Chapter 5
Phase 1: Reconnaissance

Reconnaissance

- Finding as much information about the target as possible before launching the first attack packet
- Reconnaissance techniques
  - Low tech methods
  - General web searches
  - Whois databases
  - DNS

Low-Technology Reconnaissance

- Social Engineering
- Physical Break-In
- Dumpster Diving

Social Engineering

- Finding pretext to obtain privileged information or services
- Defense
  - user awareness

Physical Break-In

- Methods
  - Walking past unlocked doors to data center
  - Piggyback behind legitimate employee
- Defense
  - security badges
  - track computers leaving premises
  - physically lock down servers
  - Use locks on cabinets containing sensitive information
  - Use automatic password-protected screen savers
  - Encrypt stored files

Dumpster Diving

- Retrieving sensitive information from trash
- Defense
  - Paper shredder

Reconnaissance via Searching the Web

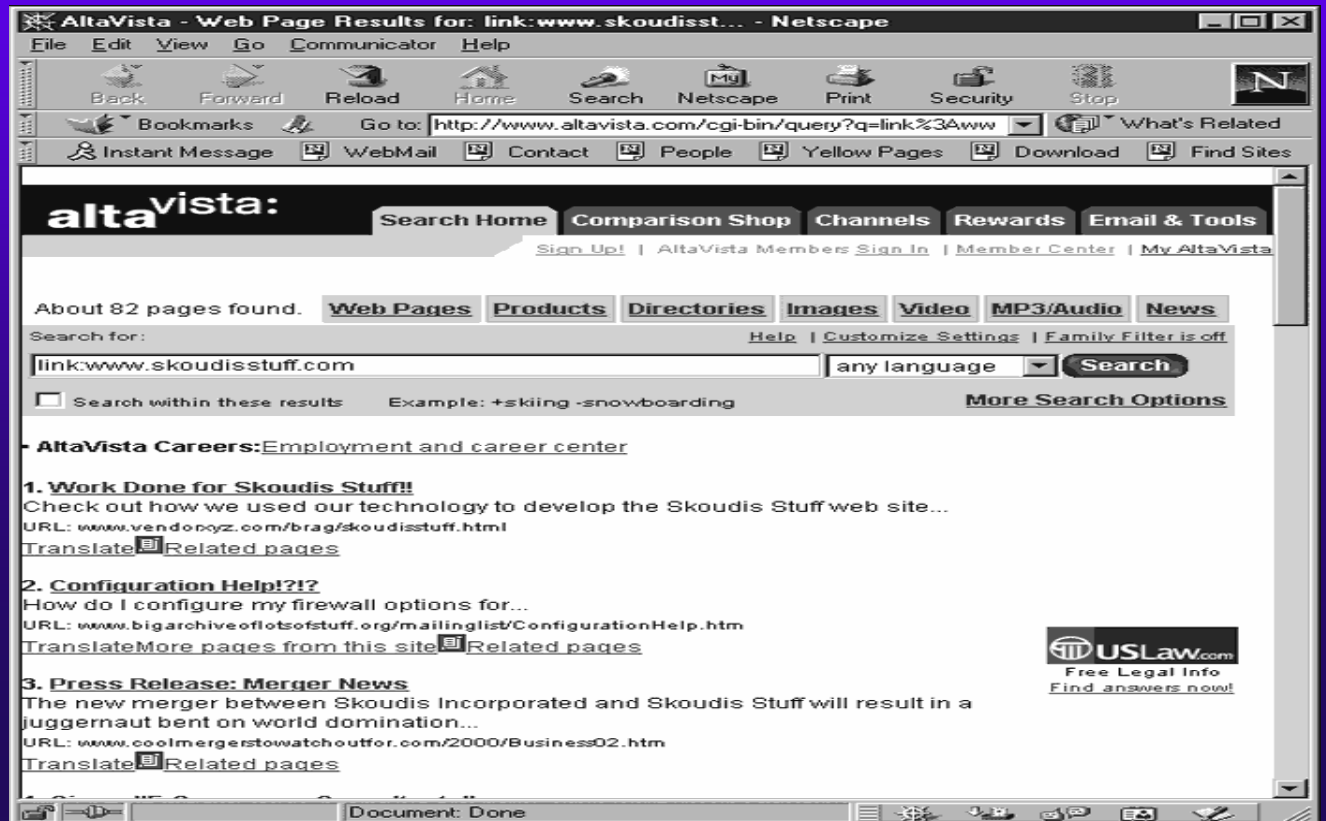
- Searching an organization's own web site
- Using search engines
- Listen in at the virtual watering hole: USENET

