Justin Wong  
CMPE 150/L  
Katia Obraczka  
2/5/16

Lab 2: HTTP and DNS

**HTTP Part 1:**

1. [5pts] What was the IP address of the “www.example.com” web server and what port number was the web server located on?

The ip address of www.example.com is found at “93.184.216.34”. The source port number was 59998 and the destination port is 80.

2. [5pts] What is a “Request URI”?

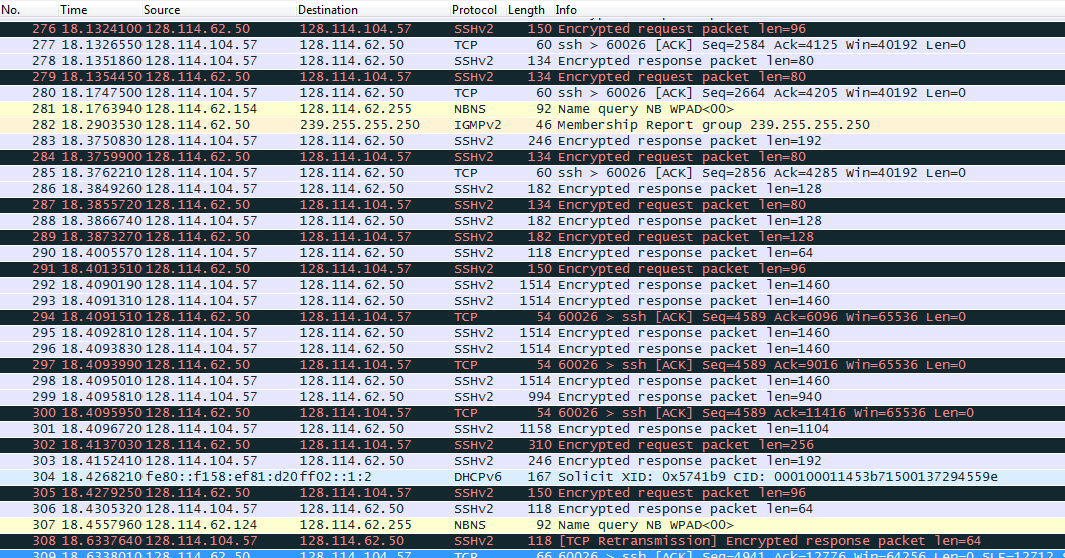
A request Uniform Resource Identifier (URI) is what identifier that the resource that was requested has.

3. [5pts] What version(s) of HTTP is the server using? How do you know?

The server is using “HTTP 1.1”, this is seen through the info that uses “HTTP/1.1”.

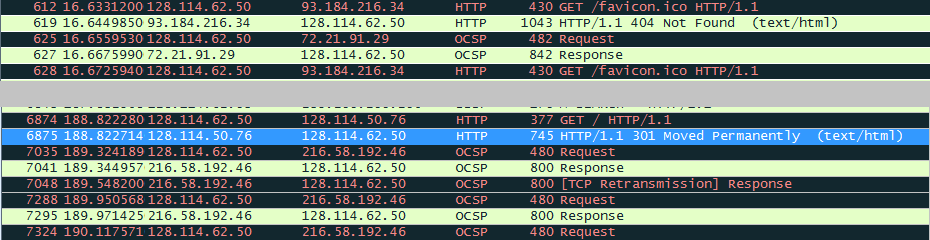
4. [10pts] Open another application on the Windows machine while capturing packets. Without filters added, what do you see this application doing? What evidence is given that this application is responsible for the traffic. Include the summary of the packet exchanges in your report.

While Wireshark was capturing filters I opened up SSH to the unix.ucsc.edu server. It is clear that the SSH is the reason for the packets since for the source ip address “128.114.62.50” the windows computer in POD A in the lab, the destination ip address is 128.114.104.57 being the ip address of unix3.lt.ucsc.edu. The packets exchanged involves the SSHv2 to the unix.ucsc.edu server then a TCP and SSHv2 response from the unix server, the packets exchanged via SSHv2 are all encrypted.



5. [10pts] What status code was returned in response to the initial request to “www.example.com”? What about when “www.soe.ucsc.edu” was requested?

