|  |
| --- |
| ***Reconnaissance*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Penetrasyon testinin ilk adımı olan keşif aşamasında kullanabileceğimiz araçlar hakkında bilgi vereceğim. |

**24.11.2021**

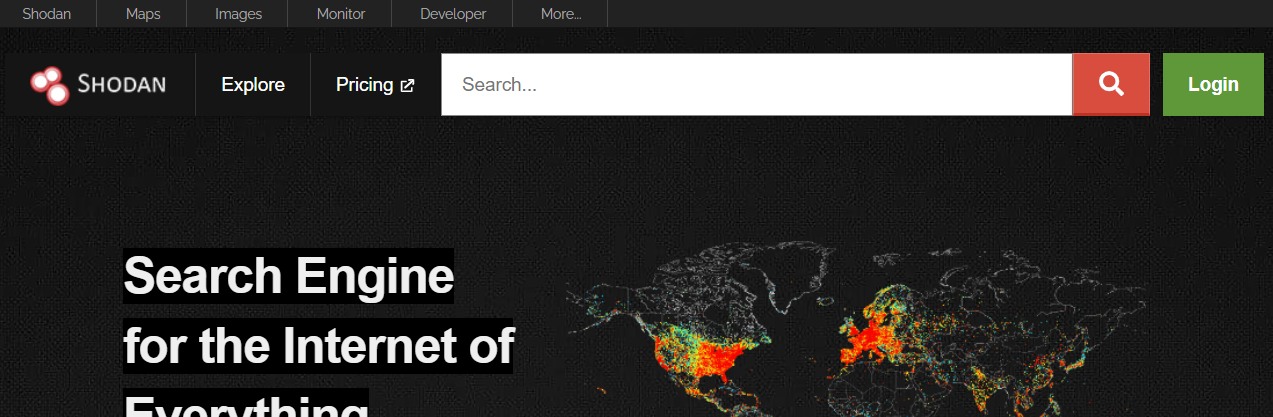
***Shodan***

-Shodan IoT cihazlarının arama motorudur.IoT internete erişebilen nesne diyebiliriz.

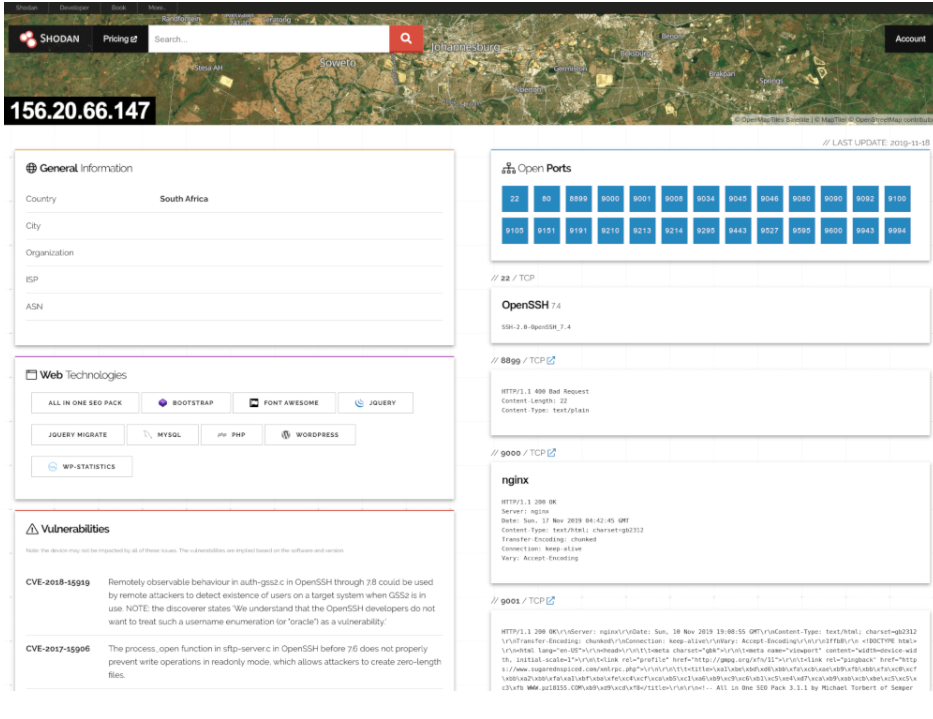
-Bulunduğu ağ da sorgulara atar ve gelen cevabı indexler.Bu cevaplar üzerinde açık port düşük servisler görüntülenebilir.

-Ücretli bir araçtır.

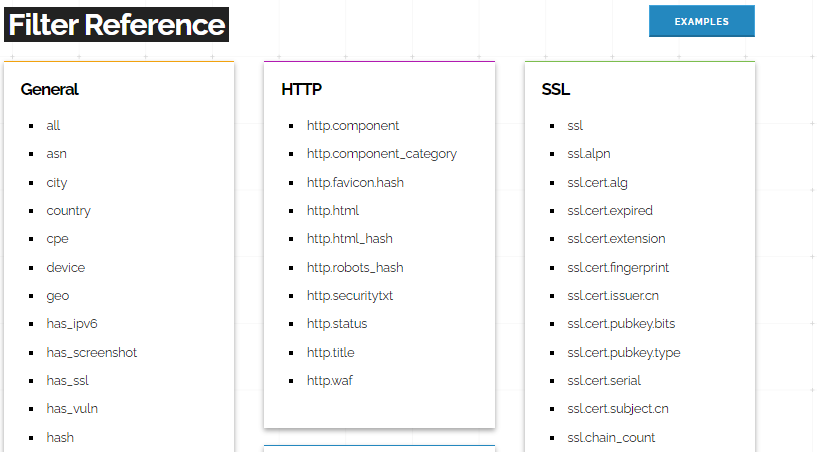
-Edu uzantılı bir mail üzerinden giriş yapılır ise ücretsiz olarak erişim sağlanabilir.



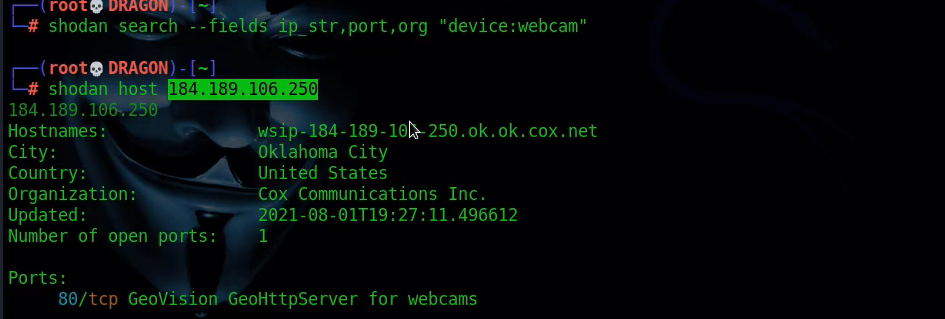
- "shodan.io" bağlantısı üzerinden web sayfasına erişim sağlayabiliriz.



