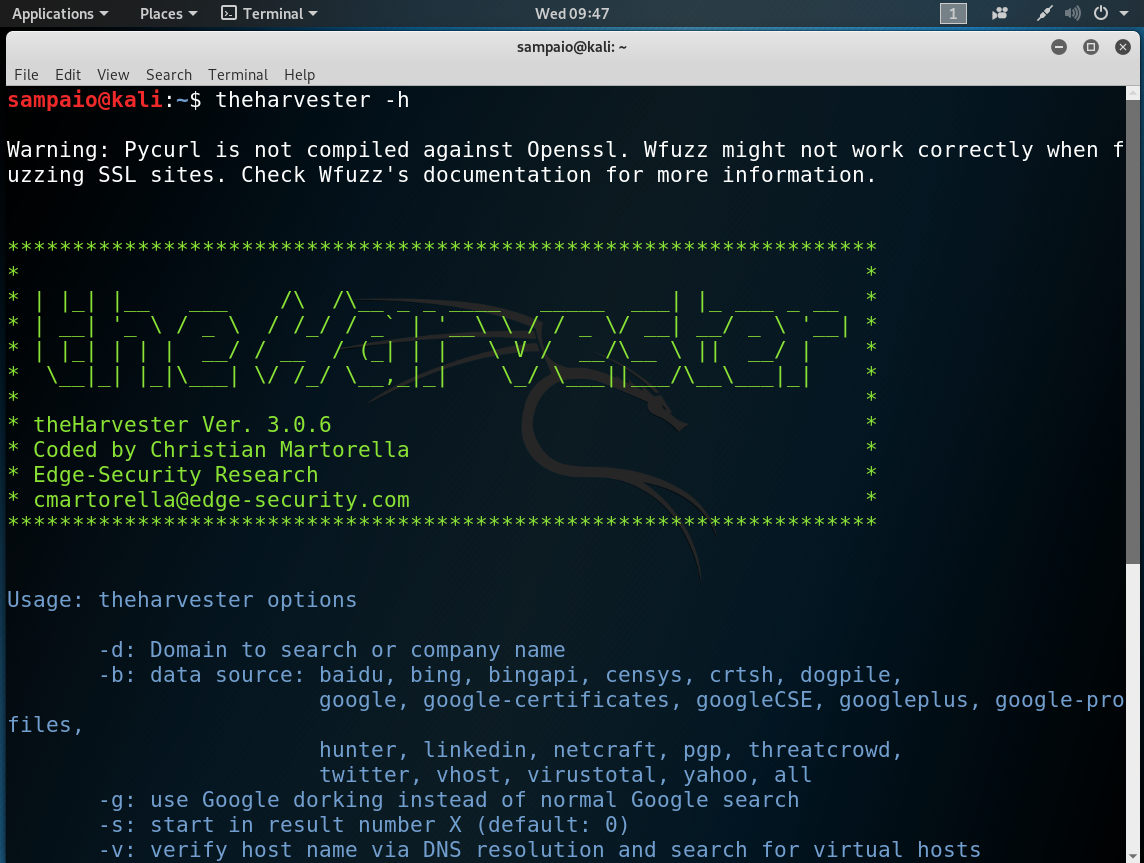
**TheHarvester Nedir? Ne İşe Yarar?**

TheHarvester, e-postalar, alt alan adları, sunucular ve URL'ler gibi bilgileri herkese açık kaynaklardan toplamak için tasarlanmış güçlü bir açık kaynaklı istihbarat (OSINT) aracıdır. Penetrasyon test uzmanları, güvenlik araştırmacıları ve etik hackerlar tarafından hedef alan adı veya kuruluş hakkında veri toplamak için yaygın olarak kullanılır. Bu kılavuzda, Kali Linux'ta TheHarvester'ı nasıl kuracağınızı, yapılandıracağınızı ve kullanacağınızı adım adım anlatacağız.



**TheHarvester nedir?**

TheHarvester, aşağıdakiler de dahil olmak üzere çeşitli kamu kaynaklarından veri toplayan bir keşif aracıdır:

* Arama motorları (Google, Bing, DuckDuckGo, vb.)
* PGP anahtar sunucuları
* Sosyal medya platformları
* DNS kayıtları
* Shodan (IoT arama motoru)
* Tehdit istihbarat platformları (örneğin, AlienVault OTX)
* Ve daha fazlası.

Özellikle bir penetrasyon testinin veya güvenlik değerlendirmesinin ilk aşamalarında bilgi toplamak için oldukça faydalıdır.

**TheHarvester'ı Kali Linux'a Kurmak**

TheHarvester, Kali Linux'ta önceden yüklü olarak gelir. Ancak yüklü değilse veya güncellemek istiyorsanız, şu adımları izleyin:

**Sisteminizi Güncelleyin:**

sudo apt update

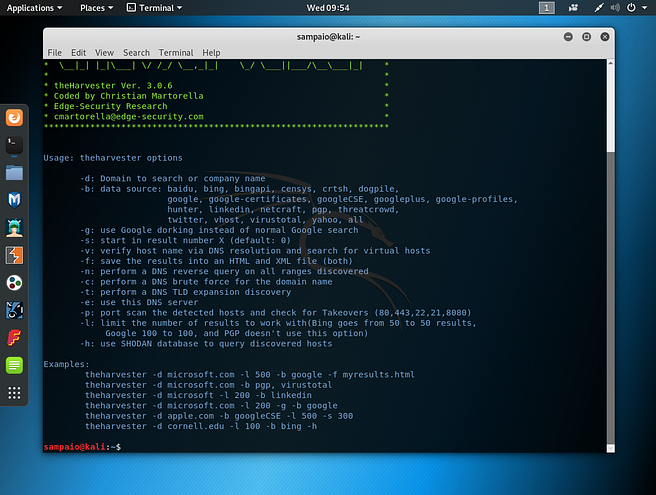
**TheHarvester'ı yükleyin:**

sudo apt install theharvester

**Kurulumu Doğrulayın:**

theharvester -h

Bu komut, aracın kurulu olduğunu ve kullanıma hazır olduğunu onaylayan yardım menüsünü görüntüler.



