Apache & GoAccess

Apache Log Analizi ve GoAccess Kullanımı

Web sunucuları, web sitelerine giden isteklere cevap döndürerek ziyaretçiye istediği dosyaların ve web sayfasının gönderilmesini sağlar. Köklü web sunucularından olan Apache, çok yerde karşınıza çıkacaktır. Bu yazıda, Apache'ye ait log kayıtlarını analiz edeceğiz. Siz de kendi sunucunuzu oluşturarak test edebilirsiniz.
Öncelikle DigitalOcean üzerinden aldığın sunucuma Apache kuruyorum.
apt-get install Apache2
Apache'nin error.log ve access.log isimli iki temel kaydı bulunmakta. Bu dosyalar /var/log/apache2 dizininde yer alır. Adından da anlaşılacağı üzere access.log, web sunucunuza gelen istekleri kaydeder. 200, 300, 400, 500 gibi dönen tüm istekleri sınıflandırır.

20X: Bu aralıktaki tüm log kayıtlarının sorunsuz olarak döndüğünü, var olan bir sayfaya ulaştığını söyleyebiliriz.
30X: Yönlendirme işlemleri ve hatalarının yer aldığını belirtir.

40X: Bulunamayan sayfalar, yetkisiz sayfaların yer aldığı kayıtlardır.

50X: Sunucudan kaynaklanan hatalardan döndürülen durum kodlarıdır.

Detaylı liste için: https://www.mediaclick.com.tr/blog/http-server-durum-hata-kodlari-ve-anlamlari

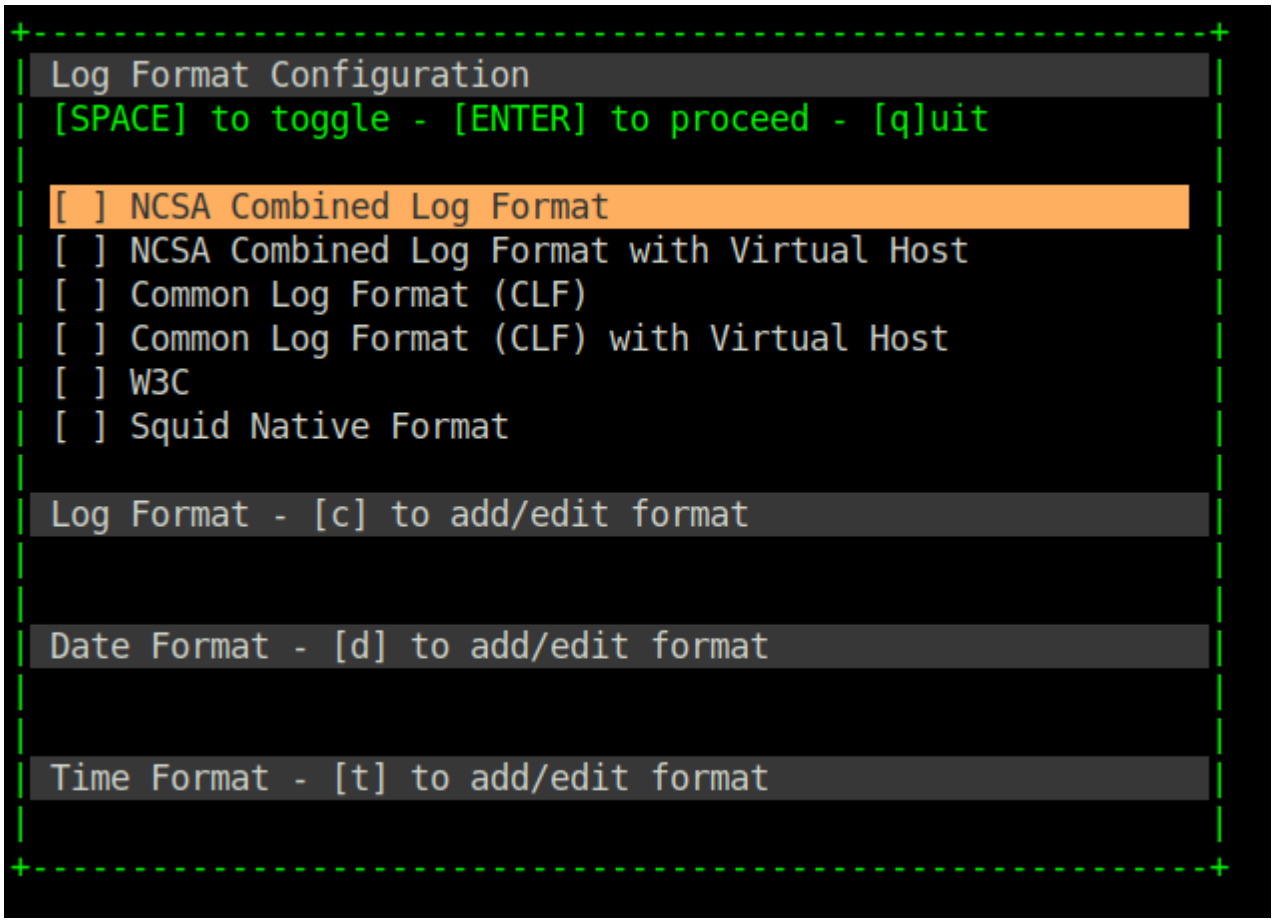
Bu loglarda farklı formatlarda istediğiniz verileri tutmanız mümkün. Örneğin dosya boyutunu kaldırabilirsiniz veya ilk sütunda yer alan IP adresi yerine zaman damgası yerleştirebilirsiniz. Aynı zamanda farklı standartlarda log tutarak başka araçlara bu kayıtları gönderebilirsiniz.