- Örnek olarak verdiği bir aramada verdiği bilgileri görüntüleyebiliyoruz.



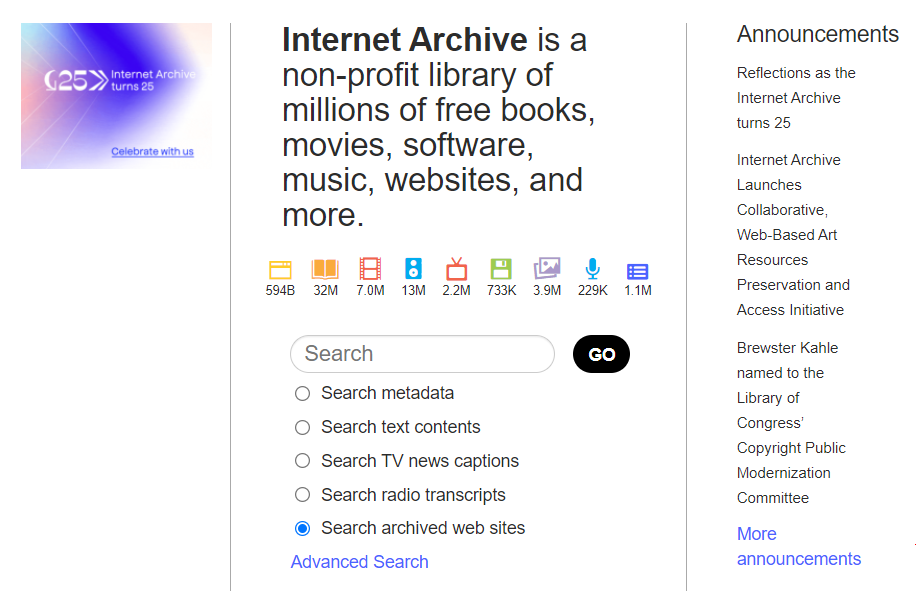
- "Shodan filters" araması ile elde ettiğim filtreler kullanılarak bilgi çekme işlemi gerçekleştirilebilir.



- Ayrıca Linux üzerinde giriş yapılmış bir Shodan hesabı var ise bu şekilde bilgi çekilebilir.

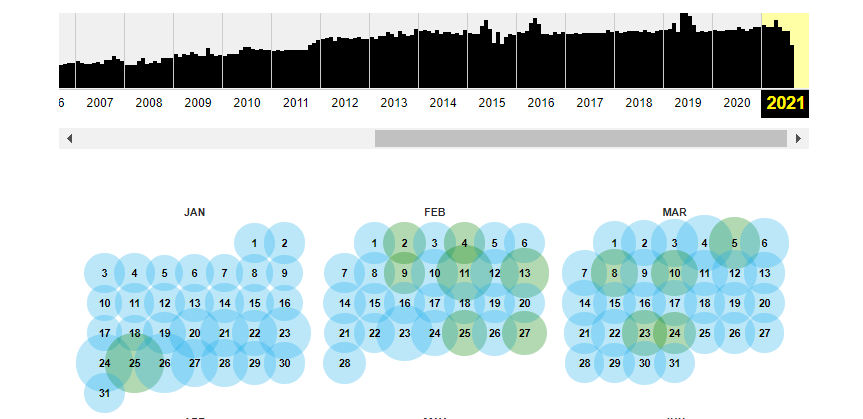
***Archive.org***

-Tarayıcımı açıyorum ve burada "Archive.org" sitesini görüntülüyorum.

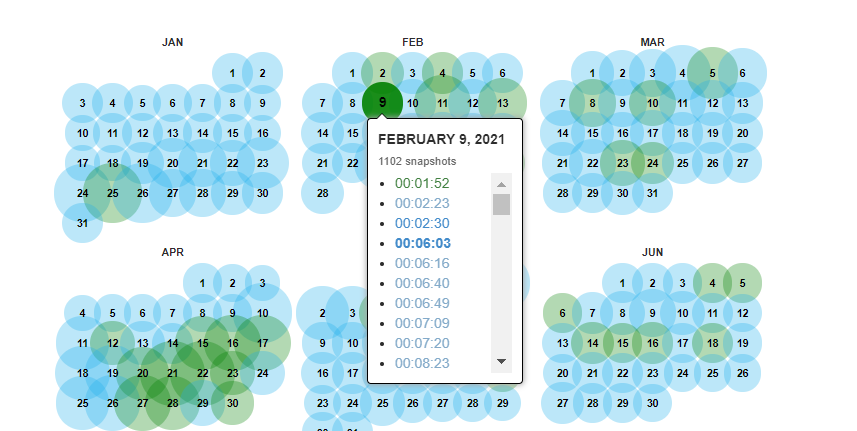


-Siteyi görüntülediğimde karşıma böyle bir ekran geliyor.Burada geçmişe dair saati ve saniyesine kadar değişimini görmek istediğim adresi yazıyorum.

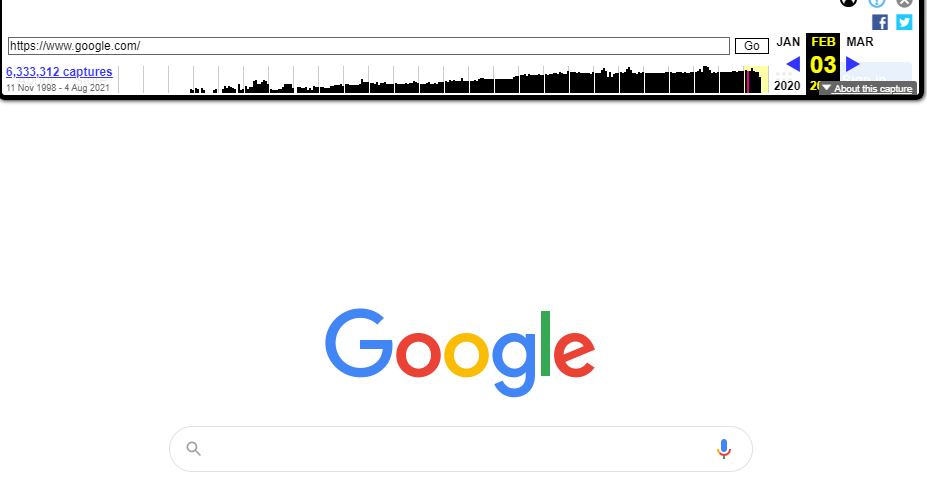
-Google sitesi üzerinden işlem gerçekleştiriyorum.



- Google sitesini görüntülediğimde bana “Google” sitesinin zamana bağlı olarak değişimini gösteriyor.



- Burada bir tarih ve saat seçiyorum ve tarayıcı üzerinden görüntülüyorum.



