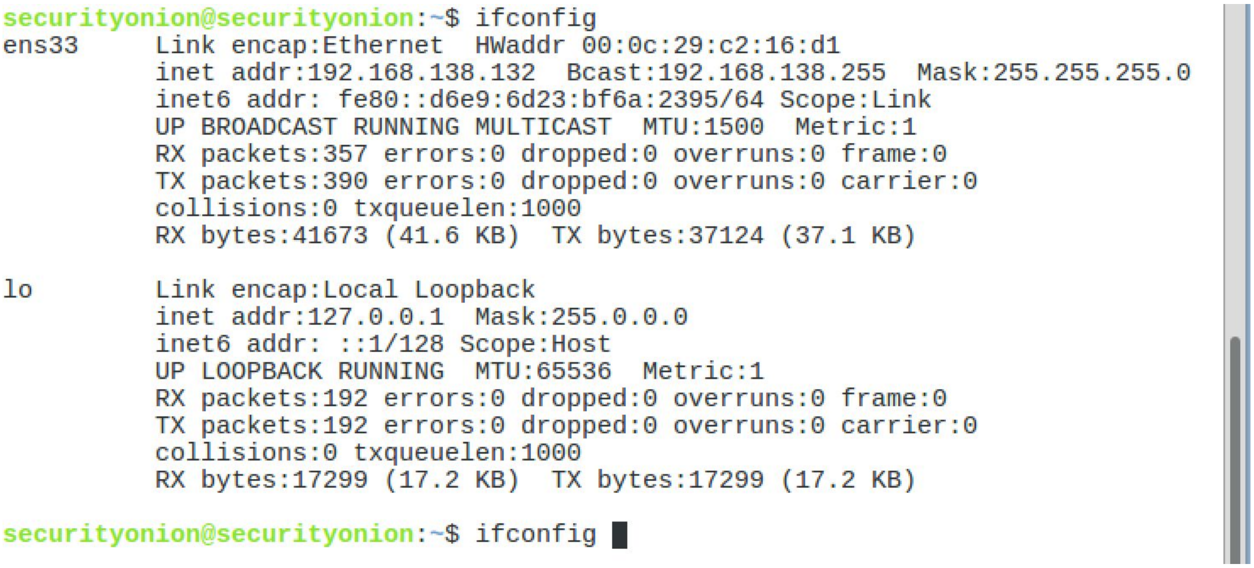
Network Security Practices
CY5150
Task 9

Submitted By:
Sonam Ghatode(001305171)

Table of Contents

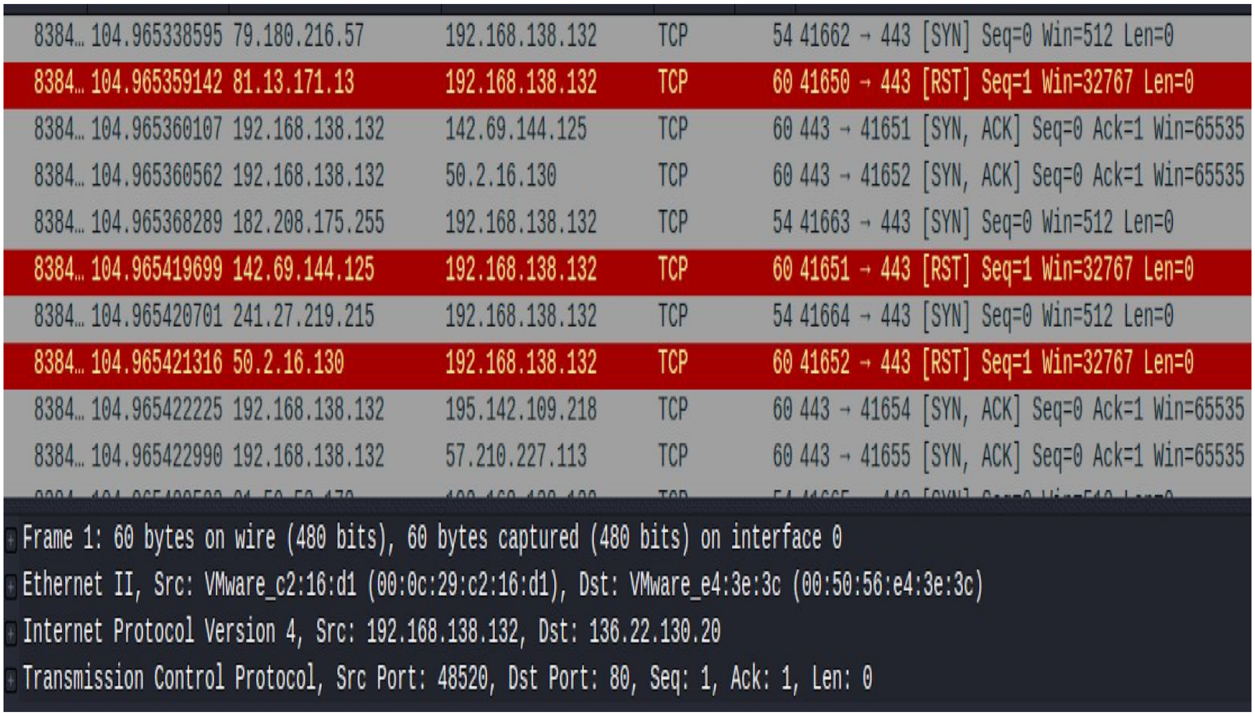
Screenshot of the SYN Flood created by Kali VM:

