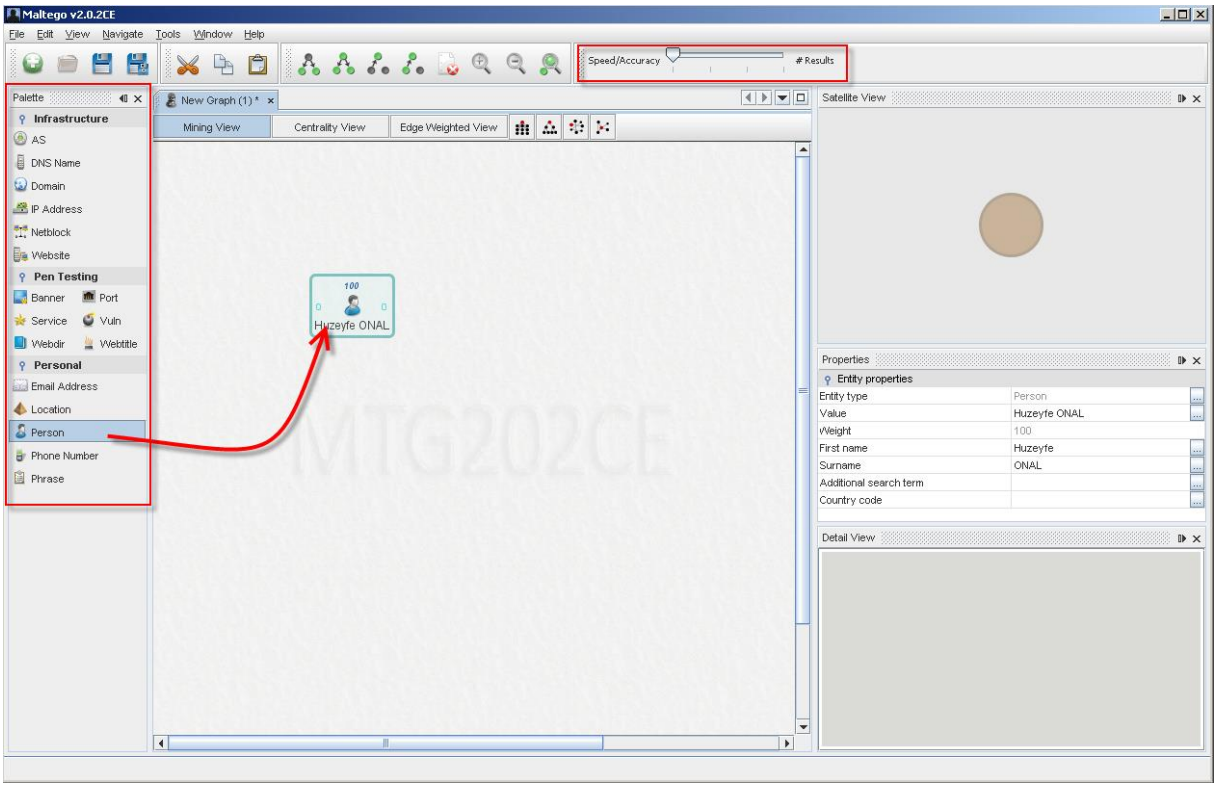
22/tcp open
>> SSH-2.0-OpenSSH_4.5p1 FreeBSD-20031110

