**Dmitry Nedir?**

**Dmitry** (tam adıyla **Deepmagic Information Gathering Tool**), bilgisayar ve ağ güvenliği alanında kullanılan açık kaynaklı bir bilgi toplama aracıdır. Temelde, bir hedef sistem veya web sitesi hakkında hızlıca bilgi toplamak için kullanılır.



**Dmitry Ne İşe Yarar?**

Bir bilgisayara veya ağa saldırmadan önce, o sistemle ilgili olabildiğince fazla bilgi toplamak çok önemlidir. Dmitry, bu bilgi toplama sürecini kolaylaştırır ve otomatikleştirir. Şöyle çalışır:

* Bir web sitesi veya IP adresi verildiğinde,
* O sistem hakkında temel bilgileri toplar,
* Örneğin o sistemin açık portlarını, çalışan servisleri,
* İletişim bilgilerini (eğer varsa),
* Hangi işletim sistemini kullandığını,
* Ve bazı durumlarda kullanıcı adlarını bile araştırabilir.

**Dmitry’nin Özellikleri**

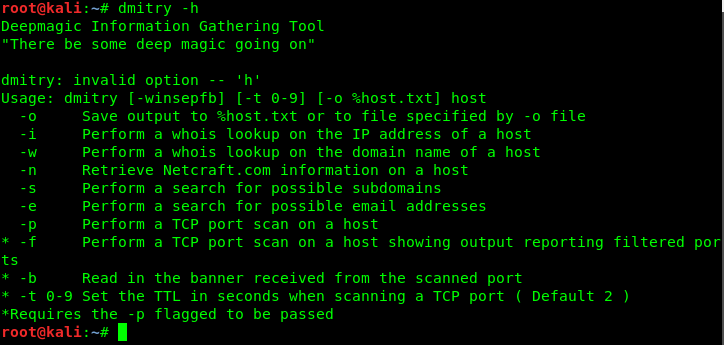
* **Port taraması:** Hedefte açık olan ağ portlarını kontrol eder.
* **WHOIS sorgulama:** Hedefin alan adı veya IP bilgilerini, kime ait olduğunu bulur.
* **E-posta adresi ve kullanıcı adı bulma:** Hedef sistemle ilişkili olabilecek e-posta veya kullanıcı adlarını arar.
* **Traceroute:** Hedefe giden yolu haritalar.
* **Basit ve hızlı:** Komut satırından kolayca çalıştırılır ve hızlı sonuç verir.

**Neden Kullanılır?**

* **Sızma testlerinde:** Etik hackerlar, yani güvenlik uzmanları, sisteme saldırmadan önce hedef hakkında bilgi toplamak için kullanır.
* **Güvenlik değerlendirmelerinde:** Sistemlerin açıkları olup olmadığını anlamak için bilgi toplanır.
* **Araştırma ve analizde:** İnternet üzerindeki sistemler hakkında genel bilgi edinmek için tercih edilir.

**Dmitry Aracının Arayüzü :**

1. Aracımızı açtıktan sonra kullanımı ile ilgili karşımıza böyle bir pencere açılacaktır.



usage (Kullanımı): dmitry -winsepfb " hakkında bilgi toplanacak site url'si "   
-o /root/Desktop/sitebilgi.txt

**Buradaki " -o " nun amacı yaptığımız bilgi taramasındaki çıkan .txt uzantılı çıktı belgesini nereye kaydedeceğimizi göstermemize olanak sağlar.**

Örnek Kullanımı : dmitry -winsepfb “site url” -o /root/Desktop/bilgi

**(buradaki -winsepfb aşağıdaki açıklamadaki harflerdir. Yani site hakkında bütün bilgileri bize gösterir. İsteğe bağlı tek harf de kullanılabilir.)**

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host (Her araçta olduğu gibi kullanımına dair bilgi gösterir)

**-o = Save output to %host.txt or to file specified by -o file (site hakında toplanan bilgileri .txt dosyasının kaydedeceği yeri gösterir)**

**-i = Perform a whois lookup on the IP address of a host (Bir sunucu IP adresinden who is araması yapar)**

**-w = Perform a whois lookup on the domain name of a host (Bilgisayarların etki alanı hakkında whois sorgusu yapar)**

**-n = Retrieve Netcraft.com information on a host (Bir ana bilgisayardaki Netcraft bilgilerini alır.)**

**-s = Perform a search for possible subdomains (Olası alt alanlar için bir arama yapar)**

**-e = Perform a search for possible email addresses(e-posta adreslerini arar)**

**-p = Perform a TCP port scan on a host (Ana bilgisayarda bir TCP port taraması gerçekleştirir)**

**-f = Perform a TCP port scan on a host showing output reporting filtered ports (Çıktı raporlamasını ve bağlantı noktalarını gösteren bir ana bilgisayarda TCP bağlantı noktası taraması gerçekleştirir)**

**-b = Read in the banner received from the scanned port (Taranan bağlantı noktasından alınan şeridi oku)**

**-t = 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 ) (Bir TCP portu tararken TTL'yi saniye cinsinden ayarlar )**