IP of Security Onion VM:

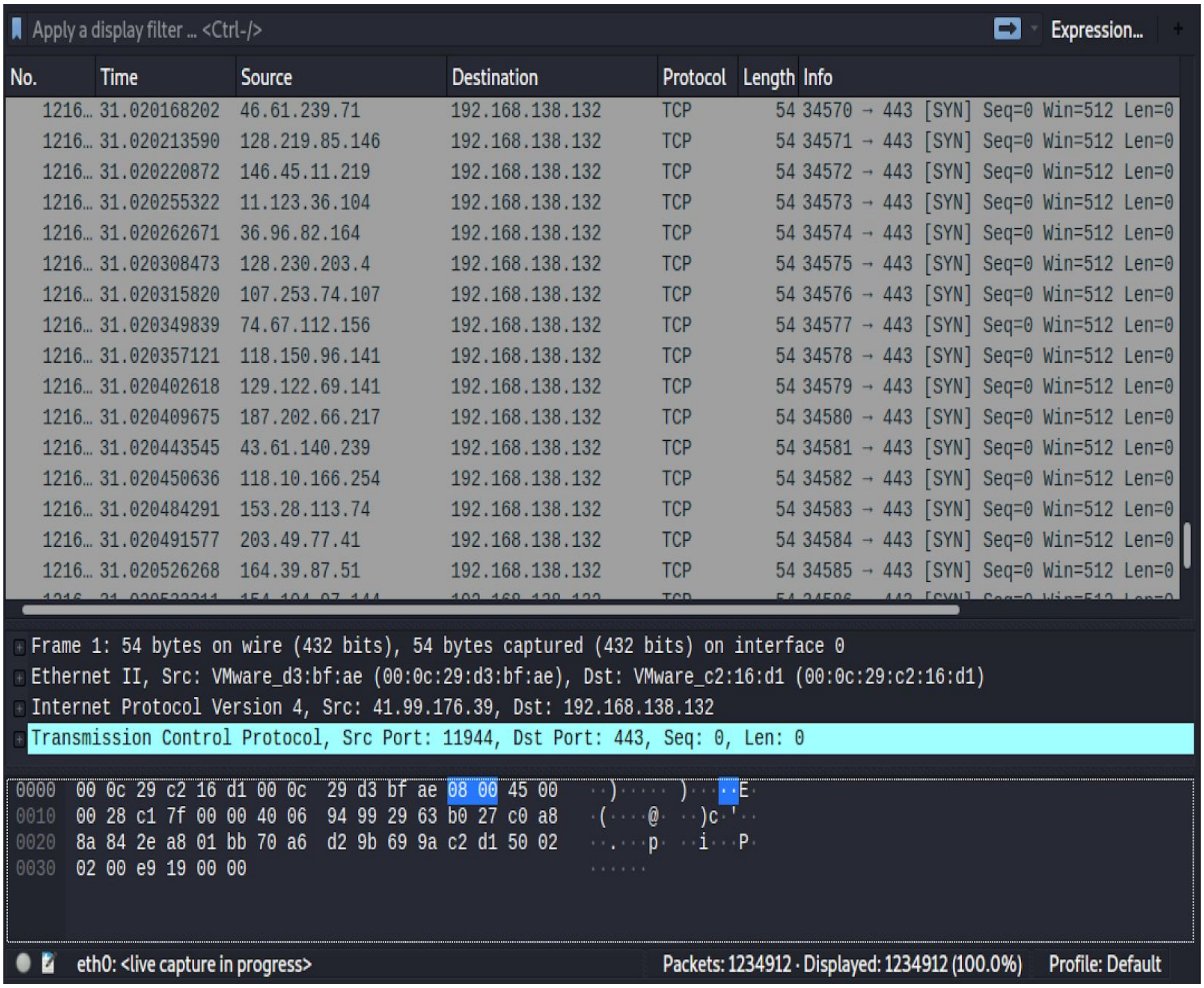


```
securityonion@securityonion:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:c2:16:d1
          inet addr:192.168.138.132  Bcast:192.168.138.255  Mask:255.255.255.0
          inet6 addr: fe80::d6e9:6d23:bf6a:2395/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:390 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41673 (41.6 KB)  TX bytes:37124 (37.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17299 (17.2 KB)  TX bytes:17299 (17.2 KB)

securityonion@securityonion:~$ ifconfig
```

