Steve Micallef tarafından yazılan ve geliştirilen, keşif, tehdit istihbaratı, çevre izlemede hızlı sonuçlar veren Spiderfoot, OSINT araçları arasında ilk 10 da yerini alıyor. Pasif taramada onu bu kadar kullanılabilir ve vazgeçilmez kılan özellikleri ve kullanım alanlarını bu yazıda bulabilirsiniz.

SPIDERFOOT NEDİR ?

Spiderfoot, Genel adlar, alan adları, e-posta adresleri ve IP adresleri dahil olmak üzere çeşitli hedefler hakkında istihbarat toplamak için 100'den fazla genel veri kaynağından yararlanır ve kullanımı kolay modül seçimi ile hedef belirleyerek süreci basitleştirir.

İnternette farklı servisler, ağlar ve protokoller hakkında tonlarca veri mevcut olduğundan tüm bu bilgileri tek tek her yerden toplamak oldukça zaman alıcı bir görev haline geliyor.

İşte tam bu noktada SpiderFoot yardımınıza koşuyor. Hedefiniz hakkında her türlü bilgiyi tek bir araçta toplayarak OSINT toplama sürecini otomatikleştirmek için tam bir uzman!

OSINT'i otomatikleştirmek için Spiderfoot, 100'den fazla kamuya açık bilgi kaynağını sorgular ve alan adlarından, e-posta adreslerinden, isimlerden, IP adreslerinden, DNS sunucularından ve daha fazlasından gelen tüm istihbarat verilerini işler.

Kısaca özetleyecek olursak Spiderfoot için sadece hedef belirlemeniz yeterli, çalıştırılacak modülleri seçin ve Spiderfoot tüm işi sizin için yapsın, araştırdığınız her şeyin tam profilini oluşturmak için tüm verileri toplasın.

Neden SpiderFoot Kullanmalı ?

Spiderfoot gibi OSINT araçları, herhangi bir hedef hakkında bilgi ilişkilendirmek, olası veri sızıntılarını ortaya çıkarmak veya ağlarında veya uygulamalarında bulunan tüm güvenlik açıklarını keşfetmek için özellikle yararlıdır.

Bu bilgiler, bir penetrasyon testi yaparken, kendi ağınızı veya üçüncü tarafça yetkilendirilmiş bir ağı denetlerken faydalı olabilir.

Temel Özellikleri

Açık Kaynak	Bu güvenlik aracı Python'da yazılmış ve Github'da barındırılıyor. En iyi yanı, açık kaynaklı olması, yani herkesin onu daha iyi hale getirmek için katkıda bulunabilmesi.
Web Arayüzü	Spiderfoot varsayılan olarak bir CLI arayüzünden çalıştırılabilir, ancak kullanım kolaylığı, gösterişli simgeler ve zengin grafik görselleştirmeleri isteyenler için harika bir web arayüzünü de destekler.
Modül Desteği	Hedef ağa karşı hemen hemen her türlü testi çalıştırmaya yardımcı olabilecek 100'den fazla modülü içerir.SpiderFoot modülleri birbirleriyle etkileşime girecek şekilde programlandı ve bu sayede ilgili tüm modüllerin hedef hakkında aynı verileri paylaşmasına olanak sağlandı.
Döküman	Diğer OSINT araçlarının aksine, Spiderfoot yalnızca kod açısından iyi yazılmış olmakla kalmamış, aynı zamanda kurulum süreci, kullanım, modüller vb. dahil her şeyin nasıl çalıştığını keşfetmenize, okumanıza ve anlamanıza olanak tanıyan mükemmel bir dokümantasyon alanına sahiptir.
Çoklu Platform	Spiderfoot hem Linux hem de Windows işletim sistemlerinde çalıştırılabilir.
Spiderfoot HX	Standart sürüm her ortamda çalışsa da, Spiderfoot'u kendi barındırdığı

	bulut platformundan çalıştırmayı da seçebilirsiniz; bu platform, kendi barındırdığı sürümden daha gelişmiş özellikler içerir.

