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"?

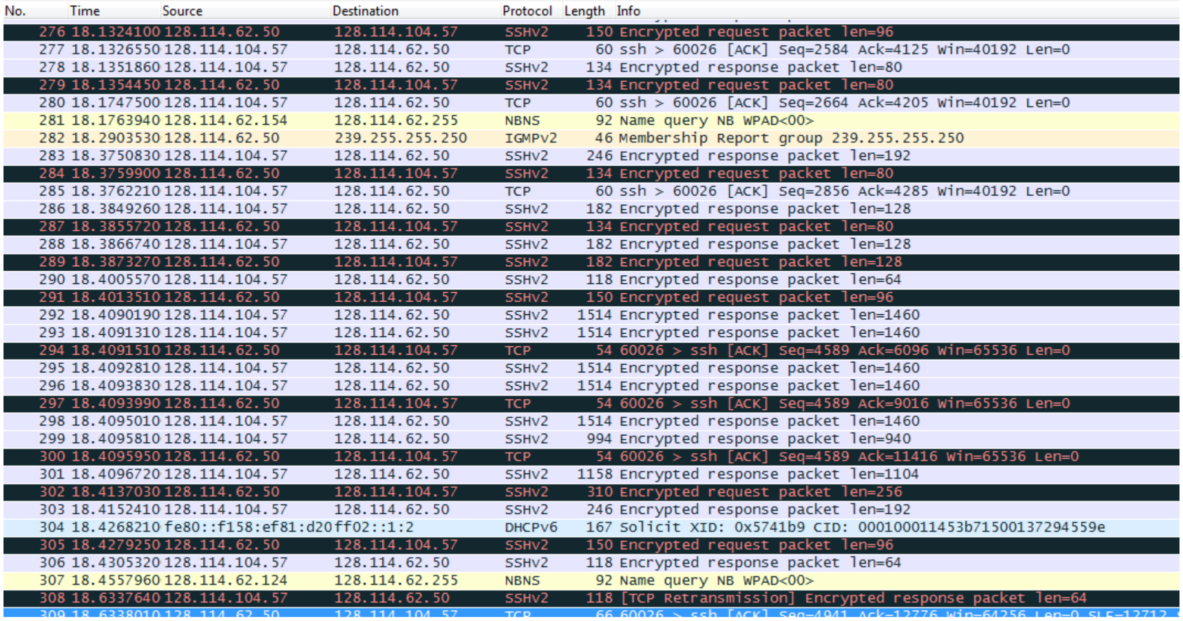
A request Uniform Resource Identifier (URI) is what identifier that the resource that was requested has.

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.

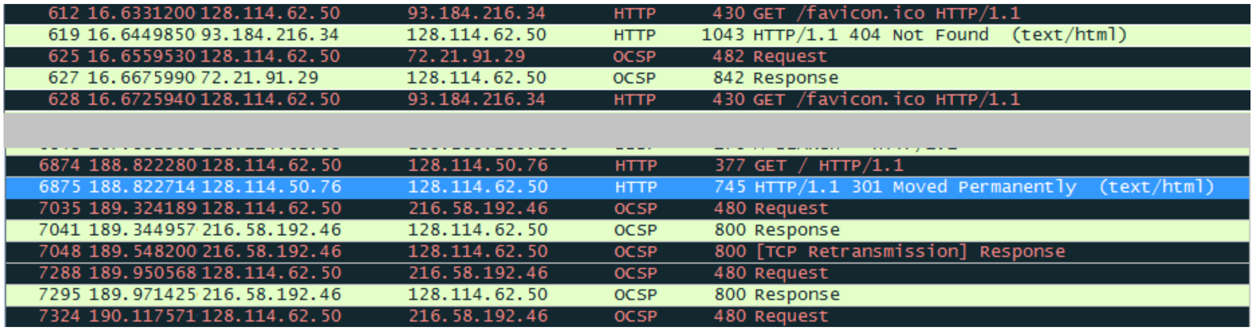
While Wireshark was capturing filters I opened up SSH to the unix.ucsc.edu server. It is clear that the SSH is the reason for the packets since for the source ip address "128.114.62.50" the windows computer in POD A in the lab, the destination ip address is 128.114.104.57 being the ip address of unix3.lt.ucsc.edu. 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.



