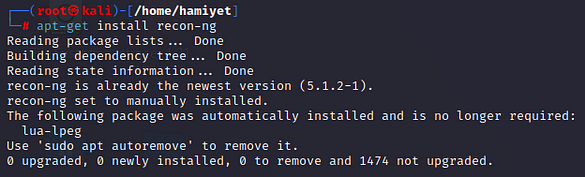
**Recon-ng Nedir? Ne İşe Yarar?**

Recon-ng web sitelerini kullanarak hedef site hakkında çeşitli istihbarat bilgisini bize sunabilen bir araçtır. Hedef sitenin kullandığı subdomains, ip adresleri, hedef sitenin açıklarının bulunduğu database’leri bulmamıza olanak sağlar ve içerisinde 100'den fazla modül barındırır ama modüller kurulu olarak gelmiyor. Tek satırlık kodla modüllerin hepsi kurulabilir. Tüm modülleri kurmak için (marketplace install all) komutu kullanılır. Recon-ng, hedef hakkında internet üzerinden bilgi toplamaya yarayan ve sonuçlarını raporlayan web tabanlı keşif aracıdır.

**Recon-ng Kurulumu**

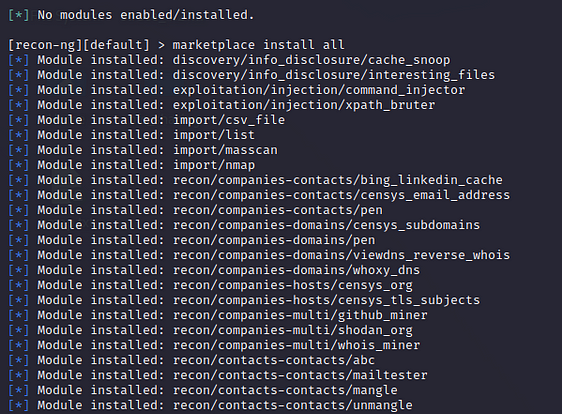
Recon-ng kurulumu için Kali’de terminale <apt-get install recon-ng> yazılmalıdır. Eğer kurulu ise alınacak çıktı şu şekildedir:



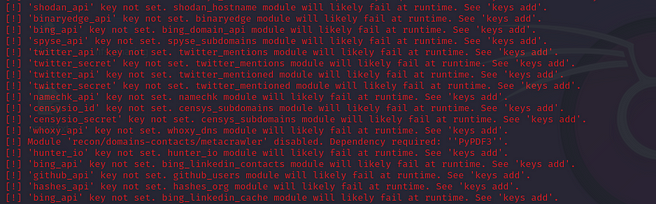
Aracın çalıştırılması için terminale <recon-ng> yazılmalıdır.



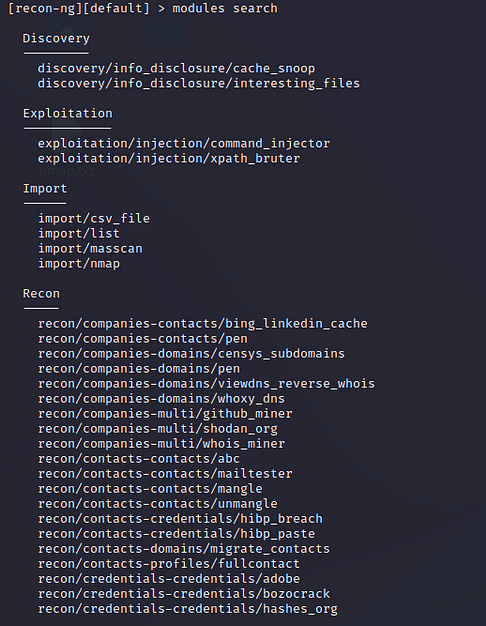
“Recon-ng’nin içerisinde 100'den fazla modül barındırır ama modüller kurulu olarak gelmiyor, tek satırlık kodla modüllerin hepsi kurulabilir: Tüm modülleri kurmak için <marketplace install all> komutu kullanılır.” demiştik.



Recon-ng deki modülleri kullanmak için API gerekiyor. Modüller kurulduktan sonra API bilgisi girilmeyen modüller açılışta kırmızı yazılı uyarı verir.



