Jakub Szpunar

CS4480

WS Lab 1

1. Three protocols seen:
   a. pnrp (Peer Name Resolution Protocol)
   b. SSDP (Simple Service Discovery Protocol)
   c. ICMPv6 (Internet Control Message Protocol version 6)
2. 79ms Between HTTP GET and HTTP OK.
3. 128.119.245.12 (gaia.cs.umass.edu). My own computer is 192.168.11.41 (on home network).
4. Packets:

No.   Time   Source   Destination   Protocol Length Info
26 9.181536000   192.168.11.41   128.119.245.12   HTTP   444   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 26: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0
Ethernet II, Src: AsustekC_40:d8:45 (f4:6d:04:40:d8:45), Dst: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46)
Internet Protocol Version 4, Src: 192.168.11.41 (192.168.11.41), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 30204 (30204), Dst Port: http (80), Seq: 1, Ack: 1, Len: 390
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/INTRO-wireshark-file1.html
    Request Version: HTTP/1.1
  User-Agent: Opera/9.80 (Windows NT 6.2; WOW64) Presto/2.12.388 Version/12.12\r\n
  Host: gaia.cs.umass.edu\r\n
  Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

No.   Time   Source   Destination   Protocol Length Info
28 9.260564000   128.119.245.12   192.168.11.41   HTTP   434   HTTP/1.1 200 OK (text/html)

Frame 28: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 0
Ethernet II, Src: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46), Dst: AsustekC_40:d8:45 (f4:6d:04:40:d8:45)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.11.41 (192.168.11.41)
Transmission Control Protocol, Src Port: http (80), Dst Port: 30204 (30204), Seq: 1, Ack: 391, Len: 380
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Tue, 08 Jan 2013 20:27:35 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Tue, 08 Jan 2013 20:27:01 GMT\r\n
    ETag: "8734b-51-c4a2af40"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
Line-based text data: text/html
    <html>\n
    Congratulations! You've downloaded the first Wireshark lab file!\n
    </html>\n