- Google sitesinin o tarihlerde kullandığı uygulamaları,arka planı veya sürümünü bu şekilde görsel olarak görüntüleyebiliyorum.

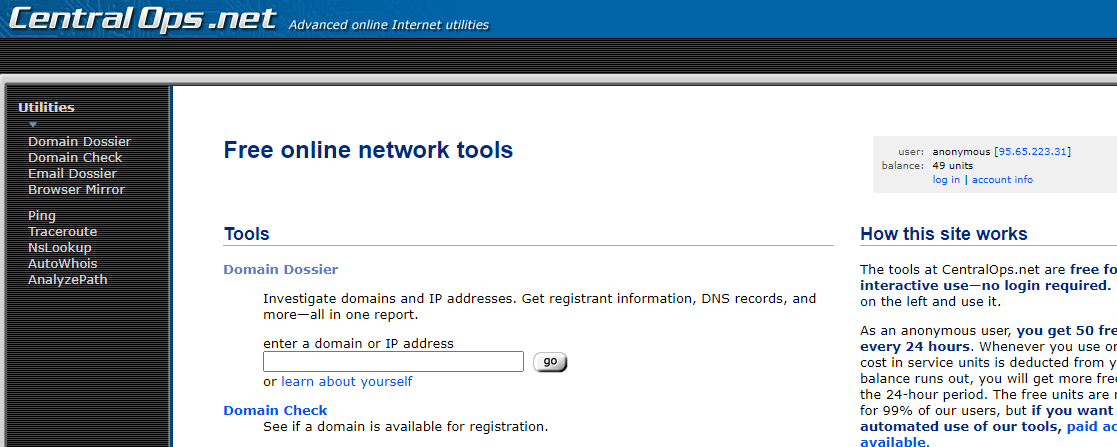
***Domain Enumeration***

-Listeleme,sıralama gibi anlamlara gelmektedir.

-Enum olarakta kısaltılabilir.

-DNS'e Whois sorgusu atılır ve onun üzerinden bilgi alınmaya çalışır.

-"https://centralops.net/co/" bağlantısı üzerinden işlem gerçekleştirilebilir.



-Site arayüzüne baktığımızda bu şekilde basit bir kullanımı vardır.

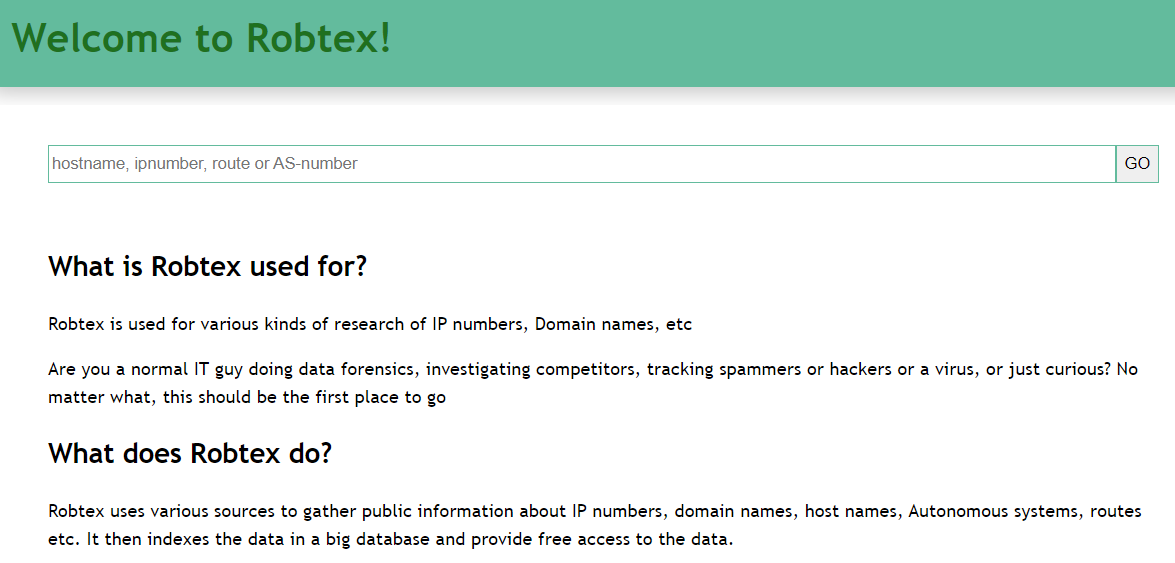


- "teknosa.com" bağlantısı üzerinden bir arama gerçekleştirdiğim de burada Domain'in kime ait olduğu ve domain süresinin biteceği tarih yer almaktadır.

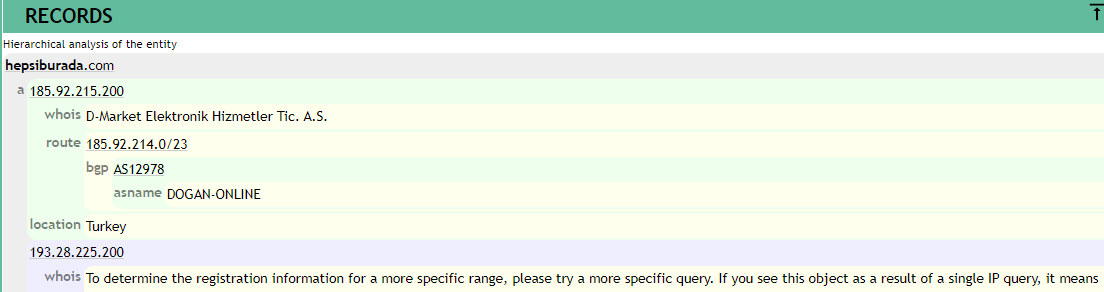
-Bu tarihi rapora eklemek bize bir artı puan kazandırır.

-Domain avcıları bu süreleri takip edip bu domain ismini alıp yüksek meblalara geri satmayı teklif eder.

***Robtex***



-Benzer işlemler "robtex.com" üzerinden de gerçekleştirilebilir.Arayüzü bu şekilde olan bir web sitesidir.



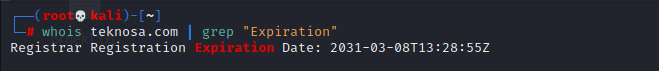
-"hepsiburada.com" üzerinden bir arama gerçekleştirdiğim de tarafıma getirdiği bilgileri görüntüleyelim.

-Arama gerçekleştirdiğim de bu ve benzeri bilgileri bana getirir.

- Bu işlemleri tarayıcı üzerinden gerçekleştirebileceğim gibi Linux üzerinde komut satırı üzerinden de gerçekleştirebilirim.



- "teknosa.com" üzerinden yapmış olduğum tarama ile elde ettiğim bilgileri görüntüleyebiliyorum.