Flood Screenshot showing number of packets 1234912:



```
8384… 104.965338595 79.180.216.57     192.168.138.132   TCP   54 41662 → 443 [SYN] Seq=0 Win=512 Len=0
8384… 104.965359142 81.13.171.13      192.168.138.132   TCP   60 41650 → 443 [RST] Seq=1 Win=32767 Len=0
8384… 104.965360107 192.168.138.132   142.69.144.125    TCP   60 443 → 41651 [SYN, ACK] Seq=0 Ack=1 Win=65535
8384… 104.965360562 192.168.138.132   50.2.16.130       TCP   60 443 → 41652 [SYN, ACK] Seq=0 Ack=1 Win=65535
8384… 104.965368289 182.208.175.255   192.168.138.132   TCP   54 41663 → 443 [SYN] Seq=0 Win=512 Len=0
8384… 104.965419699 142.69.144.125    192.168.138.132   TCP   60 41651 → 443 [RST] Seq=1 Win=32767 Len=0
8384… 104.965420701 241.27.219.215    192.168.138.132   TCP   54 41664 → 443 [SYN] Seq=0 Win=512 Len=0
8384… 104.965421316 50.2.16.130       192.168.138.132   TCP   60 41652 → 443 [RST] Seq=1 Win=32767 Len=0
8384… 104.965422225 192.168.138.132   195.142.109.218   TCP   60 443 → 41654 [SYN, ACK] Seq=0 Ack=1 Win=65535
8384… 104.965422990 192.168.138.132   57.210.227.113    TCP   60 443 → 41655 [SYN, ACK] Seq=0 Ack=1 Win=65535

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: VMware_c2:16:d1 (00:0c:29:c2:16:d1), Dst: VMware_e4:3e:3c (00:50:56:e4:3e:3c)
Internet Protocol Version 4, Src: 192.168.138.132, Dst: 136.22.130.20
Transmission Control Protocol, Src Port: 48520, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```



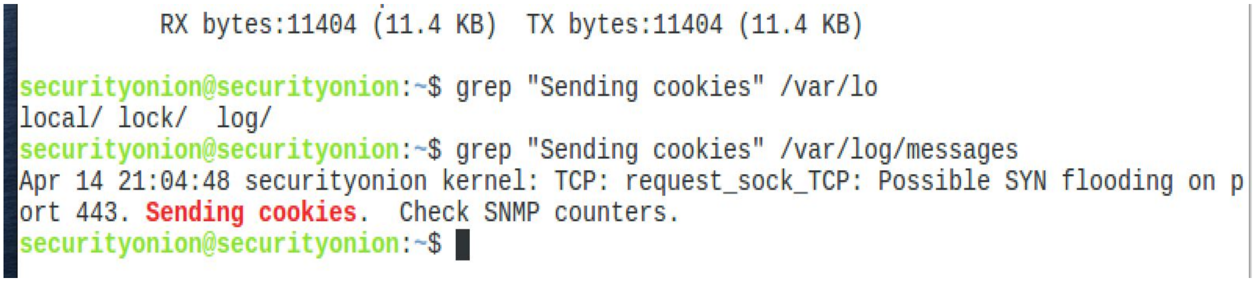
No.	Time	Source	Destination	Protocol	Length	Info
1216…	31.020168202	46.61.239.71	192.168.138.132	TCP	54	34570 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020213590	128.219.85.146	192.168.138.132	TCP	54	34571 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020220872	146.45.11.219	192.168.138.132	TCP	54	34572 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020255322	11.123.36.104	192.168.138.132	TCP	54	34573 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020262671	36.96.82.164	192.168.138.132	TCP	54	34574 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020308473	128.230.203.4	192.168.138.132	TCP	54	34575 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020315820	107.253.74.107	192.168.138.132	TCP	54	34576 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020349839	74.67.112.156	192.168.138.132	TCP	54	34577 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020357121	118.150.96.141	192.168.138.132	TCP	54	34578 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020402618	129.122.69.141	192.168.138.132	TCP	54	34579 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020409675	187.202.66.217	192.168.138.132	TCP	54	34580 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020443545	43.61.140.239	192.168.138.132	TCP	54	34581 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020450636	118.10.166.254	192.168.138.132	TCP	54	34582 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020484291	153.28.113.74	192.168.138.132	TCP	54	34583 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020491577	203.49.77.41	192.168.138.132	TCP	54	34584 → 443 [SYN] Seq=0 Win=512 Len=0
1216…	31.020526268	164.39.87.51	192.168.138.132	TCP	54	34585 → 443 [SYN] Seq=0 Win=512 Len=0

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: VMware_d3:bf:ae (00:0c:29:d3:bf:ae), Dst: VMware_c2:16:d1 (00:0c:29:c2:16:d1)
Internet Protocol Version 4, Src: 41.99.176.39, Dst: 192.168.138.132
Transmission Control Protocol, Src Port: 11944, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 0c 29 c2 16 d1 00 0c  29 d3 bf ae 08 00 45 00   ··)·····)·····E·
0010  00 28 c1 7f 00 00 40 06  94 99 29 63 b0 27 c0 a8   ·(····@·  ··)c·'··
0020  8a 84 2e a8 01 bb 70 a6  d2 9b 69 9a c2 d1 50 02   ··.···p·  ··i···P·
0030  02 00 e9 19 00 00                                  ······
```