Spiderfoot Yükleme

Öncelikle: Spiderfoot'u çalıştırmak için aşağıdaki gerekli Python modüllerini yükleyin:

```
pip install lxml netaddr M2Crypto cherrypy mako requests bs4
```

Spiderfoot indirme sayfasından(GitHub - smicallef/spiderfoot: SpiderFoot automates OSINT for threat in...) bağlantıyı alın, ardından indirin ve çıkarın:

```
wget http://www.spiderfoot.net/files/spiderfoot-2.12.0-src.tar.gz
tar zxvf spiderfoot-2.12.0-src.tar.gz
cd spiderfoot-2.12
```

Spiderfoot'u başlatmak kolaydır, sadece şunu yazın:

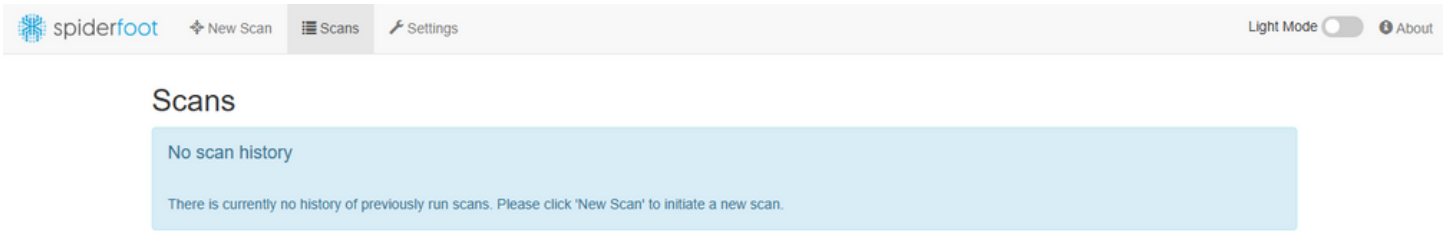
```
python ./sf.py
```

Aşağıda gördüğünüz gibi:

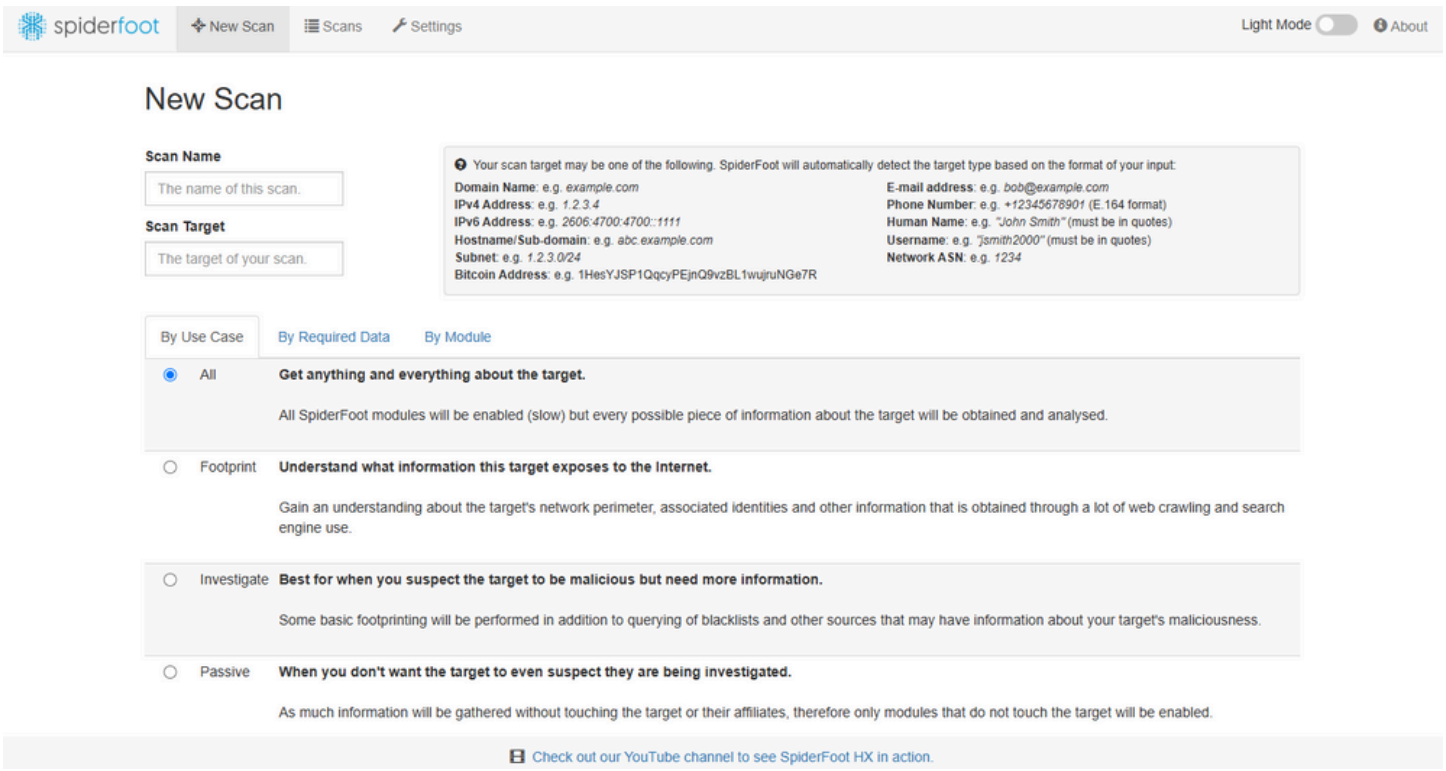
```
[root@localhost spiderfoot-2.12]# python ./sf.py
Starting web server at http://127.0.0.1:5001 ...

\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|
 Use SpiderFoot by starting your web browser of choice and
 browse to http://127.0.0.1:5001
\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|*\*|

[19/Apr/2018:10:58:53] ENGINE Listening for SIGHUP.
[19/Apr/2018:10:58:53] ENGINE Listening for SIGTERM.
[19/Apr/2018:10:58:53] ENGINE Listening for SIGUSR1.
[19/Apr/2018:10:58:53] ENGINE Bus STARTING
[19/Apr/2018:10:58:53] ENGINE Serving on http://127.0.0.1:5001
[19/Apr/2018:10:58:53] ENGINE Bus STARTED
```

