Class Outline

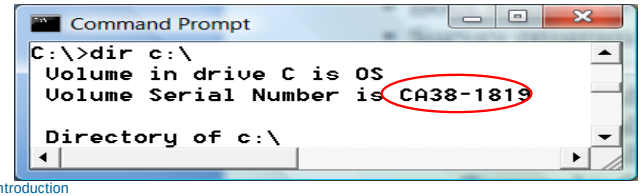
A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   Human access
   Physical access
   LAN (insider) access
   Remote (Internet) access
   Wireless access
E. Anatomy of an Attack
   Step 1: Target survey
   Step 2: Vulnerability assessment
   Step 3: Vulnerability exploitation
   Step 4: Maintaining access/persistence
   Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

Research Tools

- Tools used for researching attack targets include ping sweeps, port scanners, OS fingerprinting, and traceroutes – *and many more*
- Collections are available: Tools For Newbs
  - Professional Edition ?

Scripted Survey

- Initial visit: Local Target - Automated Survey
- Boot from USB or CD to survey program
- Copy files to exfil medium
- HD volume s/n (dir) & directory tree (dir/s c:\ )
- List of installed and/or running applications
- Word, email, spreadsheet files data files
- Personal information on the users
- Copy Linux shadow or Windows SAM & SYSTEM



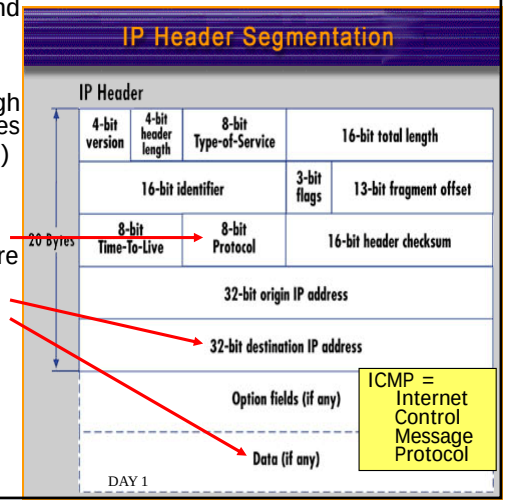
Remote Target Survey

- Ping sweeps (what computers are running?)
- Port scans (Any programs listening for connections?)
- Traceroutes (what's between this network and me?)
- OS fingerprinting (what OS is running?)
- Vulnerability scan

- Once an attacker has the above information, a remotely run Local Target Survey may be possible

Ping Sweeps

- Uses **ping** command to send an "echo request"
- Destination IP incremented through a range of addresses
- Protocol = 1 (ICMP)
- Increments destination IP address
- ICMP type goes here
  8 = echo (request)
  0 = echo reply
  11 = TTL ➔ 0
  3 = dest. unreach.



Anyone There?

You can see if a single box is up by simply pinging it:

DNS (Domain Name Service) at work!

Command Prompt

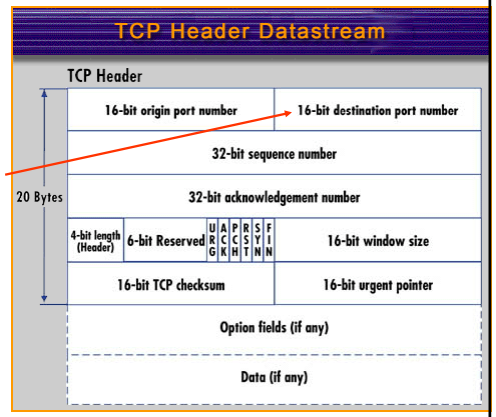
```
C:\>ping www.google.com

Pinging www.google.akadns.net [64.233.161.99] with 32 bytes of data:

Reply from 64.233.161.99: bytes=32 time=8ms TTL=248
Reply from 64.233.161.99: bytes=32 time=7ms TTL=248
Reply from 64.233.161.99: bytes=32 time=7ms TTL=248
Reply from 64.233.161.99: bytes=32 time=7ms TTL=248

Ping statistics for 64.233.161.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms
```


Port Scans

- Why do port scans?
  - Attackers wish to discover services they can break into.
- Security audit: Why are certain ports open?
- What is involved?
  - Sending a packet to each port, one at a time.
  - Based on the type of response, an attacker knows if the port is used.
  - The used ports can be probed further for weakness.