eth0: <live capture in progress> Packets: 1234912 · Displayed: 1234912 (100.0%) Profile: Default

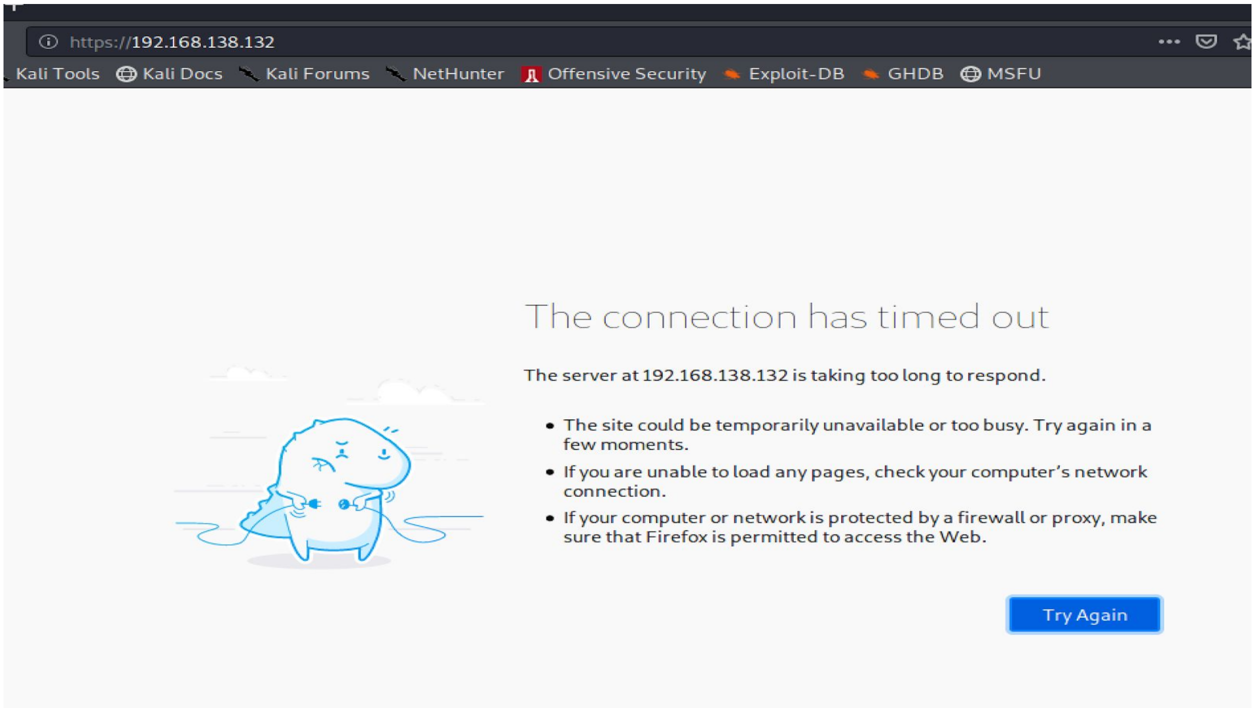
Screenshot for command *grep "Sending cookies" /var/log/messages*:



```
          RX bytes:11404 (11.4 KB)  TX bytes:11404 (11.4 KB)

securityonion@securityonion:~$ grep "Sending cookies" /var/lo
local/ lock/  log/
securityonion@securityonion:~$ grep "Sending cookies" /var/log/messages
Apr 14 21:04:48 securityonion kernel: TCP: request_sock_TCP: Possible SYN flooding on p
ort 443. Sending cookies.  Check SNMP counters.
securityonion@securityonion:~$ 
```

Screenshot when SYN cookies were disabled:

Kali VM trying to access Security Onion Apache Server:

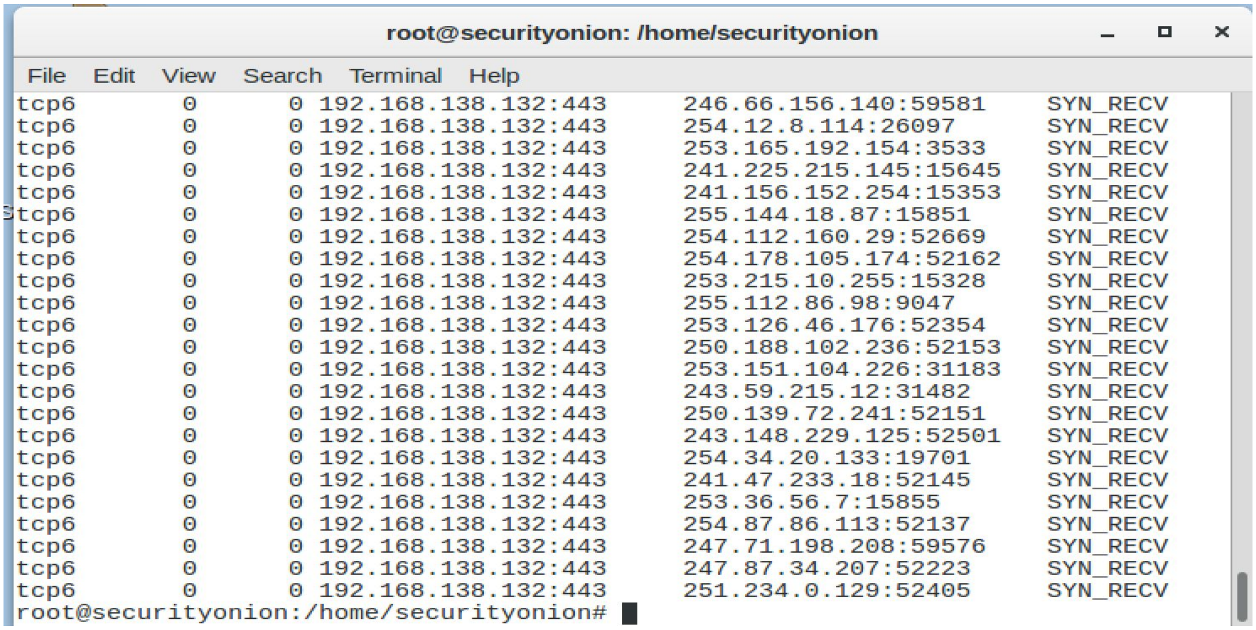


The connection has timed out

The server at 192.168.138.132 is taking too long to respond.

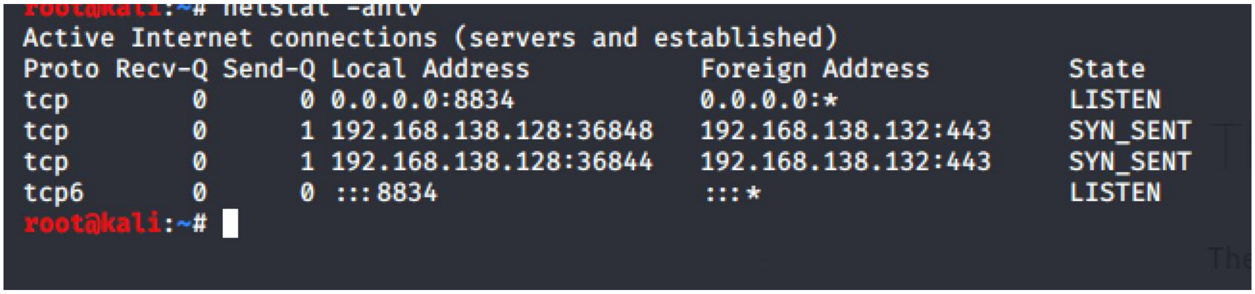
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Security Onion VM *netstat -antv* command output:



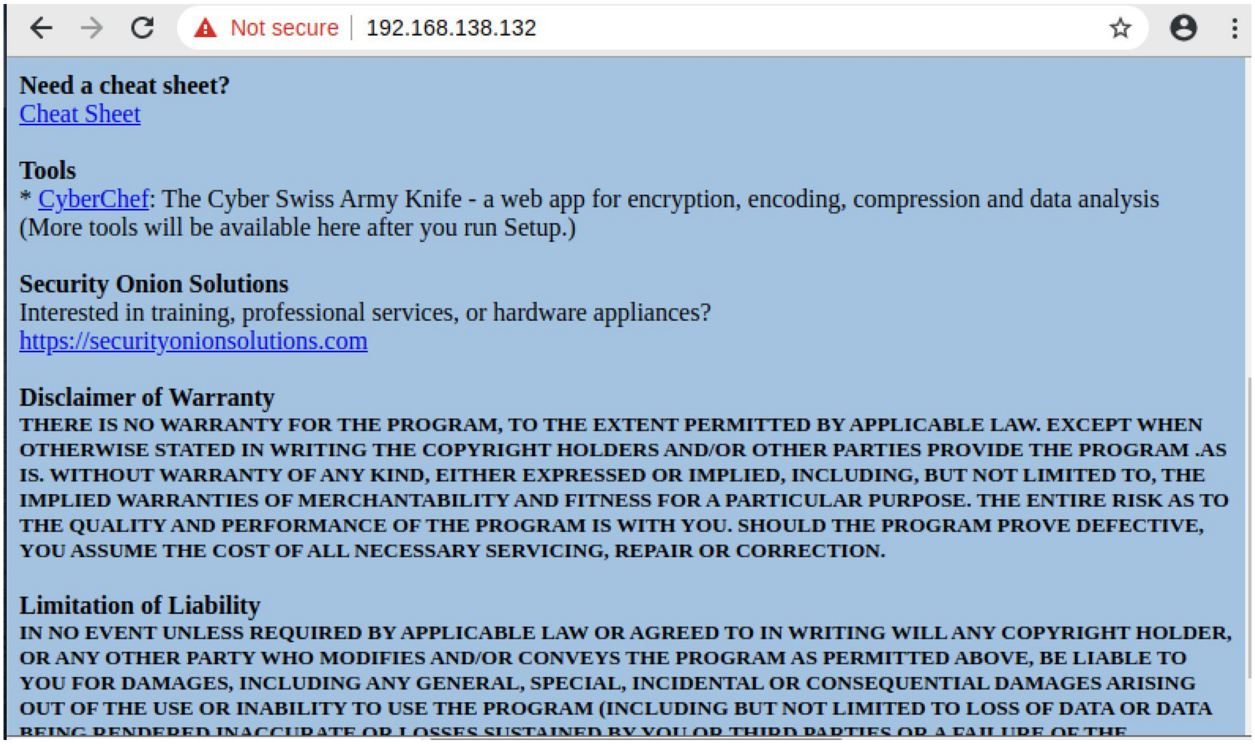
```
tcp6       0      0 192.168.138.132:443     246.66.156.140:59581    SYN_RECV
tcp6       0      0 192.168.138.132:443     254.12.8.114:26097      SYN_RECV
tcp6       0      0 192.168.138.132:443     253.165.192.154:3533    SYN_RECV
tcp6       0      0 192.168.138.132:443     241.225.215.145:15645   SYN_RECV
tcp6       0      0 192.168.138.132:443     241.156.152.254:15353   SYN_RECV
tcp6       0      0 192.168.138.132:443     255.144.18.87:15851     SYN_RECV
tcp6       0      0 192.168.138.132:443     254.112.160.29:52669    SYN_RECV
tcp6       0      0 192.168.138.132:443     254.178.105.174:52162   SYN_RECV
tcp6       0      0 192.168.138.132:443     253.215.10.255:15328    SYN_RECV
tcp6       0      0 192.168.138.132:443     255.112.86.98:9047      SYN_RECV
tcp6       0      0 192.168.138.132:443     253.126.46.176:52354    SYN_RECV
tcp6       0      0 192.168.138.132:443     250.188.102.236:52153   SYN_RECV
tcp6       0      0 192.168.138.132:443     253.151.104.226:31183   SYN_RECV
tcp6       0      0 192.168.138.132:443     243.59.215.12:31482     SYN_RECV
tcp6       0      0 192.168.138.132:443     250.139.72.241:52151    SYN_RECV
tcp6       0      0 192.168.138.132:443     243.148.229.125:52501   SYN_RECV
tcp6       0      0 192.168.138.132:443     254.34.20.133:19701     SYN_RECV
tcp6       0      0 192.168.138.132:443     241.47.233.18:52145     SYN_RECV
