



4. Culegerea de informații (recunoașterea)



Rol

- **Primul pas în etapa de testare**
- **Nu poți ataca ceea ce nu cunoști**
- **Black-box / gray-box test**
- **Obținerea a cât mai multor informații despre țintă**
- **Activitate non-intruzivă pentru țintă**
- **Se efectuează de obicei manual însă poate fi și automatizată prin intermediul scripturilor**

Perspective asupra țintei

- **System view**
 - tehnologii, dispozitive, sisteme de operare
- **Functional / logical view**
 - rolul fiecărui dispozitiv / sistem
- **Physical view**
 - sedii, locațiile în care sunt dispuse echipamentele
- **Temporal view**
 - programul de lucru
- **Social view**
 - date despre angajați
- **Lifecycle view**
 - fazele unui proces de business
- **Consequence view**
 - dacă producerea unui eveniment generează alt eveniment (e.g. accesul neautorizat în clădire duce la apariția poliției / firmei de pază la fața locului)

De unde se pot obține informații?

- **Paginile de web ale companiei / angajaților**
- **Căutare pe Internet**
 - Google, Yahoo
- **Interogare baze de date publice**
 - Whois
 - DNS
- **Social networks**
 - Facebook, LinkedIn
- **Social engineering**

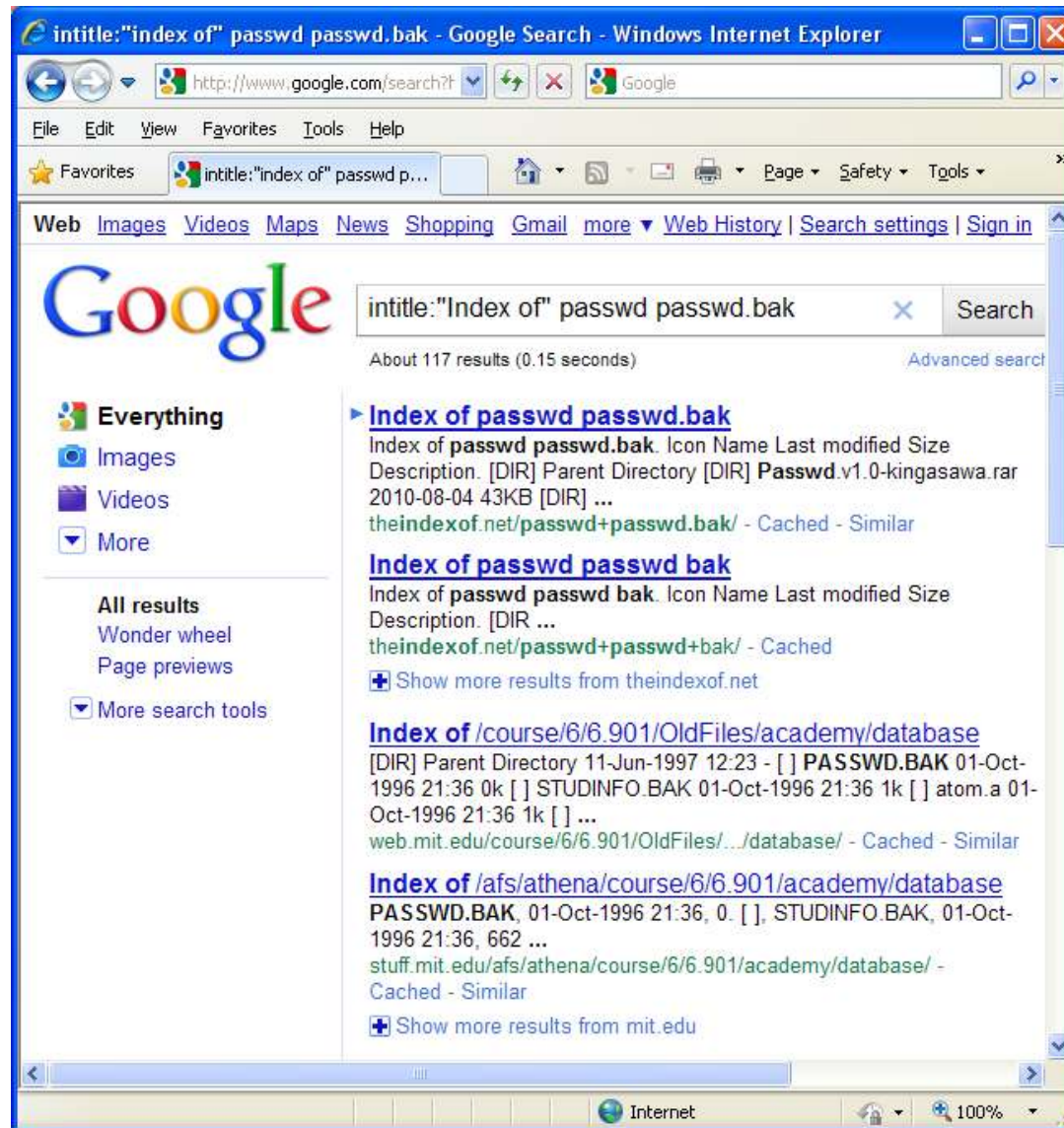
Paginile de web ale companiei

- **Vizitare pasivă a serverelor de Web**
- **Adrese, persoane de contact, numere de telefon, e-mail, evenimente, etc**
- **Mirror Web site**
 - Wget, Teleport Pro
 - grep, findstr
- **Outlook Web Access / Webmail**
 - <https://owa.abc.ro>
 - <https://outlook.abc.ro>
 - <https://webmail.abc.ro>
- **Virtual Private Network**
 - <http://vpn.abc.ro>
 - <http://www.abc.ro/vpn>

