

# Performing a Penetration Test



# Presentation Outline

- **Recap of Yesterday**
- **Penetration Test Phases**
  - **Discovery**
  - **Footprint Analysis**
  - **Penetration**
- **Q & A**

# Recap



# Yesterday

- **Set Objectives & Scope**
  - You'll spend your time and money on valuable results
- **Select an Appropriate Approach**
  - If you take a generic approach, you get generic results
- **Choose the Right Partner**
  - Just like ballroom dancing, if your partner has no experience, you will probably end up face down on the floor
- **Use the Results**
  - The knowledge is only as good as how you use it

# Types of Assessments

## External Penetration

- Attempt to gain access to systems, networks, and applications from an external network / Internet.

## Internal Security Assessment

- Attempt to gain access to systems, networks, and applications from the internal network.

## Application Testing

- Focused attempt to gain access to a single specific application and the infrastructure supporting it.

# Types of Assessments

## Wireless Penetration

- Attempt to gain access to servers, networks, and applications through wireless networks.

## Telephony / Remote Access Testing

- Attempt to gain access to servers, networks, and applications through both traditional PBX and VoIP systems.

## Social Engineering

- Attempt to gain information, knowledge, or access through non-technology sources. “Dumpster-diving”, impersonating an employee, piggy-backing, creative discussions.

# Assessment Approaches

- BLACKBOX
  - Also known as “Zero Knowledge”
  - Requires 100% discovery on the part of the tester
- WHITEBOX
  - Sometimes called “Crystal Box” Approach
  - Tester is provided with network diagrams, IP Addresses, Configurations, and Source Code
- GREYBOX
  - A hybrid approach

# Scan vs. Penetration

A **vulnerability assessment** is the process of identifying and quantifying *vulnerabilities* in a system.

A **penetration test** is a method of evaluating the security of a computer system or network by simulating an attack by a malicious cracker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities, and can involve active exploitation of security vulnerabilities.

Source: Wikipedia - [http://en.wikipedia.org/wiki/Penetration\\_test](http://en.wikipedia.org/wiki/Penetration_test)

# More Than Just NESSUS

## SCAN:

- Point a Vulnerability Scanner at a list of systems and retrieve a list of known vulnerabilities associated with the discovered technology
- Can result in false positives

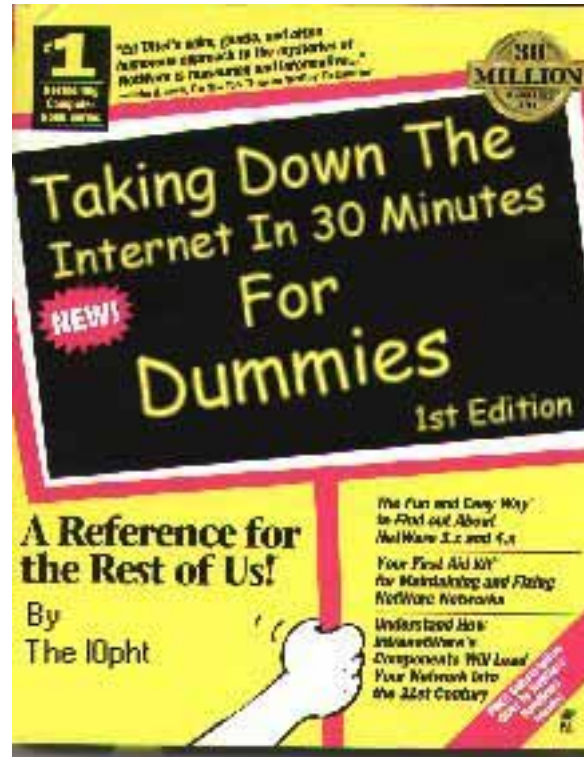
## PENETRATION TEST:

- Identifying targets from publicly available information
- Unauthorized Internet Connection Detection
- War Dialing
- War Driving or War Walking
- Manual Detailed Testing
- Attempt to exploit weaknesses in employee activity
- Exploit physical controls
- Minimal possibility of false positives

# The Meat



# It Is Really Easy, Right?



# Step 1: Discovery



# What We Are Looking For

- **Public Information About the Target**
- **Anything that tells us about their infrastructure**
  - Domains
  - Systems
  - Networks
  - Usernames

# Where Do We Look?

- **Internet Registrars**

[www.arin.net](http://www.arin.net)

[www.afriNIC.net](http://www.afriNIC.net)

[www.LACNIC.net](http://www.LACNIC.net)

[www.nic.mil/DoDNIC.net](http://www.nic.mil/DoDNIC.net)

[www.internic.net](http://www.internic.net)

[www.APNIC.org](http://www.APNIC.org)

[www.RIPE.net](http://www.RIPE.net)

- **Whois**

- Numerous Tools: whois, Sam Spade

- **Google / Yahoo / Altavista...**

- Look for system references

- Scavenge for login names

- Look for blogs & email lists with domain name

# Google

The screenshot shows a Microsoft Internet Explorer browser window with the title "daniel j blander - Google Search - Microsoft Internet Explorer". The address bar contains the URL "http://www.google.com/search?hl=en&lr=&safe=off&q=daniel+j+blander". The search results page displays the Google logo, a search bar with "daniel j blander" entered, and navigation links for "Web", "Images", "Groups", "News", "Froogle", "Maps", and "more ». The search results are for "daniel j blander" and show three entries:

- 1996: SUMMARY: DNS and IP registration tools.**  
SUMMARY: DNS and IP registration tools. From: **Daniel J Blander** - Sr. Systems Engineer for ACS ([Daniel.Blander@ACSacs.Com](mailto:Daniel.Blander@ACSacs.Com)) ...  
[www.sunmanagers.org/archives/1996/1330.html](http://www.sunmanagers.org/archives/1996/1330.html) - 8k - Cached - Similar pages
- X-Sun-Data-Type: text X-Sun-Data-Description: text X-Sun-Data-Name ...**  
If you have the new hardware you can ask for the CD. From: "**Daniel J Blander** - Sr. Systems Engineer for ACS" <[Daniel.Blander@ACSacs.com](mailto:Daniel.Blander@ACSacs.com)> It adds support for ...  
[www.sunmanagers.org/archives/1996/att-0193/00-part](http://www.sunmanagers.org/archives/1996/att-0193/00-part) - 7k - Cached - Similar pages  
[ More results from [www.sunmanagers.org](http://www.sunmanagers.org) ]
- NETSYS.COM - The Intelligent Hacker's Choice! Firewalls Archives**  
Jose Luis Delgado; RE: PIX and Firewall-1 (Thesis Length) **Daniel J Blander** - Sr. Systems Engineer for ACS; [SNI-14]: Solaris rpcbind vulnerability Oliver ...  
[www.netsys.com/firewalls/firewalls-9706/date.html](http://www.netsys.com/firewalls/firewalls-9706/date.html) - 33k - Cached - Similar pages

The second and third entries also include the text "NETSYS.COM - The Intelligent Hacker's Choice! Firewalls Archives" and "Sidewinder **Daniel J Blander** - Sr. Systems Engineer for ACS; RE: NT Security Keith McCammon; Re: Information Seeking Anthony R. Plastino III ...".

# Exercise 1:

## Objective:

Obtain Information Regarding ISACA

## Tasks:

- Search Arin
- Search Internic
- Search Whois
- Sub-searches – netblocks
- Perform DNS “dig”
- Search Google

# Exercise 1:

Open Web Server

Go to: [www.arin.net](http://www.arin.net)

Input into “Whois” Search box:  
“Information Systems Audit”

Select “Search”

# Arin.Net

ARIN: WHOIS Database Search - Microsoft Internet Explorer

File Edit View Favorites Tools Help Back Address http://ws.arin.net/whois/?queryinput=Information+Systems+Audit

## ARIN WHOIS Database Search

relevant Links: [ARIN Home Page](#) [ARIN Site Map](#) Training: [Querying ARIN's WHOIS](#)

Search ARIN WHOIS for: Information Systems Audit

Submit Query

Information Systems Audit and Control Association UU-208-215-18 (NET-208-215-18-0-1) 208.215.18.0 - 208.215.18.255  
Information Systems Audit and Control Assoc SBC07022819513629060302115324 (NET-70-228-195-136-1) 70.228.195.136 - 70.228.195.143

# ARIN WHOIS database, last updated 2006-07-19 19:10  
# Enter ? for additional hints on searching ARIN's WHOIS database.

Other WHOIS Servers: [AfrinIC](#) [APNIC](#) [LACNIC](#) [RIPE](#) [DoDNIC](#) [InterNIC](#)

[Request Bulk Copies of ARIN WHOIS Data](#)

Copyright © 2005 American Registry for Internet Numbers. All Rights Reserved.



# Arin.Net

Search ARIN WHOIS for: ! NET-208-215-18-0-1

Submit Query

CustName: Information Systems Audit and Control Association  
Address: 3701 Algonquin Rd., Suite 1010  
City: Rolling Meadows  
StateProv: IL  
PostalCode: 60008  
Country: US  
RegDate: 1997-02-05  
Updated: 2003-05-30

NetRange: 208.215.18.0 - 208.215.18.255  
CIDR: 208.215.18.0/24  
NetName: UU-208-215-18  
NetHandle: NET-208-215-18-0-1  
Parent: NET-208-192-0-0-1  
NetType: Reassigned  
Comment:  
RegDate: 1997-02-05  
Updated: 2003-05-30

RTechHandle: OA12-ARIN  
RTechName: UUnet Technologies, Inc., Technologies  
RTechPhone: +1-800-900-0241  
RTechEmail: help4u@mci.com

OrgAbuseHandle: ABUSE3-ARIN  
OrgAbuseName: abuse  
OrgAbusePhone: +1-800-900-0241  
OrgAbuseEmail: abuse-mail@mci.com

OrgNOCHandle: OA12-ARIN  
OrgNOCHandle: UUnet Technologies, Inc., Technologies  
OrgNOCHandlePhone: +1-800-900-0241  
OrgNOCHandleEmail: help4u@mci.com

OrgTechHandle: SWIPP-ARIN  
OrgTechName: swipper

Done Internet

# Discovery

## **www.Internic.net**

**Domain Name:ISACA.ORG**

**UTC Sponsoring Registrar:Network Solutions LLC (R63-LRMS)**

**Registrant ID:6073105-NSI**

**Registrant Name:Inf.Sys.Audit and Control Association**

**Registrant Organization:Inf.Sys.Audit and Control Association**

**Registrant Street1:3701 Algonquin Rd, Suite 1010**

**Registrant City:Rolling Meadows**

**Registrant State/Province:IL Registrant Postal Code:60008**

**Registrant Country:**

**US Registrant Phone:+1.8475907461**

**Registrant Phone Ext.:**

**Registrant FAX:**

**Registrant FAX Ext.:**

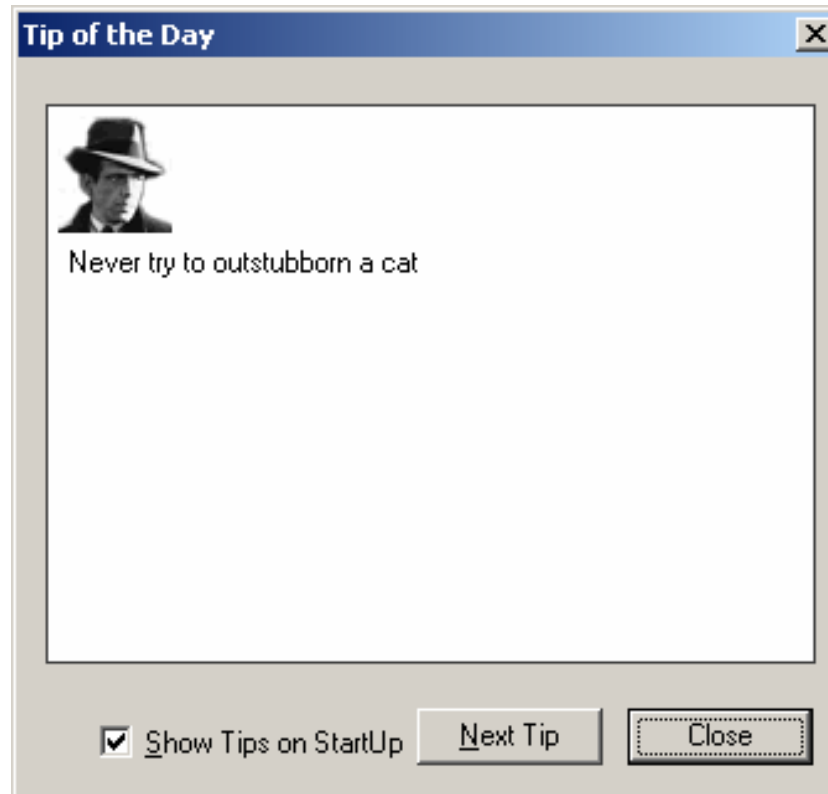
**Registrant Email:rriba@isaca.org**

**Name Server:NS49.WORLDDNIC.COM**

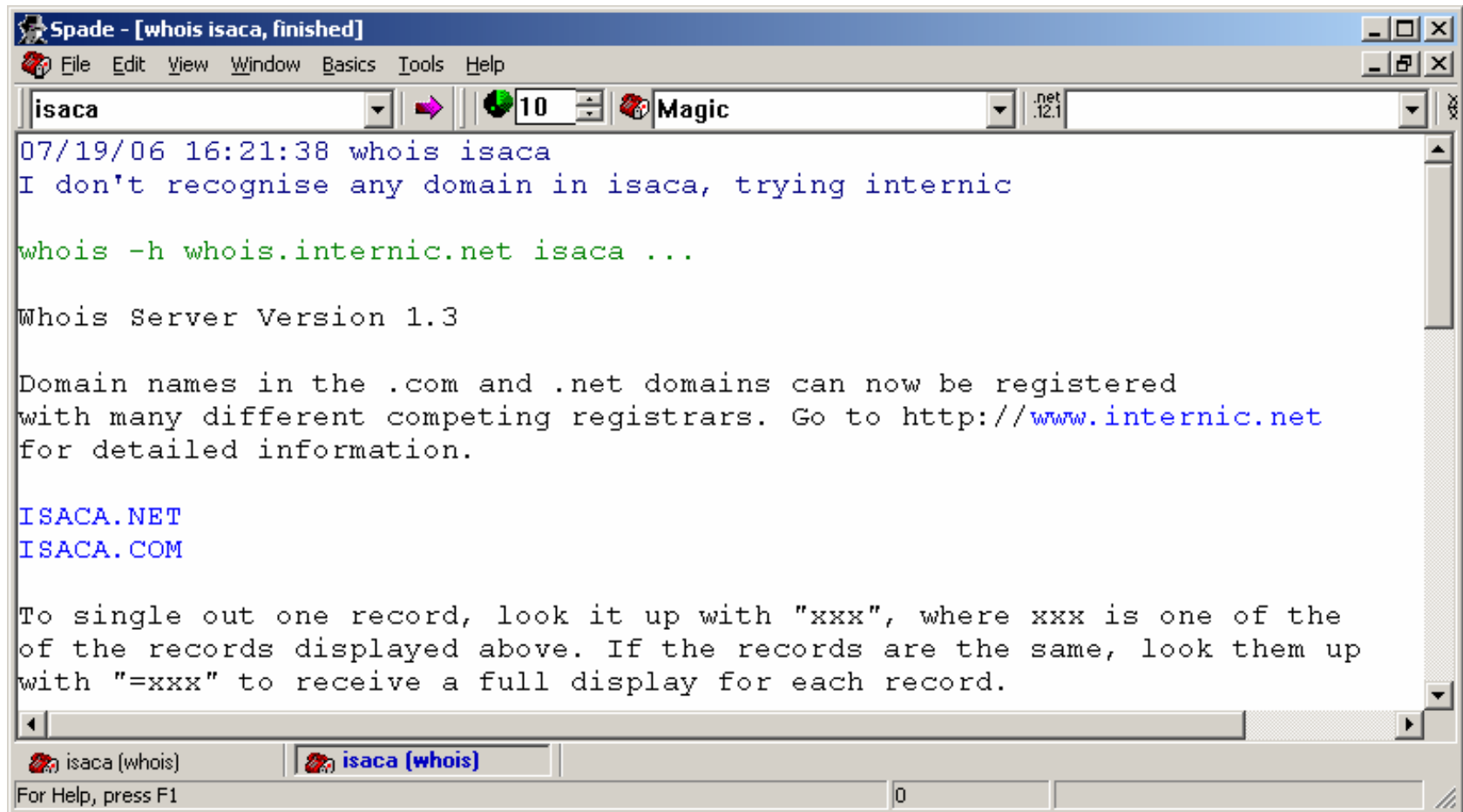
**Name Server:NS50.WORLDDNIC.COM**



# Sam Spade



# Sam Space



The screenshot shows a terminal window titled "Spade - [whois isaca, finished]". The window has a menu bar with "File", "Edit", "View", "Window", "Basics", "Tools", and "Help". Below the menu bar is a toolbar with icons for "isaca", a green circle with "10", and "Magic". The main text area contains the following output:

```
07/19/06 16:21:38 whois isaca
I don't recognise any domain in isaca, trying internic

whois -h whois.internic.net isaca ...

Whois Server Version 1.3

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

ISACA.NET
ISACA.COM

To single out one record, look it up with "xxx", where xxx is one of the
of the records displayed above. If the records are the same, look them up
with "=xxx" to receive a full display for each record.
```

At the bottom of the window, there are two tabs labeled "isaca (whois)" and a status bar that says "For Help, press F1".

# Sam Spade

```
Spade - [whois ISACA.NET, finished]
File Edit View Window Basics Tools Help
ISACA.NET 8 Magic .net
Registrant:
Isaca.Net
3-9-11, Akagawa, Asahi-ku,
Osaka, Osaka 5350005
JP
81669220393

Domain Name: ISACA.NET

Administrative Contact:
Kunishi, Teruo kuni@gol.com
3-9-11, Akagawa, Asahi-ku,
Osaka, Osaka 5350005
JP
669220393

Technical Contact:
Kunishi, Teruo kuni@gol.com
3-9-11, Akagawa, Asahi-ku,
Osaka, Osaka 5350005
JP
669220393

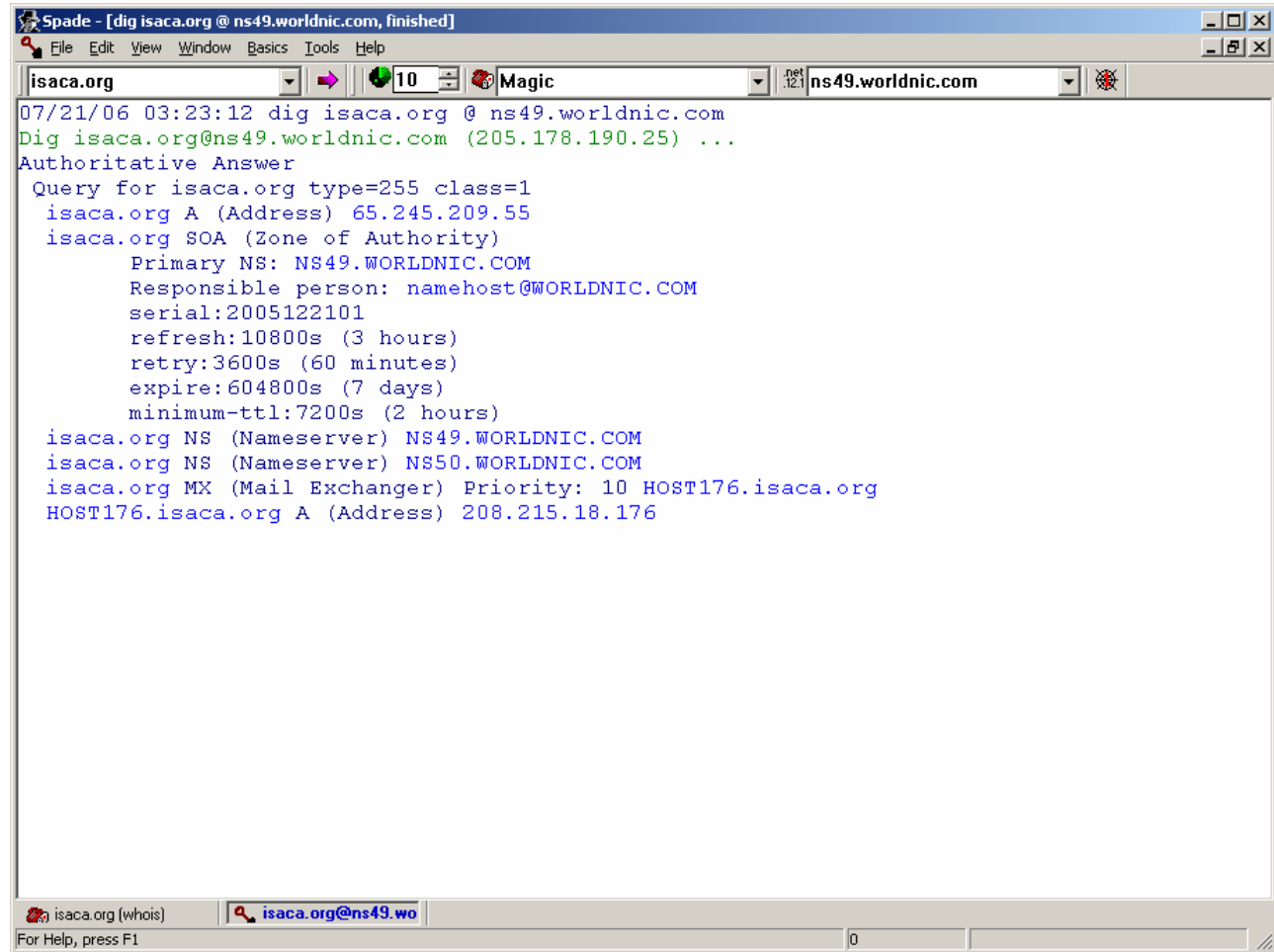
Record last updated 11-01-2004 10:42:43 PM
Record expires on 02-12-2007
Record created on 02-12-2002

Domain servers in listed order:
NS0.DIRECTNIC.COM 204.251.10.100
isaca (whois) isaca (whois) ISACA.NET (whois)
For Help, press F1
```



# Sam Spade

Dig

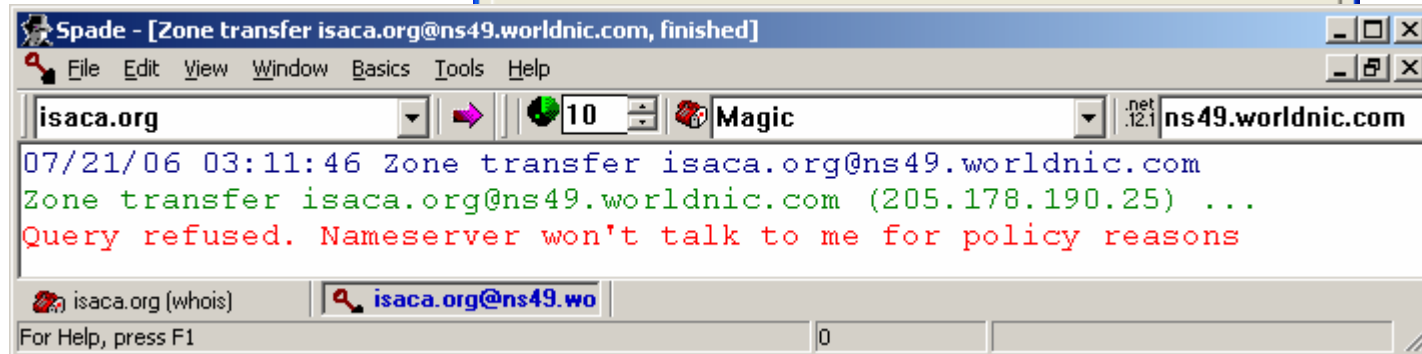
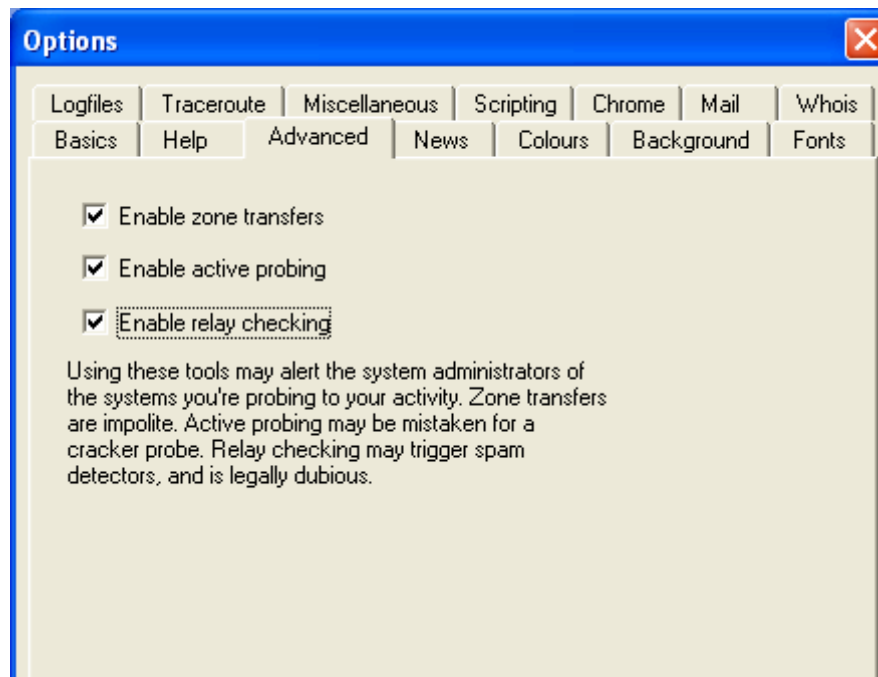


```
Spade - [dig isaca.org @ ns49.worldnic.com, finished]
File Edit View Window Basics Tools Help
isaca.org 10 Magic ns49.worldnic.com
07/21/06 03:23:12 dig isaca.org @ ns49.worldnic.com
Dig isaca.org@ns49.worldnic.com (205.178.190.25) ...
Authoritative Answer
Query for isaca.org type=255 class=1
isaca.org A (Address) 65.245.209.55
isaca.org SOA (Zone of Authority)
  Primary NS: NS49.WORLDNIC.COM
  Responsible person: namehost@WORLDNIC.COM
  serial:2005122101
  refresh:10800s (3 hours)
  retry:3600s (60 minutes)
  expire:604800s (7 days)
  minimum-ttl:7200s (2 hours)
isaca.org NS (Nameserver) NS49.WORLDNIC.COM
isaca.org NS (Nameserver) NS50.WORLDNIC.COM
isaca.org MX (Mail Exchanger) Priority: 10 HOST176.isaca.org
HOST176.isaca.org A (Address) 208.215.18.176
isaca.org (whois) isaca.org@ns49.wo
For Help, press F1
```



# Sam Spade

## Zone Transfer



# Step 2: Footprinting



# What We Are Looking For

- **Systems and Devices to Target**
- **What Type of System or Device**
- **Where They Exist in the Network**
- **What Vulnerabilities They Have**

# How?

- Ping
- Traceroute
- Nmap
- Nessus

# Ping

```
C:\ Command Prompt
C:\Documents and Settings\phaedrus>ping 200.215.18.0

Pinging 200.215.18.0 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.215.18.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\phaedrus>ping 208.215.18.176

Pinging 208.215.18.176 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 208.215.18.176:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\phaedrus>
```

# Traceroute

```
C:\ Command Prompt
'traceroute' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\phaedrus>tracert 208.215.18.176

Tracing route to host176.isaca.org [208.215.18.176]
over a maximum of 30 hops:

  0  404 ms    351 ms    337 ms    9.sub-66-174-217.myvzw.com [66.174.217.9]
  1  *         *         *         Request timed out.
  2  357 ms    517 ms    458 ms    113.sub-66-174-217.myvzw.com [66.174.217.113]
  3  415 ms    398 ms    357 ms    129.sub-66-174-31.myvzw.com [66.174.31.129]
  4  353 ms    356 ms    358 ms    98.sub-66-174-31.myvzw.com [66.174.31.98]
  5  395 ms    577 ms    378 ms    153.sub-66-174-28.myvzw.com [66.174.28.153]
  6  434 ms    578 ms    401 ms    129.sub-66-174-99.myvzw.com [66.174.99.129]
  7  520 ms    436 ms    397 ms    73.sub-66-174-98.myvzw.com [66.174.98.73]
  8  532 ms    598 ms    576 ms    ge-2-1-0.GW3.DFW13.ALTER.NET [63.97.48.49]
  9  413 ms    656 ms    398 ms    0.so-2-0-0.XL1.DFW13.ALTER.NET [152.63.100.74]
 10  490 ms    496 ms    438 ms    0.so-6-0-0.XL1.CHI6.ALTER.NET [152.63.64.202]
 11  413 ms    418 ms    418 ms    POS6-0.GW7.CHI6.ALTER.NET [152.63.64.37]
 12  473 ms    437 ms    437 ms    host1.isaca.org [208.215.18.1]
 13  *         *         *         Request timed out.
 14  *         *         *         Request timed out.
 15  *         *         *         Request timed out.
 16  *         *         *         ^C

C:\Documents and Settings\phaedrus>
```

# Nmap

- **-P0** = Scan hosts even if they don't ping
  - **-s** = set type of ping (TCP, SYN, ACK...)
  - **-p** <port ranges, UDP, TCP>
  - **-O** = operating system detection
- 
- All kinds of techniques to identify hosts
  - IDS Evasion options

# Nmap

```
C:\Documents and Settings\phaedrus>nmap -v -O -P0 66.174.217.9
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-07-21 04:37 Hawaiian
Standard Time
DNS resolution of 1 IPs took 16.54s. Mode: Async [#: 5, OK: 0, NX: 0, DR: 1, SF:
0, TR: 6, CN: 0]
Initiating SYN Stealth Scan against 66.174.217.9 [1672 ports] at 04:37
SYN Stealth Scan Timing: About 6.34% done; ETC: 04:45 (0:07:34 remaining)
The SYN Stealth Scan took 347.59s to scan 1672 total ports.
Warning: OS detection will be MUCH less reliable because we did not find at lea
st 1 open and 1 closed TCP port
Host 66.174.217.9 appears to be up ... good.
All 1672 scanned ports on 66.174.217.9 are: filtered
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SIInfo(U=4.01%P=i686-pc-windows-windows%D=7/21%Tm=44C0E82B%0=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Nmap finished: 1 IP address (1 host up) scanned in 398.503 seconds
Raw packets sent: 3368 (150KB) | Rcvd: 0 (0B)

C:\Documents and Settings\phaedrus>
```

# Nessus

The screenshot shows a web browser window titled "Tenable Nessus Security Report - Microsoft Internet Explorer". The address bar shows the local file path: "C:\Documents and Settings\phaedrus\Tenable\Nessus\reports\html\current...".

The report content is as follows:

- Tenable Nessus Security Report**
- Start Time:** Fri Jul 21 04:38:45 2006
- Finish Time:** Fri Jul 21 04:42:46 2006
- 127.0.0.1** 6 Open Ports, 18 Notes, 0 Warnings, 0 Holes.
- 127.0.0.1** [Return to top]
- apex-mesh (912/tcp)**
  - Port is open  
Plugin ID : 11219
  - A VMWare authentication daemon is running on this port:  
220 VMWare Authentication Daemon Version 1.10: SSL Required, MKSDisplayProtocol:VNC  
Plugin ID : 10330
- ideafarm-chat (902/tcp)**
  - Port is open  
Plugin ID : 11219
  - A VMWare authentication daemon is running on this port:  
220 VMWare Authentication Daemon Version 1.10: SSL Required, MKSDisplayProtocol:VNC  
Plugin ID : 10330
  - Synopsis :**  
The remote host appears to be running VMware ESX or GSX Server.
  - Description :**  
According to its banner, the remote host appears to be running a VMware server authentication daemon, which likely indicates the remote host is running VMware ESX or GSX Server.
  - See Also :**  
<http://www.vmware.com/>
  - Risk Factor :**