Port Scans

- Port scanners send a series of packets while incrementing the destination port number (e.g. from 1 to 1023)
- Scans can include both TCP & UDP ports by setting the Protocol byte in the IP header



GOAL: What services are running?

State of a Port

Open

- A service process is listening at the port. The OS receives packets arriving at this port and gives the messages to the service process. If the OS receives a SYN at an open port, this is the first packet of the three way handshake.

Closed

- No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.

Filtered

- A packet filter is listening at the port. How do we know? The packet is dropped!

Nmap Scanner

The most popular tool used to scan a network for active IP address and open ports is Nmap. It is available, for free, for DOS & Linux.

1. Ping sweep

```
> nmap 192.168.0.2-10
```

2. Ping sweep + port scan

```
> nmap -p 1-3389 192.168.0.2-10
```

3. Ping sweep + port scan + OS fingerprinting

```
> nmap -O -p 1-3389 192.168.0.2-10
```

This ping sweeps IP addresses 192.168.0.1 to 192.168.0.10

And port scans 1 to 3389 (-p 1-3389) at each live address

And fingerprints the operating systems (-O)

More on Nmap later…

A Legal Note

Port Scans Legal, Judge Says **12/18/00 SecurityFocus.com**

- A federal court [United States District Court, Southern District of Florida] found that scanning a network doesn't cause damage, or threaten public health and safety.
- Judge Thomas Thrash found that the value of time spent investigating a port scan can not be considered damage. "The statute clearly states that the damage must be an impairment to the integrity and availability of the network," wrote the judge, who found that a port scan impaired neither.
- "It says you can't create your own damages by investigating something that would not otherwise be a crime," says hacker defense attorney Jennifer Granick. "It's a good decision for computer security researchers."

Types of Port Scans

TCP connect(0) scanning

- Try connect()-ing to every port
- If port is listening, connect() will succeed
- Otherwise, the port isn't reachable
- No need for any special privileges
- Speed - slow
- Scanner can be identified

Types of Port Scans

TCP SYN scanning

- Often referred to as half-open scanning.
- Send a SYN packet
- Wait for a response.
  - A SYN/ACK indicates the port is listening.
  - If a SYN/ACK is received, send an RST to tear down the connection immediately.
- Most sites do not log these.
- Need root privileges to build SYN packets.

Types of Port Scans

TCP FIN Scanning (Stealth)

Send a FIN packet (without a preceding SYN etc.)

- FIN packets may pass through firewalls
- Closed ports reply with RST.
- Open ports ignore the FIN packet.
- Some hosts violate RFC 793.
  - Reply with RST's regardless of the port state
  - Thus, are not vulnerable to this scan.

Types of Port Scans

TCP reverse identd scanning

- identd protocol (rfc1413): Disclose the username of the owner of any process connected via TCP, even if that process didn't initiate the connection.
- Example: connect to the http port (80), and then use identd to find out whether the server is running as root.
- Must have full TCP connection to the port.

Types of Port Scans

Fragmentation scanning

- Not a new scanning method in and of itself. A modification of other techniques.
- Split the probe packet into IP fragments.
- By splitting up the TCP header over several packets, it is harder for packet filters to detect a probe.

Types of Port Scans

FTP Bounce Scan

- A port scanner can exploit this to scan TCP ports from a proxy ftp server
- Connect to an FTP server behind a firewall, then scan ports more likely to be blocked
- If FTP server allows reading from and writing to a directory (such as /incoming), you can send arbitrary data to ports that you find open
- Hard to trace – but slow
- Many printers have FTP running!

Types of Port Scans

UDP Scans

- UDP is simpler, but the scanning is more difficult
- Open ports do not have to send an ACK.
- Closed ports are not *required* to send an error packet.
  - Most hosts send an ICMP PORT UNREACH error when you send a packet to a closed UDP port.
  - Can find out if a port is NOT open.
  - Neither UDP packets, nor the ICMP errors are guaranteed to arrive.