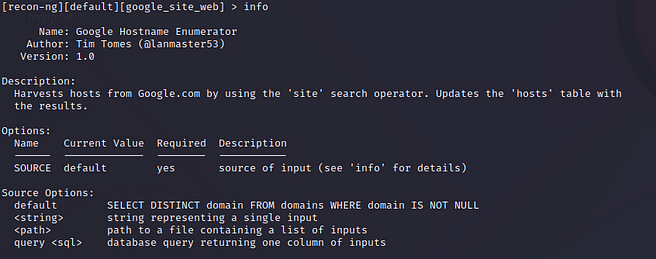
Terminale <module search> yazarak entegre edilmiş modüller görüntülenebilir.



Herhangi bir modülü seçmek için <modules load> parametresi kullanılarak modül eklenir.

https://miro.medium.com/v2/resize:fit:546/1*zFbvIMqrcDrmyUY4dVSpXw.png

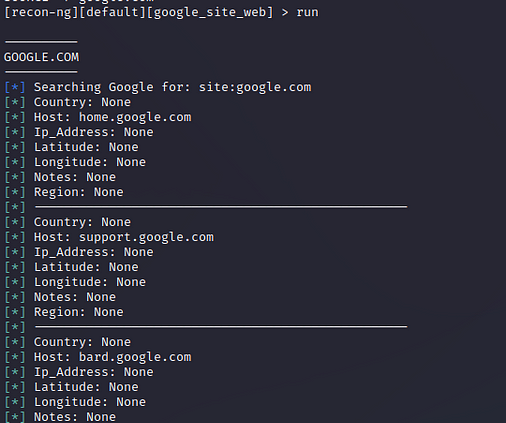
Modül hakkında detaylı bilgi almak için <info> komutu kullanılır.



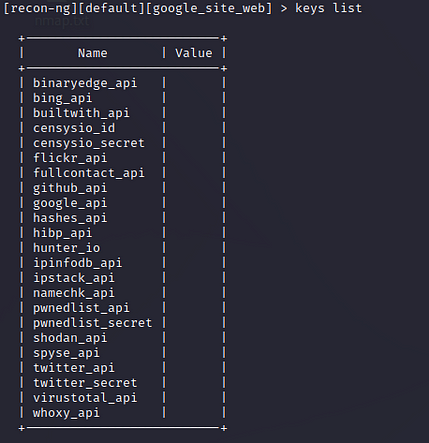
Modülün çalışması için eklenmesi gereken bilgiler “Options” bölümünde yer alır. Bilgileri modüle eklemek için <options set SOURCE> parametreleri kullanılır.

https://miro.medium.com/v2/resize:fit:533/1*cw7_GzrHM2FdaonpyKNK5A.png

Bilgiler modüle eklendikten sonra modülü çalıştırmak için <run> komutu kullanılır.



Hangi API’lere ihtiyaç olduğunu öğrenmek isterseniz <keys list> komutuyla tümünü listeleyebilirsiniz.

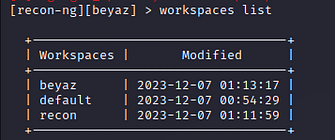


**Recon-ng Kullanım Örneği**

<workspaces create isim/site> komutuyla çalışma alanı oluşturalım.

https://miro.medium.com/v2/resize:fit:467/1*j4O8nwngbWfwYi6JTrvCXw.png

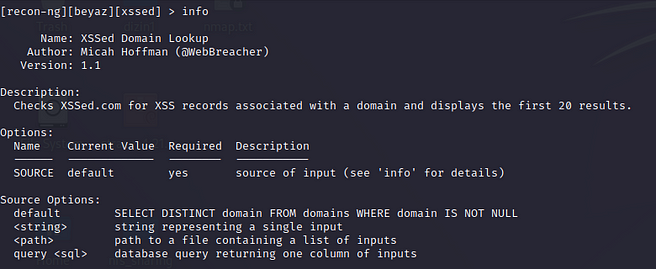
<workspaces list> komutuyla çalışma alanlarını listeleyip görüntüleyebiliriz.



<modules load recon/domains-vulnerabilities/xssed> komutuyla bir adet modül seçiyoruz.

https://miro.medium.com/v2/resize:fit:533/1*mbdkiwBNbhNuYN50XX_VoA.png

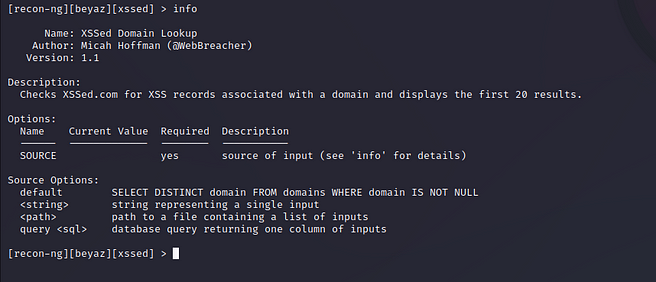
<info> komutuyla modülün içeriğini kontrol ediyoruz.



