Netwerken en systeembeveiliging
Assignment 1

Inge Becht

November 1, 2012

1. IP-address of ss64.com : 216.92.29.160
   IP-address of the sending computer : 145.18.214.201

2. 8 HTTP GET messages were sent. I used filter `http and ip.src == 145.18.214.201 and ip.dst == 216.92.29.160`

3. I chose the `GET /bash.ping.html HTTP/1.1` message. The included protocols were:

   - Internet Protocol version 4 (IPv4)
   - Transmission Control Protocol
   - Hypertext Transfer Protocol (HTTP)

4. If by your computer is meant the computer from which the dump is taken: 8 HTTP OK messages from ss64.com(filter : `http and ip.src == 145.18.214.201 and ip.dst == 216.92.29.160`)

5. By filtering on `http` the first two messages are a HTTP GET and HTTP OK messages. Then, choosing the `Seconds since Previously Displayed Packet` option as the time display you get approximately 0.4345 seconds.

6. Yes, 6 images were sent:

   - ss64.gif

- bash-l.gif
- syntax-r.gif
- top-4.gif
- roll-left.png
- roll-right.png

7. Done by right clicking on the packet and choosing `print`. (You do have to make certain that the things you want to print are opened in the list of information when you double click on a packet). The packets from which the messages were extracted are `GET /bash/ping.html HTTP/1.1` (entry 86) and `HTTP/1.1 200 OK (text/html)` (entry 114). The messages can be seen in Appendix A(at the back).

8. Computer sent 38 packets(total of 5650 bytes) to the server and ss64.com sent 39 packets(total of 32908 bytes) to the computer There is a lot more received by the computer than sent, this because all the images needed to be sent to the computer and the computer only asked for permission to get this content. So the received data contains more bytes than the data sent out.

9. See figure 1 for the graph. This graph seems not all that clear to me so also see figure 2 for the HTTP messages sent between ss64.com and the computer. Here the seems to be consistent with earlier answers(8 HTTP GET messages were sent and 8 received)