Types of Port Scans

Stealth Scan

- Scan slowly
  - Port scanner typically scans host too rapidly
  - Some detectors recognize these “signatures”
  - Scanning very slowly (e.g., over several days) is a stealth technique (China 1/day)
- Firing packets with fake IPs
  - Flood with spoofed scans and embed one scan from the real source (network) address

Remote Target Survey

OS Fingerprinting - Why OS Fingerprint?

- Every OS has unique vulnerabilities (like locks)
- Lame targeting /etc/passwd on a Windows XP
- NT/2K/XP/W2003 passwords stored in a SAM (Security Account Manager) file
- Lame using an IIS-specific exploit on a Linux box
  - IIS (Internet Information Service), a Web server, is a Windows-only program
- A traceroute can help geolocate the target

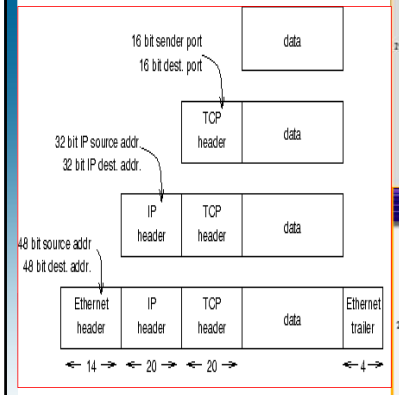
Introduction 21

OS Fingerprinting

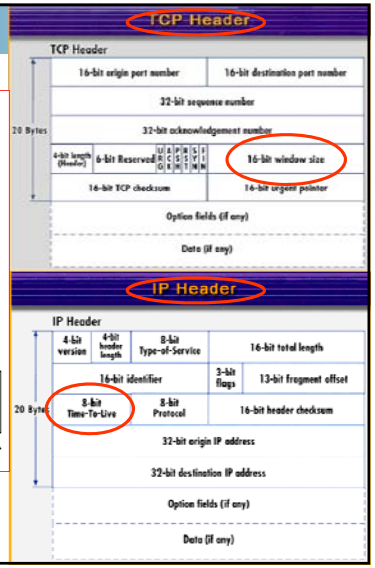
- Request for Comments - RFC's - standards
- Don't cover everything, TCP/IP stack coders must decide:
- What the TCP window size should be
  - RFC dictates nothing
- What TCP options, if any, should be used
  - RFC dictates nothing
- What IP 16-bit identifier value in the IP header should be
  - RFC dictates only that it uniquely identify a series of fragments; most increment it by 1 with each packet
- What the IP TTL (Time To Live) value must be
  - RFC dictates only that it be large enough to get to the destination

Introduction 22

OS Fingerprinting



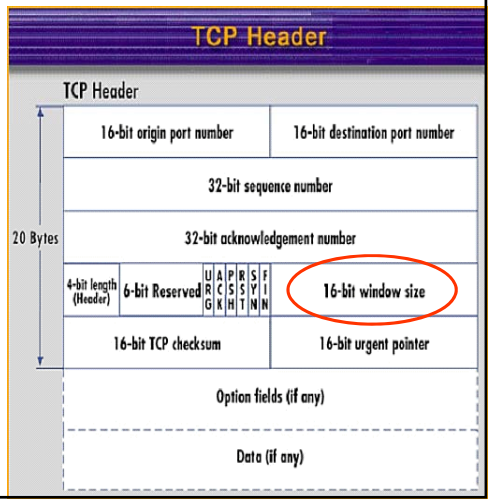
See next two slides...



Introduction

OS Fingerprinting

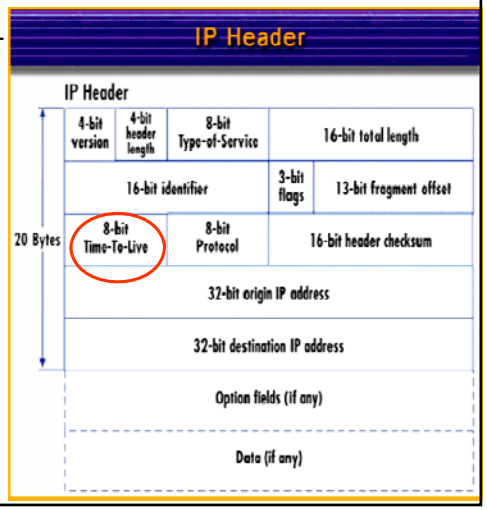
Example:
16-bit Window Size
Win 98: 8192
Win 2000: 16384
Win XP: 64240
Vista/Win 7 autotune
Linux 2.2: 32120
Linux 2.4: 5840



Introduction

OS Fingerprinting

Example: 8-bit TTL
Win 9x/NT: 32
Win 2K/XP: 128
Digital Unix: 60
Linux 2.2.x: 64
Solaris 2.x: 255
Avg. decrement
via Internet 30
maximum 60



OS Fingerprinting

- TCP/IP stack fingerprinting
- TCP option support enumeration
- ICMP response
- Number of SYN+ACK packets sent before timeout
- Time interval of SYN+ACK packets
- Presence of RST at timeout

OS Fingerprinting

Application-level OS Fingerprinting

- Attempts to identify the OS based on information gained from an application
- Passes through gateways, firewalls, NAT
- Current methods:
  - Identification of OS-specific applications
    - Remote desktop (= Windows)
  - Banner-grabbing
    - Fairly trivial to spoof
    - "Why yes, I'm running Apache on an Nintendo Ds!"
    - MS-DNS spoof that burned konsultant

OS Fingerprinting via IIS

- Different versions of IIS run on different Windows versions
- Enumerate IIS version to find Windows version!

IIS Version	OS Version
1.0	NT 3.51 SP3
2.0	NT 4.0
3.0	NT 4.0 SP3
4.0	NT 4.0 SP3
5.0	Win2k
5.1	XP Pro
6.0	Server 2003
7.0	Vista, Server 2008
7.5	Server 2008R2, 7

OS Fingerprinting

Internal fingerprinting
used as a security & support tool

- Find printers/appliances running what OS
- Find devices (video encoders etc.) running ?
- Find rogue wireless access points
- Identify EOL systems
- Policy compliance tool

Traceroute, Pathping

Traceroute

- Uses the TTL (Time To Live) field in the IP header
- Sets TTL to 1,2,3... and sends the packet
- When a router decrements the TTL to zero, it returns a "TTL exceeded message to the originator (source IP address) and (usually) identifies itself
- Builds list of responses & delays (latency)

Note: On Windows boxes, it's called "tracert"

Goals

- Where's my target (geolocation)?
- What is the address of the target's edge router?
- Where is host that is scanning me?

Traceroute

```
Command Prompt

C:\Documents and Settings\Name>tracert www.google.com

Tracing route to www.l.google.com [64.233.161.99]
over a maximum of 30 hops:

  1     4 ms     9 ms     5 ms  192.168.1.1
  2    34 ms    26 ms    27 ms  ip68-227-192-1.dc.dc.cox.net [68.227.192.1]
  3    19 ms    12 ms    16 ms  68.100.1.113
  4    22 ms    18 ms    22 ms  ip68-100-0-65.dc.dc.cox.net [68.100.0.65]
  5    32 ms    26 ms    27 ms  mrfddsrj02gex070003.rd.dc.cox.net [68.100.0

  6    13 ms    19 ms    17 ms  mrfdbbrc02-pos0101.rd.dc.cox.net [68.1.1.6]
  7    38 ms    42 ms    35 ms  ashbbbrj01-pos020100.r2.as.cox.net [68.1.1.

  8    41 ms    88 ms    16 ms  68.105.30.118
  9    34 ms    27 ms    20 ms  216.239.47.153
 10    37 ms    29 ms    27 ms  216.239.48.198
 11    36 ms    42 ms    40 ms  64.233.161.99

Trace complete.
```

← **First, DNS request**


```
Command Prompt

C:\>pathping www.pacific.edu

Tracing route to www.pacific.edu [138.9.110.12]
over a maximum of 30 hops:
  0  MarchHare.treacle.com [10.0.0.5]
  1  hatter.treacle.com [10.0.0.2]
  2  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
  3  dist2-vlan50.skt2ca.sbcglobal.net [68.120.211.67]
  4  ppp-151-164-39-79.rcsntx.swbell.net [151.164.39.79]
  5  ppp-151-164-52-213.rcsntx.swbell.net [151.164.52.213]
  6  gar7.sffca.ip.att.net [12.122.79.97]
  7  cr83.sffca.ip.att.net [12.122.110.118]
  8  cr1.sffca.ip.att.net [12.123.15.109]
  9  cr1.la2ca.ip.att.net [12.122.3.122]
 10  gar7.la2ca.ip.att.net [12.122.104.13]
 11  12.91.226.10
 12  oak1-ar1-xe-1-0-0-0.us.twtelecom.net [206.222.120.198]
 13  *        *        *
Computing statistics for 300 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           MarchHare.treacle.com [10.0.0.5]
                                     0/ 100 =  0%  |
  1   0ms     0/ 100 =  0%     0/ 100 =  0%  hatter.treacle.com [10.0.0.2]
                                     0/ 100 =  0%  |
  2  45ms     0/ 100 =  0%     0/ 100 =  0%  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
                                     0/ 100 =  0%  |
  3  ---     100/ 100 =100%   100/ 100 =100%  dist2-vlan50.skt2ca.sbcglobal.net [68.120.211.67]
                                     0/ 100 =  0%  |
  4  ---     100/ 100 =100%   100/ 100 =100%  ppp-151-164-39-79.rcsntx.swbell.net [151.164.39.79]
                                     0/ 100 =  0%  |
  5  ---     100/ 100 =100%   100/ 100 =100%  ppp-151-164-52-213.rcsntx.swbell.net [151.164.52.213]
                                     0/ 100 =  0%  |
  6  ---     100/ 100 =100%   100/ 100 =100%  gar7.sffca.ip.att.net [12.122.79.97]
                                     0/ 100 =  0%  |
  7  ---     100/ 100 =100%   100/ 100 =100%  cr83.sffca.ip.att.net [12.122.110.118]
                                     0/ 100 =  0%  |
  8  ---     100/ 100 =100%   100/ 100 =100%  cr1.sffca.ip.att.net [12.123.15.109]
                                     0/ 100 =  0%  |
  9  ---     100/ 100 =100%   100/ 100 =100%  cr1.la2ca.ip.att.net [12.122.3.122]
                                     0/ 100 =  0%  |
 10  ---     100/ 100 =100%   100/ 100 =100%  gar7.la2ca.ip.att.net [12.122.104.13]
                                     0/ 100 =  0%  |
 11  61ms     0/ 100 =  0%     0/ 100 =  0%  12.91.226.10
                                   100/ 100 =100%  |
 12  ---     100/ 100 =100%     0/ 100 =  0%  oak1-ar1-xe-1-0-0-0.us.twtelecom.net [206.222.120.198]

Trace complete.
```

Money Talks, Packets Walk

```
Tracing route to www.pacific.edu [138.9.110.12]
over a maximum of 30 hops:

  1   1 ms   <1 ms   <1 ms  hatter.treacle.com [10.0.0.2]
  2   44 ms  44 ms   43 ms  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
  3   43 ms  42 ms   42 ms  dist2-vlan50.skt2ca.sbcglobal.net [68.120.211.67]
  4   43 ms  43 ms   42 ms  ppp-151-164-39-79.resntx.swbell.net [151.164.39.79]
  5   46 ms  45 ms   47 ms  ppp-151-164-52-213.resntx.swbell.net [151.164.52.213]
  6   46 ms  46 ms   47 ms  gar7.nffca.ip.att.net [12.122.79.97]
  7   57 ms  58 ms   58 ms  cr03.cfjca.ip.att.net [12.122.110.110]
  8   59 ms  59 ms   59 ms  cr1.9ffca.ip.att.net [12.123.15.109]
  9   62 ms  59 ms   61 ms  cr1.la2ca.ip.att.net [12.122.3.122]
 10   57 ms  58 ms   57 ms  gar7.la2ca.ip.att.net [12.122.104.13]
 11   56 ms  56 ms   58 ms  12.91.226.10
 12   65 ms  66 ms   67 ms  oakl-sr1-xe-1-0-0-0.ux.tutelacom.net [206.222.120.198]
 13    *      *      *     Request timed out.
 14    *      *      *     Request timed out.
```

```
Tracing route to www.dot.ca.gov [149.136.20.66]
over a maximum of 30 hops:

  1   <1 ms  <1 ms   <1 ms  hatter.treacle.com [10.0.0.2]
  2   44 ms  43 ms   43 ms  adsl 63 206 191 201.dsl.sktn01.pacbell.net [63.206.191.201]
  3   41 ms  42 ms   43 ms  dist1-vlan50.skt2ca.sbcglobal.net [68.120.211.65]
  4   42 ms  42 ms   42 ms  12.83.48.180
  5   46 ms  45 ms   46 ms  12.122.200.9
  6   46 ms  54 ms   49 ms  192.205.37.190
  7   51 ms  51 ms   51 ms  207.88.14.225.ptr.ex.xo.net [207.88.14.225]
  8   52 ms  50 ms   51 ms  ae010.mpr1.mscoville-ca.ex.xo.net [216.156.0.154]
  9   51 ms  52 ms   51 ms  216.55.44.26
 10    *      *      *     Request timed out.
 11    *      *      *     Request timed out.
 12    *     ^C
```

```
C:\>tracert www.cisco.com

Tracing route to c141.cd.akamaiedge.net [196.6.224.170]
over a maximum of 30 hops:

  1   <1 ms  <1 ms   <1 ms  hatter.treacle.com [10.0.0.2]
  2   48 ms  44 ms   45 ms  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
  3   44 ms  43 ms   42 ms  dist1-vlan50.skt2ca.sbcglobal.net [68.120.211.65]
  4   42 ms  43 ms   41 ms  12.83.48.180
  5   47 ms  45 ms   46 ms  151.164.181.206
  6   48 ms  49 ms   48 ms  xe-0-2-0-7.r07.snjsca04.us.bb.gin.ntt.net [129.250.9.141]
  7   49 ms  49 ms   49 ms  196-6-224-170.deploy.akamaitechnologies.com [196.6.224.170]
```