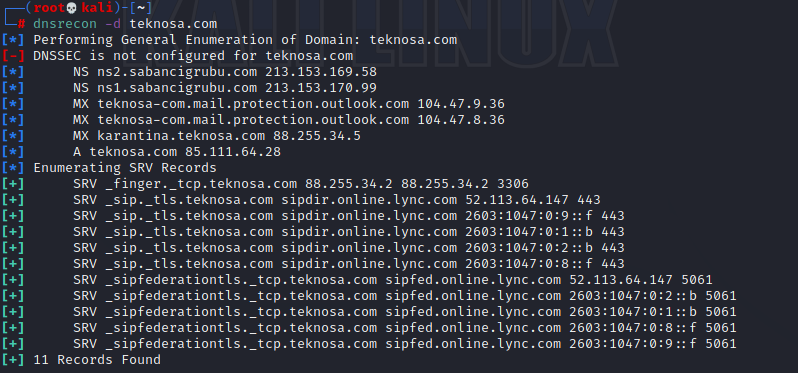
- Ayrıca bu sorgu üzerinde "grep" komutunu kullanarak bir filtreleme işlemi gerçekleştirebilirim.



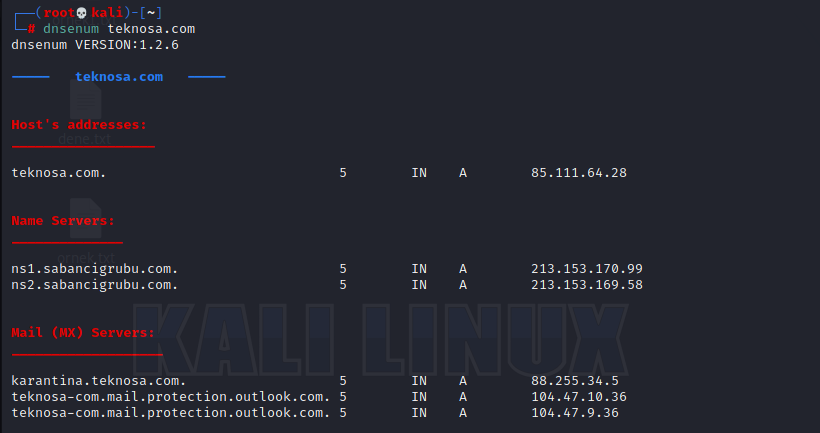
-Basit bir şekilde syn paketlerini kabul edip etmediğini de ping komutu ile takip edebilirim.



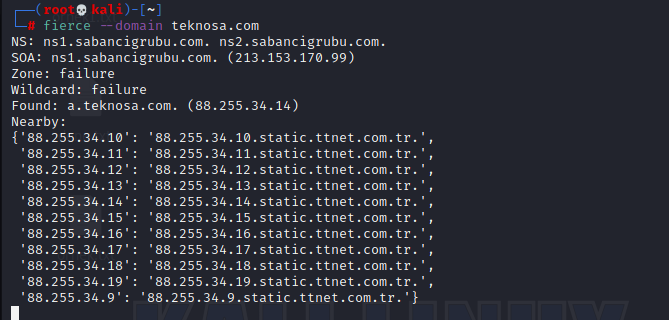
-"nslookup" ile domain hakkında basit bir şekilde bilgi sahibi olabilirim.



-"dnsrecon" aracı ile dns kayıtlarını da bu şekilde görüntüleyebilirim.



-"dnsenum" aracı ile de enumlar hakkında bu şekilde bilgi sahibi olabiliyoruz.Ayrıca burada basit bir Bruteforce işlemi gerçekleştirmektedir.



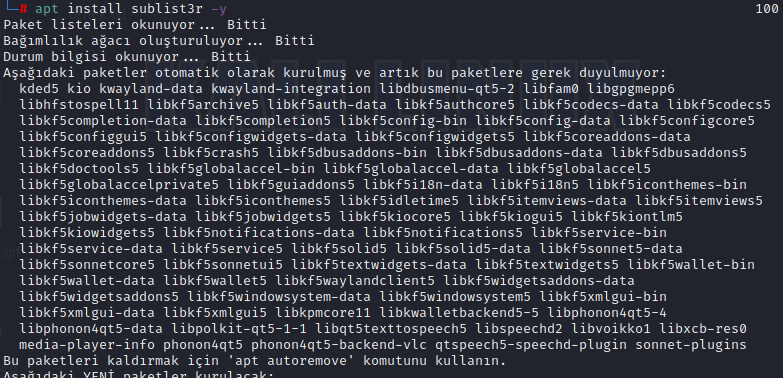
-Son olarak "fierce" aracı ile de subdomain tespiti gerçekleştirebiliriz.

---------------------------------------------------------------------------------------------------------------

***Subdomain Tespiti***

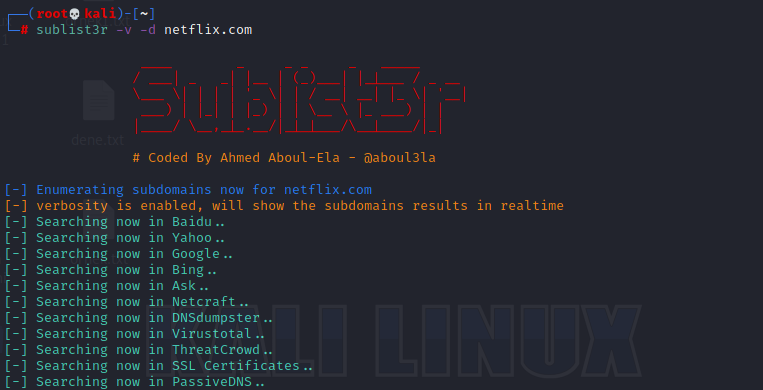
-Subdomainler domainlerin altlarıdır.

Domain = gmail.com Subdomain : mail.gmail.com örnek olarak verilebilir.



-Bu işlem için repolarda bulunan "sublist3r" aracı kullanılabilir.

-"apt install sublist3r" komutu ile kurulum gerçekleştiriyorum.

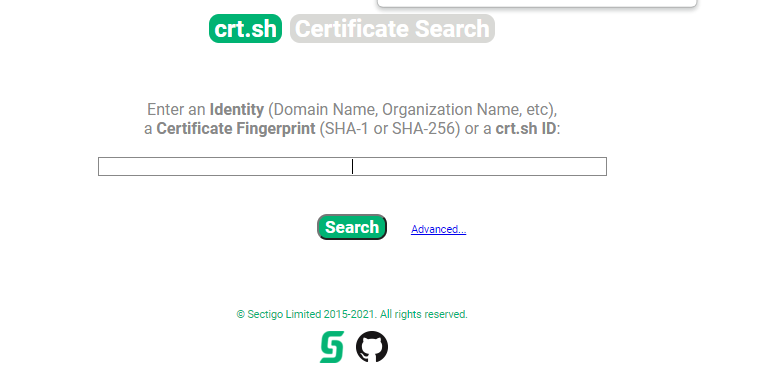


-Tarama gerçekleştirdiğim de subdomainleri hakkında bilgi sahibi olabilirim.Buradan nadir de olsa bir açık tespiti gerçekleşebilir.