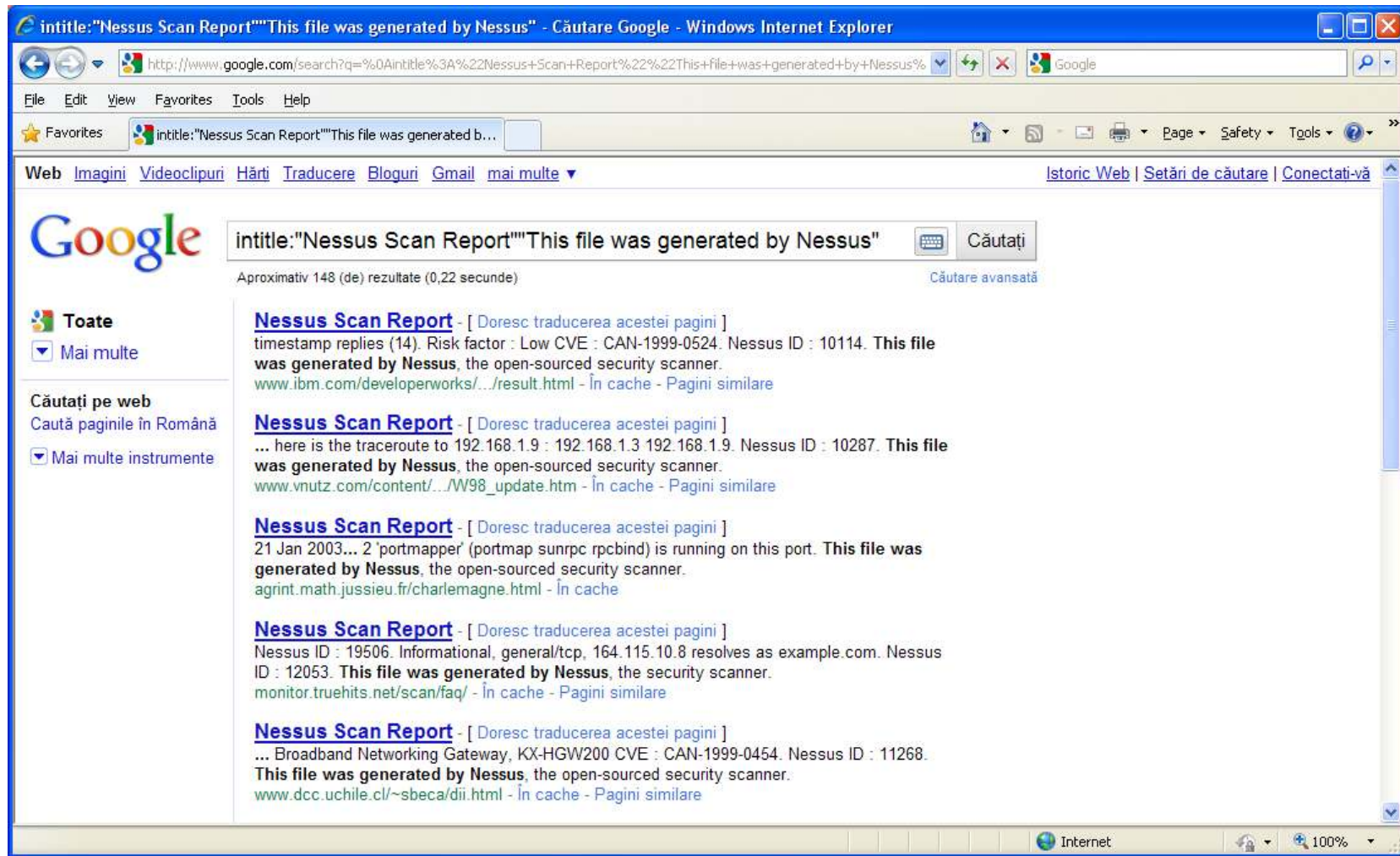
Google Hacking

- Johnny Long, “Google Hacking for Penetration Testers”, Syngress, 2005
- Google search syntax
 - filetype:doc filetype:pdf filetype:xls
 - intext:, intitle:, inurl:
 - allintext:, allintitle:, allinurl:
 - site:gov site:mil site:abc.ro
 - related:www.abc.ro
 - http://www.googleguide.com/advanced_operators.html
- Google cache

Google Hacking (cont.)



Google Hacking (cont.)



The screenshot shows a Windows Internet Explorer browser window displaying Google search results. The search query is "intitle:Nessus Scan Report". The results list several entries, each starting with "Nessus Scan Report" followed by a brief description and a link to the source page. The first result is from www.ibm.com, the second from www.vnutz.com, the third from agrint.math.jussieu.fr, the fourth from monitor.truehits.net, and the fifth from www.dcc.uchile.cl.

intitle:"Nessus Scan Report""This file was generated by Nessus" - Căutare Google - Windows Internet Explorer

http://www.google.com/search?q=%0Aintitle%3A%22Nessus+Scan+Report%22%22This+file+was+generated+by+Nessus%...

File Edit View Favorites Tools Help

intitle:"Nessus Scan Report""This file was generated b...

Web Imagini Videoclipuri Hărți Traducere Bloguri Gmail mai multe

Istoric Web | Setări de căutare | Conectati-vă

Google

intitle:"Nessus Scan Report""This file was generated by Nessus" Căutați

Aproximativ 148 (de) rezultate (0,22 secunde) Căutare avansată

Toate
Mai multe

Căutați pe web
Caută paginile în Română
Mai multe instrumente

Nessus Scan Report - [[Doresc traducerea acestei pagini](#)]
timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524. Nessus ID : 10114. **This file was generated by Nessus**, the open-sourced security scanner.
www.ibm.com/developerworks/.../result.html - În cache - [Pagini similare](#)

Nessus Scan Report - [[Doresc traducerea acestei pagini](#)]
... here is the traceroute to 192.168.1.9 : 192.168.1.3 192.168.1.9. Nessus ID : 10287. **This file was generated by Nessus**, the open-sourced security scanner.
www.vnutz.com/content/.../W98_update.htm - În cache - [Pagini similare](#)

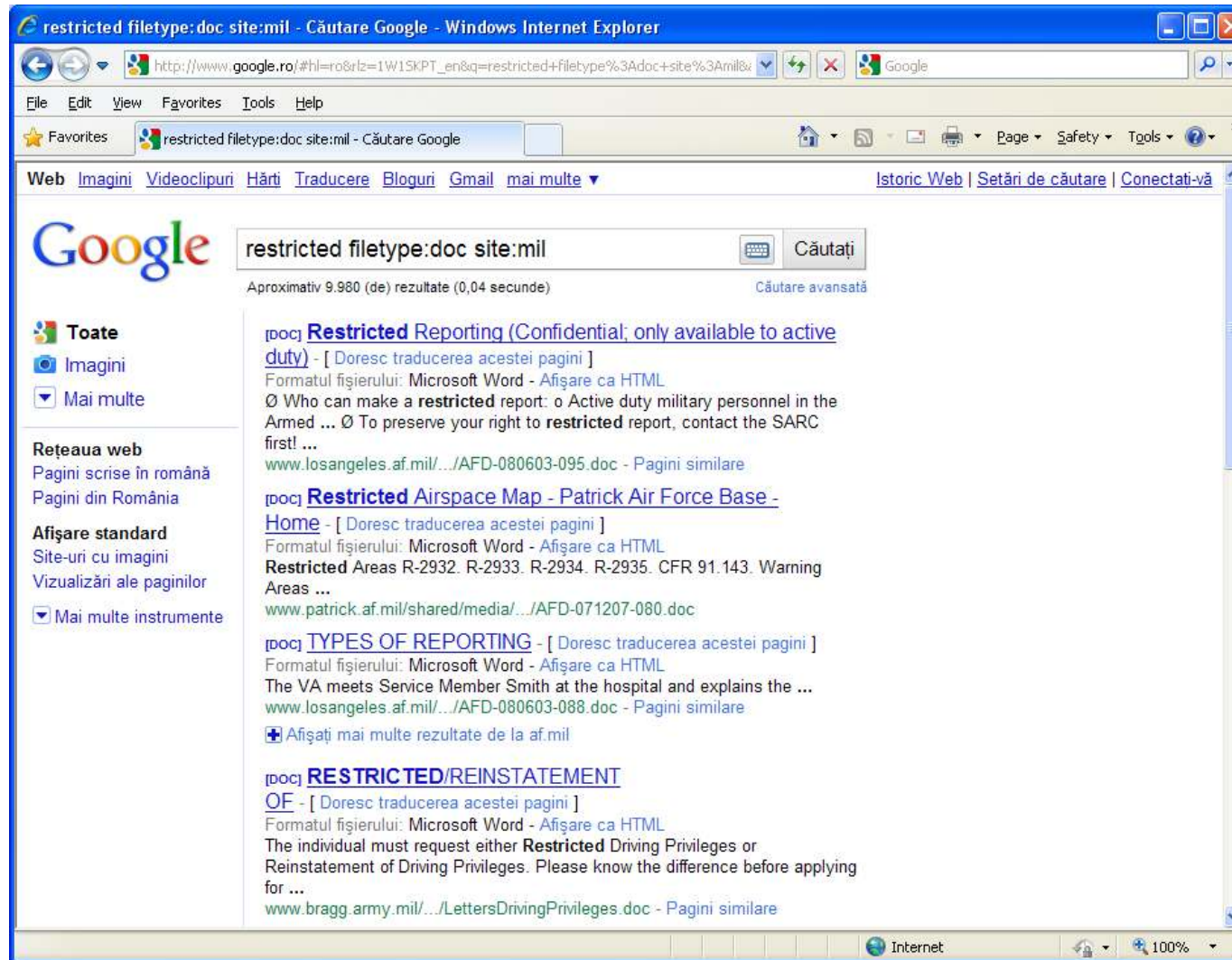
Nessus Scan Report - [[Doresc traducerea acestei pagini](#)]
21 Jan 2003... 2 'portmapper' (portmap sunrpc rpcbind) is running on this port. **This file was generated by Nessus**, the open-sourced security scanner.
agrint.math.jussieu.fr/charlemagne.html - În cache

Nessus Scan Report - [[Doresc traducerea acestei pagini](#)]
Nessus ID : 19506. Informational, general/tcp, 164.115.10.8 resolves as example.com. Nessus ID : 12053. **This file was generated by Nessus**, the security scanner.
monitor.truehits.net/scan/faq/ - În cache - [Pagini similare](#)

Nessus Scan Report - [[Doresc traducerea acestei pagini](#)]
... Broadband Networking Gateway, KX-HGW200 CVE : CAN-1999-0454. Nessus ID : 11268. **This file was generated by Nessus**, the open-sourced security scanner.
www.dcc.uchile.cl/~sbeca/dii.html - În cache - [Pagini similare](#)