tcp6       0      0 192.168.138.132:443     253.36.56.7:15855       SYN_RECV
tcp6       0      0 192.168.138.132:443     254.87.86.113:52137     SYN_RECV
tcp6       0      0 192.168.138.132:443     247.71.198.208:59576    SYN_RECV
tcp6       0      0 192.168.138.132:443     247.87.34.207:52223     SYN_RECV
tcp6       0      0 192.168.138.132:443     251.234.0.129:52405     SYN_RECV
root@securityonion:/home/securityonion# 
```

Kali VM *netstat -antv* command output showing two connection requests stuck at SYN_SENT state:



```
root@kali:~# netstat -antv
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp        0      1 192.168.138.128:36848   192.168.138.132:443     SYN_SENT
tcp        0      1 192.168.138.128:36844   192.168.138.132:443     SYN_SENT
tcp6       0      0 :::8834                 :::*                    LISTEN
root@kali:~# 
```

Screenshot of Kali VM trying to access Security Onion after enabling SYN cookies (Server accessible):



Need a cheat sheet?
Cheat Sheet

Tools
* CyberChef: The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis
(More tools will be available here after you run Setup.)

Security Onion Solutions
Interested in training, professional services, or hardware appliances?
https://securityonionsolutions.com

Disclaimer of Warranty
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM .AS IS. WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Limitation of Liability
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE