15-441: Computer Networks
Homework 3

Assigned: Nov 2, 2006
Due: Nov 9, 2006

1 Using 'dig' to Understand DNS

1. In this question you will use the unix utility 'dig' to explore the contents of DNS messages. Please use dig on unix.andrew.cmu.edu.

   The format of a dig request issimple. Just type: *dig www.princeton.edu* to perform a look-up for that DNS name. As you now know, DNS requests can do more than just ask for the IP address corresponding to a single DNS name. Type *dig princeton.edu ANY* to see DNS records of all types that are associated with the domain 'princeton.edu'.

   (a) What IP address did the computer you are logged into contact to make the DNS request? Where do you think this server is located?

   (b) List all of the different types of records received as a result of your query. For each record, explain its purpose, using one of the entries provided in the reply as a concrete example.

   (c) Note that some of the names in the reply are not in the domain 'princeton.edu'. Use the DNS names and/or 'traceroute' to find the general location of one of these servers. Where is it? Given the type of record, why would Princeton do this?

   (d) Use dig to find the names of two non-local servers you *could* contact in the process of identifying the nameserver for the domain 'cnn.com' (assume no DNS information is cached anywhere).

   (e) Use dig to find the TTL for the DNS mappings of 'www.cnn.com' and 'www.cs.stanford.edu'. What are they? If your boss asks you to provide two positive and two negative effects of having a short DNS TTL for the company's e-commerce site, what would you say?

2 Tools

2. In this section, you will learn a couple of practical tools: **route**, and **ifconfig**, and **netstat**. Below is a very brief description of what they do. For more detailed information, check the man pages (Note on unix.andrew route and ifconfig are located under /sbin/. Either add this to your PATH or use the full path to run the commands).

   route The `route` command can be used to view and manipulate the IP routing table.

   netstat is a tool that can be used to display network connections, routing tables, interface statistics and many other things.

   ifconfig The `ifconfig` command is used to configure a network interface and to display the status of the currently active interfaces.

(a) Run the `route` command. What is the use of the entry with netmask 0.0.0.0?

(b) Suppose a malicious attacker runs "route del " to delete the routing entry corresponding to 128.2.13.128/26 on one of the unix.andrew.cmu.edu machines. Now you try to run "ping www.cnn.com". Do you expect the ping to get through? Harry Bovik, the local networking guru argues that "Well, there is still a default route, so the ping should go through!". Harry's pessimistic alter ego suggests otherwise, but does not have a reason. Should Harry believe his alter ego or dismiss it as a case of unjustified pessimism? Give a short 1-2 line answer why.

(c) What does the command netstat -a show you? Explain the two parts of the output.

(d) What is the command to view the routing table of your machine using netstat? What is the command to only show IP addresses and not host names in the routing table?

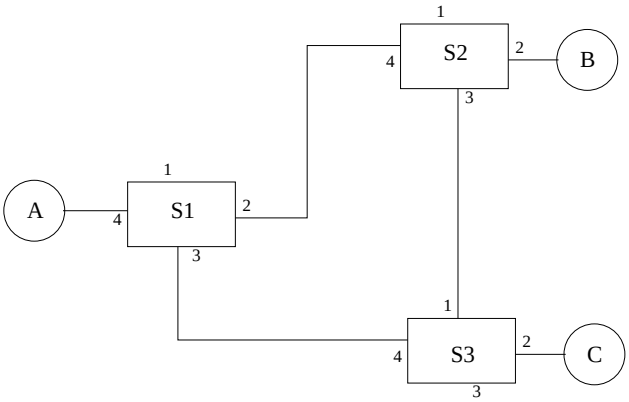
(e) How can you use netstat to find out what the network interfaces of your machine are? What is the MTU of your Ethernet interface?

(f) Run ifconfig. What information does the field "Mask" give you?

(g) What happens if you run ifconfig and configure an interface to be in promiscuous mode?

3 Understanding label switching

You are trying to debug a problem with your company's virtual circuit-based network. A diagram of the network is shown below. A, B, and C are hosts attached to the network. S1, S2, and S3 are switches configured to act as label swapping virtual circuit switches.



The label swapping tables for the switches are configured as follows. Some of the entries are stale and not actually in use right now.

Switch	Input Port	Input Label	Output Port	Output Label
S1	2	2	3	4
S1	4	2	3	1
S1	4	17	2	2
S2	2	19	4	2
S2	3	1	2	19
S2	3	2	2	15
S2	3	5	4	2
S2	4	2	2	1
S2	4	1	4	1
S3	2	1	1	2
S3	2	2	4	5
S3	4	1	1	1
S3	4	4	1	5

3. Write the sequence of (Switch, Input Port, Input Label) tuples and the destination node and label for each of these packets. We've given you the start node and starting label. The intermediate tuples should look like (S1, 1, 999) [e.g., switch S1, input port 1, label 999].

   (a) Start node A, label 17.
   Switch tuples:

   Dest node and final label:

   (b) Start node A, label 2.
   Switch tuples:

   Dest node and final label:

   (c) Start node C, label 1.
   Switch tuples:

   Dest node and final label:

4. You are explaining your network to a colleague, who remarks on an interesting feature of your network.

   (a) What do you tell your colleague when she asks why you configured the paths for packets (a) and (b) above?

   (b) Your colleague thinks this feature is neat, and asks you how to implement it in her packet-switched, IP network. What do you tell her?

5. You notice that the network seems much more sluggish than normal. Packets are getting through, but they take a lot longer than they did before your assistant made some changes to the label swapping tables yesterday. You do some debugging and find that the problem shows up when node B starts transmitting with local label 19. What's going on?

4 TCP Forensics

You are the TCP specialist at the FBI. One day an FBI agent gives you a packet trace of a TCP connection between two machines on the Internet. The trace is believed to contain important information pertaining to national security.

This packet trace contains 63 packets and each line in the trace is one packet, identified by its packet number (from 1 to 63). The rest of the line in a sequence of bytes, represented as hex numbers. For example, consider the first line of the trace:

1 45 00 00 3c fd b1 40 00 40 06 fd 45 80 02 8c ea 8c
d3 a6 04 8f 37 1a 0b b5 3c c0 85 00 00 00 00 a0 02
16 d0 88 c6 00 00 02 04 05 b4 04 02 08 0a 0c 6c
3d 34 00 00 00 00 01 03 03 07

The first number "1" (packet number 1) implies that this is the first packet received at the trace point.

The first byte of the packet is "45" in hex, which is "69" in decimal. As a hint, the first byte seems to indicate that this is an IPv4 packet, where the IP header contains 20 bytes. The fourth byte of the packet is "3c".

This trace, hw3.trace.txt, is available on the course web page under the Assignments link. To reduce the amount of work you have, we provide a template code tcptrace.c (also available on the course web page under the Assignments link) which parses the trace file into an array of bytes. You are free to use perl or any other tools (and even by hand if you wish) to analyze this trace file.

6. Please answer the following questions (and determine whether this is a threat to national security):

   (a) What is the client's IP address, the client's port number, the server's IP address, and the server's port number of this TCP connection? Based on the IP addresses of the client and server, what are their respective DNS names? You may assume that the computer which initiates the connection is the client, and the other computer is the server.

   `Client IP: __________`

   `Client Port: ________`

   `Client DNS Name: ____________________________`

   `Server IP: __________`

   `Server Port: ________`

   `Server DNS Name: ____________________________`

   (b) Which Internet application (i.e. web, FTP, gopher...) is running on top of this TCP connection?

   How do you arrive at this conclusion? (hint: information from your previous answers and Google can help!)

(c) Using the TCP connection state diagram in Figure 6 of RFC 793, identify which packets (by their packet number) cause or result from the TCP state transitions of the TCP client? Your answer should be in the form: when a client receives packet X or user request Y, its TCP state is changed from A to B, and packet Z is sent (or some other action takes place). For example, when a client receives user request OPEN, the TCP state is changed from CLOSED to SYN-SENT, and a packet Z is sent.

(d) Using the same format as used in (c), identify the state transitions with respect to the server.

(e) Can you recreate the "crime scene" at the client's end user terminal? We do not want you to include the exact text in your solution, only a brief description. What is contained in packets 13 and 14's TCP payload, specific to the protocol? What was the client doing, who was the client looking for,

and where was the client looking? (packets 32+)

(f) BONUS(+2): Can you identify a piece of information in the trace that was clear text and would be considered insecure? Please state the piece of information verbatim.

(g) Staple a printout of the source code, script, etc. that you used to answer this problem. This is evidence that you are indeed a qualified FBI TCP expert and did not "hire" someone else to perform this trace analysis.