ECE435: Network Engineering – Homework 6

Internet Protocol v4

Due: Thursday, 19 October 2016, 12:30pm

For this homework short answers will suffice.

To submit, create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 6" and be sure your name is included in the document.

1. If you recall from previous homeworks we looked at a packet similar to this:

```
0x0000:  0013 3b10 667f b827 ebaf 3711 0800 4500  ..;.f..'..7...E.
0x0010:  0038 572a 4000 4006 69cc c0a8 0833 826f  .8W*@.@.i....3.o
0x0020:  2e7f bda5 0050 cdc4 6a49 3c7b 6ca5 8018  .....P..jI<{l...
0x0030:  00e5 79f4 0000 0101 080a 0104 3e58 34a8  ..y.........>X4.
0x0040:  7bc3 4745 540a                           {.GET.
```

   The IPv4 header begins at offset 0xe. Fill in the name of the field as well as decode the value. For help decoding the IPv4 header see the class notes or else RFC791.

BEGIN IPv4 HEADER	Name of Field	Decoded Value
0x000e: 4		
0x000e: 5		
0x000f: 00		
0x0010: 0038		
0x0012: 572a		
0x0014: 4000		
0x0016: 40		
0x0017: 06		
0x0018: 69cc		
0x001a: c0a8 0833		
0x001e: 826f 2e7f		
END IPv4 HEADER		

2. Security

You notice your computer is running slowly and the activity LED on your router is blinking rapidly. You are running Linux, and you know that running either `netstat` or `ss -a` will tell you at the socket level what's going on.

The `ss -a` command gives a report similar to the following (the u_str and u_dgm entries are removed; those are UNIX domain sockets which are local-to-the system equivalents of tcp/udp used for interprocess communication).

```
Netid  State      Recv-Q Send-Q Local Address:Port       Peer Address:Port
tcp    CLOSE-WAIT 1      0      192.168.8.38:34466       74.125.202.108:imaps
tcp    CLOSE-WAIT 1      0      192.168.8.38:35610       216.58.192.194:https
tcp    CLOSE-WAIT 1      0      192.168.8.38:36884       216.58.192.196:https
tcp    ESTAB      0      0      192.168.8.38:35496       74.125.202.109:imaps
tcp    ESTAB      0      0      192.168.8.38:36888       130.111.218.16:ssh
tcp    ESTAB      0      0      192.168.8.38:37284       23.45.134.221:https
tcp    ESTAB      0      0      192.168.8.38:42308       100.16.227.202:ssh
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53074
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53075
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53076
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53086

... 200 more just like this

tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53150
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53151
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53152
tcp    SYN-RECV   0      0      192.168.8.38:ssh         192.168.8.51:53153
tcp    TIME-WAIT  0      0      192.168.8.38:52020       172.217.9.66:https
tcp    TIME-WAIT  0      0      192.168.8.38:52242       172.217.9.34:https
tcp    TIME-WAIT  0      0      192.168.8.38:56936       216.58.192.196:https
tcp    TIME-WAIT  0      0      192.168.8.38:57386       216.58.216.106:https
udp    UNCONN     0      0       *:789                   *:*
udp    UNCONN     0      0       *:ipp                   *:*
udp    UNCONN     0      0       *:mdns                  *:*
udp    UNCONN     0      0       *:netbios-dgm           *:*
udp    UNCONN     0      0       *:netbios-ns            *:*
udp    UNCONN     0      0       *:sunrpc                *:*
tcp    LISTEN     0      128     *:ssh                   *:*
tcp    LISTEN     0      128     *:sunrpc                *:*
tcp    LISTEN     0      20      127.0.0.1:smtp          *:*
tcp    LISTEN     0      50      *:microsoft-ds          *:*
tcp    LISTEN     0      50      *:netbios-ssn           *:*
tcp    LISTEN     0      5       127.0.0.1:ipp           *:*
```

(a) Should you worry about the tcp/CLOSE-WAIT connections? Why or why not?

(b) Should you worry about the tcp/ESTAB connections? Why or why not?

(c) Should you worry about the copious tcp/SYN-RECV connections? Why or why not?

(d) Should you worry about the tcp/TIME-WAIT connections? Why or why not?

(e) Should you worry about the udp/UNCONN connections? Why or why not?

(f) Should you worry about the tcp/LISTEN connections? Why or why not?

3. Using tcpdump you also notice a lot of packets going to a different machine you have, but if you run `ss -a` it does not show all of those SYN-RECV connections. You view the system log `demsg` and it says:

```
[1832748.308978] TCP: request_sock_TCP: Possible SYN flooding on port 22.
                 Sending cookies.  Check SNMP counters.
[1832752.416011] DCCP: Activated CCID 2 (TCP-like)
[1832752.416014] DCCP: Activated CCID 3 (TCP-Friendly Rate Control)
[1832752.422698] sctp: Hash tables configured (bind 256/256)
```

   What probably happened here?

4. I'm trying to get a coding segment to this homework together. If I get it ready in time I'll send an e-mail to announce it.