Searching an Organization's Own Web Site

- Employees' contact information and phone numbers
- Clues about the corporate culture and language
- Business partners
- Recent mergers and acquisitions
- Server and application platforms in use

Using Search Engines

- Conduct search based on organization name, product names, employee names
- Retrieve information about history, current events, and future plans of the target organization
- Search for links to target organization via "link:www.companyname.com" in a search engine



Listening in at the Virtual Watering Hole: Usenet

- Posting of questions by employees to technical Newsgoups
- Google newsgroup archive web search engine at http://groups.google.com

Defenses against Web searches

- Security by obscurity
- Security policy regarding posting of sensitive information on web site, newsgroups, and mailing lists

Whois Databases

- Contain information regarding assignment of Internet addresses, domain names, and individual contacts
- Internet Corporation for Assigned Names and Numbers (ICANN)
- Complete list of accredited registrars available at www.internic.net/alpha.html
- InterNIC's whois database available at www.internic.net/whois.html
- Whois database for organizations outside the United States available at ALLwhois web site
- Whois database for U.S. military organizations available at whois.nic.mil
- Whois database for U.S. government agencies available at whois.nic.gov
- Netwwork Solutions whois database

InterNIC - Registrar List - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Real.com

Links Customize Links Free Hotmail Windows RealPlayer

Address http://www.internic.net/alpha.html Go

InterNIC

Home Registrars FAQ Whois

The Accredited Registrar Directory:

Alphabetical Listing of Registrars by Company/Organization Name

The information that appears for each registrar, including the referral web address and contact information, has been provided by each individual registrar.

Companies accredited as registrars by ICANN and currently operational:

1st Domain.net	US	Contact Information
A+ Net	US	Contact Information
A Technology	Canada	Contact Information
Active ISP ASA	Norway	Contact Information
AWRegistry	US	Contact Information
Alldomains.com, Inc.	US	Contact Information
America Online	US	Contact Information
BB Online UK Ltd.	UK	Contact Information
Bulk Register.com	US	Contact Information

Internet

Figure 5.2 List of accredited registrars on the InterNIC site

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: http://www.internic.net/cgi-bin/whois?whois_nic=skoudisstuff.com&type=do What's Related

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels

InterNIC

Home Registrars FAQ Whois

Whois Search Results

Search again:

skoudisstuff.com

(•) Domain (ex. nsiregistry.net)
( ) Registrar (ex. ABC Registrar, Inc.)
( ) Nameserver (ex.NS.NETSOL.COM or 198.41.0.196)

Submit

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

Domain Name: SKOUDISSTUFF.COM
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: www.networksolutions.com
Name Server: NS.SKOUDISSTUFF.COM
Name Server: NS2.SKOUDISSTUFF.COM
Updated Date: 07-jun-2001

>>> Last update of whois database: Thu, 21 Dec 2000 10:59:44 EST <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and