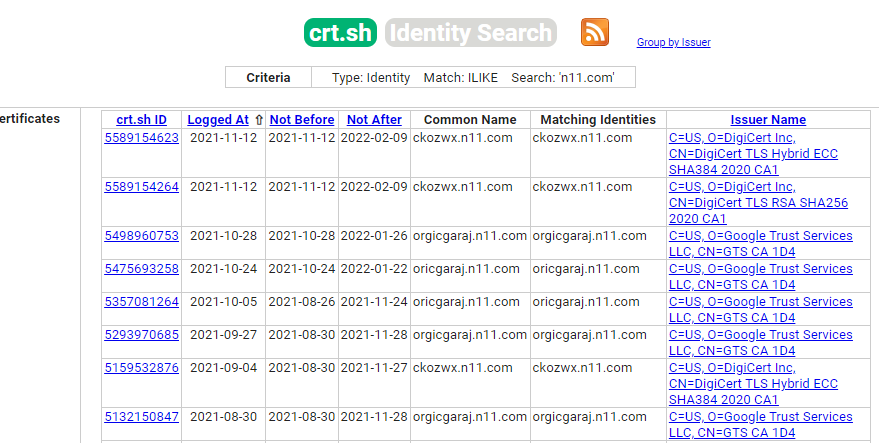


-Basit bir şekilde bulduğu sorguları gösterebilirim.

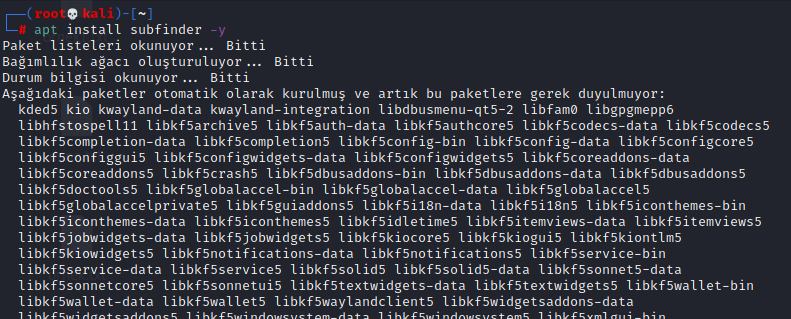
-Ayrıca yine tarayıcı üzerinden de bir subdomain taraması yapabiliriz.



-"crt.sh" bağlantısı üzerine geçiş yaptığımızda karşımıza böyle bir site arayüzü çıkmaktadır.



-"n11.com" link'i üzerinden bir tarama gerçekleştirdiğim de subdomainler hakkında bilgi sahibi yapmaktadır.



-Subdomainler için kullanılan başka bir araçta "subfinder"dır.

-Bu aracı "apt-get install subfinder" komutu ile yükleyebiliriz.



-Aracın "n11.com" sitesi üzerinden işlemini başlattığımda bana sonuçlarını bu şekilde döndürüyor.

-Ayrıca subdomain işlemi için "https://github.com/chris408/ct-exposer" bağlantısında bulunan araç kullanılır.

-İndirme işleminin ardından "pip install -r requirements.txt" ile gerekli kurulumlar gerçekleştirilir.Ardından araç çalıştırılabilir.

***Dns-Zone Transfer Kontrolü***

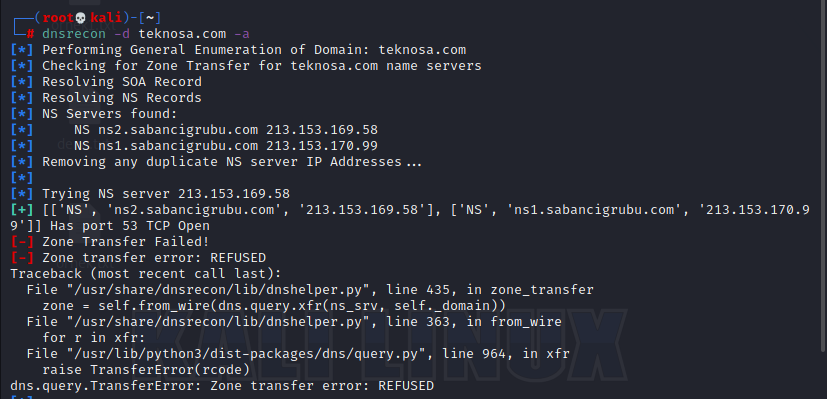
-DNS sunucular birbirini replike edebilirler.

-İçlerinde ki veritabanlarını birbirine aktarım yapabilir.

-Primary ve Secondary Dns server oluşur.

-Aralarında ki senkronizasyonuna da DNS Zone adı verilir.

-Aralarından bir tanesini Yetkisiz olarak DNS Zone'a erişim verir ise tüm veritabanı sızabilir.



Bu işlem için "dnsrecon" aracı kullanılmaktadır.

-Kullanım yöntemi ve çıktı şekli bu şekildedir.

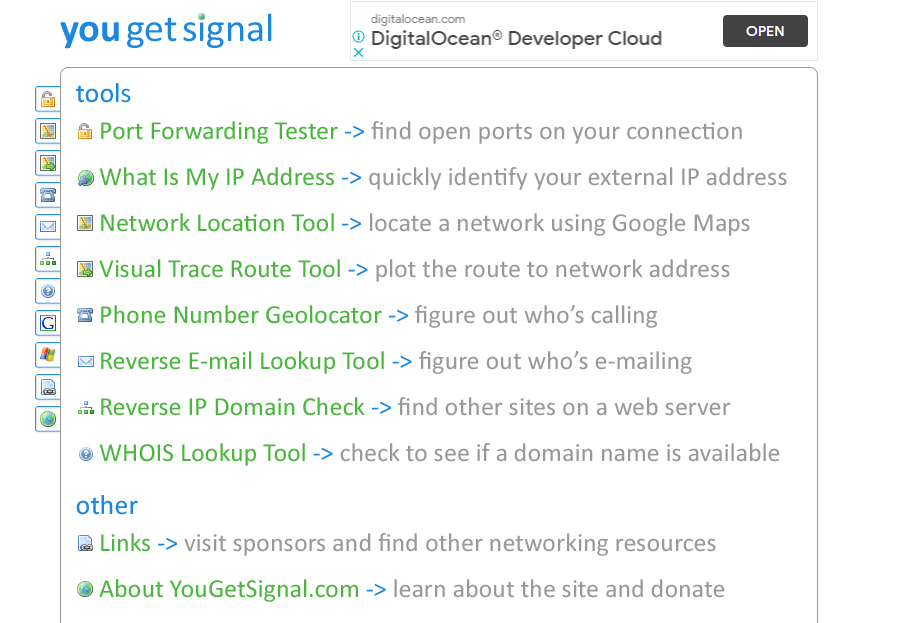
***Reverse IP Lookup***

-Türkçesi tersine bakıştır.

