

Subdomain Enumeration

Task 1 Brief (Kısa)

Alt alan adı numaralandırma, bir alan adı için geçerli alt alan adlarını bulma işlemidir, peki bunu neden yapıyoruz? Bunu, daha fazla potansiyel güvenlik açığı noktası keşfetmek amacıyla saldırı yüzeyimizi genişletmek için yaparız.

Üç farklı alt alan adı numaralandırma yöntemini inceleyeceğiz: Brute Force, OSINT (Açık Kaynak İstihbaratı) ve Virtual Host.

Makineyi çalıştırın ve ardından bir sonraki göreve geçin.

soru ⇒ **B ile başlayan bir alt alan numaralandırma yöntemi nedir?**

cevap ⇒ **Brute Force**

soru ⇒ **O ile başlayan bir alt alan numaralandırma yöntemi nedir?**

cevap ⇒ **OSINT**

soru ⇒ **V ile başlayan bir alt alan numaralandırma yöntemi nedir?**

cevap ⇒ **Virtual Host**

Task 2 OSINT - SSL/TLS Certificates (OSINT - SSL/TLS Sertifikaları)

SSL/TLS Sertifikaları

Bir CA (Sertifika Yetkilisi) tarafından bir alan adı için SSL/TLS (Secure Sockets Layer/Transport Layer Security) sertifikası oluşturulduğunda, CA'lar "Sertifika Şeffaflığı (CT) günlükleri" olarak adlandırılan günlüklerde yer alır. Bunlar, bir alan adı için oluşturulan her SSL/TLS sertifikasının halka açık günlükleridir. Sertifika Şeffaflığı günlüklerinin amacı, kötü niyetli ve yanlışlıkla oluşturulmuş sertifikaların kullanılmasını engellemektir. Bir alan adına ait alt alanları keşfetmek için bu hizmeti kendi avantajımıza kullanabiliriz, <https://crt.sh> ve

<https://ui.ctsearch.entrust.com/ui/ctsearchui> gibi siteler, güncel ve geçmiş sonuçları gösteren aranabilir bir sertifika veritabanı sunar.

crt.sh adresine gidin ve tryhackme.com alan adını arayın, 2020-12-26 tarihinde kaydedilen girişi bulun ve soruyu yanıtlamak için aşağıdaki alan adını girin.

soru ⇒ 2020-12-26'da crt.sh'de hangi alan adı günlüğe kaydedildi?

cevap ⇒ store.tryhackme.com

Task 3 OSINT - Search Engines (Arama Motorları)

Arama Motorları

Arama motorları bir milyardan fazla web sitesine ait trilyonlarca bağlantı içerir ve bu da yeni alt alan adları bulmak için mükemmel bir kaynak olabilir. Google gibi web sitelerinde site: filtresi gibi gelişmiş arama yöntemlerini kullanmak arama sonuçlarını daraltabilir. Örneğin, "-site:www.domain.com site:*.domain.com" yalnızca domain.com alan adına yönlendiren sonuçları içerir, ancak www.domain.com'a herhangi bir bağlantıyı hariç tutar; bu nedenle, bize yalnızca domain.com'a ait alt alan adlarını gösterir.

Google'a gidin ve -site:www.tryhackme.com site:*.tryhackme.com arama terimini kullanın, bu tryhackme.com için bir alt alan adı ortaya çıkaracaktır; aşağıdaki soruyu yanıtlamak için bu alt alan adını kullanın.

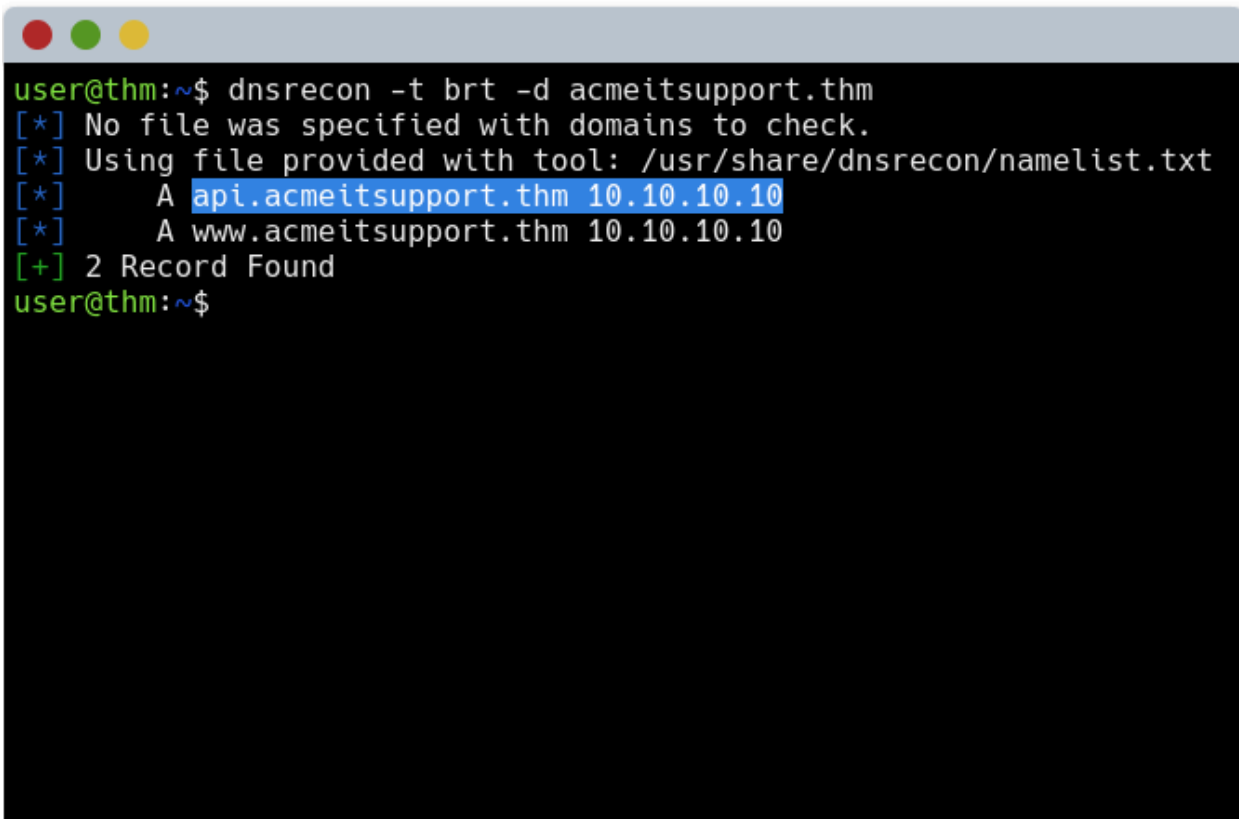
soru ⇒ Yukarıdaki Google araması kullanılarak keşfedilen S ile başlayan TryHackMe alt alan adı nedir?

cevap ⇒ store.tryhackme.com

Task 4 DNS Bruteforce (DNS Bruteforce)

Bruteforce DNS (Alan Adı Sistemi) numaralandırma, yaygın olarak kullanılan alt alan adlarının önceden tanımlanmış bir listesinden onlarca, yüzlerce, binlerce ve hatta milyonlarca farklı olası alt alan adını deneme yöntemidir. Bu yöntem çok

sayıda istek gerektirdiğinden, süreci daha hızlı hale getirmek için araçlarla otomatikleştiriyoruz. Bu örnekte, bunu gerçekleştirmek için dnsrecon adlı bir araç kullanıyoruz. Statik siteyi açmak için "View Site" düğmesine tıklayın, simülasyonu başlatmak için "Run DNSrecon Request" düğmesine basın ve ardından aşağıdaki soruyu yanıtlayın.

A terminal window with a dark background and light green text. The window has three colored window control buttons (red, green, yellow) in the top-left corner. The text inside the terminal shows a command being executed and its output.

```
user@thm:~$ dnsrecon -t brt -d acmeitsupport.thm
[*] No file was specified with domains to check.
[*] Using file provided with tool: /usr/share/dnsrecon/namelist.txt
[*]      A api.acmeitsupport.thm 10.10.10.10
[*]      A www.acmeitsupport.thm 10.10.10.10
[+] 2 Record Found
user@thm:~$
```

soru ⇒ dnsrecon aracı ile bulunan ilk alt alan adı nedir?

cevap ⇒ api.acmeitsupport.thm

Task 5 OSINT - Sublist3r

Sublist3r Kullanarak Otomasyon

OSINT alt alan adı keşif sürecini hızlandırmak için, Sublist3r gibi araçların yardımıyla yukarıdaki yöntemleri otomatikleştirebiliriz, statik siteyi açmak için

"Siteyi Görüntüle" düğmesine tıklayın ve aşağıdaki soruyu yanıtlamaya yardımcı olacak yeni bir alt alan adı keşfetmek için sublist3r simülasyonunu çalıştırın.

```
[_] _____  
[_] | _ )|_|_|_|_|_)|_|_|_\__\___)|_|_|_  
[_] |_|_|/_\_|\_|_|_|_|_|_|_|_|_|_|_|_|_|
```

Coded By Ahmed Aboul-Ela - @aboul3la

```
[_] Enumerating subdomains now for acmeitsupport.thm  
[-] Searching now in Baidu..  
[-] Searching now in Yahoo..  
[-] Searching now in Google..  
[-] Searching now in Bing..  
[-] Searching now in Ask..  
[-] Searching now in Netcraft..  
[-] Searching now in Virustotal..  
[-] Searching now in ThreatCrowd..  
[-] Searching now in SSL Certificates..  
[-] Searching now in PassiveDNS..  
[-] Searching now in Virustotal..  
[-] Total Unique Subdomains Found: 2  
web55.acmeitsupport.thm  
www.acmeitsupport.thm  
user@thm:~$
```

soru ⇒ sublist3r tarafından keşfedilen ilk alt alan adı nedir?

cevap ⇒ web55.acmeitsupport.thm

Task 6 Virtual Hosts (Sanal Ana Bilgisayarlar)

Bir web uygulamasının geliştirme sürümleri veya yönetim portalları gibi bazı alt alan adları her zaman genel erişime açık DNS sonuçlarında barındırılmaz. Bunun yerine, DNS kaydı özel bir DNS sunucusunda tutulabilir veya geliştiricinin makinelerinde alan adlarını IP adresleriyle eşleyen /etc/hosts dosyasına (veya Windows kullanıcıları için c:\windows\system32\drivers\etc\hosts dosyasına) kaydedilebilir.

Web sunucuları bir istemciden bir web sitesi talep edildiğinde tek bir sunucudan birden fazla web sitesi barındırabildiğinden, sunucu istemcinin Host başlığından hangi web sitesini istediğini bilir. Bu ana bilgisayar başlığında değişiklik yaparak ve yeni bir web sitesi keşfedip keşfetmediğimizi görmek için yanıtı izleyerek kullanabiliriz.

DNS Bruteforce'da olduğu gibi, yaygın olarak kullanılan alt alan adlarından oluşan bir kelime listesi kullanarak bu işlemi otomatikleştirebiliriz.

Bir AttackBox başlatın ve ardından yeni bir alt alan adı bulmaya çalışmak için Acme IT Support makinesine karşı aşağıdaki komutu deneyin.

Yukarıdaki komut, kullanacağımız kelime listesini belirtmek için -w anahtarını kullanır. H anahtarı bir başlık ekler/düzenler (bu örnekte Host başlığı), bir alt alan adının normalde gideceği yerde FUZZ anahtar sözcüğümüz vardır ve burası kelime listesindeki tüm seçenekleri deneyeceğimiz yerdir.

Yukarıdaki komut her zaman geçerli bir sonuç üreteceğinden, çıktıyı filtrelememiz gerekir. Bunu -fs anahtarı ile sayfa boyutu sonucunu kullanarak yapabiliriz.

Aşağıdaki komutu {size} yerine bir önceki sonuçtan en çok çıkan boyut değerini koyarak düzenleyin ve AttackBox üzerinde deneyin.

Bu komut, ffuf'a belirtilen boyuttaki sonuçları göz ardı etmesini söyleyen -fs anahtarı dışında ilkinde benzer bir sözdizimine sahiptir.

Yukarıdaki komut, daha önce karşılaşmadığımız iki olumlu sonucu ortaya çıkarmış olmalıdır.

soru ⇒ Keşfedilen ilk alt alan adı nedir?

cevap ⇒ delta

soru ⇒ Bulunan ikinci alt alan adı nedir?

cevap ⇒ yellow