**TheHarvester'ın Temel Kullanımı**

TheHarvester bir komut satırı aracıdır ve temel sözdizimi aşağıdaki gibidir:

theharvester -d <alan> -b <veri\_kaynağı> -f <çıktı\_dosyası>

**Ana Seçenekler:**

* **d** <alan adı>: Hedef alan adını belirtin (örneğin, example.com).
* **b** <data\_source>: Kullanılacak veri kaynağını belirtin (örneğin, google, bing, all).
* **f** <çıktı\_dosyası>: Sonuçları bir dosyaya kaydedin (örneğin, output.xml).
* **l** <limit>: Sonuç sayısını sınırla (varsayılan 500'dür).
* **s** : DNS kaba kuvvet araması gerçekleştir.
* **v** : VirtualHost doğrulama özelliğini kullanın.
* **h** : Yardım menüsünü görüntüler.

**Adım Adım Örnekler**

**1. E-postaları ve Alt Alan Adlarını Toplama**

Google'ı veri kaynağı olarak kullanarak hedef alan adına ait e-postaları ve alt alan adlarını toplamak için:

theharvester -d example.com -b google -f output.txt

Bu komut Google'ı kullanarak example.com ile ilgili e-postaları ve alt alan adlarını arayacak ve sonuçları output.txt dosyasına kaydedecektir.

**2. Birden Fazla Veri Kaynağının Kullanılması**

Birden fazla veri kaynağı kullanmak için (örneğin Google, Bing ve LinkedIn):

theharvester -d example.com -b google,bing,linkedin -f output.xml

**3. DNS Kaba Kuvvet Araması Gerçekleştirme**

Alt etki alanları için DNS kaba kuvvet araması yapmak için:

theharvester -d example.com -b all -s -f output.txt

-s bayrağı, ortak önekleri (örneğin, mail.example.com, ftp.example.com) deneyerek alt etki alanlarını keşfetmeye çalışan DNS kaba kuvvet özelliğini etkinleştirir.

**4. Sonuç Sayısını Sınırlandırma**

Sonuç sayısını 100 ile sınırlamak için:

theharvester -d example.com -b google -l 100 -f output.txt

**5. VirtualHost Doğrulaması**

Keşfedilen IP adresleri için VirtualHosts'u doğrulamak için:

theharvester -d example.com -b all -v -f output.txt

-v bayrağı, keşfedilen IP adreslerinin birden fazla etki alanına ev sahipliği yapıp yapmadığını kontrol eden VirtualHost doğrulamasını etkinleştirir.

**Gelişmiş Kullanım**

**1. IoT Keşfi için Shodan Kullanımı**

Shodan'ı veri kaynağı olarak kullanmak için bir Shodan API anahtarına ihtiyacınız var. Anahtarı aldıktan sonra şu komutu çalıştırın:

theharvester -d example.com -b shodan -s -f output.txt

Shodan, özellikle hedef etki alanıyla ilişkili IoT cihazlarını ve açık portları keşfetmek için kullanışlıdır.

**2. AlienVault OTX Kullanımı**

AlienVault OTX'ten tehdit istihbarat verilerini toplamak için:

theharvester -d example.com -b otx -f output.txt

**3. Sonuçları Farklı Formatlarda Dışa Aktarma**

TheHarvester, XML, JSON ve HTML dahil olmak üzere birden fazla çıktı biçimini destekler. Örneğin, sonuçları JSON formatında dışa aktarmak için:

theharvester -d example.com -b all -f output.json

**Çıktıyı Analiz Etme**

TheHarvester, toplanan verileri içeren çıktı dosyaları oluşturur. Çıktıyı cat, grep veya less gibi araçlar kullanarak analiz edebilirsiniz:

**1. Çıktıyı Görüntüle:**

cat çıktısı.txt

**2. E-postaları Filtrele:**

cat çıktı.txt | grep “@example.com”

**3. Alt Alan Adlarını Filtrele:**

cat çıktı.txt | grep “example.com”

**Etkili Kullanım İçin İpuçları**

Veri Kaynaklarını Birleştirin: Kapsamlı sonuçlar için birden fazla veri kaynağı kullanın (-b **all ).**

Proxy Kullanın: Arama motorları tarafından engelleniyorsanız, TheHarvester'ı bir proxy kullanacak şekilde yapılandırın.

Betiklerle Otomatikleştirin: Otomatik veri toplama için TheHarvester'ı keşif betiklerinize entegre edin.

**Çözüm:**

TheHarvester, Kali Linux'ta OSINT ve keşif için olmazsa olmaz bir araçtır. Yeteneklerinden yararlanarak, hedefiniz hakkında daha ileri analiz veya sızma testleri için kullanılabilecek değerli bilgiler toplayabilirsiniz. Bu aracı sorumlu bir şekilde ve yasal sınırlar dahilinde kullanmayı unutmayın.