Bu, http://127.0.0.1:5001/ adresinde çalışan bir web sunucusunu başlatacak ve buradan taramalarınızı başlatabilir ve GUI tabanlı bir ekrandan

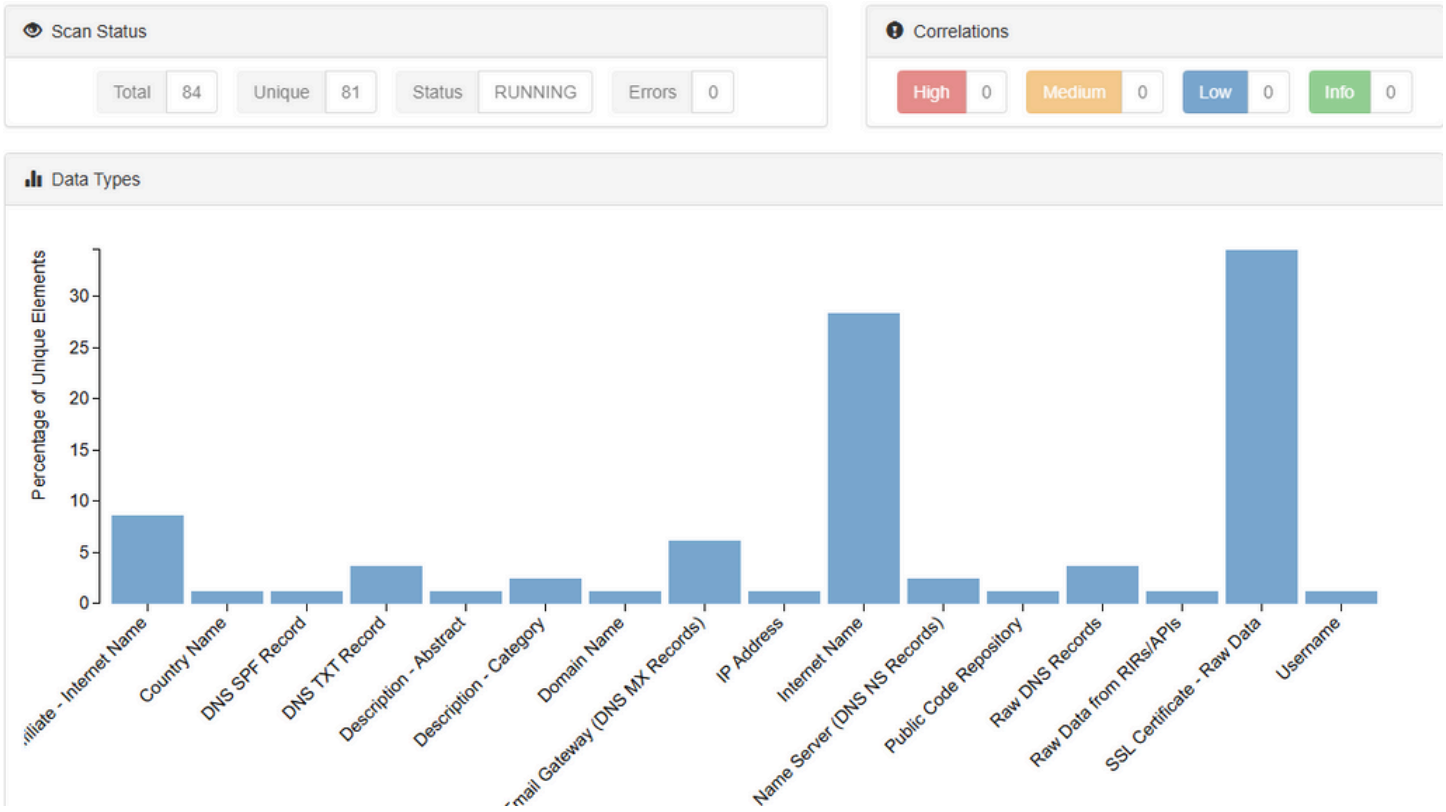
çalışabilirsiniz.