No.	Time	Source	Destination	Protocol	Length	Info
276	18.1324100	128.114.62.50	128.114.104.57	SSHv2	150	Encrypted request packet len=96
277	18.1326550	128.114.104.57	128.114.62.50	TCP	60	ssh > 60026 [ACK] Seq=2584 Ack=4125 Win=40192 Len=0
278	18.1351860	128.114.104.57	128.114.62.50	SSHv2	134	Encrypted response packet len=80
279	18.1354450	128.114.62.50	128.114.104.57	SSHv2	134	Encrypted request packet len=80
280	18.1747500	128.114.104.57	128.114.62.50	TCP	60	ssh > 60026 [ACK] Seq=2664 Ack=4205 Win=40192 Len=0
281	18.1763940	128.114.62.154	128.114.62.255	NBNS	92	Name query NB WPAD<00>
282	18.2903530	128.114.62.50	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
283	18.3750830	128.114.104.57	128.114.62.50	SSHv2	246	Encrypted response packet len=192
284	18.3759900	128.114.62.50	128.114.104.57	SSHv2	134	Encrypted request packet len=80
285	18.3762210	128.114.104.57	128.114.62.50	TCP	60	ssh > 60026 [ACK] Seq=2856 Ack=4285 Win=40192 Len=0
286	18.3849260	128.114.104.57	128.114.62.50	SSHv2	182	Encrypted response packet len=128
287	18.3855720	128.114.62.50	128.114.104.57	SSHv2	134	Encrypted request packet len=80
288	18.3866740	128.114.104.57	128.114.62.50	SSHv2	182	Encrypted response packet len=128
289	18.3873270	128.114.62.50	128.114.104.57	SSHv2	182	Encrypted request packet len=128
290	18.4005570	128.114.104.57	128.114.62.50	SSHv2	118	Encrypted response packet len=64
291	18.4013510	128.114.62.50	128.114.104.57	SSHv2	150	Encrypted request packet len=96
292	18.4090190	128.114.104.57	128.114.62.50	SSHv2	1514	Encrypted response packet len=1460
293	18.4091310	128.114.104.57	128.114.62.50	SSHv2	1514	Encrypted response packet len=1460
294	18.4091510	128.114.62.50	128.114.104.57	TCP	54	60026 > ssh [ACK] Seq=4589 Ack=6096 Win=65536 Len=0
295	18.4092810	128.114.104.57	128.114.62.50	SSHv2	1514	Encrypted response packet len=1460
296	18.4093830	128.114.104.57	128.114.62.50	SSHv2	1514	Encrypted response packet len=1460
297	18.4093990	128.114.62.50	128.114.104.57	TCP	54	60026 > ssh [ACK] Seq=4589 Ack=9016 Win=65536 Len=0
298	18.4095010	128.114.104.57	128.114.62.50	SSHv2	1514	Encrypted response packet len=1460
299	18.4095810	128.114.104.57	128.114.62.50	SSHv2	994	Encrypted response packet len=940
300	18.4095950	128.114.62.50	128.114.104.57	TCP	54	60026 > ssh [ACK] Seq=4589 Ack=11416 Win=65536 Len=0
301	18.4096720	128.114.104.57	128.114.62.50	SSHv2	1158	Encrypted response packet len=1104
302	18.4137030	128.114.62.50	128.114.104.57	SSHv2	310	Encrypted request packet len=256
303	18.4152410	128.114.104.57	128.114.62.50	SSHv2	246	Encrypted response packet len=192
304	18.4268210	fe80::f158:ef81:d20	ff02::1:2	DHCPv6	167	Solicit XID: 0x5741b9 CID: 000100011453b71500137294559e
305	18.4279250	128.114.62.50	128.114.104.57	SSHv2	150	Encrypted request packet len=96
306	18.4305320	128.114.104.57	128.114.62.50	SSHv2	118	Encrypted response packet len=64
307	18.4557960	128.114.62.124	128.114.62.255	NBNS	92	Name query NB WPAD<00>
308	18.6337640	128.114.104.57	128.114.62.50	SSHv2	118	[TCP Retransmission] Encrypted response packet len=64
309	18.6338010	128.114.62.50	128.114.104.57	TCP	66	60026 > ssh [ACK] Seq=4941 Ack=12776 Win=64256 Len=0 SLE=12712

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).



```
 612 16.6331200 128.114.62.50   93.184.216.34   HTTP    430 GET /favicon.ico HTTP/1.1
 619 16.6449850 93.184.216.34   128.114.62.50   HTTP   1043 HTTP/1.1 404 Not Found  (text/html)
 625 16.6559530 128.114.62.50   72.21.91.29     OCSP    482 Request
 627 16.6675990 72.21.91.29     128.114.62.50   OCSP    842 Response
 628 16.6725940 128.114.62.50   93.184.216.34   HTTP    430 GET /favicon.ico HTTP/1.1

6874 188.822280 128.114.62.50   128.114.50.76   HTTP    377 GET / HTTP/1.1
6875 188.822714 128.114.50.76   128.114.62.50   HTTP    745 HTTP/1.1 301 Moved Permanently  (text/html)
7035 189.324189 128.114.62.50   216.58.192.46   OCSP    480 Request
7041 189.344957 216.58.192.46   128.114.62.50   OCSP    800 Response
7048 189.548200 216.58.192.46   128.114.62.50   OCSP    800 [TCP Retransmission] Response
7288 189.950568 128.114.62.50   216.58.192.46   OCSP    480 Request
7295 189.971425 216.58.192.46   128.114.62.50   OCSP    800 Response
7324 190.117571 128.114.62.50   216.58.192.46   OCSP    480 Request
```

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.