23/tcp open

Yeni Nesil Bilgi Toplama Aracı:Maltego

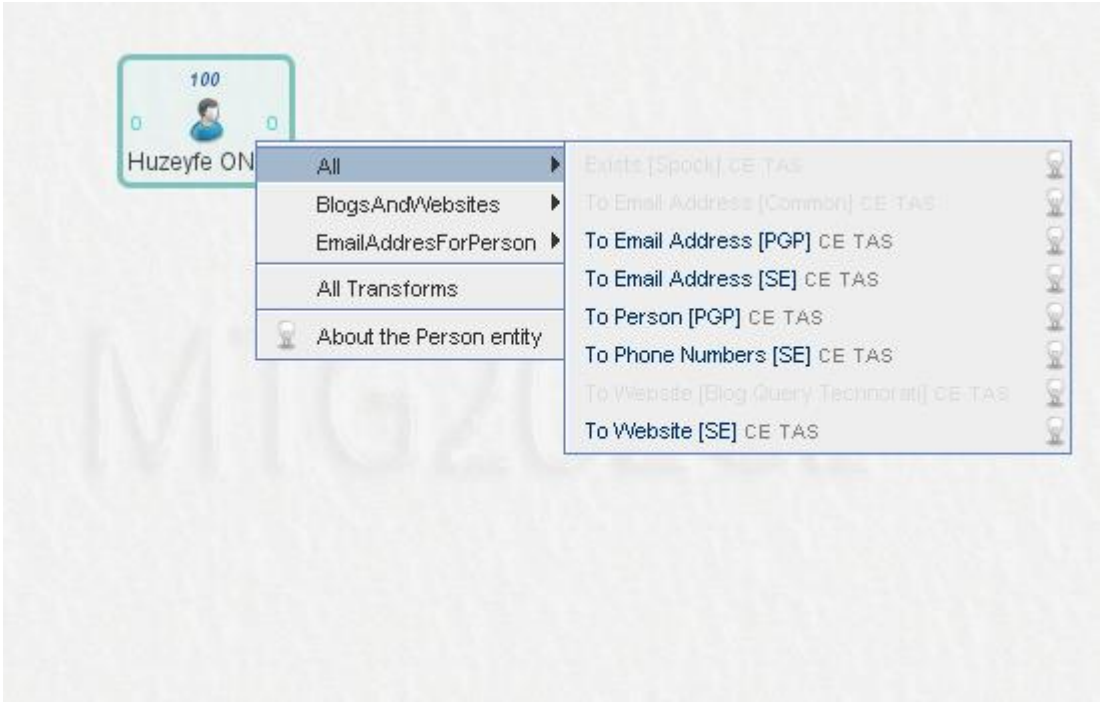
Maltego, bildiğimiz tüm klasik bilgi toplama yöntemlerini birleştirerek merkezi bir yerden kontrol ve raporlama imkanı sunar. Bu sebeple yeni nesil (ikinci nesil) bilgi toplama aracı olarak sınıflandırılır.

Maltego dört ana ekrandan oluşur. Bu ekranlar arama kriterlerin, ana sorgu sayfası, sorgu özellikleri ve üst menüdür.

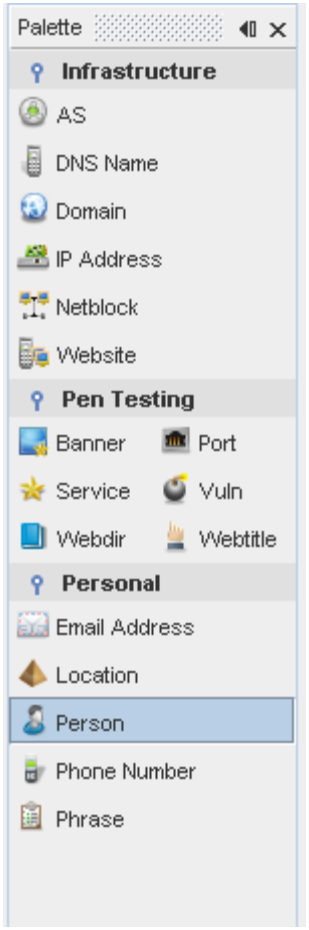


Maltego ile Arama Yapma

Sol taraftaki menüden arama kriteri(şahıs arama, e-posta arama, domain, ip arama vs) belirlenerek ortadakı alana sürüklenir. Sonra ortadaki alanda arama yapılacak kritere ait özellikler çift tıklanarak girilir ve son olarak da objenin üzerinde sağ fare tuşu ile ne tür aramalar yapılacağı belirtilir.