-IP'lerin isim karşılığını bulmaya çalışacaz.

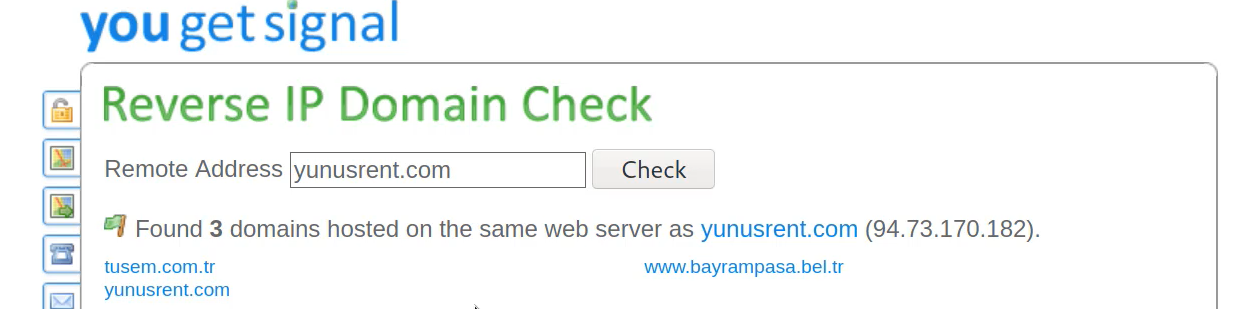
-Hosting sayfalarında server bir tanedir fakat bütün sunuculara dağıtılır eğer burada bir açık bulabilirsek tüm sistemlere sızmış oluruz.

Bu işlem için tarayıcı üzerinden işlem gerçekleştirilir.

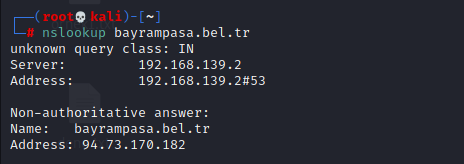


-"https://www.yougetsignal.com/" bağlantısı üzerinden yapmak istediğimiz işlemi seçebiliriz.

-Reverse IP Domain Check ile devam ediyorum.



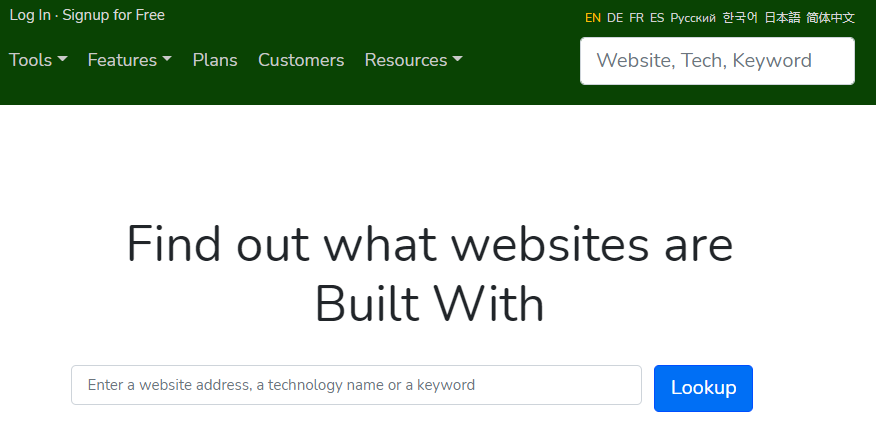
-Basit bir site buluyorum ve bunun üzerinden bir arama gerçekleştiriyorum.Burada bir belediyenin de aynı server'ı kullandığını görüntülüyorum.



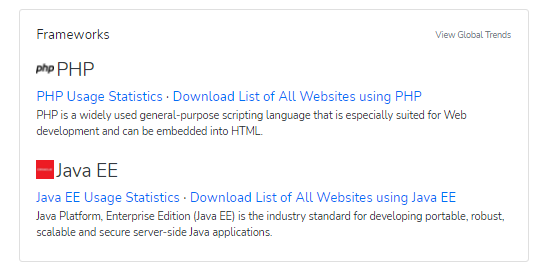
-Bu işlemi “nslookup” üzerinde teyit ettiğimde de aynı IP adreslerini kullandığını görüntülüyorum.

Web sitesinde kullanılan Servis tespiti

-Bu işlem için de tarayıcı üzerinde bulunan "https://builtwith.com/" bağlantısından yararlanacağız.



-Sayfayı görüntülediğimiz de bu şekilde bir ekran bizi karşılamaktadır.



-Tarayıcı üzerinden bulduğum basit bir siteyi taradığım da bana kullanılan teknolojiler hakkında bilgi vermektedir.

-Geri döndürdüğü tüm ayrıntıları size aktarmam mümkün olmadığı için bir kesitini göstermek istiyorum.

-Aynı işlemi "https://webtechsurvey.com/" bağlantısı üzerinden de gerçekleştirebiliriz.

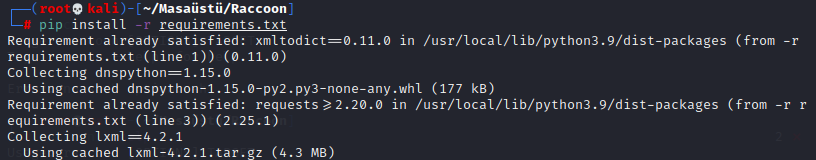
***Raccoon***

-Bu araçlar tümleşik tespitler yapabilmektedir.

C:\Users\ogutk\AppData\Local\Microsoft\Windows\INetCache\Content.Word\1.png

-Öncelikle raccoon adlı aracımızı indirelim.

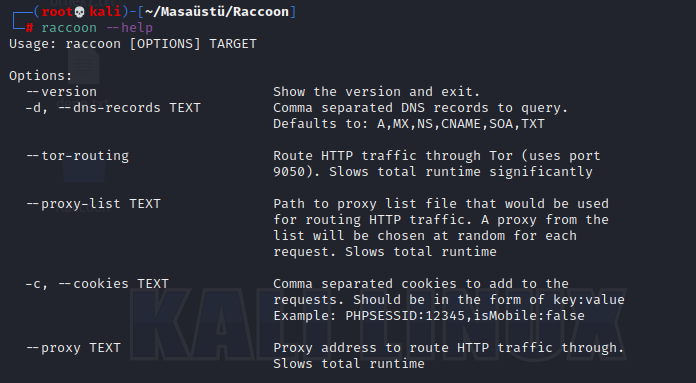
-"git clone https://github.com/evyatarmeged/Raccoon" komutu ile gerekli dosyaları indiriyorum.