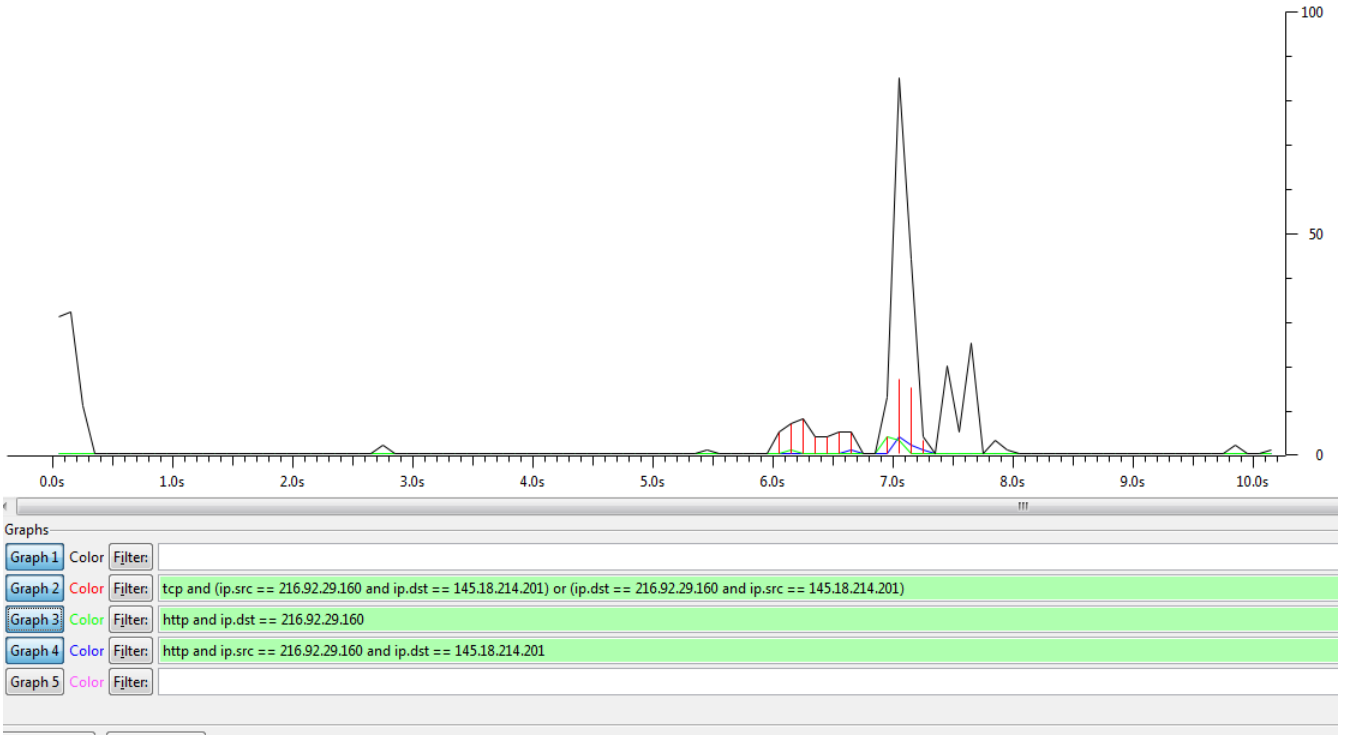

Figure 1: Packet distribution

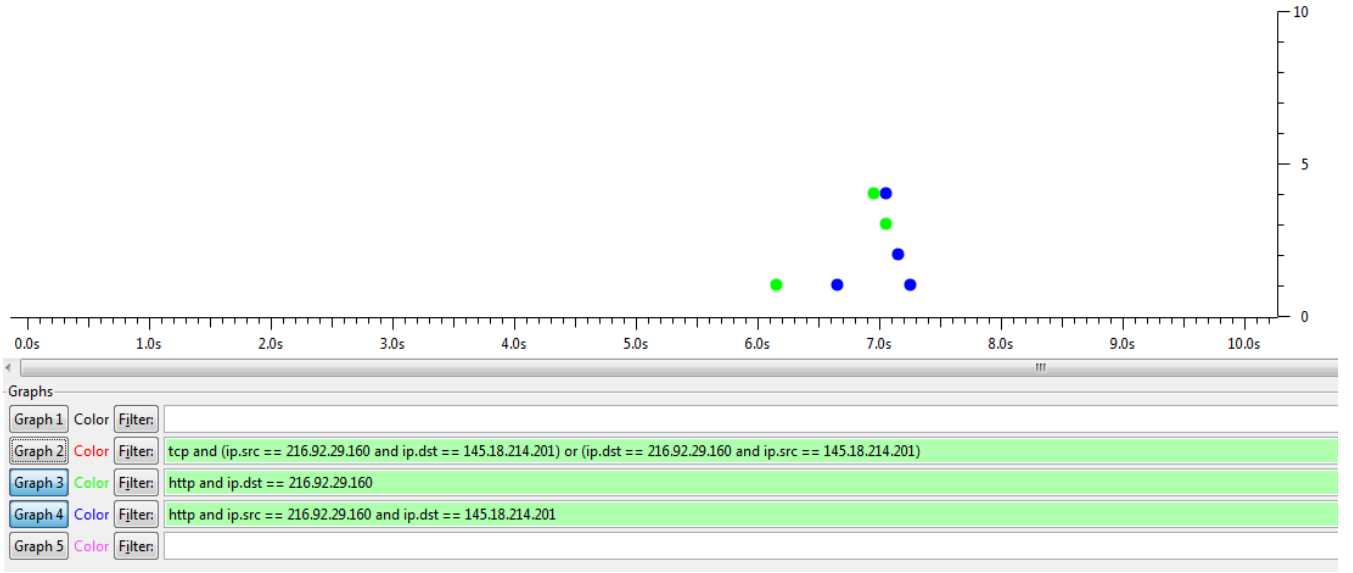

Figure 2: HTTP GET and OK distribution between computer and ss64.com

10. The passwords sent are `wrong!` and `network`. First I filtered on `http` to show all readable data. Here I found the ip 145.100.102.253 making a HTTP GET request towards ip 145.00.102.153. So the first ip belonged to the computer and the other ip to some site that the computer tried to connect to. In the HTML sent to the computer I could read when the user did not have access to the page tried to visit and when he did (entry 13 and 25 respectively). So then I read the data in the requests, and found the authorization section with the credentials and the things that were different between both requests. The correct password is network. This because after applying this password the computer receives the sites content that shows it was the right password. I myself went to the protected page as well, to check if this password worked (together with the username wireshark-student) and it worked.