Örnek bir access.log: **192.168.0.77 – – [24/Dec/2019:12:19:16 +0000] "GET /caglar HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0"**
Yukarıdaki logta IP adresi, zaman damgası, HTTP isteğinin metodu, hangi URL'e yapıldığı, cevabın ne döndüğü ve tarayıcı bilgileri yer alır.

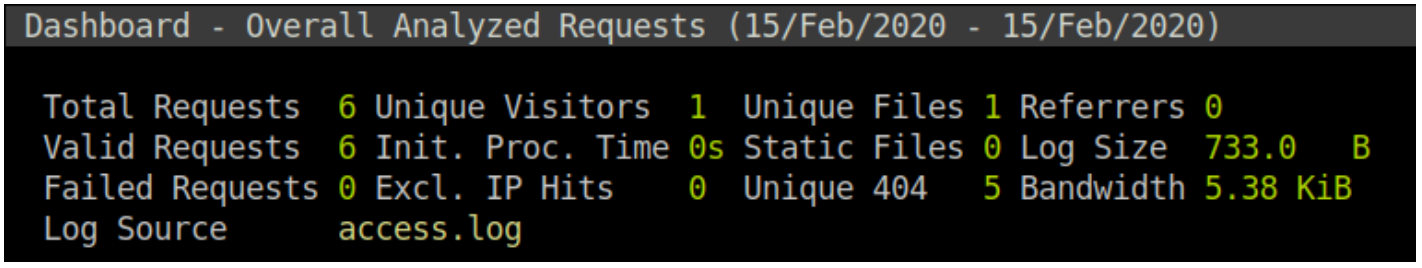
[Tue Dec 24 11:58:18.959786 2019] [core:notice] [pid 1505:tid 140073209799808] AH00094: Command line: ‘/usr/sbin/apache2’

Yukarıda ise error.log dosyasından örnek bir satır. Adres damgası, hatanın kaynağı ve önem derecesi, pid adresi ve hatanın önem derecesi yer alıyor.