Internet 100%

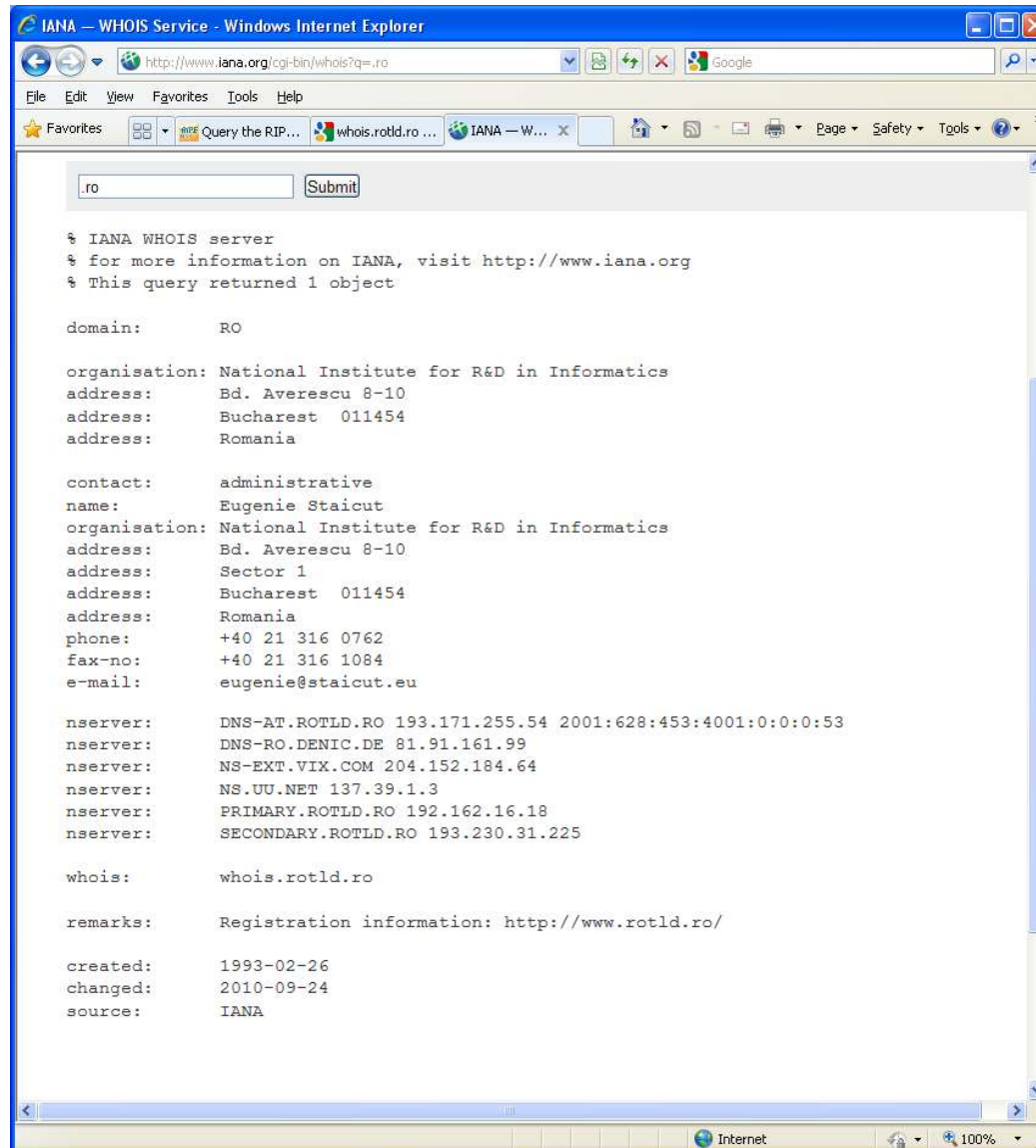
Google Hacking (cont.)



Whois

- **Gestiunea numelor de domeniu, adreselor IP, protocoalelor și numerelor de porturi în Internet:**
 - Internet Assigned Numbers Authority (IANA)
 - <http://www.iana.org>
 - Internet Corporation for Assigned Names and Numbers (ICANN)
 - <http://www.icann.org>
- **Alocarea Adreselor IP - Regional Internet Registries (RIR)**
 - African Network Information Centre (AfriNIC) pentru Africa
 - American Registry for Internet Numbers (ARIN) pentru SUA și Canada
 - Asia-Pacific Network Information Centre (APNIC) pentru Asia și Australia
 - Latin America and Caribbean Network Information Centre (LACNIC) pentru America Latină
 - RIPE NCC pentru Europe, Orientul Mijlociu și Asia Centrală

IANA Search



The screenshot shows a Windows Internet Explorer browser window titled "IANA - WHOIS Service". The address bar contains the URL "http://www.iana.org/cgi-bin/whois?q=.ro". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The Favorites bar shows several items, including "Query the RIP...", "whois.rotld.ro...", and "IANA - W...". The main content area displays the results of a WHOIS query for the ".ro" domain. The results are formatted as text and include the following information:

```
.ro [Submit]

% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:          RO

organisation:    National Institute for R&D in Informatics
address:         Bd. Averescu 8-10
address:         Bucharest 011454
address:         Romania

contact:         administrative
name:            Eugenie Staicut
organisation:    National Institute for R&D in Informatics
address:         Bd. Averescu 8-10
address:         Sector 1
address:         Bucharest 011454
address:         Romania
phone:           +40 21 316 0762
fax-no:          +40 21 316 1084
e-mail:          eugenie@staicut.eu

nserver:         DNS-AT.ROTLD.RO 193.171.255.54 2001:628:453:4001:0:0:0:53
nserver:         DNS-RO.DENIC.DE 81.91.161.99
nserver:         NS-EXT.VIX.COM 204.152.184.64
nserver:         NS.UU.NET 137.39.1.3
nserver:         PRIMARY.ROTLD.RO 192.162.16.18
nserver:         SECONDARY.ROTLD.RO 193.230.31.225

whois:           whois.rotld.ro

remarks:         Registration information: http://www.rotld.ro/

created:         1993-02-26
changed:         2010-09-24
source:          IANA
```

ROTLD Search

The screenshot shows the ROTLD website interface in Internet Explorer. The browser title is "RoTLD - Romanian Top Level Domain - Windows Internet Explorer". The address bar shows "http://www.rotld.ro/". The page content includes a navigation menu on the left with categories like "Acasă", "Domenii .ro", "Adrese IP", "Contact Info", and "Hartă Site". The main content area displays a search result for "mta.ro".

RoTLD - Romanian Top Level Domain

Whois | Domeniu Nou | Intrebari Frecvente | Contact Info

RoTLD > Domenii.ro > Whois

Cautare in baza de date Whois:

Este interzisa folosirea datelor de pe acest server in oricare alt scop decat operarea retelei. In special este interzisa folosirea lor in scopuri publicitare.

Domain Info

Domain Name: mta.ro
Registrar: ICI - ROTLD
Registration Date: Before 2001
Nameservers:
dns1.mta.ro
ns2.afraid.org
Domain Status: OK

Domain Holder

Military Technical Academy Bucharest
Military Technical Academy Bucharest
George Cosbuc Blvd., 81-83
Bucharest, xx, RO
Phone: +40.213363309
Email: adrian.hada@gmail.com

Technical Contact

Private personal data. Restricted from publishing.
For contacting domain technical person please click [here](#).

17 - Octombrie - 2010 © 2006 RoTLD. All Rights Reserved.

RIPE Search

Query the RIPE Database - Windows Internet Explorer

http://www.db.ripe.net/whois?form_type=simple&full_query_string=6

File Edit View Favorites Tools Help

Query the RIPE Database


Query the RIPE Database

Search for 213.177.4.170 Search Reset Form

By pressing the "Search" button you explicitly express your agreement with the [RIPE Database Terms and Conditions](#).

Advanced Search Form

[Switch to the RIPE TEST Database](#)

 **RIPE NCC E-Learning Centre**

§ This is the RIPE Database query service.
§ The objects are in RPSL format.
§
§ The RIPE Database is subject to Terms and Conditions.
§ See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

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

§ Information related to '213.177.4.160 - 213.177.4.175'

```
inetnum:      213.177.4.160 - 213.177.4.175
netname:      MTA-NET
descr:        Academia Tehnica Militara
country:      RO
admin-c:      AG10287-RIPE
tech-c:       MA3173-RIPE
status:       ASSIGNED PA
mnt-by:       ROSTIS-MNT
source:       RIPE # Filtered

person:       Adrian Gagi
address:      Bulevardul George Cosbuc, nr.81-83, sector 5, Bucuresti
phone:        +4021 335 46 60
nic-hdl:      AG10287-RIPE
mnt-by:       ROSTIS-MNT
e-mail:       webadmin@mta.ro
source:       RIPE # Filtered

person:       Minta Adrian
address:      Special Telecommunications Service
address:      323A Splaiul Independentei, Bucharest 6
phone:        +40212022660
e-mail:       adrian.minta@stsisp.ro
nic-hdl:      MA3173-RIPE
mnt-by:       ROSTIS-MNT
source:       RIPE # Filtered
```

Internet 100%

Interogări DNS

- nslookup, dig, host

- Tipuri de înregistrări

SOA	Indicates authority for the domain
NS	Host's or domain's name server(s)
MX	Host's or domain's mail exchanger(s)
A	A host's IP address
PTR	Host's domain name, host identified by its IP address
SRV	Service location record
HINFO	Host information record
TXT	Generic text record
CNAME	Host's canonical name (aliases)
RP	Responsible person

- \$dig mta.ro SOA

- Transfer de zone

- \$dig @server domain AXFR

- de regulă, această operație este restricționată în mod corespunzător

Interogări DNS (cont.)

```
C:\WINDOWS\system32\cmd.exe - nslookup

C:\>nslookup
Default Server:
Address: 192.168.2.1

> set type=SOA
> mta.ro
Server:
Address: 192.168.2.1

Non-authoritative answer:
mta.ro
      primary name server = dns1.mta.ro
      responsible mail addr = root.mta.ro
      serial = 2009040103
      refresh = 28800 (8 hours)
      retry = 7200 (2 hours)
      expire = 604800 (7 days)
      default TTL = 86400 (1 day)

mta.ro nameserver = dns1.mta.ro
mta.ro nameserver = ns2.afraid.org
dns1.mta.ro internet address = 213.177.4.170
ns2.afraid.org internet address = 174.37.196.55
>
```

Interogări DNS (cont.)

```
C:\WINDOWS\system32\cmd.exe - nslookup

C:\>nslookup
Default Server:
Address: 192.168.2.1

> server dns1.mta.ro
Default Server: dns1.mta.ro
Address: 213.177.4.170

> set type=MX
> mta.ro
Server: dns1.mta.ro
Address: 213.177.4.170

mta.ro MX preference = 5, mail exchanger = mail.mta.ro
mta.ro MX preference = 10, mail exchanger = relay.mta.ro
mta.ro nameserver = ns2.afraid.org
mta.ro nameserver = dns1.mta.ro
mail.mta.ro internet address = 213.177.4.170
relay.mta.ro internet address = 213.177.4.170
dns1.mta.ro internet address = 213.177.4.170
>
```


Recunoaștere la nivel de rețea

- **Traceroute**
 - descoperire rute, localizare firewall, routere, etc
- **tracert (Windows)**
 - folosește ICMP
- **traceroute (Linux)**
 - folosește UDP
- **NeoTrace, VisualRoute, VisualLookout**
 - interfață grafică

tracert

```
C:\WINDOWS\system32\cmd.exe

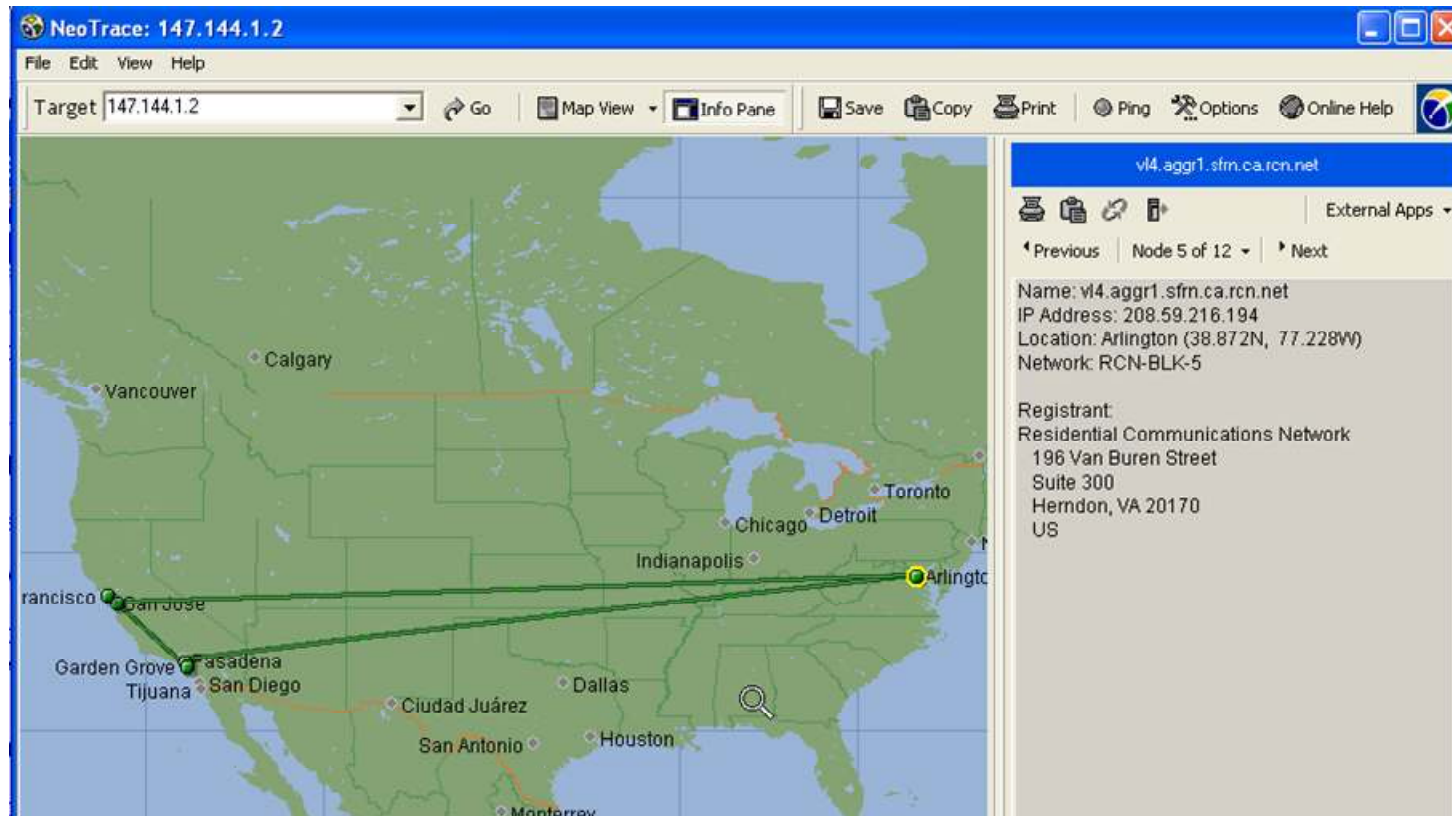
C:\>tracert mta.ro

Tracing route to mta.ro [213.177.4.170]
over a maximum of 30 hops:

  0  3 ms    3 ms    3 ms    . [192.168.2.1]
  1  5 ms    5 ms    6 ms    10.0.0.1
  2  7 ms   17 ms   6 ms    172.19.212.73
  3  7 ms    4 ms    5 ms    xr01.bucuresti.rdsnet.ro [213.154.124.52]
  4  6 ms    6 ms    4 ms    sts.bucuresti.rdsnet.ro [82.76.246.246]
  5  6 ms    6 ms    6 ms    v15-viil.stsisp.ro [193.151.28.39]
  6  8 ms   11 ms   8 ms    mta.ro [213.177.4.170]

Trace complete.
```

NeoTrace



Unelte online

- whois.net
- www.dnsstuff.com
- www.netcraft.com
- www.sampade.com