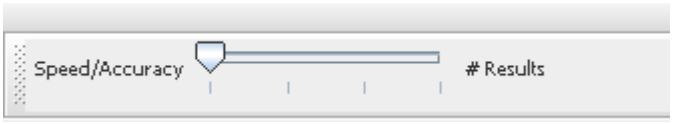


Arama Kriterleri

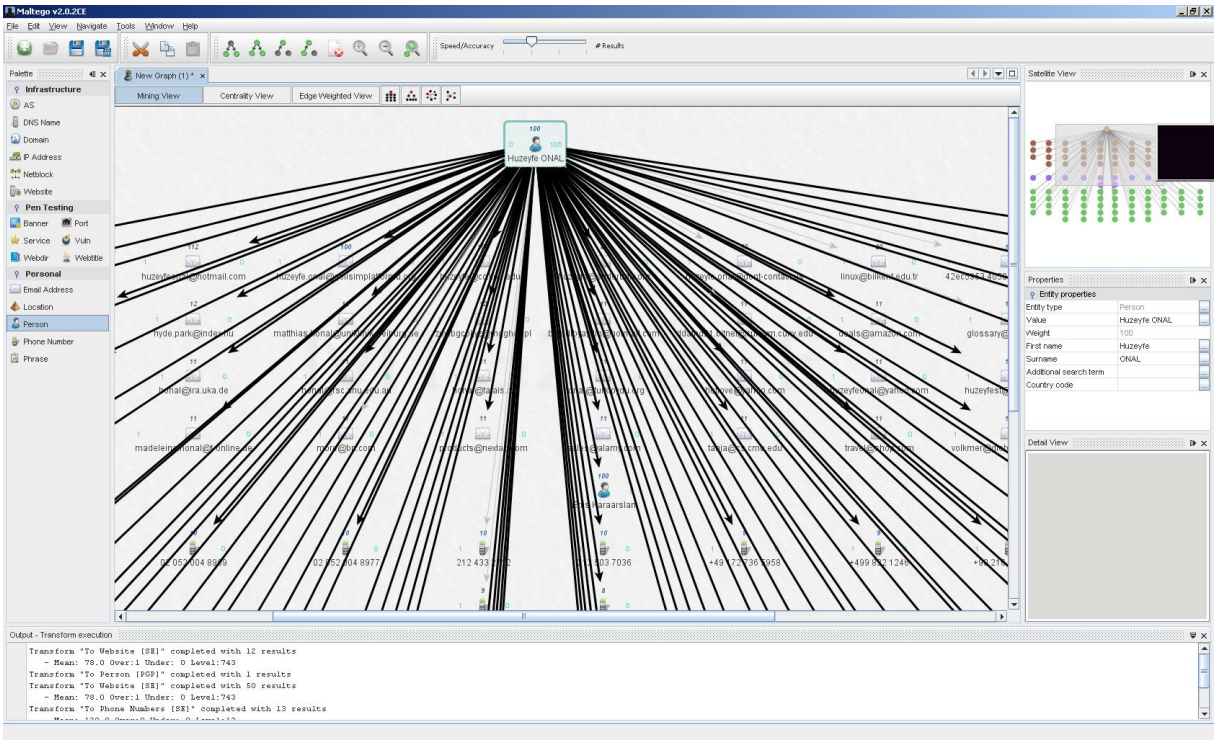


Arama Sonuçları

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 gelinirse o objeye ait özellikler ekranın sağ kısmında belirir.


Maltego v2.0.2CE
File Edit View Navigate Tools Window Help
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1) *
Mining View
Centrality View
Edge Weighted View
Huzeyfe ONAL
Satellite View
Properties
Entity properties
Entity type Person
Value Huzeyfe ONAL
Weight 100
First name Huzeyfe
Surname ONAL
Additional search term
Country code
Detail View
Output - Transform execution
Transform "To Website [SE]" completed with 12 results
- Mean: 78.0 Over:1 Under: 0 Level:743
Transform "To Person [PGP]" completed with 1 results
Transform "To Website [SE]" completed with 50 results
- Mean: 78.0 Over:1 Under: 0 Level:743
Transform "To Phone Numbers [SE]" completed with 13 results