Burada “Current Value” kısmında “default” yazdığını görüyoruz. Hadi bunu değiştirelim. Konsola <options unset SOURCE> yazalım.

https://miro.medium.com/v2/resize:fit:441/1*gUc8oKDir9c0GcmqeJYuXQ.png

Tekrar <info> alalım.

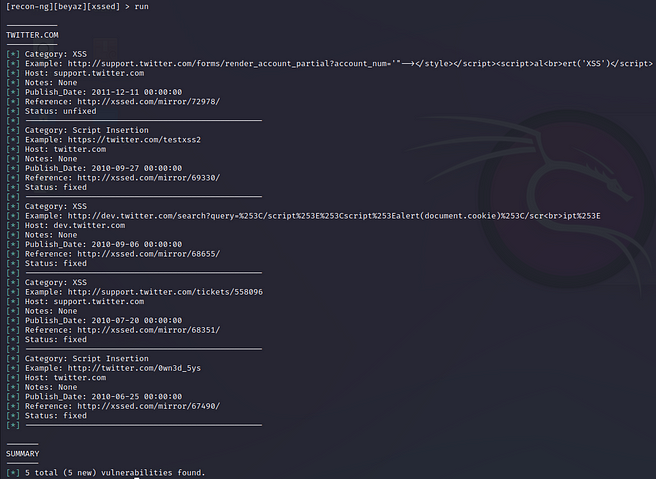


Görmüş olduğunuz gibi “Current Value” silindi ve şu an içi boş. İçerisine hedefimizi ekleyelim. (Lütfen yasal olarak veya eğitim amaçlı olarak kullanınız, illegal olarak bir suça karışmayın.)

Konsola <options set SOURCE hedef site.com> yazıyoruz (site.com=twitter.com).

https://miro.medium.com/v2/resize:fit:518/1*2lRXoXFpqcpk7JxziPUmbw.png

Artık buradan sonra yapmamız gereken <run> komutuyla modülü çalıştırmak ve beklemek. Şu anda kullandığımız modül hedef sitenin daha önce raporlanmış XSS açıklarını taramakta. Tarama sonucunda bize verdiği çıktılarda "fixed" veya "unfixed" yazmaktadır.



**Recon-ng Türevleri**

**OSINT-SPY**

IP adresi, etki alanı, e-posta adresi ve hatta Bitcoin adresi gibi farklı konularda bilgi sorgulamak için modüler bir araçtır. Bu araç, bir penetrasyon testinin keşif aşamasında değerli olabilir. Kuruluşunuz ve varlıkları hakkında hangi bilgilerin herkese açık olduğunu öğrenmek gibi savunma amacıyla da kullanılabilir.

**Wa**[**ppalyzer**](https://linuxsecurity.expert/tools/wappalyzer/)

Bir web uygulaması veya web sitesi gibi belirli bir hedef üzerinde keşif yaparken yararlı bir varlık olabilir. Belirli bir sayfayı çalıştırmak için hangi yazılımın kullanıldığını bulmaya yardımcı olur. Tespit edilebilen bileşenler, içerik yönetim sistemi (CMS), JavaScript çerçevesi, e-ticaret yazılımı, web sunucusu ve daha fazlasıdır.

**Infoga**

E-posta adresleriyle ilgili hangi bilgilerin sızdırıldığını öğrenmek için sızma testi sırasında kullanılabilir. Bir şirket için güvenlik izlemesi yapmak ve aynısını öğrenmek faydalı olabilir.

**Domain Analyzer**

Bir bilgi toplama aracıdır ve keşif için kullanışlıdır. Sızma testi yapmak veya kendi alan adlarınız hakkında hangi bilgilerin herkese açık olduğunu değerlendirmek için yararlı olabilir. Bulunabilecek bazı bilgiler arasında DNS sunucuları, IP adresleri, posta sunucuları, SPF bilgileri, açık bağlantı noktaları ve daha fazlası bulunur.