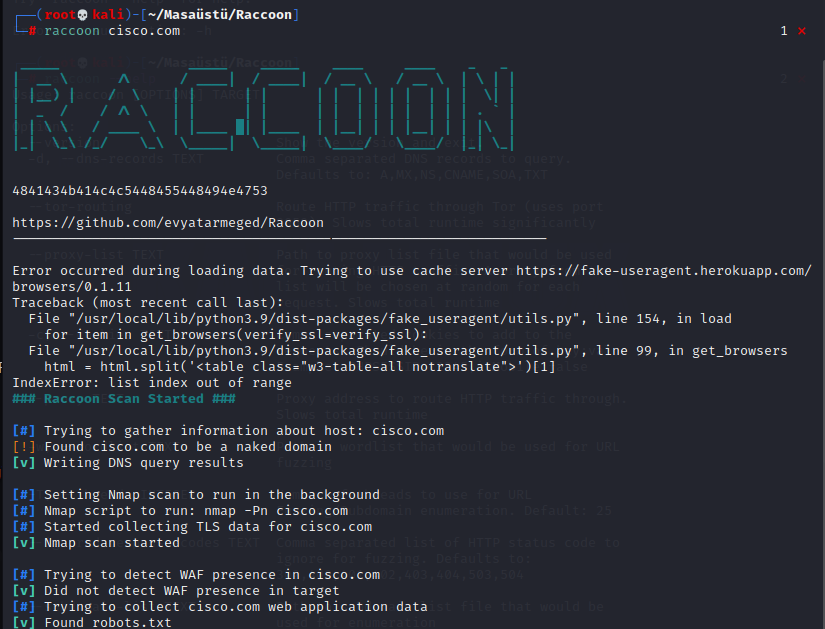
-İndirdiğim dosya içerisine geçiş yaıyorum ve burada ("pip -r requirements.txt" komutunu çalıştırıyorum.

-Gerekli kütüphaneleri kurduktan sonra aracı çalıştırıyorum.

-Daha sonrasında "python setup.py install" kodunu çalıştırıp gerekli kurulumları yapıyorum.



-Aracı "--help" komutları ile çalıştırıyorum ve çalışma düzeni hakkında bilgi sahibi oluyorum.



-Raccoon aracını cisco.com üzerinde tarıyorum ve burada robots.txt dosyasından “nmap” “taramasına kadar tarama yaptığını görüntülüyorum.

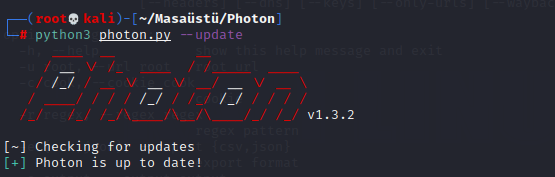
-Bu tarama çok kapsamlı bir taramadır.

***Photon***

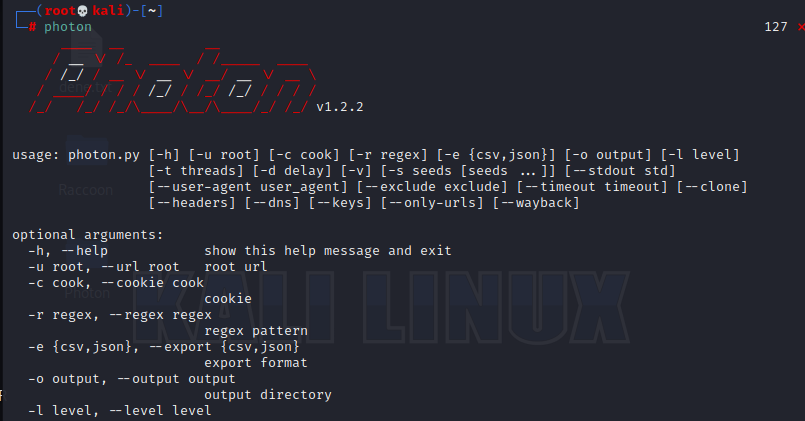


-Diğer arama gerçekleştireceğimiz araç photon aracıdır.Bu aracı da github üzerinden indirebiliriz

-"git clone https://github.com/s0md3v/Photon" komutu ile indirme gerçekleştiriyorum.



-Kurulum öncesi bir update işlemi gerçekleştiriyorum ve ardından kurulum gerçekleştiriyorum.



-Kurulum sonrasında aracı çalıştırdığım da yine çok genel bir işlem gerçekleştirdiğini ve buradan bilgi edinebileceğimi görüntülüyorum.



-Ardından cisco.com üzerine bir tarama gerçekleştiriyorum.

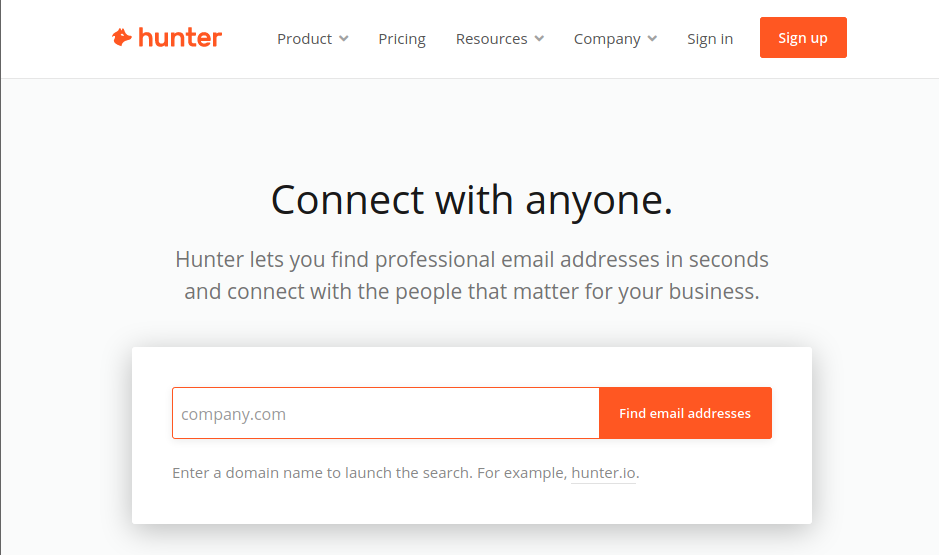
-Bu işlemler sırasında Google Dorking'e kadar bakmaktadır.

-Bunlarla ilgili uygulamaları diğer adımlarda gerçekleştireceğiz.