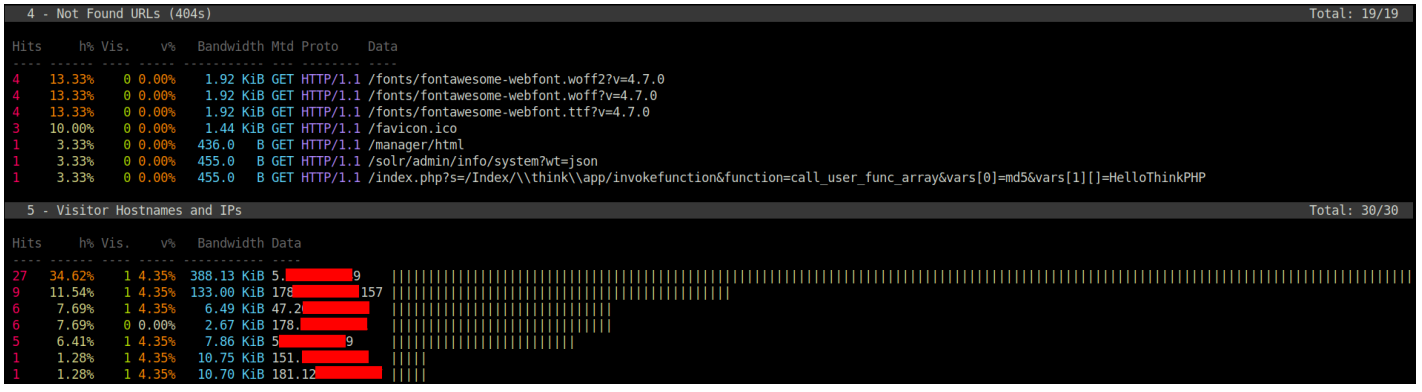
Bana kalırsa apache log kayıtları oldukça basit. Peki nasıl kullanabiliriz? En temelde web sitemize gelen atakları tespit edebiliriz, olağan dışı trafikleri gözlemleyebiliriz. Ben honeypot olarak kullanıyorum. Farklı sunuculara kurduğum inandırıcı sayfalara gelen isteklerin log kayıtlarını analiz ederek komuta kontrol merkezlerini, farklı payloadları ve IP adreslerini topluyorum. Kimisi saniyede beş kez **/wp-login veya /phpmyadmin** dizinlerine deneme yapıyor. Buradan o IP adresini brute force yaptığına dair not alıyorum. Kimisi girdi alanlarına standart XSS payloadları denerken kimisi de kendi geliştirdiği payloadları giriyor. Veya kimisi RFI açığını zorlayarak kendi komuta kontrol panelinden bir URL’e yönlendiriyor. Bu sayede bu panelleri de toparlayabiliyorum. Doğru filtrelemeler ile birçok çıkarımda bulunabiliriz.
GoAccess aracına geçelim. GoAccess, Apache log dosyalarının tamamını, güzel grafiklerle görmemizi sağlar. Terminalde veya web arayüzünde, gerçek zamanlı veya belirli bir zamana kadarki kayıtları tercih edebiliriz. Aynı zamanda Docker yapısını da destekliyor. Ben Apache logları için kullanıyorum fakat neredeyse bütün web servisleri için GoAccess kullanmak mümkün.
Öncelikle **apt-get install goaccess** ile Linux sistemimize indiriyoruz. Farklı sistemler için buradan faydalanabilirsiniz. Daha sonrasında log kayıtlarının bulunduğu dizine gitmemiz gerekiyor. Eğer daha önceden ayırdığınız bir log kaydı ile değil de o sistemdeki anlık kayıtları kullanacaksanız /var/log/apache2 dizinine geçmeniz gerekiyor. İlk komutumuzu çalıştıralım.
goaccess access.log -c
Bu komut ile access loglarının gerçek zamanlı çıktısını terminal üzerinden basit grafiklerle görüntüleyeceksiniz. Ancak öncelikle log formatını belirlemeniz gerekir. Varsayılan olan ve benim de kullandığım format en baştaki NCSA formatı. Mevcut standartların dışında özelleştirilmiş log formatlarını da klavyenizden c tuşuna basarak ilgili alana girebilirsiniz. Hazır standartlardan birini kullanacaksanız space ile seçip entera basıyoruz. Seçtiğimiz format aşağıdaki kutucuklara da yerleşiyor.

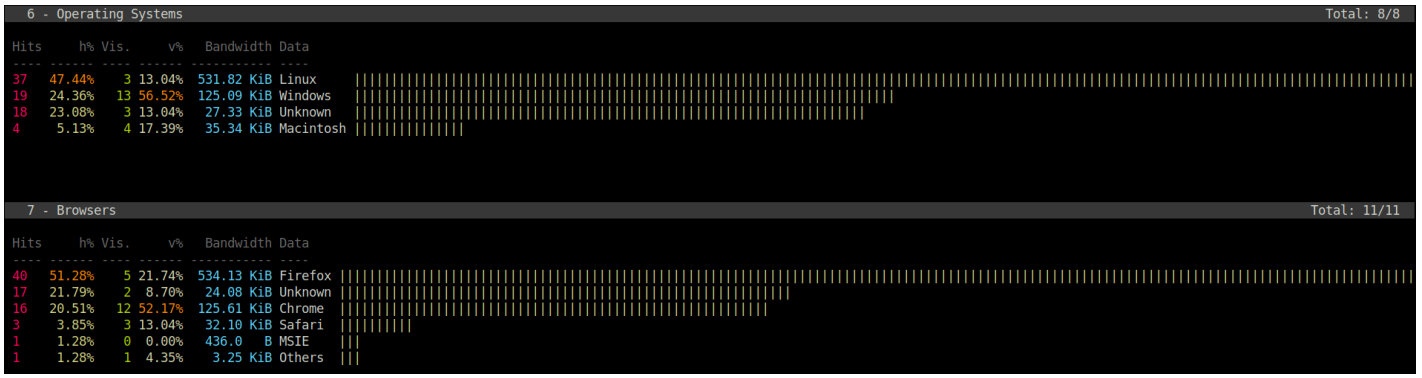


Daha sonrasında terminalde log kayıtlarına dair detaylar grafikleştiriliyor. En başta access loglarına dair genel istatistikler yer alıyor.



Birçok bilginin yanı sıra 404 denemeleri, en çok ziyaret eden IP adresleri, en çok kullanılan işletim sistemleri ve tarayıcılar listeleniyor. 404 kayıtlarının es geçilmemesi gerekir. Genelde başarısız da olsa saldırı kayıtlarının çoğu burada yer alır. Bu yazı için hazırladığım sunucuya dahi kısa zamanda saldırı denemeleri oldu.





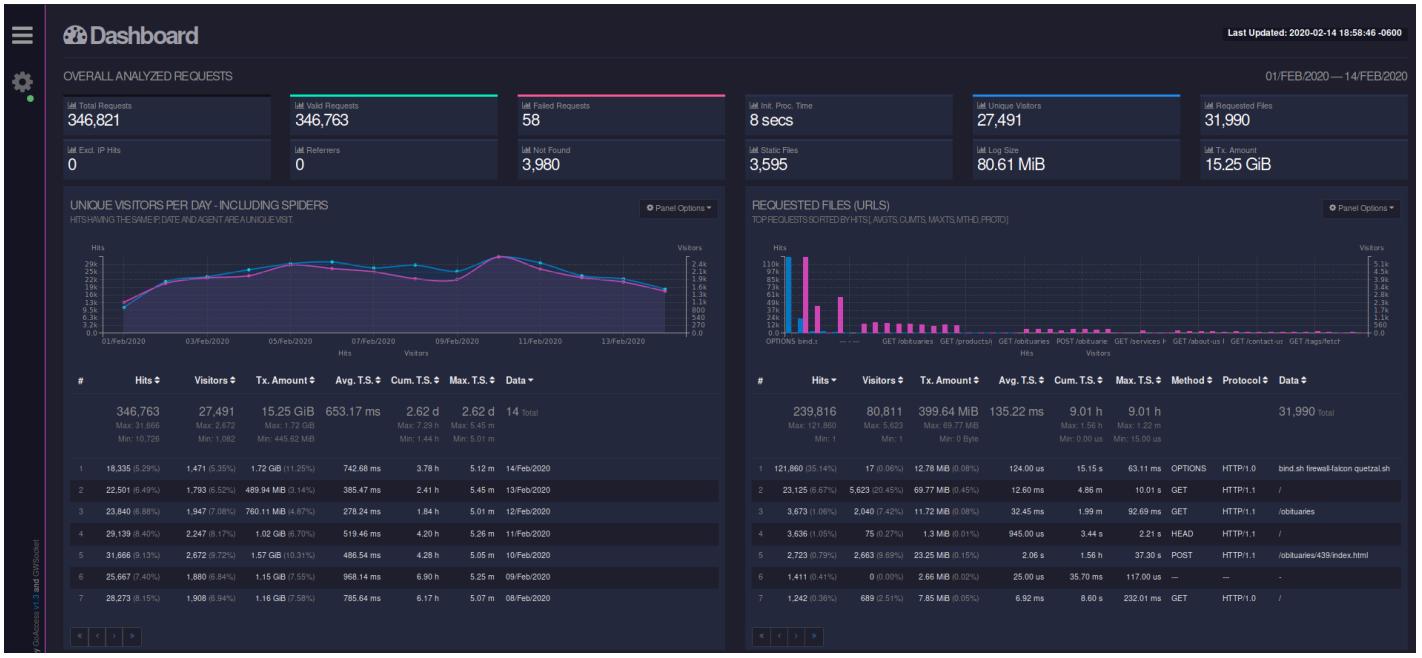
Daha kullanışlı bir arayüz sunan esas yöntem ise HTML output yöntemi.

goaccess access.log -o /var/www/html/report.html –log-format=COMBINED

Hala apache log dosyalarının yer aldığı dizinde bulunduğunuzu varsayıyorum. web sitemin yayın yaptığı dizine report.html adında log analiz raporu çıkartmak istiyorum. Arkasından verdiğim parametre ile log formatımı belirliyorum. Eğer belirtmezsem çıktı alamam. Bu komutla beraber o ana kadarki log kayıtlarını inceleyebilirim. Ancak ben log dosyası değiştiğinde de gerçek zamanlı olarak arayüzüme göndersin istiyorum. Bu durumda şu komutu kullanacağız:

goaccess access.log -o /var/www/html/report.html –log-format=COMBINED –real-time-html

–real-time-html parametresini ekledik. Bu durumda socket açılacak, terminalde CTRL+C yapmadıkça işlem yapamazsınız. Bundan sonraki arayüzümüzde log kaydının gerçek zamanlı birçok analizini görebiliriz. Bende yeteri kadar log birikmediği için GoAccess web sitesinde yer alan canlı demodan bir görüntü paylaşacağım.



Sol menüden tema değişikliği ve yer düzenlemesi yapabiliriz. Aynı zamanda JSON formatında çıktı alabiliriz.