The status code returned for example.com was 404 page not found (above the grey bar). The status code for soe.ucsc.edu was 301 Moved Permanently (below the grey bar).



6. [5pts] What is the IP address and port number of the my.ucsc.edu web server?

The IP address is “128.114.119.200” the port number is 443 since it is https instead of http.

7. [5pts] What is different about the ‘payload’ (the contents of the packet), from those of the example.com packet?

The difference between my.ucsc.edu and the www.example.com payloads is that the my.ucsc.edu packages have OCSP protocol in between them.

**DNS Part 1:**

1. [50 pts] List and explain the output of the host –v commands run on PC4 & PC1. Which names were resolved?

Host is usually used to for DNS lookups where it will convert ip addresses to names or vice-versa. The “-v” option will ask the host to make a query of type “ANY”.

(1) host –v PC2.mylab.com returned 10.0.1.21 and PC2.mylab.com as the answer and the authority being PC4 since that is the host for pc2  
(2) host –v 10.0.1.21 returned 21.1.0.10.in-addr.arpa and PC2.mylab.com as the answer and PC4.mylab.com and 10.0.1.41 as the authority   
(3) host –v localhost returned localhost.localhost root.localhost.localhost since it is locating itself, the return from the lookup also returned in 0ms since it is sending it to itself. In our hosts file we also set the loopback to be 127.0.0.1 for IPv4 or ::1 for IPv6.  
(4) host –v tcpip­-lab.net returns “connection timed out; no servers could be reached” meaning it failed

(5) host –v PC4.mylab.com returned PC4.mylab.com and 10.0.1.41 since PC4 is the host  
(6) host –v 10.0.1.21 returned PC2.mylab.com and 10.0.1.21  
(7) host –v localhost returned PC4lab.com and 10.0.1.41 since PC4 is the localhost  
(8) host –v tcp-ip­lab.net returned “connection timed out; no servers could be reached”

2. [10 pts] Did all 4 ping commands generate a DNS message?

Yes, they all created an entry in Wireshark but the “ping –c 3 tcpip­lab.net” gave a failure message.

3. [20 pts] What happens if a DNS query that cannot be resolved is issued? Were all of the queries in the trace resolved?

If the DNS query cannot be resolved, it will try a couple of times (in my case it was 3) and then it will give up. The only query that failed was the “ping –c 3 tcpip­lab.net”.

4. [10 pts] When you repeated the ping to PC4, did PC1 issue another DNS request or was the previous response cached?

PC1 issued another DNS request to PC4, it was not a cached response.

**DNS PART 2**

1. [40 pts] For each command, explain how the observed DNS queries are resolved.

In my testing, these were the results of what I observed.

Router1:

(1) *ping R2.mylab.com*: Starting at R1 it went to PC4 (the name server) then to PC2 (the domain) back to PC4 and then back to R1

(2) *ping R3.lab9.net*: Starting at R1 to PC4(the name server) to root to PC3(domain) to PC4 back to R1

(3) *ping Router4.com*: Starting at R1

Router 3:

(4) *ping R1.mylab.com*: Starting at R3 to PC3 (the name server) to root to PC2 to PC4 back to PC3 and finally to R3

(5) *ping Router4.com*: Starting at R3 to PC3 (the name server) to root to PC2 back to PC3 ending at R3

(6) *ping root-server.net*: Starting at R3 to PC3 (the name server) to PC1 back to PC3 ending at R3

Router 4:

(7) *ping R3.lab9.net*: Starting at R4 go to PC2 (the name server) and recursively go to PC1 (root) then go through PC3 (.net domain) and returns via the same path to R4.

Router 2:

(8) *ping R3.lab9.net*: Since we used the command “Kill the root name server on PC1”, it is not possible to get to R3 from R2 without the root server, the pathway has been disconnected

2. [10 pts] Which queries have the recursion-­desired flag set?

The recursion flag was set for all of the them, except for the last query since it was not a successful query.

3. [5 pts] List the authoritative servers for the .net and .com domains.

PC3 was the .net authoritative server and PC2 was the .com authoritative server.

4. [10 pts] Do you observe recursive or iterative DNS queries, or both?

In my experience, I had only observed recursive DNS queries.