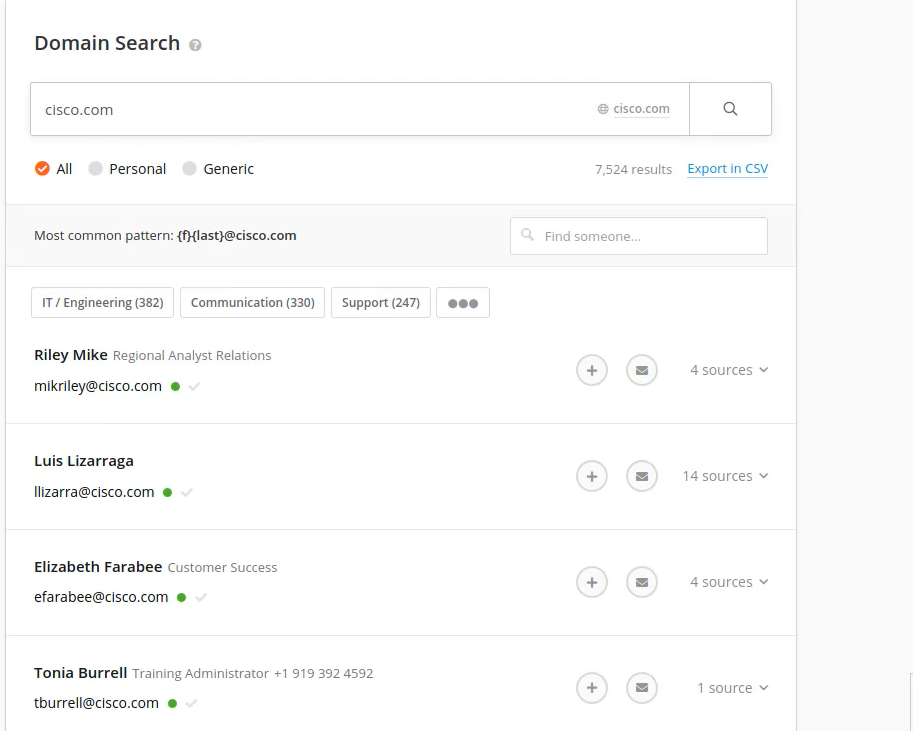
***OSINT Kavramı ve Personel(Mail) Tespiti***

-Açık kaynak kodlardan yararlanmamız durumunda OSINT yapmış oluruz.

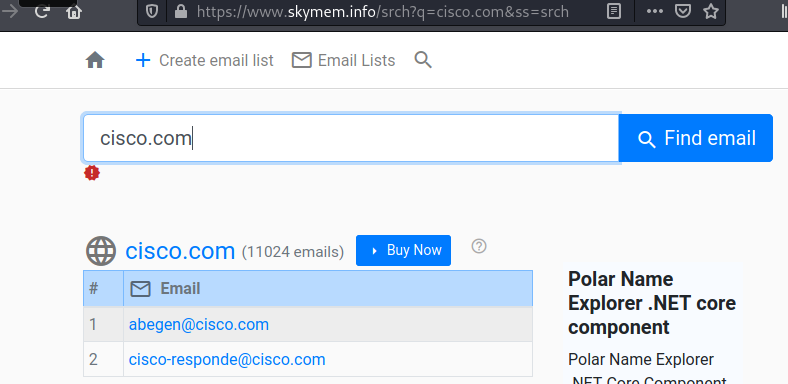
-Bu işlem için "hunter.io" bağlantısını kullanacağız.Normalde ücretli olan program için basic bir şekilde hesap oluşturmamız yeterli olacaktır.



-"hunter.io" bağlantısını tarayıcı üzerinde görüntülediğimizde bu şekildedir.



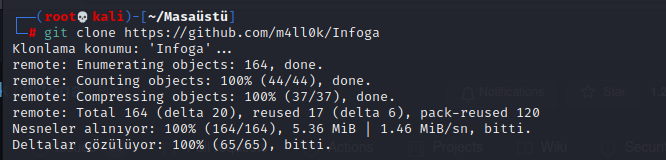
-"cisco.com" üzerinde bir tarama gerçekleştirdiğimiz de burada bulunan mail'leri görüntüleyebiliyoruz.



-Benzer işlemi "skymem.info" adresi üzerinden de gerçekleştirebiliriz.

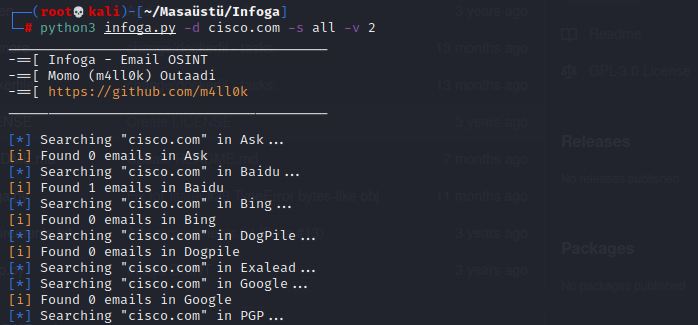


-Ayrıca Linux üzerinde kurulu olarak gelen TheHarvester aracı ile de bu işlemi gerçekleştirebiliriz.



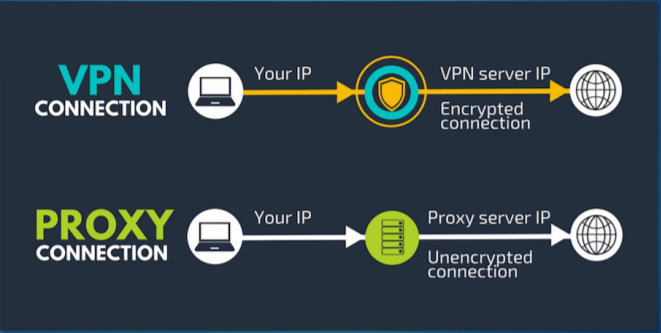
-Son olarakta Infoga isimli araç ile OSINT için bir işlem gerçekleştirmek istiyorum.

-Bu aracı "https://github.com/m4ll0k/Infoga" adresinden indirebiliriz.



-Aracın çalışma düzeni bu şekildedir buradan da OSINT Hakkında gerekli bilgiler alınabilir.

***Proxy&VPN Farkı***



-Proxy,çevrimiçi bir kaynağa erişmek isteyenler için aracılık eden servistir. İnternet erişimine aracılık eden vekil sunucular (proxy server) için yerleşik bir tanımdır.

-Proxy iletişimi şifresizdir; anonimlik (gizlilik) sağlamaz. Proxy sunucu gizlilik taahhüt etse bile, proxy sunucuya giderken akan trafik (ISP veya üçüncü aracılar tarafından) okunabilirdir.

-VPN,, iki uç arasındaki iletişimin şifrelendirildiği bir servistir. Bu şifrelendirilmiş kanala (hatta) tünel adı verilir.

-VPN trafiği, VPN sunucusuna kadar okunur değildir.

-Her iki serviste de IP değişikliği sağlanır.

-Her iki serviste de sunucu üzerinde kayıt(log) alımı ve izleme(monitöring) yapabilir.