A Data for question 7

Data from `GET /bash/ping.html HTTP/1.1` (entry 86):

```
No. Time         Source          Destination    Protocol Length Info
86  6.195787000  145.18.214.201  216.92.29.160  HTTP     485    GET /bash/ping.html

Frame 86: 485 bytes on wire (3880 bits),
                            485 bytes captured (3880 bits) on interface 0
Ethernet II, Src: Apple_11:f3:14 (e4:ce:8f:11:f3:14),
                            Dst: Cisco_45:2c:00 (00:0a:42:45:2c:00)
Internet Protocol Version 4, Src: 145.18.214.201 (145.18.214.201),
                            Dst: 216.92.29.160 (216.92.29.160)
Transmission Control Protocol, Src Port: 50839 (50839),
                            Dst Port: http (80), Seq: 1, Ack: 1, Len: 419
Hypertext Transfer Protocol
    GET /bash/ping.html HTTP/1.1\r\n
    Host: ss64.com\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5)
                        AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94 S
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    \r\n
    [Full request URI: http://ss64.com/bash/ping.html]
```

Data from `HTTP/1.1 200 OK (text/html)` (entry 114):

```
    No.     Time           Source                Destination           Protocol Le
```

```
    114 6.630232000    216.92.29.160         145.18.214.201        HTTP     1341

Frame 114: 1341 bytes on wire (10728 bits), 1341 bytes captured (10728 bits) on int
Ethernet II, Src: Cisco_45:2c:00 (00:0a:42:45:2c:00), Dst: Apple_11:f3:14 (e4:ce:8
Internet Protocol Version 4, Src: 216.92.29.160 (216.92.29.160), Dst: 145.18.214.2
Transmission Control Protocol, Src Port: http (80), Dst Port: 50839 (50839), Seq:
[10 Reassembled TCP Segments (12362 bytes): #96(279), #101(1351), #102(1351), #103
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Oct 2012 14:21:03 GMT\r\n
    Server: Apache/2.2.22\r\n
    Last-Modified: Mon, 27 Aug 2012 10:50:53 GMT\r\n
    ETag: "2f33-4c83d197c9d40"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 12083\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.
    <head>\n
    <link rel="STYLESHEET" href="../main.css" type="text/css">\n
    <title>ping Man Page | SS64.com</title>\n
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">\n
    </head><!-- #BeginLibraryItem "/Library/head_bash.lbi" --><div id="nav-menu"><u
    <li><a class="rl" href="../index.html"><img src="../images/ss64.gif" alt="Home"
    <li><a class="rl" href="../bash"><img src="../images/bash-l.gif" alt="bash" wi
    <li><form action="http://www.google.com/search" method="get" style="margin:0px
    <input name="q" type="text" alt="search" id="question" size="20" maxlength="255
    <input class="submit" type="submit" value="Search" id="btn">\n
    <input type="hidden" name="sitesearch" value="ss64.com/bash/">\n
    </form></li>\n
    <li><a class="rr" href="syntax.html"><img src="../images/syntax-r.gif" width="1
```

```
</div> <!-- #EndLibraryItem --><h1>ping</h1> \n
<p>Test a network connection. When using ping for fault isolation, it should fi
Then, hosts and gateways further and further away should be ‘pinged’.</p>\n
<pre>Syntax<br>      ping [<i>options</i>] <i>destination_host</i>\n
\n
Options\n
\n
   -a         Audible ping. \n
\n
   -A         Adaptive ping. Interpacket interval adapts to round-trip time, \n
              so that effectively not more than one (or more, if preload is set
              present in the network. Minimal interval is 200msec for not super
              On networks with low rtt this mode is essentially equivalent to i
\n
   -b         Allow pinging a broadcast address. \n
\n
   -B         Do not allow ping to change source address of probes. The address
\n
   -c <i>count</i>   Stop after sending (and receiving) <i>count</i> ECHO_RESPO
\n
   -d         Debug, Set the SO_DEBUG option on the socket being used.\n
\n
   -F <i>flow_label</i>  Allocate and set 20 bit flow label on echo request pac
                  If value is zero, kernel allocates random flow label.\n
\n
   -f         Flood ping, output packets as fast as they come back or 100 times
\n
   -i <i>wait</i>    Set an interval of <i>wait </i>seconds between sending eac
              Only super-user may set <i>wait</i> to values less 0.2 seconds.\n
              (incompatible with -f)\n
\n
   -I <i>interface address<br></i>              Set source address to specified
              Argument may be numeric IP address or name of device.\n
              Required when pinging an IPv6 link-local address.\n
```

```
\n
   -l <i>preload</i> If preload is specified, ping sends that many packets as
              possible before falling into its normal mode of behavior.\n
              Only the super-user may select preload more than 3.\n
\n
   -L         Suppress loopback of multicast packets.\n
              only applies if the ping destination is a multicast address.\n
\n
   -n         Numeric output only. No attempt will be made to lookup symbolic\