Odd + SYN

2011

```
Tracing route to www.pacific.edu [138.9.110.12]
over a maximum of 30 hops:

  1   1 ms   <1 ms   <1 ms  hatter.treacle.com [10.0.0.2]
  2   44 ms  44 ms   43 ms  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
  3   43 ms  42 ms   42 ms  dist2-vlan50.skt2ca.sbcglobal.net [68.120.211.67]
  4   43 ms  43 ms   42 ms  ppp-151-164-39-79.resntx.swbell.net [151.164.39.79]
  5   46 ms  45 ms   47 ms  ppp-151-164-52-213.resntx.swbell.net [151.164.52.213]
  6   46 ms  46 ms   47 ms  gar7.nffca.ip.att.net [12.122.79.97]
  7   57 ms  58 ms   58 ms  cr03.cfjca.ip.att.net [12.122.110.110]
  8   59 ms  59 ms   59 ms  cr1.9ffca.ip.att.net [12.123.15.109]
  9   62 ms  59 ms   61 ms  cr1.la2ca.ip.att.net [12.122.3.122]
 10   57 ms  58 ms   57 ms  gar7.la2ca.ip.att.net [12.122.104.13]
 11   56 ms  56 ms   58 ms  12.91.226.10
 12   65 ms  66 ms   67 ms  oakl-sr1-xe-1-0-0-0.ux.tutelacom.net [206.222.120.198]
 13    *      *      *     Request timed out.
 14    *      *      *     Request timed out.
```

2012

```
Tracing route to www.pacific.edu [138.9.110.12]
over a maximum of 30 hops:

  1   <1 ms  <1 ms   <1 ms  hatter.treacle.com [10.0.0.2]
  2   43 ms  43 ms   43 ms  adsl 63 206 191 201.dsl.sktn01.pacbell.net [63.206.191.201]
  3   42 ms  42 ms   42 ms  dist2-vlan50.skt2ca.sbcglobal.net [68.120.211.67]
  4   43 ms  43 ms   41 ms  ppp-151-164-39-79.resntx.swbell.net [151.164.39.79]
  5   56 ms  56 ms   55 ms  gar7.la2ca.ip.att.net [12.122.104.13]
  6   55 ms  57 ms   57 ms  12.91.226.10
  7   66 ms  66 ms   65 ms  oakl-sr1-xe-1-0-0-0.ux.tutelacom.net [206.222.120.198]
  8   70 ms  70 ms   69 ms  mail.pfib.com [74.202.6.6]
  9    *      *      *     Request timed out.
 10    *     ^C
```

SYN

```
root@hatter:~# traceroute -I www.pacific.edu
traceroute to www.pacific.edu (138.9.110.12), 30 hops max, 60 byte packets
 1  adsl-63-206-191-201.dsl.sktn01.pacbell.net (63.206.191.201)  43.220 ms  46.000 ms  47.407 ms
 2  dist2-vlan50.skt2ca.sbcglobal.net (68.120.211.67)  47.800 ms  48.440 ms  50.288 ms
 3  ppp-151-164-39-79.resntx.swbell.net (151.164.39.79)  51.859 ms  53.561 ms  55.039 ms
 4  gar7.la2ca.ip.att.net (12.122.104.13)  70.699 ms  72.067 ms  74.115 ms
 5  12.91.226.10 (12.91.226.10)  76.080 ms  77.497 ms  78.878 ms
 6  oakl-sr1-xe-1-0-0-0.ux.tutelacom.net (206.222.120.198)  80.378 ms  83.040 ms  83.484 ms
 7  mail.pfib.com (74.202.6.6)  68.786 ms  69.726 ms  71.549 ms
 8  iisprod.uop.edu (138.9.110.12)  72.120 ms  71.539 ms  72.063 ms
 9  iisprod.uop.edu (138.9.110.12)  73.025 ms  68.602 ms  71.706 ms
10  iisprod.uop.edu (138.9.110.12)  73.698 ms  70.578 ms  71.553 ms
11  iisprod.uop.edu (138.9.110.12)  73.068 ms  73.732 ms  75.305 ms
12  iisprod.uop.edu (138.9.110.12)  80.299 ms  70.612 ms  71.059 ms
root@hatter:~#
```


iisprod

- DNS query about `iisprod.uop.edu`
- Ask `g.root-servers.net -> edu.`
- Ask `g.edu-servers.net`
- `udns2.ultradns.net. ns1.pacific.edu. udns1.ultradns.net.`
- `iisprod.uop.edu` is 1 of 13 domains using 138.9.110.12
  web.pacific.edu www.pacific.edu www.uop.edu
  brubeckinstitute.org universityofthepacific.com
  brubeckfestival.com
  jedediahsmithsociety.org
- ns1 also asnwers for
  pacificspecialcare.com 1800victims.com

iisprod

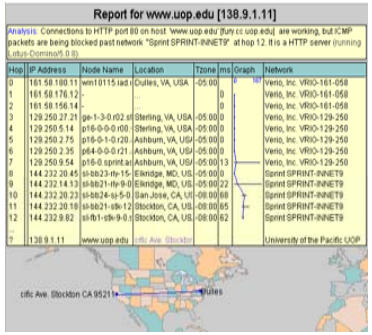
- iisprod > production 138.9.110.12
- Implies there might be an iistest

;; ANSWER SECTION:
iistest.pacific.edu. 86237 IN A 138.9.0.10

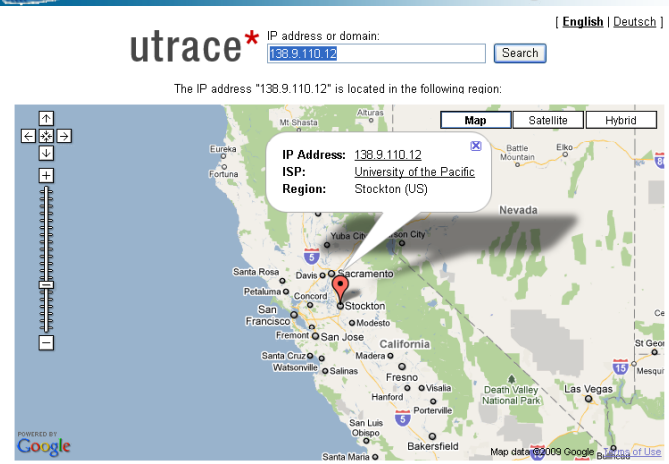
Q: Any Comments?

Visual Traceroutes

- Other traceroutes attempt to locate router hops
- Online traceroutes are available
- Offer additional features
  - Reinvent wheel



Geolocation with Map



Sweeps, Scans, Prints

Next up:

- **Attacker Profiles**
- **Attack Points**