



Nebrija
Universidad MADRID

Hacking Ético

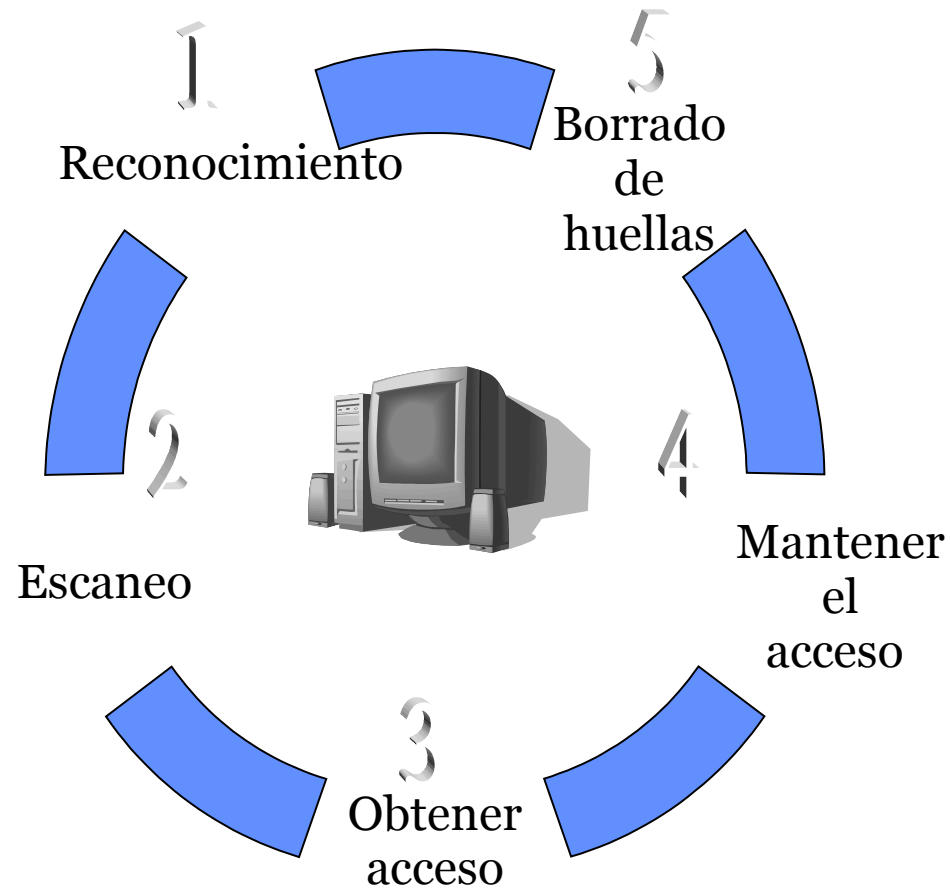
Módulo I

Fase 1: Obtención de
información

Objetivos

- Visión general de la fase de reconocimiento
- Entender la metodología de obtención de información de los hackers
- Repaso de algunas herramientas

Obtención de información



Obtención de información

- Dos fases en el pre-ataque:
 - Footprinting (obtención de información)
 - Escaneo / Enumeración
- Obtención de los perfiles de seguridad de una organización haciendo uso de una metodología (*footprinting*).
- El resultado del *footprinting* es un perfil único de la organización en cuanto a sus redes (Internet / Intranet / Extranet / Wireless) y sistemas.

Fase 1 (pre ataque)- *Footprinting*

1.- Obtener información inicial

- whois
- nslookup

2.- Localizar el rango de red

- Traceroute

Metodología para la obtención de información

- Obtener información inicial
 - Localizar el rango de la red
 - Averiguar qué máquinas están activas
 - Puertos abiertos / access points
 - Detectar sistemas operativos
 - Descubrir servicios escuchando en puertos
 - Topología de la red
- } Footprinting
} Footprinting

Obtener información inicial

■ Incluiría:

- Nombres servidores DNS, algunas IPs
- Localizaciones geográficas de la empresa.
- Contactos (Teléfono / mail)

■ Fuentes de Información:

- Web de la empresa
- Whois: <http://www.internic.net/whois.html>
- Nslookup – posible transferencia de zona DNS
- www.all-nettols.com
- Infojobs / monster
- Google:
 - allinurl:tsweb/default.htm

Whois

Registrant:
targetcompany (targetcompany-DOM)
XXX Everest Blk A.Enclave
Ameerpet
Hyderabad
Andrapradesh, 500038
IN
Domain Name: targetcompany.COM

Administrative Contact:
R****, J**** (RJXXZ-ORG) targetcompany@HD1.VSML.NET.IN
targetcompany
XXX, Everest Block, A.Enclave,
Ameerpet
Hyderabad, Andrapradesh 500038
IN 91 40 XXXX 329X Fax- 91 40 XXXX 329X
Technical Contact:
S****, V**** (VSXX) techcontact@WEBINDIA.COM
XXS Inc
XXX R Lane
Hoffman Estates, IL 60194
US. 408/XXX-XXXX 408/XXX-XXXX
Record expires on 14-Oct-200X.
Record created on 13-Oct-1997.
Database last updated on 17-Mar-2003 07:49:04 EST.

Domain servers in listed order:
NS1.WEBINDIA.COM 204.XXX.140.X01
NS2.WEBINDIA.COM 204.XXX.141.X01

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: targetcompany.COM

Administrative Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Technical Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Domain servers in listed order:
NS1.WEBHOST.COM XXX.XXX.XXX.XXX
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

ARIN

- ARIN permite hacer búsquedas whois
- Podemos obtener el rango de red
- Y dirigir nuestros esfuerzos en ese rango

The screenshot displays the ARIN website interface. At the top, there is a navigation bar with links for Contact Us, Mailing Lists, Site Map, Statistics, Network Abuse, and Newsletter. Below this is a search bar for WHOIS with a 'SEARCH WHOIS' button. A secondary navigation bar contains links for Registration, Policy, Meetings, Membership, Library, Internet Info, Tools, and About Us. The main content area features the ARIN logo and the text 'American Registry for Internet Numbers'. A quote describes ARIN's mission: 'Applying the principles of stewardship, ARIN, a nonprofit corporation, allocates Internet Protocol resources; develops consensus-based policies; and facilitates the advancement of the Internet through information and educational outreach'. A prominent yellow box highlights the 'Database & Template Conversion Information Center'. Below this, there are sections for Registration, Policy, Meetings, and Library, each with a brief description of the services or information provided. A left sidebar contains 'Template Conversion Tips' and 'Announcements' with dates and links to more information.

Screenshot: ARIN Whois Output

Output from ARIN Whois

[ARIN Home Page](#) [ARIN Site Map](#) [ARIN Whois Help](#) [NEW! Database & Template Conversion Information Center](#)

Search for:

Search results for: 207.46.230.218

Microsoft ([NETBLK-MICROSOFT-GLOBAL-NET](#))
One Redmond Way
Redmond, WA 98052
US

Netname: MICROSOFT-GLOBAL-NET
Netblock: 207.46.0.0 - 207.46.255.255

Coordinator:
Microsoft ([ZM39-ARIN](#)) noc@microsoft.com
425-936-4200

Domain System inverse mapping provided by:

DNS1.CP.MSFT.NET	207.46.138.20
DNS2.CP.MSFT.NET	207.46.138.21
DNS1.TK.MSFT.NET	207.46.232.37
DNS2.TK.MSFT.NET	207.46.232.38

IP Address block allocated to the domain [microsoft.com](#)

Nslookup

- Nslookup – resolución DNS.

Nslookup y DNS

- Nslookup – resolución DNS.
- Dominios y zonas.
- Fichero de zona
- Registros de recursos (RR)
- Registros de recursos: SOA, NS, A, CNAME, MX
- Transferencia de zona entre servidores DNS – ya lo haremos.

Determinar el rango de red

■ Incluiría:

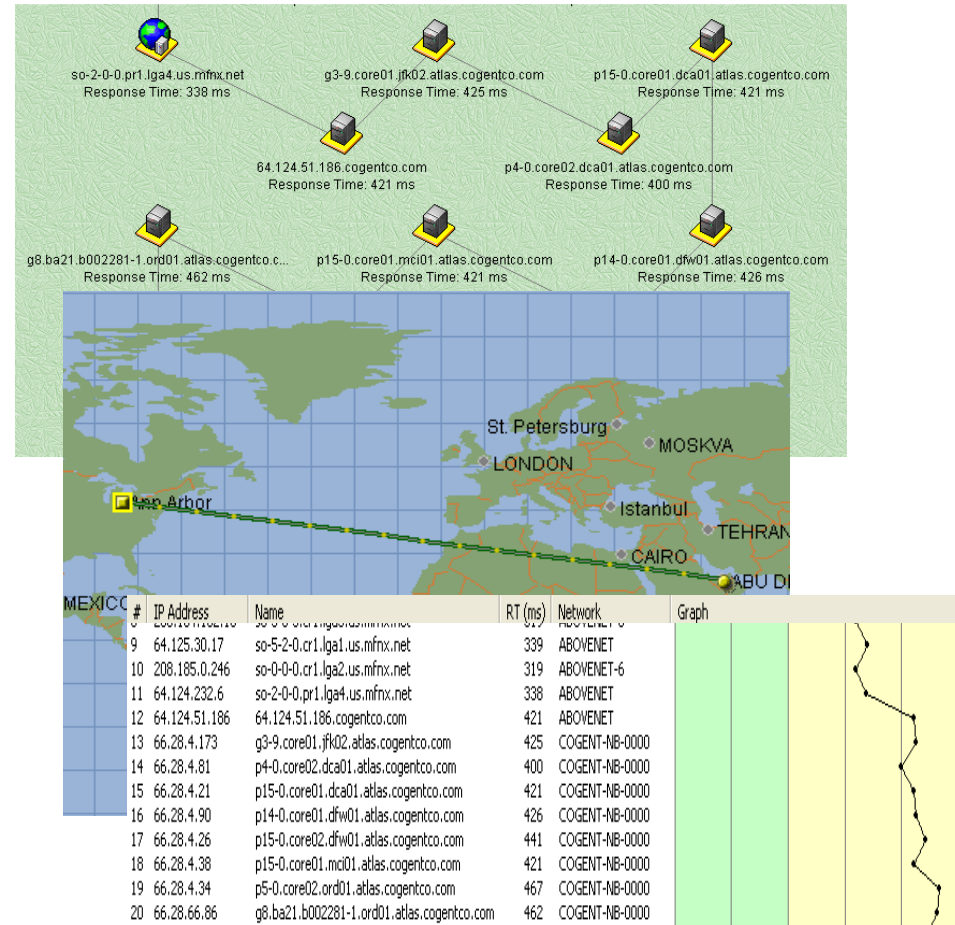
- Encontrar el rango de Ips
- Encontrar la máscara de subred

■ Fuentes de información:

- ARIN (American Registry of Internet Numbers)
- Traceroute

■ Hacking Tool:

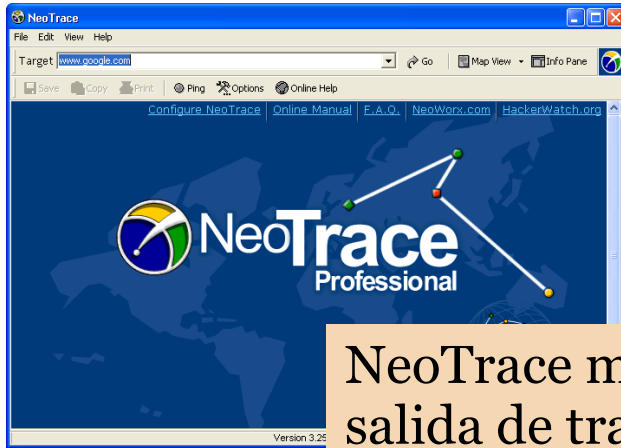
- NeoTrace / Geotrace
- VisualRoute /Xroute (xt)
- Whatroute



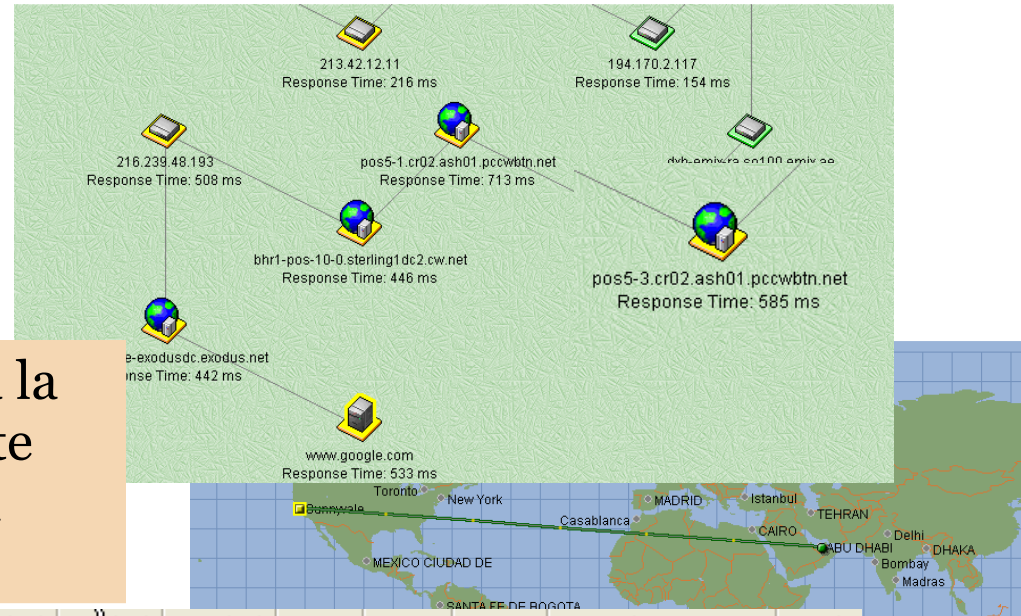
Traceroute

- Traceroute se basa en el parámetro de IP TTL (Time To Live).
- Saltos de routers.
- Cada router en un salto disminuye el TTL. Cuando el TTL se hace cero, devuelve un mensaje "TTL exceeded" (usando ICMP) al origen.

Tool: NeoTrace (Now McAfee Visual Trace) – Geotrace (GNU)



NeoTrace muestra la salida de traceroute visualmente en un mapa.



#	IP Address	Name	RT (ms)	Ave (ms)	Min (ms)	Max (ms)	# S...	# D...	% Loss	Network	Graph
1	217.165.236.73	SAM	0	0	0	0	1	0	0 %	----	
2	213.42.12.11	----	216	216	216	216	1	0	0 %	AE-EMIRNET-990929	
3	213.42.12.130	----	135	135	135	135	1	0	0 %	AE-EMIRNET-990929	
4	194.170.2.117	----	154	154	154	154	1	0	0 %	EMIRNET-EMIRNET	
5	195.229.31.66	dxh-emix-rb.ge130.emix.ae	159	159	159	159	1	0	0 %	AE-EMIRNET-971125	
6	195.229.0.234	dxh-emix-ra.so100.emix.ae	139	139	139	139	1	0	0 %	EMIRNET-EMIRNET	
7	166.63.210.62	bcr2.thamesside.cw.net	442	442	442	442	1	0	0 %	CW-NETCS2	
8	63.216.0.42	pos5-1.cr02.ash01.pccwbtn.net	713	713	713	713	1	0	0 %	CAIS-CIDR7	
9	206.24.238.166	bhr1-pos-10-0.sterling1dc2.cw.net	446	446	446	446	1	0	0 %	CW-05BLK	
10	216.239.48.193	----	508	508	508	508	1	0	0 %	GOOGLE	
11	216.109.88.218	218-google-exodusdc.exodus.net	442	442	442	442	1	0	0 %	DC3-8	
12	216.239.39.99	www.google.com	533	533	533	533	1	0	0 %	GOOGLE	

Tool: VisualRoute Trace

VisualRoute 7.1c Trial Version

File Edit Options Tools Help

Address IP Addresses Advanced mode

Report for www.visualware.com [198.64.153.97]

Analysis: www.visualware.com [pop.visualware.com] was found in 14 hops (TTL=244). It is a HTTP server (running Apache/1.3.27 (Unix) mod_jk/1.2.0).

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0 467	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		125		Emirates Telecommunicati
2		213.42.12.195	-	(United Arab Emirates)		122		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		124		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		122		Emirates Telecommunicati
5		64.86.138.117	if-0-0.core2.Newark.tel	Newark, NJ, USA	-05:00	420		Teleglobe Inc. TELEGLOBE
6		129.250.9.229	p4-2-0-0.r00.nwrknj01.i	Newark, NJ, USA	-05:00	419		Verio, Inc. VRIO-129-250
7		129.250.2.217	p16-0-1-1.r20.nycmny0	New York, NY, USA	-05:00	418		Verio, Inc. VRIO-129-250
8		129.250.2.33	p64-0-0-0.r21.nycmny0	New York, NY, USA	-05:00	421		Verio, Inc. VRIO-129-250
9		129.250.5.99	p16-1-0-1.r21.asbnva0	Ashburn, VA, USA	-05:00	418		Verio, Inc. VRIO-129-250
10		129.250.2.34	p64-0-0-0.r20.asbnva0	Ashburn, VA, USA	-05:00	436		Verio, Inc. VRIO-129-250
11		129.250.2.74	p16-3-0-0.r00.stngva01	Sterling, VA, USA	-05:00	420		Verio, Inc. VRIO-129-250
12		129.250.27.184	ge-4-1.c00.stngva01.us	Sterling, VA, USA	-05:00	429		Verio, Inc. VRIO-129-250
13		161.58.157.61	-	...		420		Verio, Inc. VRIO-161-058
14		198.64.153.97	www.visualware.com	...		430		Verio, Inc. VRIO-198-063

Roundtrip time to www.visualware.com, average = 430ms, min = 420ms, max = 436ms -- Mar 18, 2003 2:36:39 PM

Tool: VisualRoute Mail Tracker

Report for olympus.bic.nus.edu.sg [137.132.19.100]

Analysis: 'olympus.bic.nus.edu.sg' was found in 24 hops (TTL=240). It is a SMTP server (ESMTP Sendmail 8.12.8/8.12.7).

eMailTracker by Visualware

tinwee@bic.nus.edu.sg

Server	Prio	IP Address	Status
olympus.bic.nus.edu.sg	10	137.132.19.100	ESMTP Sendmail 8.12.8/8.12.7

Click on a server name to start a VisualRoute trace

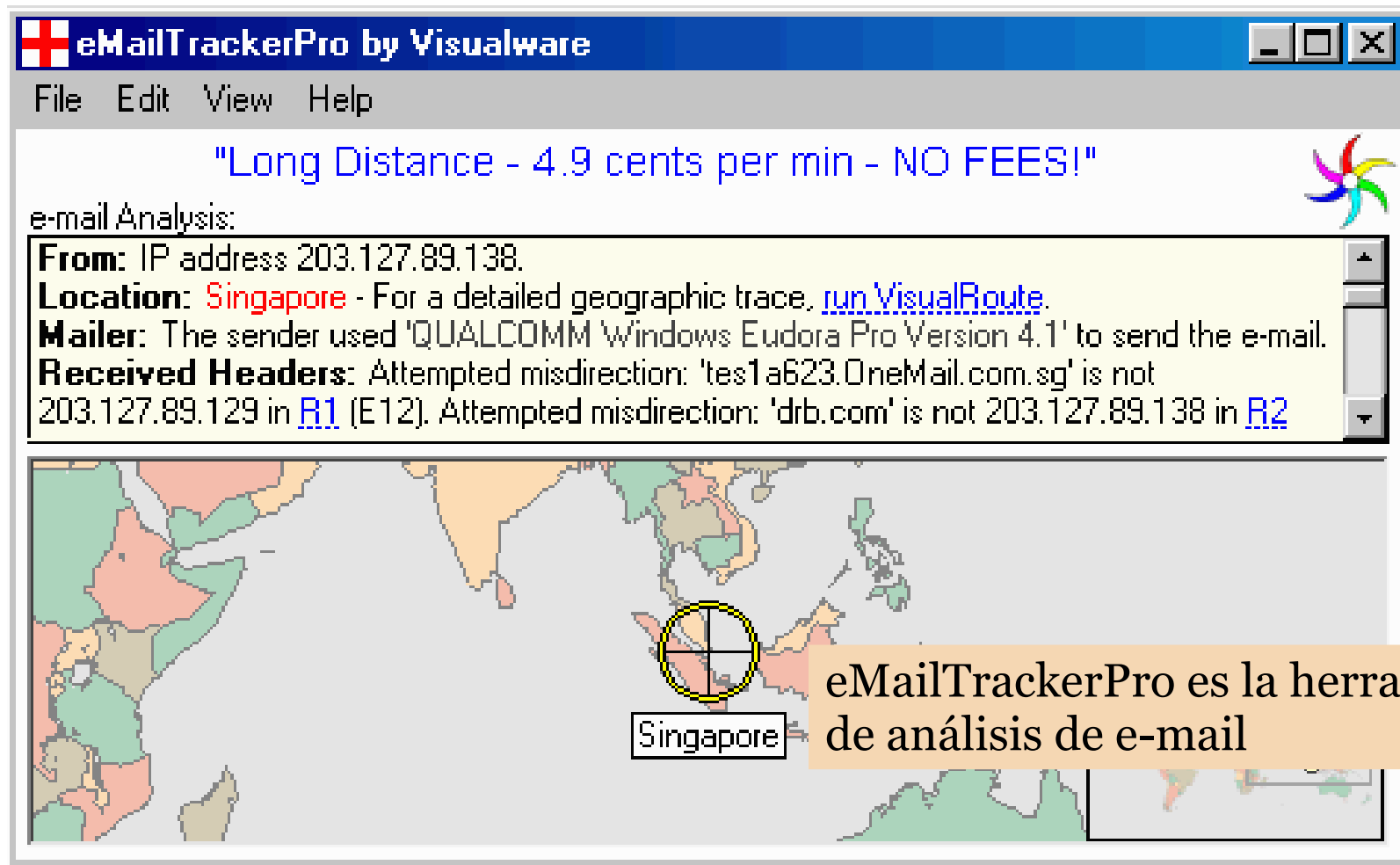
Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		2537		Emirates Telecommunicati
2		213.42.12.131	-	(United Arab Emirates)		2513		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunicati
5		195.229.31.34	auh-emix-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunicati
6		62.216.144.25	-	(United Kingdom)	*	2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.0.core1.sfr1.fi	(United Kingdom)	*	2894		FLAG Telecom Limited
8		166.90.133.165	gige4-1-116.ipcolo2.Sa	San Francisco, CA, US	-08:00	2655		Level 3 Communications, It
9		209.244.14.201	gigabitethernet4-2.core	San Francisco, CA, US	-08:00	2695		Level 3 Communications, It
10		209.247.10.233	so-4-0-0.mp2.SanFran	San Francisco, CA, US	-08:00	3008		Level 3 Communications, It

Screenshot: VisualRoute Mail Tracker

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		2537		Emirates Telecommunicati
2		213.42.12.131	-	(United Arab Emirates)		2513		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunicati
5		195.229.31.34	auh-emix-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunicati
6		62.216.144.25	-	(United Kingdom)	*	2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.0.core1.sfr1.fl	(United Kingdom)	*	2894		FLAG Telecom Limited
8		166.90.133.165	gige4-1-116.ipcolo2.Sa	San Francisco, CA, US	-08:00	2655		Level 3 Communications, It
9		209.244.14.201	gigabithernet4-2.core	San Francisco, CA, US	-08:00	2695		Level 3 Communications, It
10		209.247.10.233	so-4-0-0.mp2.SanFran	San Francisco, CA, US	-08:00	3008		Level 3 Communications, It
11		64.159.0.218	so-2-0-0.mp2.SanJose	San Jose, CA, USA	-08:00	3073		Level 3 Communications, It
12		64.159.2.165	gigabithernet5-2.core	San Jose, CA, USA	-08:00	3009		Level 3 Communications, It
13		209.244.3.246	GigabitEthernet5-0.edg	Palo Alto, CA, USA	-08:00	2996		Level 3 Communications, It
14		209.245.146.150	Singtel-Level3-oc3.ix.si	...		2962		Level 3 Communications, It
15		203.208.182.21	-	Singapore	+08:00	2974		SingTel Internet Exchange
16		203.208.172.29	p6-8.sngtp-cr2.ix.singte	Singapore	+08:00	3061		SingTel Internet Exchange
17		202.160.250.154	-	Singapore	+08:00	3029		Singapore Telecommunica
18		165.21.12.78	FE-4-0-0.lavender.sing	(Singapore)	+08:00	2995		Singapore Telecommunica
19	20	165.21.48.102	-	Singapore	+08:00	3201		Singapore Telecommunica
20	30	137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3473		National University of Singa
21	30	137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3276		National University of Singa
22		137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3179		National University of Singa
23		137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3159		National University of Singa
24		137.132.19.100	olympus.bic.nus.edu.sg	(Singapore)	+08:00	3115		National University of Singa

Roundtrip time to olympus.bic.nus.edu.sg, average = 3115ms, min = 1183ms, max = 4296ms -- Mar 18, 2003 2:28:03 PM

Tool: eMailTrackerPro



The screenshot displays the eMailTrackerPro application window. The title bar reads "eMailTrackerPro by Visualware". The menu bar includes "File", "Edit", "View", and "Help". The main content area shows an email analysis report for the subject "Long Distance - 4.9 cents per min - NO FEES!". The report includes the following details:

- From:** IP address 203.127.89.138.
- Location:** Singapore - For a detailed geographic trace, [run VisualRoute](#).
- Mailer:** The sender used 'QUALCOMM Windows Eudora Pro Version 4.1' to send the e-mail.
- Received Headers:** Attempted misdirection: 'tes1a623.OneMail.com.sg' is not 203.127.89.129 in [R1](#) (E12). Attempted misdirection: 'drb.com' is not 203.127.89.138 in [R2](#)

Below the text is a map of Southeast Asia with a yellow circle highlighting Singapore. A text box labeled "Singapore" is positioned over the map. An orange callout box on the right side of the map contains the text: "eMailTrackerPro es la herramienta de análisis de e-mail".

Ejemplo

■ wikipedia.org

- whois (www.betterwhois.org)
 - nombres servidores DNS
 - ...
- nslookup – sacar la IP del servidor DNS
- traceroute – obtener el nombre del servidor web
- nslookup – obtener la IP del servidor web

Resumen

- Siete fases en el proceso de obtención de información.
- Footprinting – deberíamos obtener como resultado un perfil del objetivo.
- Whois y ARIN pueden darnos información pública de un dominio muy valiosa.
- Traceroute y mail tracking pueden ser usados para identificar Ips de la red (que podría venir bien para hacer luego IP spoofing)
- Nslookup puede revelar usuarios específicos y permitirnos realizar una transferencia de zona.
- En el siguiente módulo veremos más fases.