              names for host addresses.\n
   -p <i>pattern</i>\n
              Specify up to 16 ‘pad’ bytes to fill out the packet sent.\n
              This is useful for diagnosing data-dependent problems in a\n
              network. eg, ‘-p ff’ will fill the packet sent with all ones.\n
\n
   -q         Quiet output. Only display the summary lines at startup time and
 \n
   -Q <i>tos    </i> Set Quality of Service -related bits in ICMP datagrams. <
              Multiple TOS bits should not be set simultaneously. For detail se
\n
   -R         Record route(IPv4 only). Includes the RECORD_ROUTE option in the
              display the route buffer on returned packets.\n
              Note that the IP header is only large enough for nine such routes
              Many hosts ignore or discard this option.\n
 \n
   -r         Bypass the normal routing tables and send directly to a host on a
              If the host is not on a directly-attached network, an error is re
              This option can be used to ping a local host through an interface
              (e.g., after the interface was dropped by routed(8)).\n
\n
   -s <i>packetsize\n
            </i>  The number of data bytes to be sent. The default is 56, which
              64 ICMP data bytes when combined with the 8 bytes of ICMP header
\n
```

```
   -S <i>sndbuf</i>  Set socket <i>sndbuf</i>. If not specified, it is selected
   -t <i>ttl</i>     Set the IP Time to Live. <br>\n
   -T <i>timestamp_option</i><br>              Set special IP timestamp options
              'tsandaddr' (timestamps and addresses)\n
              or 'tsprespec host1 [host2 [host3 [host4]]]' (timestamp prespeci
   -M <i>hint</i>    Select Path MTU Discovery strategy. <i>hint</i> may be eit
              even local one), 'want' (do PMTU discovery, fragment locally when
              or 'dont' (do not set DF flag). <br>\n
   -U         Print full user-to-user latency (the old behaviour).\n
              Normally ping prints network round trip time, which can be differ
\n
   -v         Verbose output. ICMP packets other than ECHO_RESPONSE that are re
 \n
</pre>\n
<p>\n
Ping is intended for use in network testing, measurement and management. Becaus
[truncated] <p>If ping does not receive any reply packets at all it will exit w
<p>PING is <a href="http://ftp.arl.mil/~mike/ping.html">named</a> after the sou
[truncated] <p>Ping response times below 10 milliseconds often have low accurac
<p><b>Flood Ping</b><br>\n
[truncated] For every ECHO_REQUEST sent a period '.' is printed, while for ever
[truncated] <p>Round-trip times and packet loss statistics are computed. If dup
<p>Flood pinging is not recommended in general, and flood pinging the broadcast
<p><b>ICMP Packet Details</b><br>\n
[truncated] An IP header without options is 20 bytes. An ICMP ECHO_REQUEST pack
[truncated] <p> If the data space is at least eight bytes large, ping uses the
<p><b>Duplicate and Damaged Packets</b><br>\n
Ping will report duplicate and damaged packets. <br>\n
Duplicate packets are rarely; if ever; a good sign, although the presence of lo
Damaged packets are a serious cause for alarm and often indicate broken hardwar
<p><b>Different Data Patterns</b><br>\n
The (inter)network layer should never treat packets differently depending on th
[truncated] problems have been known to sneak into networks and remain undetect
<p><b>TTL Details</b><br>\n
```

```
[truncated] The <a href="http://en.wikipedia.org/wiki/Time_to_live">Time To Liv
<p> The TCP/IP specification states that the TTL field for TCP packets should b
[truncated] <p> The maximum possible value of this field is 255, and most Unix
<p> In normal operation ping prints the ttl value from the packet it receives.
<ul>\n
<li> Not change it; this is what Berkeley Unix systems did before the 4.3BSD-Ta
<li> Set it to 255; this is what current Berkeley Unix systems do. In this case
<li> Set it to some other value. Some machines use the same value for ICMP pack
</ul>\n
<p class="quote"><i>&ldquo;There's a Nong Nang Ning, Where the trees go Ping!&r
<p><b> Related</b>:</p>\n
<p>netstat(1), \n
ifconfig(8), \n
routed(8)<br>\n
Windows PowerShell equivalent: \n
<a href="../ps/test-connection.html">Test-Connection</a> - Ping one or more com
<!-- #BeginLibraryItem "/Library/foot_bash.lbi" --><p align="left"><script type
google_ad_client = "ca-pub-6140977852749469";\n
/* bash */\n
google_ad_slot = "0284073368";\n
google_ad_width = 300;\n
google_ad_height = 250;\n
//-->\n
</script>\n
<script type="text/javascript"\n
src="http://pagead2.googlesyndication.com/pagead/show_ads.js">\n
</script><br>\n
</p>\n
<div align="center"><hr size="1">\n
<p id="top"><a href="#"><img src="../images/top-4.gif" width="47" height="53" b
<p class="tagline">&copy; Copyright <a href="http://ss64.com/">SS64.com</a> 199
Some rights reserved</p></div><!-- #EndLibraryItem --></body>\n
</html>\n
```