Bu arayüzden ilk taramanızı başlatabilir ve üç model seçebilirsiniz: kullanım durumuna göre, gerekli verilere göre veya modüle göre.



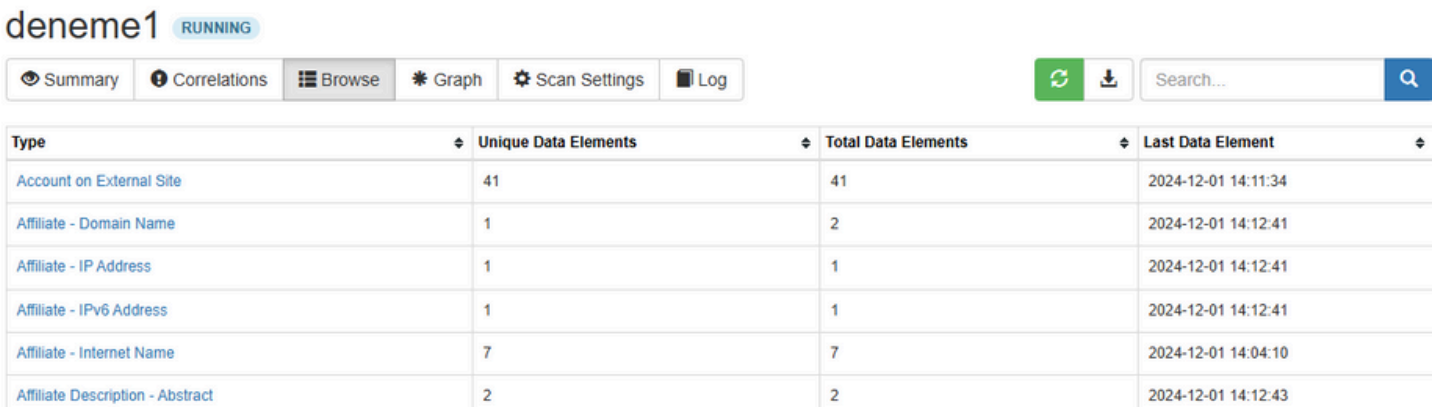
'Taramayı Çalıştır'a tıkladığınızda, tarama işlemlerinin gerçek zamanlı olarak görünmeye başlayacağı sonuç sayfasına yönlendirileceksiniz:



Bu ekran, Spiderfoot modüllerinden toplanan tüm verileri, her taramanın dahili günlük mesajlarıyla birlikte gösteren grafikleri ve tıklanabilir çubukları gösterecektir.

Time	Component	Type	Event
2024-12-01 14:07:24	sfp_s3bucket	STATUS	Spawning thread to check bucket: https://gelisimedutrstaging.s3-us-west-2.amazonaws.com
2024-12-01 14:07:24	sfp_s3bucket	STATUS	Spawning thread to check bucket: https://gelisimedutrprod.s3-us-west-2.amazonaws.com
2024-12-01 14:07:24	sfp_s3bucket	STATUS	Spawning thread to check bucket: https://gelisimedutrdata.s3-us-west-2.amazonaws.com

Tarama tamamlandıktan sonra, aşağıda gördüğünüz gibi, verileri görüntülemek ve analiz etmek için sonuçlara göz atmaya başlayabilirsiniz:



Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	41	41	2024-12-01 14:11:34
Affiliate - Domain Name	1	2	2024-12-01 14:12:41
Affiliate - IP Address	1	1	2024-12-01 14:12:41
Affiliate - IPv6 Address	1	1	2024-12-01 14:12:41
Affiliate - Internet Name	7	7	2024-12-01 14:04:10
Affiliate Description - Abstract	2	2	2024-12-01 14:12:43