Document: Done

Figure 5.3 Using the InterNIC whois database to find the target's registrar

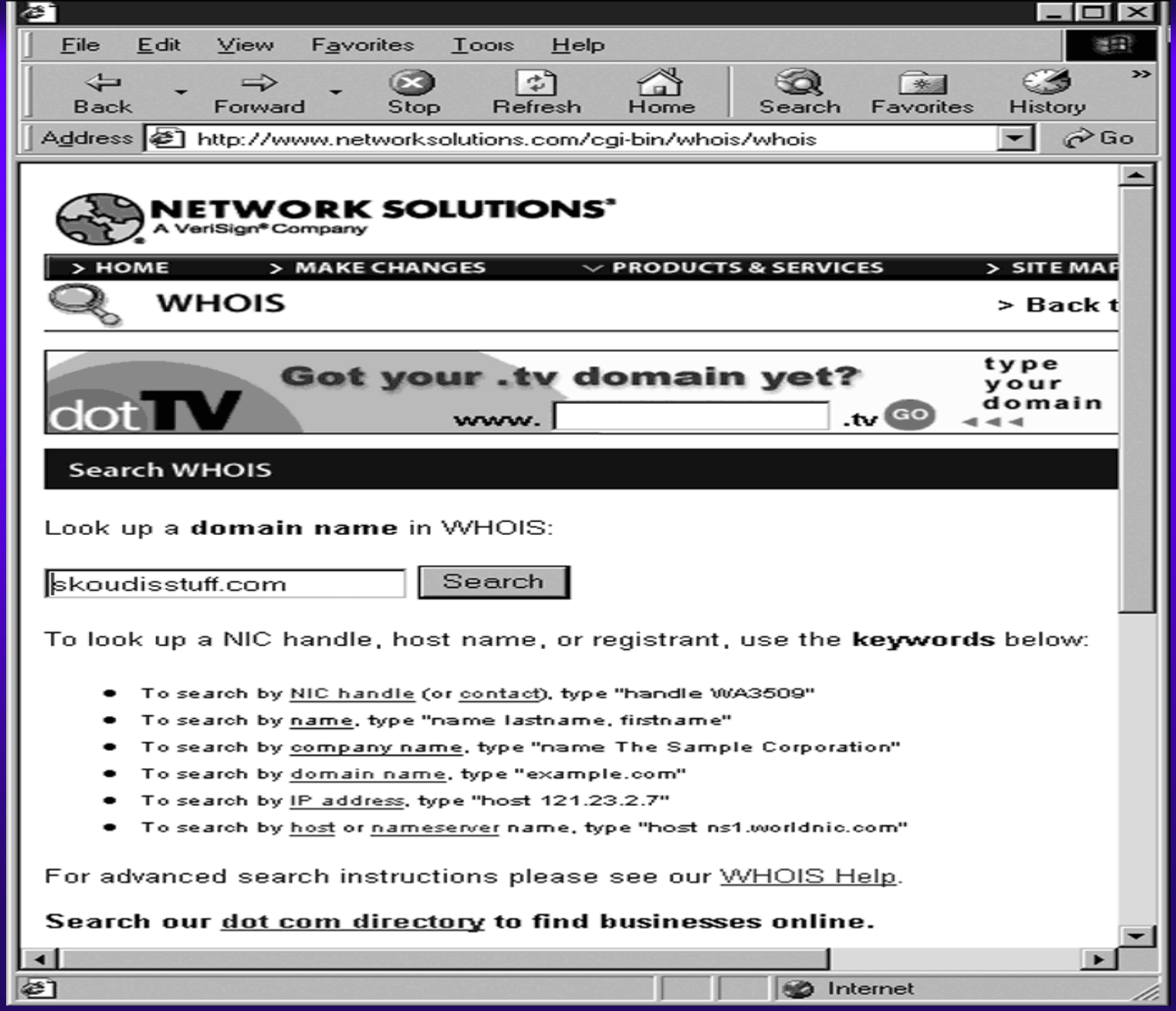


Figure 5.4 Looking up a domain name at a particular registrar

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: http://www.networksolutions.com/cgi-bin/whois/whois?STRING=skoudisstuff.com What's Related

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels RealPl

Search Result

Get it now! NETWORK SOLUTIONS

Registrant:
Skoudis Stuff, Inc. (SKOUDISSTUFF-DOM)
55 Skoudis Avenue
New York, NY 10010
US

Domain Name: SKOUDISSTUFF.COM

Administrative Contact:
Ed Skoudis (ES1234-ORG) ed@SKOUDISSTUFF.COM
55 Skoudis Avenue
New York, NY 10010
+1 212 555 1212 Fax- - +1 212 555 1212
Technical Contact:
Edward Skoudis (ES1234-ORG) edward@SKOUDISSTUFF.COM
55 Skoudis Avenue
New York, NY 10010
+1 212 555 1212 Fax- - +1 212 555 1212
Billing Contact:
Eddie Skoudis (ES1234-ORG) eddie@SKOUDISSTUFF.COM
55 Skoudis Avenue
New York, NY 10010
+1 212 555 1212 Fax- - +1 212 555 1212

Record last updated on 07-Jun-2001.
Record expires on 06-Dec-2001.
Record created on 15-Apr-1998.
Database last updated on 21-Dec-2000 04:35:05 EST.

Domain servers in listed order:

NS.SKOUDISSTUFF.COM 10.1.1.34
NS2.SKOUDISSTUFF.COM 10.2.42.1

Document: Done

Figure 5.5 Results of a registrar whois search

Useful Information in Registar

- Names (administrative, technical, billing contacts)
  - Used for social engineering attack
- Telephone numbers
  - Used in war-dialing attacks
- Email addresses
  - Format of email addresses eg. First.last@abc.com
- Postal address
  - Used in dumpster diving
- Name servers
  - DNS servers

IP Address Range Assignments

- North/South America
  - American Registry for Internet Numbers (ARIN)
- Europe
  - RIPE NCC
- Asia
  - Asia Pacific Network Information Center (APNIC)

ARIN: Whois - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Netsite: http://www.arin.net/whois/index.html What's Related

Instant Message WebMail Contact People Yellow Pages Download Find Sites Ch

ARIN

About Arin Registration Services Whois Minutes & Presentations
Routing Registry Membership Internet Coordination Library

Other Whois Searches

InterNIC

Department of Defense

RIPE

APNIC

The **IP Registration Services Help Desk** is open from 8 a.m. to 7 p.m., Eastern Time to assist you and may be reached by E-mail: hostmaster@arin.net

Whois Database Search

skoudisstuff Submit

ARIN's Whois program searches ARIN's database to locate information on networks, autonomous system numbers (ASNs), network-related handles, and other related Points of Contact (POCs). This search tool will not provide information relating to domains, military networks (NIPRNET) or networks registered through RIPE NCC or APNIC.

If the information you are seeking is located within ARIN's database, your search may be initiated by inserting relevant words or numbers in the "Search For" dialogue box. Unless your search string is specific, the results you obtain may be very broad. Your search has the potential to provide information on network names, network numbers, ASNs and host information as well as the names, addresses, telephone numbers, and email addresses for Points of Contact.

Document: Done

Figure 5.6 Searching for IP Address Assignments in ARIN

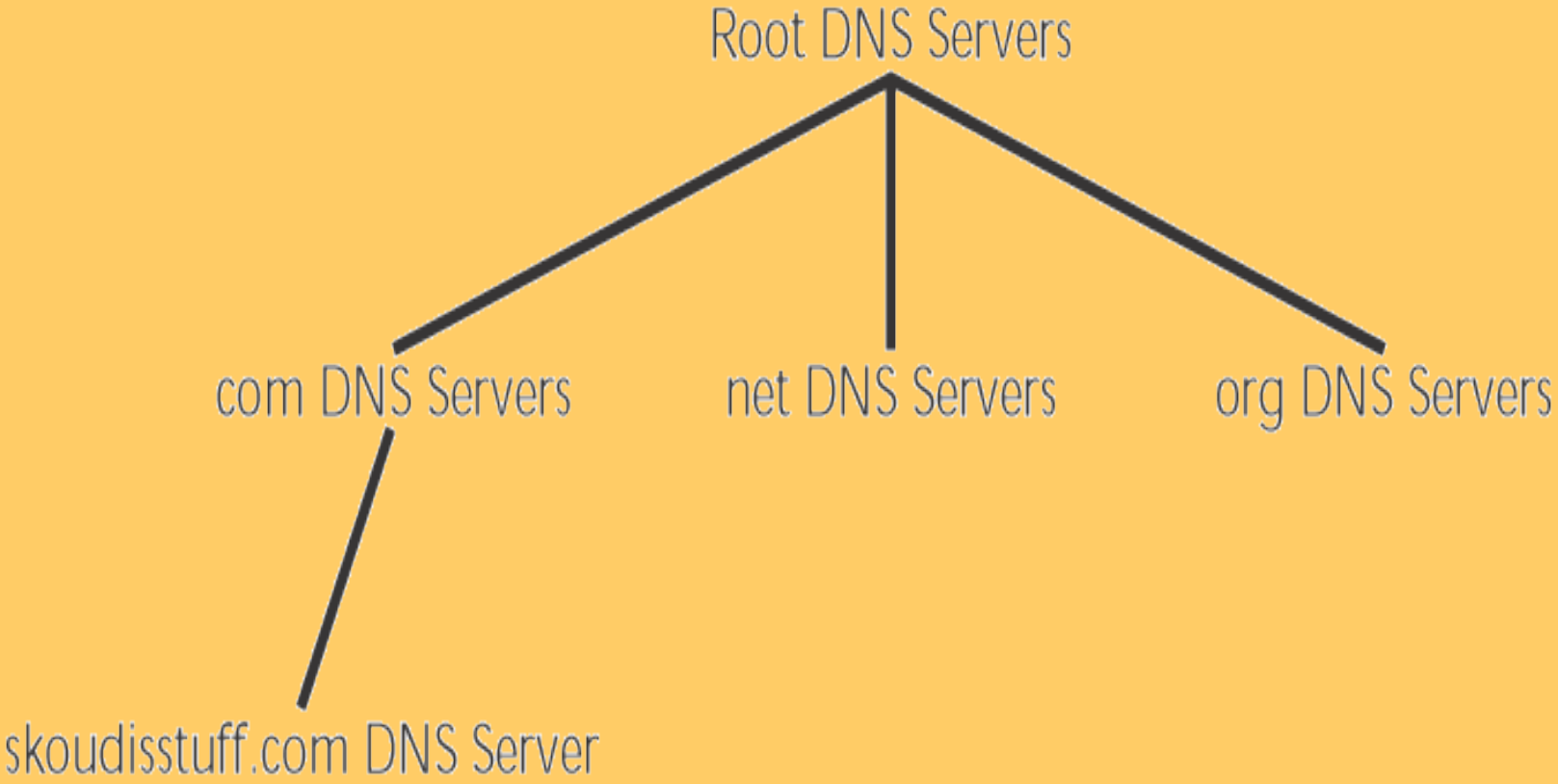


Fig 5.7 DNS Hierarchy

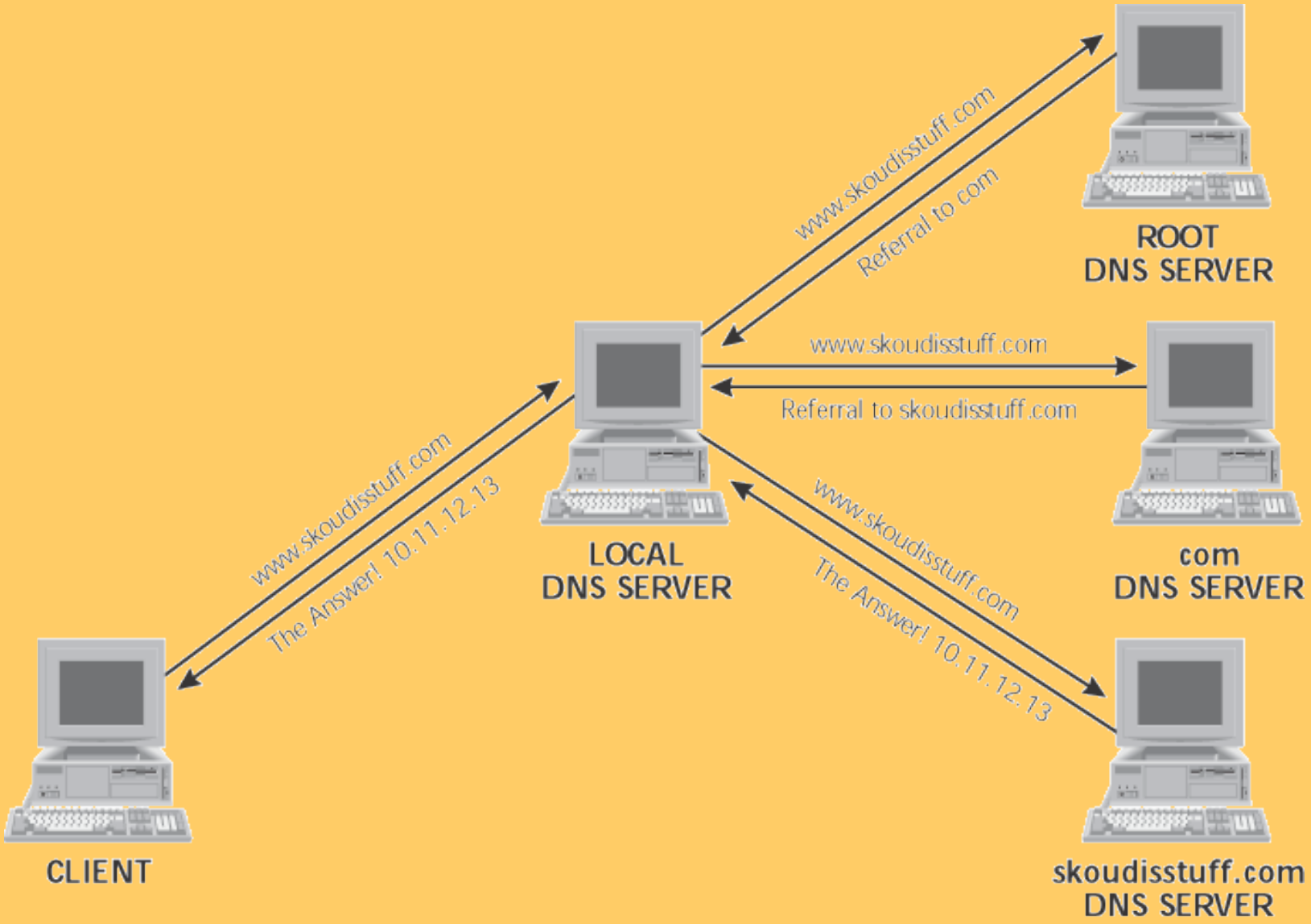


Fig 5.8 Recursive search to resolve a domain name to IP address

DNS Record Types

- Address (A) record
  - Maps a domain name to a specific IP address
  - Eg. www IN A 130.182.3.1
- Host Information (HINFO) record
  - Describes host type associated with host name
  - Eg. www IN HINFO Solaris8
- Mail Exchange (MX) record
  - Identifies a mail system accepting mail for the given domain
  - Eg. calstatela.edu MX 10 mars
- Name Server (NS) record
  - Identifies DNS servers of domain
  - Eg. calstatela.edu IN NS eagle
- Text (TXT) record
  - Used for comments
  - Eg. serverx IN TXT “ this system contains sensitive info”

Interrogating DNS Servers

- Host
- Dig tool for Unix
- Advanced Dig tool for MS Windows
- Nslookup
- Zone transfer
  - Eg. Nslookup

    server 130.182.1.1

    set type=any

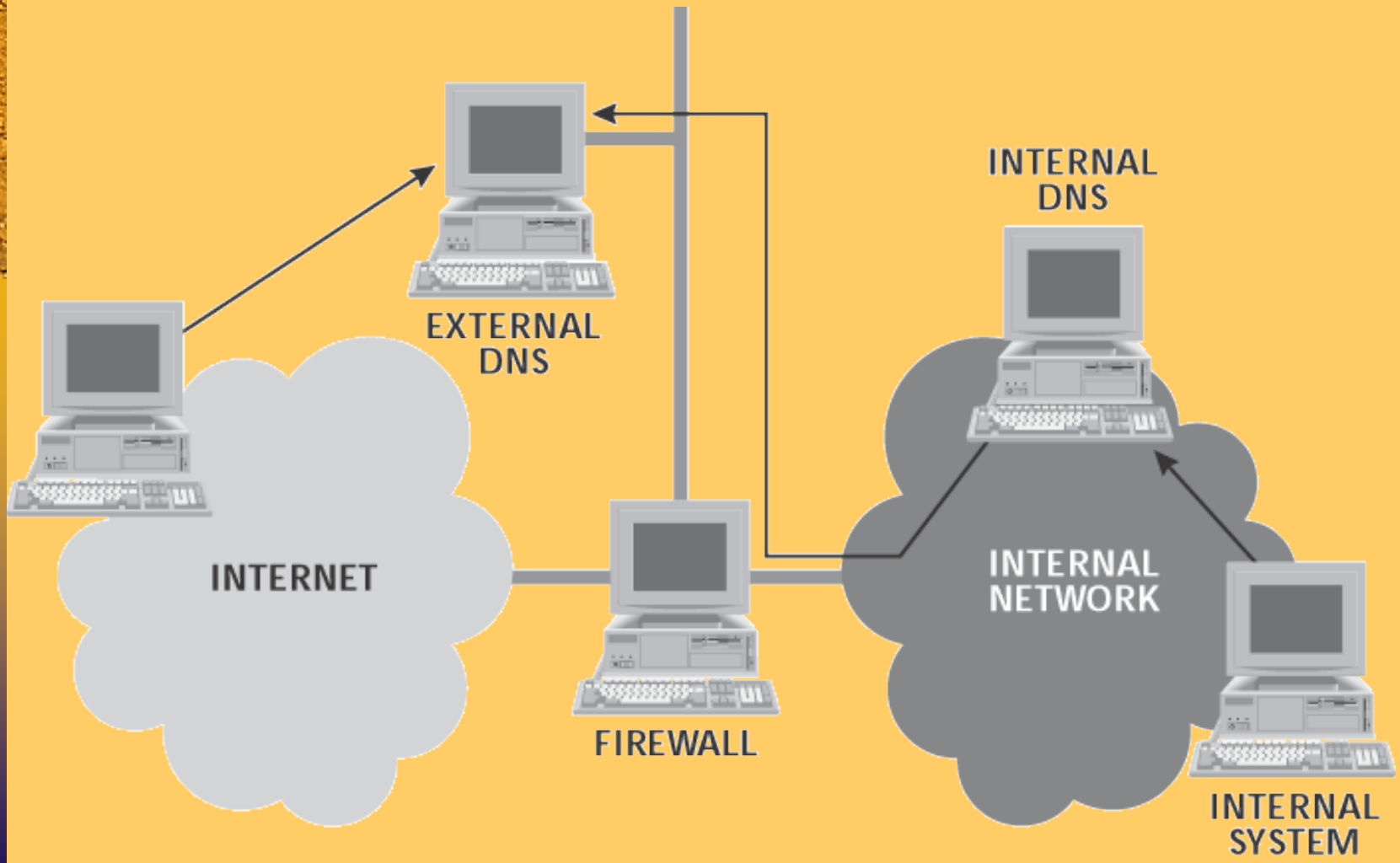
    ls –d calstatela.edu

Defenses from DNS-based Reconnaissance

- Do not include HINFO or TXT records
- Restrict zone transfers to secondary DNS only
  - "allow-transfer" directive or "xfernets" in BIND
- Configure firewall or external router to allow access to TCP port 53 only to secondary DNS servers
  - No restriction on UDP port 53
- Split-Horizon DNS

Split DNS

- Internal users can resolve both internal and external names
- External users can only access external names



General Purpose Reconnaissance GUI Client Tools for MS Windows

- Sam Spade
  - Ping
  - Whois
  - IP Block Whois
  - Nslookup
  - Dig
  - DNS Zone Transfer
  - Traceroute
  - Finger
  - SMTP VRFY
  - Web browser
- CyberKit
- NetScan Tools
- iNetTools

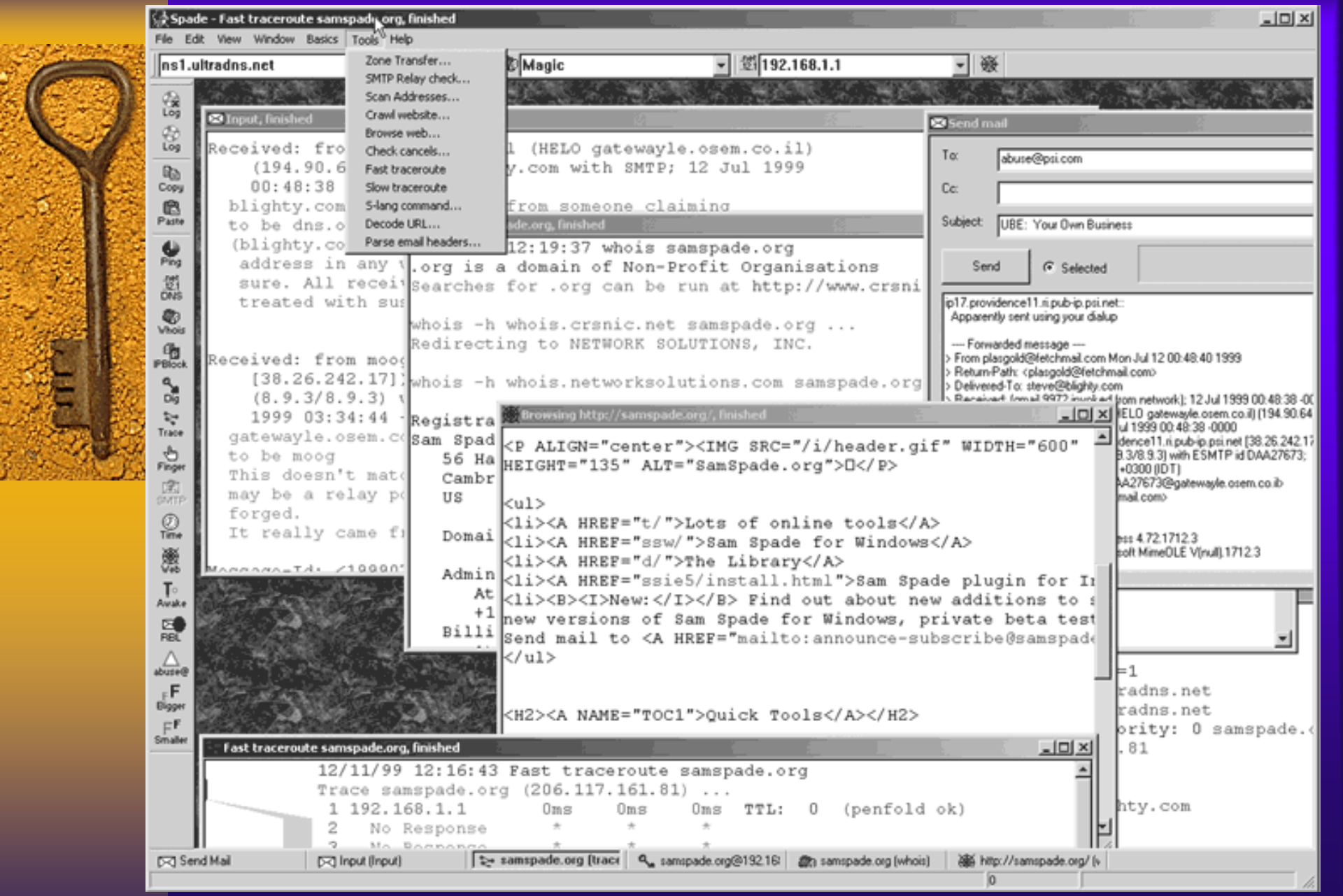


Figure 5.10 Sam Spade user interface

Web-based Reconnaissance Tools: Research and Attack Portals

- nettool.false.net
- www.samspade.org
- members.tripod.com/mixtersecurity/evil.html
- www.network-tools.com
- www.cotse.com/refs.htm
- suicide.netfarmers.net
- www.jtan.com/resources/winnuke.html
- www.securityspace.com
- crypto.yashy.com
- www.grc.com/x/ne.dll?bh0bkyd2
- privacy.net/analyze
- www.webtrends.net/tools/sercurity/scan.asp
- www.doshelp.com/dostest.htm
- www.dslreports.com/r3/dsl/secureme

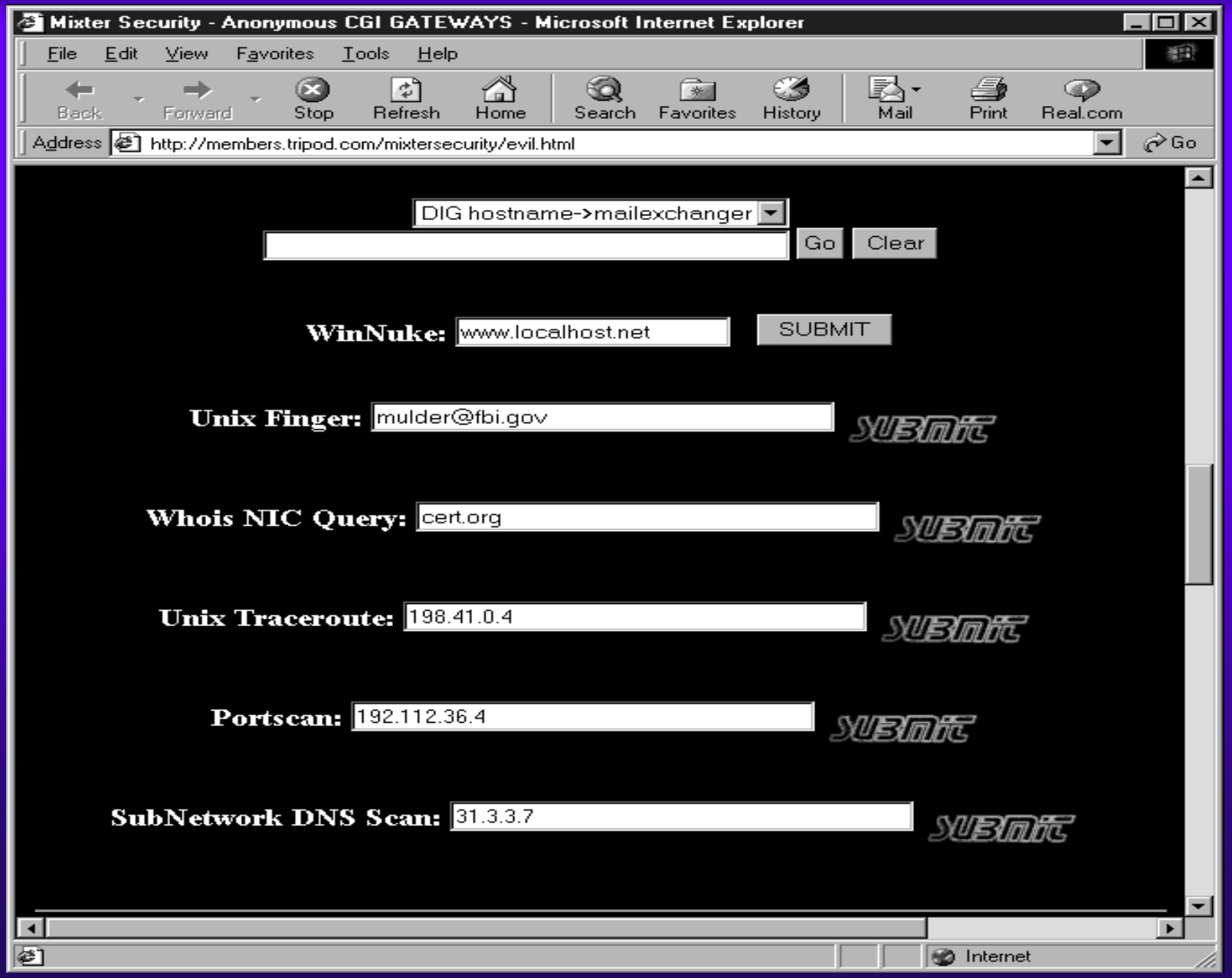


Figure 5.11 a Web-based reconnaissance and attack tool